Commencez

Setup and administration

NetApp
April 26, 2024

Sommaire

Commencez

Découvrez les bases

En savoir plus sur BlueXP

NetApp BlueXP fournit à votre entreprise un plan de contrôle unique qui vous permet de créer, de protéger et de régir les données dans vos environnements sur site et cloud. La plateforme SaaS BlueXP inclut des services de gestion du stockage, de mobilité des données, de protection, d'analyse et de contrôle des données. Les fonctionnalités de gestion sont fournies via une console Web et des API.

Caractéristiques

La plateforme BlueXP offre quatre piliers fondamentaux pour la gestion des données : stockage, mobilité, protection, analyse et contrôle.

Stockage

Découvrez, déployez et gérez le stockage, que ce soit dans AWS, Azure, Google Cloud ou sur site.

- Configuration et utilisation "Cloud Volumes ONTAP" pour une gestion efficace des données multiprotocole sur l'ensemble des clouds.
- Configurez et utilisez les services cloud de stockage de fichiers :
  - "Azure NetApp Files"
  - "Amazon FSX pour ONTAP"
  - "Cloud Volumes Service pour Google Cloud"
- Détection et gestion "le stockage sur site":
  - Systèmes E-Series
  - Clusters ONTAP
  - Systèmes StorageGRID

Mobilité

Déplacez vos données là où vous en avez besoin grâce à la synchronisation, la copie, le Tiering et la mise en cache.

- "Copie et synchronisation"
- "La mise en cache en périphérie"
- "Tiering"

La protection

Utilisez des mécanismes de protection automatisés pour protéger vos données contre les pertes de données, les pannes imprévues, les ransomware et autres cybermenaces.

- "Sauvegarde et restauration"
- "La réplication"

- "Protection des données pour les workloads Kubernetes"

Analyse et contrôle

Utilisez des outils pour surveiller, cartographier et optimiser votre infrastructure et votre stockage de données. Bénéficiez d'informations exploitables pour optimiser l'état, la résilience et les coûts du stockage.

- "Classement"
- "Conseiller digital"
- "Efficacité économique"
- "Résilience opérationnelle"

"Découvrez comment utiliser BlueXP pour aider votre entreprise"

Fournisseurs cloud pris en charge

BlueXP vous permet de gérer le stockage cloud et d'utiliser les services cloud dans Amazon Web Services, Microsoft Azure et Google Cloud.

Le coût

Le prix de BlueXP dépend des services que vous prévoyez d'utiliser. "En savoir plus sur les tarifs BlueXP"

Fonctionnement de BlueXP

BlueXP inclut une console web fournie via la couche SaaS, des comptes fournissant une colocation, et des connecteurs qui gèrent les environnements de travail et permettent les services cloud BlueXP.

Services à la demande

BlueXP est accessible via un "console web" Et les API. Cette expérience SaaS vous permet d'accéder automatiquement aux dernières fonctionnalités dès leur sortie et de basculer facilement entre vos comptes BlueXP et les connecteurs.

Compte BlueXP

Lorsque vous vous connectez à BlueXP pour la première fois, vous êtes invité à créer un compte *BlueXP*. Ce compte fournit la colocation et vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés.

"En savoir plus sur les comptes".

Connecteurs

Vous n'avez pas besoin d'un connecteur pour démarrer avec BlueXP, mais vous devez créer un connecteur pour déverrouiller toutes les fonctionnalités et tous les services BlueXP. Un connecteur vous permet de gérer les ressources et les processus dans vos environnements sur site et cloud. Il est nécessaire de gérer les environnements de travail (par exemple, les clusters ONTAP Cloud Volumes ONTAP et sur site) et d'utiliser de nombreux services de données BlueXP.

"En savoir plus sur les connecteurs".

Mode restreint et mode privé

BlueXP est également pris en charge dans les environnements soumis à des restrictions de sécurité et de connectivité. Vous pouvez utiliser *restricted mode* ou *private mode* pour limiter la connectivité sortante à la couche SaaS de BlueXP.

"En savoir plus sur les modes de déploiement BlueXP".

Certification SOC 2 Type 2

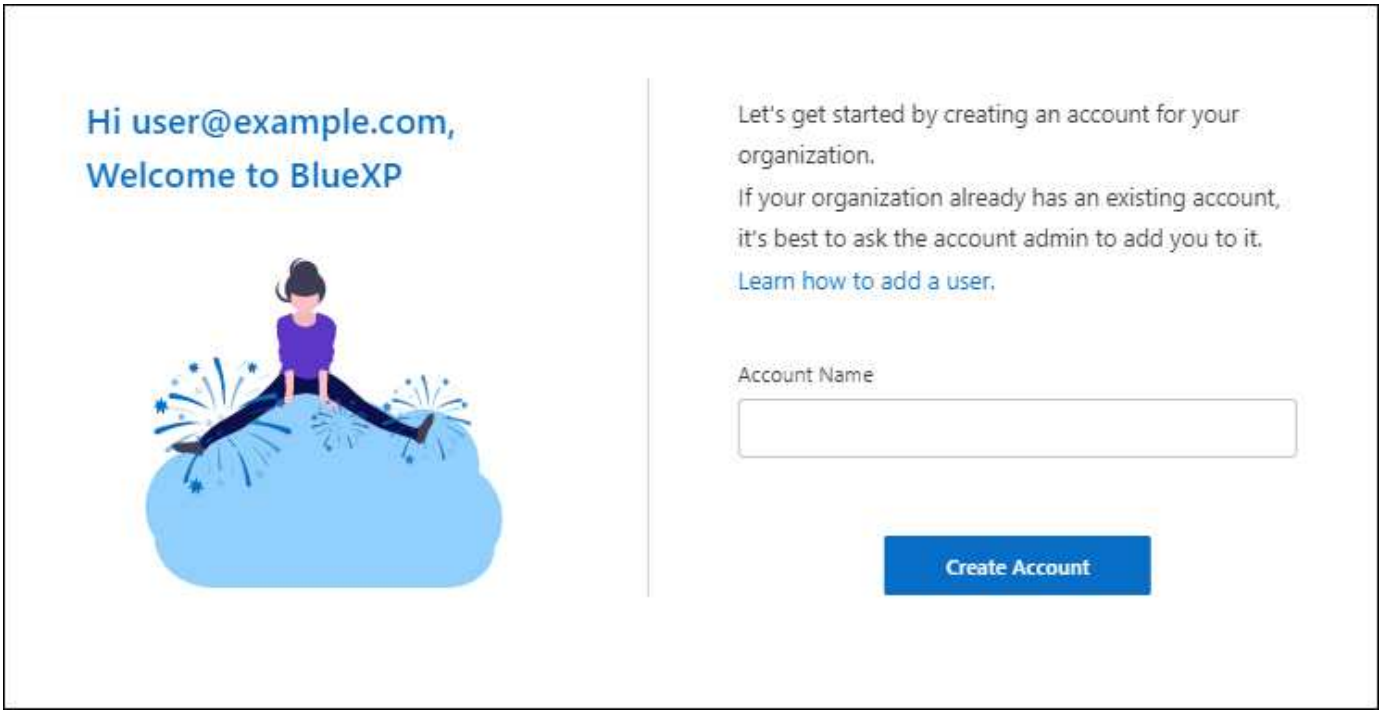
Un comptable public indépendant et un vérificateur des services ont examiné BlueXP et confirmé qu'il a obtenu des rapports SOC 2 de type 2 en fonction des critères des services de fiducie applicables.

"Consultez les rapports SOC 2 de NetApp"

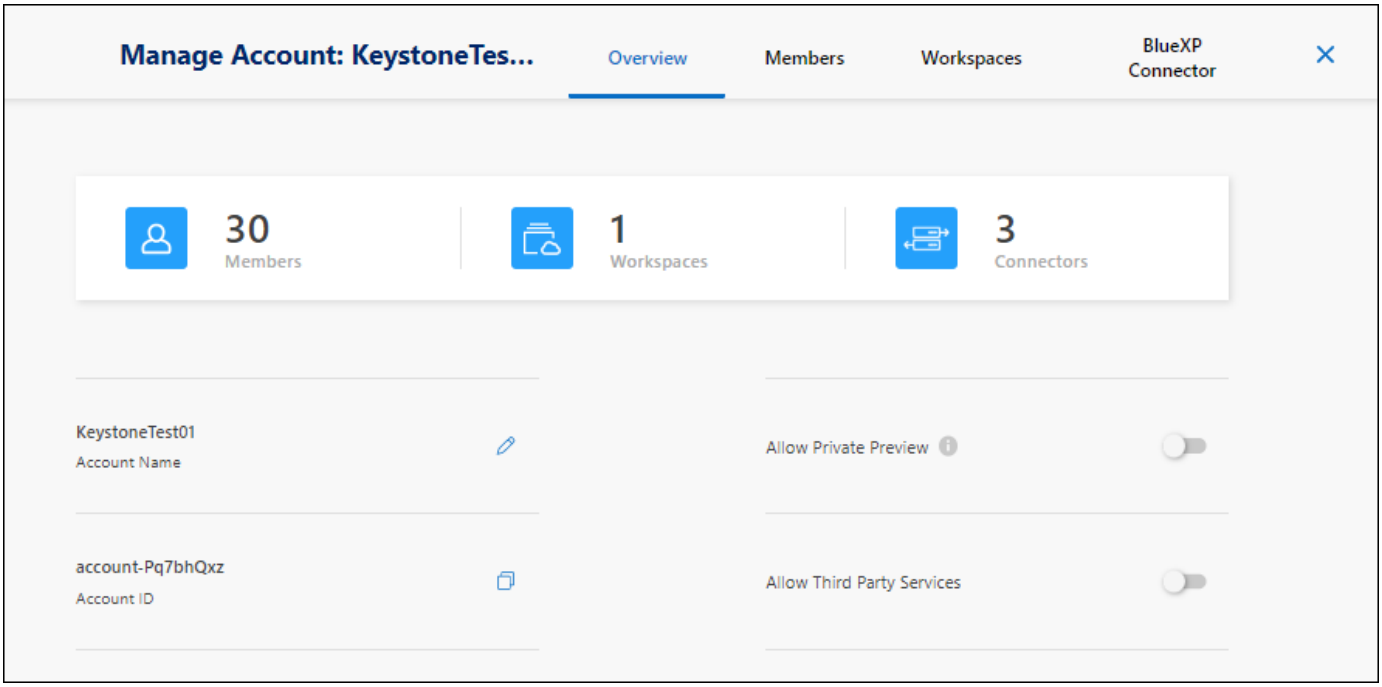
Découvrez les comptes BlueXP

Un compte *BlueXP* fournit une colocation pour votre entreprise, qui vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés. Par exemple, un groupe d'utilisateurs peut déployer et gérer des environnements de travail Cloud Volumes ONTAP dans un espace de travail qui n'est pas visible pour les utilisateurs qui gèrent des environnements de travail dans un autre espace de travail.

Lors de votre premier accès à BlueXP, vous êtes invité à sélectionner ou à créer un compte. Par exemple, l'écran suivant s'affiche si vous n'avez pas encore de compte :



Les administrateurs de compte BlueXP peuvent ensuite modifier les paramètres de ce compte en gérant les utilisateurs (membres), les espaces de travail et les connecteurs :



"Découvrez comment gérer votre compte BlueXP".

Modes de déploiement

BlueXP propose pour votre compte les modes de déploiement suivants : mode standard, mode restreint et mode privé. Ces modes prennent en charge les environnements présentant différents niveaux de sécurité et de restrictions de connectivité.

"En savoir plus sur les modes de déploiement BlueXP".

Membres

Les membres sont des utilisateurs BlueXP que vous associez à votre compte BlueXP. L'association d'un utilisateur à un compte et d'un ou plusieurs espaces de travail dans ce compte permet à ces utilisateurs de créer et de gérer des environnements de travail dans BlueXP.

Lorsque vous associez un utilisateur, vous lui attribuez un rôle :

- *Account Admin*: Peut effectuer n'importe quelle action dans BlueXP.
- *Workspace Admin* : permet de créer et de gérer des ressources dans l'espace de travail affecté.
- *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.

"En savoir plus sur ces rôles".

Espaces de travail

Dans BlueXP, un espace de travail isole tous les *environnements de travail* des autres utilisateurs du compte. Les administrateurs de l'espace de travail ne peuvent pas accéder aux environnements de travail dans un espace de travail à moins que l'administrateur du compte n'associe l'administrateur à cet espace de travail.

Un environnement de travail représente un système de stockage. Par exemple :

- Un système Cloud Volumes ONTAP
- Un cluster ONTAP sur site
- Un cluster Kubernetes

"Découvrez comment ajouter un espace de travail".

Connecteurs

Un connecteur exécute les actions que BlueXP doit effectuer pour gérer votre infrastructure de données. Le connecteur s'exécute sur une instance de machine virtuelle que vous déployez auprès de votre fournisseur cloud ou sur un hôte sur site que vous avez configuré.

Vous pouvez utiliser un connecteur avec plusieurs services BlueXP. Par exemple, si vous utilisez un connecteur pour gérer Cloud Volumes ONTAP, vous pouvez utiliser ce même connecteur avec un autre service tel que le Tiering BlueXP.

"En savoir plus sur les connecteurs".

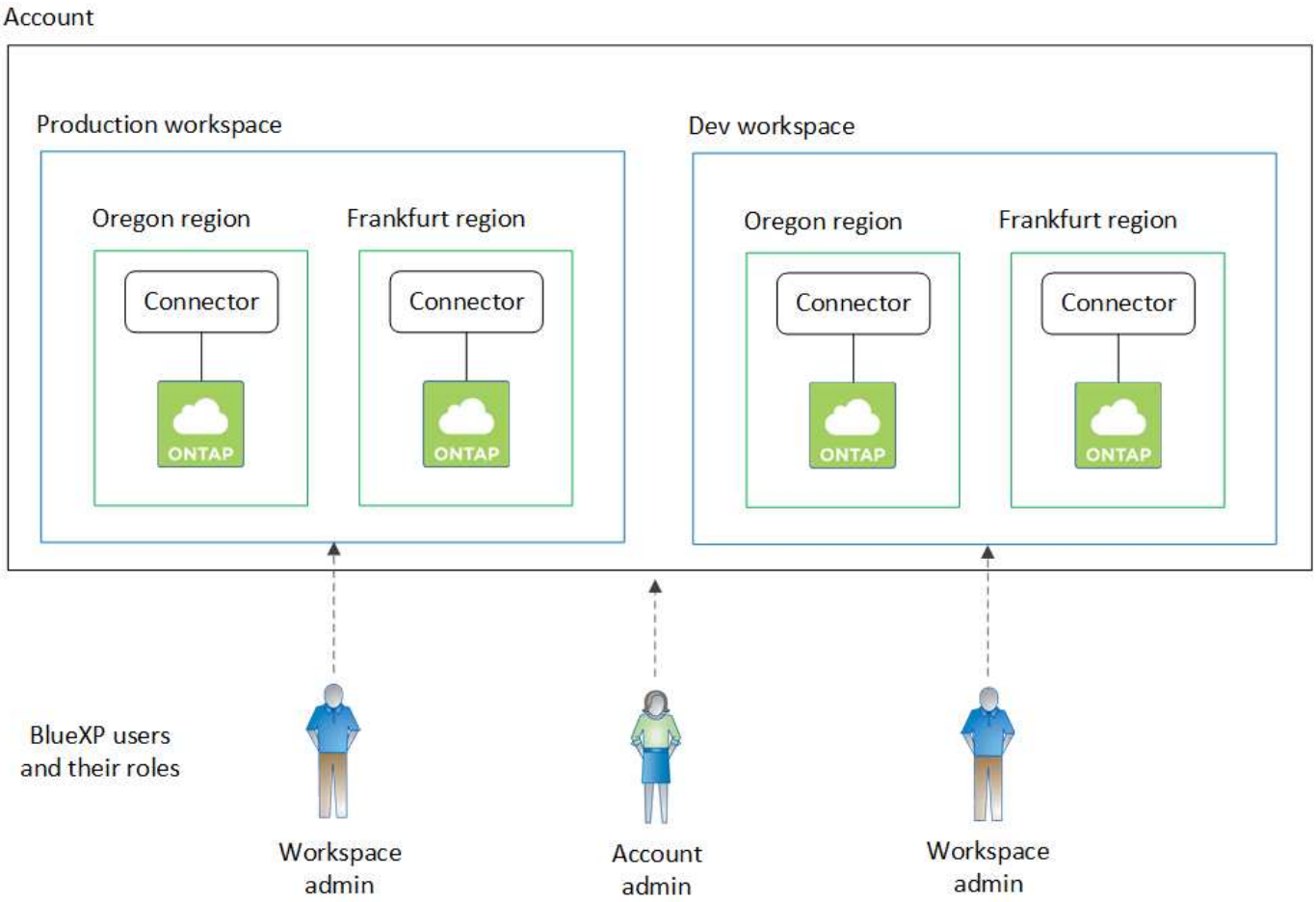
Exemples

Les exemples suivants décrivent comment configurer vos comptes.

> Dans les deux exemples d'images qui suivent, le connecteur et les systèmes Cloud Volumes ONTAP ne résident pas *dans* le compte BlueXP—ils s'exécutent dans un fournisseur cloud. Il s'agit d'une représentation conceptuelle de la relation entre chaque composant.

Plusieurs espaces de travail

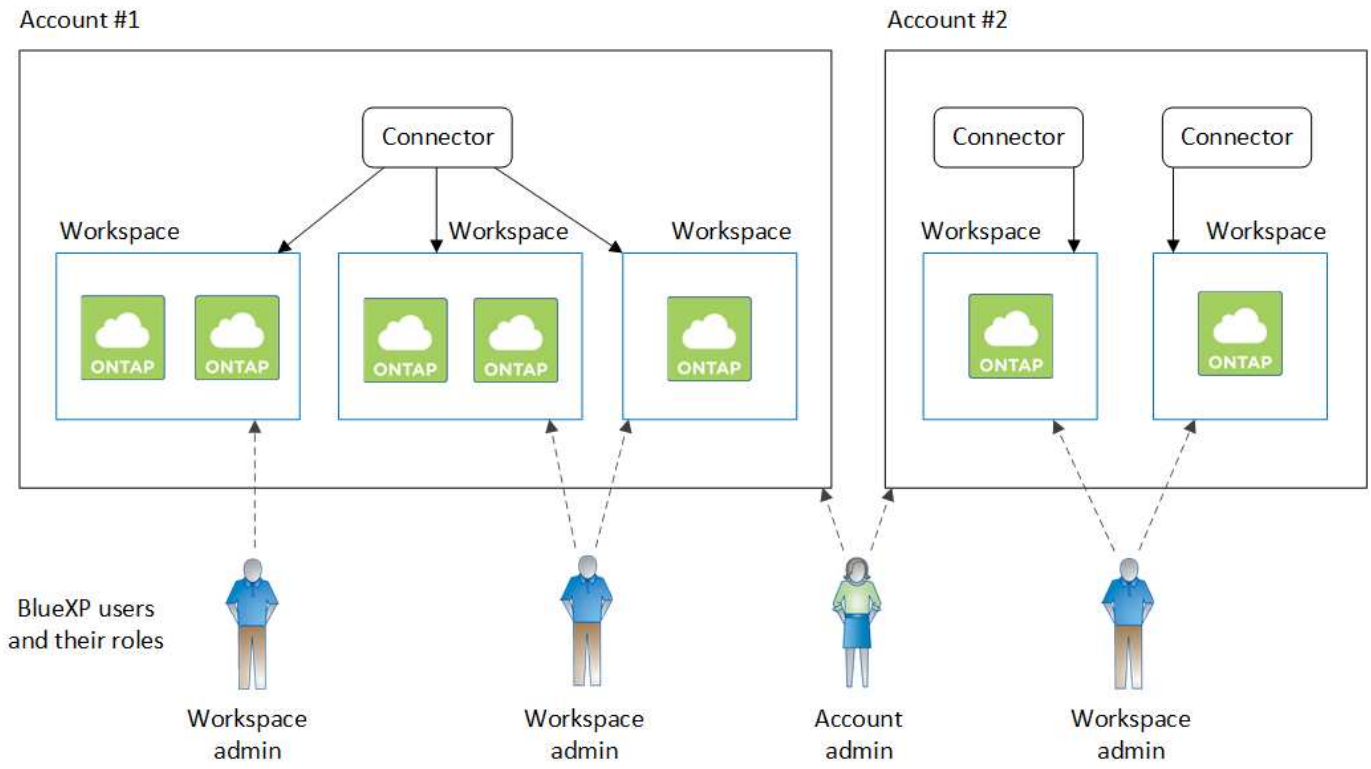
L'exemple suivant montre un compte qui utilise deux espaces de travail pour créer des environnements isolés. Le premier espace de travail est pour un environnement de production et le second pour un environnement de développement.



Plusieurs comptes

Voici un autre exemple illustrant le niveau le plus élevé de colocation grâce à l'utilisation de deux comptes BlueXP distincts. Par exemple, un fournisseur de services peut utiliser BlueXP pour fournir des services à ses clients, tout en utilisant un autre compte pour fournir une reprise après incident pour l'une de ses unités commerciales.

Notez que le compte 2 comprend deux connecteurs distincts. Cela peut arriver si vous disposez de systèmes dans des régions distinctes ou dans des fournisseurs cloud distincts.



En savoir plus sur les connecteurs

Un *connecteur* est un logiciel NetApp s'exécutant dans votre réseau cloud ou sur site. Il exécute les actions que BlueXP doit exécuter pour gérer votre infrastructure de données. Le connecteur interroge constamment la couche SaaS BlueXP afin de détecter les actions à entreprendre. Vous n'avez pas besoin d'un connecteur pour démarrer avec BlueXP, mais vous devez créer un connecteur pour déverrouiller toutes les fonctionnalités et tous les services BlueXP.

Ce que vous pouvez faire sans connecteur

Il n'est pas nécessaire de disposer d'un connecteur pour démarrer avec BlueXP. Vous pouvez utiliser plusieurs fonctionnalités et services au sein de BlueXP sans créer de connecteur.

Vous pouvez utiliser les fonctionnalités et services BlueXP suivants sans connecteur :

- Création d'un environnement de travail Amazon FSX pour NetApp ONTAP

  Aucun connecteur n'est nécessaire pour créer un environnement de travail, mais il est nécessaire de créer et de gérer des volumes, de répliquer des données et d'intégrer FSX pour ONTAP avec des services tels que la classification BlueXP et la copie et la synchronisation BlueXP.

- Catalogue d'automatisation
- Azure NetApp Files

  Aucun connecteur n'est nécessaire pour configurer et gérer Azure NetApp Files, mais vous devez utiliser un connecteur pour analyser les données Azure NetApp Files à l'aide de la classification BlueXP.

- Cloud Volumes Service pour Google Cloud

- Copie et synchronisation
- Conseiller digital
- Portefeuille digital

  Dans presque tous les cas, vous pouvez ajouter une licence au portefeuille numérique sans connecteur.

  La seule fois qu'un connecteur est nécessaire pour ajouter une licence au portefeuille numérique est pour les licences Cloud Volumes ONTAP *basées sur le nœud*. Dans ce cas, un connecteur est requis car les données sont extraites des licences installées sur les systèmes Cloud Volumes ONTAP.

- Découverte directe des clusters ONTAP sur site

  Même si aucun connecteur n'est nécessaire pour la découverte directe d'un cluster ONTAP sur site, un connecteur est nécessaire pour tirer parti des fonctionnalités BlueXP supplémentaires.

  "En savoir plus sur les options de découverte et de gestion des clusters ONTAP sur site"

- Durabilité

Lorsqu'un connecteur est nécessaire

Lorsque vous utilisez BlueXP en mode standard, un connecteur est requis pour les fonctionnalités et les services suivants dans BlueXP :

- Fonctions de gestion d'Amazon FSX pour ONTAP
- Le stockage Amazon S3
- Stockage Azure Blob
- Sauvegarde et restauration
- Classement
- Cloud Volumes ONTAP
- Reprise après incident
- Systèmes E-Series
- Efficacité économique [1]
- La mise en cache en périphérie
- Compartiments de stockage Google Cloud
- Clusters Kubernetes
- Rapports de migration
- Intégration de clusters ONTAP sur site avec les services de données BlueXP
- Résilience opérationnelle [1]
- Protection par ransomware
- Systèmes StorageGRID
- Tiering
- Mise en cache du volume

[1] bien que vous puissiez accéder à ces services sans connecteur, un connecteur est nécessaire pour lancer des actions à partir des services.

Un connecteur est nécessaire pour utiliser BlueXP en mode restreint ou privé.

Les connecteurs doivent toujours être opérationnels

Les connecteurs sont un élément fondamental de l'architecture de service BlueXP. Il est de votre responsabilité de vous assurer que les connecteurs appropriés sont en place, opérationnels et accessibles à tout moment. Bien que le service soit conçu pour surmonter les courtes pannes de la disponibilité des connecteurs, vous devez prendre des mesures immédiates pour remédier aux défaillances de l'infrastructure.

Cette documentation est régie par le CLUF. Si le produit n'est pas utilisé conformément à la documentation, la fonctionnalité et le fonctionnement du produit, ainsi que vos droits en vertu du CLUF, peuvent être affectés.

Impact sur Cloud Volumes ONTAP

Un connecteur est un composant clé de l'intégrité et du fonctionnement de Cloud Volumes ONTAP. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO et les systèmes BYOL basés sur la capacité sont arrêtés après avoir perdu la communication avec un connecteur pendant plus de 14 jours. Cela se produit car le connecteur actualise les licences du système chaque jour.

Si votre système Cloud Volumes ONTAP dispose d'une licence BYOL basée sur des nœuds, le système reste opérationnel au bout de 14 jours, car la licence est installée sur le système Cloud Volumes ONTAP.

Emplacements pris en charge

Un connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure

  Un connecteur dans Azure doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le "Paire de régions Azure" Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés. "Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"

- Google Cloud

  Si vous souhaitez utiliser les services BlueXP avec Google Cloud, vous devez utiliser un connecteur exécuté dans Google Cloud.

- Sur site

Mode restreint et mode privé

Pour utiliser BlueXP en mode restreint ou privé, vous commencez à utiliser BlueXP en installant le connecteur, puis en accédant à l'interface utilisateur qui s'exécute localement sur le connecteur.

"Découvrez les modes de déploiement BlueXP".

Comment créer un connecteur

Un administrateur de compte BlueXP peut créer un connecteur directement à partir de BlueXP, du marché de votre fournisseur cloud ou en installant manuellement le logiciel sur votre propre hôte Linux. La manière de commencer dépend si vous utilisez BlueXP en mode standard, en mode restreint ou en mode privé.

- "Découvrez les modes de déploiement BlueXP"
- "Commencez à utiliser BlueXP en mode standard"
- "Démarrez avec BlueXP en mode restreint"
- "Commencez à utiliser BlueXP en mode privé"

Autorisations

Des autorisations spécifiques sont nécessaires pour créer le connecteur directement à partir de BlueXP et un autre ensemble d'autorisations est nécessaire pour l'instance de connecteur elle-même. Si vous créez le connecteur dans AWS ou Azure directement à partir de BlueXP, BlueXP crée le connecteur avec les autorisations dont il a besoin.

Lorsque vous utilisez BlueXP en mode standard, la façon dont vous fournissez les autorisations dépend de la façon dont vous prévoyez de créer le connecteur.

Pour savoir comment configurer des autorisations, consultez les sections suivantes :

- Mode standard
  - "Options d'installation des connecteurs dans AWS"
  - "Options d'installation des connecteurs dans Azure"
  - "Options d'installation de Connector dans Google Cloud"
  - "Configurez les autorisations cloud pour les déploiements sur site"
- "Définissez les autorisations pour le mode restreint"
- "Configurez les autorisations pour le mode privé"

Pour afficher les autorisations exactes dont le connecteur a besoin pour les opérations quotidiennes, reportez-vous aux pages suivantes :

- "Découvrez comment Connector utilise les autorisations AWS"
- "Découvrez comment le connecteur utilise les autorisations Azure"
- "Découvrez comment Connector utilise les autorisations Google Cloud"

Mises à niveau des connecteurs

Nous mettons généralement à jour le logiciel de connecteur chaque mois pour introduire de nouvelles fonctions et améliorer la stabilité. Bien que la plupart des services et fonctionnalités de la plate-forme BlueXP soient proposés par le logiciel SaaS, quelques fonctionnalités dépendent de la version du connecteur. Qui inclut la gestion Cloud Volumes ONTAP, la gestion de clusters ONTAP sur site, la configuration et l'aide.

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. Si vous utilisez BlueXP en mode privé, vous devez mettre à niveau manuellement le connecteur.

"Apprenez à mettre à niveau manuellement le logiciel du connecteur".

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.

Plusieurs environnements de travail

Un connecteur peut gérer plusieurs environnements de travail dans BlueXP. Le nombre maximum d'environnements de travail qu'un seul connecteur doit gérer varie. Cela dépend du type d'environnements de travail, du nombre de volumes, de la capacité gérée et du nombre d'utilisateurs.

Si vous disposez d'un déploiement à grande échelle, contactez votre représentant NetApp pour dimensionner votre environnement. Si vous rencontrez des problèmes pendant le trajet, contactez-nous en utilisant le chat produit.

Connecteurs multiples

Dans certains cas, vous n'avez peut-être besoin que d'un seul connecteur, mais vous pourriez avoir besoin de deux connecteurs ou plus.

Voici quelques exemples :

- Vous avez un environnement multicloud (AWS et Azure, par exemple) et vous préférez avoir un connecteur dans AWS et un autre dans Azure. Chacun gère les systèmes Cloud Volumes ONTAP exécutés dans ces environnements.
- Un fournisseur de services peut utiliser un compte BlueXP pour fournir des services à ses clients, tout en utilisant un autre compte pour assurer la reprise après incident pour l'une de ses unités commerciales. Chaque compte aurait des connecteurs distincts.

Quand changer

Lorsque vous créez votre premier connecteur, BlueXP utilise automatiquement ce connecteur pour chaque environnement de travail supplémentaire créé. Une fois que vous avez créé un connecteur supplémentaire, vous devrez passer de l'un à l'autre pour voir les environnements de travail spécifiques à chaque connecteur.

"Apprenez à passer d'un connecteur à un autre".

Reprise après incident

Vous pouvez gérer un environnement de travail à l'aide de plusieurs connecteurs en même temps pour la reprise après sinistre. Si un connecteur tombe en panne, vous pouvez passer à l'autre connecteur pour gérer immédiatement l'environnement de travail.

Pour configurer cette configuration :

1. "Basculer vers un autre connecteur".
2. Découvrir l'environnement de travail existant
    - "Ajout de systèmes Cloud Volumes ONTAP existants à BlueXP"
    - "Découvrir les clusters ONTAP"

3. Réglez le "Mode de gestion de la capacité"

   Seul le connecteur principal doit être réglé sur **mode automatique**. Si vous basculez vers un autre connecteur pour la reprise après incident, vous pouvez modifier le mode de gestion de la capacité selon vos besoins.

Découvrez les modes de déploiement BlueXP

BlueXP propose plusieurs *modes de déploiement* qui vous permettent d'utiliser BlueXP en fonction de vos exigences métier et de sécurité. *Standard mode* exploite la couche SaaS de BlueXP pour fournir des fonctionnalités complètes, tandis que *restricted mode* et *private mode* sont disponibles pour les entreprises ayant des restrictions de connectivité.

BlueXP inhibe le flux du trafic, de la communication et des données lorsqu'il est en mode restreint ou en mode privé. Il est de votre responsabilité de veiller au respect des réglementations requises par votre environnement (sur site et dans le cloud).

Présentation

BlueXP propose les modes de déploiement suivants pour votre compte. Chaque mode varie en fonction des exigences de connectivité sortante, de l'emplacement de déploiement, du processus d'installation, de la méthode d'authentification, des services de données et de stockage disponibles et des méthodes de facturation.

Mode standard

BlueXP est accessible en tant que service cloud à partir de la console web. Selon les services BlueXP que vous prévoyez d'utiliser, un administrateur BlueXP crée un ou plusieurs connecteurs pour gérer les données au sein de votre environnement de cloud hybride.

Ce mode utilise la transmission de données chiffrées sur Internet public.

Mode restreint

Un connecteur BlueXP est installé dans le cloud (dans une région gouvernementale, une région cloud souveraine ou une région commerciale) et sa connectivité sortante est limitée vers la couche SaaS de BlueXP. Les utilisateurs accèdent à BlueXP en local à partir de la console web disponible depuis le connecteur, et non depuis la couche SaaS.

Ce mode est généralement utilisé par les gouvernements d'état et locaux et les entreprises réglementées.

En savoir plus sur la connectivité sortante à la couche SaaS.

Mode privé

Un connecteur BlueXP est installé sur site ou dans le cloud (dans une région sécurisée, une région cloud souveraine ou une région commerciale) et ne dispose d'aucune connectivité à la couche SaaS de BlueXP. Les utilisateurs accèdent à BlueXP en local à partir de la console web disponible depuis le connecteur, et non depuis la couche SaaS.

Une région sécurisée inclut "Cloud secret AWS", "Le cloud le plus secret d'AWS", et "Azure IL6"

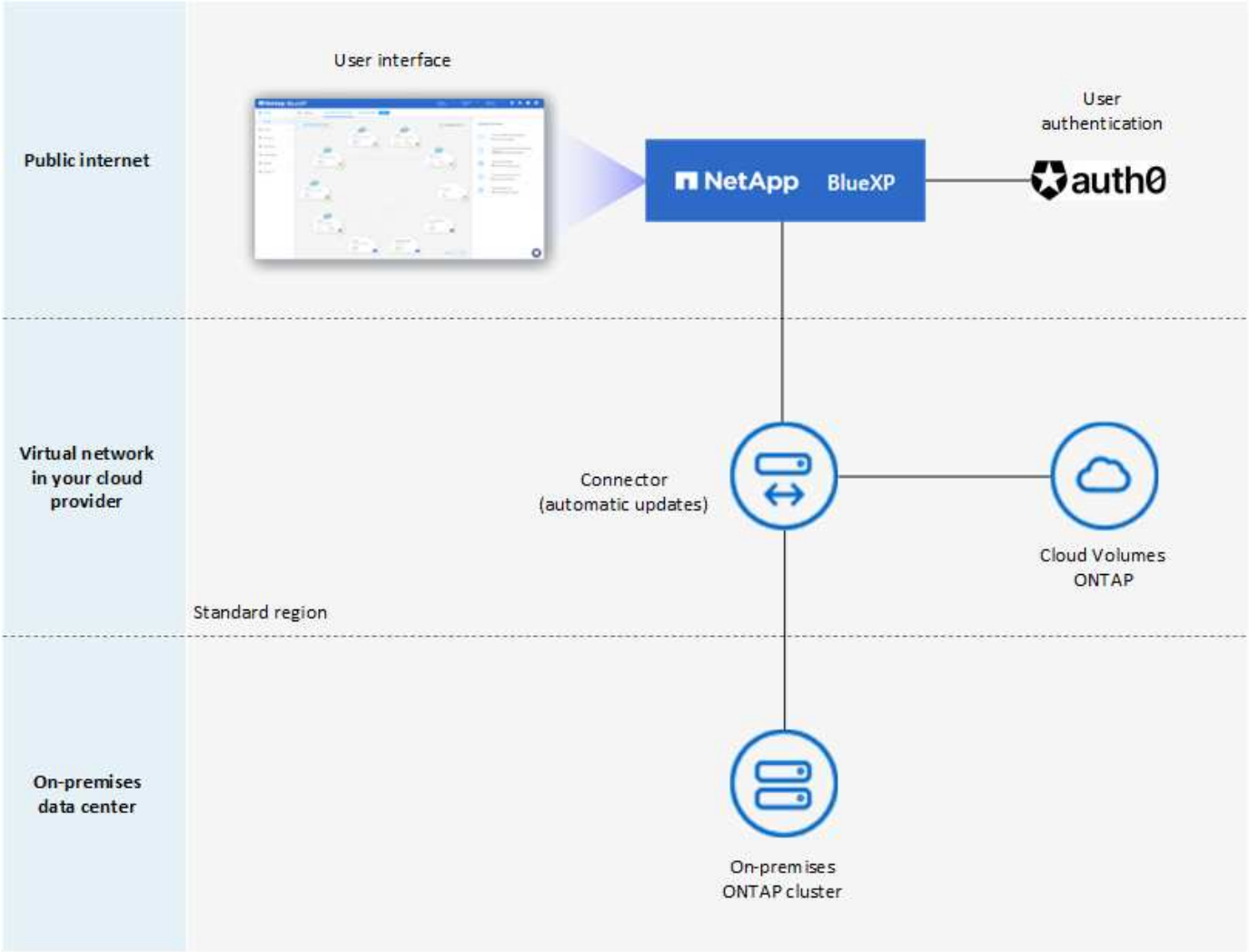
Le tableau suivant fournit une comparaison de ces modes.

	Mode standard	Mode restreint	Mode privé
Connexion requise à la couche SaaS BlueXP ?	Oui.	Sortant uniquement	Non
Connexion requise à votre fournisseur de cloud ?	Oui.	Oui, dans la région	Oui, dans la région (si vous utilisez Cloud Volumes ONTAP)
Installation du connecteur	Depuis BlueXP, Cloud Marketplace ou une installation manuelle	Cloud Marketplace ou installation manuelle	Installation manuelle
Mises à niveau des connecteurs	Mises à niveau automatiques du logiciel NetApp Connector	Mises à niveau automatiques du logiciel NetApp Connector	Mise à niveau manuelle requise
Accès à l'interface utilisateur	De la couche SaaS BlueXP	Localement à partir de la VM connecteur	Localement à partir de la VM connecteur
Terminal API	La couche SaaS de BlueXP	Le connecteur	Le connecteur
Authentificatio n	Via SaaS en utilisant auth0, la connexion NSS ou la fédération des identités	Via SaaS en utilisant auth0 ou la fédération d'identité	Authentification utilisateur locale
Et les services de données	Tous sont pris en charge	Nombre d'entre elles sont prises en charge	Plusieurs sont pris en charge
Options de licence	Abonnements Marketplace et BYOL	Abonnements Marketplace et BYOL	BYOL

Consultez les sections suivantes pour en savoir plus sur ces modes, notamment les fonctionnalités et les services BlueXP pris en charge.

Mode standard

L'image suivante est un exemple de déploiement en mode standard.



BlueXP fonctionne comme suit en mode standard :

Communication sortante

La connectivité est requise du connecteur à la couche SaaS BlueXP, aux ressources accessibles au public de votre fournisseur cloud et à d'autres composants essentiels pour les opérations quotidiennes.

- "Terminaux que le connecteur contacte dans AWS"
- "Terminaux que le connecteur contacte dans Azure"
- "Terminaux que le connecteur contacte dans Google Cloud"

Emplacement pris en charge pour le connecteur

En mode standard, le connecteur est pris en charge dans le cloud ou sur site.

Installation du connecteur

L'installation du connecteur est possible à partir d'un assistant d'installation de BlueXP, d'AWS ou d'Azure Marketplace, ou à l'aide d'un programme d'installation pour installer manuellement le connecteur sur votre propre hôte Linux dans votre data Center ou dans le cloud.

Mises à niveau des connecteurs

Les mises à niveau automatisées du logiciel du connecteur sont disponibles depuis BlueXP avec des mises à jour mensuelles.

Accès à l'interface utilisateur

L'interface utilisateur est accessible depuis la console Web fournie via la couche SaaS.

Terminal API

Les appels d'API sont effectués vers le terminal suivant :
https://cloudmanager.cloud.netapp.com

Authentification

L'authentification est fournie via le service cloud de BlueXP via auth0 ou des connexions au site du support NetApp (NSS). la fédération des identités est disponible.

Services BlueXP pris en charge

Tous les services BlueXP sont disponibles pour les utilisateurs.

Options de licence prises en charge

Les abonnements Marketplace et BYOL sont pris en charge en mode standard. Toutefois, les options de licence prises en charge dépendent du service BlueXP que vous utilisez. Consultez la documentation de chaque service pour en savoir plus sur les options de licence disponibles.

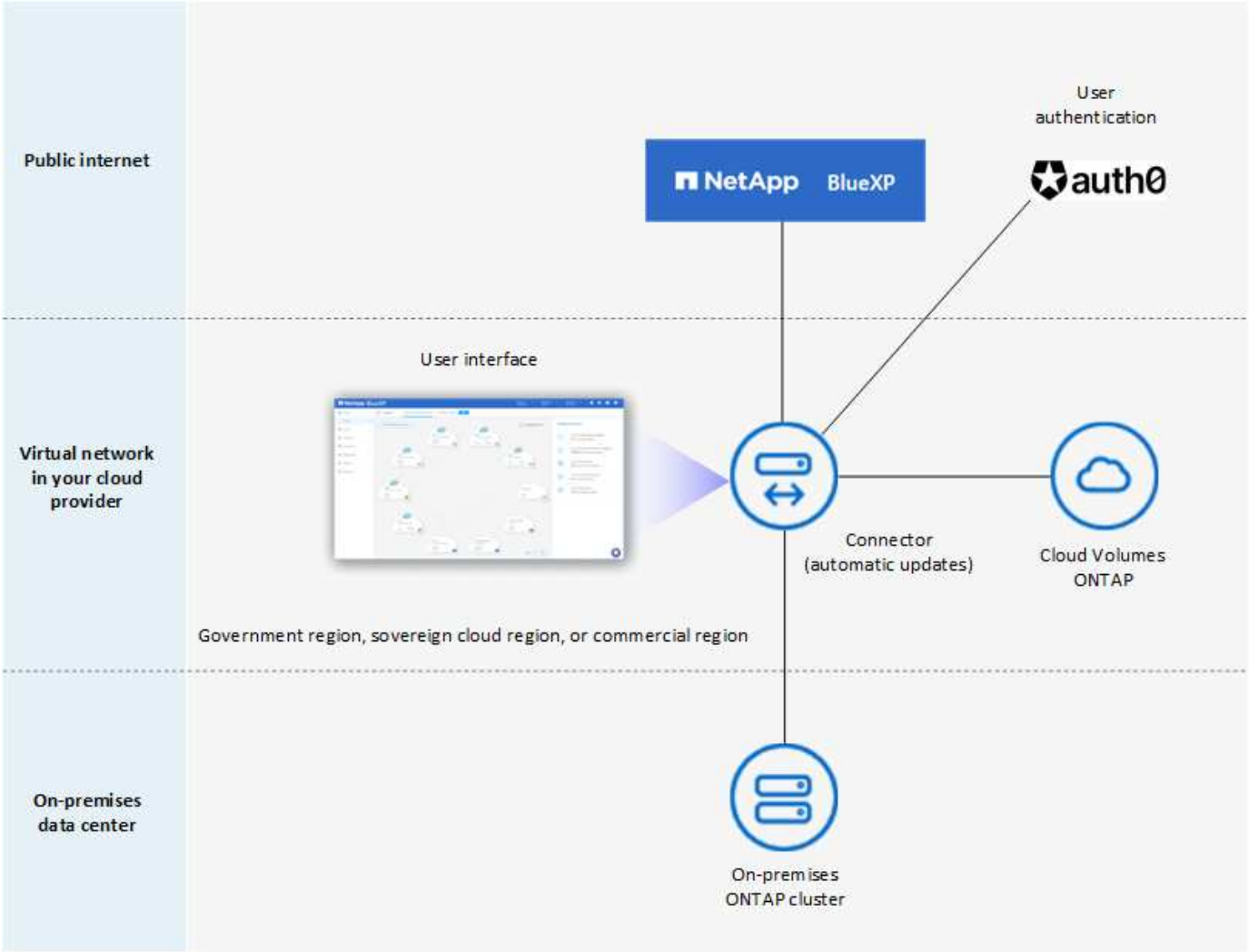
Comment démarrer avec le mode standard

Accédez au "Console web BlueXP" et s'inscrire.

"Découvrez comment vous lancer avec le mode standard".

Mode restreint

L'image suivante est un exemple de déploiement en mode restreint.



BlueXP fonctionne comme suit en mode restreint :

Communication sortante

Une connectivité sortante est requise du connecteur vers la couche SaaS BlueXP pour utiliser les services de données BlueXP, pour permettre les mises à niveau logicielles automatiques du connecteur, pour utiliser l'authentification basée sur auth0 et pour envoyer des métadonnées à des fins de facturation (nom de la VM de stockage, capacité allouée, UUID, type et IOPS de volume).

La couche SaaS de BlueXP n'initie pas la communication avec le connecteur. Toutes les communications sont initiées par le connecteur, qui peut extraire ou envoyer des données de ou vers la couche SaaS, selon les besoins.

Une connexion est également requise pour les ressources du fournisseur cloud provenant de la région.

Emplacement pris en charge pour le connecteur

En mode restreint, le connecteur est pris en charge dans le cloud : dans une région gouvernementale, une région souveraine ou une région commerciale.

Installation du connecteur

L'installation du connecteur est possible depuis AWS Marketplace ou Azure Marketplace, ou une installation manuelle sur votre propre hôte Linux.

Mises à niveau des connecteurs

Les mises à niveau automatisées du logiciel du connecteur sont disponibles depuis BlueXP avec des mises à jour mensuelles.

Accès à l'interface utilisateur

L'interface utilisateur est accessible à partir de la machine virtuelle Connector déployée dans votre région cloud.

Terminal API

Les appels API sont effectués vers la machine virtuelle du connecteur.

Authentification

L'authentification est fournie via le service cloud de BlueXP via auth0. la fédération des identités est également disponible.

Services BlueXP pris en charge

BlueXP prend en charge les services de données et de stockage suivants avec un mode restreint :

Services pris en charge	Remarques
Amazon FSX pour ONTAP	Support complet
Azure NetApp Files	Support complet
Sauvegarde et restauration	Pris en charge dans les régions gouvernementales et commerciales avec mode restreint. Non pris en charge dans les régions souveraines avec mode restreint. En mode restreint, la sauvegarde et la restauration BlueXP prennent en charge la sauvegarde et la restauration des données de volume ONTAP uniquement. "Affichez la liste des destinations de sauvegarde prises en charge pour les données ONTAP" La sauvegarde et la restauration des données applicatives, des données de machines virtuelles et des données Kubernetes ne sont pas prises en charge.
Classement	Pris en charge dans les régions gouvernementales avec mode restreint. Non pris en charge dans les régions commerciales ou les régions souveraines en mode restreint. Les limitations suivantes s'appliquent : • Les comptes OneDrive, les comptes SharePoint et Google Drive ne peuvent pas être analysés. • Impossible d'intégrer la fonctionnalité de label Microsoft Azure information protection (AIP).
Cloud Volumes ONTAP	Support complet

Services pris en charge	Remarques
Portefeuille digital	Vous pouvez utiliser le portefeuille numérique avec les options de licence prises en charge répertoriées ci-dessous pour le mode restreint.
Clusters ONTAP sur site	La découverte avec un connecteur et la découverte sans connecteur (découverte directe) sont toutes deux prises en charge. La vue avancée (System Manager) n'est pas prise en charge lorsque vous découvrez un cluster sur site avec un connecteur.
La réplication	Pris en charge dans les régions gouvernementales avec mode restreint. Non pris en charge dans les régions commerciales ou les régions souveraines en mode restreint.

Options de licence prises en charge

Les options de licence suivantes sont prises en charge avec le mode restreint :

- Abonnements aux marchés (contrats à l'heure et à l'année)

  Notez ce qui suit :

  - Pour Cloud Volumes ONTAP, seules les licences basées sur la capacité sont prises en charge.
  - Dans Azure, les contrats annuels ne sont pas pris en charge par les régions gouvernementales.
- BYOL

  Pour Cloud Volumes ONTAP, les licences basées sur la capacité et les licences basées sur les nœuds sont prises en charge par le modèle BYOL.

Comment démarrer avec le mode restreint

Vous devez activer le mode restreint lorsque vous créez votre compte BlueXP.

Si vous n'avez pas encore de compte, vous serez invité à créer votre compte et à activer le mode restreint lorsque vous vous connecterez à BlueXP pour la première fois à partir d'un connecteur que vous avez installé manuellement ou que vous avez créé à partir du Marketplace de votre fournisseur cloud.

Si vous avez déjà un compte et que vous souhaitez en créer un autre, vous devez utiliser l'API de location.

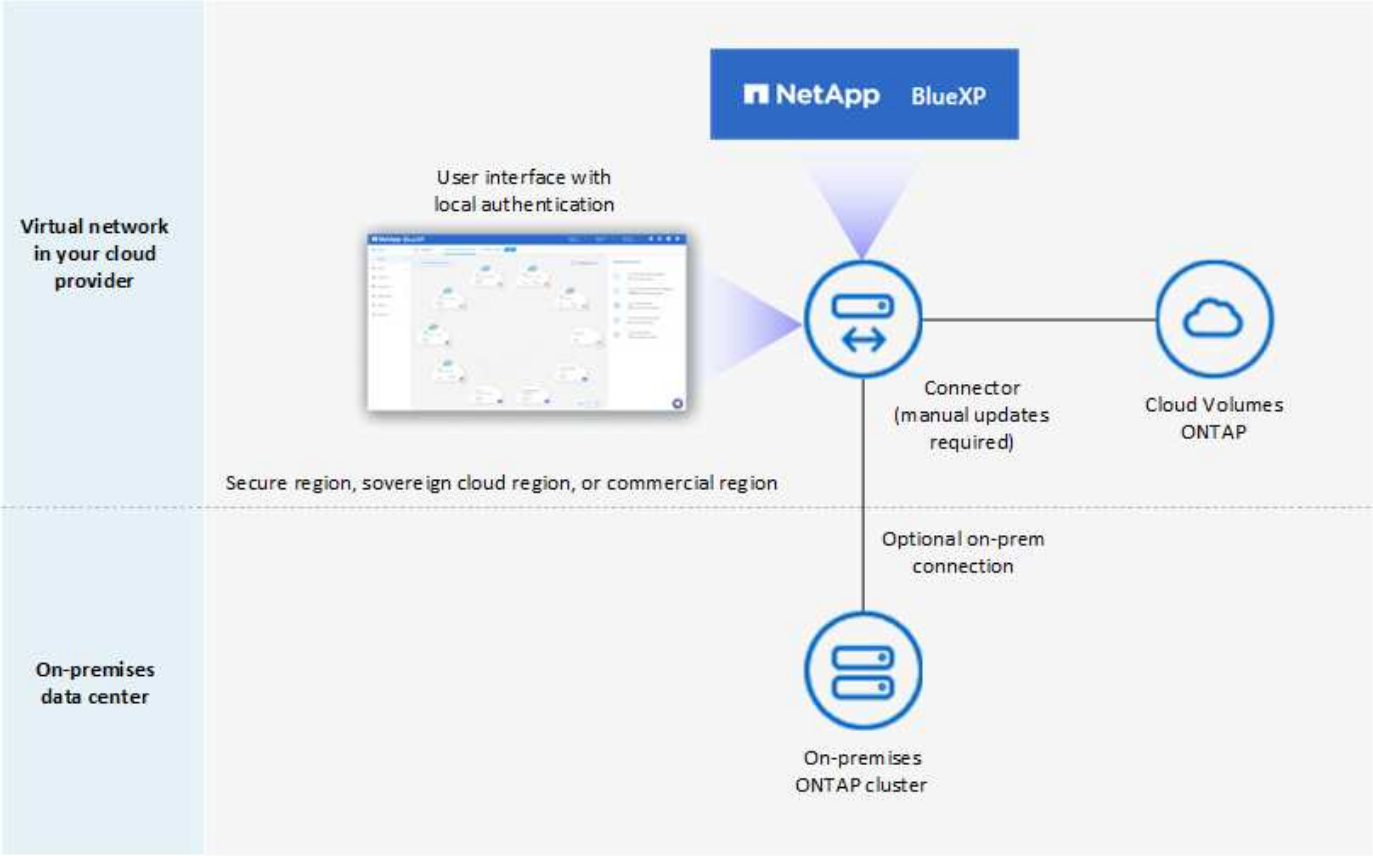
Notez que vous ne pouvez pas modifier le paramètre du mode restreint après la création du compte par BlueXP. Vous ne pouvez pas activer le mode restreint ultérieurement et vous ne pouvez pas le désactiver ultérieurement. Elle doit être définie au moment de la création du compte.

- "Découvrez comment vous lancer avec le mode restreint".
- "Découvrez comment créer un compte BlueXP supplémentaire".

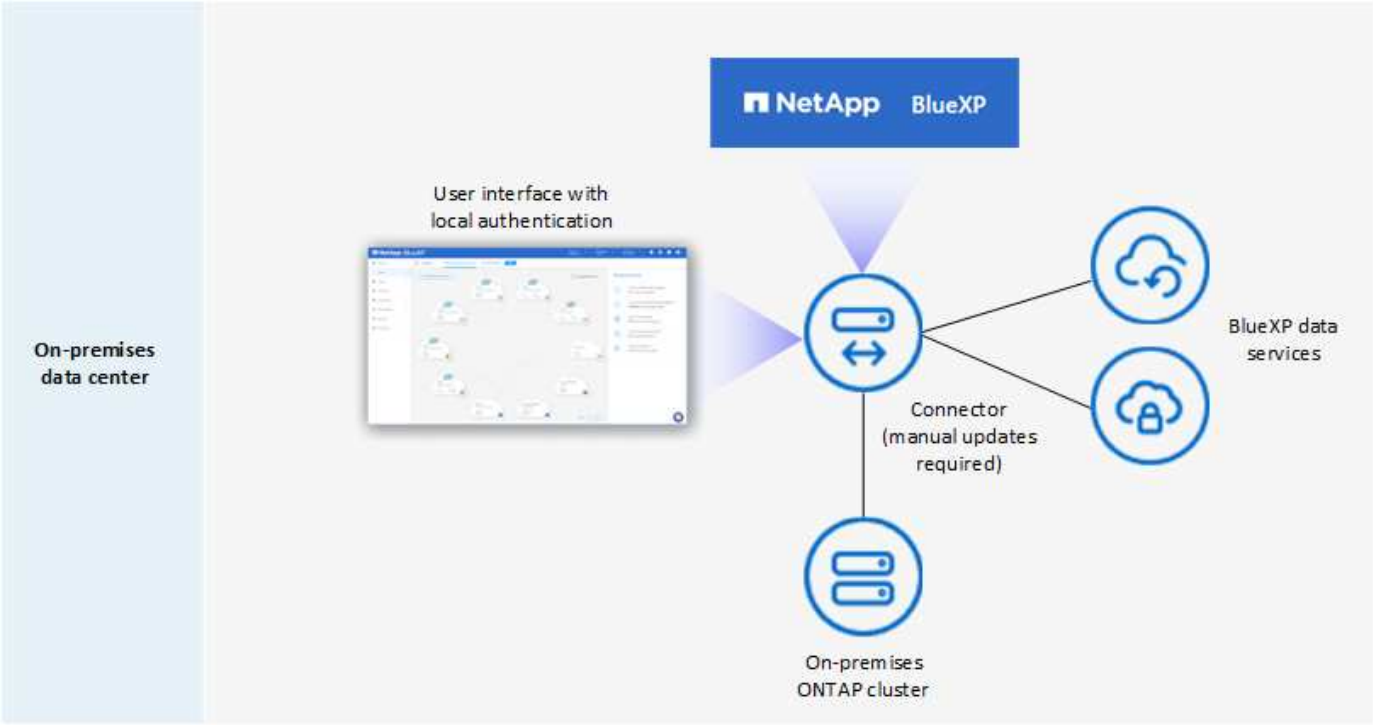
Mode privé

En mode privé, vous pouvez installer un connecteur sur site ou dans le cloud, puis utiliser BlueXP pour gérer les données dans votre cloud hybride. La couche SaaS BlueXP n'est pas connectée.

L'image suivante montre un exemple de déploiement en mode privé où le connecteur est installé dans le cloud et gère à la fois Cloud Volumes ONTAP et un cluster ONTAP sur site.



Pendant ce temps, la deuxième image présente un exemple de déploiement en mode privé où le connecteur est installé sur site, gère un cluster ONTAP sur site et permet d'accéder aux services de données BlueXP pris en charge.



BlueXP fonctionne comme suit en mode privé :

Communication sortante

Aucune connectivité sortante n'est requise vers la couche SaaS BlueXP. Tous les packages, dépendances et composants essentiels sont emballés avec le connecteur et servis à partir de la machine locale. La connectivité aux ressources accessibles au public de votre fournisseur cloud n'est requise que si vous déployez Cloud Volumes ONTAP.

Emplacement pris en charge pour le connecteur

En mode privé, le connecteur est pris en charge dans le cloud ou sur site.

Installation du connecteur

Les installations manuelles du connecteur sont prises en charge sur votre propre hôte Linux dans le cloud ou sur site.

Mises à niveau des connecteurs

Vous devez mettre à niveau le logiciel du connecteur manuellement. Le logiciel du connecteur est publié sur le site de support NetApp à intervalles non définis.

Accès à l'interface utilisateur

L'interface utilisateur est accessible depuis le connecteur déployé dans votre région cloud ou sur site.

Terminal API

Les appels API sont effectués vers la machine virtuelle du connecteur.

Authentification

L'authentification est assurée par la gestion et l'accès des utilisateurs locaux. L'authentification n'est pas fournie via le service cloud de BlueXP.

Services BlueXP pris en charge dans les déploiements cloud

BlueXP prend en charge les services de stockage et de données suivants avec le mode privé lorsque le connecteur est installé dans le cloud :

Services pris en charge	Remarques
Sauvegarde et restauration	Pris en charge dans les régions commerciales AWS et Azure. Non pris en charge dans Google Cloud ou dans "Cloud secret AWS", "Le cloud le plus secret d'AWS", ou "Azure IL6" En mode privé, la sauvegarde et la restauration BlueXP prennent en charge la sauvegarde et la restauration des données de volume ONTAP uniquement. "Affichez la liste des destinations de sauvegarde prises en charge pour les données ONTAP" La sauvegarde et la restauration des données applicatives, des données de machines virtuelles et des données Kubernetes ne sont pas prises en charge.

Services pris en charge	Remarques
Cloud Volumes ONTAP	Comme il n'y a pas d'accès à Internet, les fonctionnalités suivantes ne sont pas disponibles : mises à niveau logicielles automatisées et AutoSupport.
Portefeuille digital	Vous pouvez utiliser le portefeuille numérique avec les options de licence prises en charge répertoriées ci-dessous pour le mode privé.
Clusters ONTAP sur site	Requiert une connectivité du cloud (où le connecteur est installé) à l'environnement sur site. La découverte sans connecteur (découverte directe) n'est pas prise en charge.

Prise en charge des services BlueXP dans les déploiements sur site

BlueXP prend en charge les services de stockage et de données suivants avec le mode privé lorsque le connecteur est installé sur votre site :

Services pris en charge	Remarques
Sauvegarde et restauration	En mode privé, la sauvegarde et la restauration BlueXP prennent en charge la sauvegarde et la restauration des données de volume ONTAP uniquement. "Affichez la liste des destinations de sauvegarde prises en charge pour les données de volume ONTAP" La sauvegarde et la restauration des données applicatives, des données de machines virtuelles et des données Kubernetes ne sont pas prises en charge.
Classement	• Les seules sources de données prises en charge sont celles que vous pouvez découvrir localement. "Affichez les sources que vous pouvez découvrir localement" • Les fonctionnalités nécessitant un accès Internet sortant ne sont pas prises en charge. "Afficher les limites de la fonction"
Portefeuille digital	Vous pouvez utiliser le portefeuille numérique avec les options de licence prises en charge répertoriées ci-dessous pour le mode privé.
Clusters ONTAP sur site	La découverte sans connecteur (découverte directe) n'est pas prise en charge.
La réplication	Support complet

Options de licence prises en charge

Seul le modèle BYOL est pris en charge avec le mode privé.

Pour Cloud Volumes ONTAP BYOL, seules les licences basées sur les nœuds sont prises en charge. Les licences basées sur la capacité ne sont pas prises en charge. Aucune connexion Internet sortante n'est disponible. Vous devrez donc charger manuellement votre fichier de licence Cloud Volumes ONTAP dans le portefeuille digital BlueXP.

"Découvrez comment ajouter des licences au portefeuille digital BlueXP"

Comment démarrer avec le mode privé

Le mode privé est disponible en téléchargeant le programme d'installation « hors ligne » depuis le site de support NetApp.

"Découvrez comment vous lancer avec le mode privé".

> Si vous souhaitez utiliser BlueXP dans le "Cloud secret AWS" ou le "Le cloud le plus secret d'AWS", vous devez alors suivre des instructions séparées pour démarrer dans ces environnements. "Découvrez comment vous lancer avec Cloud Volumes ONTAP dans le cloud secret AWS ou le cloud secret"

Comparaison des services et des fonctionnalités

Le tableau suivant vous aide à identifier rapidement les services et fonctionnalités BlueXP pris en charge en mode restreint et en mode privé.

Notez que certains services peuvent être pris en charge avec des limitations. Pour plus d'informations sur la prise en charge de ces services en mode restreint et en mode privé, reportez-vous aux sections ci-dessus.

Zone du produit	Service ou fonctionnalité BlueXP	Mode restreint	Mode privé
Environnements de travail Cette partie du tableau répertorie la prise en charge de la gestion de l'environnement de travail depuis le canevas BlueXP. Il n'indique pas les destinations de sauvegarde prises en charge pour la sauvegarde et la restauration BlueXP.	Amazon FSX pour ONTAP	Oui.	Non
	Amazon S3	Non	Non
	Blob d'Azure	Non	Non
	Azure NetApp Files	Oui.	Non
	Cloud Volumes ONTAP	Oui.	Oui.
	Cloud Volumes Service pour Google Cloud	Non	Non
	Google Cloud Storage	Non	Non
	Clusters Kubernetes	Non	Non
	Clusters ONTAP sur site	Oui.	Oui.
	E-Series	Non	Non
	StorageGRID	Non	Non

Zone du produit	Service ou fonctionnalité BlueXP	Mode restreint	Mode privé
Services	Sauvegarde et restauration	Oui. "Affichez la liste des destinations de sauvegarde prises en charge pour les données de volume ONTAP"	Oui. "Affichez la liste des destinations de sauvegarde prises en charge pour les données de volume ONTAP"
	Classement	Oui.	Oui.
	OPS cloud	Non	Non
	Copie et synchronisation	Non	Non
	Conseiller digital	Non	Non
	Portefeuille digital	Oui.	Oui.
	Reprise après incident	Non	Non
	Efficacité économique	Non	Non
	La mise en cache en périphérie	Non	Non
	Rapports de migration	Non	Non
	Résilience opérationnelle	Non	Non
	Protection par ransomware	Non	Non
	La réplication	Oui.	Oui.
	Durabilité	Non	Non
	Tiering	Non	Non
	Mise en cache du volume	Non	Non
Caractéristiques	Informations d'identification	Oui.	Oui.
	Comptes NSS	Oui.	Non
	Notifications	Oui.	Non
	Recherche	Oui.	Non
	De la chronologie	Oui.	Oui.

Commencez avec le mode standard

Mise en route du flux de travail (mode standard)

Commencez à utiliser BlueXP en mode standard en préparant la mise en réseau de la console BlueXP, en vous inscrivant et en créant un compte, en option, un connecteur et en vous abonnant à BlueXP.

En mode standard, BlueXP est accessible en tant que service cloud à partir de la console web. Avant de commencer, vous devez avoir une compréhension de "Comptes BlueXP", "Connecteurs", et "modes de

déploiement".

1 **"Préparez la mise en réseau à l'aide de la console BlueXP"**

Les ordinateurs qui accèdent à la console BlueXP doivent être connectés à des terminaux spécifiques pour effectuer quelques tâches d'administration. Si votre réseau restreint l'accès sortant, vous devez vous assurer que ces points finaux sont autorisés.

2 **"Inscrivez-vous et créez un compte"**

Accédez au "Console BlueXP" et s'inscrire. Vous aurez la possibilité de créer un compte, mais vous pouvez ignorer cette étape si vous êtes invité à un compte existant.

À ce stade, vous êtes connecté et pouvez commencer à utiliser plusieurs services BlueXP tels que Digital Advisor, Amazon FSX pour ONTAP, Azure NetApp Files, etc. "Découvrez ce que vous pouvez faire sans connecteur".

3 **Créer un connecteur**

Vous n'avez pas besoin d'un connecteur pour démarrer avec BlueXP, mais vous pouvez créer un connecteur pour déverrouiller toutes les fonctionnalités et tous les services BlueXP. Le connecteur est le logiciel NetApp qui permet à BlueXP de gérer les ressources et les processus dans votre environnement de cloud hybride.

Un administrateur de compte BlueXP peut créer un connecteur dans votre réseau cloud ou sur site.

- "En savoir plus sur le moment où les connecteurs sont nécessaires et leur fonctionnement"
- "Découvrez comment créer un connecteur dans AWS"
- "Découvrez comment créer un connecteur dans Azure"
- "Découvrez comment créer un connecteur dans Google Cloud"
- "Découvrez comment créer un connecteur sur site"

Notez que si vous souhaitez utiliser les services BlueXP pour gérer le stockage et les données dans Google Cloud, le connecteur doit être exécuté dans Google Cloud.

4 **"Abonnez-vous à BlueXP"**

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel.

Préparez la mise en réseau à l'aide de la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, il contacte plusieurs terminaux lorsqu'il effectue quelques tâches d'administration. Les ordinateurs qui accèdent à la console BlueXP doivent avoir des connexions à ces terminaux.

Ces terminaux sont contactés depuis l'ordinateur d'un utilisateur lorsqu'ils effectuent des actions spécifiques à partir de la console BlueXP. Vous devez également consulter les exigences réseau pour le connecteur et pour des services BlueXP spécifiques. Pour plus de détails, reportez-vous aux liens connexes à la fin de cette page.

Terminaux	Objectif
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Votre navigateur web contacte ces URL lorsque vous utilisez la console web BlueXP.
https://aiq.netapp.com	Requis pour accéder au conseiller digital BlueXP.
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Nécessaire pour déployer un connecteur depuis BlueXP dans AWS. Le point final exact dépend de la région dans laquelle vous déployez le connecteur. "Reportez-vous à la documentation AWS pour plus de détails."
https://management.azure.com https://login.microsoftonline.com	Nécessaire au déploiement d'un connecteur depuis BlueXP dans la plupart des régions Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Nécessaire au déploiement d'un connecteur depuis BlueXP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Nécessaire au déploiement d'un connecteur de BlueXP dans les régions Azure Government.
https://www.googleapis.com	Nécessaire pour déployer un connecteur depuis BlueXP dans Google Cloud.
https://signin.b2c.netapp.com	Requis pour mettre à jour les identifiants du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via BlueXP.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Au-delà de ces terminaux, vous devez également vous assurer que le connecteur dispose d'un accès Internet sortant pour contacter des terminaux spécifiques pour les opérations quotidiennes. Vous trouverez la liste de ces points d'extrémité en suivant les liens de la section suivante ci-dessous.

Liens connexes

- Préparez la mise en réseau pour le connecteur
  - "Configuration du réseau AWS"
  - "Configuration du réseau Azure"
  - "Configuration du réseau Google Cloud"
  - "Configuration du réseau sur site"

- Préparez la mise en réseau pour les services BlueXP

  Consultez la documentation de chaque service BlueXP.

  "Documentation BlueXP"

Inscrivez-vous à BlueXP

BlueXP est accessible depuis une console web. Lorsque vous commencez à utiliser BlueXP, vous commencez par vous inscrire à l'aide de vos identifiants du site du support NetApp ou en créant un identifiant de connexion cloud NetApp.

Description de la tâche

Vous pouvez vous inscrire à BlueXP à l'aide de l'une des options suivantes :

- Vos identifiants existants du site de support NetApp (NSS)
- Une connexion au cloud NetApp en indiquant votre adresse e-mail et votre mot de passe

Les deux options prennent en charge une connexion fédérée, qui permet une authentification unique à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). Vous pouvez configurer une connexion de fédération après vous être inscrit. "Découvrez comment utiliser la fédération des identités avec BlueXP".

Étapes

1. Ouvrez un navigateur Web et accédez au "Console BlueXP"
2. Si vous possédez un compte sur le site de support NetApp, entrez l'adresse e-mail associée à votre compte NSS directement sur la page **connexion**.

   Vous pouvez ignorer la page d'inscription si vous avez un compte NSS. BlueXP vous inscrit dans le cadre de cette connexion initiale.

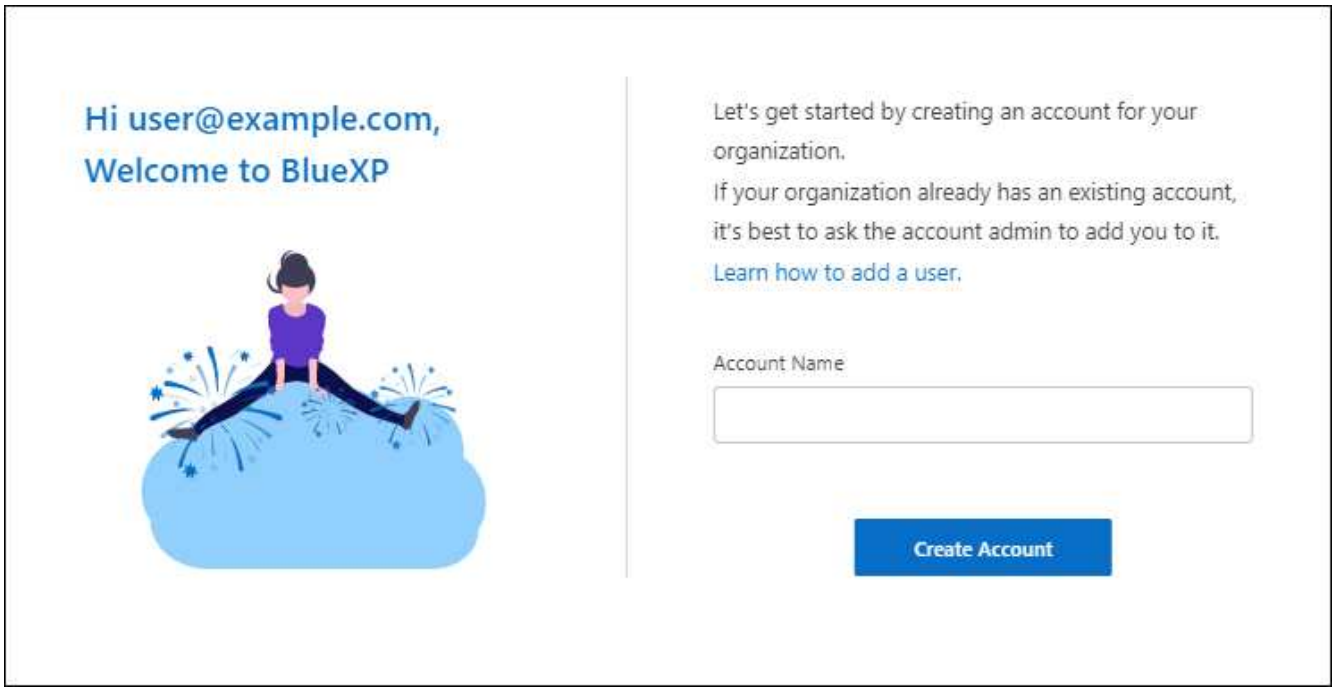
3. Si vous ne possédez pas de compte NSS et que vous souhaitez vous inscrire en créant un identifiant cloud NetApp, sélectionnez **s'inscrire**.
4. Sur la page **s'inscrire**, entrez les informations requises pour créer un identifiant NetApp Cloud.

   Notez que seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

5. Lorsque vous y êtes invité, consultez le contrat de licence de l'utilisateur final et acceptez les conditions.
6. Sur la page **Bienvenue**, saisissez un nom pour votre compte.

   Si votre entreprise dispose déjà d'un compte et que vous souhaitez le rejoindre, fermez BlueXP et demandez au propriétaire de vous associer au compte. Une fois que le propriétaire vous a ajouté, vous pouvez vous connecter et accéder au compte. "Découvrez comment ajouter des membres à un compte existant".

   Un compte est la partie supérieure de la plateforme d'identités de NetApp. Il vous permet d'ajouter et de gérer des utilisateurs, des rôles, des autorisations et des environnements de travail.



7. Sélectionnez **Créer un compte**.

Résultat

Vous disposez maintenant d'un identifiant BlueXP et d'un compte. Dans la plupart des cas, l'étape suivante consiste à créer un connecteur qui connecte les services de BlueXP à votre environnement de cloud hybride.

Créer un connecteur

AWS

Options d'installation des connecteurs dans AWS

Il existe plusieurs façons de créer un connecteur dans AWS. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- "Créez le connecteur directement à partir de BlueXP" (il s'agit de l'option standard)

  Cette action lance une instance EC2 exécutant Linux et le logiciel Connector dans un VPC de votre choix.

- "Créez un connecteur à partir d'AWS Marketplace"

  Cette action lance également une instance EC2 exécutant Linux et le logiciel Connector, mais le déploiement est initié directement à partir d'AWS Marketplace plutôt que de BlueXP.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans AWS.

Créez un connecteur dans AWS à partir de BlueXP

Pour créer un connecteur dans AWS à partir de BlueXP, vous devez configurer votre réseau, préparer les autorisations AWS, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.

Terminaux	Objectif
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

"Consultez la liste des terminaux contactés depuis la console BlueXP".

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : configurez les autorisations AWS

BlueXP doit s'authentifier auprès d'AWS avant de pouvoir déployer l'instance de connecteur dans votre VPC. Vous pouvez choisir l'une des méthodes d'authentification suivantes :

- BlueXP assume un rôle IAM qui dispose des autorisations requises
- Fournissez une clé d'accès AWS et une clé secrète pour un utilisateur IAM qui dispose des autorisations nécessaires

Quelle que soit l'option choisie, la première étape consiste à créer une politique IAM. Cette politique contient uniquement les autorisations nécessaires pour lancer l'instance Connector dans AWS à partir de BlueXP.

Si nécessaire, vous pouvez restreindre la politique IAM à l'aide de l'IAM `Condition` elément. "Documentation AWS : élément de condition"

Lorsque BlueXP crée le connecteur, il applique un nouvel ensemble d'autorisations à l'instance Connector qui permet au connecteur de gérer les ressources AWS.

Étapes

1. Accédez à la console IAM AWS.
2. Sélectionnez **stratégies > Créer une stratégie**.
3. Sélectionnez **JSON**.
4. Copiez et collez la stratégie suivante :

   Pour rappel, cette règle contient uniquement les autorisations nécessaires pour lancer l'instance Connector dans AWS à partir de BlueXP. "Droits d'accès requis pour l'instance de connecteur elle-même".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
```

```
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
```

```
        ],
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
          }
        },
        "Resource": [
          "arn:aws:ec2:*:*:instance/*"
        ]
      }
    ]
  }
```

5. Sélectionnez **Suivant** et ajoutez des balises, si nécessaire.
6. Sélectionnez **Suivant** et entrez un nom et une description.
7. Sélectionnez **Créer une stratégie**.
8. Reliez la règle à un rôle IAM que BlueXP peut assumer ou à un utilisateur IAM pour que vous puissiez fournir BlueXP avec des clés d'accès :
   - (Option 1) configurer un rôle IAM que BlueXP peut assumer :
     i. Accédez à la console IAM AWS dans le compte cible.
     ii. Sous gestion des accès, sélectionnez **rôles > Créer un rôle** et suivez les étapes pour créer le rôle.
     iii. Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
     iv. Sélectionnez **un autre compte AWS** et saisissez l'ID du compte BlueXP SaaS : 952013314444
     v. Sélectionnez la stratégie que vous avez créée dans la section précédente.
     vi. Après avoir créé le rôle, copiez le rôle ARN afin de pouvoir le coller dans BlueXP lorsque vous créez le connecteur.
   - (Option 2) configurez les autorisations d'accès pour un utilisateur IAM afin que vous puissiez fournir BlueXP avec des clés d'accès :
     i. Dans la console IAM AWS, sélectionnez **Users**, puis sélectionnez le nom d'utilisateur.
     ii. Sélectionnez **Ajouter des autorisations > joindre des stratégies existantes directement**.
     iii. Sélectionnez la stratégie que vous avez créée.
     iv. Sélectionnez **Suivant**, puis **Ajouter des autorisations**.
     v. Assurez-vous que vous disposez de la clé d'accès et de la clé secrète pour l'utilisateur IAM.

Résultat

Vous devez maintenant disposer d'un rôle IAM qui possède les autorisations requises ou d'un utilisateur IAM qui dispose des autorisations requises. Lorsque vous créez le connecteur à partir de BlueXP, vous pouvez fournir des informations sur le rôle ou les clés d'accès.

Étape 3 : créer le connecteur

Créez le connecteur directement à partir de la console web BlueXP.

Description de la tâche

La création du connecteur à partir de BlueXP déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à un type d'instance EC2 plus petit qui a moins de CPU ou de RAM. "En savoir plus sur la configuration par défaut du connecteur".

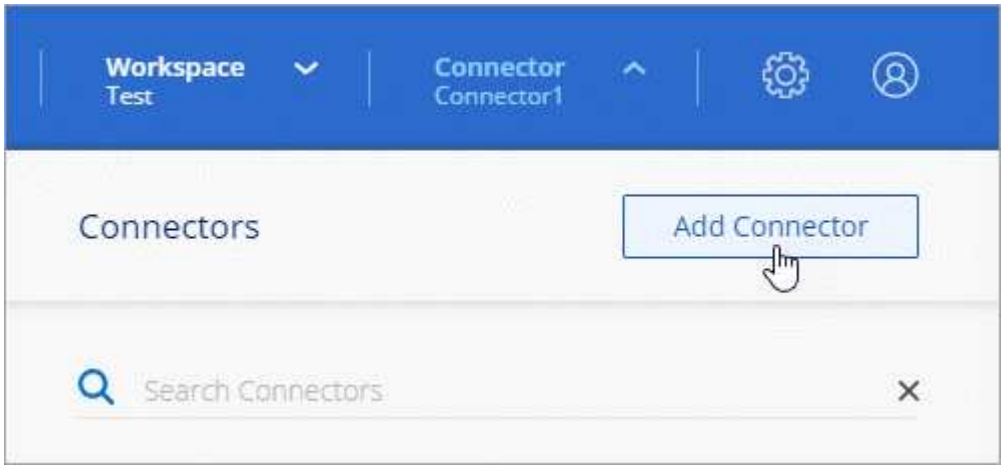
Avant de commencer

Vous devez disposer des éléments suivants :

- Méthode d'authentification AWS : rôle IAM ou clés d'accès pour un utilisateur IAM disposant des autorisations requises.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Une paire de clés pour l'instance EC2.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Amazon Web Services** comme fournisseur de cloud et sélectionnez **Continuer**.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
   a. Sélectionnez **Continuer** pour préparer le déploiement à l'aide du guide produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
   b. Sélectionnez **passer au déploiement** si vous êtes déjà préparé en suivant les étapes de cette page.
4. Suivez les étapes de l'assistant pour créer le connecteur :
   - **Soyez prêt**: Passez en revue ce dont vous aurez besoin.
   - **Informations d'identification AWS** : spécifiez votre région AWS puis choisissez une méthode d'authentification, qui est soit un rôle IAM que BlueXP peut assumer, soit une clé d'accès AWS et une clé secrète.

     Si vous choisissez **supposons rôle**, vous pouvez créer le premier ensemble d'informations d'identification à partir de l'assistant de déploiement de connecteur. Tout ensemble supplémentaire d'informations d'identification doit être créé à partir de la page informations d'identification. Ils seront ensuite disponibles à partir de l'assistant dans une liste déroulante. "Découvrez comment ajouter des identifiants supplémentaires".

   - **Détails** : fournir des détails sur le connecteur.

    - Entrez un nom pour l'instance.
    - Ajoutez des balises personnalisées (métadonnées) à l'instance.
    - Choisissez si vous souhaitez que BlueXP crée un nouveau rôle avec les autorisations requises, ou si vous souhaitez sélectionner un rôle existant que vous avez configuré avec "les autorisations requises".
    - Indiquez si vous souhaitez chiffrer les disques EBS du connecteur. Vous pouvez utiliser la clé de chiffrement par défaut ou utiliser une clé personnalisée.
  - **Network** : spécifiez un VPC, un sous-réseau et une paire de clés pour l'instance, choisissez d'activer ou non une adresse IP publique et, éventuellement, spécifiez une configuration proxy.

    Assurez-vous que vous disposez de la paire de clés appropriée à utiliser avec le connecteur. Sans paire de clés, vous ne pourrez pas accéder à la machine virtuelle Connector.

  - **Groupe de sécurité** : choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

    "Afficher les règles des groupes de sécurité pour AWS".

  - **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.
5. Sélectionnez **Ajouter**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. "Découvrez comment gérer des compartiments S3 à partir de BlueXP"

Créez un connecteur à partir d'AWS Marketplace

Pour créer un connecteur à partir d'AWS Marketplace, vous devez configurer votre réseau, préparer les autorisations AWS, examiner les exigences d'instance, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces

informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : configurez les autorisations AWS

Pour préparer un déploiement Marketplace, créez des politiques IAM dans AWS et associez-les à un rôle IAM. Lorsque vous créez le connecteur à partir d'AWS Marketplace, vous êtes invité à sélectionner ce rôle IAM.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle. Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".
3. Créer un rôle IAM :

a. Sélectionnez **rôles > Créer un rôle**.
b. Sélectionnez **AWS service > EC2**.
c. Ajoutez des autorisations en joignant la stratégie que vous venez de créer.
d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous pouvez désormais associer un rôle IAM à l'instance EC2 lors du déploiement depuis AWS Marketplace.

Étape 3 : passez en revue les exigences relatives aux instances

Lorsque vous créez le connecteur, vous devez choisir un type d'instance EC2 qui répond aux exigences suivantes.

CPU
: 4 cœurs ou 4 CPU virtuels

RAM
: 14 GO

Type d'instance AWS EC2
: Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge.

Étape 4 : créer le connecteur

Créez le connecteur directement à partir d'AWS Marketplace.

Description de la tâche

La création du connecteur à partir d'AWS Marketplace déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. "En savoir plus sur la configuration par défaut du connecteur".

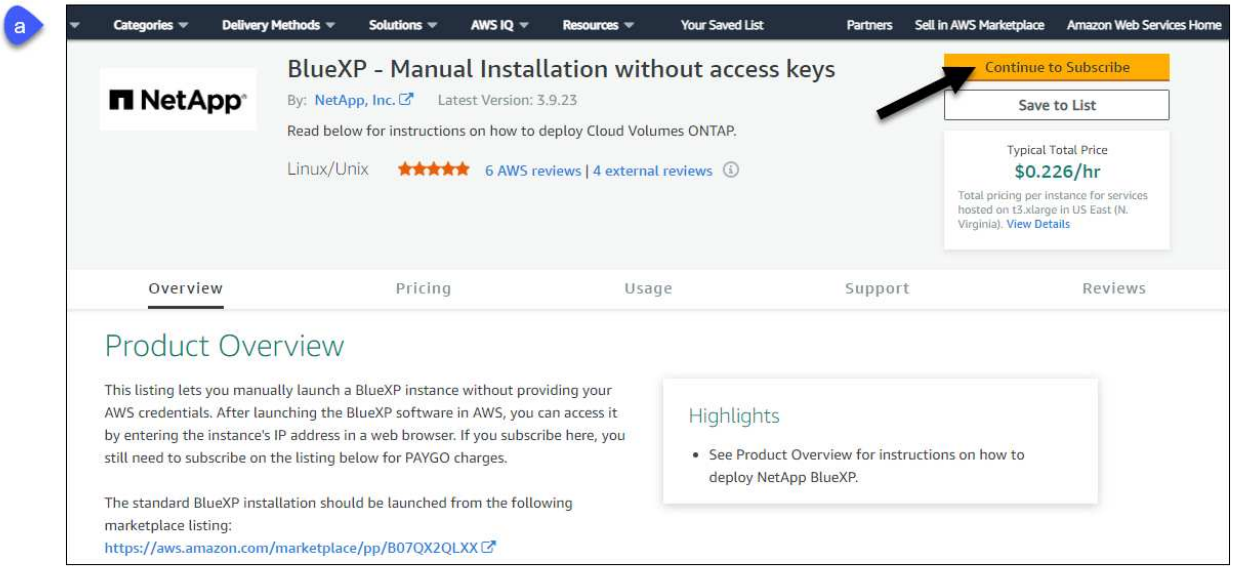
Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.
- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.
- Autorisations de vous abonner à AWS Marketplace et de vous désabonner pour votre utilisateur IAM.
- Compréhension des exigences en termes de CPU et de RAM pour l'instance.
- Une paire de clés pour l'instance EC2.

Étapes

1. Accédez au "BlueXP, page sur AWS Marketplace"
2. Sur la page Marketplace, sélectionnez **Continuer pour s'abonner**, puis sélectionnez **Continuer à la configuration**.



3. Modifiez l'une des options par défaut et sélectionnez **Continuer pour lancer**.
4. Sous **Choisissez action**, sélectionnez **lancer via EC2**, puis **lancer**.

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

5. Suivez les invites pour configurer et déployer l'instance :
   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Image de l'application et de l'OS** : passez cette section. Le connecteur ami est déjà sélectionné.
   - **Type d'instance** : en fonction de la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.xlarge est recommandé).
   - **Paire de clés (login)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
   - **Paramètres réseau** : modifiez les paramètres réseau selon vos besoins :
     - Choisissez le VPC et le sous-réseau souhaités.
     - Spécifiez si l'instance doit avoir une adresse IP publique.
     - Spécifiez les paramètres de pare-feu qui activent les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.

Quelques règles supplémentaires sont requises pour des configurations spécifiques.

"Afficher les règles des groupes de sécurité pour AWS".

- **Configurer le stockage** : conservez la taille et le type de disque par défaut pour le volume racine.

  Si vous souhaitez activer le chiffrement Amazon EBS sur le volume racine, sélectionnez **Avancé**, développez **Volume 1**, sélectionnez **crypté**, puis choisissez une clé KMS.

- **Détails avancés** : sous **profil d'instance IAM**, choisissez le rôle IAM qui inclut les autorisations requises pour le connecteur.
- **Résumé** : passez en revue le résumé et sélectionnez **lancer l'instance**.

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

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

   https://ipaddress

7. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte BlueXP à associer au connecteur.
   b. Entrez un nom pour le système.
   c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

      Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "Suivez les étapes pour démarrer avec BlueXP en mode restreint".

   d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Ouvrez un navigateur Web et accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. "Découvrez comment gérer des compartiments S3 à partir de BlueXP"

Installez manuellement le connecteur dans AWS

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer le réseau, préparer les autorisations AWS, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : vérifiez la configuration requise pour l'hôte

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

Hôte dédié

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

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

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

Paire de clés

Lorsque vous créez le connecteur, vous devez sélectionner une paire de clés EC2 à utiliser avec l'instance.

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

  "Voir les instructions d'installation"

Étape 2 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"

Terminaux	Objectif
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Étape 3 : configurer les autorisations

Vous devez fournir des autorisations AWS à BlueXP via l'une des options suivantes :

- Option 1 : créez des règles IAM et associez-les à un rôle IAM que vous pouvez associer à l'instance EC2.
- Option 2 : fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

Suivez les étapes pour préparer les autorisations pour BlueXP.

Rôle IAM

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle. Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".
3. Créer un rôle IAM :
   a. Sélectionnez **rôles > Créer un rôle**.
   b. Sélectionnez **AWS service > EC2**.
   c. Ajoutez des autorisations en joignant la stratégie que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous disposez désormais d'un rôle IAM que vous pouvez associer à l'instance EC2 après avoir installé le connecteur.

Clé d'accès AWS

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle.

   Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".
3. Associer les règles à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"
4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à BlueXP après l'installation du connecteur.

Résultat

Vous disposez désormais d'un utilisateur IAM qui dispose des autorisations requises et d'une clé d'accès que vous pouvez fournir à BlueXP.

Étape 4 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.

Description de la tâche

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

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

   ```
   unset http_proxy
   unset https_proxy
   ```

   Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

5. Exécutez le script d'installation.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Notez ce qui suit :

  - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
  - Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
  - BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

--cacert spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy HTTPS ou si le proxy est un proxy interceptant.

6. Attendez la fin de l'installation.

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

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

   https://ipaddress

8. Une fois connecté, configurez le connecteur :

a. Spécifiez le compte BlueXP à associer au connecteur.

b. Entrez un nom pour le système.

c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

   Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "Suivez les étapes pour démarrer avec BlueXP en mode restreint".

d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. "Découvrez comment gérer des compartiments S3 à partir de BlueXP"

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez installé le connecteur, vous devez fournir à BlueXP les autorisations AWS que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans AWS.

Rôle IAM

Reliez le rôle IAM que vous avez créé précédemment à l'instance Connector EC2.

Étapes

1. Accédez à la console Amazon EC2.
2. Sélectionnez **instances**.
3. Sélectionnez l'instance de connecteur.
4. Sélectionnez **actions > sécurité > Modifier le rôle IAM**.
5. Sélectionnez le rôle IAM et sélectionnez **mettre à jour le rôle IAM**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Clé d'accès AWS

Fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

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

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Azure

Options d'installation des connecteurs dans Azure

Il existe plusieurs façons de créer un connecteur dans Azure. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- "Créez un connecteur directement à partir de BlueXP" (il s'agit de l'option standard)

  Cette action lance une machine virtuelle exécutant Linux et le logiciel Connector dans un réseau virtuel de votre choix.

- "Créez un connecteur à partir d'Azure Marketplace"

  Cette action lance également une machine virtuelle qui exécute Linux et le logiciel Connector. Le déploiement est initié directement depuis Azure Marketplace plutôt que depuis BlueXP.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans Azure.

Créez un connecteur dans Azure à partir de BlueXP

Pour créer un connecteur dans Azure à partir de BlueXP, vous devez configurer votre réseau, préparer les autorisations Azure, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le "Paire de régions Azure" Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"

Vnet et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le réseau virtuel et le sous-réseau dans lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

"Consultez la liste des terminaux contactés depuis la console BlueXP".

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : créez un rôle personnalisé

Créez un rôle personnalisé Azure que vous pouvez attribuer à votre compte Azure ou à un principal de service Microsoft Entra. BlueXP s'authentifie auprès d'Azure et utilise ces autorisations pour créer l'instance de connecteur en votre nom.

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"

Étapes

1. Copiez les autorisations requises pour un nouveau rôle personnalisé dans Azure et enregistrez-les dans un fichier JSON.

Ce rôle personnalisé contient uniquement les autorisations nécessaires pour lancer la machine virtuelle Connector dans Azure à partir de BlueXP. N'utilisez pas cette politique dans d'autres situations. Lorsque BlueXP crée le connecteur, il applique un nouvel ensemble d'autorisations à la VM Connector qui permet au connecteur de gérer les ressources de votre environnement de cloud public.

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
```

```
"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. Modifiez le fichier JSON en ajoutant votre ID d'abonnement Azure à la portée attribuable.

   Exemple

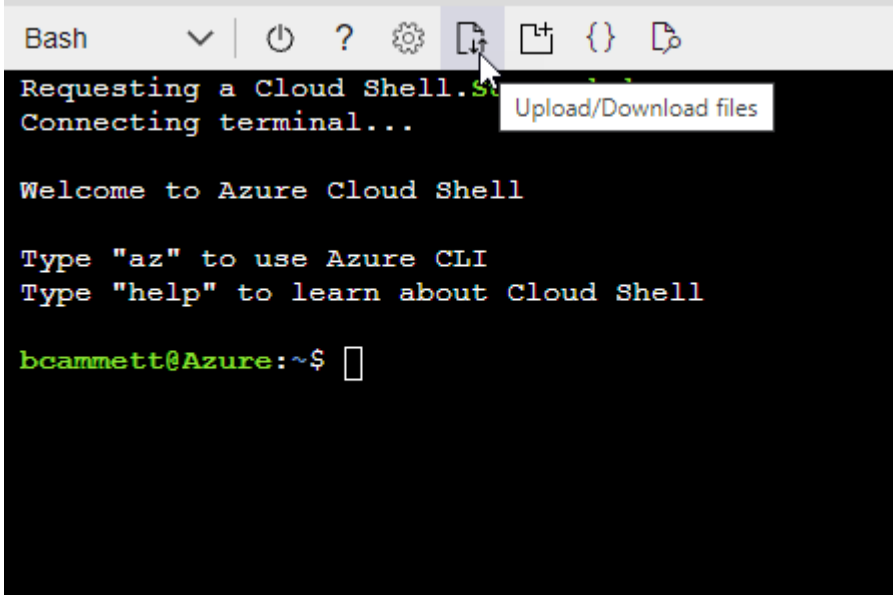
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

3. 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.

a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.

b. Téléchargez le fichier JSON.



c. Entrez la commande Azure CLI suivante :

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

Vous devez maintenant avoir un rôle personnalisé appelé *Azure SetupAsService*. Vous pouvez maintenant appliquer ce rôle personnalisé à votre compte d'utilisateur ou à un principal de service.

Étape 3 : configuration de l'authentification

Lors de la création du connecteur à partir de BlueXP, vous devez fournir un identifiant qui permet à BlueXP de s'authentifier auprès d'Azure et de déployer la machine virtuelle. Vous avez deux options :

1. Connectez-vous à l'aide de votre compte Azure lorsque vous y êtes invité. Ce compte doit disposer d'autorisations Azure spécifiques. Il s'agit de l'option par défaut.
2. Fournir des détails sur une entité de service Microsoft Entra. Ce service principal nécessite également des autorisations spécifiques.

Suivez les étapes pour préparer l'une de ces méthodes d'authentification à utiliser avec BlueXP.

Compte Azure

Attribuez le rôle personnalisé à l'utilisateur qui va déployer le connecteur à partir de BlueXP.

Étapes

1. Dans le portail Azure, ouvrez le service **Subscriptions** et sélectionnez l'abonnement de l'utilisateur.
2. Cliquez sur **contrôle d'accès (IAM)**.
3. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
   a. Sélectionnez le rôle **Azure SetupAsService** et cliquez sur **Suivant**.

   > Azure SetupAsService est le nom par défaut fourni dans la stratégie de déploiement du connecteur pour Azure. Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

   b. Conserver **utilisateur, groupe ou entité de service** sélectionnée.
   c. Cliquez sur **Sélectionner les membres**, choisissez votre compte utilisateur et cliquez sur **Sélectionner**.
   d. Cliquez sur **Suivant**.
   e. Cliquez sur **Revue + affecter**.

Résultat

L'utilisateur Azure dispose désormais des autorisations nécessaires pour déployer le connecteur depuis BlueXP.

Principal du service

Au lieu de vous connecter à votre compte Azure, vous pouvez fournir à BlueXP les identifiants d'un principal de service Azure qui dispose des autorisations requises.

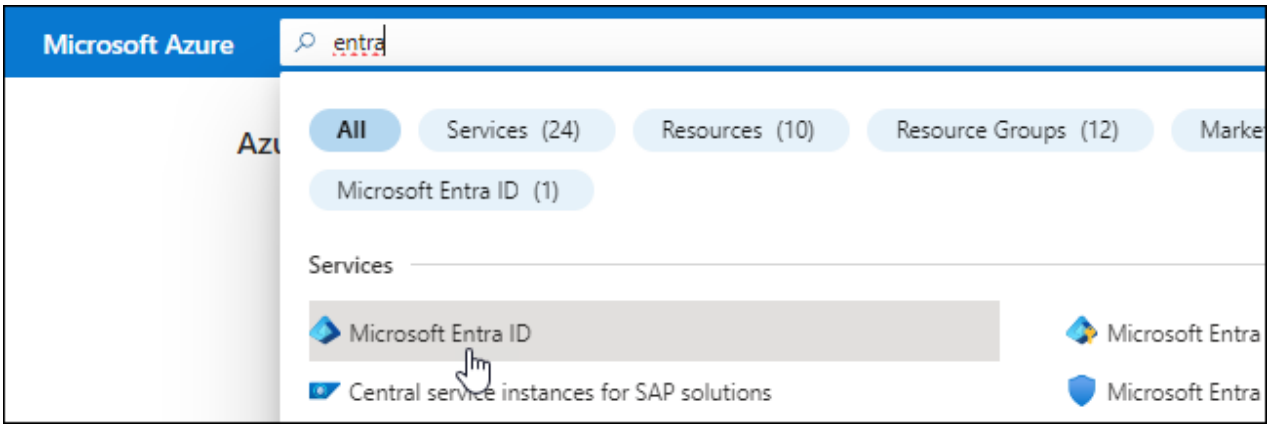
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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**.

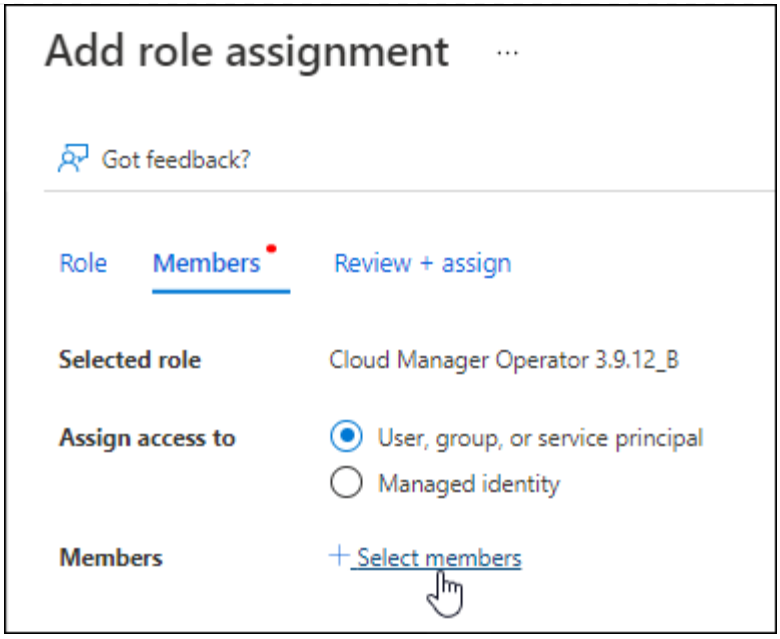
   Vous avez créé l'application AD et le principal de service.

Attribuez le rôle personnalisé à l'application

1. À partir du portail Azure, ouvrez le service **abonnements**.
2. Sélectionnez l'abonnement.
3. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
4. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et cliquez sur **Next**.
5. Dans l'onglet **membres**, procédez comme suit :

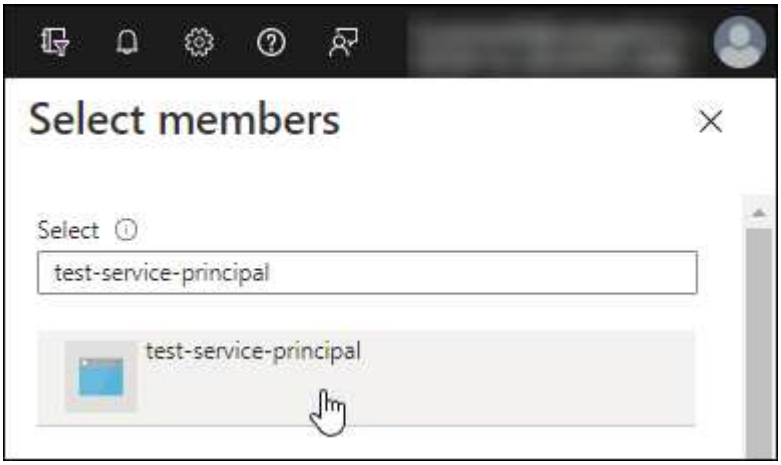
   a. Conserver **utilisateur, groupe ou entité de service** sélectionnée.

   b. Cliquez sur **Sélectionner les membres**.



c. Recherchez le nom de l'application.

   Voici un exemple :



   a. Sélectionnez l'application et cliquez sur **Sélectionner**.
   b. Cliquez sur **Suivant**.

6. Cliquez sur **Revue + affecter**.

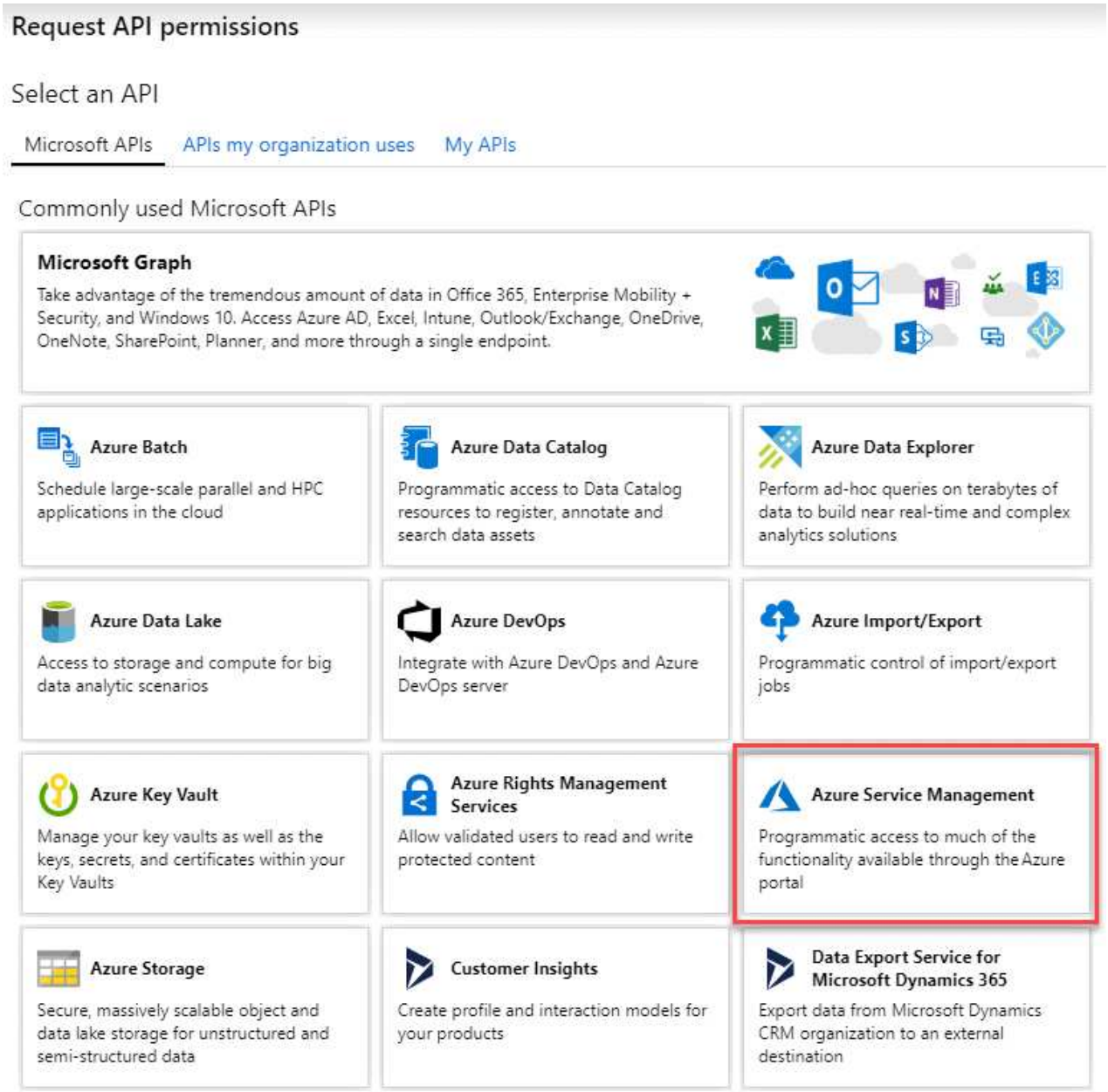
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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

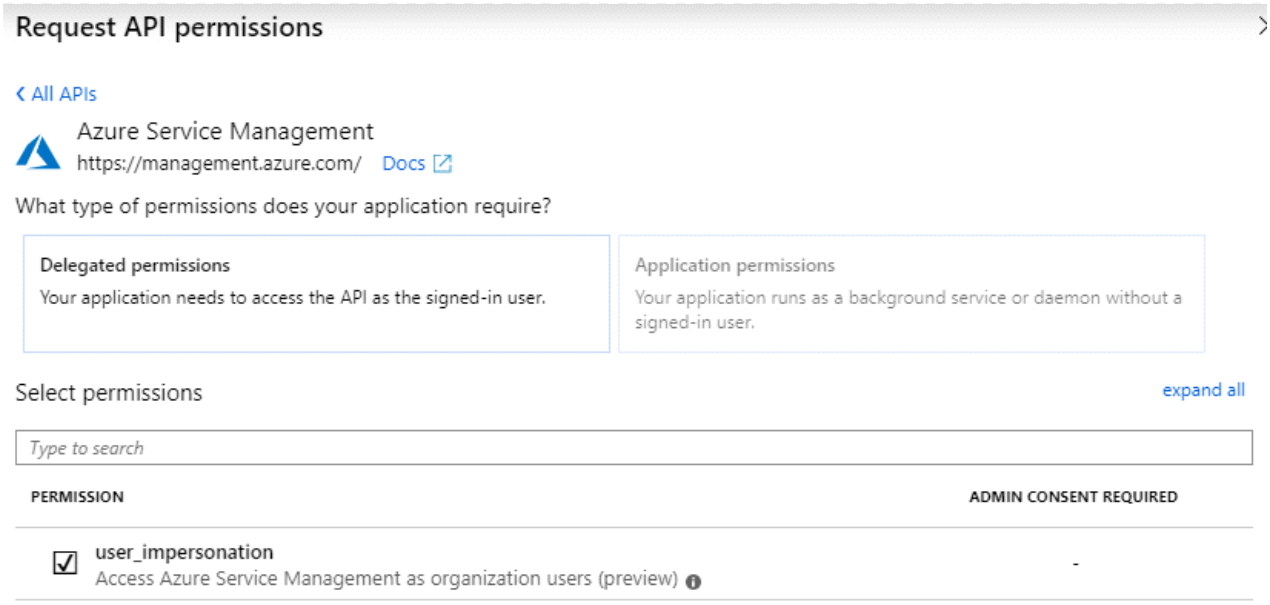
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

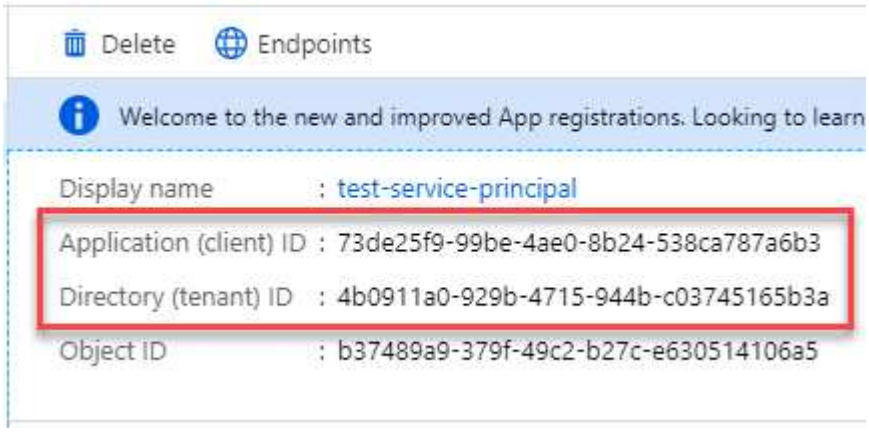


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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 créez le connecteur.

Étape 4 : créer le connecteur

Créez le connecteur directement à partir de la console web BlueXP.

Description de la tâche

La création du connecteur à partir de BlueXP déploie une machine virtuelle dans Azure à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à un type de machine virtuelle plus petit qui a moins de CPU ou de RAM. "En savoir plus sur la configuration par défaut du connecteur".

Avant de commencer

Vous devez disposer des éléments suivants :

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation nécessite un proxy pour tout le trafic Internet sortant :
  - Adresse IP
  - Informations d'identification
  - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle Connector. L'autre option de la méthode d'authentification est d'utiliser un mot de passe.

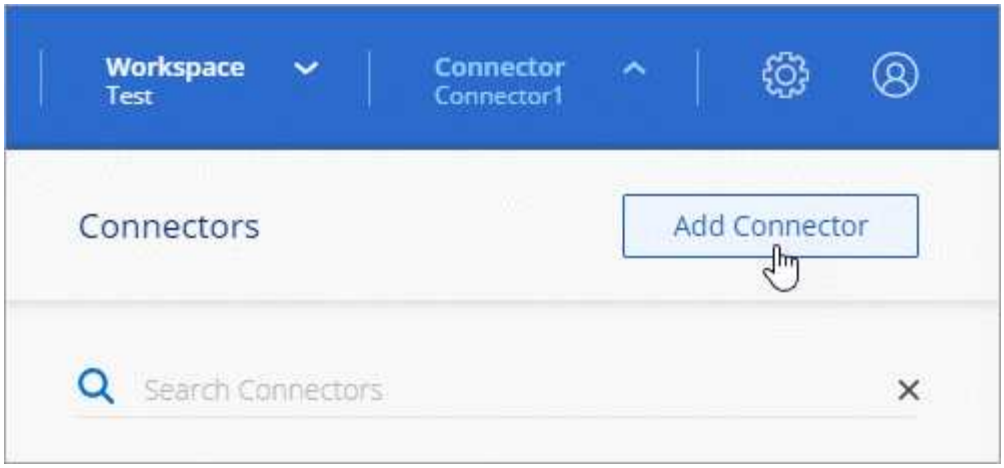
  "Découvrez comment vous connecter à une VM Linux dans Azure"

- Si vous ne souhaitez pas que BlueXP crée automatiquement un rôle Azure pour le connecteur, vous devrez créer votre propre rôle "utilisation de la stratégie sur cette page".

  Ces autorisations sont pour l'instance de connecteur elle-même. Il s'agit d'un ensemble d'autorisations différent de ce que vous avez configuré précédemment pour déployer la machine virtuelle Connector.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Microsoft Azure** comme fournisseur cloud.
3. Sur la page **déploiement d'un connecteur** :

   a. Sous **Authentication**, sélectionnez l'option d'authentification qui correspond à la façon dont vous configurez les autorisations Azure :

      - Sélectionnez **compte utilisateur Azure** pour vous connecter à votre compte Microsoft, qui doit disposer des autorisations requises.

        Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

        > Si vous êtes déjà connecté à un compte Azure, BlueXP utilisera automatiquement ce compte. Si vous avez plusieurs comptes, vous devrez peut-être vous déconnecter d'abord pour vous assurer que vous utilisez le bon compte.

      - Sélectionnez **Active Directory service principal** pour saisir des informations sur le service principal Microsoft Entra qui accorde les autorisations requises :
        - ID de l'application (client)
        - ID du répertoire (locataire)
        - Secret client

   Apprenez à obtenir ces valeurs pour un principal de service.

4. Suivez les étapes de l'assistant pour créer le connecteur :

   - **VM Authentication** : choisissez un abonnement Azure, un emplacement, un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez une méthode d'authentification pour la machine virtuelle Connector que vous créez.

     La méthode d'authentification de la machine virtuelle peut être un mot de passe ou une clé publique SSH.

   "Découvrez comment vous connecter à une VM Linux dans Azure"

   - **Détails** : saisissez un nom pour l'instance, spécifiez les balises et choisissez si vous souhaitez que BlueXP crée un nouveau rôle avec les autorisations requises ou si vous souhaitez sélectionner un rôle existant avec lequel vous avez configuré "les autorisations requises".

     Notez que vous pouvez choisir les abonnements Azure associés à ce rôle. Chaque abonnement que

vous choisissez fournit les autorisations de connecteur pour gérer les ressources de cet abonnement (par exemple, Cloud Volumes ONTAP).

- **Réseau** : choisissez un réseau VNet et un sous-réseau, si vous souhaitez activer une adresse IP publique, et spécifiez éventuellement une configuration proxy.
- **Groupe de sécurité** : choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

  "Afficher les règles des groupes de sécurité pour Azure".

- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Cliquez sur **Ajouter**.

   La machine virtuelle doit être prête en 7 minutes environ. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous disposez d'un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. "Découvrez comment gérer le stockage Azure Blob à partir de BlueXP"

Créez un connecteur à partir d'Azure Marketplace

Pour créer un connecteur à partir d'Azure Marketplace, vous devez configurer votre réseau, préparer les autorisations Azure, examiner les exigences d'instance, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le "Paire de régions Azure" Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"

Vnet et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le réseau virtuel et le sous-réseau dans lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : passez en revue les exigences relatives aux ordinateurs virtuels

Lorsque vous créez le connecteur, vous devez choisir un type de machine virtuelle répondant aux exigences suivantes.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Taille des machines virtuelles Azure

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

Étape 3 : configurer les autorisations

Vous pouvez fournir des autorisations de l'une des manières suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure en utilisant une identité gérée attribuée par le système.

- Option 2 : fournissez à BlueXP les identifiants d’un principal de service Azure qui possède les autorisations requises.

Procédez comme suit pour configurer des autorisations pour BlueXP.

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"

Étapes

1. Si vous prévoyez d'installer manuellement le logiciel sur votre propre hôte, activez une identité gérée attribuée par le système sur la machine virtuelle afin de fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'identifiant de chaque abonnement Azure que vous souhaitez utiliser avec BlueXP.

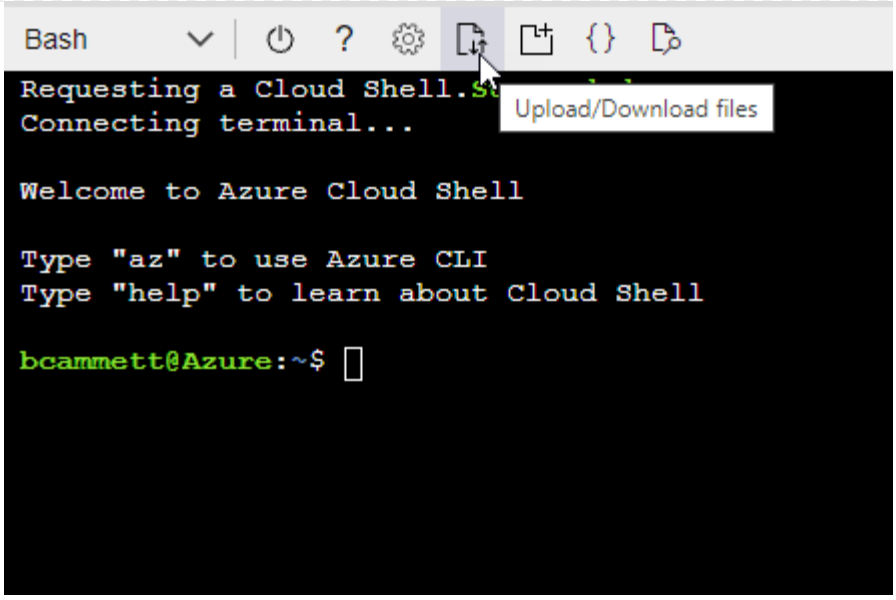
   Exemple

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

4. 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.

   a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
   b. Téléchargez le fichier JSON.



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

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

Résultat

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

Principal du service

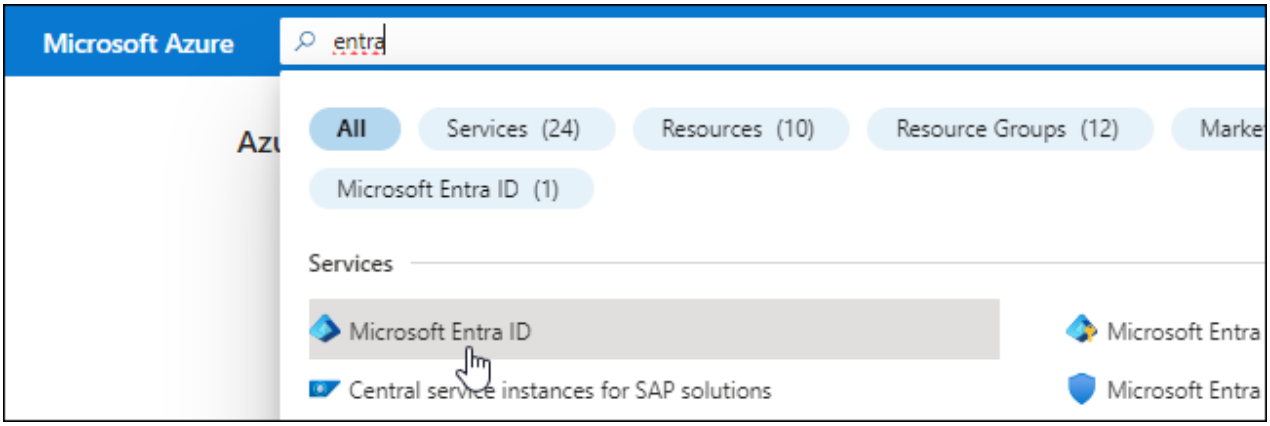
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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.

Attribuez l'application à un rôle

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.

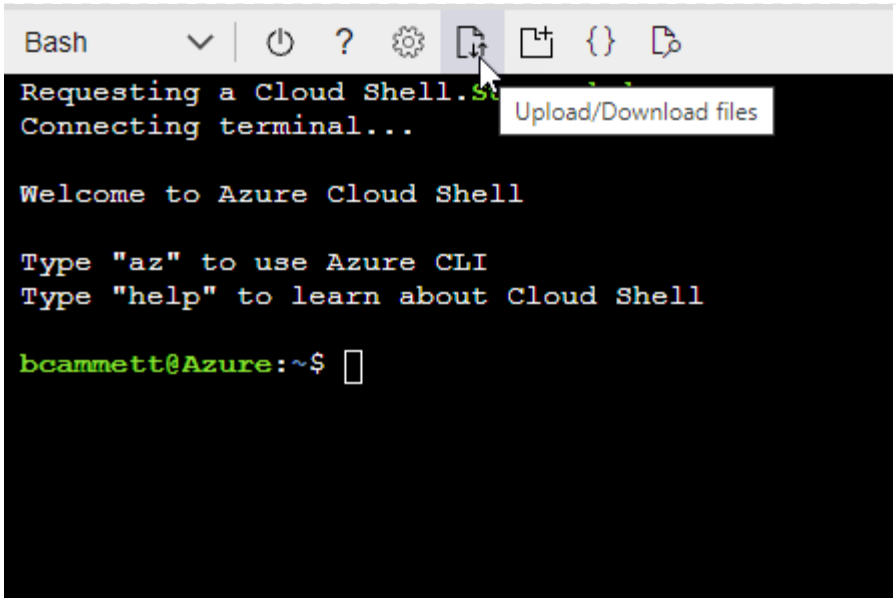
      Exemple

      ```
      "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 :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

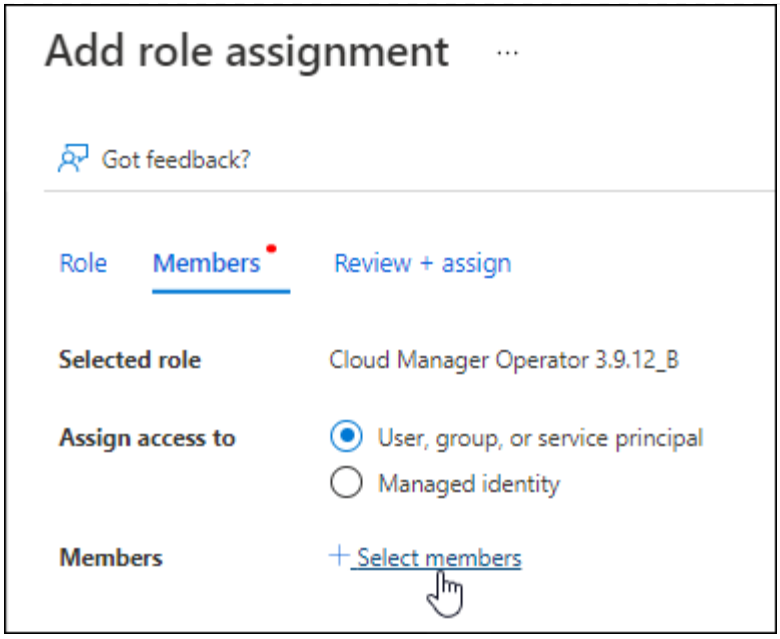
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

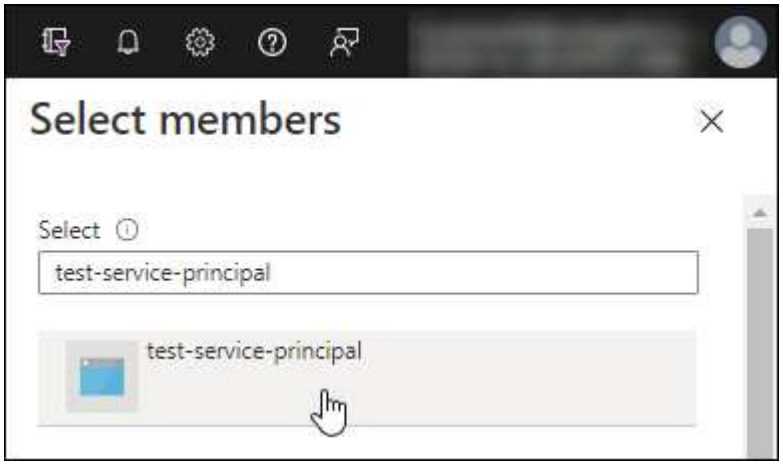
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

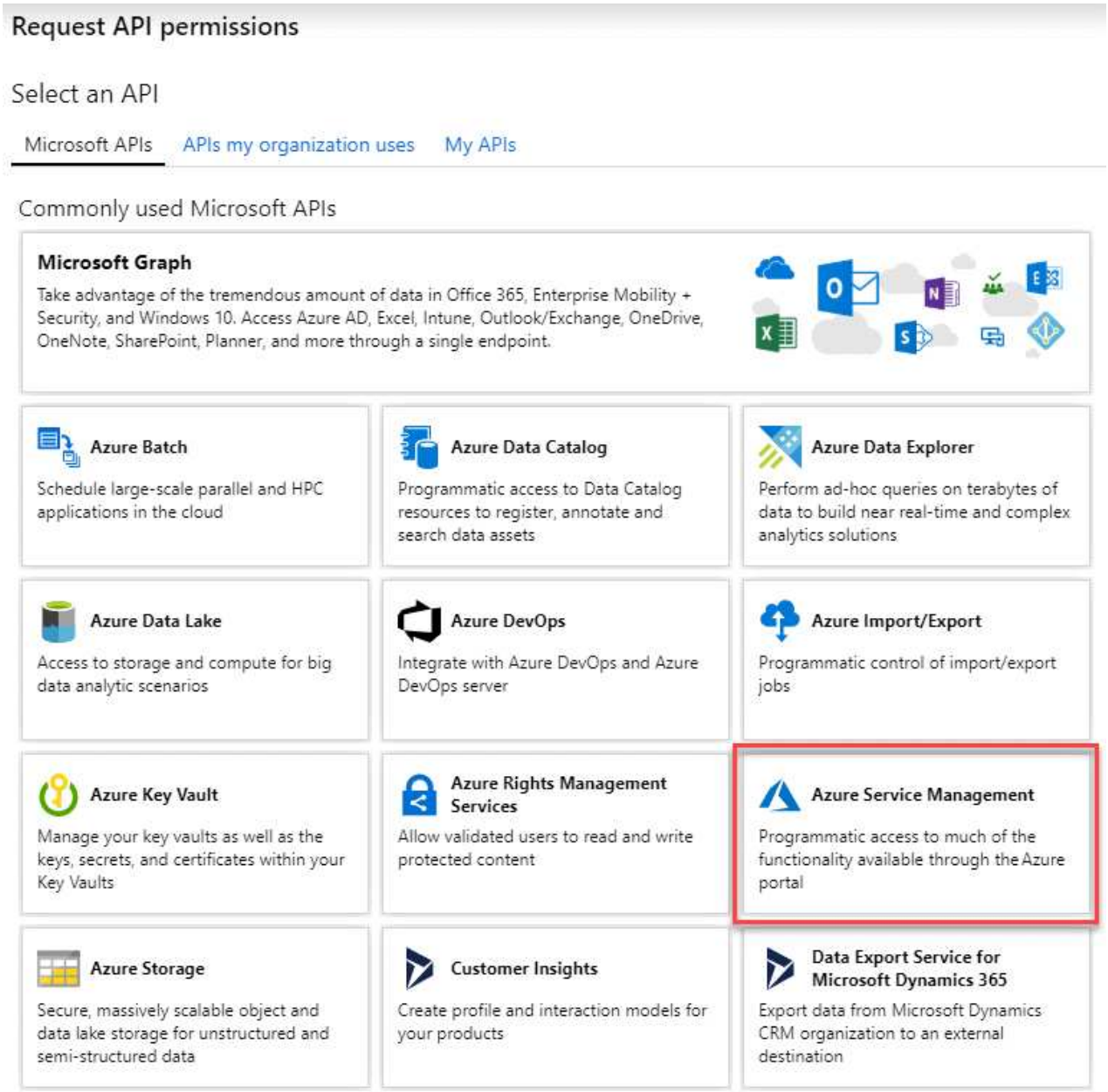
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

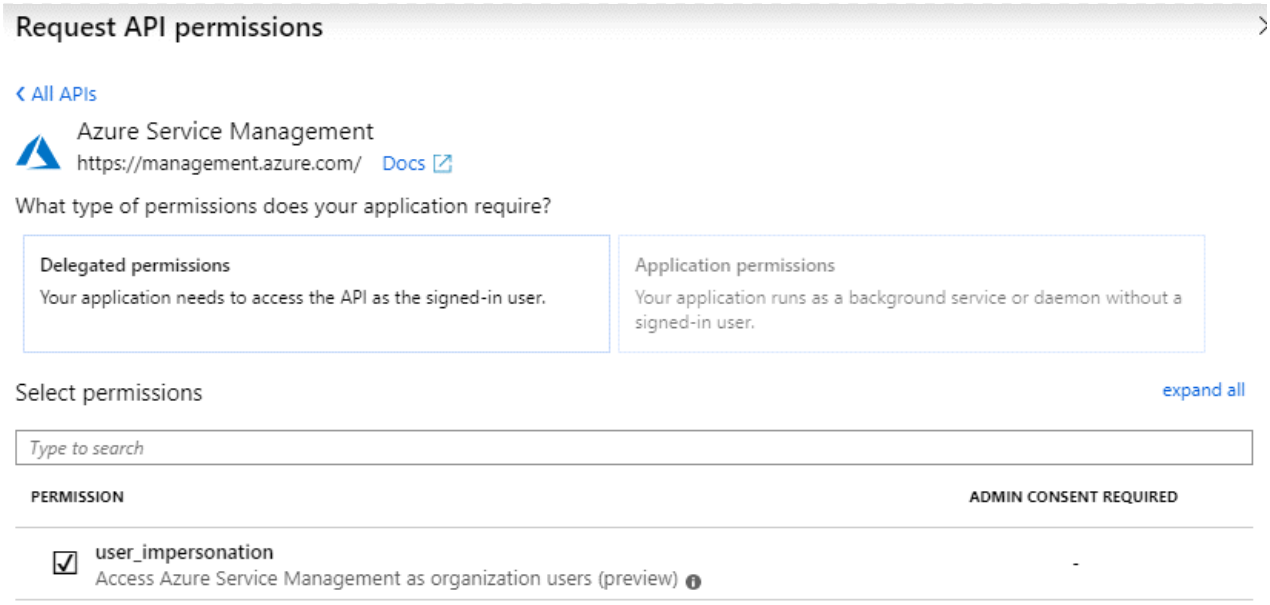
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

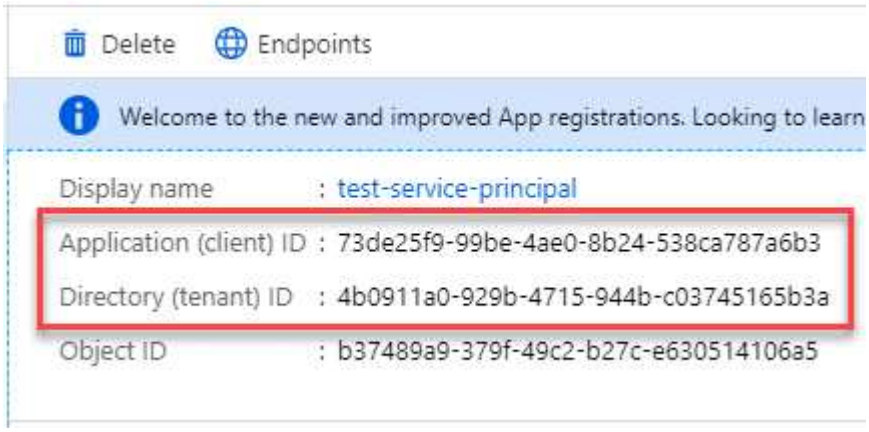


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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.

Étape 4 : créer le connecteur

Lancez Connector directement à partir d'Azure Marketplace.

Description de la tâche

La création du connecteur à partir d'Azure Marketplace déploie une machine virtuelle dans Azure à l'aide d'une configuration par défaut. "En savoir plus sur la configuration par défaut du connecteur".

Avant de commencer

Vous devez disposer des éléments suivants :

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation nécessite un proxy pour tout le trafic Internet sortant :
  - Adresse IP
  - Informations d'identification
  - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle Connector. L'autre option de la méthode d'authentification est d'utiliser un mot de passe.

  "Découvrez comment vous connecter à une VM Linux dans Azure"

- Si vous ne souhaitez pas que BlueXP crée automatiquement un rôle Azure pour le connecteur, vous devrez créer votre propre rôle "utilisation de la stratégie sur cette page".

  Ces autorisations sont pour l'instance de connecteur elle-même. Il s'agit d'un ensemble d'autorisations différent de ce que vous avez configuré précédemment pour déployer la machine virtuelle Connector.

Étapes

1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.

   "Page Azure Marketplace pour les régions commerciales"

2. Sélectionnez **obtenir maintenant**, puis **Continuer**.
3. Dans le portail Azure, sélectionnez **Create** et suivez les étapes pour configurer la machine virtuelle.

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

   - **Taille de la VM** : choisissez une taille de VM qui répond aux exigences de CPU et de RAM. Nous recommandons DS3 v2.
   - **Disques** : le connecteur peut fonctionner de manière optimale avec des disques durs ou SSD.
   - **Groupe de sécurité réseau** : le connecteur nécessite des connexions entrantes utilisant SSH, HTTP et HTTPS.

     "Afficher les règles des groupes de sécurité pour Azure".

   - **Identité** : sous **gestion**, sélectionnez **Activer l'identité gérée attribuée par le système**.

     Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Microsoft Entra ID sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Sur la page **consulter + créer**, vérifiez vos sélections et sélectionnez **Créer** pour démarrer le déploiement.

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

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

   https://ipaddress

6. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte BlueXP à associer au connecteur.
   b. Entrez un nom pour le système.
   c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

      Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "Suivez les étapes pour démarrer avec BlueXP en mode restreint".

   d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous disposez d'un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. "Découvrez comment gérer le stockage Azure Blob à partir de BlueXP"

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez créé le connecteur, vous devez fournir à BlueXP les autorisations que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et

votre infrastructure de stockage dans Azure.

Rôle personnalisé

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Sur le portail Azure, ouvrez le service **Subscriptions** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Subscriptions** car cela spécifie la portée de l'affectation de rôle au niveau de l'abonnement. Le *scope* définit l'ensemble des ressources auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau des machines virtuelles), votre capacité à effectuer des actions depuis BlueXP sera affectée.

   "Documentation Microsoft Azure : étendue du contrôle d'accès basé sur des rôles Azure"

2. Sélectionnez **contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une affectation de rôle**.
3. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

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

4. Dans l'onglet **membres**, procédez comme suit :
   a. Attribuez l'accès à une identité **gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée, sous **identité gérée**, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle du connecteur.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **consulter + affecter**.
   f. Si vous souhaitez gérer les ressources d'autres abonnements Azure, passez à cet abonnement, puis répétez ces étapes.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Et la suite ?

Accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Principal du service

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

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Installez manuellement le connecteur dans Azure

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer votre réseau, préparer les autorisations Azure, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : vérifiez la configuration requise pour l'hôte

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

Hôte dédié

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

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Taille des machines virtuelles Azure

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

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

"Voir les instructions d'installation"

Étape 2 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le "Paire de régions Azure" Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Étape 3 : configurer les autorisations

Vous devez fournir des autorisations Azure à BlueXP via l'une des options suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure en utilisant une identité gérée attribuée par le système.
- Option 2 : fournissez à BlueXP les identifiants d'un principal de service Azure qui possède les autorisations requises.

Suivez les étapes pour préparer les autorisations pour BlueXP.

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"

Étapes

1. Si vous prévoyez d'installer manuellement le logiciel sur votre propre hôte, activez une identité gérée attribuée par le système sur la machine virtuelle afin de fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'identifiant de chaque abonnement Azure que vous souhaitez utiliser avec BlueXP.

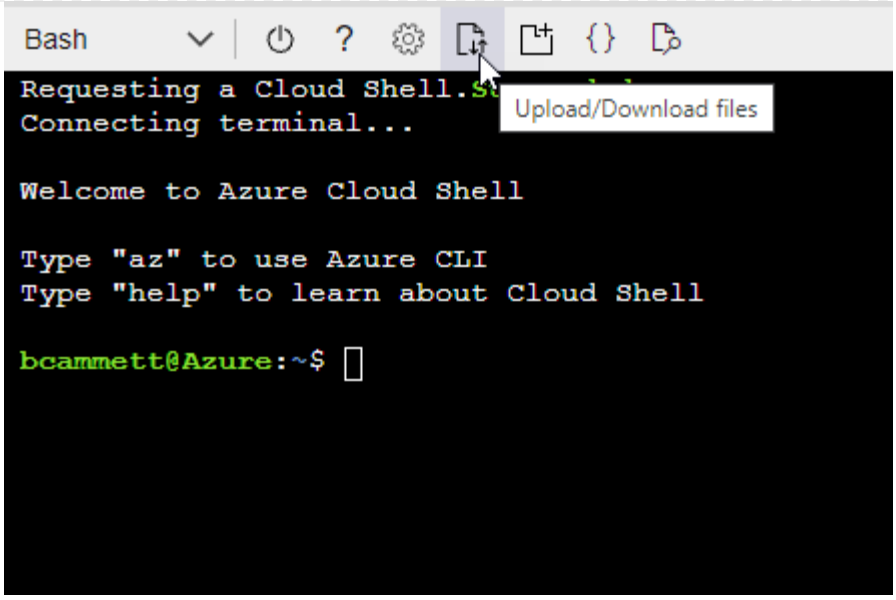
   Exemple

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

4. 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.

   a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
   b. Téléchargez le fichier JSON.



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

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

Résultat

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

Principal du service

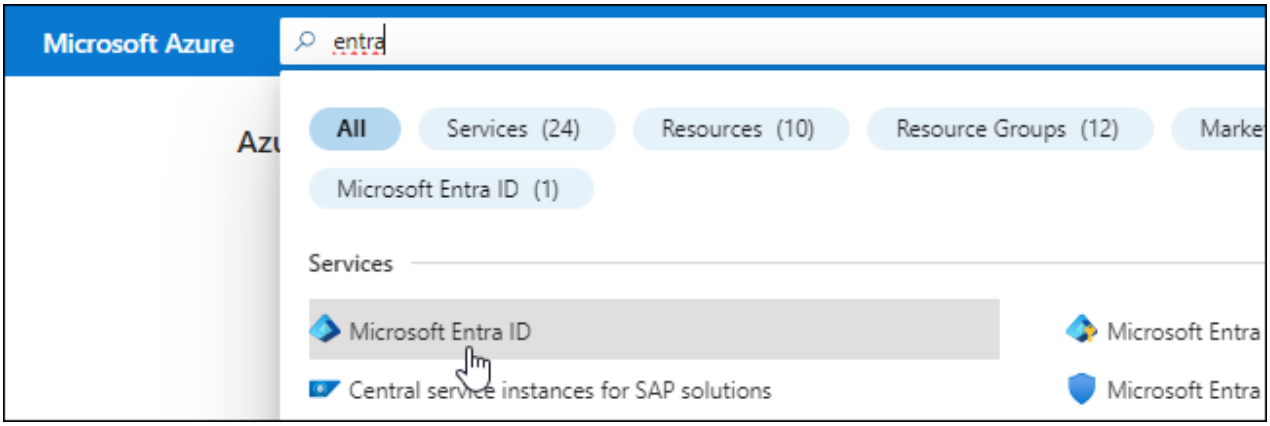
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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.

Attribuez l'application à un rôle

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.

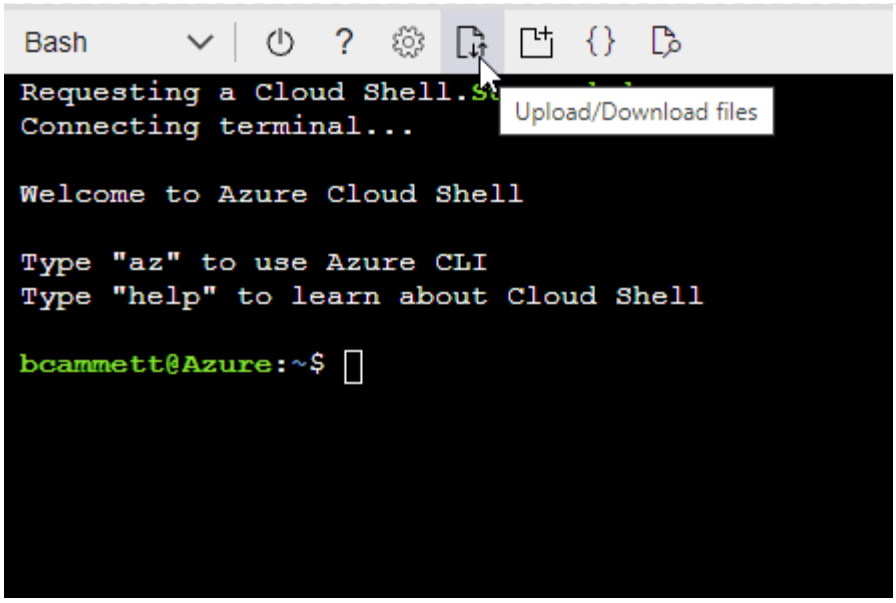
      Exemple

      ```
      "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 :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

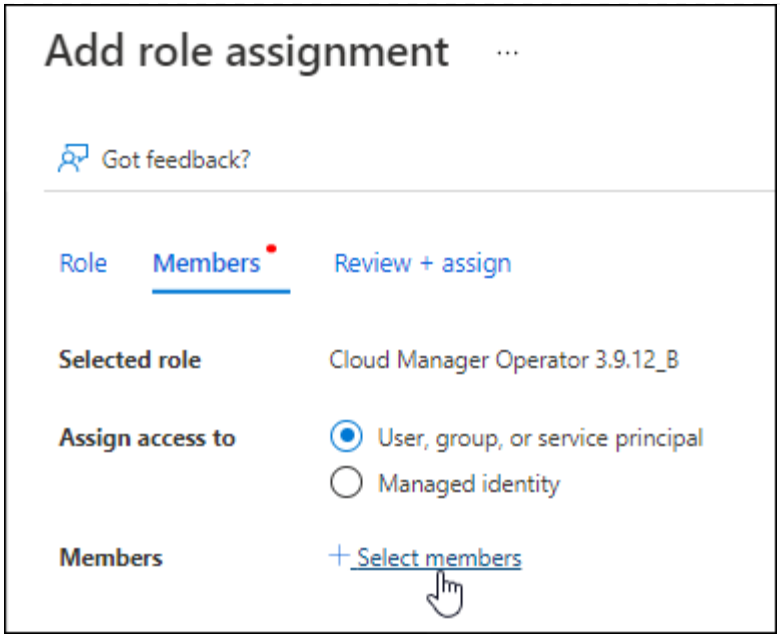
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

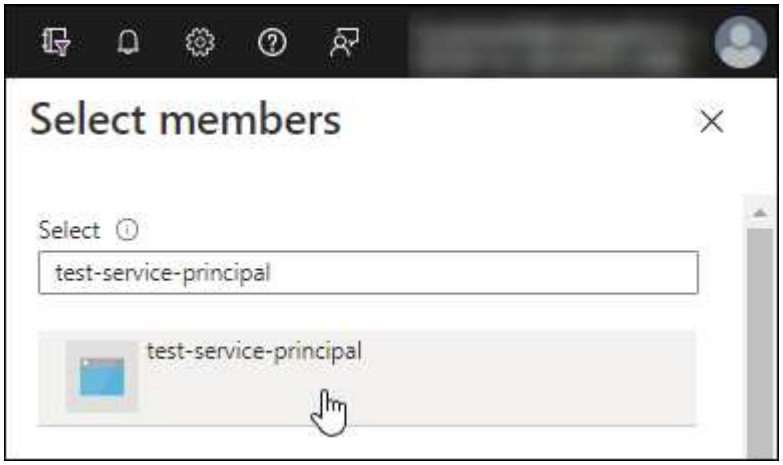
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

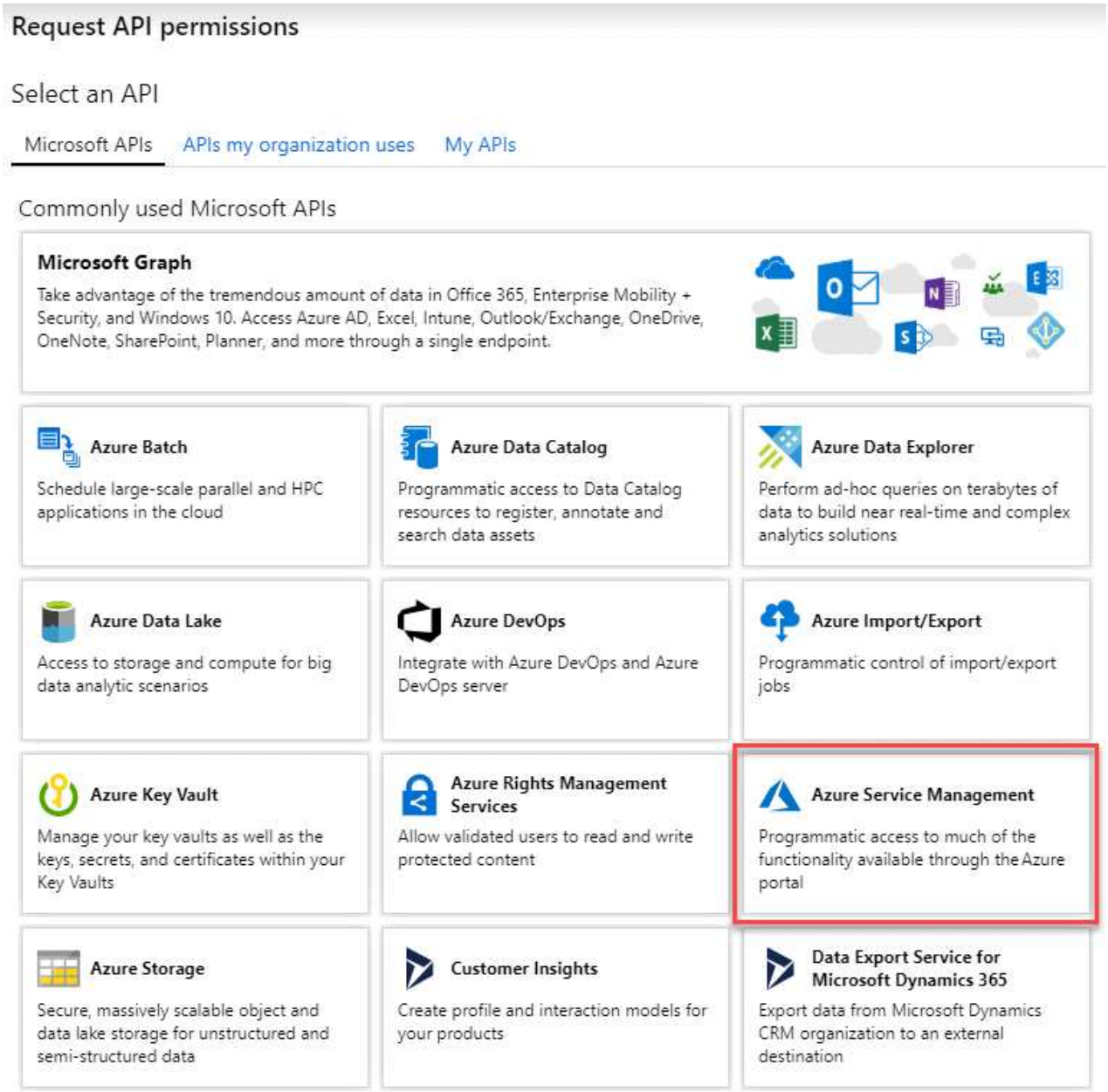
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

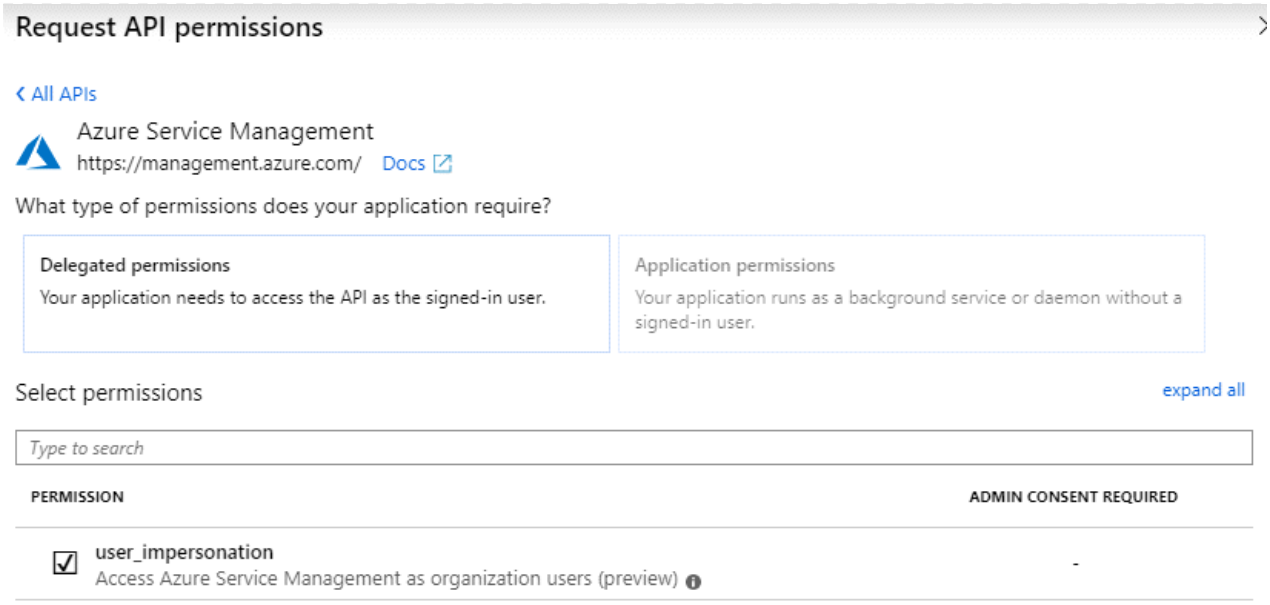
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

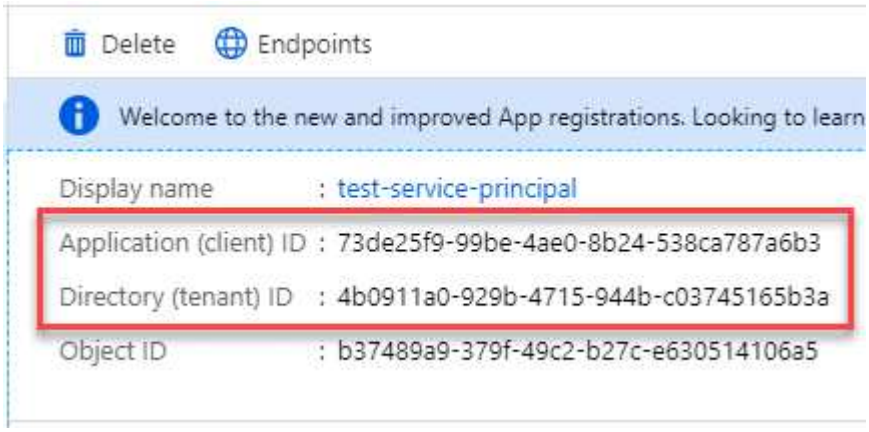


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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.

Étape 4 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.
- Identité gérée activée sur la machine virtuelle dans Azure, qui permet de fournir les autorisations Azure requises via un rôle personnalisé.

  "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

Description de la tâche

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

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

```
unset http_proxy
unset https_proxy
```

   Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Exécutez le script d'installation.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

   Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Notez ce qui suit :

- L’utilisateur peut être un utilisateur local ou un utilisateur de domaine.
- Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
- BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

--cacert spécifie un certificat signé par une autorité de certification à utiliser pour l’accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy HTTPS ou si le proxy est un proxy interceptant.

6. Attendez la fin de l’installation.

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

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

   https://ipaddress

8. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte BlueXP à associer au connecteur.
   b. Entrez un nom pour le système.
   c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

      Vous devez désactiver le mode restreint, car ces étapes décrivent l’utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d’un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c’est le cas, "Suivez les étapes pour démarrer avec BlueXP en mode restreint".

   d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous disposez d’un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. "Découvrez comment gérer le stockage Azure Blob à partir de BlueXP"

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez installé le connecteur, vous devez fournir à BlueXP les autorisations Azure que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans Azure.

Rôle personnalisé

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Sur le portail Azure, ouvrez le service **Subscriptions** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Subscriptions** car cela spécifie la portée de l'affectation de rôle au niveau de l'abonnement. Le *scope* définit l'ensemble des ressources auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau des machines virtuelles), votre capacité à effectuer des actions depuis BlueXP sera affectée.

   "Documentation Microsoft Azure : étendue du contrôle d'accès basé sur des rôles Azure"

2. Sélectionnez **contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une affectation de rôle**.
3. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

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

4. Dans l'onglet **membres**, procédez comme suit :
   a. Attribuez l'accès à une identité **gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée, sous **identité gérée**, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle du connecteur.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **consulter + affecter**.
   f. Si vous souhaitez gérer les ressources d'autres abonnements Azure, passez à cet abonnement, puis répétez ces étapes.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Et la suite ?

Accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Principal du service

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

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Google Cloud

Options d'installation de Connector dans Google Cloud

Il existe plusieurs façons de créer un connecteur dans Google Cloud. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- "Créez le connecteur directement à partir de BlueXP" (il s'agit de l'option standard)

  Cette action lance une instance de serveur virtuel exécutant Linux et le logiciel Connector dans un VPC de votre choix.

- "Créer le connecteur à l'aide de gcloud"

  Cette action lance également une instance de VM exécutant Linux et le logiciel Connector, mais le déploiement est initié directement depuis Google Cloud plutôt que depuis BlueXP.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans Google Cloud.

Créez un connecteur dans Google Cloud à partir de BlueXP ou gcloud

Pour créer un connecteur dans Google Cloud à partir de BlueXP ou à l'aide de gcloud, vous devez configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.

Terminaux	Objectif
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

"Consultez la liste des terminaux contactés depuis la console BlueXP".

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : définissez les autorisations nécessaires pour créer le connecteur

Avant de déployer un connecteur à partir de BlueXP ou à l'aide de gcloud, vous devez définir des autorisations pour l'utilisateur Google Cloud qui va déployer la VM Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

    a. Créez un fichier YAML qui inclut les autorisations suivantes :

```yaml
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
```

```
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Dans Google Cloud, activez le shell cloud.

c. Téléchargez le fichier YAML qui inclut les autorisations requises.

d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

   L'exemple suivant crée un rôle nommé « connectorDeployment » au niveau du projet :

   Les rôles iam gcloud créent connectDeployment --project=myproject --file=Connector-deployment.yaml

"Documents Google Cloud : création et gestion de rôles personnalisés"

2. Attribuez ce rôle personnalisé à l'utilisateur qui va déployer le connecteur à partir de BlueXP ou à l'aide de gcloud.

   "Documents Google Cloud : attribuez un rôle unique"

Résultat

L'utilisateur Google Cloud dispose désormais des autorisations nécessaires pour créer le connecteur.

Étape 3 : définissez les autorisations pour le connecteur

Un compte de service Google Cloud est requis pour fournir le connecteur avec les autorisations dont BlueXP a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez le connecteur, vous devez associer ce compte de service à la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut le contenu du "Autorisations de compte de service pour le connecteur".

   b. Dans Google Cloud, activez le shell cloud.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises.

   d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

      L'exemple suivant crée un rôle nommé « connecteur » au niveau du projet :

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Documents Google Cloud : création et gestion de rôles personnalisés"

2. Créer un compte de service dans Google Cloud et attribuer le rôle au compte de service :

   a. Dans le service IAM & Admin, sélectionnez **comptes de service > Créer un compte de service**.

   b. Entrez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

      "Documents Google Cloud : création d'un compte de service"

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans différents projets que le projet sur lequel réside le connecteur, vous devrez fournir au compte de service du connecteur l'accès à ces projets.

   Disons, par exemple, que le connecteur est dans le projet 1 et que vous voulez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

   a. Dans le service IAM & Admin, sélectionnez le projet Google Cloud où vous souhaitez créer les systèmes Cloud Volumes ONTAP.

   b. Sur la page **IAM**, sélectionnez **accorder accès** et fournissez les détails nécessaires.

      - Saisissez l'e-mail du compte de service du connecteur.
      - Sélectionnez le rôle personnalisé du connecteur.
      - Sélectionnez **Enregistrer**.

   Pour plus de détails, reportez-vous à "Documentation Google Cloud"

Résultat

Le compte de service de la machine virtuelle Connector est configuré.

Étape 4 : configuration des autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter la table des autorisations lorsque la configuration IAM est terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte Google pour déployer le connecteur	Personnalisées	Projet de service	"Stratégie de déploiement de connecteur"	compute.networkUser	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	"Stratégie de compte de service de connecteur"	compute.networkUser deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Personnalisées	Projet de service	storage.admin Membre: Compte de service BlueXP à partir de serviceAccount.user	S/O	(Facultatif) pour le Tiering des données et la sauvegarde et la restauration BlueXP
Agent de service Google API	Google Cloud	Projet de service	Editeur (par défaut)	compute.networkUser	Interagit avec les API Google Cloud pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.
Compte de service par défaut Google Compute Engine	Google Cloud	Projet de service	Editeur (par défaut)	compute.networkUser	Déploie les instances Google Cloud et l'infrastructure de calcul pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.Editor est uniquement requis au niveau du projet hôte si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. BlueXP créera un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. Firewall.create et firewall.delete ne sont nécessaires que si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte BlueXP. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.

3. Pour le Tiering des données, le compte de service de Tiering doit avoir le rôle serviceAccount.user sur le compte de service, et pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 5 : activez les API Google Cloud

Vous devez activer plusieurs API Google Cloud avant de pouvoir déployer le connecteur et Cloud Volumes ONTAP dans Google Cloud.

Étape

1. Activez les API Google Cloud suivantes dans votre projet :
   - API Cloud Deployment Manager V2
   - API de journalisation cloud
   - API Cloud Resource Manager
   - API du moteur de calcul
   - API de gestion des identités et des accès
   - API KMS (Cloud Key Management Service

     (Requis uniquement si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec des clés de chiffrement gérées par le client (CMEK))

"Documentation Google Cloud : activation des API"

Étape 6 : créer le connecteur

Créez un connecteur directement à partir de la console web BlueXP ou à l'aide de gcloud.

Description de la tâche

La création du connecteur déploie une instance de machine virtuelle dans Google 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. "En savoir plus sur la configuration par défaut du connecteur".

BlueXP

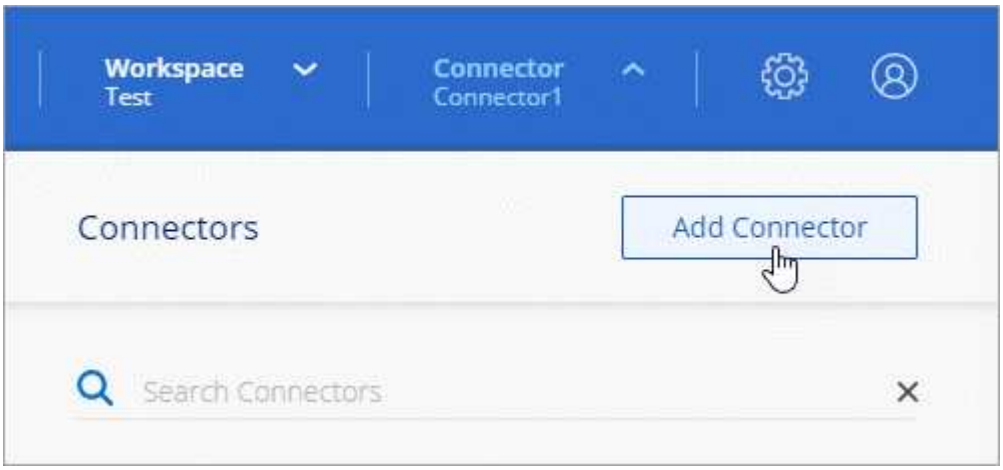
Avant de commencer

Vous devez disposer des éléments suivants :

- Les autorisations Google Cloud requises pour créer le connecteur et un compte de service pour la VM Connector.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Google Cloud Platform** comme fournisseur de cloud.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
   a. Sélectionnez **Continuer** pour préparer le déploiement à l'aide du guide produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
   b. Sélectionnez **passer au déploiement** si vous êtes déjà préparé en suivant les étapes de cette page.
4. Suivez les étapes de l'assistant pour créer le connecteur :
   - Si vous y êtes invité, connectez-vous à votre compte Google, qui devrait disposer des autorisations requises pour créer l'instance de machine virtuelle.

     Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.
   - **Détails** : saisissez un nom pour l'instance de machine virtuelle, spécifiez des balises, sélectionnez un projet, puis sélectionnez le compte de service qui dispose des autorisations requises (reportez-vous à la section ci-dessus pour plus de détails).
   - **Location** : spécifiez une région, une zone, un VPC et un sous-réseau pour l'instance.
   - **Réseau** : permet d'activer ou non une adresse IP publique et de spécifier éventuellement une configuration proxy.
   - **Stratégie de pare-feu** : choisissez de créer une nouvelle politique de pare-feu ou de sélectionner une politique de pare-feu existante qui autorise les règles entrantes et sortantes requises.

"Règles de pare-feu dans Google Cloud"

- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Sélectionnez **Ajouter**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous avez des compartiments Google Cloud Storage dans le même compte Google Cloud où vous avez créé le connecteur, un environnement de travail Google Cloud Storage s'affiche automatiquement sur le canevas BlueXP. "Découvrez comment gérer le stockage Google Cloud à partir de BlueXP"

gcloud

Avant de commencer

Vous devez disposer des éléments suivants :

- Les autorisations Google Cloud requises pour créer le connecteur et un compte de service pour la VM Connector.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Compréhension des exigences des instances VM.
  - **CPU** : 4 cœurs ou 4 vCPU
  - **RAM**: 14 GO
  - **Type de machine**: Nous recommandons n2-standard-4.

    Le connecteur est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation qui prend en charge les fonctionnalités de machine virtuelle blindée.

Étapes

1. Connectez-vous au SDK gcloud à l'aide de la méthodologie que vous préférez.

   Dans nos exemples, nous allons utiliser un shell local avec le SDK gcloud installé, mais vous pouvez utiliser le Google Cloud Shell natif dans la console Google Cloud.

   Pour plus d'informations sur le kit de développement logiciel Google Cloud, rendez-vous sur le "Page de documentation du SDK Google Cloud".

2. Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des autorisations requises définies dans la section ci-dessus :

   ```
   gcloud auth list
   ```

   Le résultat doit indiquer les éléments suivants où le compte d'utilisateur * est le compte d'utilisateur souhaité pour être connecté en tant que :

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Exécutez le `gcloud compute instances create` commande :

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nom de l'instance
: Nom d'instance souhaité pour l'instance de VM.

projet
: (Facultatif) le projet où vous souhaitez déployer la machine virtuelle.

compte de service
: Compte de service spécifié dans la sortie de l'étape 2.

zone
: La zone où vous souhaitez déployer la machine virtuelle

pas d'adresse
: (Facultatif) aucune adresse IP externe n'est utilisée (vous avez besoin d'un NAT ou d'un proxy cloud pour acheminer le trafic vers l'Internet public)

balise réseau
: (Facultatif) Ajouter un marquage réseau pour lier une règle de pare-feu à l'aide de balises à l'instance de connecteur

chemin du réseau

(Facultatif) Ajoutez le nom du réseau dans lequel déployer le connecteur (pour un VPC partagé, vous avez besoin du chemin complet)

chemin-sous-réseau

(Facultatif) Ajouter le nom du sous-réseau dans lequel déployer le connecteur (pour un VPC partagé, vous devez disposer du chemin complet)

km-key-path

(Facultatif) Ajouter une clé KMS pour chiffrer les disques du connecteur (les autorisations IAM doivent également être appliquées)

Pour plus d'informations sur ces indicateurs, visitez le "Documentation du kit de développement logiciel de calcul Google Cloud".

+
L'exécution de la commande déploie le connecteur à l'aide de l'image de référence NetApp. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

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

   https://ipaddress

2. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte BlueXP à associer au connecteur.

      "Découvrez les comptes BlueXP".

   b. Entrez un nom pour le système.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Ouvrez un navigateur Web et accédez au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Installez manuellement le connecteur dans Google Cloud

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : vérifiez la configuration requise pour l'hôte

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

Hôte dédié

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

Systèmes d’exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L’hôte doit être enregistré auprès de Red Hat Subscription Management. S’il n’est pas enregistré, l’hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l’installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l’exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type de machine Google Cloud

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

Ce connecteur est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d’exploitation pris en charge "Fonctionnalités MV blindées"

Espace disque dans /opt

100 Gio d’espace doit être disponible

Espace disque dans /var

20 Gio d’espace doit être disponible

Moteur Docker

Docker Engine est requis sur l’hôte avant d’installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

  "Voir les instructions d’installation"

Étape 2 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.

Terminaux	Objectif
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Étape 3 : définissez les autorisations pour le connecteur

Un compte de service Google Cloud est requis pour fournir le connecteur avec les autorisations dont BlueXP a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez le connecteur, vous devez associer ce compte de service à la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut le contenu du "Autorisations de compte de service pour le connecteur".

   b. Dans Google Cloud, activez le shell cloud.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises.

   d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

      L'exemple suivant crée un rôle nommé « connecteur » au niveau du projet :

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Documents Google Cloud : création et gestion de rôles personnalisés"

2. Créer un compte de service dans Google Cloud et attribuer le rôle au compte de service :

   a. Dans le service IAM & Admin, sélectionnez **comptes de service > Créer un compte de service**.

   b. Entrez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

      "Documents Google Cloud : création d'un compte de service"

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans différents projets que le projet sur lequel réside le connecteur, vous devrez fournir au compte de service du connecteur l'accès à ces projets.

   Disons, par exemple, que le connecteur est dans le projet 1 et que vous voulez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

   a. Dans le service IAM & Admin, sélectionnez le projet Google Cloud où vous souhaitez créer les systèmes Cloud Volumes ONTAP.

   b. Sur la page **IAM**, sélectionnez **accorder accès** et fournissez les détails nécessaires.

      - Saisissez l'e-mail du compte de service du connecteur.
      - Sélectionnez le rôle personnalisé du connecteur.
      - Sélectionnez **Enregistrer**.

   Pour plus de détails, reportez-vous à "Documentation Google Cloud"

Résultat

Le compte de service de la machine virtuelle Connector est configuré.

Étape 4 : configuration des autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter la table des autorisations lorsque la configuration IAM est terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte Google pour déployer le connecteur	Personnalisées	Projet de service	"Stratégie de déploiement de connecteur"	compute.networkUser	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	"Stratégie de compte de service de connecteur"	compute.networkUser deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Personnalisées	Projet de service	storage.admin Membre: Compte de service BlueXP à partir de serviceAccount.user	S/O	(Facultatif) pour le Tiering des données et la sauvegarde et la restauration BlueXP
Agent de service Google API	Google Cloud	Projet de service	Editeur (par défaut)	compute.networkUser	Interagit avec les API Google Cloud pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.
Compte de service par défaut Google Compute Engine	Google Cloud	Projet de service	Editeur (par défaut)	compute.networkUser	Déploie les instances Google Cloud et l'infrastructure de calcul pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.Editor est uniquement requis au niveau du projet hôte si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. BlueXP créera un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. Firewall.create et firewall.delete ne sont nécessaires que si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte BlueXP. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.

3. Pour le Tiering des données, le compte de service de Tiering doit avoir le rôle serviceAccount.user sur le compte de service, et pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 5 : activez les API Google Cloud

Vous devez activer plusieurs API Google Cloud avant de pouvoir déployer les systèmes Cloud Volumes ONTAP dans Google Cloud.

Étape

1. Activez les API Google Cloud suivantes dans votre projet :
   - API Cloud Deployment Manager V2
   - API de journalisation cloud
   - API Cloud Resource Manager
   - API du moteur de calcul
   - API de gestion des identités et des accès
   - API KMS (Cloud Key Management Service

     (Requis uniquement si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec des clés de chiffrement gérées par le client (CMEK))

"Documentation Google Cloud : activation des API"

Étape 6 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.

Description de la tâche

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

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

```
unset http_proxy
unset https_proxy
```

   Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Exécutez le script d'installation.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

   Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port

- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Notez ce qui suit :

  - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
  - Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
  - BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

--cacert spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy HTTPS ou si le proxy est un proxy interceptant.

6. Attendez la fin de l'installation.

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

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

   https://ipaddress

8. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte BlueXP à associer au connecteur.
   b. Entrez un nom pour le système.
   c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

      Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "Suivez les étapes pour démarrer avec BlueXP en mode restreint".

   d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous avez des compartiments Google Cloud Storage dans le même compte Google Cloud où vous avez créé le connecteur, un environnement de travail Google Cloud Storage s'affiche automatiquement sur le canevas BlueXP. "Découvrez comment gérer le stockage Google Cloud à partir de BlueXP"

Étape 7 : fournissez des autorisations à BlueXP

Vous devez fournir à BlueXP les autorisations Google Cloud que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans Google Cloud.

Étapes

1. Accédez au portail Google Cloud et attribuez le compte de service à l'instance de la VM Connector.

   "Documentation Google Cloud : modification du compte de service et des étendues d'accès pour une

instance"

2. Si vous souhaitez gérer des ressources dans d'autres projets Google Cloud, autorisez l'accès en ajoutant le compte de service doté du rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions en votre nom dans Google Cloud.

Installez et configurez un connecteur sur site

Installez un connecteur sur site, puis connectez-vous et configurez-le pour qu'il fonctionne avec votre compte BlueXP.

Avant de commencer

Vous devriez passer en revue "Limitations du connecteur".

Étape 1 : vérifiez la configuration requise pour l'hôte

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc. Assurez-vous que votre hôte répond à ces exigences avant d'installer le connecteur.

Hôte dédié

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

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

  "Voir les instructions d'installation"

Étape 2 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Points d'extrémité contactés depuis le connecteur

Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.

Terminaux	Objectif
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Étape 3 : configurez les autorisations cloud

Si vous souhaitez utiliser les services BlueXP dans AWS ou Azure avec un connecteur sur site, vous devez configurer des autorisations dans votre fournisseur cloud afin de pouvoir ajouter les informations d'identification au connecteur une fois que vous l'avez installé.

> Pourquoi ne pas Google Cloud ? Une fois le connecteur installé sur votre site, il ne peut pas gérer vos ressources dans Google Cloud. Le connecteur doit être installé dans Google Cloud pour gérer toutes les ressources qui y résident.

AWS

Lorsque le connecteur est installé sur site, vous devez fournir BlueXP avec des autorisations AWS en ajoutant des clés d'accès à un utilisateur IAM qui dispose des autorisations requises.

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

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :

   a. Sélectionnez **stratégies > Créer une stratégie**.

   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".

   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle.

   Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".

3. Associer les règles à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"
4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à BlueXP après l'installation du connecteur.

Résultat

Vous devez maintenant disposer des clés d'accès pour un utilisateur IAM qui dispose des autorisations requises. Après avoir installé le connecteur, vous devez associer ces informations d'identification au connecteur de BlueXP.

Azure

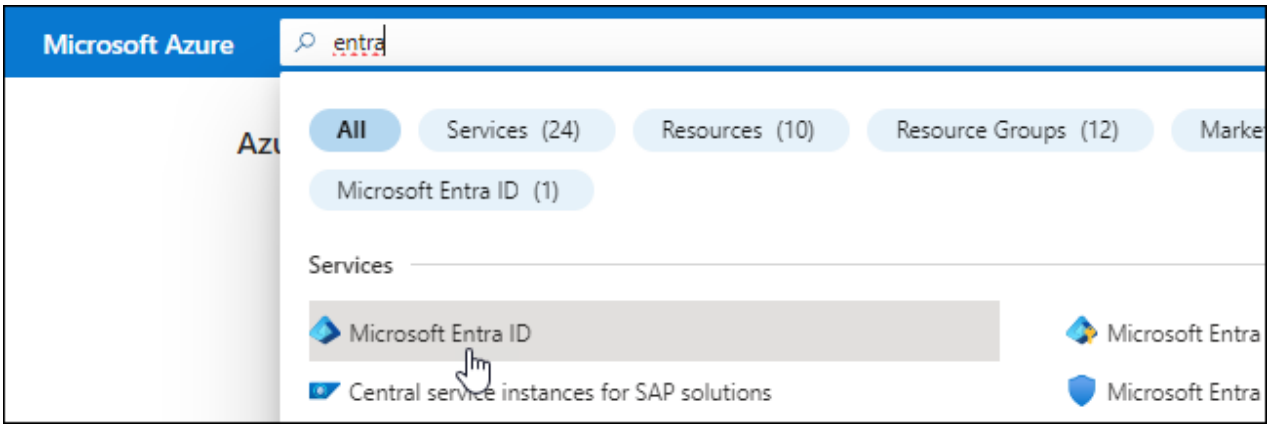
Lorsque le connecteur est installé sur site, vous devez fournir BlueXP avec des autorisations Azure en configurant une entité de service dans Microsoft Entra ID et en obtenant les identifiants Azure requis par BlueXP.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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.

Attribuez l'application à un rôle

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.

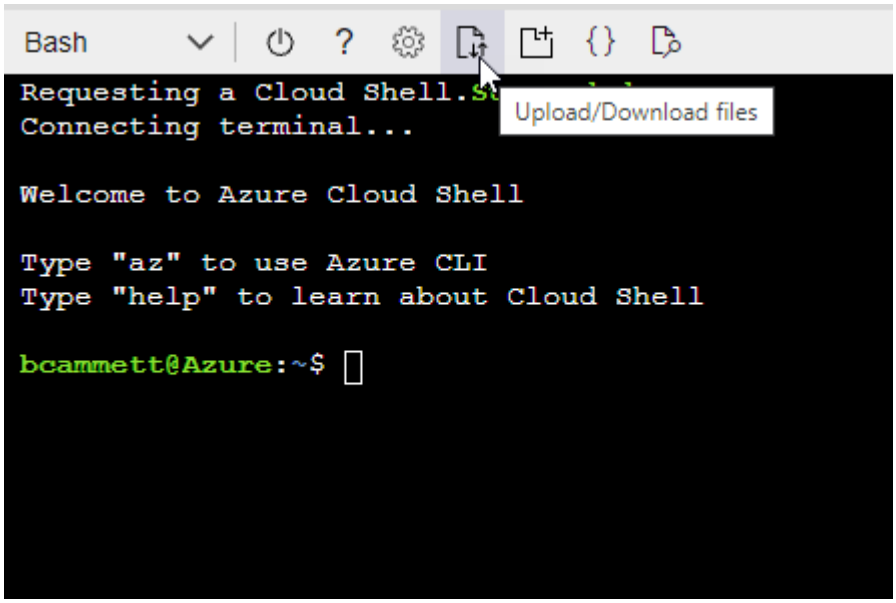
      Exemple

      ```
      "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 :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

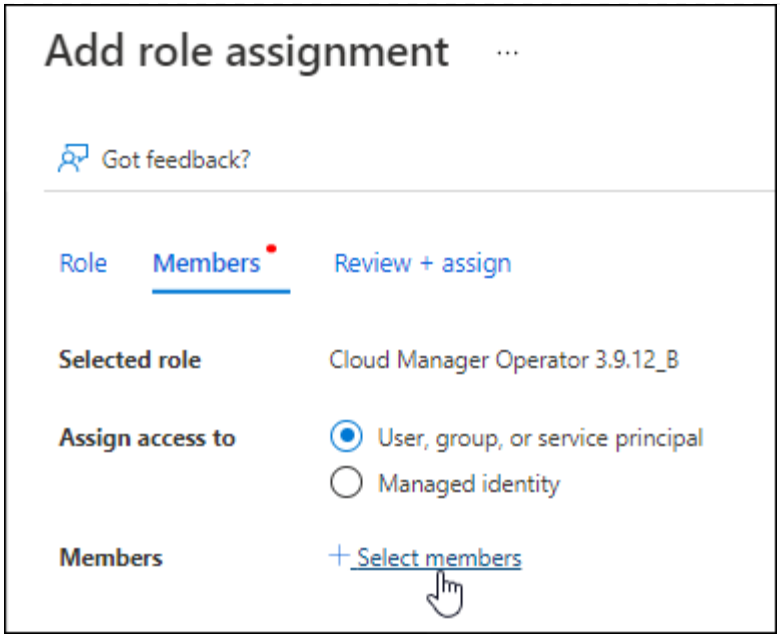
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

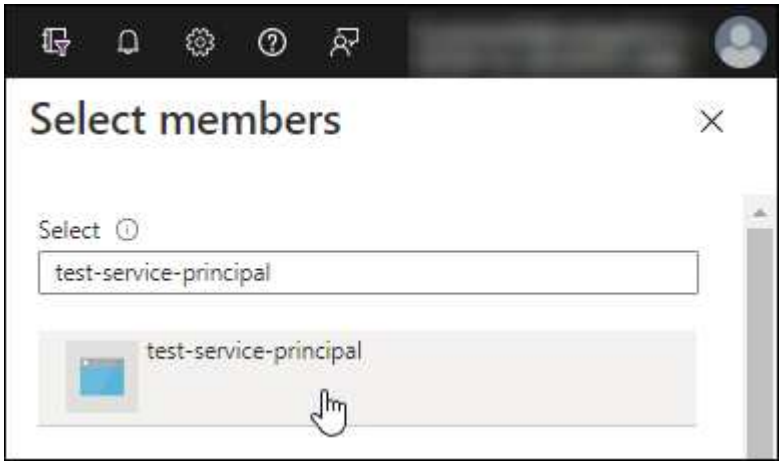
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

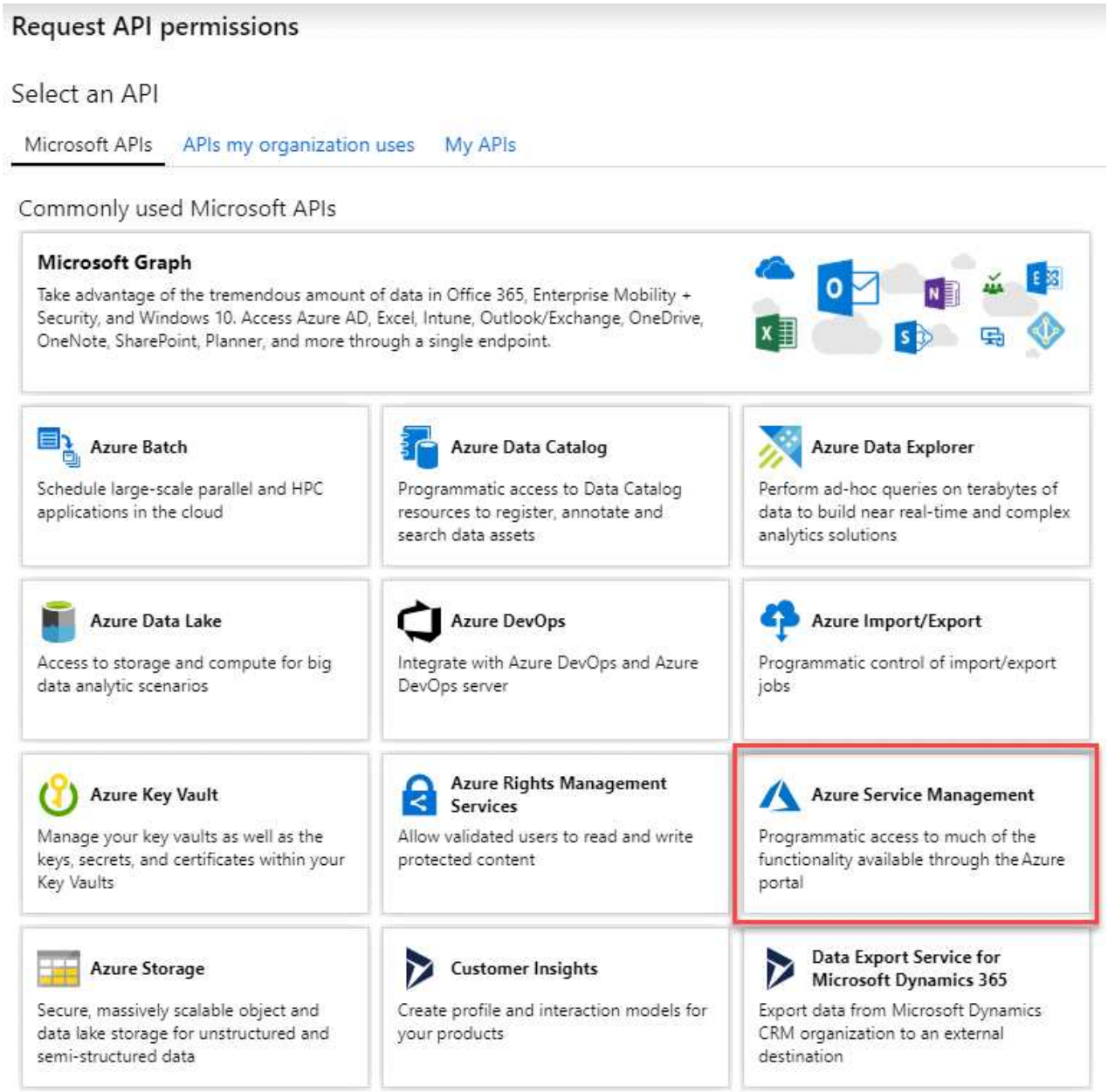
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

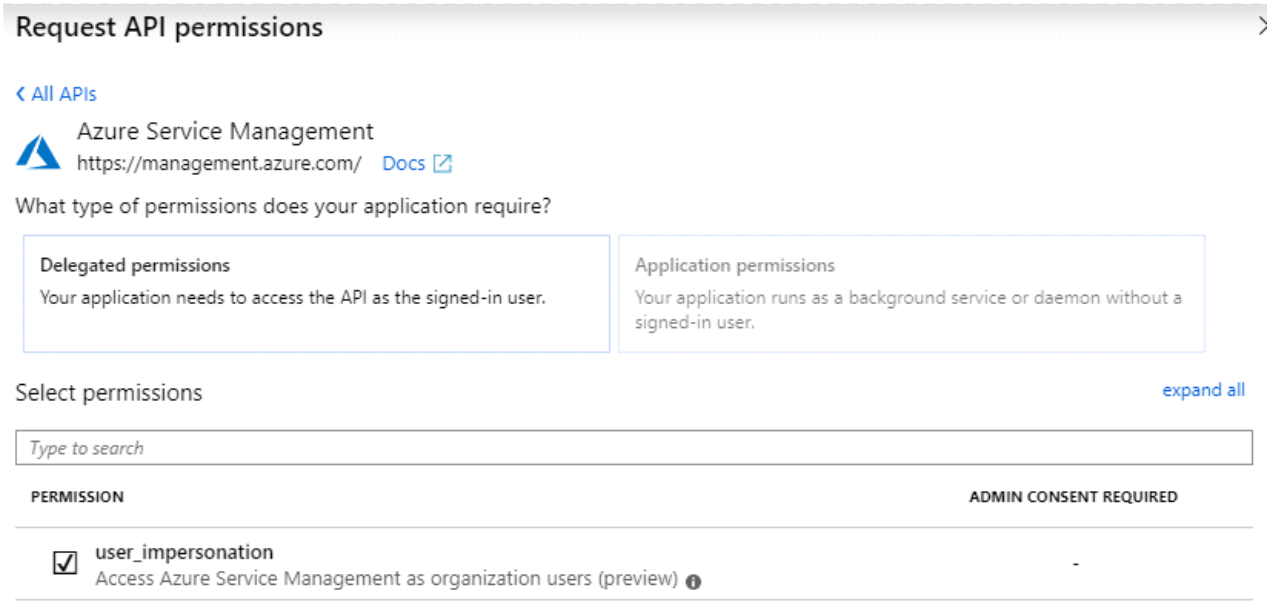
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

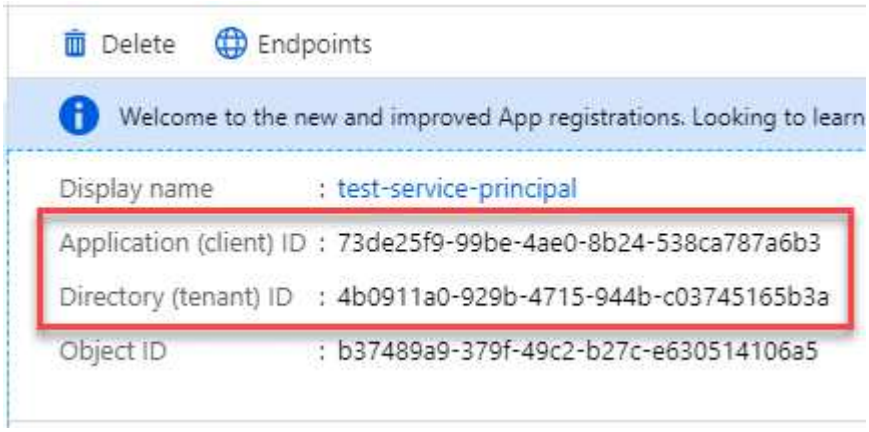


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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. Après avoir installé le connecteur, vous devez associer ces informations d'identification au connecteur de BlueXP.

Étape 4 : installez le connecteur

Téléchargez et installez le logiciel Connector sur un hôte Linux existant sur site.

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.

Description de la tâche

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

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

```
unset http_proxy
unset https_proxy
```

Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

5. Exécutez le script d'installation.

   ```
    ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
   --cacert <path and file name of a CA-signed certificate>
   ```

   Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

   Voici un exemple de commande utilisant les deux paramètres facultatifs :

   ```
    ./BlueXP-Connector-Cloud-v3.9.38 --proxy
   https://user:password@10.0.0.30:8080/ --cacert
   /tmp/cacert/certificate.cer
   ```

   --proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Notez ce qui suit :

     - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
     - Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
     - BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

   --cacert spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy

HTTPS ou si le proxy est un proxy interceptant.

Résultat

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

Étape 5 : configurer le connecteur

Inscrivez-vous ou connectez-vous, puis configurez le connecteur pour qu'il fonctionne avec votre compte BlueXP.

Étapes

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

   https://ipaddress

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

2. S'inscrire ou se connecter.
3. Une fois connecté, configurez BlueXP :
   a. Spécifiez le compte BlueXP à associer au connecteur.
   b. Entrez un nom pour le système.
   c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

      Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. (En outre, le mode restreint n'est pas pris en charge lorsque le connecteur est installé sur site.)

   d. Sélectionnez **commençons**.

Résultat

BlueXP est maintenant configuré avec le connecteur que vous venez d'installer.

Étape 6 : fournissez des autorisations à BlueXP

Une fois que vous avez installé et configuré le connecteur, ajoutez vos identifiants cloud afin que BlueXP dispose des autorisations requises pour effectuer des actions dans AWS ou Azure.

AWS

Avant de commencer

Si vous venez de créer ces identifiants dans AWS, leur 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. 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** : saisissez 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.
   d. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Vous pouvez maintenant accéder au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Azure

Avant de commencer

Si vous venez de créer ces identifiants dans Azure, leur mise à disposition 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. 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

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom. Vous pouvez maintenant accéder au "Console BlueXP" Pour commencer à utiliser le connecteur avec BlueXP.

Abonnement à BlueXP (mode standard)

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel. Si vous avez acheté une licence NetApp (BYOL), vous devez également souscrire à l'offre Marketplace. Votre licence est toujours facturée en premier, mais vous serez facturé au taux horaire si vous dépassez votre capacité sous licence ou si la période de validité de la licence expire.

Un abonnement Marketplace permet de facturer les services BlueXP suivants :

- Sauvegarde et restauration
- Classement
- Cloud Volumes ONTAP
- Tiering

Avant de commencer

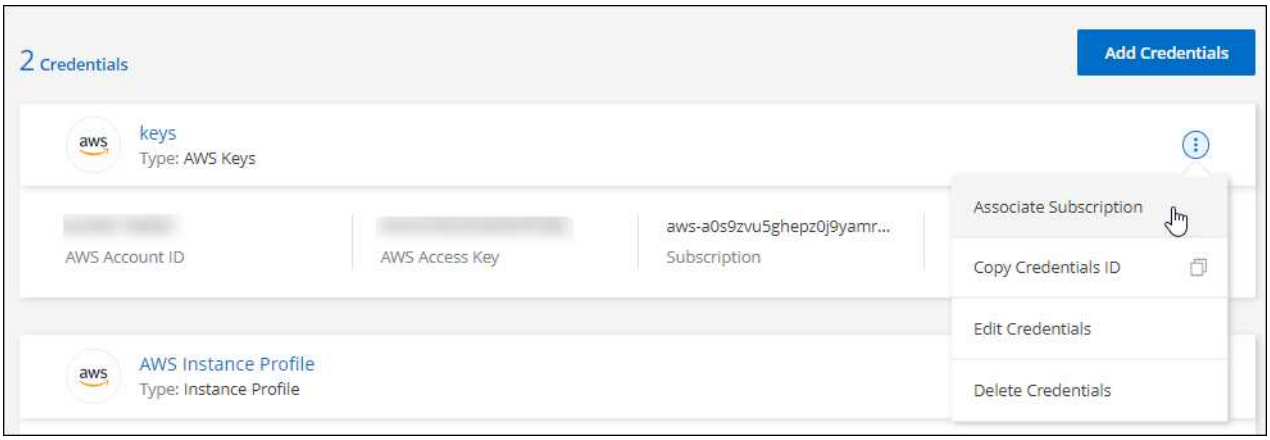
L'abonnement à BlueXP implique d'associer un abonnement Marketplace aux informations d'identification cloud associées à un connecteur. Si vous avez suivi le flux de travail « commencer avec le mode standard », vous devriez déjà avoir un connecteur. Pour en savoir plus, consultez le "Démarrage rapide de BlueXP en mode standard".

AWS

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 :

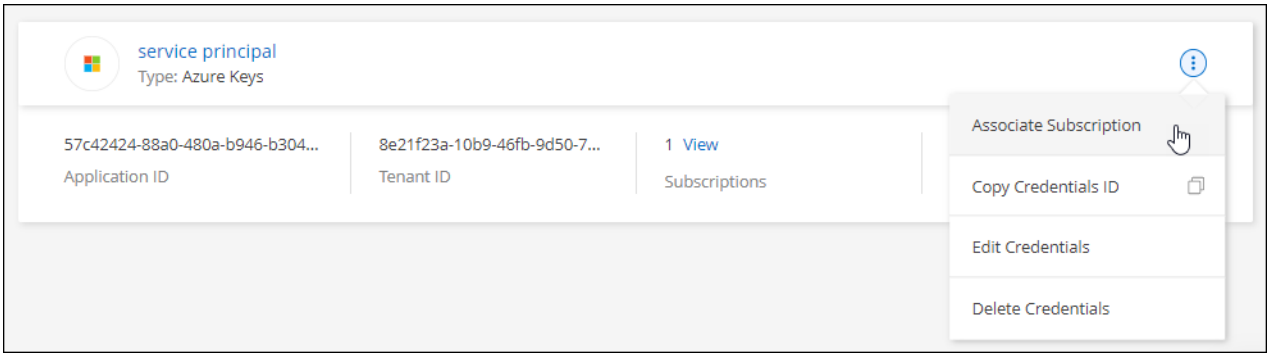
Abonnez-vous à BlueXP sur AWS Marketplace

Azure

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**.

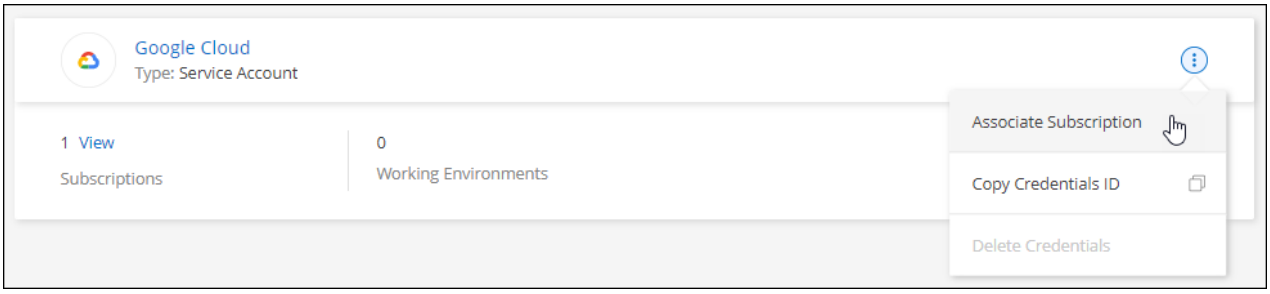
La vidéo suivante explique comment vous abonner à Azure Marketplace :

Abonnez-vous à BlueXP depuis Azure Marketplace

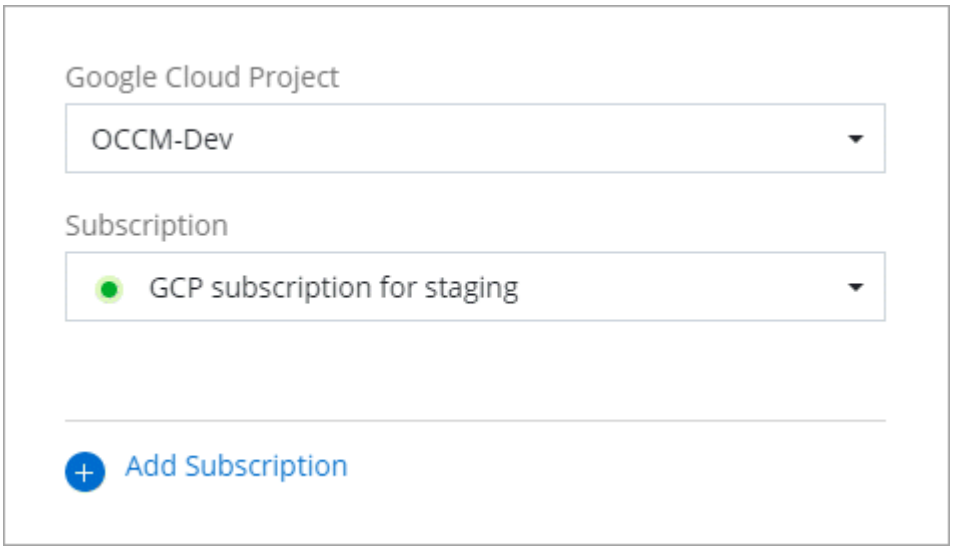
Google Cloud

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**.



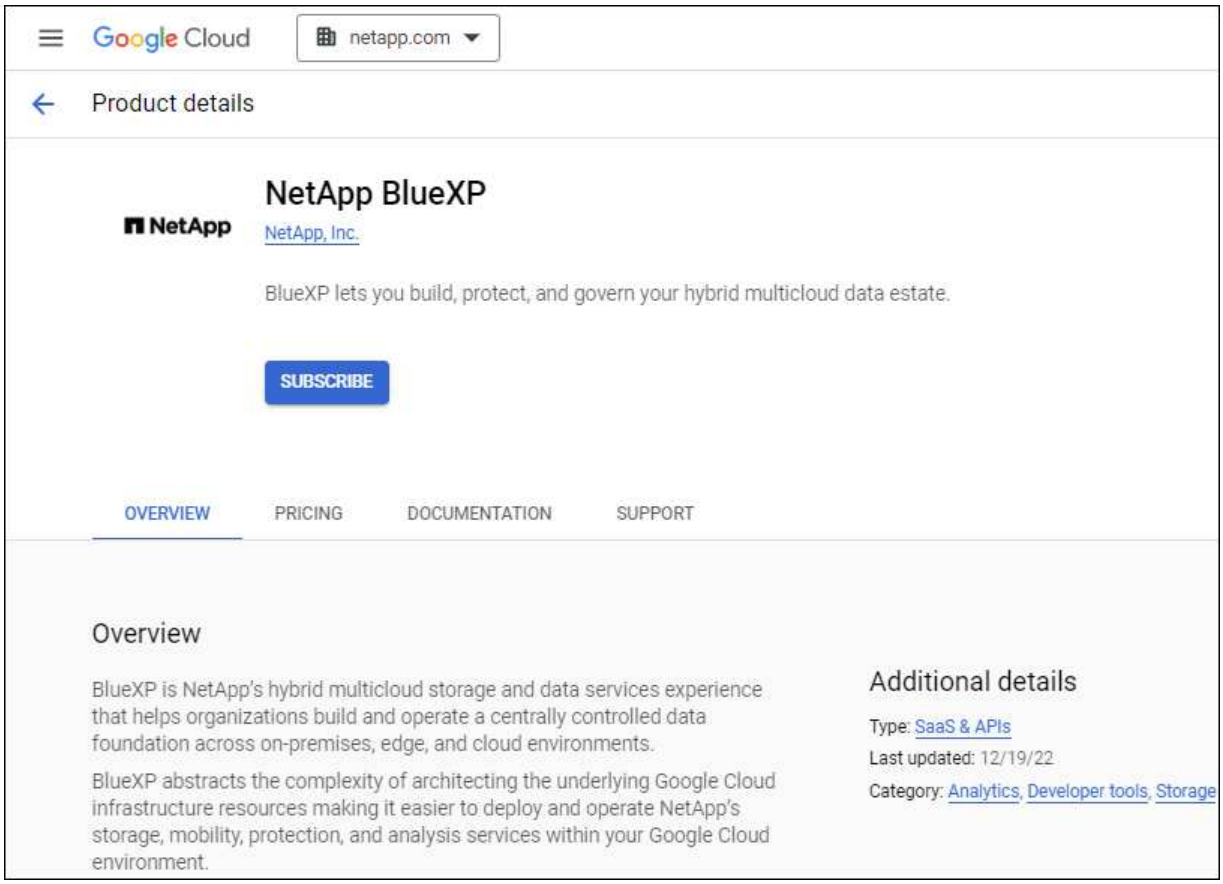
3. Pour associer les informations d'identification à un abonnement existant, sélectionnez un projet Google Cloud et un abonnement dans la liste déroulante, puis sélectionnez **associer**.



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.



b. Sélectionnez **s'abonner**.

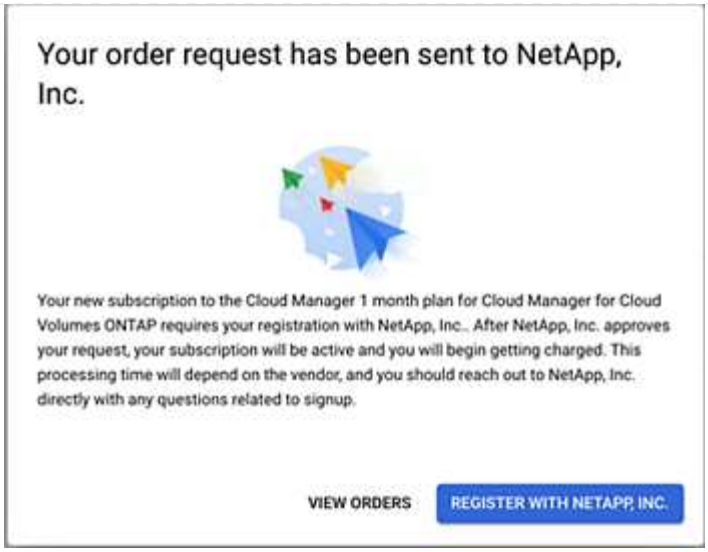
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.

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.

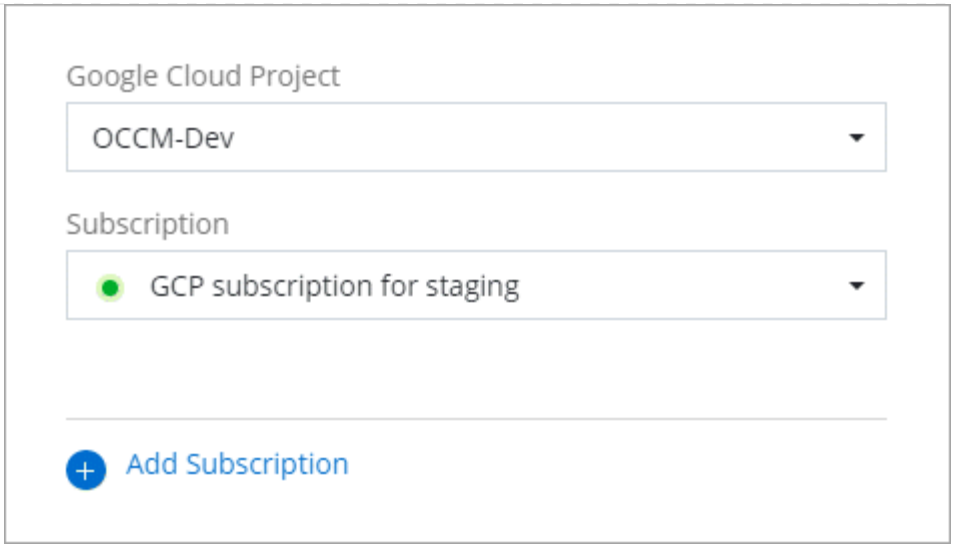
Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- 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.



Liens connexes

- "Gérez les licences BYOL basées sur la capacité pour Cloud Volumes ONTAP"
- "Gérez les licences BYOL pour les services de données BlueXP"
- "Gérez les informations d'identification et les abonnements AWS pour BlueXP"
- "Gérez les informations d'identification et les abonnements Azure pour BlueXP"
- "Gérez les identifiants Google Cloud et les abonnements pour BlueXP"

Ce que vous pouvez faire ensuite (mode standard)

Maintenant que vous vous êtes connecté et que vous avez configuré BlueXP en mode standard, les utilisateurs peuvent créer et découvrir des environnements de travail et utiliser les services de données BlueXP.

> Si vous avez installé un connecteur dans AWS, Microsoft Azure ou Google Cloud, BlueXP découvre automatiquement des informations sur les compartiments Amazon S3, le stockage Azure Blob ou les compartiments Google Cloud Storage à l'emplacement où le connecteur est installé. Un environnement de travail est automatiquement ajouté au canevas BlueXP.

Pour obtenir de l'aide, consultez le "Page d'accueil de la documentation BlueXP" Pour afficher les documents relatifs à tous les services BlueXP.

Lien associé

"Modes de déploiement BlueXP"

Commencez avec le mode restreint

Démarrage du flux de travail (mode restreint)

Commencez à utiliser BlueXP en mode restreint en préparant votre environnement, en déployant le connecteur et en vous abonnant à BlueXP.

Le mode restreint est généralement utilisé par les administrations publiques et locales, ainsi que par les entreprises réglementées, y compris les déploiements dans les régions AWS GovCloud et Azure Government. Avant de commencer, vous devez avoir une compréhension de "Comptes BlueXP", "Connecteurs", et "modes de déploiement".

1 **"Préparation du déploiement"**

1. Préparez un hôte Linux dédié qui répond aux exigences en matière de processeur, de RAM, d'espace disque, de moteur Docker et bien plus encore.
2. Configurez le réseau qui fournit un accès aux réseaux cibles, un accès Internet sortant pour les installations manuelles et un accès Internet sortant pour un accès quotidien.
3. Configurez des autorisations dans votre fournisseur de cloud afin que vous puissiez les associer à l'instance Connector après le déploiement.

2 **"Déployez le connecteur"**

1. Installez le connecteur à partir du Marketplace de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux.
2. Configurez BlueXP en ouvrant un navigateur Web et en entrant l'adresse IP de l'hôte Linux.
3. Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

3 **"Abonnez-vous à BlueXP"**

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel.

Préparez le déploiement en mode restreint

Préparez votre environnement avant de déployer BlueXP en mode restreint. Par exemple, vous devez examiner les exigences relatives aux hôtes, préparer la mise en réseau, configurer les autorisations, etc.

Étape 1 : comprendre le fonctionnement du mode restreint

Avant de commencer, vous devez connaître le fonctionnement de BlueXP en mode restreint.

Par exemple, vous devez comprendre que vous devez utiliser l'interface web disponible localement à partir du connecteur BlueXP que vous devez installer. BlueXP n'est pas accessible depuis la console web fournie via la couche SaaS.

En outre, les services BlueXP ne sont pas tous disponibles.

"Découvrez le fonctionnement du mode restreint".

Étape 2 : passez en revue les options d'installation

En mode restreint, vous pouvez uniquement installer le connecteur dans le nuage. Les options d'installation suivantes sont disponibles :

- Depuis AWS Marketplace
- À partir d'Azure Marketplace
- Installation manuelle du connecteur sur votre propre hôte Linux exécuté dans AWS, Azure ou Google Cloud

Étape 3 : vérifiez la configuration requise pour l'hôte

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

Lorsque vous déployez le connecteur à partir d'AWS ou d'Azure Marketplace, l'image inclut le système d'exploitation et les composants logiciels requis. Il vous suffit de choisir un type d'instance qui répond aux exigences en termes de processeur et de RAM.

Hôte dédié

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

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

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

Taille des machines virtuelles Azure

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

Type de machine Google Cloud

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

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

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

"Voir les instructions d'installation"

Étape 4 : préparer le réseau

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexions aux réseaux cibles

Le connecteur doit disposer d'une connexion réseau à l'emplacement où vous prévoyez de gérer le stockage. Par exemple, le VPC ou le vnet sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, ou le data Center dans lequel résident vos clusters ONTAP sur site.

Préparez la mise en réseau pour l'accès utilisateur à la console BlueXP

En mode restreint, l'interface utilisateur BlueXP est accessible depuis le connecteur. Lorsque vous utilisez l'interface utilisateur BlueXP, le service est en contact avec quelques terminaux pour effectuer les tâches de gestion des données. Ces terminaux sont contactés depuis l'ordinateur d'un utilisateur lorsqu'ils effectuent des actions spécifiques à partir de la console BlueXP.

Terminaux	Objectif
https://signin.b2c.netapp.com	Requis pour mettre à jour les identifiants du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via BlueXP.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Ce terminal n'est pas requis dans les régions Azure Government.

- https://occmclientinfragov.azurecr.us

  Ce terminal n'est requis que dans les régions Azure Government.

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

Accès Internet sortant pour les opérations quotidiennes

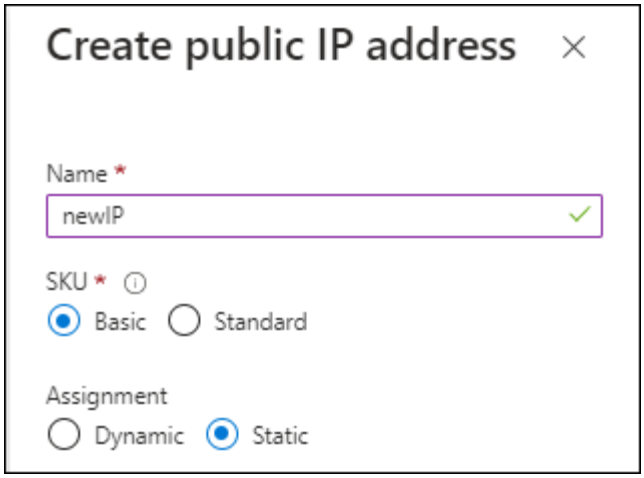
L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante. Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	De gérer les ressources dans les régions Azure Government.

Terminaux	Objectif
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Ce terminal n’est pas requis dans les régions Azure Government. https://occmclientinfragov.azurecr.us Ce terminal n’est requis que dans les régions Azure Government.	Pour mettre à niveau le connecteur et ses composants Docker.

Adresse IP publique dans Azure

Si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle du connecteur dans Azure, l’adresse IP doit utiliser une référence de base pour garantir que BlueXP utilise cette adresse IP publique.



Si vous utilisez une adresse IP de référence standard, BlueXP utilise l'adresse IP *private* du connecteur, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console BlueXP n'a pas accès à cette adresse IP privée, les actions de la console BlueXP échouent.

"Documentation Azure : référence IP publique"

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

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

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur

la classification BlueXP"

Si vous prévoyez de créer le connecteur à partir du marché de votre fournisseur de cloud, vous devrez mettre en œuvre cette exigence de mise en réseau après avoir créé le connecteur.

Étape : 5 Préparez les autorisations cloud

BlueXP requiert l'autorisation de votre fournisseur cloud pour déployer Cloud Volumes ONTAP dans un réseau virtuel et utiliser les services de données BlueXP. Vous devez définir des autorisations dans votre fournisseur de cloud, puis les associer au connecteur.

Pour afficher les étapes requises, sélectionnez l'option d'authentification que vous souhaitez utiliser pour votre fournisseur de cloud.

Rôle IAM AWS

Utilisez un rôle IAM pour fournir au connecteur des autorisations.

Si vous créez le connecteur à partir d'AWS Marketplace, vous serez invité à sélectionner ce rôle IAM au lancement de l'instance EC2.

Si vous installez manuellement le connecteur sur votre propre hôte Linux, vous devrez associer le rôle à l'instance EC2.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.
3. Créer un rôle IAM :
   a. Sélectionnez **rôles > Créer un rôle**.
   b. Sélectionnez **AWS service > EC2**.
   c. Ajoutez des autorisations en joignant la stratégie que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous disposez désormais d'un rôle IAM pour l'instance de connecteur EC2.

Clé d'accès AWS

Configurer les autorisations et une clé d'accès pour un utilisateur IAM. Une fois le connecteur installé et configuré BlueXP, vous devez fournir BlueXP avec la clé d'accès AWS.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :

   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle.

   Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".

3. Associer les règles à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"

4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à BlueXP après l'installation du connecteur.

Résultat

Le compte dispose désormais des autorisations requises.

Rôle d'Azure

Créez un rôle Azure personnalisé avec les autorisations requises. Vous allez attribuer ce rôle à la machine virtuelle Connector.

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"

Étapes

1. Si vous prévoyez d'installer manuellement le logiciel sur votre propre hôte, activez une identité gérée attribuée par le système sur la machine virtuelle afin de fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'identifiant de chaque abonnement Azure que vous souhaitez utiliser avec BlueXP.

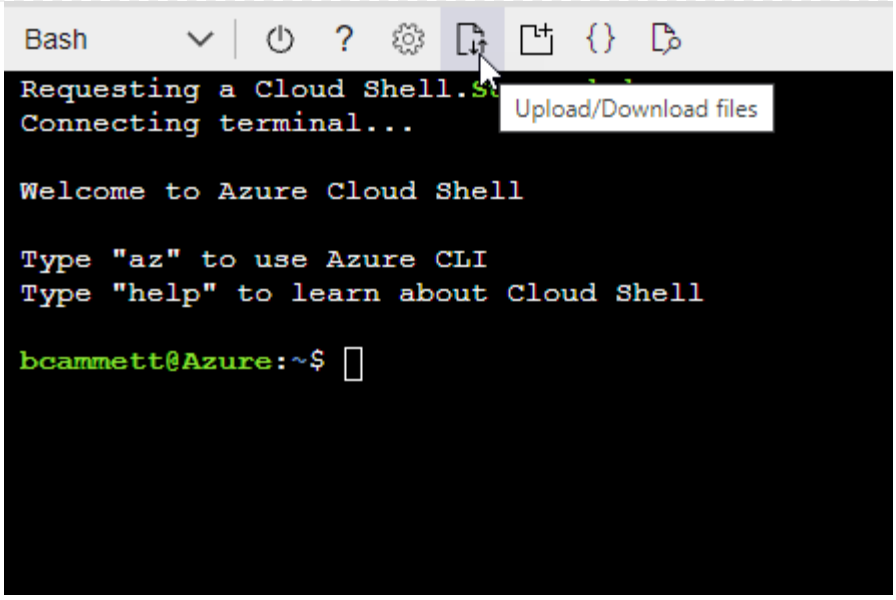
   Exemple

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

4. 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.

   a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
   b. Téléchargez le fichier JSON.



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

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

Résultat

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

Principal de service Azure

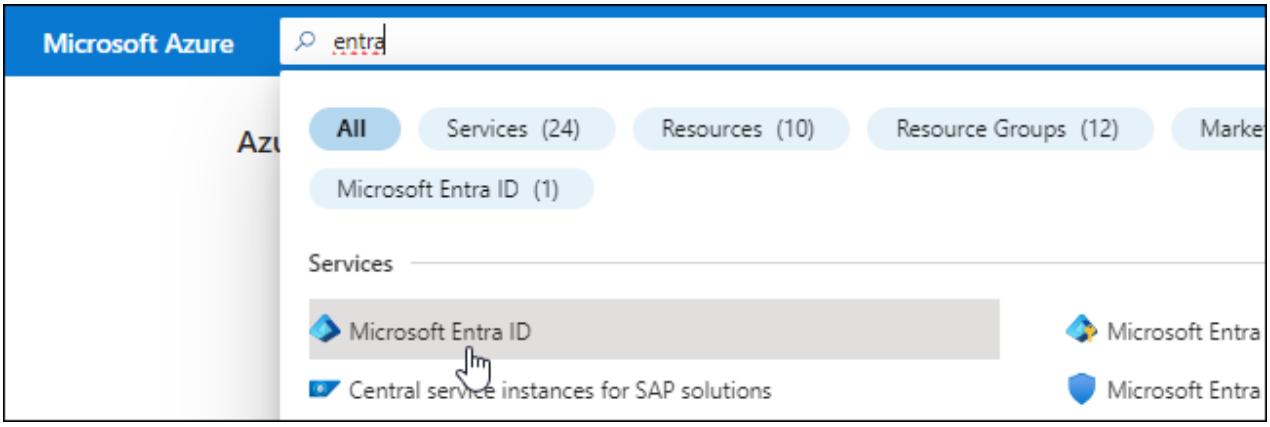
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin. Après avoir installé le connecteur et configuré BlueXP, vous devez fournir ces informations d'identification à BlueXP.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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.

Attribuez l'application à un rôle

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.

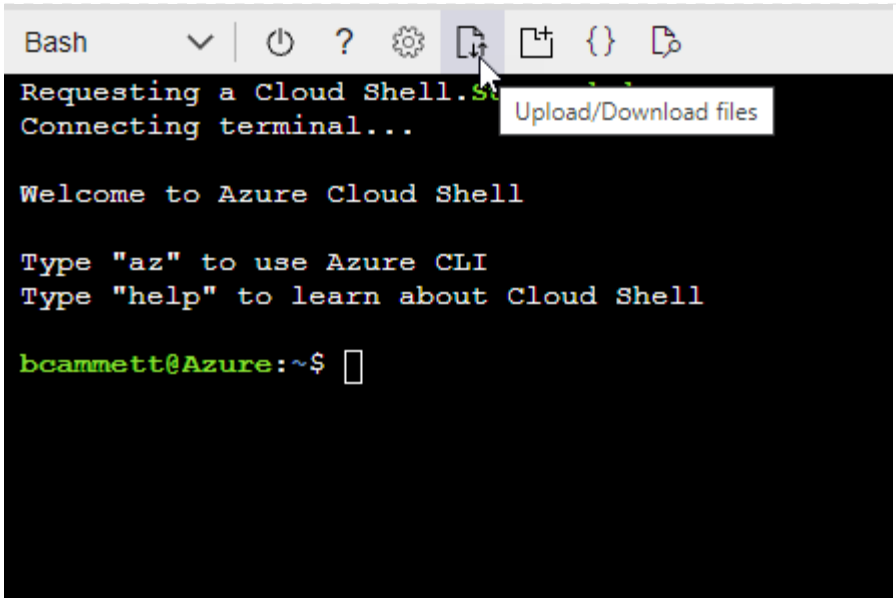
      Exemple

      ```
      "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 :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

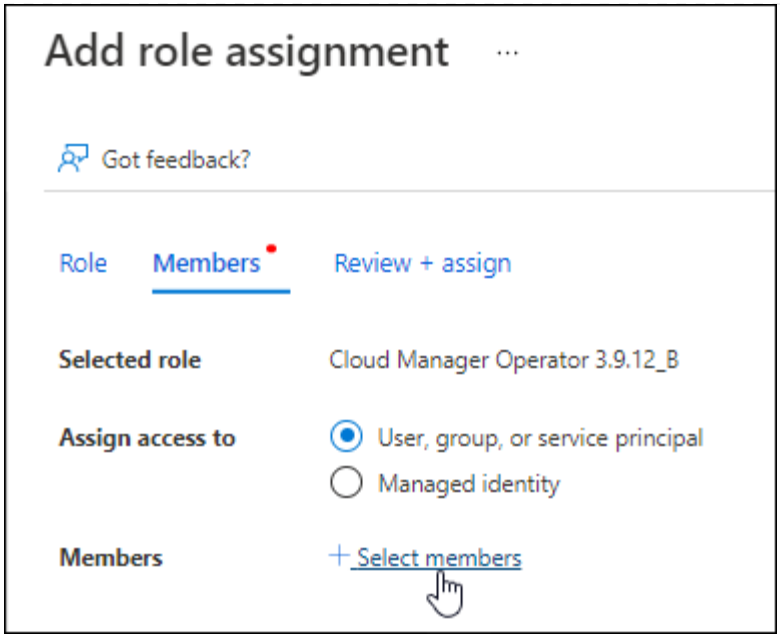
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

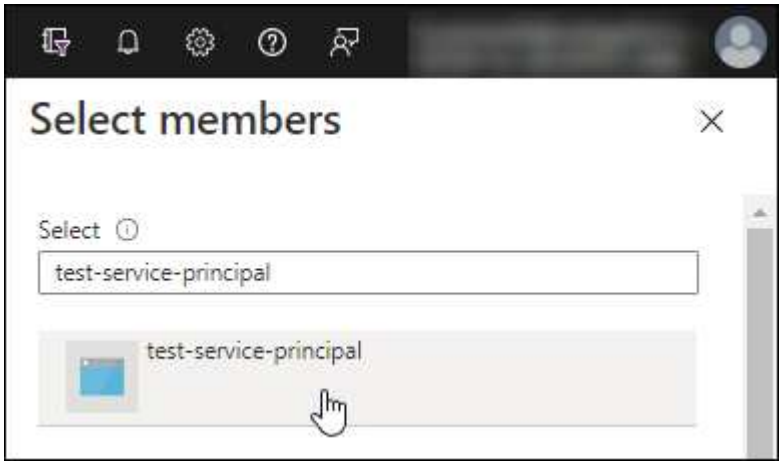
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

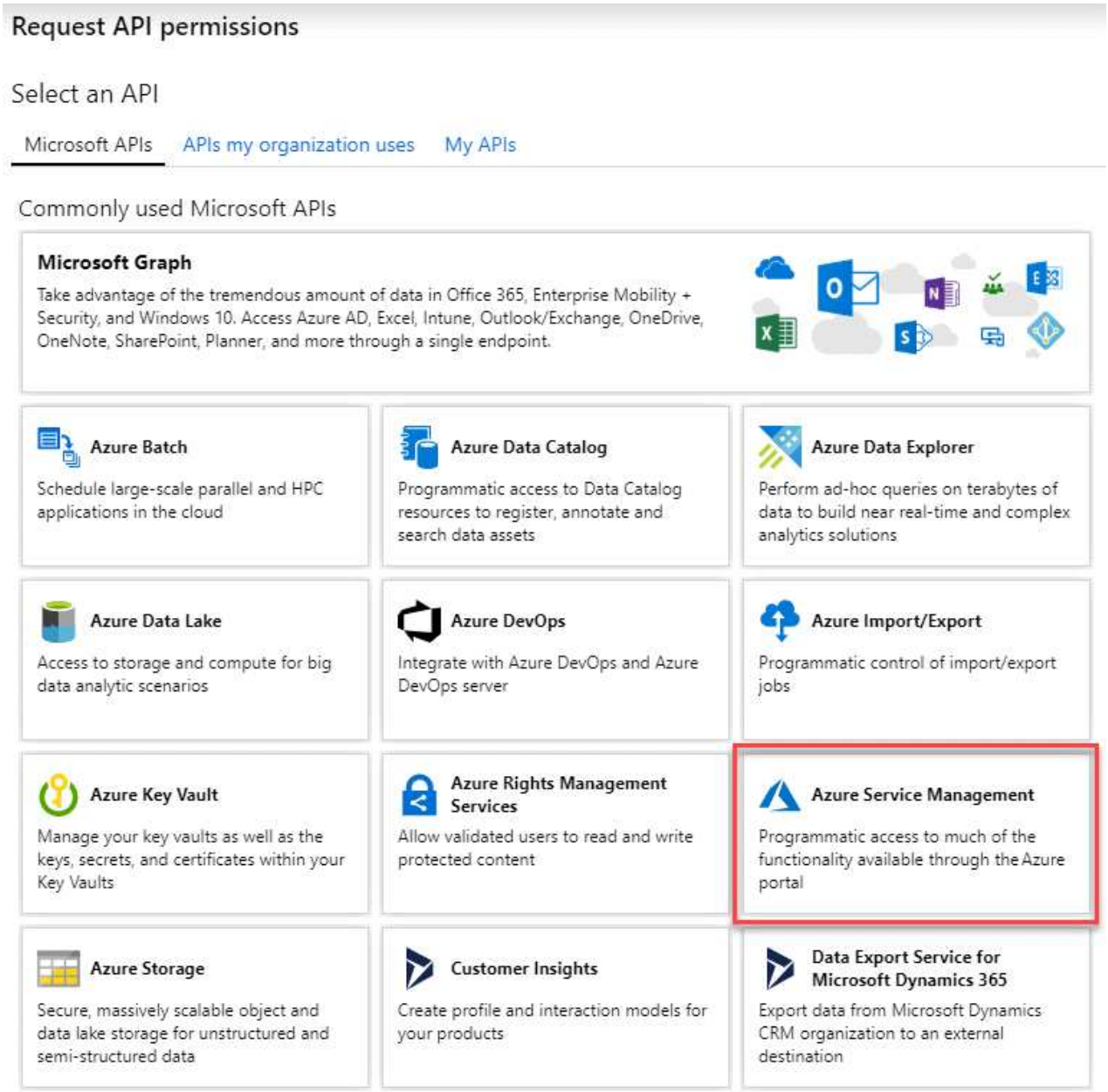
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

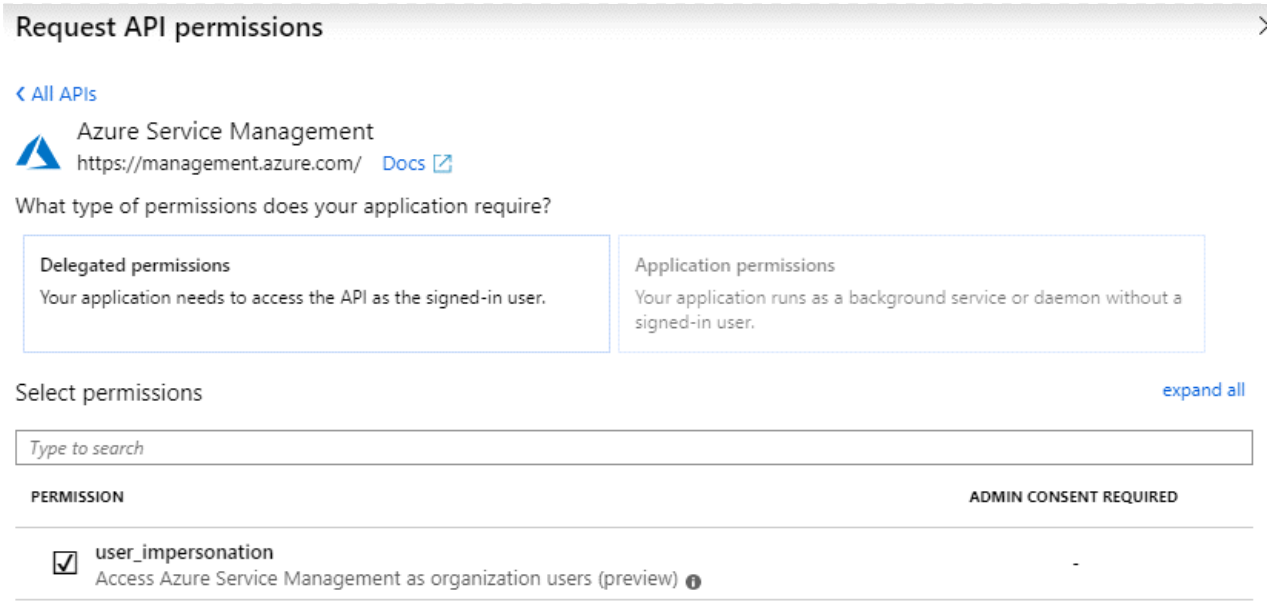
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

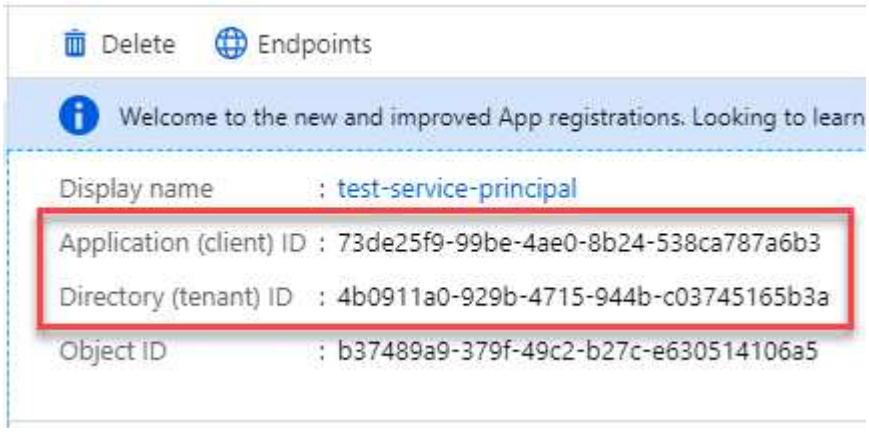


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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.

Compte de service Google Cloud

Créez un rôle et appliquez-le à un compte de service que vous utiliserez pour l'instance de la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut les autorisations définies dans le "Règle de connecteur pour Google Cloud".

   b. Dans Google Cloud, activez le shell cloud.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises pour le connecteur.

   d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

   L'exemple suivant crée un rôle nommé « connecteur » au niveau du projet :

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documents Google Cloud : création et gestion de rôles personnalisés"

2. Créez un compte de service dans Google Cloud :

   a. Dans le service IAM & Admin, sélectionnez **comptes de service > Créer un compte de service**.

   b. Entrez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

   "Documents Google Cloud : création d'un compte de service"

Résultat

Vous disposez désormais d'un compte de service que vous pouvez attribuer à l'instance VM Connector.

Étape 6 : activez les API Google Cloud

Plusieurs API sont requises pour déployer Cloud Volumes ONTAP dans Google Cloud.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API Cloud Deployment Manager V2
    - API de journalisation cloud
    - API Cloud Resource Manager
    - API du moteur de calcul
    - API de gestion des identités et des accès
    - API KMS (Cloud Key Management Service

      (Requis uniquement si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec des clés de chiffrement gérées par le client (CMEK))

Déployez le connecteur en mode restreint

Déployez le connecteur en mode restreint pour utiliser BlueXP avec une connectivité sortante limitée vers la couche SaaS BlueXP. Pour commencer, installez le connecteur, configurez BlueXP en accédant à l'interface utilisateur exécutée sur le connecteur, puis fournissez les autorisations cloud que vous avez précédemment configurées.

Étape 1 : installez le connecteur

Installez le connecteur à partir du Marketplace de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux.

AWS commercial Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations AWS"

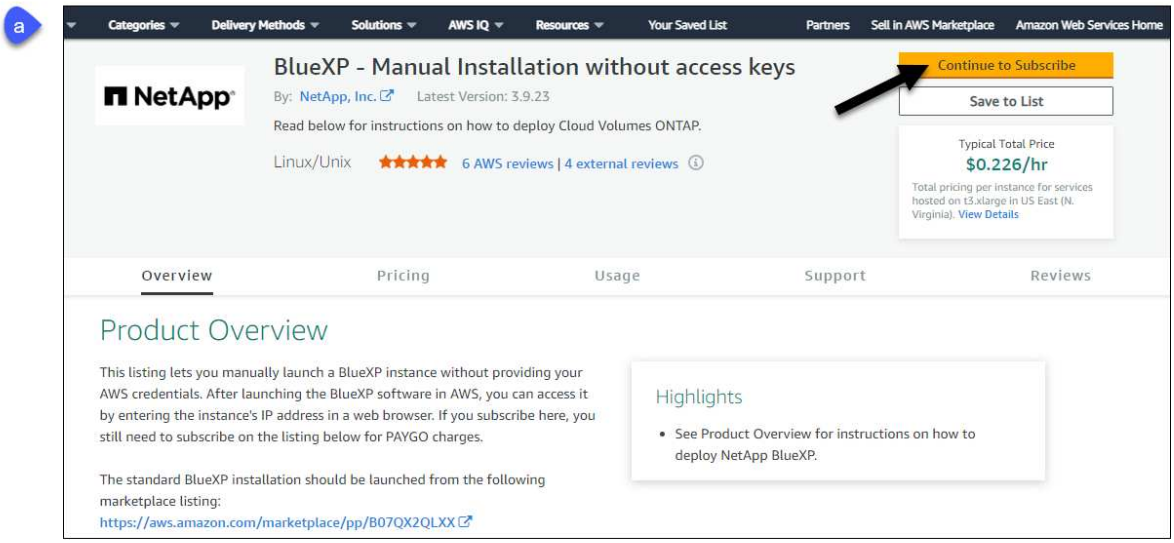
- Autorisations de vous abonner à AWS Marketplace et de vous désabonner pour votre utilisateur IAM.
- Compréhension des exigences en termes de CPU et de RAM pour l'instance.

  "Passez en revue les exigences relatives aux instances".

- Une paire de clés pour l'instance EC2.

Étapes

1. Accédez au "BlueXP, page sur AWS Marketplace"
2. Sur la page Marketplace, sélectionnez **Continuer pour s'abonner**, puis sélectionnez **Continuer à la configuration**.



3. Modifiez l'une des options par défaut et sélectionnez **Continuer pour lancer**.
4. Sous **Choisissez action**, sélectionnez **lancer via EC2**, puis **lancer**.

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

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

   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Image de l'application et de l'OS** : passez cette section. Le connecteur ami est déjà sélectionné.
   - **Type d'instance** : en fonction de la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.xlarge est recommandé).
   - **Paire de clés (login)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
   - **Paramètres réseau** : modifiez les paramètres réseau selon vos besoins :
     - Choisissez le VPC et le sous-réseau souhaités.
     - Spécifiez si l'instance doit avoir une adresse IP publique.
     - Spécifiez les paramètres de pare-feu qui activent les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.

       Quelques règles supplémentaires sont requises pour des configurations spécifiques.

   "Afficher les règles des groupes de sécurité pour AWS".

   - **Configurer le stockage** : conservez la taille et le type de disque par défaut pour le volume racine.

     Si vous souhaitez activer le chiffrement Amazon EBS sur le volume racine, sélectionnez **Avancé**, développez **Volume 1**, sélectionnez **crypté**, puis choisissez une clé KMS.

   - **Détails avancés** : sous **profil d'instance IAM**, choisissez le rôle IAM qui inclut les autorisations requises pour le connecteur.
   - **Résumé** : passez en revue le résumé et sélectionnez **lancer l'instance**.

Résultat

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

Et la suite ?

Configurez BlueXP.

AWS Gov Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.

  "En savoir plus sur les exigences de mise en réseau"

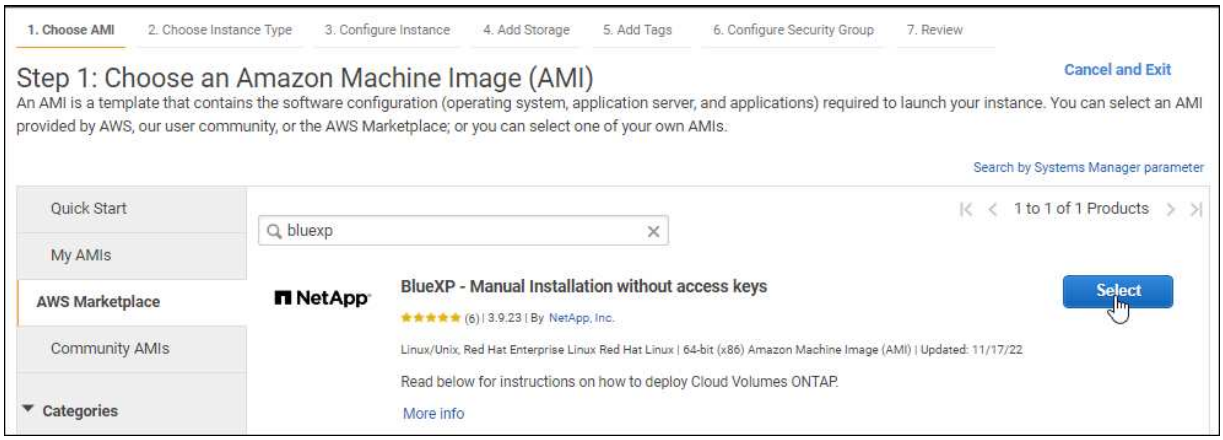
- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations AWS"

- Autorisations de vous abonner à AWS Marketplace et de vous désabonner pour votre utilisateur IAM.
- Une paire de clés pour l'instance EC2.

Étapes

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

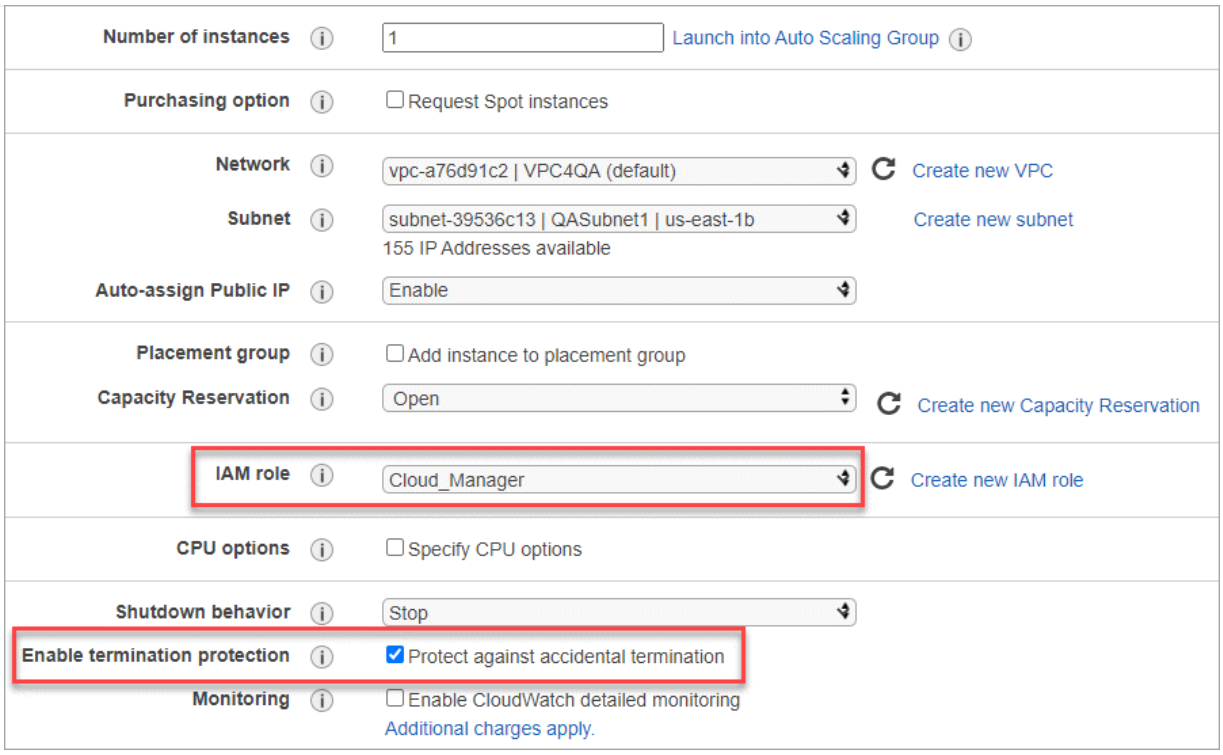


   d. Sélectionnez **Continuer**.

2. Suivez les invites pour configurer et déployer l'instance :
   - **Choisissez un type d'instance** : selon la disponibilité de la région, choisissez un des types d'instance pris en charge (t3.XLarge est recommandé).

     "Vérifiez les conditions requises pour l'instance".

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



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

Résultat

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

Et la suite ?

Configurez BlueXP.

Azure Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- Vnet et sous-réseau répondant aux exigences de mise en réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Rôle personnalisé Azure qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations Azure"

Étapes

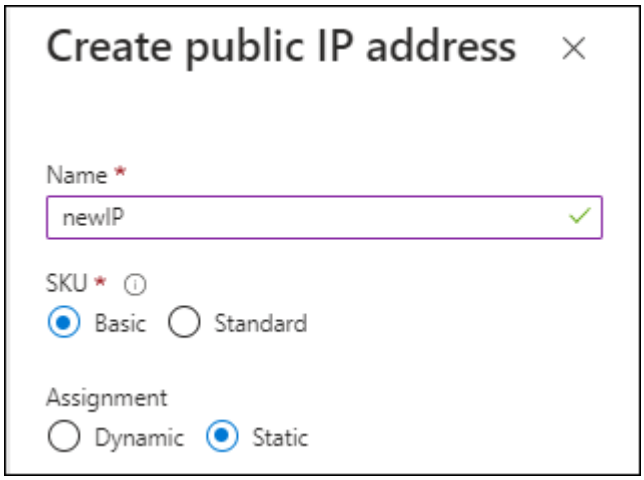
1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.
   - "Page Azure Marketplace pour les régions commerciales"

- "Page Azure Marketplace pour les régions Azure Government"

2. Sélectionnez **obtenir maintenant**, puis **Continuer**.
3. Dans le portail Azure, sélectionnez **Create** et suivez les étapes pour configurer la machine virtuelle.

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

   - **Taille de la VM** : choisissez une taille de VM qui répond aux exigences de CPU et de RAM. Nous recommandons DS3 v2.
   - **Disques** : le connecteur peut fonctionner de manière optimale avec des disques durs ou SSD.
   - **Public IP** : si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle du connecteur, l'adresse IP doit utiliser une référence SKU de base pour garantir que BlueXP utilise cette adresse IP publique.



     Si vous utilisez une adresse IP de référence standard, BlueXP utilise l'adresse IP *private* du connecteur, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console BlueXP n'a pas accès à cette adresse IP privée, les actions de la console BlueXP échouent.

   "Documentation Azure : référence IP publique"

   - **Groupe de sécurité réseau** : le connecteur nécessite des connexions entrantes utilisant SSH, HTTP et HTTPS.

     "Afficher les règles des groupes de sécurité pour Azure".

   - **Identité** : sous **gestion**, sélectionnez **Activer l'identité gérée attribuée par le système**.

     Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Microsoft Entra ID sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Sur la page **consulter + créer**, vérifiez vos sélections et sélectionnez **Créer** pour démarrer le déploiement.

Résultat

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

Et la suite ?

Configurez BlueXP.

Installation manuelle

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.

Description de la tâche

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

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

   ```
   unset http_proxy
   unset https_proxy
   ```

   Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

5. Exécutez le script d'installation.

```
./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Notez ce qui suit :

  - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
  - Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
  - BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

--cacert spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy HTTPS ou si le proxy est un proxy interceptant.

Résultat

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

Et la suite ?

Configurez BlueXP.

Étape 2 : configuration de BlueXP

Lorsque vous accédez pour la première fois à la console BlueXP, vous êtes invité à choisir un compte auquel associer le connecteur et vous devez activer le mode restreint.

Si vous avez déjà un compte et que vous souhaitez en créer un autre, vous devez utiliser l'API de location. "Découvrez comment créer un compte BlueXP supplémentaire".

Étapes

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

   https://ipaddress

2. Inscrivez-vous ou connectez-vous à BlueXP.
3. Une fois connecté, configurez BlueXP :

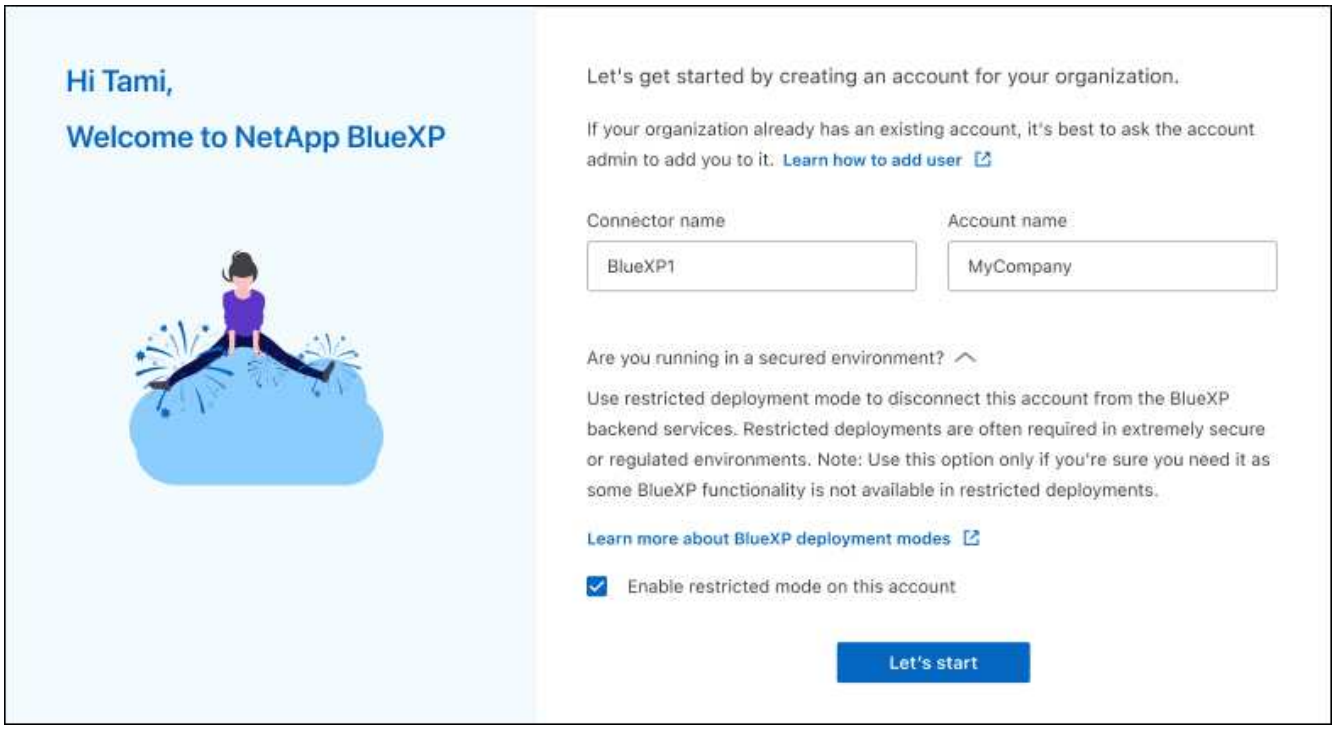
   a. Entrez un nom pour le connecteur.
   b. Entrez le nom d'un nouveau compte BlueXP ou sélectionnez un compte existant.

      Vous pouvez sélectionner un compte existant si votre connexion est déjà associée à un compte BlueXP.

   c. Sélectionnez **exécutez-vous dans un environnement sécurisé ?**
   d. Sélectionnez **Activer le mode restreint sur ce compte**.

      Notez que vous ne pouvez pas modifier ce paramètre après la création du compte par BlueXP. Vous ne pouvez pas activer le mode restreint ultérieurement et vous ne pouvez pas le désactiver ultérieurement.

      Si vous avez déployé le connecteur dans une région gouvernementale, la case à cocher est déjà activée et ne peut pas être modifiée. En effet, le mode restreint est le seul mode pris en charge dans les régions gouvernementales.



   a. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP. Tous les utilisateurs doivent accéder à BlueXP via l'adresse IP de l'instance de connecteur.

Et la suite ?

Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Étape 3 : fournissez des autorisations à BlueXP

Si vous avez déployé le connecteur à partir d'Azure Marketplace ou si vous avez installé manuellement le logiciel Connector, vous devez fournir les autorisations que vous avez précédemment configurées pour vous permettre d'utiliser les services BlueXP.

Ces étapes ne s'appliquent pas si vous avez déployé Connector à partir d'AWS Marketplace, car vous avez choisi le rôle IAM requis pendant le déploiement.

"Découvrez comment préparer les autorisations cloud".

Rôle IAM AWS

Reliez le rôle IAM que vous avez créé précédemment à l'instance EC2 sur laquelle vous avez installé le connecteur.

Ces étapes s'appliquent uniquement si vous avez installé manuellement le connecteur dans AWS. Pour les déploiements AWS Marketplace, vous avez déjà associé l'instance Connector à un rôle IAM qui inclut les autorisations requises.

Étapes

1. Accédez à la console Amazon EC2.
2. Sélectionnez **instances**.
3. Sélectionnez l'instance de connecteur.
4. Sélectionnez **actions > sécurité > Modifier le rôle IAM**.
5. Sélectionnez le rôle IAM et sélectionnez **mettre à jour le rôle IAM**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Clé d'accès AWS

Fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

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 **Amazon Web Services > connecteur**.
   b. **Définir les informations d'identification** : saisissez 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.
   d. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Rôle d'Azure

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Sur le portail Azure, ouvrez le service **Subscriptions** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Subscriptions** car cela spécifie la portée de l'affectation de rôle au niveau de l'abonnement. Le *scope* définit l'ensemble des ressources auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau des machines virtuelles), votre capacité à effectuer des actions depuis BlueXP sera affectée.

   "Documentation Microsoft Azure : étendue du contrôle d'accès basé sur des rôles Azure"

2. Sélectionnez **contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une affectation de rôle**.
3. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

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

4. Dans l'onglet **membres**, procédez comme suit :
   a. Attribuez l'accès à une identité **gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée, sous **identité gérée**, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle du connecteur.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **consulter + affecter**.
   f. Si vous souhaitez gérer les ressources d'autres abonnements Azure, passez à cet abonnement, puis répétez ces étapes.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Principal de service Azure

Fournissez à BlueXP les informations d'identification du principal de service Azure que vous avez précédemment configuré.

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

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Compte de service Google Cloud

Associez le compte de service à la VM Connector.

Étapes

1. Accédez au portail Google Cloud et attribuez le compte de service à l'instance de la VM Connector.

   "Documentation Google Cloud : modification du compte de service et des étendues d'accès pour une instance"

2. Si vous souhaitez gérer des ressources dans d'autres projets, accordez l'accès en ajoutant le compte de service doté du rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions en votre nom dans Google Cloud.

Abonnement à BlueXP (mode restreint)

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel. Si vous avez acheté une licence NetApp (BYOL), vous devez également souscrire à l'offre Marketplace. Votre licence est toujours facturée en premier, mais vous serez facturé au taux horaire si vous dépassez votre capacité sous licence ou si la période de validité de la licence expire.

Un abonnement Marketplace permet de facturer les services BlueXP suivants en mode restreint :

- Sauvegarde et restauration
- Classement
- Cloud Volumes ONTAP

Avant de commencer

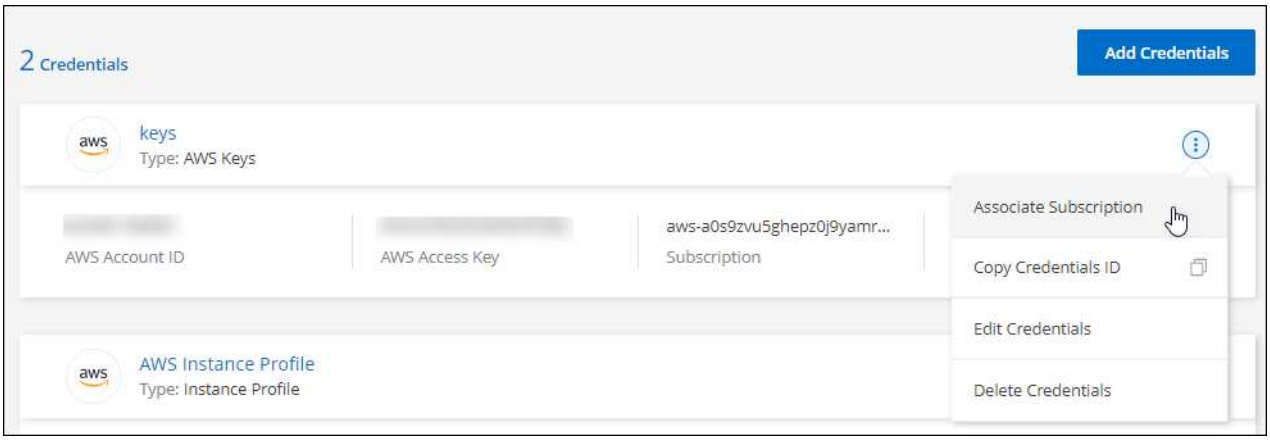
L'abonnement à BlueXP implique d'associer un abonnement Marketplace aux informations d'identification cloud associées à un connecteur. Si vous avez suivi le flux de travail « commencer avec le mode restreint », vous devriez déjà avoir un connecteur. Pour en savoir plus, consultez le "Démarrage rapide de BlueXP en mode restreint".

AWS

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 :

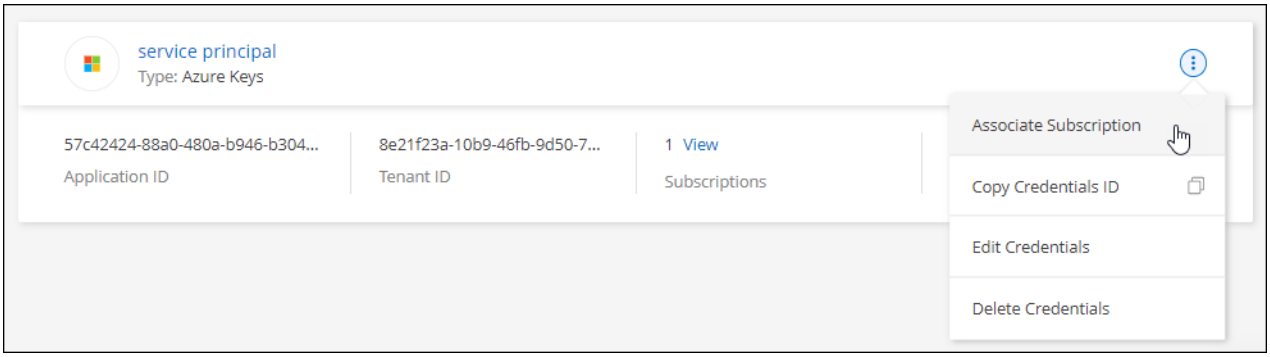
Abonnez-vous à BlueXP sur AWS Marketplace

Azure

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**.

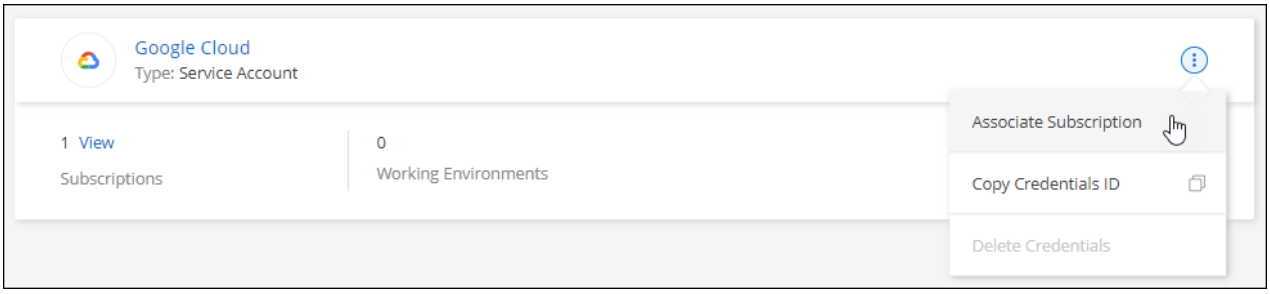
La vidéo suivante explique comment vous abonner à Azure Marketplace :

Abonnez-vous à BlueXP depuis Azure Marketplace

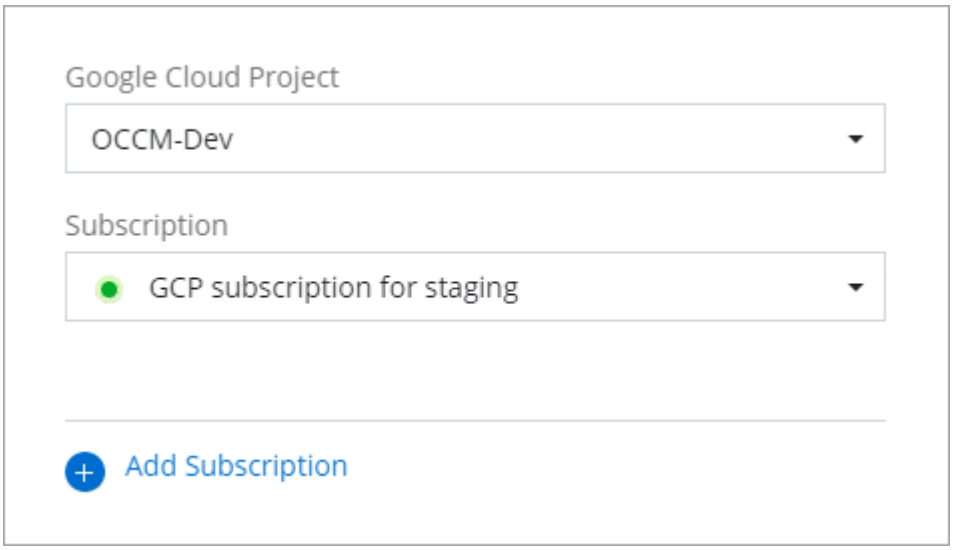
Google Cloud

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**.



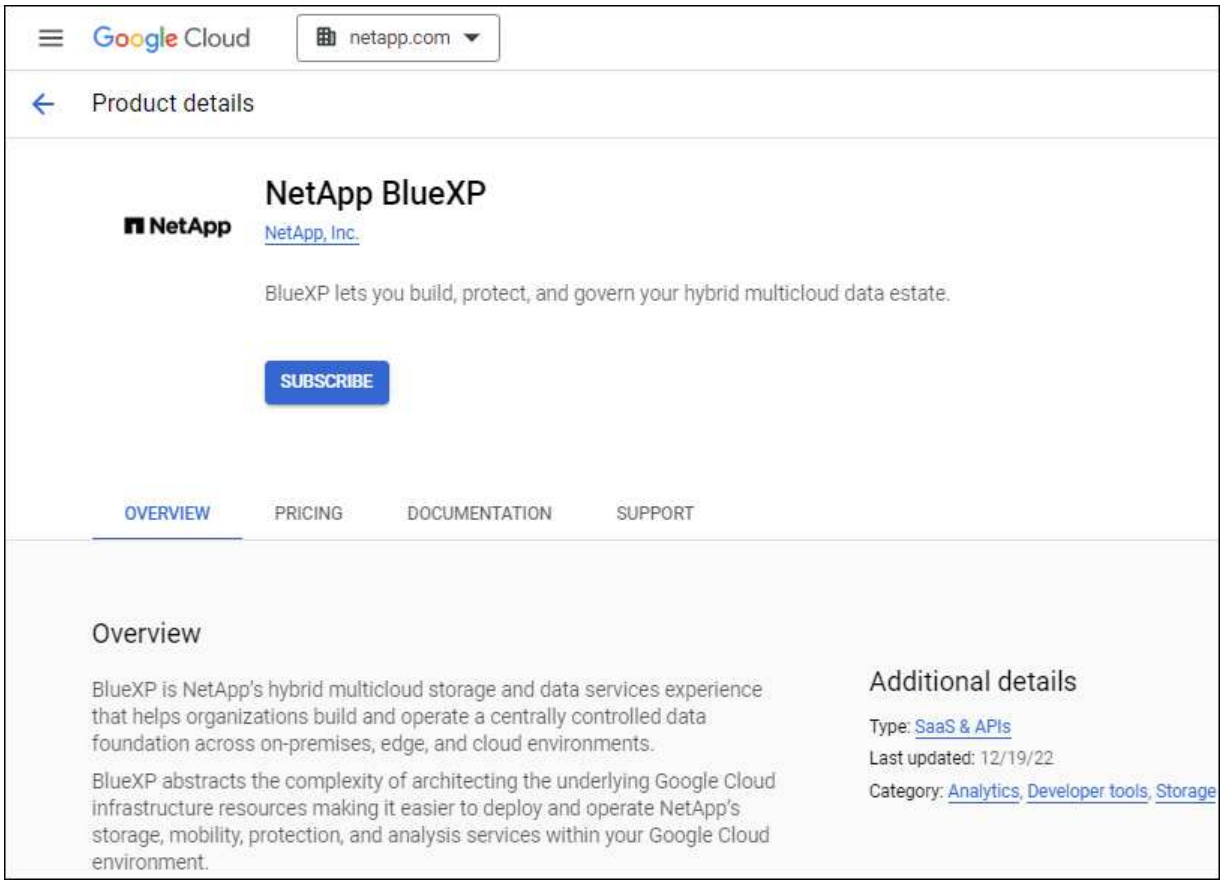
3. Pour associer les informations d'identification à un abonnement existant, sélectionnez un projet Google Cloud et un abonnement dans la liste déroulante, puis sélectionnez **associer**.



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.



b. Sélectionnez **s'abonner**.

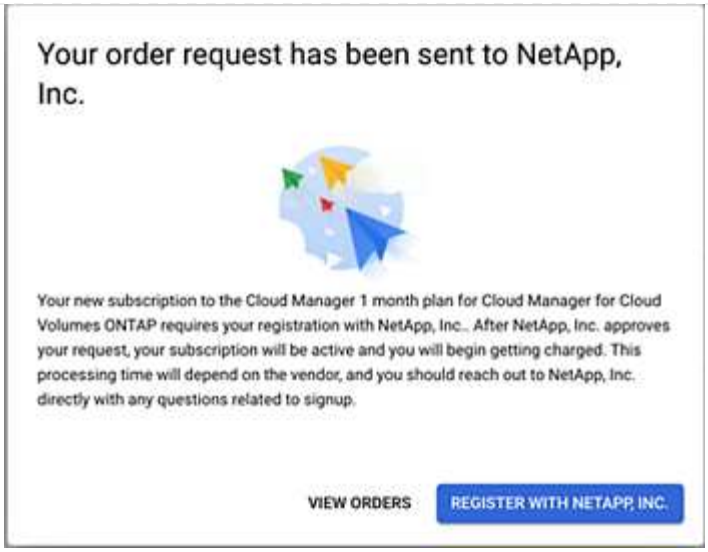
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.

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.

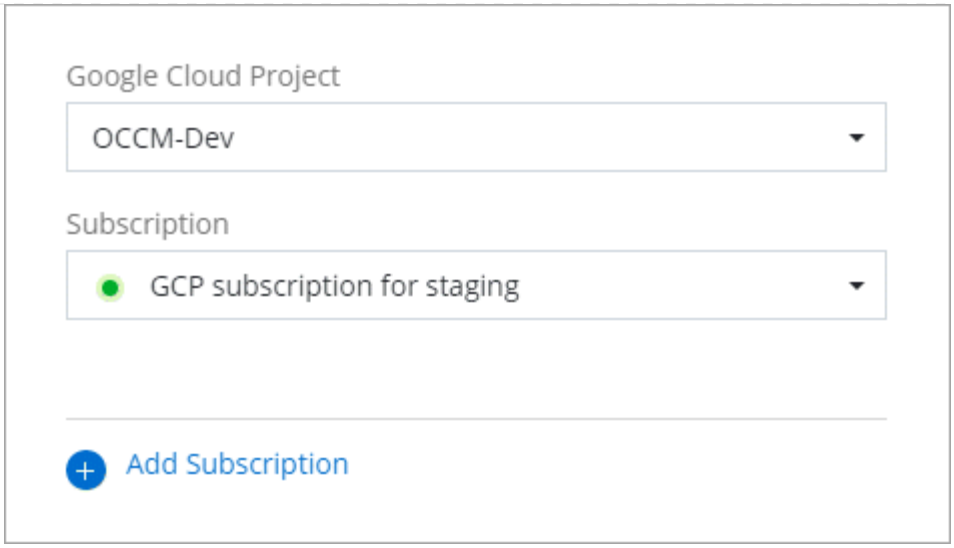
Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- 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.



Liens connexes

- "Gérez les licences BYOL basées sur la capacité pour Cloud Volumes ONTAP"
- "Gérez les licences BYOL pour les services de données BlueXP"
- "Gérez les informations d'identification et les abonnements AWS pour BlueXP"
- "Gérez les informations d'identification et les abonnements Azure pour BlueXP"
- "Gérez les identifiants Google Cloud et les abonnements pour BlueXP"

Ce que vous pouvez faire ensuite (mode restreint)

Une fois que vous êtes opérationnel avec BlueXP en mode restreint, vous pouvez commencer à utiliser les services BlueXP pris en charge avec le mode restreint.

Pour obtenir de l'aide, reportez-vous à la documentation de ces services :

- "Documents Amazon FSX pour ONTAP"
- "Documentation Azure NetApp Files"
- "Documents de sauvegarde et de restauration"
- "Documents de classification"
- "Documentation Cloud Volumes ONTAP"
- "Documentation sur le cluster ONTAP sur site"
- "Documents de réplication"

Lien associé

"Modes de déploiement BlueXP"

Commencez en mode privé

Mise en route du flux de travail (mode privé)

Commencez à utiliser BlueXP en mode privé en préparant votre environnement et en déployant Connector.

Le mode privé est généralement utilisé avec les environnements sur site qui ne disposent pas de connexion Internet et avec les régions cloud sécurisées, notamment "Cloud secret AWS", "Le cloud le plus secret d'AWS", et "Azure IL6"

Avant de commencer, vous devez avoir une compréhension de "Comptes BlueXP", "Connecteurs", et "modes de déploiement".

1 **"Préparation du déploiement"**

1. Préparez un hôte Linux dédié qui répond aux exigences en matière de processeur, de RAM, d'espace disque, de moteur Docker et bien plus encore.
2. Configurez le réseau qui permet d'accéder aux réseaux cibles.
3. Pour les déploiements cloud, configurez des autorisations dans votre fournisseur de cloud afin que vous puissiez les associer au connecteur après avoir installé le logiciel.

2 **"Déployez le connecteur"**

1. Installez le logiciel Connector sur votre propre hôte Linux.
2. Configurez BlueXP en ouvrant un navigateur Web et en entrant l'adresse IP de l'hôte Linux.
3. Pour les déploiements cloud, fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Préparez le déploiement en mode privé

Préparez votre environnement avant de déployer BlueXP en mode privé. Par exemple, vous devez examiner les exigences relatives aux hôtes, préparer la mise en réseau, configurer les autorisations, etc.

> Si vous souhaitez utiliser BlueXP dans le "Cloud secret AWS" ou le "Le cloud le plus secret d'AWS", vous devez alors suivre des instructions séparées pour démarrer dans ces environnements. "Découvrez comment vous lancer avec Cloud Volumes ONTAP dans le cloud secret AWS ou le cloud secret"

Étape 1 : comprendre le fonctionnement du mode privé

Avant de commencer, vous devez connaître le fonctionnement de BlueXP en mode privé.

Par exemple, vous devez comprendre que vous devez utiliser l'interface web disponible localement à partir du connecteur BlueXP que vous devez installer. BlueXP n'est pas accessible depuis la console web fournie via la couche SaaS.

En outre, les services BlueXP ne sont pas tous disponibles.

"En savoir plus sur le fonctionnement du mode privé".

Étape 2 : passez en revue les options d'installation

En mode privé, vous pouvez installer le connecteur sur site ou dans le cloud en installant manuellement le connecteur sur votre propre hôte Linux.

L'emplacement d'installation du connecteur détermine les services et fonctionnalités BlueXP disponibles lorsque vous utilisez le mode privé. Par exemple, le connecteur doit être installé dans le cloud si vous souhaitez déployer et gérer Cloud Volumes ONTAP. "En savoir plus sur le mode privé".

Étape 3 : vérifiez la configuration requise pour l'hôte

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

Hôte dédié

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

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

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

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

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

Taille des machines virtuelles Azure

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

Type de machine Google Cloud

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

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

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

"Voir les instructions d'installation"

Étape 4 : préparer la mise en réseau pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexions aux réseaux cibles

Le connecteur doit disposer d'une connexion réseau à l'emplacement où vous prévoyez de gérer le stockage. Par exemple, le VPC ou le vnet sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, ou le data Center dans lequel résident vos clusters ONTAP sur site.

Terminaux des opérations quotidiennes

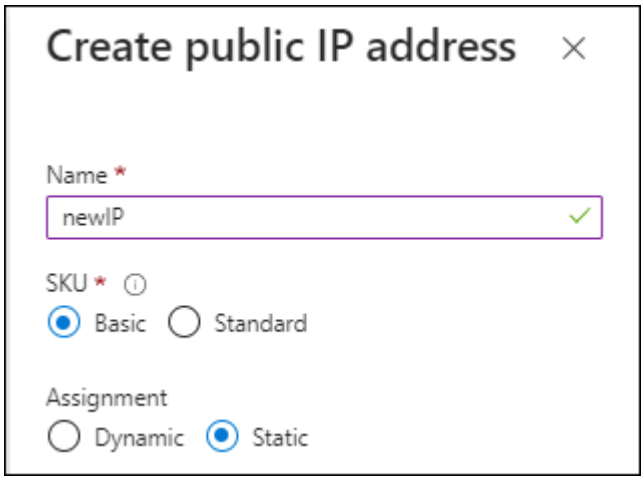
Le connecteur contacte les terminaux suivants pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.

Terminaux	Objectif
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Pour gérer les ressources dans la région d'Azure IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.

Adresse IP publique dans Azure

Si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle du connecteur dans Azure, l'adresse IP doit utiliser une référence de base pour garantir que BlueXP utilise cette adresse IP publique.



Si vous utilisez une adresse IP de référence standard, BlueXP utilise l'adresse IP *private* du connecteur, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console BlueXP n'a pas accès à cette adresse IP privée, les actions de la console BlueXP échouent.

"Documentation Azure : référence IP publique"

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

+
Avec le mode privé, la seule fois que BlueXP envoie le trafic sortant est à votre fournisseur cloud pour créer un système Cloud Volumes ONTAP.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez.

HTTP (80) et HTTPS (443) permettent d'accéder à la console BlueXP. SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Étape 5 : préparez les autorisations cloud

Si le connecteur est installé dans le cloud et que vous prévoyez de créer des systèmes Cloud Volumes ONTAP, BlueXP requiert les autorisations de votre fournisseur cloud. Vous devez définir des autorisations dans votre fournisseur de cloud, puis les associer à l'instance Connector après l'avoir installée.

Pour afficher les étapes requises, sélectionnez l'option d'authentification que vous souhaitez utiliser pour votre fournisseur de cloud.

Rôle IAM AWS

Utilisez un rôle IAM pour fournir au connecteur des autorisations. Vous devrez associer manuellement le rôle à l'instance EC2 du connecteur.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.
3. Créer un rôle IAM :
   a. Sélectionnez **rôles > Créer un rôle**.
   b. Sélectionnez **AWS service > EC2**.
   c. Ajoutez des autorisations en joignant la stratégie que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous disposez désormais d'un rôle IAM pour l'instance de connecteur EC2.

Clé d'accès AWS

Configurer les autorisations et une clé d'accès pour un utilisateur IAM. Une fois le connecteur installé et configuré BlueXP, vous devez fournir BlueXP avec la clé d'accès AWS.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :

   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle.

   Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".

3. Associer les règles à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"
4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à BlueXP après l'installation du connecteur.

Résultat

Le compte dispose désormais des autorisations requises.

Rôle d'Azure

Créez un rôle Azure personnalisé avec les autorisations requises. Vous allez attribuer ce rôle à la machine virtuelle Connector.

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"

Étapes

1. Activez une identité gérée attribuée par le système sur la machine virtuelle où vous prévoyez d'installer le connecteur afin de fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'identifiant de chaque abonnement Azure que vous souhaitez utiliser avec BlueXP.

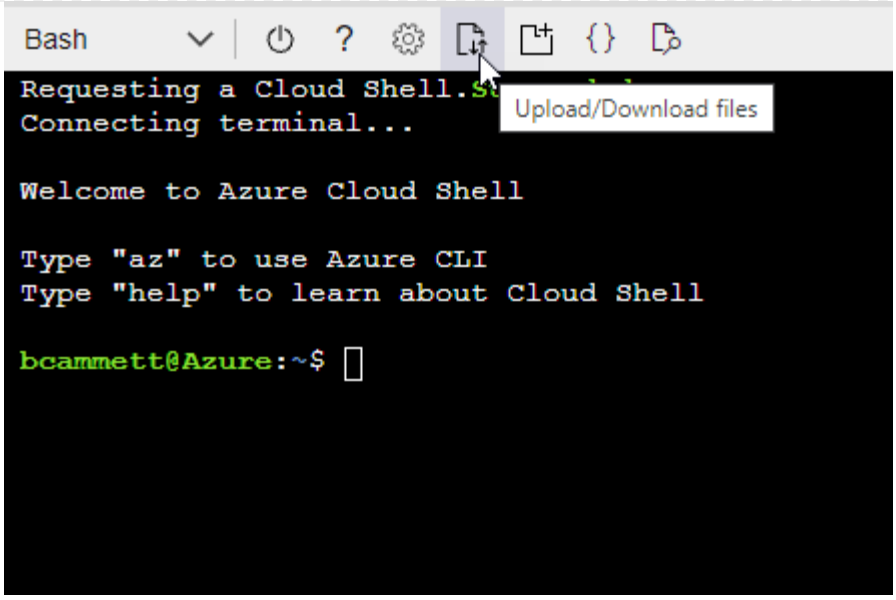
   Exemple

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

4. 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.

   a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
   b. Téléchargez le fichier JSON.



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

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

Résultat

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

Principal de service Azure

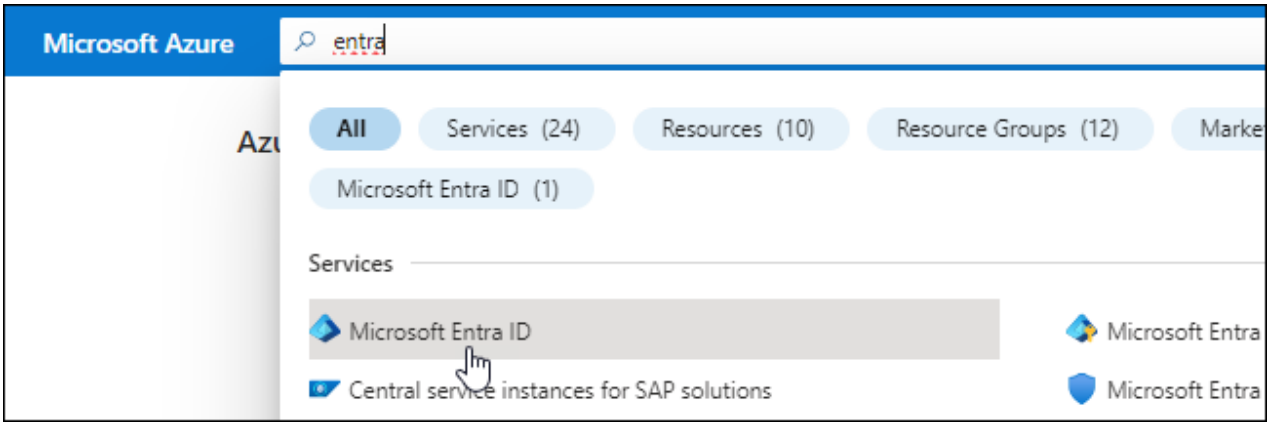
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin. Après avoir installé le connecteur et configuré BlueXP, vous devez fournir ces informations d'identification à BlueXP.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

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.

Attribuez l'application à un rôle

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.

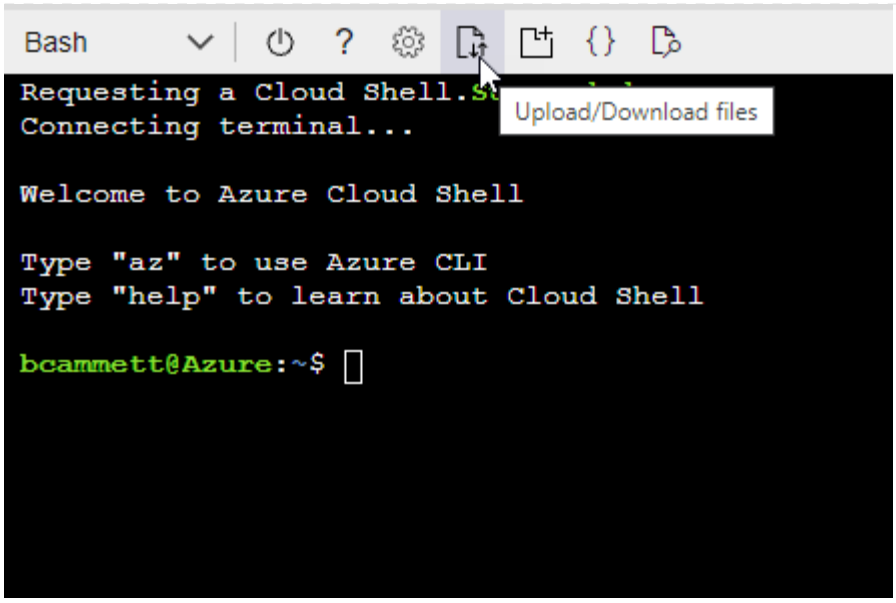
      Exemple

      ```
      "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 :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

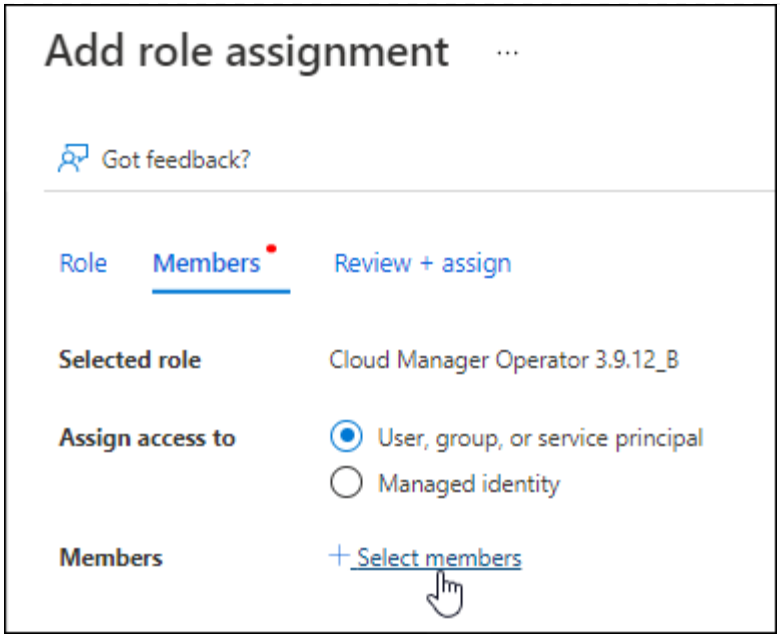
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

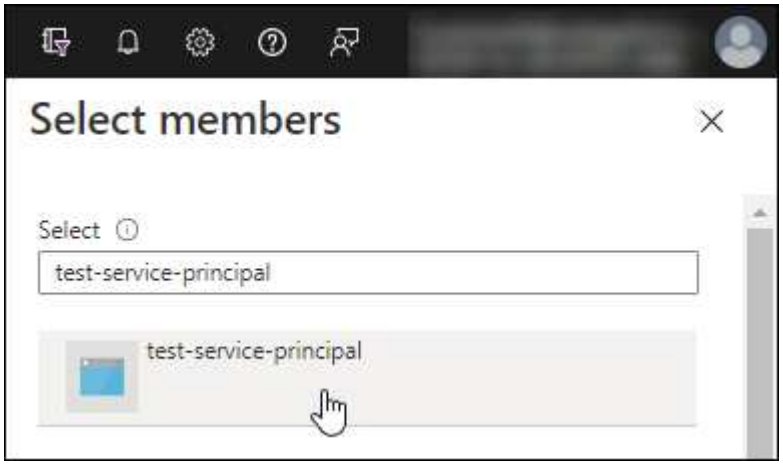
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

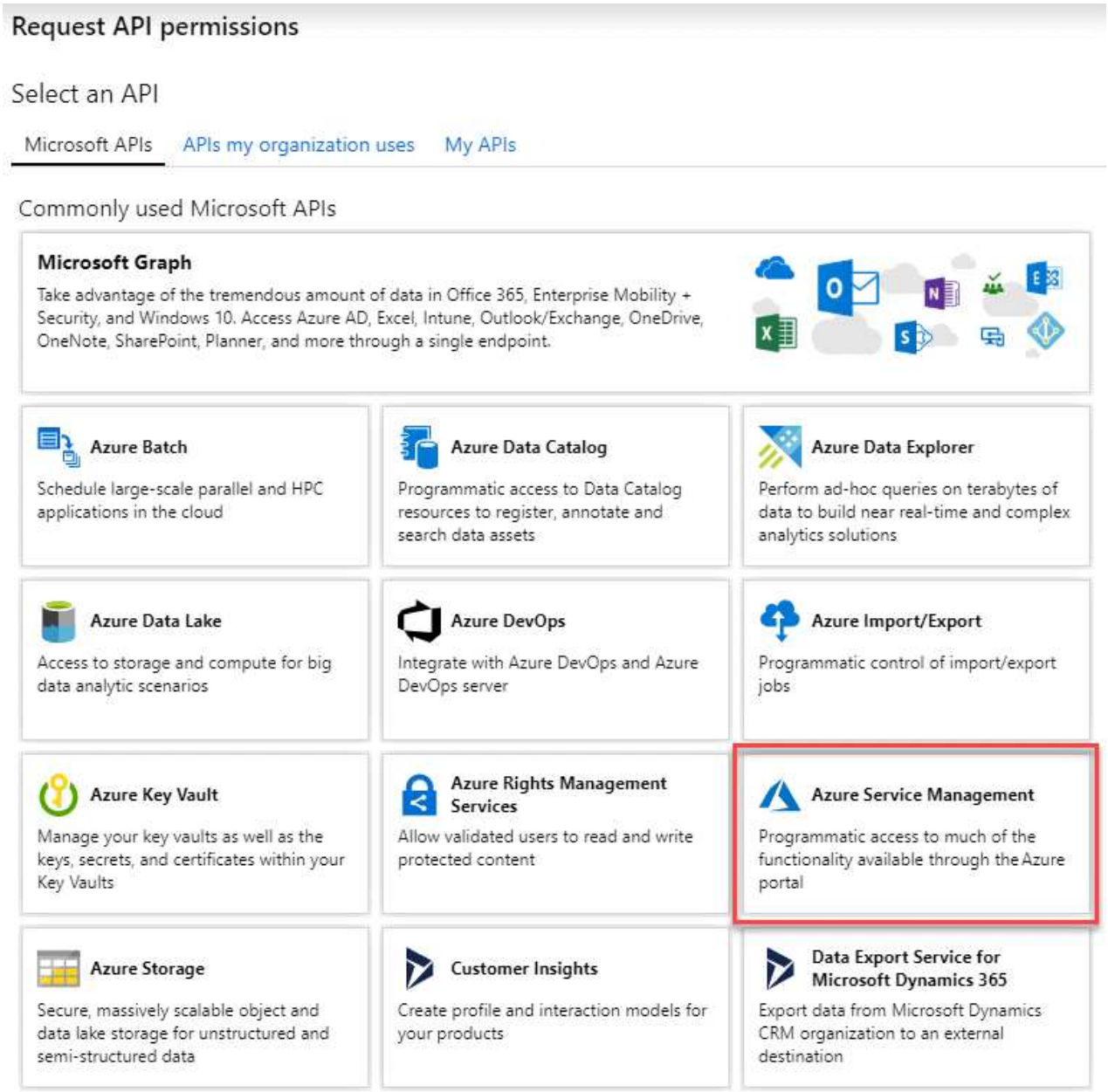
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

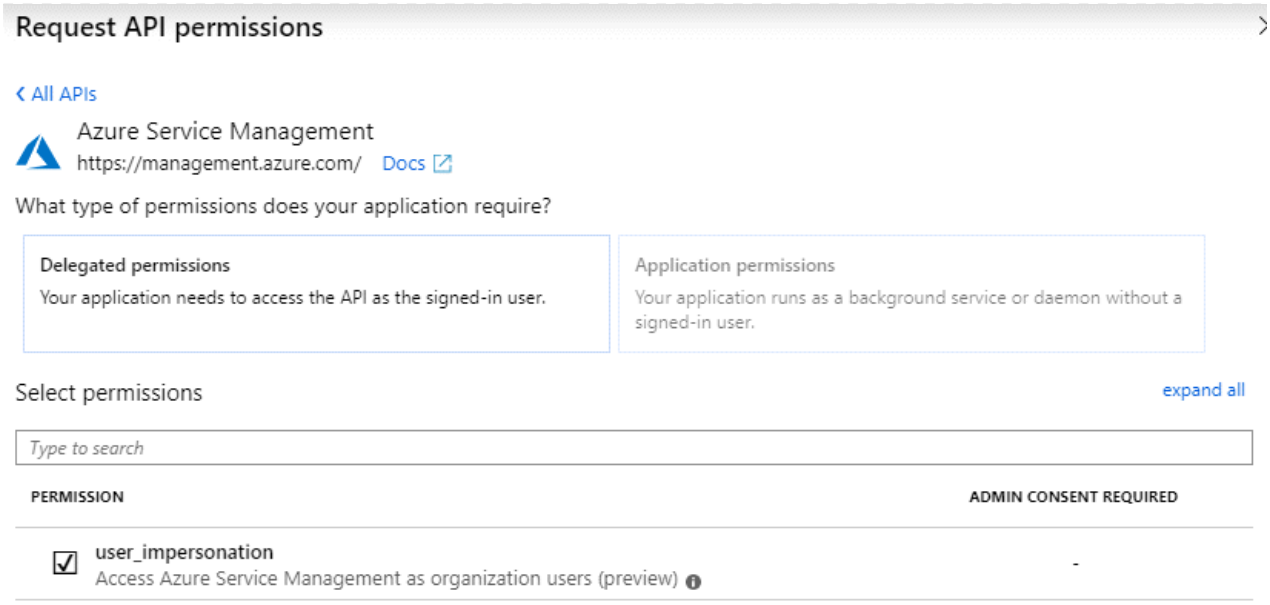
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

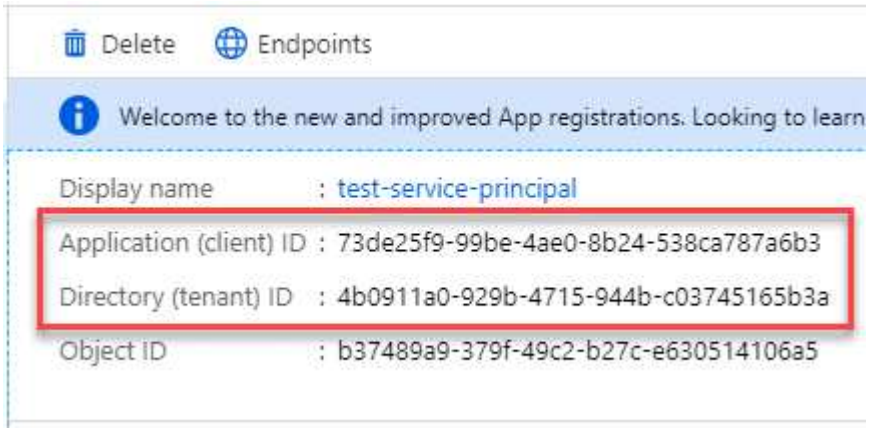


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

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

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.

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.

Compte de service Google Cloud

Créez un rôle et appliquez-le à un compte de service que vous utiliserez pour l'instance de la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut les autorisations définies dans le "Règle de connecteur pour Google Cloud".

   b. Dans Google Cloud, activez le shell cloud.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises pour le connecteur.

   d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

      L'exemple suivant crée un rôle nommé « connecteur » au niveau du projet :

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documents Google Cloud : création et gestion de rôles personnalisés"

2. Créez un compte de service dans Google Cloud :

   a. Dans le service IAM & Admin, sélectionnez **comptes de service > Créer un compte de service**.

   b. Entrez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

      "Documents Google Cloud : création d'un compte de service"

Résultat

Vous disposez désormais d'un compte de service que vous pouvez attribuer à l'instance VM Connector.

Étape 6 : activez les API Google Cloud

Plusieurs API sont requises pour déployer Cloud Volumes ONTAP dans Google Cloud.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API Cloud Deployment Manager V2
    - API de journalisation cloud
    - API Cloud Resource Manager
    - API du moteur de calcul
    - API de gestion des identités et des accès
    - API KMS (Cloud Key Management Service

      (Requis uniquement si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec des clés de chiffrement gérées par le client (CMEK))

Déployez le connecteur en mode privé

Déployez le connecteur en mode privé pour utiliser BlueXP sans connectivité sortante à la couche SaaS BlueXP. Pour commencer, installez le connecteur, configurez BlueXP en accédant à l'interface utilisateur exécutée sur le connecteur, puis fournissez les autorisations cloud que vous avez précédemment configurées.

Étape 1 : installez le connecteur

Téléchargez le programme d'installation du produit sur le site de support NetApp, puis installez manuellement le connecteur sur votre propre hôte Linux.

Si vous souhaitez utiliser BlueXP dans le "Cloud secret AWS" ou le "Le cloud le plus secret d'AWS", vous devez alors suivre des instructions séparées pour démarrer dans ces environnements. "Découvrez comment vous lancer avec Cloud Volumes ONTAP dans le cloud secret AWS ou le cloud secret"

Avant de commencer

Les privilèges root sont requis pour installer le connecteur.

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp"

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

3. Copiez le programme d'installation sur l'hôte Linux.
4. 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.

5. Exécutez le script d'installation :

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

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

Résultat

Le logiciel du connecteur est installé. Vous pouvez maintenant configurer BlueXP.

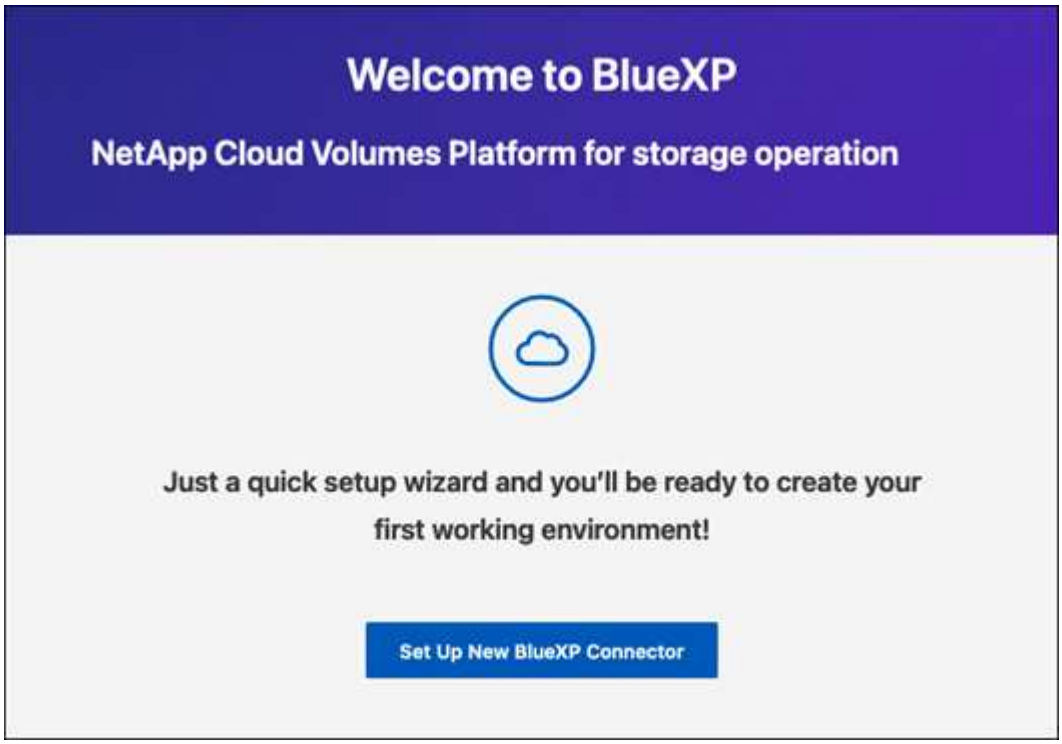
Étape 2 : configuration de BlueXP

Lorsque vous accédez pour la première fois à la console BlueXP, vous êtes invité à configurer BlueXP.

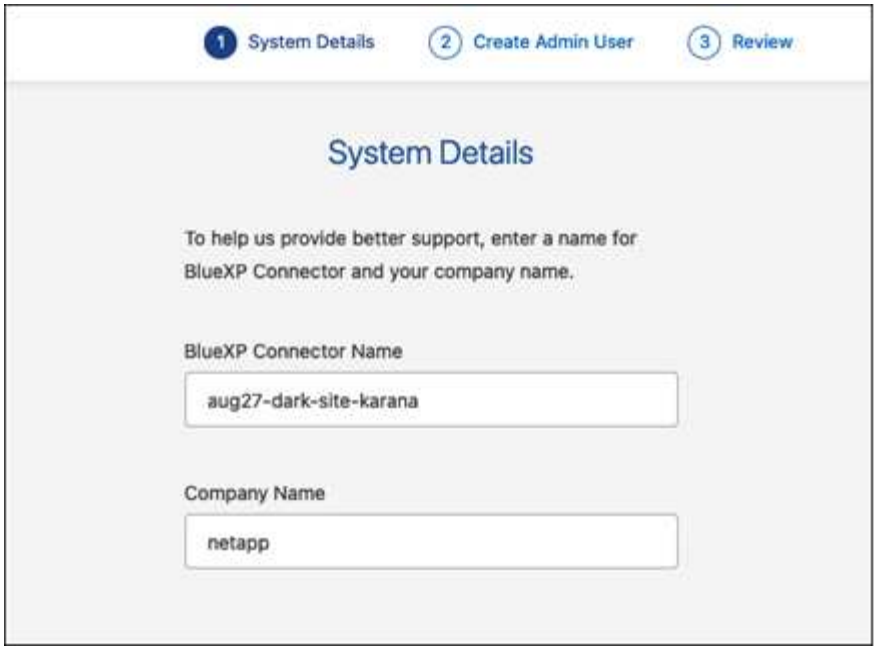
Étapes

1. Ouvrez un navigateur Web et entrez https://ipaddress Où ipaddress est l’adresse IP de l’hôte Linux où vous avez installé le connecteur.

   Vous devriez voir l'écran suivant.



2. Sélectionnez **configurer Nouveau connecteur BlueXP** et suivez les invites pour configurer le système.
   - **Détails du système** : saisissez un nom pour le connecteur et le nom de votre société.



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

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

- **Révision** : consultez les détails, acceptez le contrat de licence, puis sélectionnez **configurer**.

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

Résultat

Le connecteur est maintenant installé et configuré.

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

Et la suite ?

Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Étape 3 : fournissez des autorisations à BlueXP

Si vous souhaitez créer des environnements de travail Cloud Volumes ONTAP, vous devez fournir à BlueXP les autorisations cloud que vous avez précédemment configurées.

"Découvrez comment préparer les autorisations cloud".

Rôle IAM AWS

Reliez le rôle IAM que vous avez créé précédemment à l'instance Connector EC2.

Étapes

1. Accédez à la console Amazon EC2.
2. Sélectionnez **instances**.
3. Sélectionnez l'instance de connecteur.
4. Sélectionnez **actions > sécurité > Modifier le rôle IAM**.
5. Sélectionnez le rôle IAM et sélectionnez **mettre à jour le rôle IAM**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Clé d'accès AWS

Fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

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 **Amazon Web Services > connecteur**.
   b. **Définir les informations d'identification** : saisissez 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.
   d. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Rôle d'Azure

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Sur le portail Azure, ouvrez le service **Subscriptions** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Subscriptions** car cela spécifie la portée de l'affectation de rôle au niveau de l'abonnement. Le *scope* définit l'ensemble des ressources

auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau des machines virtuelles), votre capacité à effectuer des actions depuis BlueXP sera affectée.

"Documentation Microsoft Azure : étendue du contrôle d'accès basé sur des rôles Azure"

2. Sélectionnez **contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une affectation de rôle**.
3. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

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

4. Dans l'onglet **membres**, procédez comme suit :
   a. Attribuez l'accès à une identité **gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée, sous **identité gérée**, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle du connecteur.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **consulter + affecter**.
   f. Si vous souhaitez gérer les ressources d'autres abonnements Azure, passez à cet abonnement, puis répétez ces étapes.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Principal de service Azure

Fournissez à BlueXP les informations d'identification du principal de service Azure que vous avez précédemment configuré.

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

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Compte de service Google Cloud

Associez le compte de service à la VM Connector.

Étapes

1. Accédez au portail Google Cloud et attribuez le compte de service à l'instance de la VM Connector.

   "Documentation Google Cloud : modification du compte de service et des étendues d'accès pour une instance"

2. Si vous souhaitez gérer des ressources dans d'autres projets, accordez l'accès en ajoutant le compte de service doté du rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions en votre nom dans Google Cloud.

Que faire ensuite (mode privé)

Une fois que vous êtes opérationnel avec BlueXP en mode privé, vous pouvez commencer à utiliser les services BlueXP pris en charge par le mode privé.

Pour obtenir de l'aide, reportez-vous à la documentation suivante :

- "Création de systèmes Cloud Volumes ONTAP"
- "Découvrez les clusters ONTAP sur site"
- "Réplication des données"
- "Analysez les données de volumes ONTAP sur site à l'aide de la classification BlueXP"
- "Sauvegardez les données de volumes ONTAP sur site dans StorageGRID à l'aide de la sauvegarde et de la restauration BlueXP"

Lien associé

"Modes de déploiement BlueXP"

Connectez-vous à BlueXP

La façon dont vous vous connectez à BlueXP dépend du mode de déploiement BlueXP que vous utilisez pour votre compte.

Mode standard

Une fois que vous vous êtes inscrit à BlueXP, vous pouvez vous connecter à partir de la console web pour commencer à gérer vos données et votre infrastructure de stockage.

Description de la tâche

Vous pouvez vous connecter à la console Web BlueXP à l'aide de l'une des options suivantes :

- Vos identifiants existants du site de support NetApp (NSS)
- Un identifiant NetApp Cloud avec votre adresse e-mail et un mot de passe
- Une connexion fédérée

  Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). "Découvrez comment utiliser la fédération des identités avec BlueXP".

Étapes

1. Ouvrez un navigateur Web et accédez au "Console BlueXP"
2. Sur la page **connexion**, entrez l'adresse e-mail associée à votre connexion.
3. En fonction de la méthode d'authentification associée à votre connexion, vous serez invité à saisir vos informations d'identification :
   - Identifiants cloud NetApp : saisissez votre mot de passe
   - Utilisateur fédéré : saisissez vos informations d'identification fédérées
   - Entrez votre compte sur le site de support NetApp : saisissez vos identifiants du site de support NetApp

Résultat

Vous êtes maintenant connecté et pouvez commencer à utiliser BlueXP pour gérer votre infrastructure multicloud hybride.

Mode restreint

Lorsque vous utilisez BlueXP en mode restreint, vous devez vous connecter à la console BlueXP à partir de l'interface utilisateur qui s'exécute localement sur le connecteur.

Description de la tâche

BlueXP prend en charge la connexion avec l'une des options suivantes lorsque votre compte est configuré en mode restreint :

- Un identifiant NetApp Cloud avec votre adresse e-mail et un mot de passe
- Une connexion fédérée

  Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). "Découvrez comment utiliser la fédération des identités avec BlueXP".

Étapes

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

   https://ipaddress

Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte où vous avez installé le connecteur. Par exemple, vous devrez peut-être entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

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

Résultat

Vous êtes maintenant connecté et pouvez commencer à utiliser BlueXP pour gérer votre infrastructure multicloud hybride.

Mode privé

Lorsque vous utilisez BlueXP en mode privé, vous devez vous connecter à la console BlueXP à partir de l'interface utilisateur qui s'exécute localement sur le connecteur.

Description de la tâche

Le mode privé prend en charge la gestion et l'accès des utilisateurs locaux. L'authentification n'est pas fournie via le service cloud de BlueXP.

Étapes

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

   https://ipaddress

   Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte où vous avez installé le connecteur. Par exemple, vous devrez peut-être entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

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

Résultat

Vous êtes maintenant connecté et pouvez commencer à utiliser BlueXP pour gérer votre infrastructure multicloud hybride.