



Documentation sur les clusters Kubernetes

Kubernetes clusters

NetApp
January 04, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/bluexp-kubernetes/index.html> on January 04, 2024. Always check docs.netapp.com for the latest.

Sommaire

Documentation sur les clusters Kubernetes	1
Nouveautés de Kubernetes dans BlueXP	2
02 avril 2023	2
05 mars 2023	2
06 novembre 2022	2
18 septembre 2022	2
31 juillet 2022	2
3 juillet 2022	2
6 juin 2022	3
4 mai 2022	3
4 avril 2022	3
27 février 2022	3
11 janvier 2022	4
28 novembre 2021	4
Commencez	5
Gestion des données Kubernetes dans BlueXP	5
Commencez avec les clusters Kubernetes	6
De formation	7
Conditions requises pour les clusters Kubernetes dans AWS	7
Conditions requises pour les clusters Kubernetes dans Azure	16
Conditions requises pour les clusters Kubernetes dans Google Cloud	24
Conditions requises pour les clusters Kubernetes dans OpenShift	31
Ajouter des clusters Kubernetes	40
Ajouter un cluster Amazon Kubernetes à BlueXP	40
Ajout d'un cluster Azure Kubernetes à BlueXP	42
Ajouter un cluster Google Cloud Kubernetes à BlueXP	45
Importez un cluster OpenShift vers BlueXP	49
Gérez les clusters Kubernetes	51
Gérez Astra Trident	51
Gérer les classes de stockage	53
Afficher les volumes persistants	57
Supprimez les clusters Kubernetes de l'espace de travail	58
Utilisez les services de données cloud NetApp avec des clusters Kubernetes	59
Connaissances et support	60
S'inscrire pour obtenir de l'aide	60
Obtenez de l'aide	64
Mentions légales	70
Droits d'auteur	70
Marques déposées	70
Brevets	70
Politique de confidentialité	70
Source ouverte	70

Documentation sur les clusters Kubernetes

Nouveautés de Kubernetes dans BlueXP

Découvrez les nouveautés de Kubernetes dans BlueXP.

02 avril 2023

- C'est possible maintenant ["Désinstallez Astra Trident"](#) Qui a été installé à l'aide de l'opérateur Trident ou de BlueXP.
- Des améliorations ont été apportées à l'interface utilisateur et des captures d'écran ont été mises à jour dans la documentation.

05 mars 2023

- Kubernetes dans BlueXP prend désormais en charge Astra Trident 23.01.
- Des améliorations ont été apportées à l'interface utilisateur et des captures d'écran ont été mises à jour dans la documentation.

06 novembre 2022

Quand ["définition des classes de stockage"](#), vous pouvez maintenant activer l'économie de classe de stockage pour le stockage en mode bloc ou système de fichiers.

18 septembre 2022

Vous pouvez désormais importer des clusters OpenShift autogérés dans Cloud Manager.

- ["Conditions requises pour les clusters Kubernetes dans OpenShift"](#)
- ["Importez un cluster OpenShift vers Cloud Manager"](#)

31 juillet 2022

- Utilisation du nouveau `watch` Verbe dans la classe de stockage, la sauvegarde et la restauration des configurations YAML, Cloud Manager peut désormais surveiller les clusters Kubernetes pour les modifications apportées au back-end du cluster et activer automatiquement la sauvegarde des nouveaux volumes persistants si la sauvegarde automatique a été configurée sur le cluster.

["Conditions requises pour les clusters Kubernetes dans AWS"](#)

["Conditions requises pour les clusters Kubernetes dans Azure"](#)

["Conditions requises pour les clusters Kubernetes dans Google Cloud"](#)

- Quand ["définition des classes de stockage"](#), vous pouvez maintenant spécifier un type de système de fichiers (fstype) pour le stockage en mode bloc.

3 juillet 2022

- Si Astra Trident a été déployé avec l'opérateur Trident, vous pouvez désormais effectuer la mise à niveau

vers la dernière version d'Astra Trident avec Cloud Manager.

["Installer et gérer Astra Trident"](#)

- Vous pouvez à présent faire glisser votre cluster Kubernetes et le déposer dans l'environnement de travail AWS FSX pour ONTAP afin d'ajouter une classe de stockage directement à partir de la fenêtre Canvas.

["Ajouter une classe de stockage"](#)

6 juin 2022

Cloud Manager prend désormais en charge Amazon FSX for ONTAP en tant que stockage back-end.

4 mai 2022

Effectuez un glisser-déposer pour ajouter une classe de stockage

Vous pouvez désormais glisser votre cluster Kubernetes et le déposer dans l'environnement de travail Cloud Volumes ONTAP pour ajouter une classe de stockage directement depuis la fenêtre Canvas.

["Ajouter une classe de stockage"](#)

4 avril 2022

Gérez des clusters Kubernetes à l'aide de la page de ressources Cloud Manager

La gestion des clusters Kubernetes a maintenant amélioré l'intégration directement depuis l'environnement de travail du cluster. Une nouvelle ["Démarrage rapide"](#) vous permet de vous mettre en route rapidement.

Vous pouvez maintenant effectuer les actions suivantes à partir de la page de ressources du cluster.

- ["Installer Astra Trident"](#)
- ["Ajouter des classes de stockage"](#)
- ["Afficher les volumes persistants"](#)
- ["Supprimer les clusters"](#)
- ["Proposez des services de données"](#)

27 février 2022

Prise en charge des clusters Kubernetes dans Google Cloud

Vous pouvez désormais ajouter et gérer des clusters Google Kubernetes Engine (GKE) gérés et des clusters Kubernetes autogérés dans Google Cloud à l'aide de Cloud Manager.

["Découvrez comment se lancer avec des clusters Kubernetes dans Google Cloud"](#).

11 janvier 2022

Prise en charge des clusters Kubernetes dans Azure

Vous pouvez désormais ajouter et gérer des clusters Azure Kubernetes gérés (AKS) et des clusters Kubernetes autogérés dans Azure à l'aide de Cloud Manager.

["Mise en route des clusters Kubernetes dans Azure"](#)

28 novembre 2021

Prise en charge des clusters Kubernetes dans AWS

Vous pouvez à présent ajouter vos clusters Kubernetes gérés dans Canvas de Cloud Manager pour une gestion avancée des données.

- Découvrez les clusters Amazon EKS
- Sauvegarde des volumes persistants à l'aide de Cloud Backup

["En savoir plus sur la prise en charge de Kubernetes"](#).



Le service Kubernetes existant (disponible via l'onglet **K8s**) est obsolète et sera supprimé dans une prochaine version.

Commencez

Gestion des données Kubernetes dans BlueXP

Astra Trident est un projet open source entièrement pris en charge et géré par NetApp. Astra Trident s'intègre de manière native avec Kubernetes et son framework de volumes persistants pour provisionner et gérer les volumes de manière transparente à partir des systèmes qui exécutent toutes les combinaisons de plateformes de stockage NetApp. ["En savoir plus sur Trident"](#).

Caractéristiques

À l'aide de ["BlueXP"](#) Et une version compatible d'Astra Trident déployée à l'aide de l'opérateur Trident, vous pouvez :

- Ajoutez et gérez des clusters Kubernetes
- ["Installez, mettez à niveau ou désinstallez Astra Trident"](#)
- ["Ajouter et supprimer des classes de stockage"](#)
- ["Afficher les volumes persistants"](#)
- ["Supprimez les clusters Kubernetes"](#) depuis l'espace de travail
- ["Activez ou affichez la sauvegarde et la restauration BlueXP"](#)

Déploiements Kubernetes pris en charge

BlueXP prend en charge les clusters Kubernetes gérés dans :

- ["Amazon Elastic Kubernetes Service \(Amazon EKS\)"](#)
- ["Microsoft Azure Kubernetes Service \(AKS\)"](#)
- ["Google Kubernetes Engine \(GKE\)"](#)

Prise en charge des déploiements Astra Trident

L'une des quatre versions les plus récentes d'Astra Trident ["Déployé à l'aide de l'opérateur Trident"](#) est obligatoire.



Astra Trident déployé avec `tridentctl` n'est pas pris en charge. Si vous avez déployé Astra Trident avec `tridentctl`, Vous ne pouvez pas utiliser BlueXP pour gérer vos clusters Kubernetes. Vous devez et réinstaller ["Utilisation de l'opérateur Trident"](#) ou ["Utilisation de BlueXP"](#).

Vous pouvez installer ou mettre à niveau la dernière version d'Astra Trident directement à partir de BlueXP.

["Lisez les conditions préalables à l'Astra Trident"](#)

Stockage interne pris en charge

NetApp Astra Trident doit être installé sur chaque cluster Kubernetes, et Cloud Volumes ONTAP ou Amazon

FSX pour ONTAP doit être configuré en tant que stockage back-end pour les clusters.

Le coût

Ce n'est pas facturé pour *découvrir* vos clusters Kubernetes dans BlueXP, mais vous serez facturé lorsque vous sauvegardez des volumes persistants à l'aide de Cloud Backup Service.

Commencez avec les clusters Kubernetes

À l'aide de "BlueXP" Vous pouvez commencer à gérer les clusters Kubernetes en quelques étapes seulement.

1

Passer en revue les prérequis

Assurez-vous que votre environnement respecte les conditions préalables requises pour votre type de cluster.

["Conditions requises pour les clusters Kubernetes dans AWS"](#)

["Conditions requises pour les clusters Kubernetes dans Azure"](#)

["Conditions requises pour les clusters Kubernetes dans Google Cloud"](#)

2

Ajoutez vos clusters Kubernetes à BlueXP

Vous pouvez ajouter des clusters Kubernetes et les connecter à un environnement de travail à l'aide de BlueXP.

["Ajoutez un cluster Amazon Kubernetes"](#)

["Ajoutez un cluster Azure Kubernetes"](#)

["Ajoutez un cluster Google Cloud Kubernetes"](#)

3

Commencez le provisionnement des volumes persistants

Demandez et gérez les volumes persistants à l'aide d'interfaces et de constructions Kubernetes natives. BlueXP crée des classes de stockage NFS et iSCSI que vous pouvez utiliser pour le provisionnement de volumes persistants.

["En savoir plus sur le provisionnement de votre premier volume avec Astra Trident"](#).

4

Gérez vos clusters à l'aide de BlueXP

Après avoir ajouté des clusters Kubernetes à BlueXP, vous pouvez gérer les clusters à partir de la page de ressources BlueXP.

["Apprenez à gérer les clusters Kubernetes."](#)

De formation

Conditions requises pour les clusters Kubernetes dans AWS

Vous pouvez ajouter des clusters Amazon Elastic Kubernetes Service (EKS) gérés ou des clusters Kubernetes autogérés sur AWS à BlueXP. Avant de pouvoir ajouter les clusters à BlueXP, vous devez vous assurer que les conditions suivantes sont remplies.



Cette section utilise *Kubernetes cluster* où la configuration est la même pour les clusters EKS et Kubernetes autogérés. Le type de cluster est spécifié où la configuration diffère.

De formation

Astra Trident

Il est nécessaire de disposer de l'une des quatre versions les plus récentes d'Astra Trident. Vous pouvez installer ou mettre à niveau Astra Trident directement à partir de BlueXP. Vous devriez ["passez en revue les prérequis"](#) Avant d'installer Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP pour AWS doit être configuré en tant que système de stockage back-end pour le cluster. ["Accédez à la documentation Astra Trident pour connaître les étapes de configuration"](#).

Connecteur BlueXP

Un connecteur doit être exécuté dans AWS avec les autorisations requises. [Pour en savoir plus](#).

Connectivité réseau

La connectivité réseau est requise entre le cluster Kubernetes et le connecteur et entre le cluster Kubernetes et Cloud Volumes ONTAP. [Pour en savoir plus](#).

Autorisation RBAC

Le rôle BlueXP Connector doit être autorisé sur chaque cluster Kubernetes. [Pour en savoir plus](#).

Préparer un connecteur

BlueXP Connector est nécessaire dans AWS pour détecter et gérer les clusters Kubernetes. Vous devrez créer un nouveau connecteur ou utiliser un connecteur existant disposant des autorisations requises.

Créer un nouveau connecteur

Suivez les étapes de l'un des liens ci-dessous.

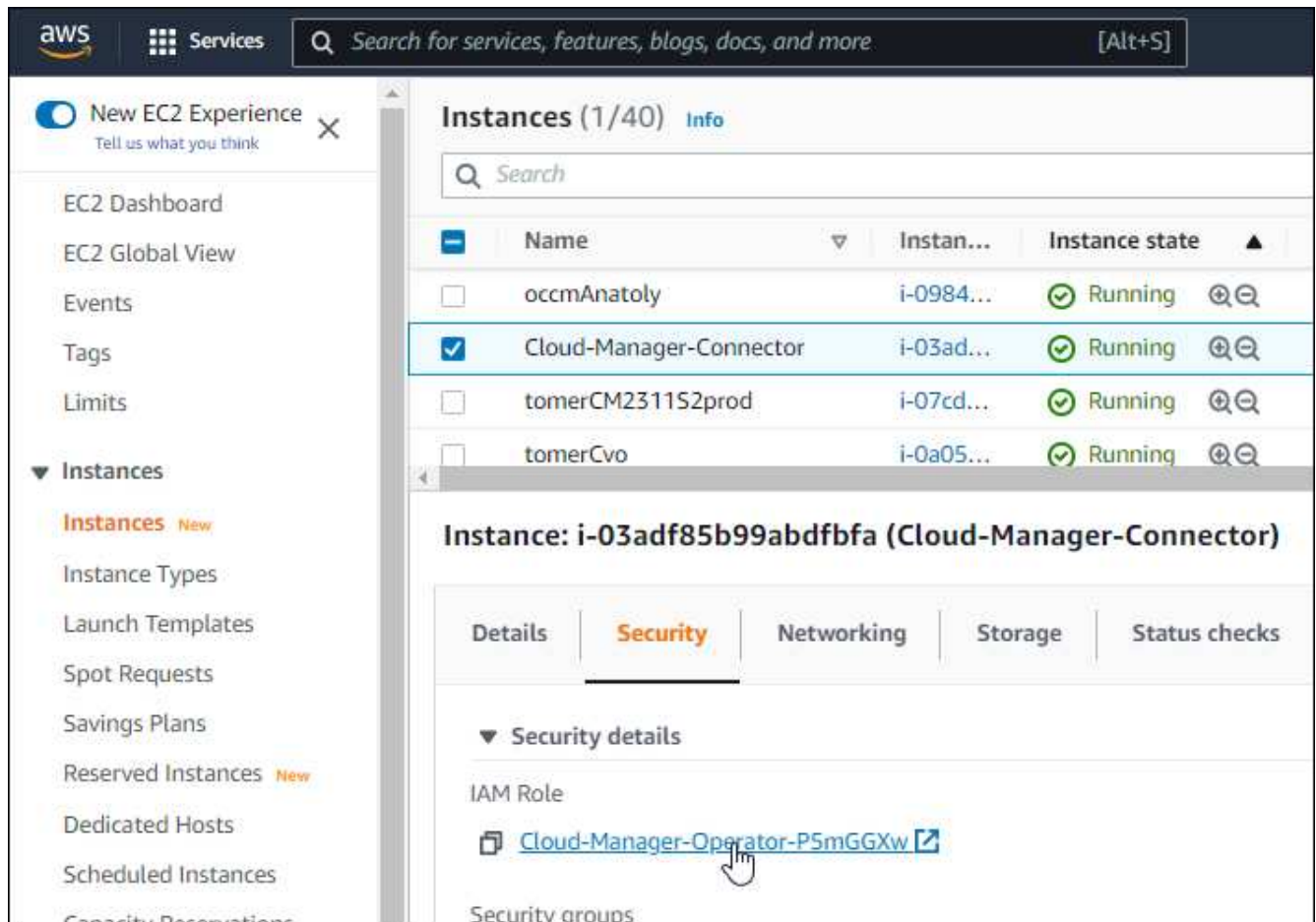
- ["Créez un connecteur depuis BlueXP"](#) (recommandé)
- ["Créez un connecteur à partir d'AWS Marketplace"](#)
- ["Installez le connecteur sur un hôte Linux existant dans AWS"](#)

Ajoutez les autorisations requises à un connecteur existant

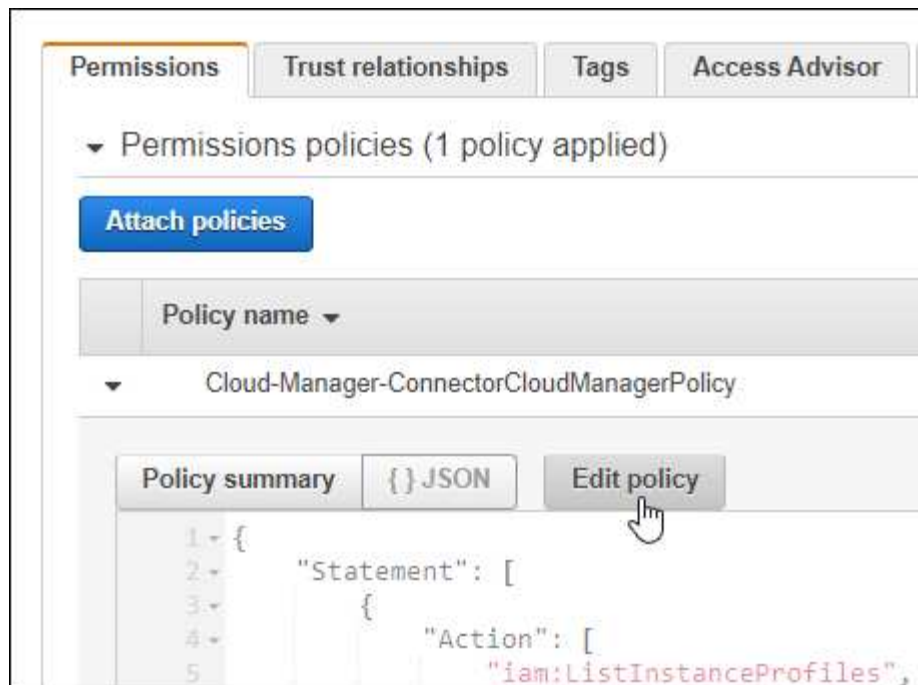
À partir de la version 3.9.13, tout *nouvellement* créé Connector inclut trois nouvelles autorisations AWS permettant la découverte et la gestion des clusters Kubernetes. Si vous avez créé un connecteur avant cette version, vous devrez modifier la stratégie existante pour le rôle IAM du connecteur afin de fournir les autorisations nécessaires.

Étapes

1. Accédez à la console AWS et ouvrez le service EC2.
2. Sélectionnez l'instance de connecteur, cliquez sur **sécurité**, puis cliquez sur le nom du rôle IAM pour afficher le rôle dans le service IAM.



3. Dans l'onglet **permissions**, développez la stratégie et cliquez sur **Modifier la stratégie**.



4. Cliquez sur **JSON** et ajoutez les autorisations suivantes dans la première série d'actions :

- ec2:régions descriptives
- eks:Listclusters
- eks:DescribeCluster
- iam:GetInstanceProfile

["Afficher le format JSON complet de la règle"](#)

5. Cliquez sur **Review Policy**, puis sur **Save Changes**.

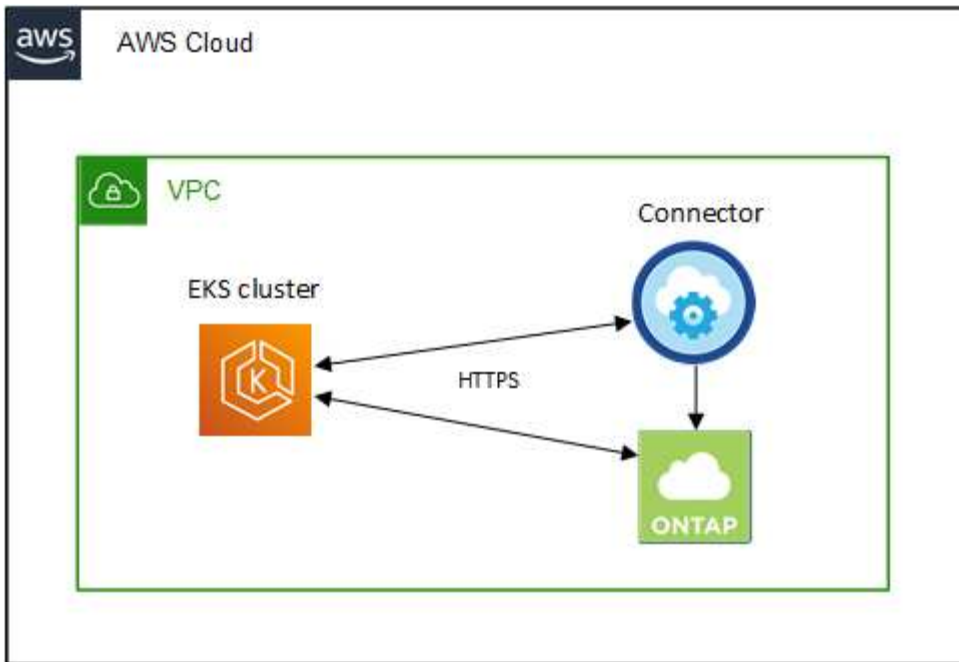
Examiner les besoins en matière de mise en réseau

Il faut assurer une connectivité réseau entre le cluster Kubernetes et le connecteur, et entre le cluster Kubernetes et le système Cloud Volumes ONTAP qui fournit un stockage back-end au cluster.

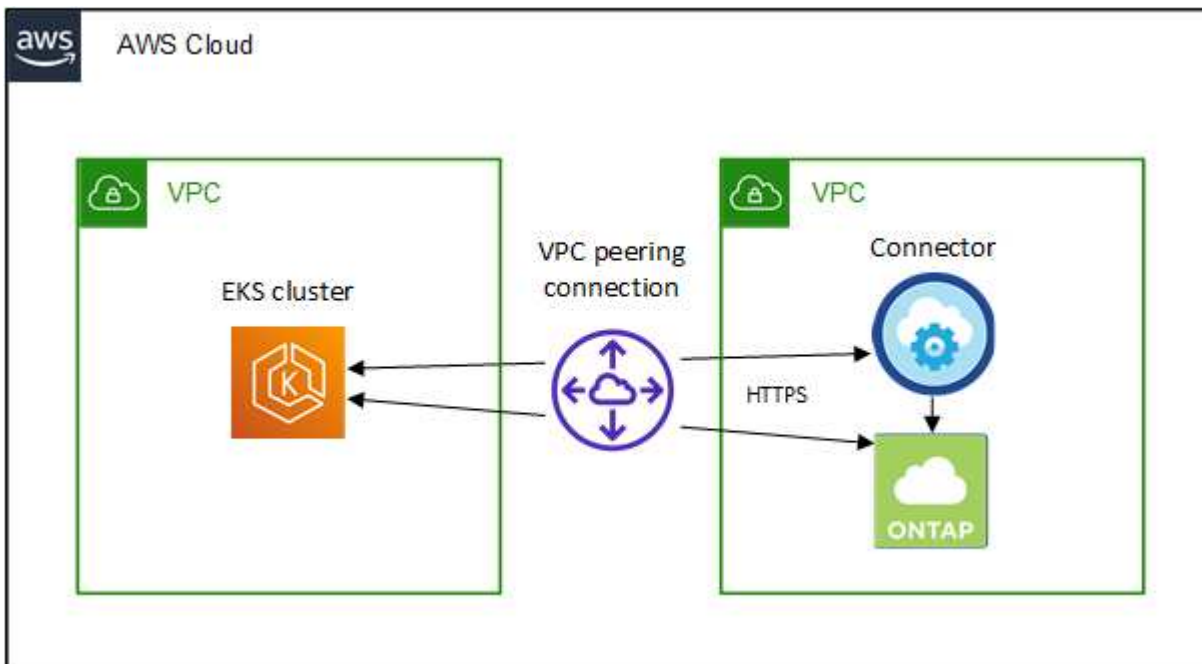
- Chaque cluster Kubernetes doit disposer d'une connexion entrante depuis le connecteur
- Le connecteur doit disposer d'une connexion sortante vers chaque cluster Kubernetes sur le port 443

Pour fournir cette connectivité, la méthode la plus simple est de déployer le connecteur et Cloud Volumes ONTAP dans le même VPC que le cluster Kubernetes. Sinon, vous devez configurer une connexion de peering VPC entre les différents VPC.

Voici un exemple illustrant chaque composant dans le même VPC.



Et voici un autre exemple de cluster EKS s'exécutant sur un autre VPC. Dans cet exemple, le VPC peering fournit une connexion entre le VPC pour le cluster EKS et le VPC pour le connecteur et le Cloud Volumes ONTAP.



Configurez l'autorisation RBAC

Vous devez autoriser le rôle de connecteur sur chaque cluster Kubernetes afin que le connecteur puisse détecter et gérer un cluster.

Une autorisation différente est requise pour activer différentes fonctionnalités.

Sauvegarde et restauration

La sauvegarde et la restauration ne nécessitent que l'autorisation de base.

Ajouter des classes de stockage

Une autorisation étendue est nécessaire pour ajouter des classes de stockage à l'aide de BlueXP et surveiller le cluster pour les modifications apportées au back-end.

Installer Astra trident

Vous devez fournir une autorisation complète pour BlueXP afin d'installer Astra Trident.



Pour installer Astra Trident, BlueXP installe le système back-end Trident et le secret Kubernetes qui contient les identifiants Astra Trident qui doit communiquer avec le cluster de stockage.

Étapes

1. Créer un rôle de cluster et une liaison de rôle.
 - a. Vous pouvez personnaliser l'autorisation en fonction de vos besoins.

Sauvegarde/restauration

Ajoutez une autorisation de base pour activer la sauvegarde et la restauration des clusters Kubernetes.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - namespaces
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
```

```

      - list
- apiGroups:
    - trident.netapp.io
  resources:
    - tridentbackends
  verbs:
    - list
    - watch
- apiGroups:
    - trident.netapp.io
  resources:
    - tridentorchestrators
  verbs:
    - get
    - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
- kind: Group
  name: cloudmanager-access-group
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

Classes de stockage

Ajoutez une autorisation étendue pour ajouter des classes de stockage à l'aide de BlueXP.

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
- apiGroups:
    - ''
  resources:
    - secrets
    - namespaces
    - persistentvolumeclaims
    - persistentvolumes
    - pods

```

```

      - pods/exec
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - create
      - list
      - watch
      - delete
      - patch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
      - tridentbackendconfigs
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: Group
    name: cloudmanager-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```


Installation de Trident

Utilisez la ligne de commande pour fournir une autorisation complète et permettre à BlueXP d'installer Astra Trident.

```
eksctl create iamidentitymapping --cluster < > --region < > --arn  
< > --group "system:masters" --username  
system:node:{{EC2PrivateDNSName}}
```

b. Appliquer la configuration à un cluster

```
kubectl apply -f <file-name>
```

2. Créez un mappage d'identité avec le groupe d'autorisations.

Utiliser eksctl

Utilisez eksctl pour créer un mappage d'identité IAM entre un cluster et le rôle IAM pour le connecteur BlueXP.

["Consultez la documentation eksctl pour obtenir des instructions complètes"](#).

Un exemple est fourni ci-dessous.

```
eksctl create iamidentitymapping --cluster <eksCluster> --region  
<us-east-2> --arn <ARN of the Connector IAM role> --group  
cloudmanager-access-group --username  
system:node:{{EC2PrivateDNSName}}
```

Modifiez aws-auth

Modifiez directement le AWS-auth ConfigMap pour ajouter un accès RBAC au rôle IAM pour le connecteur BlueXP.

["Pour obtenir des instructions complètes, consultez la documentation AWS EKS"](#).

Un exemple est fourni ci-dessous.

```
apiVersion: v1  
data:  
  mapRoles: |  
    - groups:  
      - cloudmanager-access-group  
      rolearn: <ARN of the Connector IAM role>  
      username: system:node:{{EC2PrivateDNSName}}  
kind: ConfigMap  
metadata:  
  creationTimestamp: "2021-09-30T21:09:18Z"  
  name: aws-auth  
  namespace: kube-system  
  resourceVersion: "1021"  
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth  
  uid: dcc31de5-3838-11e8-af26-02e00430057c
```

Conditions requises pour les clusters Kubernetes dans Azure

Vous pouvez ajouter et gérer des clusters Azure Kubernetes gérés (AKS) et des clusters Kubernetes autogérés dans Azure à l'aide de BlueXP. Avant de pouvoir ajouter les clusters à BlueXP, assurez-vous que les conditions suivantes sont remplies.



Cette section utilise *Kubernetes cluster* où la configuration est la même pour les clusters AKS et Kubernetes autogérés. Le type de cluster est spécifié où la configuration diffère.

De formation

Astra Trident

Il est nécessaire de disposer de l'une des quatre versions les plus récentes d'Astra Trident. Vous pouvez installer ou mettre à niveau Astra Trident directement à partir de BlueXP. Vous devriez ["passez en revue les prérequis"](#) Avant d'installer Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP doit être configuré en tant que système de stockage back-end pour le cluster. ["Accédez à la documentation Astra Trident pour connaître les étapes de configuration"](#).

Connecteur BlueXP

Un connecteur doit s'exécuter dans Azure avec les autorisations requises. [Pour en savoir plus](#).

Connectivité réseau

La connectivité réseau est requise entre le cluster Kubernetes et le connecteur et entre le cluster Kubernetes et Cloud Volumes ONTAP. [Pour en savoir plus](#).

Autorisation RBAC

BlueXP prend en charge les clusters RBAC avec et sans Active Directory. Le rôle connecteur BlueXP doit être autorisé sur chaque cluster Azure. [Pour en savoir plus](#).

Préparer un connecteur

Un connecteur BlueXP dans Azure est nécessaire pour découvrir et gérer les clusters Kubernetes. Vous devrez créer un nouveau connecteur ou utiliser un connecteur existant disposant des autorisations requises.

Créer un nouveau connecteur

Suivez les étapes de l'un des liens ci-dessous.

- ["Créez un connecteur depuis BlueXP"](#) (recommandé)
- ["Créez un connecteur à partir d'Azure Marketplace"](#)
- ["Installez le connecteur sur un hôte Linux existant"](#)

Ajoutez les autorisations requises à un connecteur existant (pour découvrir un cluster AKS géré)

Si vous souhaitez découvrir un cluster AKS géré, vous devrez peut-être modifier le rôle personnalisé du connecteur pour lui fournir les autorisations.

Étapes

1. Identifier le rôle attribué à la machine virtuelle Connector :
 - a. Dans le portail Azure, ouvrez le service Virtual machines.
 - b. Sélectionnez la machine virtuelle Connector.
 - c. Sous Paramètres, sélectionnez **identité**.
 - d. Cliquez sur **attributions de rôles Azure**.

- e. Notez le rôle personnalisé attribué à la machine virtuelle Connector.
2. Mettre à jour le rôle personnalisé :
- Sur le portail Azure, ouvrez votre abonnement Azure.
 - Cliquez sur **contrôle d'accès (IAM) > rôles**.
 - Cliquez sur les points de suspension (...) du rôle personnalisé, puis cliquez sur **Modifier**.
 - Cliquez sur JSON et ajoutez les autorisations suivantes :

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/action"  
"Microsoft.ContainerService/managedClusters/read"
```

- e. Cliquez sur **Revue + mise à jour**, puis sur **mise à jour**.

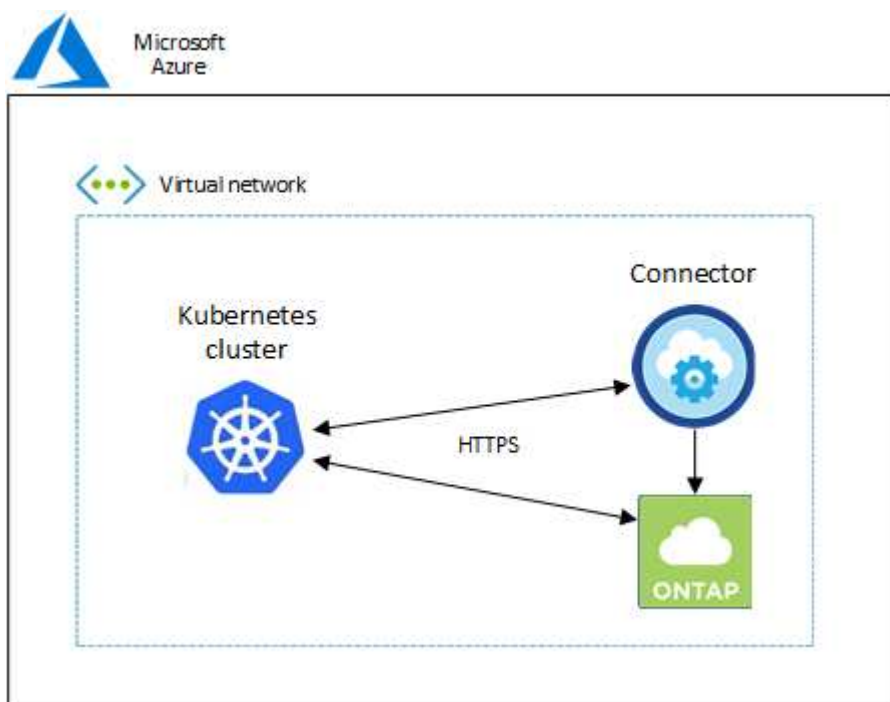
Examiner les besoins en matière de mise en réseau

Il faut assurer une connectivité réseau entre le cluster Kubernetes et le connecteur, et entre le cluster Kubernetes et le système Cloud Volumes ONTAP qui fournit un stockage back-end au cluster.

- Chaque cluster Kubernetes doit disposer d'une connexion entrante depuis le connecteur
- Le connecteur doit disposer d'une connexion sortante vers chaque cluster Kubernetes sur le port 443

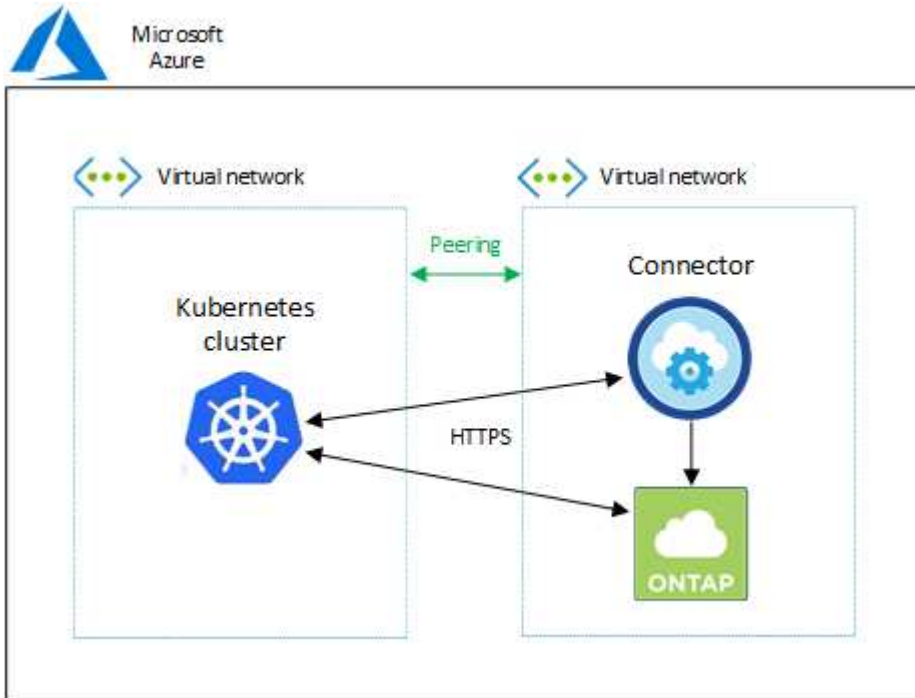
Pour obtenir cette connectivité, la méthode la plus simple consiste à déployer le connecteur et Cloud Volumes ONTAP dans le même vnet que le cluster Kubernetes. Sinon, vous devez configurer une connexion de peering entre les différents VNets.

Voici un exemple qui montre chaque composant dans le même vnet.



Et voici un autre exemple de cluster Kubernetes qui s'exécute dans un autre vnet. Dans cet exemple, peering

fournit une connexion entre le vnet pour le cluster Kubernetes et le vnet pour le connecteur et Cloud Volumes ONTAP.



Configurez l'autorisation RBAC

La validation RBAC a lieu uniquement sur les clusters Kubernetes où Active Directory (AD) est activé. Les clusters Kubernetes sans AD passent automatiquement la validation.

Vous devez autoriser le rôle de connecteur sur chaque cluster Kubernetes afin que le connecteur puisse détecter et gérer un cluster.

Sauvegarde et restauration

La sauvegarde et la restauration ne nécessitent que l'autorisation de base.

Ajouter des classes de stockage

Une autorisation étendue est nécessaire pour ajouter des classes de stockage à l'aide de BlueXP et surveiller le cluster pour les modifications apportées au back-end.

Installer Astra trident

Vous devez fournir une autorisation complète pour BlueXP afin d'installer Astra Trident.



Pour installer Astra Trident, BlueXP installe le système back-end Trident et le secret Kubernetes qui contient les identifiants Astra Trident qui doit communiquer avec le cluster de stockage.

Avant de commencer

Votre RBAC `subjects: name:` La configuration varie légèrement en fonction de votre type de cluster Kubernetes.

- Si vous déployez un cluster **Managed AKS**, vous avez besoin de l'ID objet pour l'identité gérée attribuée par le système pour le connecteur. Cet identifiant est disponible sur le portail de gestion Azure.

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. \n in code. [Learn more about Managed identities.](#)

Save Discard Refresh | Got feedback?

Status ⓘ

Off **On**

Object (principal) ID ⓘ

0c288856-adea-485b-a4dc-c15b5ce2c401

Permissions ⓘ

Azure role assignments

- Si vous déployez un cluster Kubernetes* *autogéré, vous devez disposer du nom d'utilisateur de tout utilisateur autorisé.

Étapes

Créer un rôle de cluster et une liaison de rôle.

1. Vous pouvez personnaliser l'autorisation en fonction de vos besoins.

Sauvegarde/restauration

Ajoutez une autorisation de base pour activer la sauvegarde et la restauration des clusters Kubernetes.

Remplacer l' `subjects: kind: variable` avec votre nom d'utilisateur et `subjects: name:` Avec l'ID objet pour l'identité gérée attribuée par le système ou le nom d'utilisateur de tout utilisateur autorisé, comme décrit ci-dessus.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - namespaces
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
```

```

resources:
  - storageclasses
verbs:
  - list
- apiGroups:
  - trident.netapp.io
resources:
  - tridentbackends
verbs:
  - list
  - watch
- apiGroups:
  - trident.netapp.io
resources:
  - tridentorchestrators
verbs:
  - get
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

Classes de stockage

Ajoutez une autorisation étendue pour ajouter des classes de stockage à l'aide de BlueXP.

Remplacer l' `subjects: kind: variable` avec votre nom d'utilisateur et `subjects: user:` Avec l'ID objet pour l'identité gérée attribuée par le système ou le nom d'utilisateur de tout utilisateur autorisé, comme décrit ci-dessus.

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
    - ''

```



```

resources:
  - secrets
  - namespaces
  - persistentvolumeclaims
  - persistentvolumes
  - pods
  - pods/exec
verbs:
  - get
  - list
  - watch
  - create
  - delete
  - watch
- apiGroups:
  - storage.k8s.io
  resources:
  - storageclasses
  verbs:
  - get
  - create
  - list
  - watch
  - delete
  - patch
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentbackends
  - tridentorchestrators
  - tridentbackendconfigs
  verbs:
  - get
  - list
  - watch
  - create
  - delete
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:

```

```
    apiGroup: rbac.authorization.k8s.io
  roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io
```

Installation de Trident

Utilisez la ligne de commande pour fournir une autorisation complète et permettre à BlueXP d'installer Astra Trident.

```
eksctl create iamidentitymapping --cluster < > --region < > --arn <
> --group "system:masters" --username
system:node:{{EC2PrivateDNSName}}
```

2. Appliquer la configuration à un cluster

```
kubectl apply -f <file-name>
```

Conditions requises pour les clusters Kubernetes dans Google Cloud

Vous pouvez ajouter et gérer des clusters Google Kubernetes Engine (GKE) gérés et des clusters Kubernetes autogérés dans Google à l'aide de BlueXP. Avant de pouvoir ajouter les clusters à BlueXP, assurez-vous que les conditions suivantes sont remplies.



Cette rubrique utilise *cluster Kubernetes* où la configuration est la même pour les clusters GKE et Kubernetes autogérés. Le type de cluster est spécifié où la configuration diffère.

De formation

Astra Trident

Il est nécessaire de disposer de l'une des quatre versions les plus récentes d'Astra Trident. Vous pouvez installer ou mettre à niveau Astra Trident directement à partir de BlueXP. Vous devriez ["passez en revue les prérequis"](#) Avant d'installer Astra Trident

Cloud Volumes ONTAP

Cloud Volumes ONTAP doit se trouver dans BlueXP, sous le même compte de location, espace de travail et connecteur que le cluster Kubernetes. ["Accédez à la documentation Astra Trident pour connaître les étapes de configuration"](#).

Connecteur BlueXP

Un connecteur doit être exécuté dans Google avec les autorisations requises. [Pour en savoir plus.](#)

Connectivité réseau

La connectivité réseau est requise entre le cluster Kubernetes et le connecteur et entre le cluster Kubernetes et Cloud Volumes ONTAP. [Pour en savoir plus.](#)

Autorisation RBAC

BlueXP prend en charge les clusters RBAC avec et sans Active Directory. Le rôle connecteur BlueXP doit être autorisé sur chaque cluster GKE. [Pour en savoir plus.](#)

Préparer un connecteur

BlueXP Connector dans Google est nécessaire pour découvrir et gérer les clusters Kubernetes. Vous devrez créer un nouveau connecteur ou utiliser un connecteur existant disposant des autorisations requises.

Créer un nouveau connecteur

Suivez les étapes de l'un des liens ci-dessous.

- ["Créez un connecteur depuis BlueXP"](#) (recommandé)
- ["Installez le connecteur sur un hôte Linux existant"](#)

Ajoutez les autorisations requises à un connecteur existant (pour découvrir un cluster GKE géré)

Si vous voulez détecter un cluster GKE géré, vous devrez peut-être modifier le rôle personnalisé du connecteur pour fournir les autorisations.

Étapes

1. Dans ["Console cloud"](#), Allez à la page **rôles**.
2. A l'aide de la liste déroulante située en haut de la page, sélectionnez le projet ou l'organisation qui contient le rôle que vous souhaitez modifier.
3. Cliquez sur un rôle personnalisé.
4. Cliquez sur **Modifier le rôle** pour mettre à jour les autorisations du rôle.
5. Cliquez sur **Ajouter des autorisations** pour ajouter les nouvelles autorisations suivantes au rôle.

```
container.clusters.get  
container.clusters.list
```

6. Cliquez sur **Update** pour enregistrer le rôle modifié.

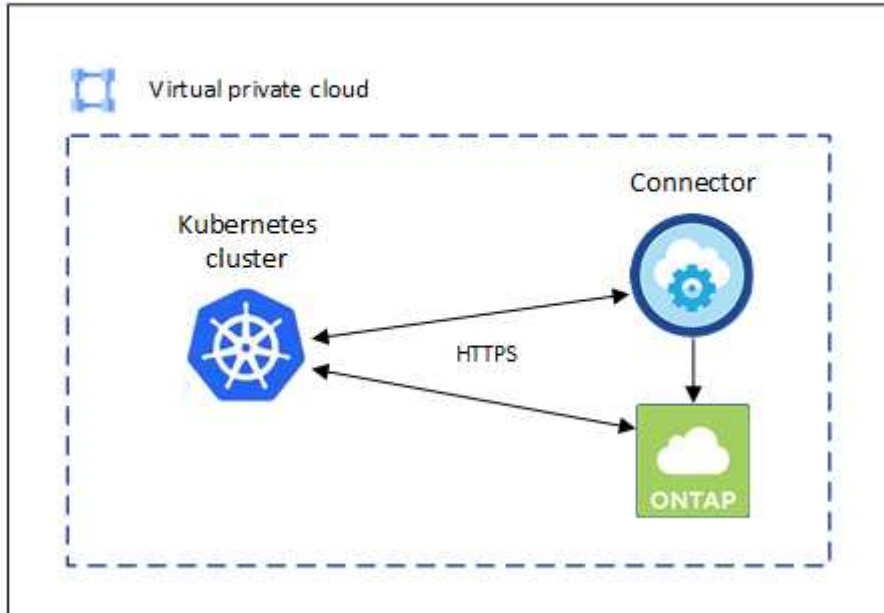
Examiner les besoins en matière de mise en réseau

Il faut assurer une connectivité réseau entre le cluster Kubernetes et le connecteur, et entre le cluster Kubernetes et le système Cloud Volumes ONTAP qui fournit un stockage back-end au cluster.

- Chaque cluster Kubernetes doit disposer d'une connexion entrante depuis le connecteur
- Le connecteur doit disposer d'une connexion sortante vers chaque cluster Kubernetes sur le port 443

Pour fournir cette connectivité, la méthode la plus simple est de déployer le connecteur et Cloud Volumes ONTAP dans le même VPC que le cluster Kubernetes. Sinon, vous devez configurer une connexion de peering entre les différents VPC.

Voici un exemple illustrant chaque composant dans le même VPC.



Configurez l'autorisation RBAC

La validation RBAC a lieu uniquement sur les clusters Kubernetes où Active Directory (AD) est activé. Les clusters Kubernetes sans AD passent automatiquement la validation.

Vous devez autoriser le rôle de connecteur sur chaque cluster Kubernetes afin que le connecteur puisse détecter et gérer un cluster.

Sauvegarde et restauration

La sauvegarde et la restauration ne nécessitent que l'autorisation de base.

Ajouter des classes de stockage

Une autorisation étendue est nécessaire pour ajouter des classes de stockage à l'aide de BlueXP et surveiller le cluster pour les modifications apportées au back-end.

Installer Astra trident

Vous devez fournir une autorisation complète pour BlueXP afin d'installer Astra Trident.



Pour installer Astra Trident, BlueXP installe le système back-end Trident et le secret Kubernetes qui contient les identifiants Astra Trident qui doit communiquer avec le cluster de stockage.

Avant de commencer

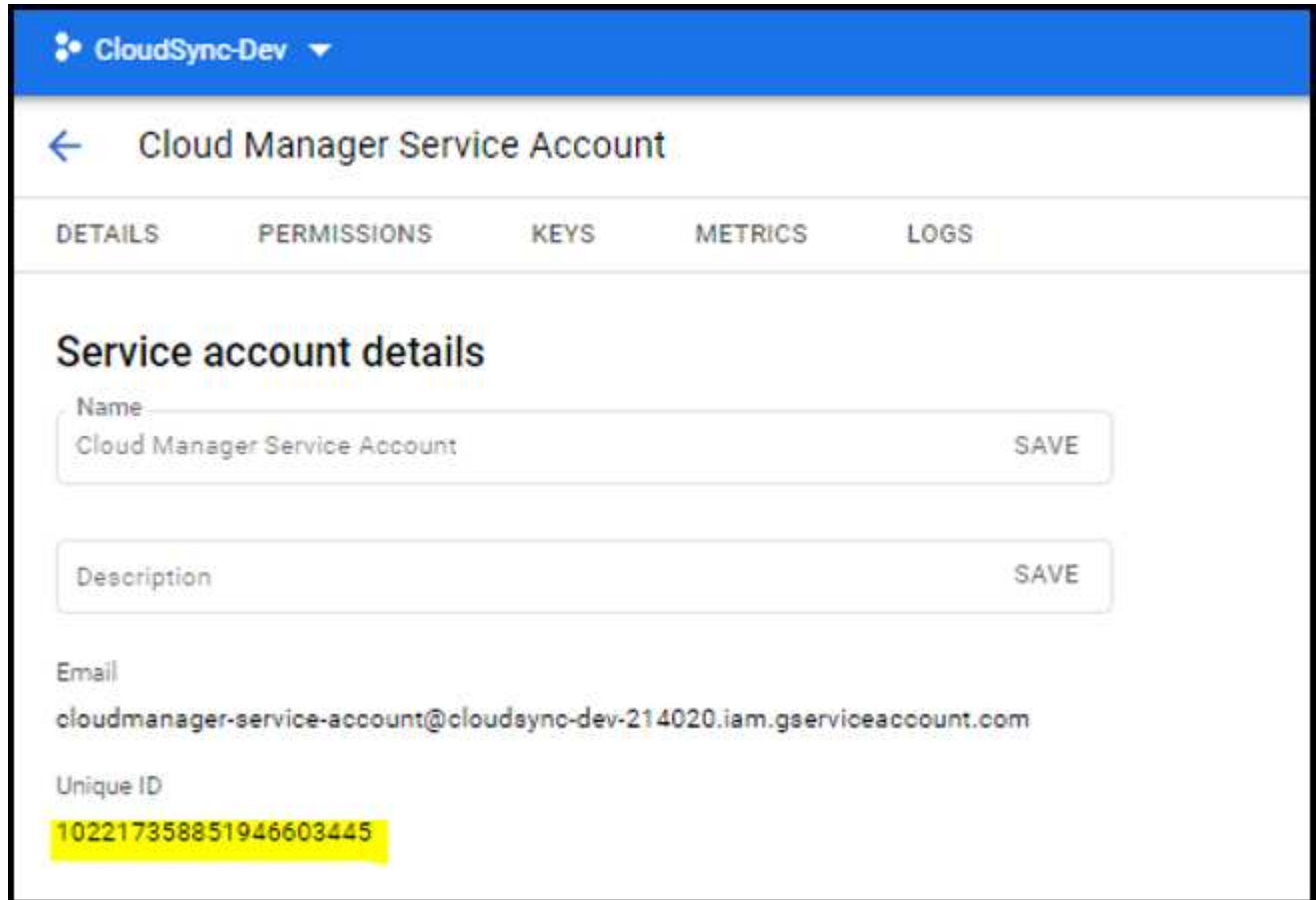
À configurer `subjects: name:` Dans le fichier YAML, vous devez connaître l'ID unique BlueXP.

Vous pouvez trouver l'ID unique de deux façons :

- À l'aide de la commande :

```
gcloud iam service-accounts list
gcloud iam service-accounts describe <service-account-email>
```

- Dans le champ Détails du compte de service du "Console cloud".



CloudSync-Dev ▼

← Cloud Manager Service Account

DETAILS PERMISSIONS KEYS METRICS LOGS

Service account details

Name
Cloud Manager Service Account SAVE

Description SAVE

Email
cloudmanager-service-account@cloudsync-dev-214020.iam.gserviceaccount.com

Unique ID
102217358851946603445

Étapes

Créer un rôle de cluster et une liaison de rôle.

1. Vous pouvez personnaliser l'autorisation en fonction de vos besoins.

Sauvegarde/restauration

Ajoutez une autorisation de base pour activer la sauvegarde et la restauration des clusters Kubernetes.

Remplacer l' `subjects: kind: variable` avec votre nom d'utilisateur et `subjects: name:` Avec l'identifiant unique du compte de service autorisé.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - namespaces
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
```

```

resources:
  - storageclasses
verbs:
  - list
- apiGroups:
  - trident.netapp.io
resources:
  - tridentbackends
verbs:
  - list
  - watch
- apiGroups:
  - trident.netapp.io
resources:
  - tridentorchestrators
verbs:
  - get
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

Classes de stockage

Ajoutez une autorisation étendue pour ajouter des classes de stockage à l'aide de BlueXP.

Remplacer l' `subjects: kind: variable` avec votre nom d'utilisateur et `subjects: user:` Avec l'identifiant unique du compte de service autorisé.

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
    - ''
    resources:

```

```

      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - create
      - list
      - watch
      - delete
      - patch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
      - tridentbackendconfigs
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name:
    apiGroup: rbac.authorization.k8s.io

```



```
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io
```

Installation de Trident

Utilisez la ligne de commande pour fournir une autorisation complète et permettre à BlueXP d'installer Astra Trident.

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Unique ID>
```

2. Appliquer la configuration à un cluster

```
kubectl apply -f <file-name>
```

Conditions requises pour les clusters Kubernetes dans OpenShift

Vous pouvez ajouter et gérer des clusters OpenShift Kubernetes autogérés avec BlueXP. Avant de pouvoir ajouter les clusters à BlueXP, assurez-vous que les conditions suivantes sont remplies.

De formation

Astra Trident

Il est nécessaire de disposer de l'une des quatre versions les plus récentes d'Astra Trident. Vous pouvez installer ou mettre à niveau Astra Trident directement à partir de BlueXP. Vous devriez ["passez en revue les prérequis"](#) Avant d'installer Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP doit être configuré en tant que système de stockage back-end pour le cluster. ["Accédez à la documentation Astra Trident pour connaître les étapes de configuration"](#).

Connecteur BlueXP

BlueXP Connector est nécessaire pour l'importation et la gestion des clusters Kubernetes. Vous devrez créer un nouveau connecteur ou utiliser un connecteur existant possédant les autorisations requises pour votre fournisseur de cloud :

- ["Connecteur AWS"](#)
- ["Connecteur Azure"](#)
- ["Google Cloud Connector"](#)

Connectivité réseau

La connectivité réseau est requise entre le cluster Kubernetes et le connecteur et entre le cluster Kubernetes et Cloud Volumes ONTAP.

Fichier de configuration Kubernetes (kubeconfig) avec autorisation RBAC

Pour importer des clusters OpenShift, il vous faut un fichier kubeconfig avec l'autorisation RBAC requise pour activer différentes fonctionnalités. [Créez un fichier kubeconfig](#).

- Sauvegarde et restauration : la sauvegarde et la restauration ne nécessitent qu'une autorisation de base.
- Ajout de classes de stockage : une autorisation étendue est nécessaire pour ajouter des classes de stockage à l'aide de BlueXP et surveiller le cluster pour les modifications apportées au back-end.
- Installer Astra Trident : vous devez fournir une autorisation complète pour BlueXP afin d'installer Astra Trident.



Pour installer Astra Trident, BlueXP installe le système back-end Trident et le secret Kubernetes qui contient les identifiants Astra Trident qui doit communiquer avec le cluster de stockage.

Créez un fichier kubeconfig

Créez un fichier kubeconfig à importer dans BlueXP à l'aide de l'interface de ligne de commande OpenShift.

Étapes

1. Connectez-vous à l'interface de ligne de commande OpenShift via `oc login` Sur une URL publique avec un utilisateur administratif.
2. Créer un compte de service comme suit :

- a. Créez un fichier de compte de service appelé `oc-service-account.yaml`.

Ajustez le nom et l'espace de noms selon vos besoins. Si des modifications sont apportées ici, vous devez appliquer les mêmes modifications dans les étapes suivantes.

```
oc-service-account.yaml
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: oc-service-account
  namespace: default
```

- a. Appliquer le compte de service :

```
kubectl apply -f oc-service-account.yaml
```

3. Créez un lien de rôle personnalisé en fonction de vos exigences d'autorisation.

a. Créer un ClusterRoleBinding fichier appelé oc-clusterrolebinding.yaml.

```
oc-clusterrolebinding.yaml
```

b. Configurez l'autorisation RBAC selon les besoins pour le cluster.

Sauvegarde/restauration

Ajoutez une autorisation de base pour activer la sauvegarde et la restauration des clusters Kubernetes.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - namespaces
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
```

```

      - list
- apiGroups:
  - trident.netapp.io
  resources:
    - tridentbackends
  verbs:
    - list
    - watch
- apiGroups:
  - trident.netapp.io
  resources:
    - tridentorchestrators
  verbs:
    - get
    - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
subjects:
  - kind: ServiceAccount
    name: oc-service-account
    namespace: default

```

Classes de stockage

Ajoutez une autorisation étendue pour ajouter des classes de stockage à l'aide de BlueXP.

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
    - ''
    resources:
      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
      - pods

```

```

      - pods/exec
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - create
      - list
      - watch
      - delete
      - patch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
      - tridentbackendconfigs
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
subjects:
  - kind: ServiceAccount
    name: oc-service-account
    namespace: default

```

Installation de Trident

Accordez l'autorisation d'administration complète et permettez à BlueXP d'installer Astra Trident.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cloudmanager-access-clusterrole
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: oc-service-account
  namespace: default
```

c. Appliquer la liaison de rôle de cluster :

```
kubectl apply -f oc-clusterrolebinding.yaml
```

4. Indiquez les secrets du compte de service, en les remplaçant <context> avec le contexte approprié pour votre installation :

```
kubectl get serviceaccount oc-service-account --context <context>
--namespace default -o json
```

La fin de la sortie doit ressembler à ce qui suit :

```
"secrets": [
{ "name": "oc-service-account-dockercfg-vhz87"},
{ "name": "oc-service-account-token-r59kr"}
]
```

Les indices pour chaque élément dans secrets la matrice commence par 0. Dans l'exemple ci-dessus, l'index de oc-service-account-dockercfg-vhz87 serait 0 et l'index pour oc-service-account-token-r59kr serait 1. Dans votre résultat, notez l'index du nom du compte de service qui contient le mot "jeton".

5. Générez le kubeconfig comme suit :

- Créer un create-kubeconfig.sh fichier. Remplacement TOKEN_INDEX au début du script suivant avec la valeur correcte.

create-kubeconfig.sh

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=oc-service-account
NAMESPACE=default
NEW_CONTEXT=oc
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```



```

set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
--token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp

```

b. Source des commandes à appliquer à votre cluster Kubernetes.

```
source create-kubeconfig.sh
```

Résultat

Vous utiliserez le résultat kubeconfig-sa Fichier pour ajouter un cluster OpenShift à BlueXP.

Ajouter des clusters Kubernetes

Ajouter un cluster Amazon Kubernetes à BlueXP

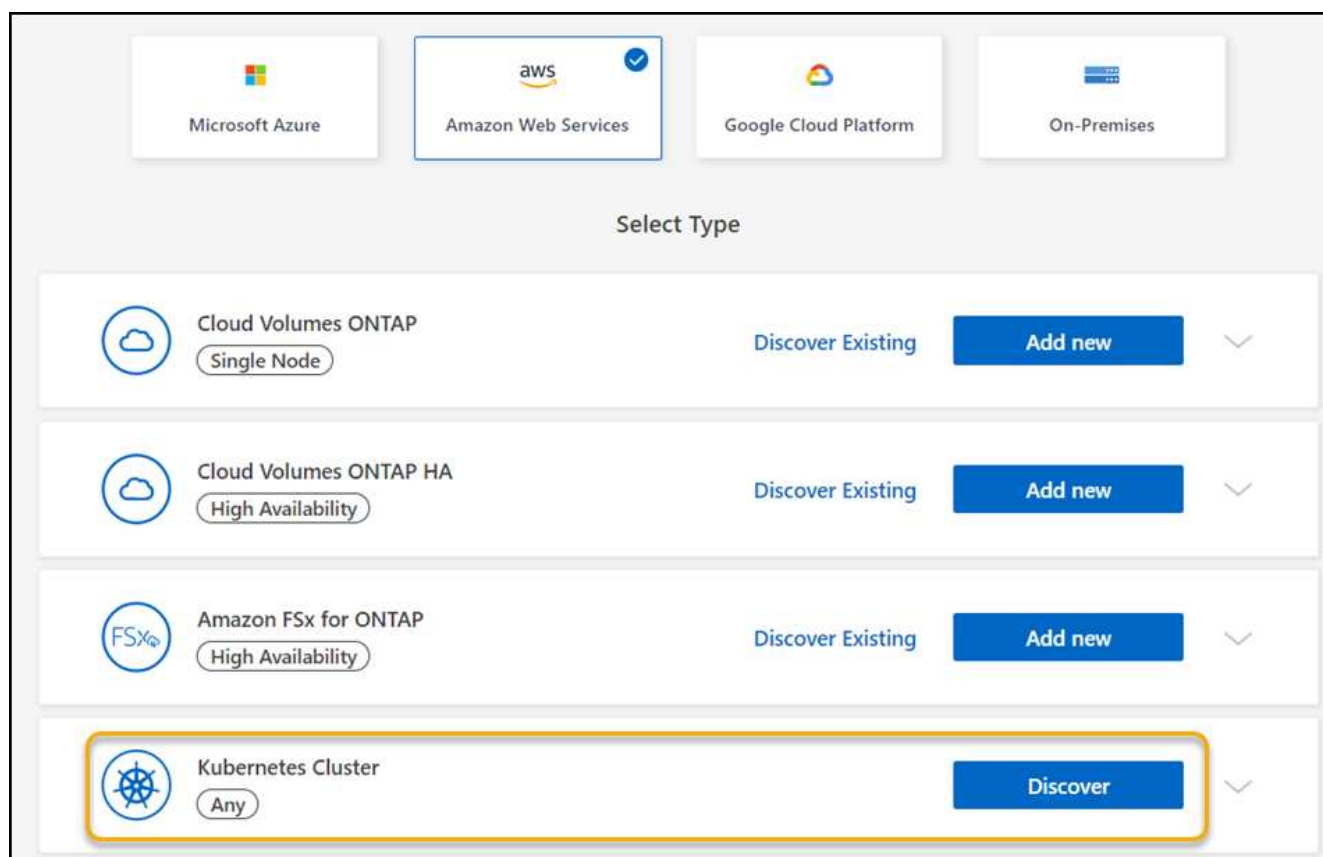
Vous pouvez détecter ou importer des clusters Kubernetes vers BlueXP, et ainsi sauvegarder des volumes persistants sur Amazon S3.

Découvrir un cluster

Vous pouvez détecter un cluster Kubernetes entièrement géré ou autogéré. Les clusters gérés doivent être découverts ; ils ne peuvent pas être importés.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Amazon Web Services > Kubernetes Cluster > Discover**.



3. Sélectionnez **Discover Cluster** et cliquez sur **Next**.
4. Choisissez une région AWS, sélectionnez un cluster Kubernetes, puis cliquez sur **Suivant**.



Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.

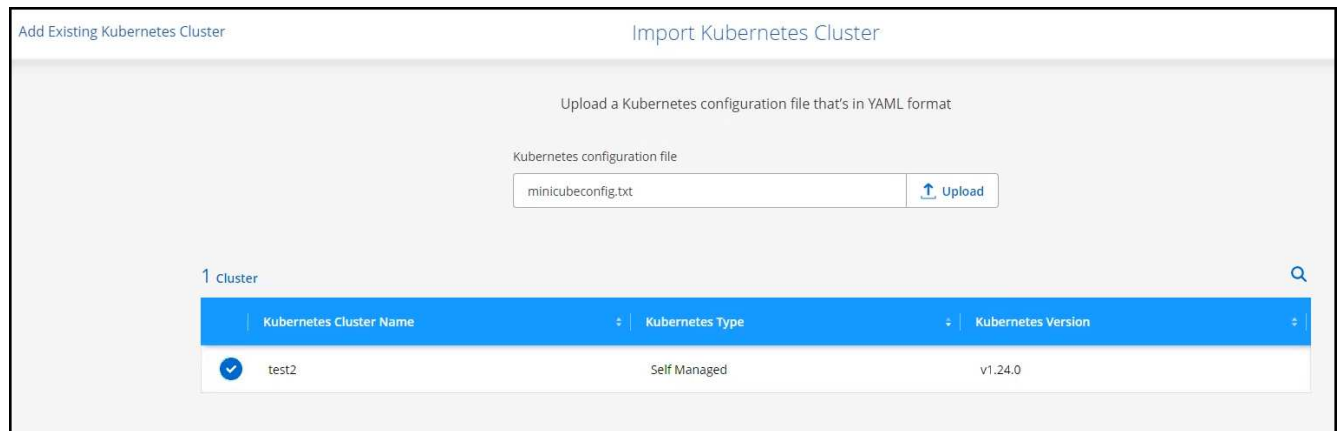


Importer un cluster

Vous pouvez importer un cluster Kubernetes autogéré à l'aide d'un fichier de configuration Kubernetes.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Amazon Web Services > Kubernetes Cluster > Discover**.
3. Sélectionnez **Import Cluster** et cliquez sur **Suivant**.
4. Téléchargez un fichier de configuration Kubernetes au format YAML.



5. Sélectionnez le cluster Kubernetes et cliquez sur **Next** (Suivant).

Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.

Ajout d'un cluster Azure Kubernetes à BlueXP

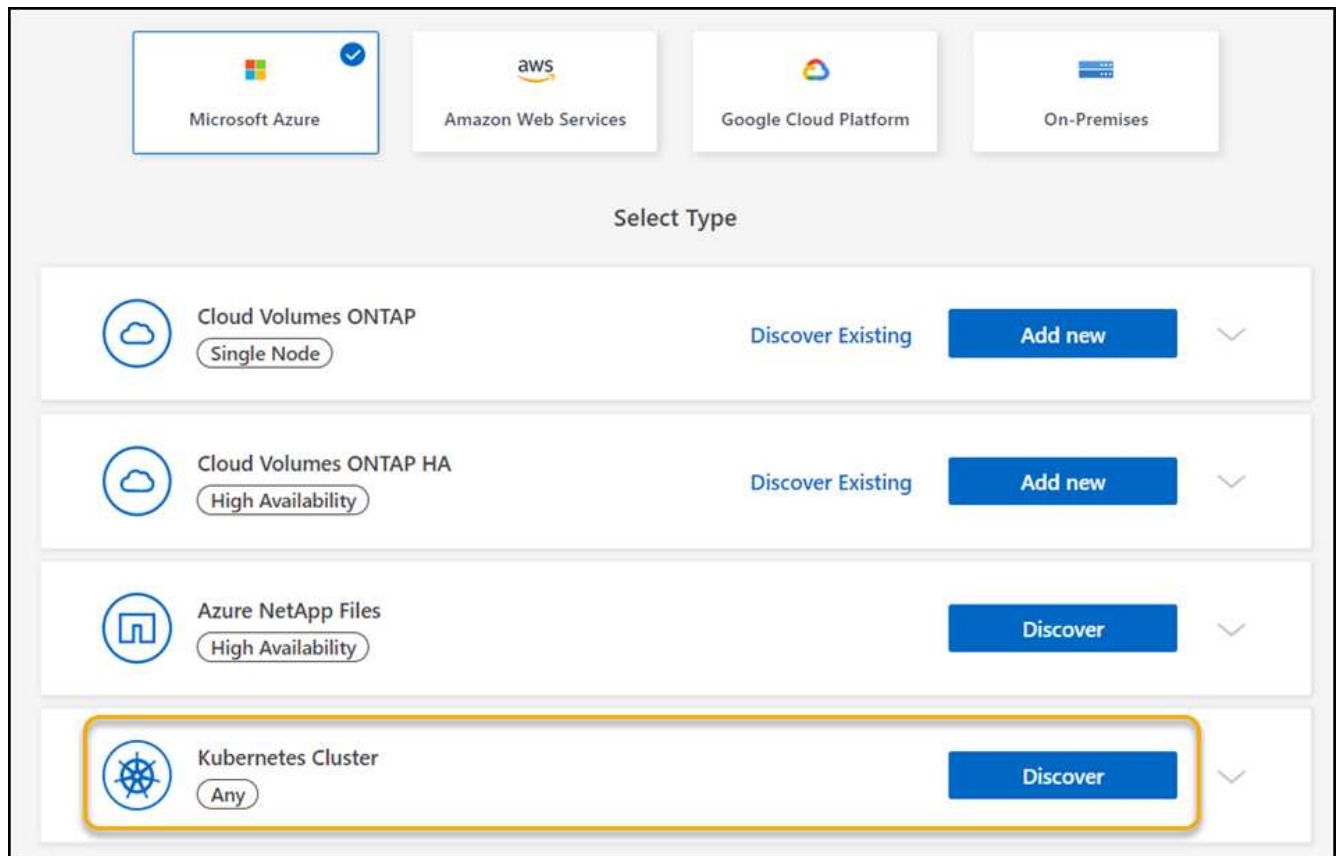
Vous pouvez détecter ou importer des clusters Kubernetes vers BlueXP, pour que vous puissiez sauvegarder des volumes persistants sur Azure.

Découvrir un cluster

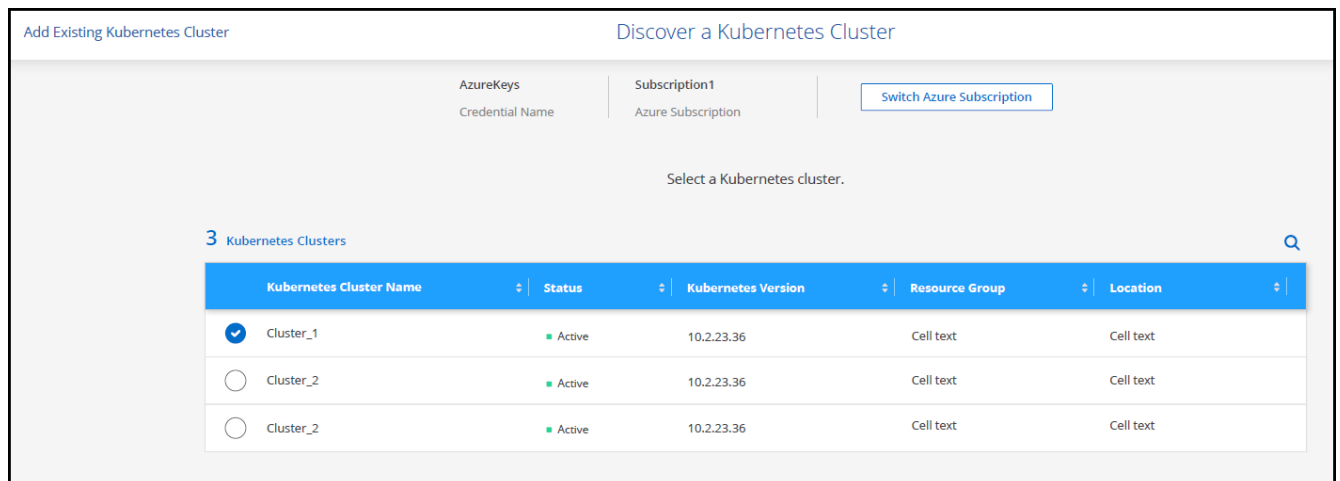
Vous pouvez détecter un cluster Kubernetes entièrement géré ou autogéré. Les clusters gérés doivent être découverts ; ils ne peuvent pas être importés.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Microsoft Azure > Cluster Kubernetes > découvrir**.

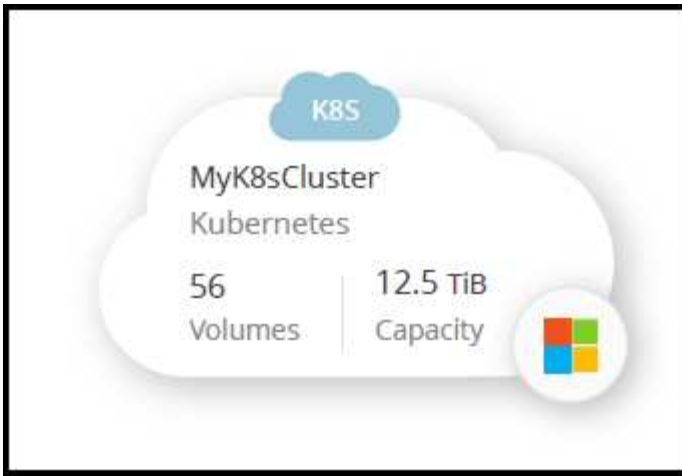


3. Sélectionnez **Discover Cluster** et cliquez sur **Next**.
4. Sélectionnez un cluster Kubernetes et cliquez sur **Suivant**.



Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.



Importer un cluster

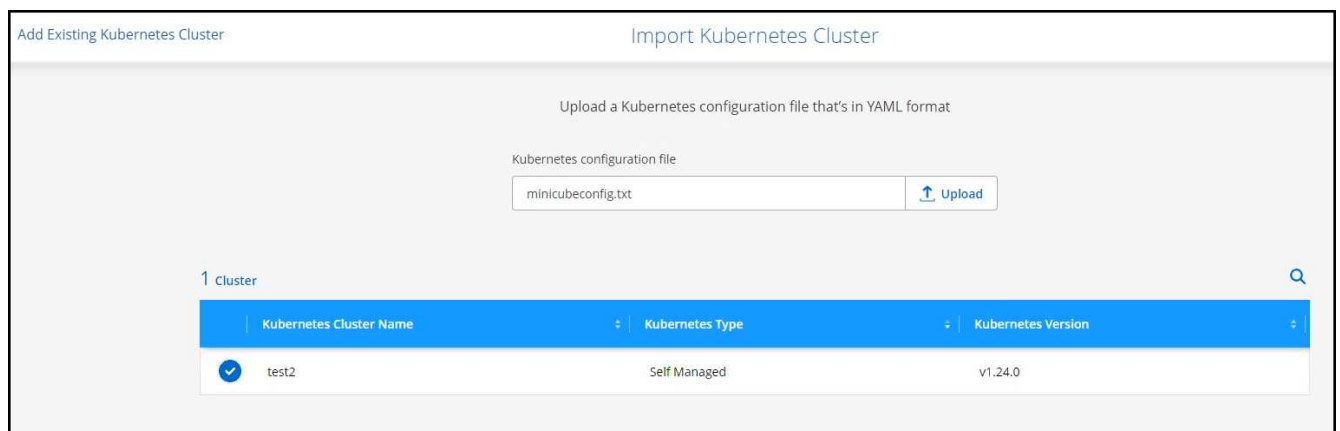
Vous pouvez importer un cluster Kubernetes autogéré à l'aide d'un fichier de configuration Kubernetes.

Avant de commencer

Vous aurez besoin de certificats d'autorité de certification, de clé client et de certificat client pour l'utilisateur spécifié dans le fichier YAML du rôle de cluster pour importer les clusters Kubernetes. L'administrateur du cluster Kubernetes reçoit ces certifications lors de la création d'utilisateurs sur le cluster Kubernetes.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Microsoft Azure > Cluster Kubernetes > découvrir**.
3. Sélectionnez **Import Cluster** et cliquez sur **Suivant**.
4. Téléchargez un fichier de configuration Kubernetes au format YAML.



5. Téléchargez les certificats de cluster fournis par l'administrateur de cluster Kubernetes.

Upload Cluster Certificates

To complete the import, upload the following cluster certificates. ⓘ

Certificate Authority

No file selected

Client Key

No file selected

Client Certificate

No file selected

Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.

Ajouter un cluster Google Cloud Kubernetes à BlueXP

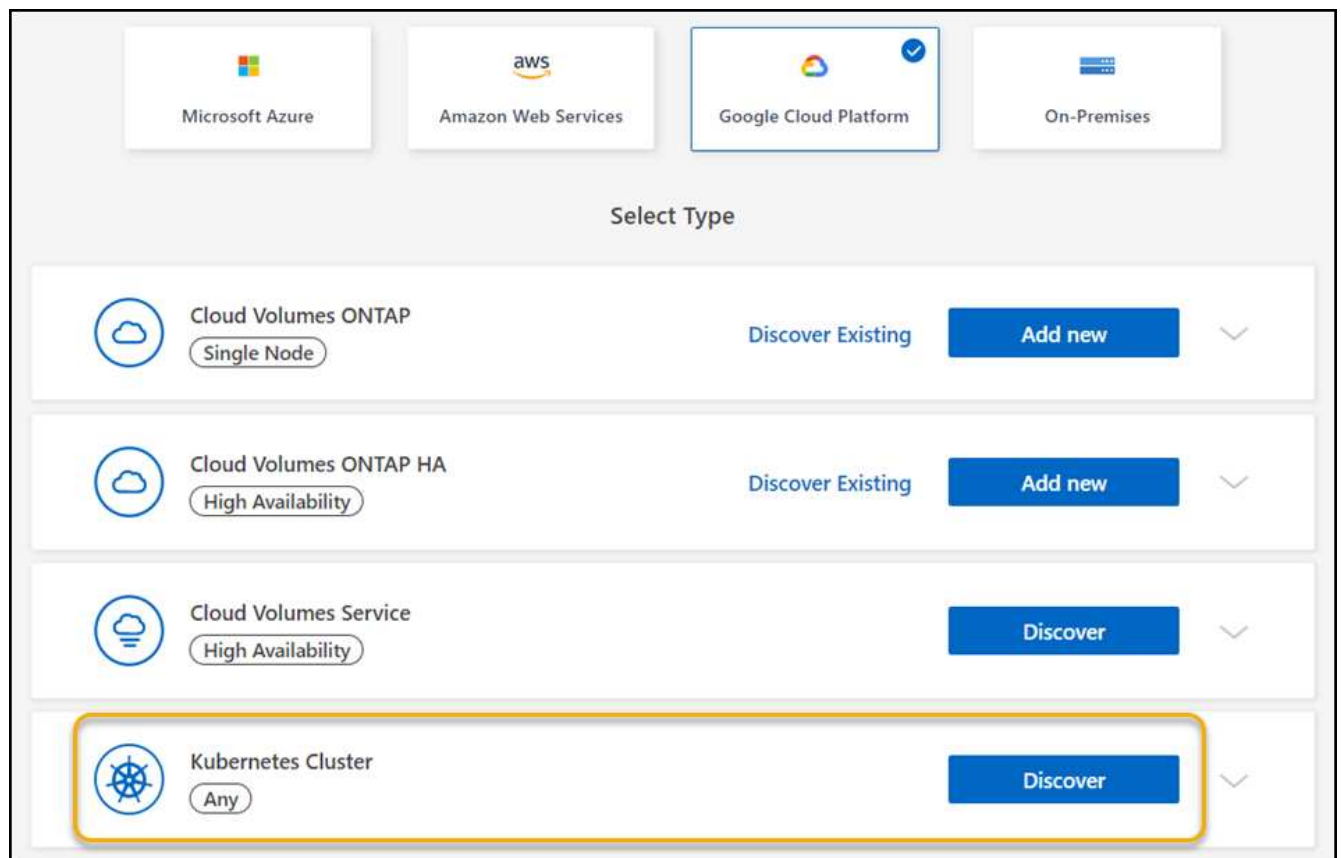
Vous pouvez découvrir ou importer des clusters Kubernetes vers BlueXP, pour sauvegarder des volumes persistants dans Google Cloud.

Découvrir un cluster

Vous pouvez détecter un cluster Kubernetes entièrement géré ou autogéré. Les clusters gérés doivent être découverts ; ils ne peuvent pas être importés.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Google Cloud Platform > Kubernetes Cluster > Discover**.



3. Sélectionnez **Discover Cluster** et cliquez sur **Next**.
4. Pour sélectionner un cluster Kubernetes dans un autre projet Google Cloud, cliquez sur **Modifier le projet** et choisissez un projet disponible.

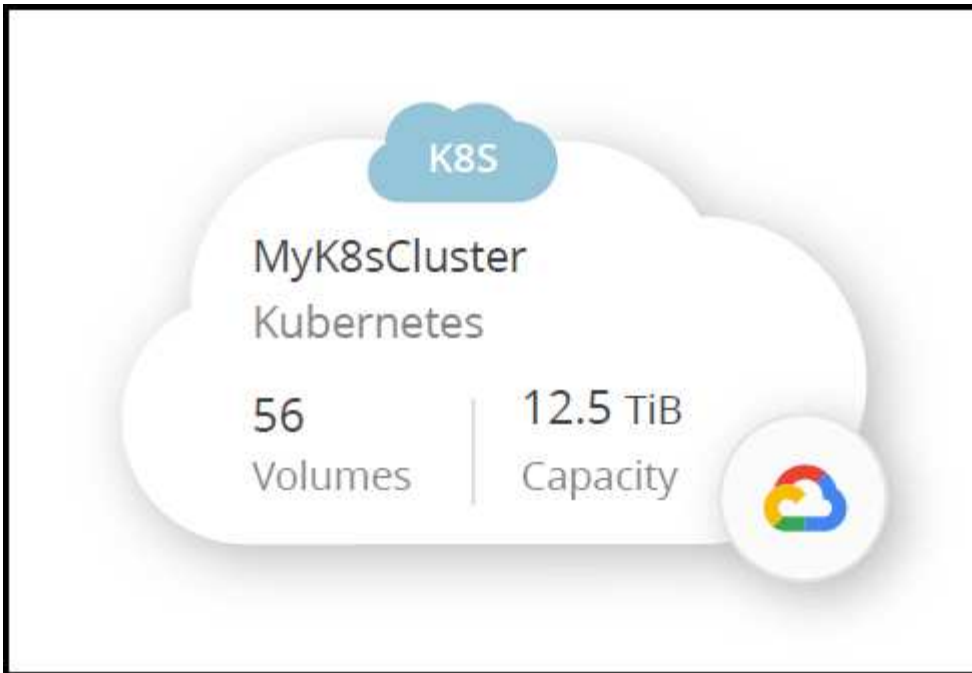


5. Sélectionnez un cluster Kubernetes et cliquez sur **Suivant**.



Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.



Importer un cluster

Vous pouvez importer un cluster Kubernetes autogéré à l'aide d'un fichier de configuration Kubernetes.

Avant de commencer

Vous aurez besoin de certificats d'autorité de certification, de clé client et de certificat client pour l'utilisateur spécifié dans le fichier YAML du rôle de cluster pour importer les clusters Kubernetes. L'administrateur du cluster Kubernetes reçoit ces certifications lors de la création d'utilisateurs sur le cluster Kubernetes.

Étapes

1. Dans **Canvas**, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Google Cloud Platform > Kubernetes Cluster > Discover**.
3. Sélectionnez **Import Cluster** et cliquez sur **Suivant**.
4. Téléchargez un fichier de configuration Kubernetes au format YAML.

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format and has the extension ".txt", ".kubeconfig", or ".config"

Kubernetes configuration file

KubConfig.txt

Upload

3 Kubernetes Clusters

Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
<input checked="" type="radio"/> Cluster_1	???	10.2.23.36
<input type="radio"/> Cluster_2	???	10.2.23.36
<input type="radio"/> Cluster_2	???	10.2.23.36

Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.

Importez un cluster OpenShift vers BlueXP

Importez un cluster OpenShift autogéré vers BlueXP, afin que vous puissiez commencer à sauvegarder les volumes persistants sur votre fournisseur de cloud.

Importer un cluster

Vous pouvez importer un cluster Kubernetes autogéré à l'aide d'un fichier de configuration Kubernetes.

Avant de commencer

Avant d'importer un cluster OpenShift, vous avez besoin des éléments suivants :

- Le fichier `kubeconfig-sa` que vous avez créé dans ["créez un fichier kubeconfig"](#).
- Les fichiers public Certificate Authority (par exemple, CA.crt), client Key (par exemple, tls.key) et client Certification (par exemple, tls.crt) pour le cluster.

Étapes

1. Dans **Canvas**, sélectionnez **Ajouter un environnement de travail**.
2. Sélectionnez votre fournisseur de cloud et sélectionnez **Kubernetes Cluster > Discover**.
3. Sélectionnez **Import Cluster** puis **Suivant**.
4. Téléchargez le kubeconfig-sa fichier créé dans ["créez un fichier kubeconfig"](#). Sélectionnez le cluster Kubernetes et sélectionnez **Suivant**.

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file

minicubeconfig.txt Upload

1 Cluster

Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
test2	Self Managed	v1.24.0

5. Télécharger les certificats de cluster.

Upload Cluster Certificates

To complete the import, upload the following cluster certificates. ⓘ

Certificate Authority

No file selected

Client Key

No file selected

Client Certificate

No file selected

Résultat

BlueXP ajoute le cluster Kubernetes à Canvas.

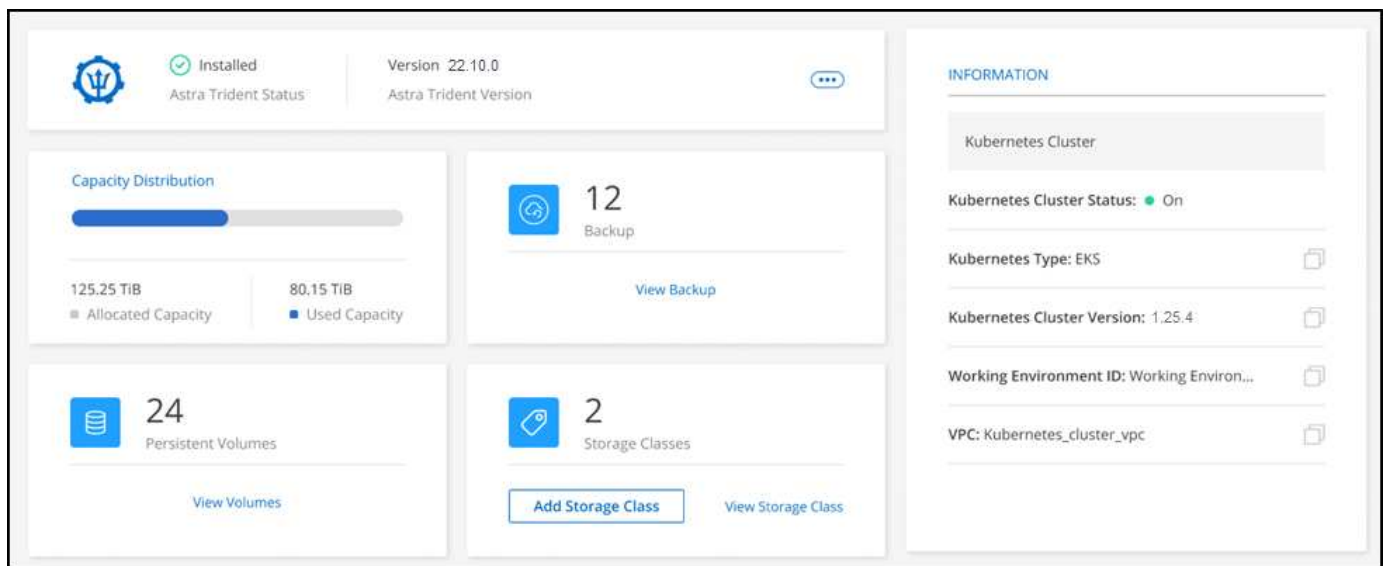
Gérez les clusters Kubernetes

Gérez Astra Trident

Une fois que vous avez ajouté un cluster Kubernetes géré à la toile, vous pouvez utiliser BlueXP pour confirmer une installation Astra Trident compatible, installer ou mettre à niveau Astra Trident vers la dernière version, ou désinstaller Astra Trident.

ASTRA Trident avec BlueXP

Après avoir ajouté des clusters Kubernetes à BlueXP, vous pouvez gérer Astra Trident et vos clusters Kubernetes à partir de la page de présentation. Pour ouvrir la page de présentation, double-cliquez sur l'environnement de travail Kubernetes sur la toile.



Versions d'Astra Trident prises en charge

L'une des quatre versions les plus récentes d'Astra Trident déployée avec l'opérateur Trident, soit manuellement ou à l'aide du graphique Helm, est requise. Si Astra Trident n'est pas installé ou qu'une version incompatible d'Astra Trident est installée, le cluster indique qu'une action est requise.



Astra Trident déployé avec `tridentctl` n'est pas pris en charge. Si vous avez déployé Astra Trident avec `tridentctl`, Vous ne pouvez pas utiliser BlueXP pour gérer vos clusters Kubernetes ni désinstaller Astra Trident. Vous devez Et réinstallez Astra Trident manuellement à l'aide de "[Opérateur Trident](#)" Ou dans BlueXP à l'aide de [Installer ou mettre à niveau Astra Trident](#).

Pour en savoir plus sur Astra Trident, rendez-vous sur "[Documentation Astra Trident](#)".

Installer ou mettre à niveau Astra Trident

Vous pouvez consulter le statut et la version de votre installation d'Astra Trident sur la page de présentation. Si Astra Trident n'est pas déjà installé ou si une version incompatible est installée, vous pouvez gérer cet élément à l'aide de BlueXP.

Étapes

1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
 - a. Si Astra Trident n'est pas installé, cliquez sur **installer Trident**.

1 | Install Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

Install Trident

- b. Si une version non prise en charge d'Astra Trident est installée, cliquez sur **Upgrade Trident**.

Upgrade Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

Upgrade Trident



Vous ne pouvez pas utiliser BlueXP pour la mise à niveau à partir de versions d'Astra Trident antérieures à la version 21.01. Pour effectuer une mise à niveau à partir d'une version antérieure, reportez-vous à la section "[Mise à niveau avec l'opérateur](#)".

Résultats

La dernière version d'Astra Trident est installée. Vous pouvez à présent ajouter des classes de stockage.

Désinstaller Astra Trident

Si vous avez installé Astra Trident à l'aide de BlueXP ou de l'opérateur Trident (Helm ou manuellement), vous pouvez le désinstaller à l'aide de BlueXP.



- Après la désinstallation d'Astra Trident, vous ne pouvez pas créer de volumes persistants, mais des volumes existants sont toujours disponibles.
- Pendant la désinstallation d'Astra Trident, la sauvegarde n'est pas disponible.
- Vous pouvez à tout moment réinstaller Astra Trident sur l'environnement de travail pour continuer à gérer les clusters.

La désinstallation d'Astra Trident à l'aide de BlueXP ne supprime pas tous les services Astra Trident appliqués lors de l'installation. Pour supprimer complètement Astra Trident, y compris toutes les définitions de ressources personnalisées (CRD) qu'il crée, reportez-vous à la section "[Désinstallez à l'aide de l'opérateur Trident](#)".

Étapes

1. Dans la page de présentation, sélectionnez les points de suspension et **Uninstall Astra Trident**.



2. Sélectionnez **Désinstaller** pour confirmer et désinstaller Astra Trident.

Résultats

ASTRA Trident est maintenant désinstallé de l'environnement de travail. Vous pouvez réinstaller Astra Trident à tout moment.

Gérer les classes de stockage

Une fois que vous avez ajouté un cluster Kubernetes géré à Canvas, vous pouvez utiliser BlueXP pour gérer les classes de stockage.



Si aucune classe de stockage n'est définie, le cluster indique qu'une action est requise. Double-cliquez sur le cluster dans Canvas pour ouvrir la page d'action permettant d'ajouter une classe de stockage.

Ajouter une classe de stockage

Étapes

1. Dans la fenêtre Canvas, glissez-déposez l'environnement de travail Kubernetes sur l'environnement de travail Cloud Volumes ONTAP ou Amazon FSX pour ONTAP pour ouvrir l'assistant de classe de stockage.
2. Indiquez un nom pour la classe de stockage.
3. Sélectionnez **Filesystem** ou **Block** Storage.
 - a. Pour le stockage **Block**, sélectionnez un type de système de fichiers (fstype)

Storage Class Name

-cm

☐ Filesystem
 ☒ Block

Storage Class

Select File System Type

ext4

ext4

ext3

xfs

Storage Class Economy ⓘ

Support Volume Expansion

☒ Yes ☐ No

Volume Binding Mode

☒ Immediate ☐ WaitForFirstConsumer

Set as Default Storage Class

☒ Yes ☐ No

- b. Pour le stockage **Block** ou **Filesystem**, vous pouvez sélectionner pour activer l'économie de classe de stockage.

Storage Class

☒ Filesystem ☐ Block

Storage Class Economy ⓘ ☒ Enable Economy for Storage Class

Support Volume Expansion

☒ Yes ☐ No

Volume Binding Mode

☒ Immediate ☐ WaitForFirstConsumer

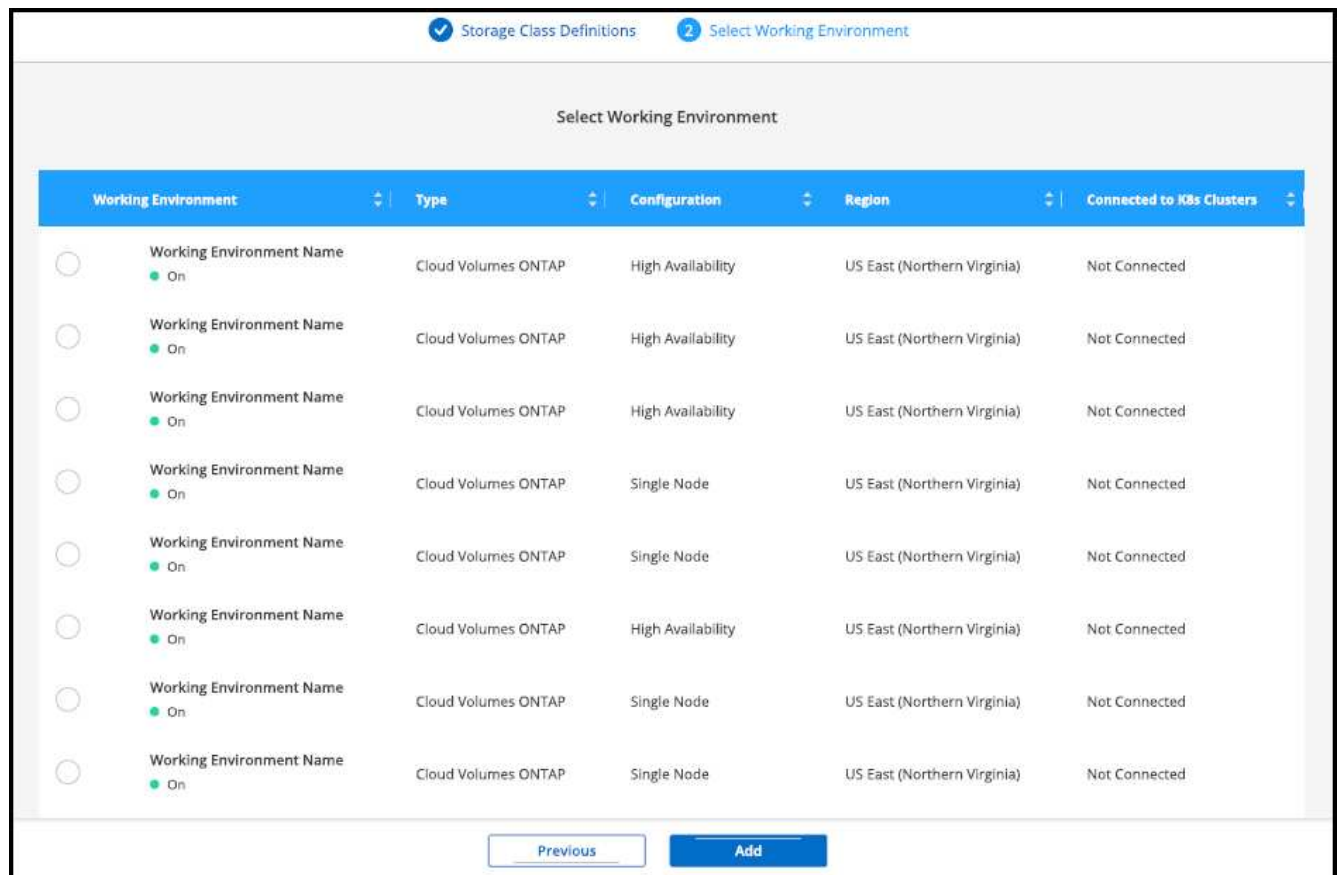
Set as Default Storage Class

☒ Yes ☐ No



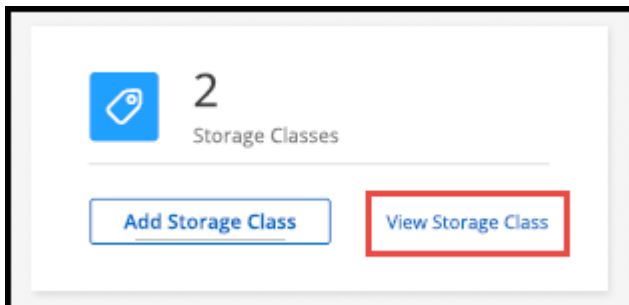
La sauvegarde et la restauration ne sont pas prises en charge dans le cas d'économies de la classe de stockage.

- Sélectionnez les options d'extension de volume, de liaison de volume et de classe de stockage par défaut. Cliquez sur **Suivant**.
- Sélectionnez un environnement de travail à connecter au cluster. Cliquez sur **Ajouter**.



Résultats

Vous pouvez cliquer sur  pour afficher la classe de stockage depuis la page de ressources du cluster Kubernetes.



Afficher les détails de l'environnement de travail

Étapes



1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
2. Cliquez sur l'onglet **classes de stockage**.
3. Cliquez sur l'icône d'information pour afficher les détails de l'environnement de travail.

Résultats


Le panneau de détails de l'environnement de travail s'ouvre.

2 Storage Classes
Add Storage Classes

Storage Class Name #1
ID: 01234567890123456789 ☆ Default Storage Class

 csi.trident.netapp.com Provisioner Name	Nas Storage Class Type (Driver)	WaitForFirstConsumer Volume Binding Mode	True Volume Expansion	 Working Environment Name Type: Cloud Volumes ONTAP Node: High Availability Provider: AWS Status : ON Region: US East (Northern Virginia)
--	------------------------------------	---	--------------------------	---

Storage Class Name #1
ID: 01234567890123456789

 csi.trident.netapp.com Provisioner Name	Nas Storage Class Type (Driver)	WaitForFirstConsumer Volume Binding Mode	True Volume Expansion	
--	------------------------------------	---	--------------------------	--

Définir la classe de stockage par défaut

Étapes



1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
2. Cliquez sur l'onglet **classes de stockage**.
3. Cliquez sur le menu d'action de la classe de stockage et cliquez sur **définir comme valeur par défaut**.



Résultats

La classe de stockage sélectionnée est définie par défaut.

Storage Class Name #2
ID: 01234567890123456789 ☆ Default Storage Class

 csi.trident.netapp.com Provisioner Name	Nas Storage Class Type (Driver)	WaitForFirstConsumer Volume Binding Mode	True Volume Expansion	 Working Environment Name Attached Working Environment
--	------------------------------------	---	--------------------------	--

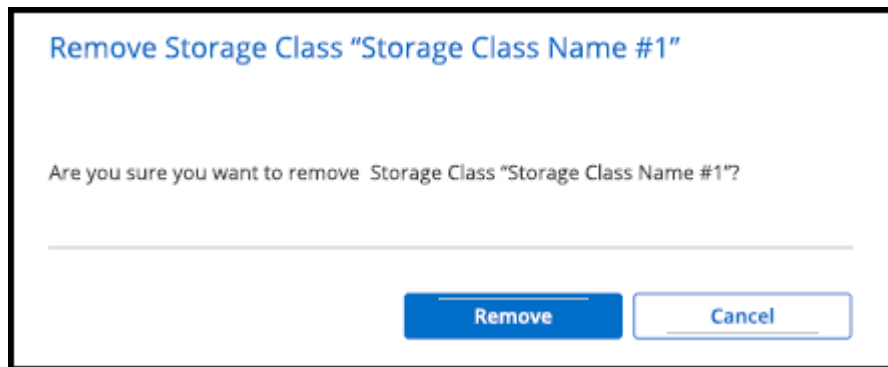
Supprimer la classe de stockage

Étapes

1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
2. Cliquez sur l'onglet **classes de stockage**.
3. Cliquez sur le menu d'action de la classe de stockage et cliquez sur **définir comme valeur par défaut**.



4. Cliquez sur **Supprimer** pour confirmer la suppression de la classe de stockage.



Résultats

La classe de stockage sélectionnée est supprimée.

Afficher les volumes persistants

Une fois que vous avez ajouté un cluster Kubernetes géré dans Canvas, vous pouvez utiliser BlueXP pour afficher les volumes persistants.



BlueXP surveille le cluster Kubernetes pour détecter les modifications apportées au back-end et met à jour la table des volumes persistants lorsque de nouveaux volumes sont ajoutés. Si la sauvegarde automatique était configurée sur le cluster, la sauvegarde est automatiquement activée sur les nouveaux volumes persistants.

Étapes

1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
2. Cliquez sur **Afficher les volumes** dans l'onglet **Présentation** ou cliquez sur l'onglet **volumes persistants**.
Si aucun volume persistant n'est configuré, voir "[Provisionnement](#)" Pour en savoir plus sur le provisionnement des volumes dans Astra Trident.

Résultats

Un tableau des volumes persistants configurés s'affiche.

Volumes Summary

8

Total Volumes

400

GiB

Total Allocated Capacity

201.2

GiB

Total Used Capacity

8 Volumes

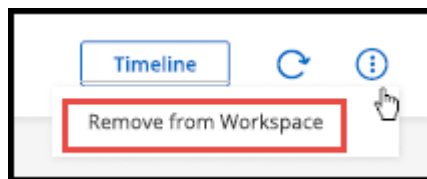
Volume Name	Name Space	Storage Class	Access Mode	Allocated Capacity	Used Capacity
<div>Volumes Very Long Name</div> <div>● On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB
<div>Volumes Very Long Name</div> <div>● On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB

Supprimez les clusters Kubernetes de l'espace de travail

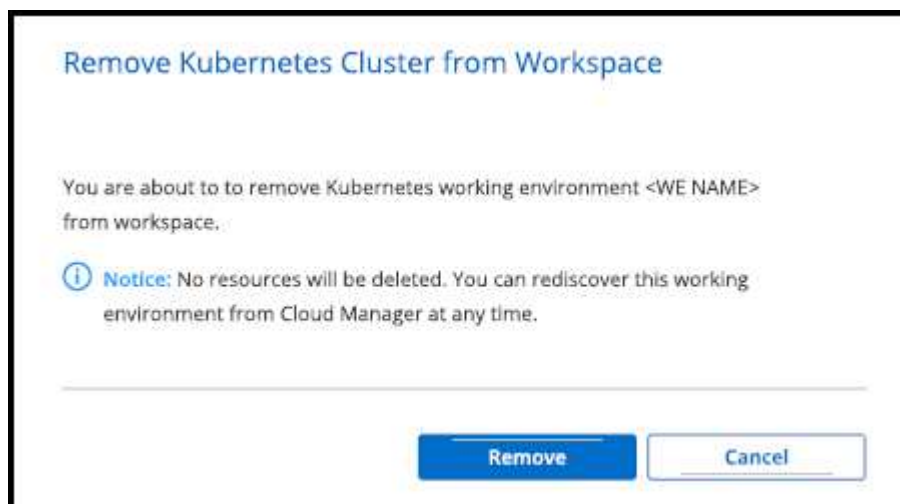
Une fois que vous avez ajouté un cluster Kubernetes géré dans Canvas, vous pouvez utiliser BlueXP pour supprimer des clusters de l'espace de travail.

Étapes

1. Double-cliquez sur l'environnement de travail Kubernetes dans la zone de travail ou cliquez sur **entrer un environnement de travail**.
2. Dans le coin supérieur droit de la page, sélectionnez le menu actions et cliquez sur **Supprimer de l'espace de travail**.



3. Cliquez sur **Supprimer** pour confirmer la suppression du cluster de l'espace de travail. Vous pouvez redécouvrir ce cluster à tout moment.



Résultats

Le cluster Kubernetes est supprimé de l'espace de travail et n'est plus visible sur la Canvas.

Utilisez les services de données cloud NetApp avec des clusters Kubernetes

Lorsque vous ajoutez un cluster Kubernetes géré à Canvas, vous pouvez utiliser les services de données cloud de NetApp pour bénéficier d'une gestion avancée des données.

Vous pouvez utiliser la sauvegarde et la restauration BlueXP pour sauvegarder des volumes persistants sur le stockage objet.


["Découvrez comment protéger les données de vos clusters Kubernetes à l'aide de la sauvegarde et de la restauration BlueXP"](#).


Restore


Kubernetes

1 Selected Kubernetes Clusters


Backup Settings


 1
Kubernetes Clusters

 5
Protected PVs











 97.66 KB
Total Backups Size

Protected Persistent Volumes Status

 5
Healthy Backup

 0
Failed Backup

5 Backup Jobs

Source K8s Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backup Copies	Backup Status	
 On	pvc-1704aa1f-af1d-49e9-87fd-6edd86125855 Online	default	Nov 25 2021, 14:56:3	2	 Enabled	...
 On	pvc-d1f839c1-d932-4f49-b620-33321dbe939e Online	trident	Nov 25 2021, 14:56:3	2	 Enabled	...
 On	pvc-f615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Online	default	Nov 25 2021, 14:56:3	2	 Enabled	...
 On	pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Online	default	Nov 25 2021, 14:56:3	2	 Enabled	...
 On	pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1 Online	default	Nov 25 2021, 14:56:3	2	 Enabled	...

Connaissances et support

S'inscrire pour obtenir de l'aide

L'enregistrement au support est requis pour recevoir le support technique spécifique à BlueXP et à ses solutions et services de stockage. L'enregistrement au support est également requis pour activer les principaux workflows des systèmes Cloud Volumes ONTAP.

L'inscription au support n'active pas le support NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- ["Amazon FSX pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service pour Google Cloud"](#)

Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxx se trouve sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets. L'inscription est terminée en ajoutant des comptes du site de support NetApp (NSS) à BlueXP, comme décrit ci-dessous.

Enregistrez votre compte BlueXP pour bénéficier de la prise en charge NetApp

Pour vous inscrire au support et activer les droits de support, un utilisateur de votre compte BlueXP doit associer un compte sur le site de support NetApp à sa connexion BlueXP. Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

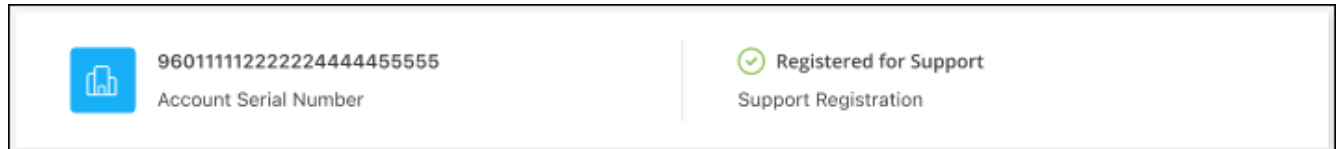
Étapes

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

informations d'identification.

2. Sélectionnez **informations d'identification utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'enregistrement a réussi, sélectionnez l'icône aide et sélectionnez **support**.

La page **Ressources** doit indiquer que votre compte est enregistré pour le support.



Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé de compte sur le site de support NetApp à leur identifiant BlueXP. Toutefois, cela ne signifie pas que votre compte BlueXP n'est pas enregistré pour le support. Tant qu'un utilisateur du compte a suivi ces étapes, votre compte a été enregistré.

Client existant mais aucun compte NSS

Si vous possédez déjà des licences et des numéros de série NetApp, mais que vous possédez un compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP.

Étapes

1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes décrites sous [Client existant avec un compte NSS](#).

Découvrez la toute nouvelle gamme NetApp

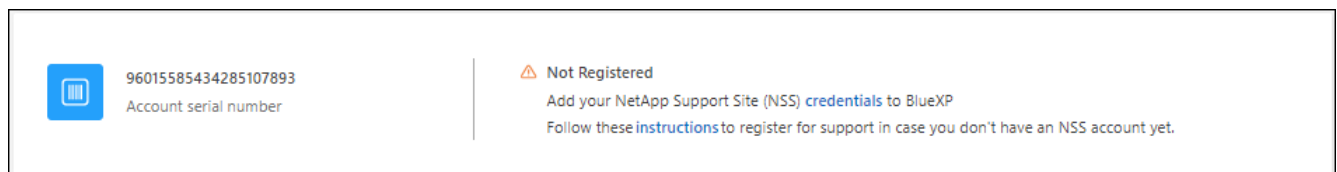
Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

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



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support NetApp](#)" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Une fois que vous avez terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous possédez votre compte sur le site de support NetApp, associez-le à votre connexion BlueXP en suivant les étapes décrites sous [Client existant avec un compte NSS](#).

Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP

Pour activer les workflows clés suivants pour Cloud Volumes ONTAP, vous devez associer les informations d'identification du site de support NetApp à votre compte BlueXP :

- Enregistrement des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation pour bénéficier d'une assistance

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

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

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

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

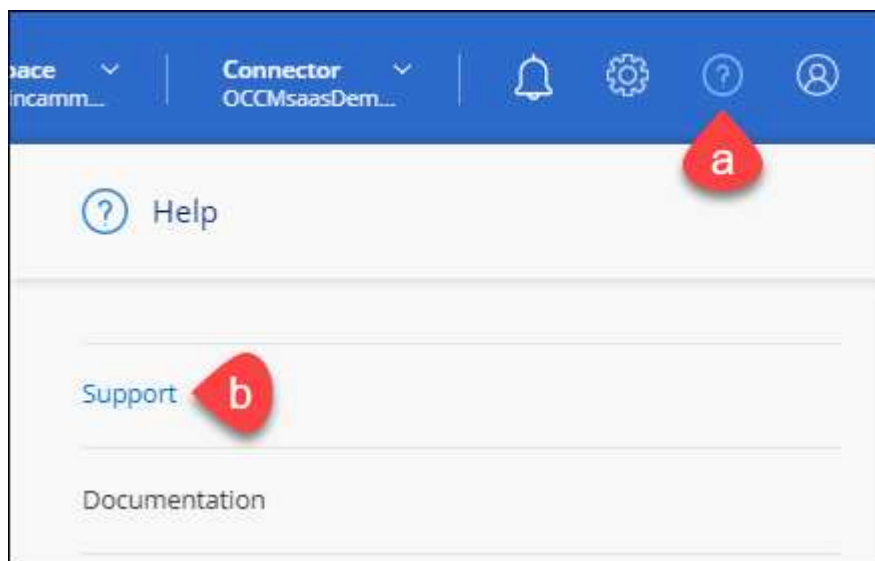
L'association des informations d'identification NSS à votre compte BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP.

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

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

Étapes

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



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

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

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

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

Notez ce qui suit :

- Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS de niveau client.
- Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

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

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

- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS.

Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.

- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu.

Cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Bénéficiez du support pour les services de fichiers d'un fournisseur cloud

Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- ["Amazon FSX pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service pour Google Cloud"](#)

Pour bénéficier du support technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options de support décrites ci-dessous.

Utilisation d'options de support en libre-service

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

La documentation BlueXP que vous consultez actuellement.

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

- Courrier électronique : ng-cloudmanager-feedback@netapp.com [E-mail de commentaires]

Nous accordons une grande importance à vos commentaires. Envoyez vos commentaires pour nous aider à améliorer BlueXP.

Créez un dossier de demande de support auprès du support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un cas**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP. ["Découvrez comment gérer les identifiants associés à votre connexion BlueXP"](#).
- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous support technique :
 - a. Sélectionnez **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
 - b. Sélectionnez **Créer un cas** pour ouvrir un ticket avec un spécialiste du support NetApp :
 - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.

- **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
- **Pièce jointe (facultatif)** : téléchargez jusqu'à cinq pièces jointes, une à la fois.

Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.

ntapitdemo
NetApp Support Site Account

Service

Working Enviroment

Select

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour un historique de vos dossiers de support, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton situé à l'extrême droite vous permet de développer l'action pour afficher les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

« Vous n'êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

Gestion de vos dossiers de demande de support (aperçu)

Vous pouvez afficher et gérer les dossiers de support actifs et résolus directement à partir de BlueXP. Vous pouvez gérer les dossiers associés à votre compte NSS et à votre entreprise.

La gestion des dossiers est disponible en tant qu'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Notez ce qui suit :

- Le tableau de bord de gestion des dossiers en haut de la page propose deux vues :
 - La vue de gauche affiche le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte NSS utilisateur que vous avez fourni.
 - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte NSS utilisateur.

Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.

- Vous pouvez ajouter ou supprimer des colonnes d'intérêt et filtrer le contenu des colonnes telles que priorité et Statut. D'autres colonnes offrent uniquement des fonctions de tri.

Pour plus d'informations, consultez les étapes ci-dessous.

- Au niveau de chaque dossier, nous offrons la possibilité de mettre à jour les notes de dossier ou de fermer un dossier qui n'est pas déjà à l'état fermé ou en attente fermée.

Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sélectionnez **case Management** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

La page **gestion des cas** affiche les cas ouverts associés au compte NSS associé à votre compte utilisateur BlueXP. Il s'agit du même compte NSS qui apparaît en haut de la page **gestion NSS**.

3. Modifiez éventuellement les informations qui s'affichent dans le tableau :

- Sous **cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre société.
- Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une autre période.


The screenshot shows a web interface for managing cases. At the top, there is a search bar and a filter dropdown set to "Cases opened on the last 3 months". A blue button "Create a case" is on the right. Below the filter, a table displays case details. The table has columns for "Date created", "Last updated", "Priority", and "Status (5)". A dropdown menu is open over the "Status (5)" column, showing options: "Assigned", "Active", "Pending customer", and "Solution proposed". The table contains four rows of data:

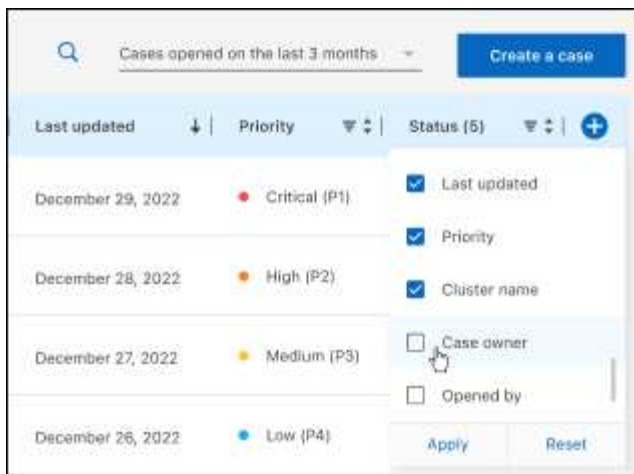
Date created	Last updated	Priority	Status (5)
December 22, 2022	December 29, 2022	Medium (P3)	Assigned
December 21, 2022	December 28, 2022	Medium (P3)	Active
December 15, 2022	December 27, 2022	Medium (P3)	Pending customer
December 14, 2022	December 26, 2022	Low (P4)	Solution proposed

- Filtrez le contenu des colonnes.

This screenshot shows the same interface as the previous one, but with a filter applied to the "Status (5)" column. The dropdown menu is open, and the "Active" status is selected. The table now only displays cases with the "Active" status:

Last updated	Priority	Status (5)
December 29, 2022	Critical (P1)	Active
December 28, 2022	High (P2)	Active
December 27, 2022	Medium (P3)	Active
December 26, 2022	Low (P4)	Active

- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant  puis choisissez les colonnes que vous souhaitez afficher.

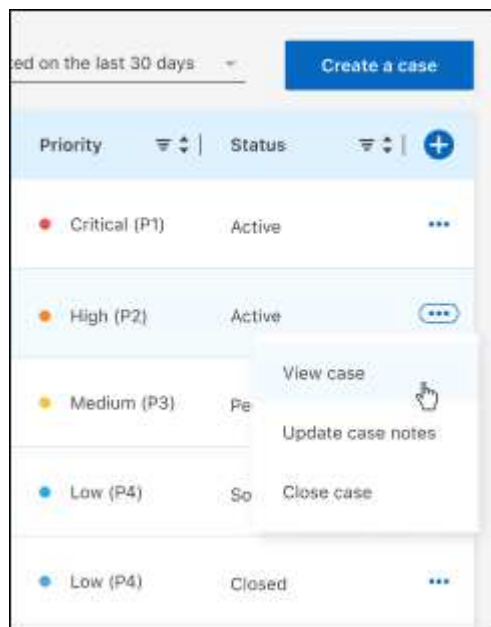


4. Gérer un dossier existant en sélectionnant ... et en sélectionnant l'une des options disponibles :

- **Voir cas**: Afficher tous les détails sur un cas spécifique.
- **Mettre à jour les notes de cas** : fournir des détails supplémentaires sur votre problème ou sélectionner **Télécharger les fichiers** pour joindre jusqu'à cinq fichiers.

Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.

- **Fermer le cas** : fournissez des détails sur la raison pour laquelle vous fermez le cas et sélectionnez **Fermer le cas**.



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

["Note pour BlueXP"](#)

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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