De formation

Kubernetes clusters

NetApp
January 04, 2024

Sommaire

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.

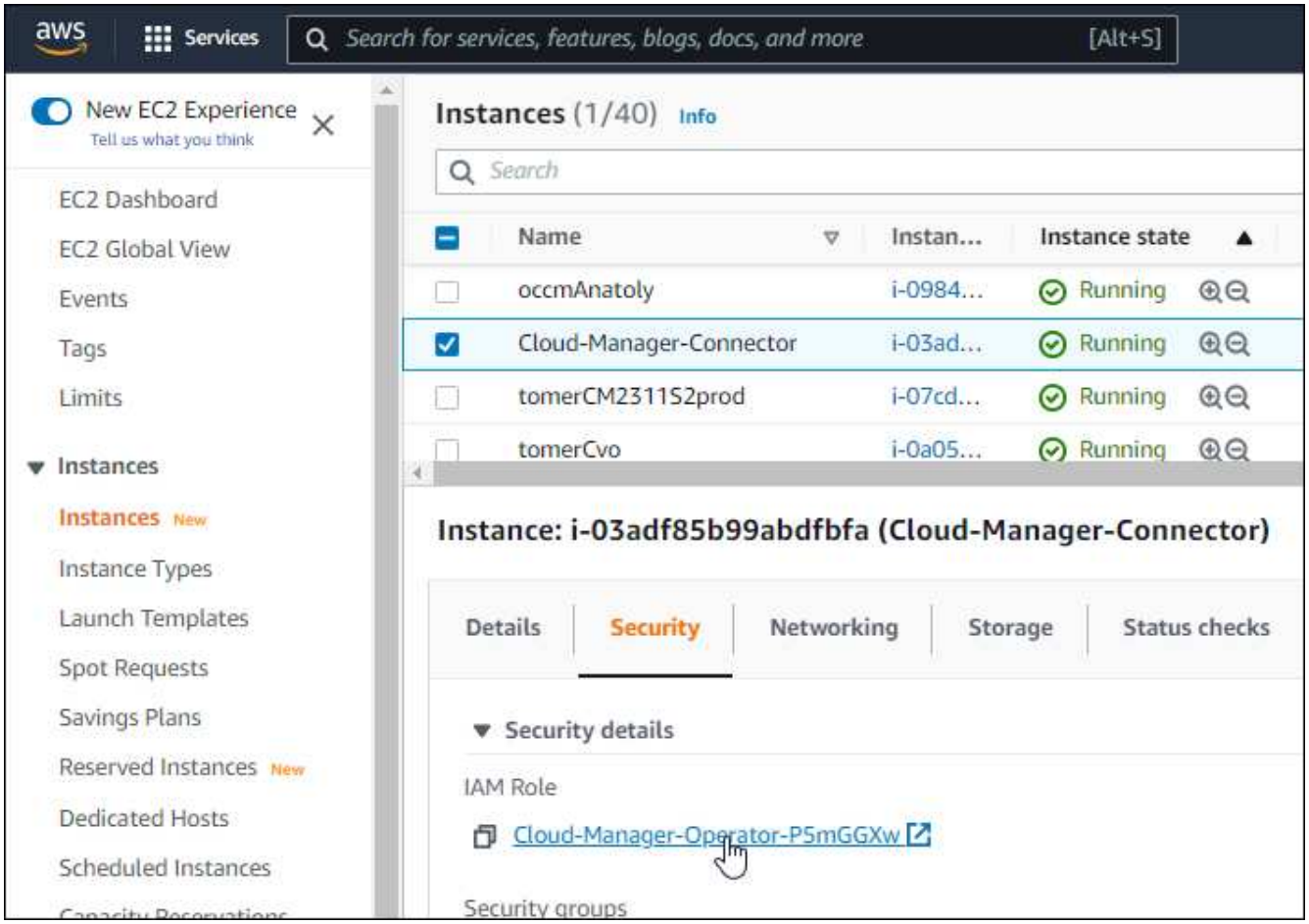
- "Créez un connecteur depuis BlueXP" (recommandé)
- "Créez un connecteur à partir d'AWS Marketplace"
- "Installez le connecteur sur un hôte Linux existant dans AWS"

Ajoutez les autorisations requises à un connecteur existant

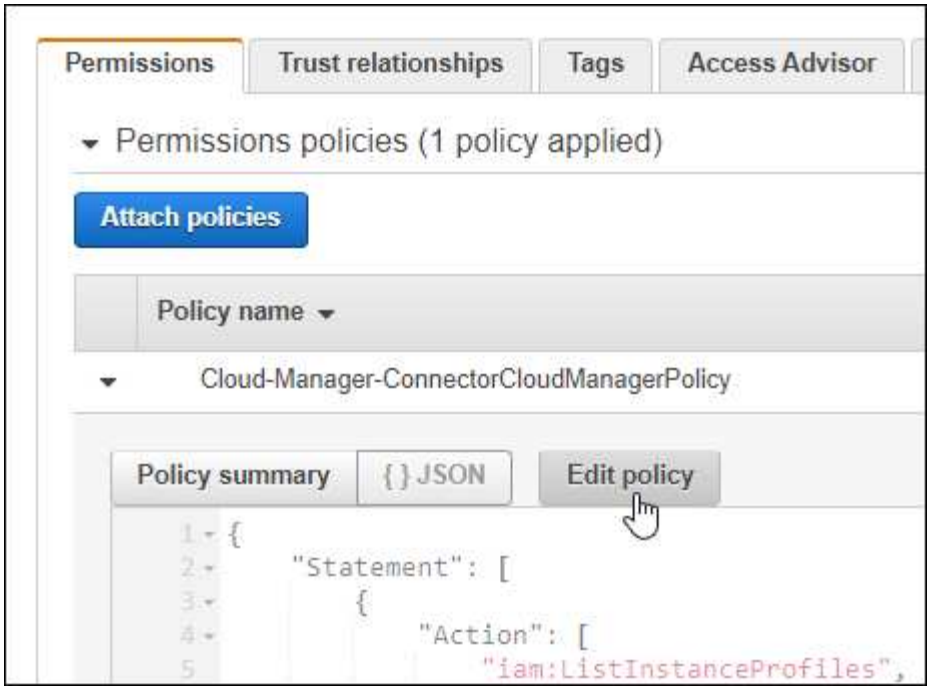
À partir de la version 3.9.13, tout *nouvellement* créé Connector inclut trois nouvelles autorisations AWS permettant la découverte et la gestion des clusters Kubernetes. Si vous avez créé un connecteur avant cette version, vous devrez modifier la stratégie existante pour le rôle IAM du connecteur afin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

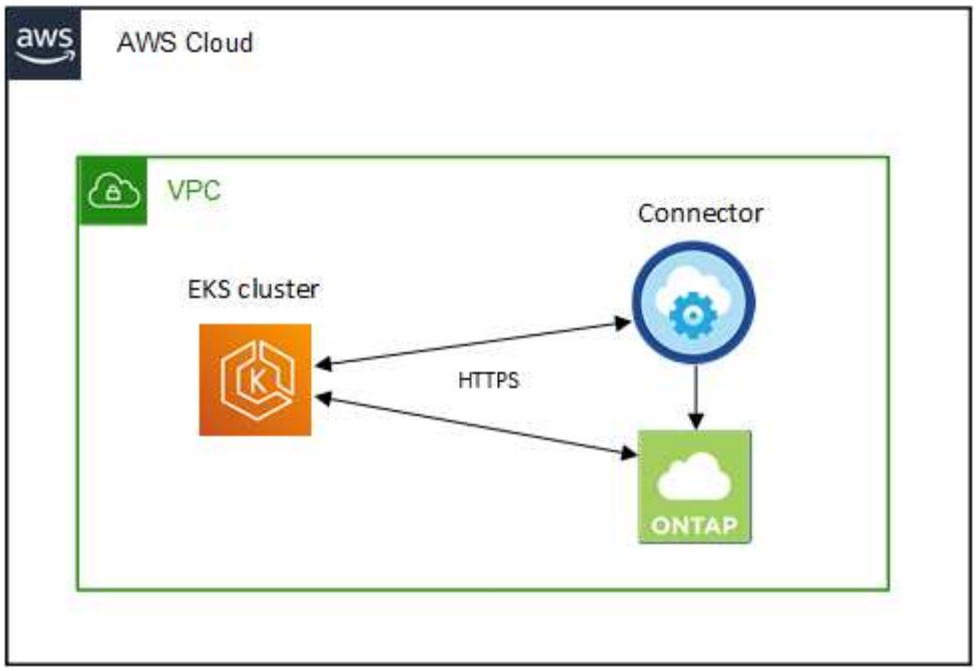
Examiner les besoins en matière de mise en réseau

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.

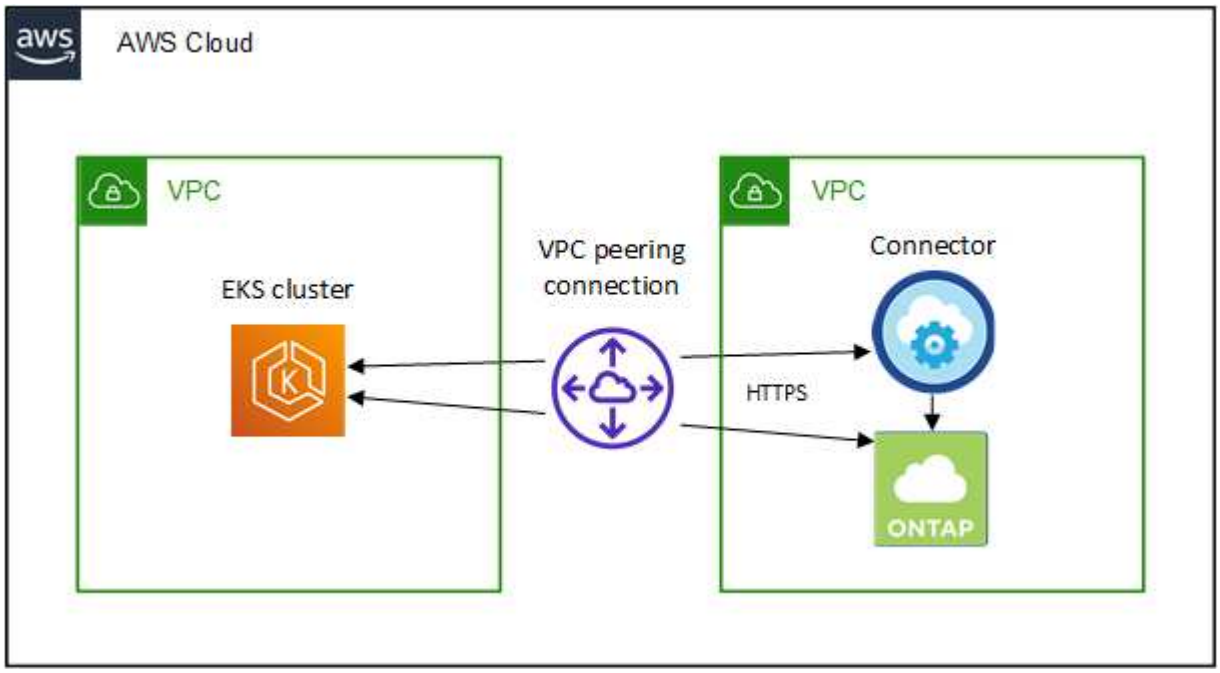
- Chaque cluster Kubernetes doit disposer d'une connexion entrante depuis le connecteur
- Le connecteur doit disposer d'une connexion sortante vers chaque cluster Kubernetes sur le port 443

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 :
   a. Sur le portail Azure, ouvrez votre abonnement Azure.
   b. Cliquez sur **contrôle d'accès (IAM) > rôles**.
   c. Cliquez sur les points de suspension (…) du rôle personnalisé, puis cliquez sur **Modifier**.
   d. 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**.

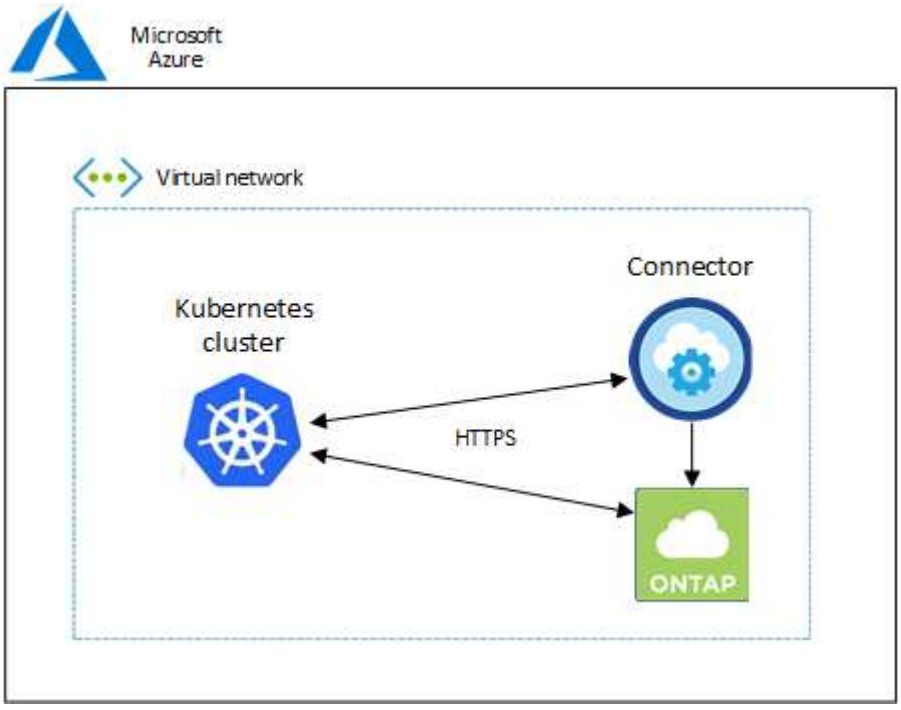
Examiner les besoins en matière de mise en réseau

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

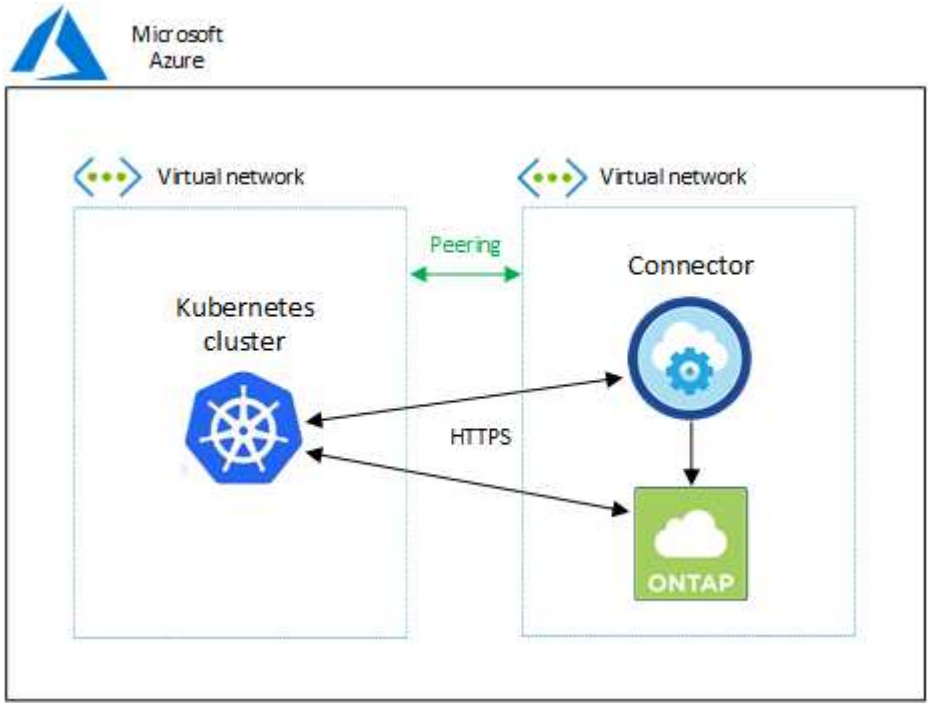
Pour obtenir cette connectivité, la méthode la plus simple consiste à déployer le connecteur et Cloud Volumes ONTAP dans le même vnet que le cluster Kubernetes. Sinon, vous devez configurer une connexion de peering entre les différents VNets.

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

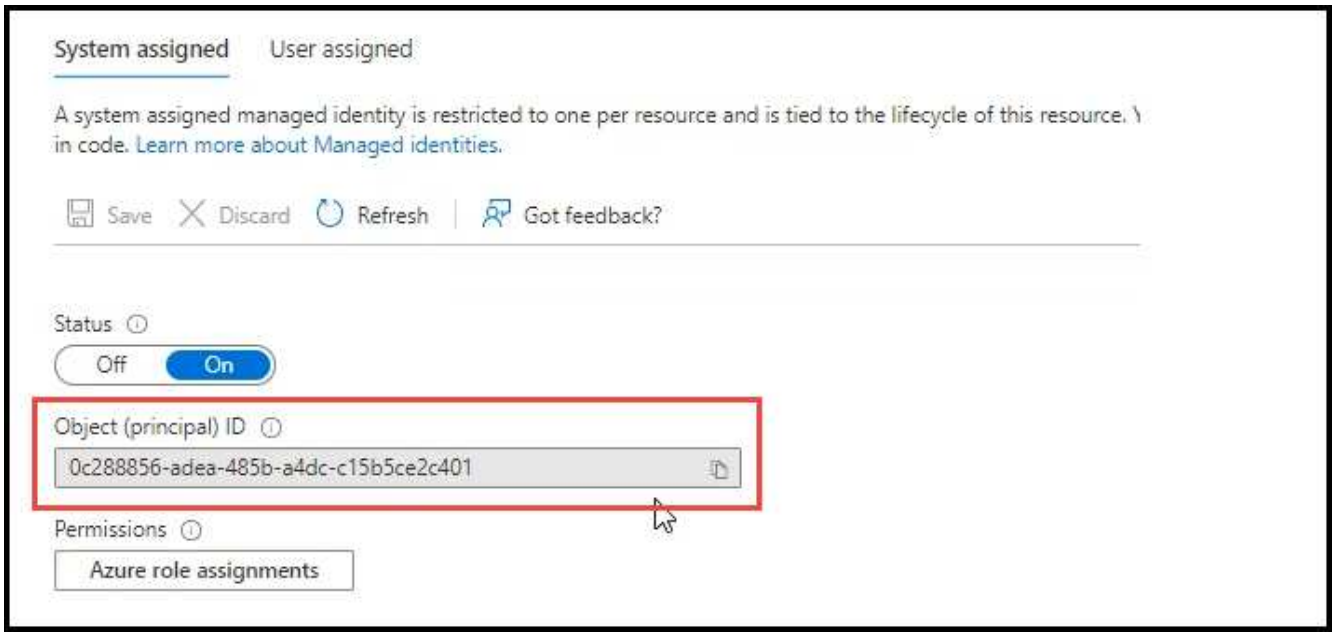
Vous devez fournir une autorisation complète pour BlueXP afin d'installer Astra Trident.

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.



- 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.

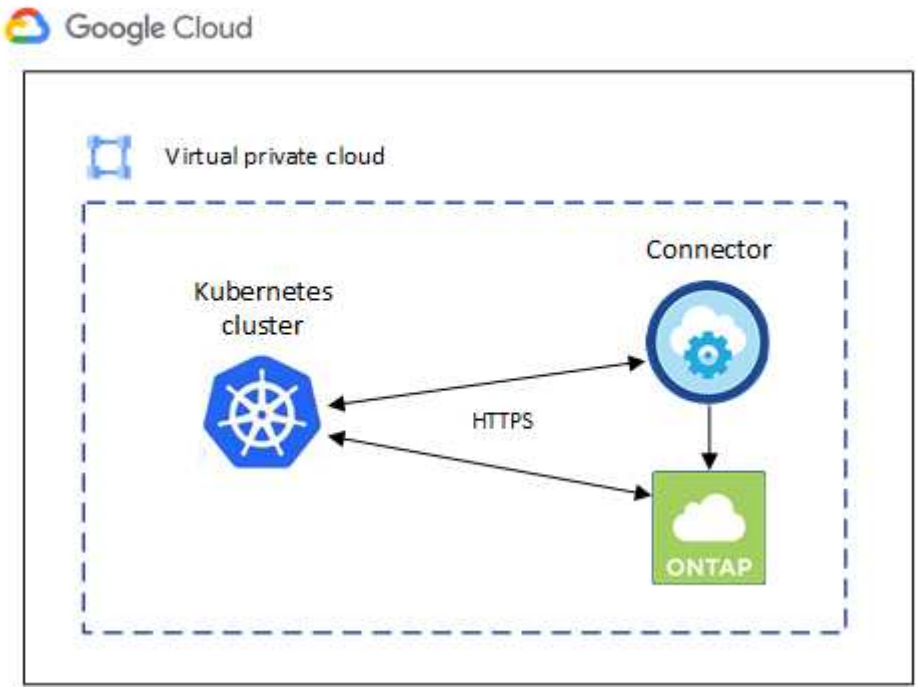
Examiner les besoins en matière de mise en réseau

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

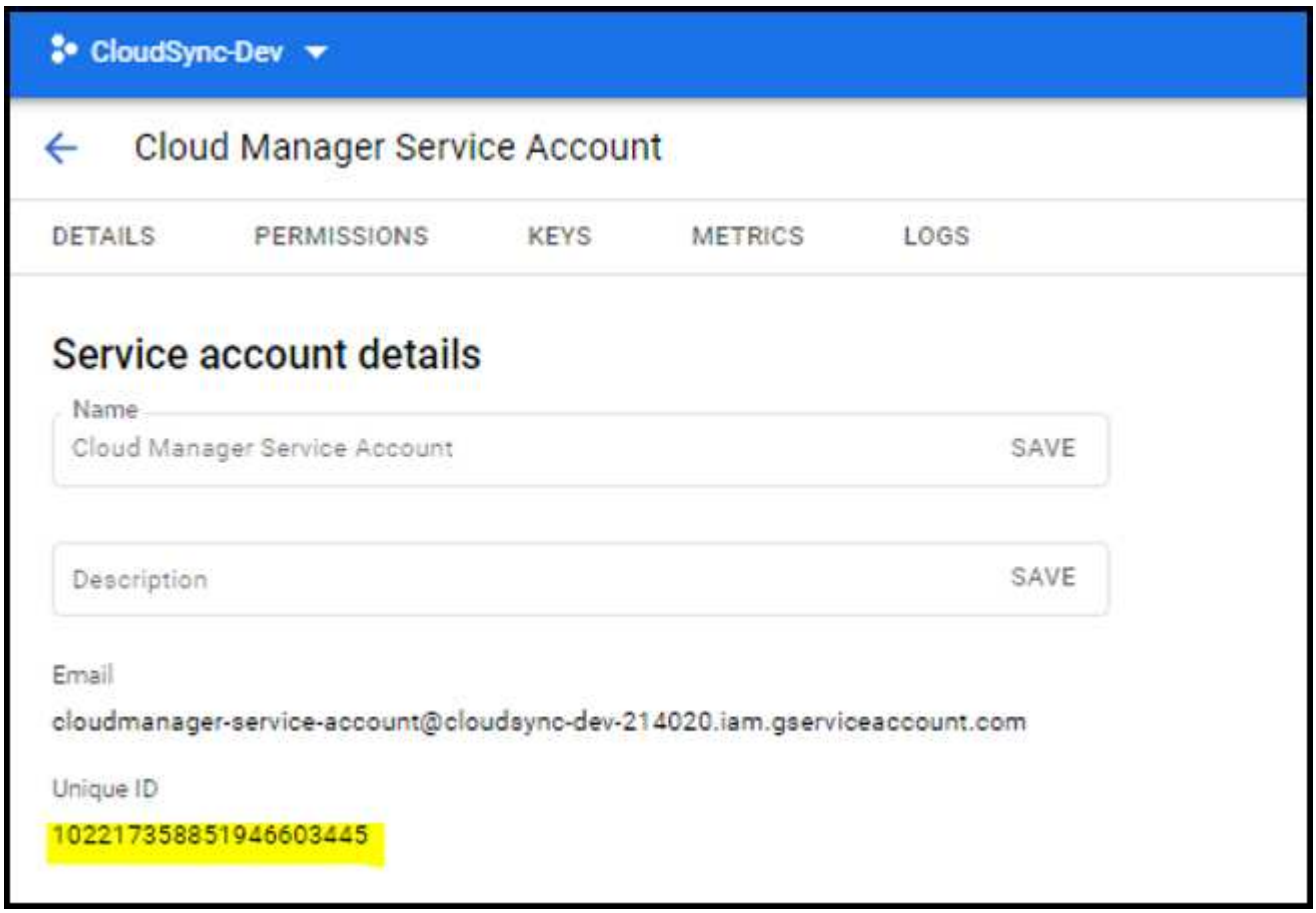
À configurer `subjects: name:` Dans le fichier YAML, vous devez connaître l'ID unique BlueXP.

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".



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 :

a. 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.

Informations sur le copyright

Informations sur les marques commerciales