Commencez

Astra Control Service

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-service/get-started/intro.html on April 18, 2024. Always check docs.netapp.com for the latest.

Sommaire

Commencez . . . 1
- Découvrez Astra Control . . . 1
- Déploiements Kubernetes pris en charge . . . 5
- Démarrage rapide pour le service Astra Control . . . 5
- Configurez votre fournisseur cloud . . . 7
- Créez un compte de service Astra Control . . . 27
- Ajoutez un cluster à Astra Control Service . . . 29
- Et la suite ? . . . 69
- Vidéos sur le service Astra Control . . . 70

Commencez

Découvrez Astra Control

Astra Control est une solution de gestion du cycle de vie des données applicatives Kubernetes qui simplifie les opérations des applications avec état. Protégez, sauvegardez et migrez facilement les workloads Kubernetes, et créez instantanément des clones d'applications de travail.

Caractéristiques

Astra Control offre des fonctionnalités stratégiques pour la gestion du cycle de vie des données d'application Kubernetes :

- Gérez automatiquement le stockage persistant
- Création de copies Snapshot et de sauvegardes à la demande intégrant la cohérence applicative
- Automatisation des opérations de sauvegarde et de snapshots basées sur des règles
- Migrez des applications et des données d'un cluster Kubernetes vers un autre
- Réplication d'applications sur un système distant à l'aide de la technologie NetApp SnapMirror (Astra Control Center)
- Clonage d'applications de la phase de transfert à la production
- Visualiser l'état de santé et de protection des applications
- Implémentation de vos workflows de sauvegarde et de migration à l'aide d'une interface utilisateur web ou d'une API

Modèles de déploiement

Astra Control est disponible dans deux modèles de déploiement :

- **Astra Control Service** : service géré par NetApp qui permet de gérer les données intégrant la cohérence applicative de clusters Kubernetes dans plusieurs environnements de fournisseurs cloud, ainsi que des clusters Kubernetes autogéré.
- **Astra Control Center** : logiciel autogéré qui assure une gestion des données compatible avec les applications de clusters Kubernetes exécutés dans votre environnement sur site. Astra Control Center peut également être installé sur plusieurs environnements de fournisseur cloud avec un système back-end de stockage NetApp Cloud Volumes ONTAP.

	Service Astra Control	**Centre de contrôle Astra**
Comment est-elle proposée ?	En tant que service cloud entièrement géré de NetApp	En tant que logiciel que vous pouvez télécharger, installer et gérer
Où est-il hébergé ?	Dans le cloud public de votre choix	Sur votre cluster Kubernetes
Comment est-elle mise à jour ?	Géré par NetApp	Vous gérez toutes les mises à jour

	Service Astra Control	Centre de contrôle Astra
Quelles sont les distributions Kubernetes prises en charge ?	• **Fournisseurs de cloud** ◦ Amazon Web Services ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure ▪ Azure Kubernetes Service (AKS) • **Clusters autogérés** ◦ Kubernetes (en amont) ◦ Rancher Kubernetes Engine (RKE) ◦ Plateforme de conteneurs Red Hat OpenShift • **Clusters sur site** ◦ Red Hat OpenShift Container Platform sur site	• Azure Kubernetes Service sur Azure Stack HCI • Anthos de Google • Kubernetes (en amont) • Rancher Kubernetes Engine (RKE) • Plateforme de conteneurs Red Hat OpenShift

	Service Astra Control	Centre de contrôle Astra
Quels sont les systèmes back-end pris en charge ?	• **Fournisseurs de cloud** ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX pour NetApp ONTAP ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disque persistant Google ▪ NetApp Cloud Volumes Service ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Disques gérés Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Clusters autogérés** ◦ Amazon EBS ◦ Disques gérés Azure ◦ Disque persistant Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • **Clusters sur site** ◦ NetApp MetroCluster ◦ Systèmes NetApp ONTAP AFF et FAS ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn"	• Systèmes NetApp ONTAP AFF et FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Fonctionnement du service Astra Control

Astra Control Service est un service cloud géré par NetApp qui est constamment disponible et mis à jour avec les dernières fonctionnalités. Elle utilise plusieurs composants pour faciliter la gestion du cycle de vie des données des applications.

À un niveau élevé, le service de contrôle Astra fonctionne comme suit :

- Commencez avec le service Astra Control en configurant votre fournisseur de services cloud et en vous inscrivant à un compte Astra.

+ ** pour les clusters GKE, Astra Control Service utilise "NetApp Cloud Volumes Service pour Google Cloud" Ou des disques persistants Google en tant que système de stockage back-end pour vos volumes persistants.

+ ** pour les grappes AKS, Astra Control Service utilise "Azure NetApp Files" Ou des disques gérés Azure en tant que backend de stockage pour les volumes persistants.

+ ** pour les clusters Amazon EKS, Astra Control Service utilise "Amazon Elastic Block Store" ou "Amazon FSX pour NetApp ONTAP" en tant que système back-end de stockage pour vos volumes persistants.

- Vous ajoutez votre première solution de calcul Kubernetes à Astra Control Service. Le service de contrôle d'Astra procède ensuite aux opérations suivantes :
  - Crée un magasin d'objets sur votre compte de fournisseur cloud, où sont stockées les copies de sauvegarde.

+ dans Azure, Astra Control Service crée également un groupe de ressources, un compte de stockage et des clés pour le conteneur Blob.

- Crée un nouveau rôle d'administrateur et un compte de service Kubernetes sur le cluster.
- Utilise ce nouveau rôle d'administration pour installer le lien../concepts/architecture#astra-control-components[astra Control Provisioner] sur le cluster et pour créer une ou plusieurs classes de stockage.
- Si vous utilisez une offre de stockage de service cloud NetApp comme système back-end de stockage, Astra Control Service utilise Astra Control provisionner pour provisionner des volumes persistants pour vos applications. Si vous utilisez des disques gérés Amazon EBS ou Azure comme système de stockage principal, vous devez installer un pilote CSI spécifique au fournisseur. Les instructions d'installation sont fournies dans le "Configurer Amazon Web Services" et "Configuration de Microsoft Azure avec des disques gérés Azure".
  - À ce stade, vous pouvez définir des applications à partir de votre cluster. Les volumes persistants seront provisionnés sur le back-end de stockage via la nouvelle classe de stockage par défaut.
  - Utilisez ensuite le service Astra Control pour gérer ces applications, et commencez à créer des copies Snapshot, des sauvegardes et des clones.

Le plan gratuit d'Astra Control vous permet de gérer jusqu'à 10 espaces de noms dans votre compte. Si vous souhaitez gérer plus de 10 espaces de noms, vous devrez configurer la facturation en passant du Plan gratuit au Plan Premium.

Fonctionnement du centre de contrôle Astra

Astra Control Center fonctionne localement dans votre propre cloud privé.

ASTRA Control Center prend en charge des clusters Kubernetes avec une classe de stockage configurée par Astra Control Provisioner et un système de stockage back-end ONTAP.

Astra Control Center est entièrement intégré à l'écosystème AutoSupport et Active IQ. Il fournit aux utilisateurs et au support NetApp des informations relatives à la résolution de problèmes et à l'utilisation.

Vous pouvez essayer Astra Control Center avec une licence d'évaluation de 90 jours. La version d'évaluation est prise en charge par courrier électronique et par les options de communauté. Vous avez également accès aux articles et à la documentation de la base de connaissances à partir du tableau de bord de support des produits.

Pour installer et utiliser Astra Control Center, vous devez vous en assurer "de formation".

À un niveau élevé, le centre de contrôle Astra ressemble à ce qui suit :

- Vous installez Astra Control Center dans votre environnement local. En savoir plus "Poser le centre de contrôle Astra".
- Vous avez effectué certaines tâches de configuration, telles que :
  - Configuration des licences.
  - Ajoutez votre premier cluster.
  - Ajout du stockage back-end découvert lorsque vous avez ajouté le cluster
  - Ajoutez un compartiment de magasin d'objets pour stocker vos sauvegardes d'applications.

En savoir plus "Configurer le centre de contrôle Astra".

Vous pouvez ajouter des applications à votre cluster. Si certaines applications sont déjà gérées dans le cluster, vous pouvez aussi utiliser Astra Control Center pour les gérer. Utilisez ensuite Astra Control Center pour créer des copies Snapshot, des sauvegardes, des clones et des relations de réplication.

Pour en savoir plus

- "Documentation de la gamme de produits NetApp Astra"
- "Documentation Astra Control Center"
- "Documentation de l'API Astra Control"
- "Documentation Astra Trident"
- "Documentation ONTAP"

Déploiements Kubernetes pris en charge

Astra Control Service gère les applications qui s'exécutent sur un cluster Kubernetes géré dans Amazon Elastic Kubernetes Service (EKS), ainsi que les clusters que vous gérez seul.

Astra Control Service peut gérer les applications qui s'exécutent sur un cluster Kubernetes géré dans Google Kubernetes Engine (GKE), ainsi que les clusters que vous gérez eux-mêmes.

Astra Control Service gère les applications qui s'exécutent sur un cluster Kubernetes géré dans Azure Kubernetes Service (AKS), ainsi que les clusters que vous gérez seul.

- "Découvrez comment configurer Amazon Web Services pour Astra Control Service".
- "Découvrez comment configurer Google Cloud pour Astra Control Service".
- "Découvrez comment configurer Microsoft Azure avec Azure NetApp Files pour le service Astra Control".
- "Découvrez comment configurer Microsoft Azure avec des disques gérés Azure pour Astra Control Service".
- "Découvrez comment préparer des clusters autogérés avant de les ajouter au service Astra Control".

Démarrage rapide pour le service Astra Control

Cette page offre un aperçu détaillé des étapes à suivre pour commencer à utiliser le service Astra Control. Les liens de chaque étape vous mènent à une page qui fournit plus de détails.

[Une seule] Configurez votre fournisseur cloud

1. Google Cloud :
    - Examiner la configuration requise du cluster Google Kubernetes Engine.
    - Achetez Cloud Volumes Service pour Google Cloud sur Google Cloud Marketplace.
    - Activez les API requises.
    - Créez un compte de service et une clé de compte de service.
    - Configurez le peering réseau de votre VPC vers Cloud Volumes Service pour Google Cloud.

      "En savoir plus sur les exigences de Google Cloud".
2. Amazon Web Services :
    - Vérifiez la configuration requise pour le cluster Amazon Web Services.
    - Créez un compte Amazon.
    - Installez l'interface de ligne de commande Amazon Web Services.
    - Créer un utilisateur IAM.
    - Créez et joignez une stratégie d'autorisations.
    - Enregistrer les informations d'identification pour l'utilisateur IAM.

      "En savoir plus sur les conditions requises pour Amazon Web Services".
3. Microsoft Azure :
    - Examinez les exigences de cluster Azure Kubernetes Service pour le système de stockage back-end que vous prévoyez d'utiliser.

      "En savoir plus sur les exigences relatives à Microsoft Azure et à Azure NetApp Files".

"En savoir plus sur les besoins en disques gérés pour Microsoft Azure et Azure".

Si vous gérez votre propre cluster et que ce dernier n'est pas hébergé par un fournisseur cloud, vérifiez les exigences en matière de clusters autogérés.
"En savoir plus sur les besoins en clusters autogérés".

[Deux] Complétez l'inscription à Astra Control

1. Créer un "NetApp BlueXP" compte.
2. Spécifiez votre ID de messagerie NetApp BlueXP lors de la création de votre compte Astra Control "À partir de la page produit Astra Control".

"En savoir plus sur le processus d'inscription".

[Trois] Ajoutez des clusters à Astra Control

Une fois connecté, sélectionnez **Ajouter un cluster** pour commencer à gérer votre cluster avec Astra Control.

"En savoir plus sur l'ajout de clusters".

Configurez votre fournisseur cloud

Configurer Amazon Web Services

Pour préparer votre projet Amazon Web Services, vous devez suivre quelques étapes pour gérer les clusters Amazon Elastic Kubernetes Service (EKS) avec Astra Control Service.

Démarrage rapide pour la configuration d'Amazon Web Services

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

[Une seule] Lisez les exigences d'Astra Control Service pour Amazon Web Services

Assurez-vous que les clusters exécutent une version prise en charge de Kubernetes, que les nœuds workers sont en ligne et exécutent Linux ou Windows, et bien plus encore. En savoir plus sur cette étape.

[Deux] Créez un compte Amazon

Si vous n'avez pas encore de compte Amazon, vous devez en créer un pour pouvoir utiliser EKS. En savoir plus sur cette étape.

[Trois] Installez l'interface de ligne de commande Amazon Web Services

Installez l'interface de ligne de commandes AWS afin de gérer AWS à partir de la ligne de commandes. Suivez les instructions étape par étape.

[Quatre] Facultatif : créez un utilisateur IAM

Créez un utilisateur Amazon Identity and Access Management (IAM). Vous pouvez également ignorer cette étape et utiliser un utilisateur IAM existant avec le service de contrôle Astra.

Lisez les instructions détaillées.

[Cinq] Créez et joignez une stratégie d'autorisations

Créez une règle avec les autorisations requises pour que le service Astra Control puisse interagir avec votre compte AWS.

Lisez les instructions détaillées.

[Six] Enregistrer les informations d'identification pour l'utilisateur IAM

Enregistrez les informations d'identification de l'utilisateur IAM pour pouvoir importer les informations d'identification dans le service de contrôle Astra.

Lisez les instructions détaillées.

Configuration requise pour le cluster EKS

Un cluster Kubernetes doit respecter les exigences suivantes pour que vous puissiez découvrir et gérer Astra Control Service.

Version Kubernetes

Un cluster doit exécuter une version Kubernetes comprise entre 1.25 et 1.28.

Type d'image

Le type d'image pour chaque nœud de travail doit être Linux.

État du cluster

Les clusters doivent être exécutés en état de fonctionnement et avoir au moins un nœud de travail en ligne sans nœuds de travail en panne.

De provisionnement Astra Control

Un mécanisme de provisionnement Astra Control et un contrôleur Snapshot externe sont requis pour les opérations avec les systèmes back-end de stockage. Pour activer ces opérations, procédez comme suit :

1. "Installez les CRD de snapshot et le contrôleur de snapshot".
2. "Activez le mécanisme de provisionnement Astra Control".
3. "Créez une VolumeSnapshotClass".

Pilotes CSI pour Amazon Elastic Block Store (EBS)

Si vous utilisez le système back-end Amazon EBS, vous devez installer le pilote Container Storage interface (CSI) pour EBS (il n'est pas installé automatiquement).

Reportez-vous aux étapes pour obtenir des instructions sur l'installation du pilote CSI.

Installez un snapshots externe

Si ce n'est déjà fait, "Installez les CRD de snapshot et le contrôleur de snapshot".

Installez le pilote CSI en tant que module complémentaire Amazon EKS

1. Créez le rôle IAM du pilote Amazon EBS CSI pour les comptes de service. Suivez les instructions "Dans la documentation Amazon", En utilisant les commandes de l'interface de ligne de commande AWS dans les instructions.
2. Ajoutez le module complémentaire Amazon EBS CSI à l'aide de la commande CLI AWS suivante, en remplaçant les informations entre parenthèses <> par des valeurs spécifiques à votre environnement. Remplacez <DRIVER_ROLE> par le nom du rôle du pilote EBS CSI que vous avez créé à l'étape précédente :

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configuration de la classe de stockage EBS

1. Clonez le référentiel GitHub du pilote Amazon EBS CSI sur votre système.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. Accédez au répertoire d'exemple de provisionnement dynamique.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Déploiement de la classe de stockage ebs-sc et de la demande de volume persistant ebs-claim dans le répertoire des manifestes.

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. Classe de stockage ebs-sc

```
kubectl describe storageclass ebs-sc
```

Vous devez voir le résultat décrivant les attributs de classe de stockage.

Créez un compte Amazon

Si vous n'avez pas encore de compte Amazon, vous devez en créer un pour activer la facturation pour Amazon EKS.

Étapes

1. Accédez au "Page d'accueil Amazon" , Sélectionnez **connexion** en haut à droite, puis **commencer ici**.
2. Suivez les invites pour créer un compte.

Installez l'interface de ligne de commande Amazon Web Services

Installez l'interface de ligne de commandes AWS afin de gérer les ressources AWS à partir de la ligne de commandes.

Étape

1. Accédez à "Mise en route de l'interface de ligne de commandes AWS" Et suivez les instructions pour installer l'interface de ligne de commande.

Facultatif : créez un utilisateur IAM

Créez un utilisateur IAM afin d'utiliser et de gérer tous les services et ressources AWS avec une sécurité renforcée. Vous pouvez également ignorer cette étape et utiliser un utilisateur IAM existant avec le service de contrôle Astra.

Étape

1. Accédez à "Création d'utilisateurs IAM" Et suivez les instructions pour créer un utilisateur IAM.

Créez et joignez une stratégie d'autorisations

Créez une règle avec les autorisations requises pour que le service Astra Control puisse interagir avec votre compte AWS.

Étapes

1. Créez un nouveau fichier appelé `policy.json`.
2. Copiez le contenu JSON suivant dans le fichier :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Création de la règle :

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. Associez la stratégie à l'utilisateur IAM. Remplacement `<IAM-USER-NAME>` Avec le nom d'utilisateur de l'utilisateur IAM que vous avez créé ou un utilisateur IAM existant :

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

Enregistrer les informations d'identification pour l'utilisateur IAM

Enregistrez les informations d'identification de l'utilisateur IAM afin de sensibiliser l'utilisateur au service de contrôle Astra.

Étapes

1. Téléchargez les informations d'identification. Remplacement `<IAM-USER-NAME>` Avec le nom d'utilisateur de l'utilisateur IAM que vous souhaitez utiliser :

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

Résultat

Le `credential.json` Le fichier est créé et vous pouvez importer les informations d'identification dans le service de contrôle Astra.

Configurez Google Cloud

Il vous faut quelques étapes pour préparer votre projet Google Cloud avant de gérer des clusters Google Kubernetes Engine avec Astra Control Service.

> Si vous ne démarrez pas à l'aide de Google Cloud Volumes Service pour Google Cloud en tant que backend de stockage, mais que vous prévoyez de l'utiliser ultérieurement, vous devez terminer les étapes nécessaires à la configuration de Google Cloud Volumes Service pour Google Cloud maintenant. Si vous créez un compte de service ultérieurement, vous risquez de perdre l'accès à vos compartiments de stockage existants.

Démarrage rapide pour la configuration de Google Cloud

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

[Une seule] Lisez les exigences d'Astra Control Service pour Google Kubernetes Engine

Assurez-vous que les clusters exécutent une version Kubernetes prise en charge, que les nœuds workers sont en ligne et exécutent un type d'image pris en charge, etc. En savoir plus sur cette étape.

[Deux] (Facultatif) : achat d'Cloud Volumes Service pour Google Cloud

Si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud en tant que backend de stockage, rendez-vous sur la page NetApp Cloud Volumes Service dans Google Cloud Marketplace et sélectionnez Acheter. En savoir plus sur cette étape.

[Trois] Intégrez des API dans votre projet Google Cloud

Activez les API Google Cloud suivantes :

- Google Kubernetes Engine
- Le stockage cloud
- API JSON de stockage cloud

- Utilisation du service
- API Cloud Resource Manager
- NetApp Cloud Volumes Service
  - Obligatoire pour Cloud Volumes Service pour Google Cloud
  - Facultatif (mais recommandé) pour les disques persistants Google
- API Service Consumer Management
- API de mise en réseau de services
- API de gestion de services

Suivez les instructions étape par étape.

[Quatre] Créez un compte de service disposant des autorisations requises

Créez un compte de service Google Cloud disposant des autorisations suivantes :

- Admin moteur Kubernetes
- Admin NetApp Cloud volumes
  - Obligatoire pour Cloud Volumes Service pour Google Cloud
  - Facultatif (mais recommandé) pour les disques persistants Google
- Administrateur du stockage
- Visualiseur d'utilisation de service
- Calculer Network Viewer

Lisez les instructions détaillées.

[Cinq] Créez une clé de compte de service

Créez une clé pour le compte de service et enregistrez le fichier de clé dans un emplacement sécurisé. Suivez les instructions étape par étape.

[Six] (Facultatif) : configurez le peering réseau pour votre VPC

Si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud en tant que backend de stockage, configurez le peering de réseau de votre VPC vers Cloud Volumes Service pour Google Cloud. Suivez les instructions étape par étape.

Configuration requise pour les clusters GKE

Un cluster Kubernetes doit respecter les exigences suivantes pour que vous puissiez découvrir et gérer Astra Control Service. Notez que certaines de ces exigences s'appliquent uniquement si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud en tant que système de stockage back-end.

Version Kubernetes

Un cluster doit exécuter une version Kubernetes comprise entre 1.26 et 1.28.

Type d'image

Le type d'image de chaque nœud de travail doit être `COS_CONTAINERD`.

État du cluster

Les clusters doivent être exécutés en état de fonctionnement et avoir au moins un nœud de travail en ligne sans nœuds de travail en panne.

Région Google Cloud

Si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud en tant que système de stockage back-end, les clusters doivent être exécutés dans un "Région Google Cloud prise en charge de Cloud Volumes Service pour Google Cloud" Notez qu'Astra Control Service prend en charge les deux types de service : CVS et CVS-Performance. Il est recommandé de choisir une région qui prend en charge Cloud Volumes Service pour Google Cloud, même si vous ne l'utilisez pas comme système de stockage principal. Il est ainsi plus facile d'utiliser Cloud Volumes Service pour Google Cloud comme système de stockage back-end, à l'avenir si vos besoins en performance évoluent.

Mise en réseau

Si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud en tant que backend de stockage, le cluster doit résider dans un VPC avec Cloud Volumes Service pour Google Cloud. Cette étape est décrite ci-dessous.

Clusters privés

Si le cluster est privé, le "réseaux autorisés" Doit autoriser l'adresse IP du service de contrôle Astra :

52.188.218.166/32

Mode d'opération pour un cluster GKE

Vous devez utiliser le mode de fonctionnement standard. Le mode pilote automatique n'a pas encore été testé. "En savoir plus sur les modes de fonctionnement".

Pools de stockage

Si vous utilisez NetApp Cloud Volumes Service comme back-end de stockage avec le type de service CVS, vous devez configurer des pools de stockage avant de pouvoir provisionner des volumes. Reportez-vous à la section "Type de service, classes de stockage et taille PV pour les clusters GKE" pour en savoir plus.

Facultatif : achetez Cloud Volumes Service pour Google Cloud

Astra Control Service peut utiliser Cloud Volumes Service pour Google Cloud comme backend de stockage pour vos volumes persistants. Si vous prévoyez d'utiliser ce service, vous devez acheter Cloud Volumes Service pour Google Cloud à partir de Google Cloud Marketplace pour activer la facturation des volumes persistants.

Étape

1. Accédez au "Page NetApp Cloud Volumes Service" Dans Google Cloud Marketplace, sélectionnez **Acheter** et suivez les invites.

   "Suivez des instructions détaillées dans la documentation Google Cloud pour acheter et activer le service".

Activez les API dans votre projet

Votre projet nécessite des autorisations pour accéder à des API Google Cloud spécifiques. Les API sont utilisées pour interagir avec les ressources Google Cloud, comme les clusters Google Kubernetes Engine (GKE) et le stockage NetApp Cloud Volumes Service.

Étape

1. "Utilisez la console Google Cloud ou l'interface de ligne de commande gCloud pour activer les API suivantes":
    - Google Kubernetes Engine
    - Le stockage cloud
    - API JSON de stockage cloud
    - Utilisation du service
    - API Cloud Resource Manager
    - NetApp Cloud Volumes Service (requis pour Cloud Volumes Service pour Google Cloud)
    - API Service Consumer Management
    - API de mise en réseau de services
    - API de gestion de services

La vidéo suivante montre comment activer les API à partir de la console Google Cloud.

► https://docs.netapp.com/fr-fr/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Créez un compte de service

Astra Control Service utilise un compte de service Google Cloud pour faciliter la gestion des données applicatives Kubernetes pour votre compte.

Étapes

1. Rendez-vous sur Google Cloud et "créez un compte de service à l'aide de la console, de la commande gcloud ou d'une autre méthode préférée".
2. Accordez au compte de service les rôles suivants :
    - **Kubernetes Engine Admin** - utilisé pour répertorier les clusters et créer un accès administrateur pour gérer les applications.
    - **NetApp Cloud volumes Admin** : permet de gérer le stockage persistant pour les applications.
    - **Administrateur de stockage** - utilisé pour gérer des compartiments et des objets pour les sauvegardes d'applications.
    - **Visualiseur d'utilisation du service** - utilisé pour vérifier si les API Cloud Volumes Service requises pour Google Cloud sont activées.
    - **Compute Network Viewer** : permet de vérifier si le VPC Kubernetes est autorisé à atteindre Cloud Volumes Service pour Google Cloud.

Si vous souhaitez utiliser gcloud, vous pouvez suivre les étapes de l'interface Astra Control. Sélectionnez **compte > informations d'identification > Ajouter informations d'identification**, puis **instructions**.

Si vous souhaitez utiliser la console Google Cloud, la vidéo suivante montre comment créer le compte de service à partir de la console.

► https://docs.netapp.com/fr-fr/astra-control-service/media/get-started/video-create-gcp-service-account.mp4

(video)

Configurez le compte de service pour un VPC partagé

Pour gérer les clusters GKE qui résident dans un projet, mais qui utilisent un VPC depuis un autre projet (un VPC partagé), vous devez spécifier le compte de service Astra comme membre du projet hôte avec le rôle **Compute Network Viewer**.

Étapes

1. Depuis la console Google Cloud, allez à **IAM & Admin** et sélectionnez **comptes de service**.
2. Découvrez le compte de service Astra "les autorisations requises" puis copiez l'adresse e-mail.
3. Rendez-vous sur votre projet hôte et sélectionnez **IAM & Admin** > **IAM**.
4. Sélectionnez **Ajouter** et ajoutez une entrée pour le compte de service.
   a. **Nouveaux membres** : saisissez l'adresse électronique du compte de service.
   b. **Rôle** : sélectionnez **Compute Network Viewer**.
   c. Sélectionnez **Enregistrer**.

Résultat

L'ajout d'un cluster GKE utilisant un VPC partagé fonctionnera entièrement avec Astra.

Créez une clé de compte de service

Au lieu de fournir un nom d'utilisateur et un mot de passe à Astra Control Service, vous fournissez une clé de compte de service lorsque vous ajoutez votre premier cluster. Astra Control Service utilise la clé du compte de service pour établir l'identité du compte de service que vous venez de configurer.

La clé de compte de service est en texte brut stockée au format JSON (JavaScript Object notation). Elle contient des informations sur les ressources GCP auxquelles vous êtes autorisé à accéder.

Vous ne pouvez afficher ou télécharger le fichier JSON que lorsque vous créez la clé. Cependant, vous pouvez créer une nouvelle clé à tout moment.

Étapes

1. Rendez-vous sur Google Cloud et "créez une clé de compte de service à l'aide de la console, de la commande gcloud ou d'une autre méthode préférée".
2. Lorsque vous y êtes invité, enregistrez le fichier de clé de compte de service dans un emplacement sécurisé.

La vidéo suivante montre comment créer la clé de compte de service à partir de la console Google Cloud.

► https://docs.netapp.com/fr-fr/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Facultatif : configurez le peering réseau pour votre VPC

Si vous prévoyez d'utiliser Cloud Volumes Service pour Google Cloud comme service interne de stockage, la dernière étape consiste à configurer le peering de réseau depuis votre VPC vers Cloud Volumes Service pour Google Cloud.

Le moyen le plus simple de configurer le peering de réseau est d'obtenir les commandes gcloud directement depuis Cloud Volumes Service. Les commandes sont disponibles depuis Cloud Volumes Service lors de la création d'un nouveau système de fichiers.

Étapes

1. "Accédez aux cartes des régions mondiales NetApp BlueXP" Et identifiez le type de service que vous allez utiliser dans la région Google Cloud où se trouve votre cluster.

   Cloud Volumes Service propose deux types de services : CVS et CVS-Performance. "En savoir plus sur ces types de service".

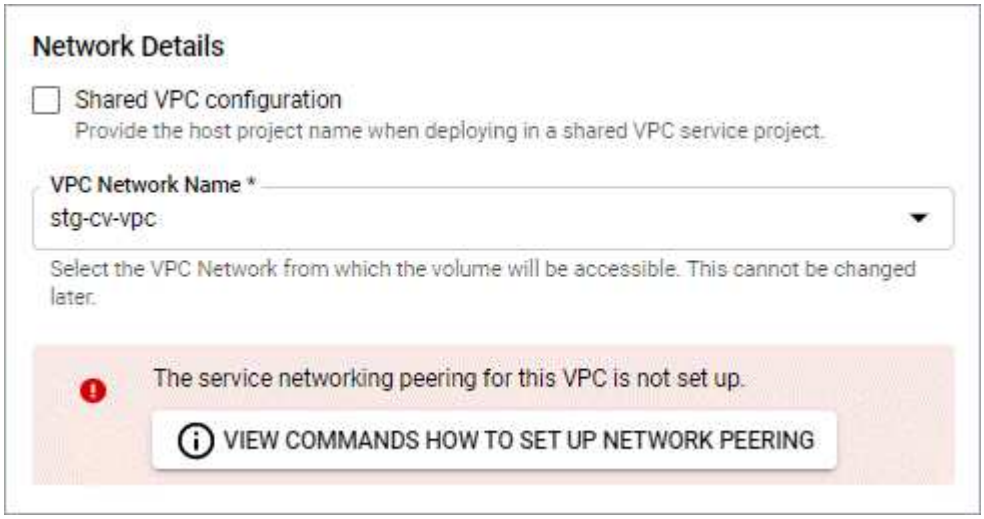
2. "Accédez à Cloud volumes dans Google Cloud Platform".
3. Sur la page **volumes**, sélectionnez **Créer**.
4. Sous **Type de service**, sélectionnez **CVS** ou **CVS-Performance**.

   Vous devez choisir le type de service adapté à votre région Google Cloud. Il s'agit du type de service que vous avez identifié à l'étape 1. Après avoir sélectionné un type de service, la liste des régions de la page est mise à jour avec les régions où ce type de service est pris en charge.

   Après cette étape, il vous suffit de saisir vos informations réseau pour obtenir les commandes.

5. Sous **région**, sélectionnez votre région et votre zone.
6. Sous **Détails du réseau**, sélectionnez votre VPC.

   Si vous n'avez pas configuré le peering de réseau, la notification suivante s'affiche :



7. Sélectionnez le bouton pour afficher les commandes de configuration du peering réseau.
8. Copiez les commandes et exécutez-les dans Cloud Shell.

Pour plus de détails sur l'utilisation de ces commandes, reportez-vous au "Service de démarrage rapide pour Cloud Volumes Service pour GCP".

"En savoir plus sur la configuration de l'accès aux services privés et la configuration du peering de réseau".

9. Une fois terminé, vous pouvez sélectionner Annuler sur la page **Créer un système de fichiers**.

   Nous avons commencé à créer ce volume uniquement pour obtenir les commandes pour le peering réseau.

Configuration de Microsoft Azure avec Azure NetApp Files

Voici quelques étapes pour préparer votre abonnement Microsoft Azure avant de gérer des clusters Azure Kubernetes Service avec Astra Control Service. Suivez ces instructions si vous prévoyez d'utiliser Azure NetApp Files en tant que système back-end de stockage.

Démarrage rapide pour la configuration d'Azure

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

[Une seule] Découvrez les exigences d'Astra Control Service pour Azure Kubernetes Service

Assurez-vous que les clusters fonctionnent correctement et qu'une version prise en charge de Kubernetes est prise en charge, que les pools de nœuds sont en ligne et exécutent Linux, etc. En savoir plus sur cette étape.

[Deux] S'inscrire à Microsoft Azure

Créez un compte Microsoft Azure. En savoir plus sur cette étape.

[Trois] Inscrivez-vous à Azure NetApp Files

Enregistrez le fournisseur de ressources NetApp. En savoir plus sur cette étape.

[Quatre] Créer un compte NetApp

Accédez à Azure NetApp Files sur le portail Azure et créez un compte NetApp. En savoir plus sur cette étape.

[Cinq] Configuration des pools de capacité

Configurez un ou plusieurs pools de capacité pour vos volumes persistants. En savoir plus sur cette étape.

[Six] Déléguer un sous-réseau à Azure NetApp Files

Déléguer un sous-réseau à Azure NetApp Files afin qu'Astra Control Service puisse créer des volumes persistants dans ce sous-réseau. En savoir plus sur cette étape.

[Sept] Créer un principal de service Azure

Créez une entité de service Azure qui a le rôle Contributor. En savoir plus sur cette étape.

[Huit] Facultatif : configurez la redondance pour les compartiments de sauvegarde Azure

Par défaut, les compartiments Astra Control Service utilisent pour stocker les sauvegardes Azure Kubernetes Service avec l'option de redondance LRS (local Redundant Storage). L'étape en option vous permet de configurer un niveau de redondance plus durable pour les compartiments Azure. En savoir plus sur cette étape.

Exigences des clusters Azure Kubernetes Service

Un cluster Kubernetes doit respecter les exigences suivantes pour que vous puissiez découvrir et gérer Astra Control Service.

Version Kubernetes

Les clusters doivent exécuter Kubernetes version 1.26 à 1.28.

Type d'image

Le type d'image pour tous les pools de nœuds doit être Linux.

État du cluster

Les clusters doivent être exécutés en état de fonctionnement et avoir au moins un nœud de travail en ligne sans nœuds de travail en panne.

Région Azure

Les clusters doivent se trouver dans une région où Azure NetApp Files est disponible. "Afficher les produits Azure par région".

Abonnement

Les clusters doivent résider dans un abonnement sur lequel Azure NetApp Files est activé. Vous choisissez un abonnement lorsque vous le souhaitez Inscrivez-vous à Azure NetApp Files.

Vnet

Prenez en compte les exigences suivantes de vnet :

- Les clusters doivent résider dans un vnet qui dispose d'un accès direct à un sous-réseau délégué Azure NetApp Files. Découvrez comment configurer un sous-réseau délégué.
- Si vos clusters Kubernetes se trouvent dans un vnet lié au sous-réseau délégué Azure NetApp Files qui est dans un autre vnet, les deux côtés de la connexion de peering doivent être en ligne.
- Notez que la limite par défaut du nombre d'adresses IP utilisées dans un réseau vnet (y compris les VNets immédiatement péré) avec Azure NetApp Files est de 1,000. "Afficher les limites de ressources Azure NetApp Files".

  Si vous êtes proche de la limite, vous avez deux options :

  - C'est possible "soumettre une demande d'augmentation de limite". Contactez votre représentant NetApp si vous avez besoin d'aide.
  - Lors de la création d'un nouveau cluster Amazon Kubernetes Service (AKS), spécifiez un nouveau réseau pour le cluster. Une fois le nouveau réseau créé, provisionnez un nouveau sous-réseau et déléguez ce sous-réseau à Azure NetApp Files.

S'inscrire à Microsoft Azure

Si vous ne possédez pas de compte Microsoft Azure, commencez par vous inscrire à Microsoft Azure.

Étapes

1. Accédez au "La page d'abonnement Azure" Pour vous abonner au service Azure.
2. Sélectionnez un plan et suivez les instructions pour terminer l'abonnement.

Inscrivez-vous à Azure NetApp Files

Accédez à Azure NetApp Files en enregistrant le fournisseur de ressources NetApp.

Étapes

1. Connectez-vous au portail Azure.
2. "Suivez la documentation Azure NetApp Files pour enregistrer le fournisseur de ressources NetApp".

Créer un compte NetApp

Créez un compte NetApp dans Azure NetApp Files.

Étape

1. "Suivez la documentation de Azure NetApp Files pour créer un compte NetApp à partir du portail Azure".

Configurez un pool de capacité

Un ou plusieurs pools de capacité sont nécessaires pour que Astra Control Service puisse provisionner les volumes persistants dans un pool de capacité. Astra Control Service ne crée pas de pools de capacité pour vous.

Prenez en compte les éléments suivants lors de la configuration de pools de capacité pour vos applications Kubernetes :

- Les pools de capacité doivent être créés dans la même région Azure où les clusters AKS seront gérés avec Astra Control Service.
- Un pool de capacité peut avoir un niveau de service Ultra, Premium ou Standard. Chacun de ces niveaux de service est conçu pour répondre à des besoins de performance très variés. Le service Astra Control est compatible avec ces trois services.

  Vous devez configurer un pool de capacité pour chaque niveau de service que vous souhaitez utiliser avec vos clusters Kubernetes.

  "En savoir plus sur les niveaux de service pour Azure NetApp Files".

- Avant de créer un pool de capacité pour les applications que vous prévoyez de protéger avec Astra Control Service, choisissez les performances et la capacité requises pour ces applications.

  Le provisionnement de la capacité adéquate permet aux utilisateurs de créer des volumes persistants selon leurs besoins. Si la capacité n'est pas disponible, les volumes persistants ne peuvent pas être provisionnés.

- Un pool de capacité Azure NetApp Files peut utiliser le type de QoS manuel ou automatique. Astra Control Service prend en charge les pools de capacité automatiques de QoS. Les pools de capacité manuels de QoS ne sont pas pris en charge.

Étape

1. "Suivez la documentation de Azure NetApp Files pour configurer un pool de capacité QoS automatique".

Déléguer un sous-réseau à Azure NetApp Files

Vous devez déléguer un sous-réseau à Azure NetApp Files afin qu'Astra Control Service puisse créer des volumes persistants dans ce sous-réseau. Notez que Azure NetApp Files vous permet d'avoir un seul sous-réseau délégué dans un vnet.

Si vous utilisez des VNets avec peering, les deux côtés de la connexion de peering doivent être en ligne : le VNet sur lequel résident vos clusters Kubernetes et le VNet sur lequel reposent le sous-réseau délégué Azure NetApp Files.

Étape

1. "Suivez la documentation Azure NetApp Files pour déléguer un sous-réseau à Azure NetApp Files".

Après avoir terminé

Attendez environ 10 minutes avant de découvrir le cluster exécuté dans le sous-réseau délégué.

Créer un principal de service Azure

Astra Control Service requiert un principal de service Azure qui est affecté au rôle de contributeur. Astra Control Service utilise ce service principal pour faciliter la gestion des données d'applications Kubernetes pour votre compte.

Un entité de service est une identité créée spécifiquement pour une utilisation avec des applications, des services et des outils. L'affectation d'un rôle principal du service restreint l'accès à des ressources Azure spécifiques.

Suivez les étapes ci-dessous pour créer une entité de service à l'aide de l'interface de ligne de commande Azure. Vous devrez enregistrer la sortie dans un fichier JSON et la fournir ultérieurement au service de contrôle Astra. "Pour plus d'informations sur l'utilisation de l'interface de ligne de commandes, consultez la documentation Azure".

Les étapes suivantes supposent que vous êtes autorisé à créer un service principal et que vous disposez du SDK Microsoft Azure (commande az) installé sur votre ordinateur.

De formation

- Le service principal doit utiliser une authentification régulière. Les certificats ne sont pas pris en charge.
- Le responsable de service doit disposer de l'accès du Contributeur ou du propriétaire à votre abonnement Azure.
- L'abonnement ou le groupe de ressources que vous choisissez pour la portée doit contenir les clusters AKS et votre compte Azure NetApp Files.

Étapes

1. Identifiez l'identifiant d'abonnement et de locataire où résident vos clusters AKS (il s'agit des clusters que vous souhaitez gérer dans le service Astra Control).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Effectuez l'une des opérations suivantes, selon que vous utilisez un abonnement complet ou un groupe de ressources :
   - Créez le principal de service, attribuez le rôle Contributor et spécifiez la portée de l'abonnement à

l'ensemble de l'abonnement où résident les clusters.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Créez le principal de service, attribuez le rôle Contributor et spécifiez le groupe de ressources où résident les clusters.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Stockez la sortie de l'interface de ligne de commandes Azure résultante en tant que fichier JSON.

   Vous devez fournir ce fichier pour qu'Astra Control Service puisse détecter vos clusters AKS et gérer les opérations de gestion des données Kubernetes. "Découvrez comment gérer les références dans le service Astra Control".

4. Facultatif : ajoutez l'ID d'abonnement au fichier JSON pour que le service de contrôle Astra renseigne automatiquement l'ID lorsque vous sélectionnez le fichier.

   Sinon, vous devrez entrer l'ID d'abonnement dans le service Astra Control lorsque vous y êtes invité.

   Exemple

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facultatif : testez votre service principal. Choisissez parmi les exemples de commandes suivants en fonction du périmètre que vos principales utilisations du service.

   Étendue de l'abonnement

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Portée du groupe de ressources

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Facultatif : configurez la redondance pour les compartiments de sauvegarde Azure

Vous pouvez configurer un niveau de redondance plus durable pour les compartiments de sauvegarde Azure. Par défaut, les compartiments Astra Control Service utilisent pour stocker les sauvegardes Azure Kubernetes Service avec l'option de redondance LRS (local Redundant Storage). Pour utiliser une option de redondance plus durable pour les compartiments Azure, vous devez effectuer les opérations suivantes :

Étapes

1. Créez un compte de stockage Azure qui utilise le niveau de redondance requis "ces instructions".
2. Créez un conteneur Azure dans le nouveau compte de stockage à l'aide de "ces instructions".
3. Ajoutez le conteneur en tant que compartiment au service Astra Control. Reportez-vous à la section "Ajouter un godet supplémentaire".
4. (Facultatif) pour utiliser le compartiment récemment créé comme compartiment par défaut pour les sauvegardes Azure, définissez-le comme compartiment par défaut pour Azure. Reportez-vous à la section "Modifier le compartiment par défaut".

Configuration de Microsoft Azure avec des disques gérés Azure

Voici quelques étapes pour préparer votre abonnement Microsoft Azure avant de gérer des clusters Azure Kubernetes Service avec Astra Control Service. Suivez ces instructions si vous prévoyez d'utiliser des disques gérés Azure en tant que système back-end.

Démarrage rapide pour la configuration d'Azure

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

[Une seule] Découvrez les exigences d'Astra Control Service pour Azure Kubernetes Service

Assurez-vous que les clusters fonctionnent correctement et qu'une version prise en charge de Kubernetes est prise en charge, que les pools de nœuds sont en ligne et exécutent Linux, etc. En savoir plus sur cette étape.

[Deux] S'inscrire à Microsoft Azure

Créez un compte Microsoft Azure. En savoir plus sur cette étape.

[Trois] Créer un principal de service Azure

Créez une entité de service Azure qui a le rôle Contributor. En savoir plus sur cette étape.

[Quatre] Configurer les détails du pilote CSI (Container Storage interface)

Vous devez configurer votre abonnement Azure et le cluster pour qu'ils fonctionnent avec les pilotes CSI. En savoir plus sur cette étape.

[Cinq] Facultatif : configurez la redondance pour les compartiments de sauvegarde Azure

Par défaut, les compartiments Astra Control Service utilisent pour stocker les sauvegardes Azure Kubernetes Service avec l'option de redondance LRS (local Redundant Storage). L'étape en option vous permet de configurer un niveau de redondance plus durable pour les compartiments Azure. En savoir plus sur cette étape.

Exigences des clusters Azure Kubernetes Service

Un cluster Kubernetes doit respecter les exigences suivantes pour que vous puissiez découvrir et gérer Astra Control Service.

Version Kubernetes

Les clusters doivent exécuter Kubernetes version 1.26 à 1.28.

Type d'image

Le type d'image pour tous les pools de nœuds doit être Linux.

État du cluster

Les clusters doivent être exécutés en état de fonctionnement et avoir au moins un nœud de travail en ligne sans nœuds de travail en panne.

Région Azure

Il est donc recommandé de choisir une région qui prend en charge Azure NetApp Files, même si vous ne l'utilisez pas comme système back-end. Ainsi, il est plus facile d'utiliser Azure NetApp Files comme système back-end de stockage si vos besoins en termes de performances évoluent. "Afficher les produits Azure par région".

Pilotes CSI

Les pilotes CSI appropriés doivent être installés sur les clusters.

S'inscrire à Microsoft Azure

Si vous ne possédez pas de compte Microsoft Azure, commencez par vous inscrire à Microsoft Azure.

Étapes

1. Accédez au "La page d'abonnement Azure" Pour vous abonner au service Azure.
2. Sélectionnez un plan et suivez les instructions pour terminer l'abonnement.

Créer un principal de service Azure

Astra Control Service requiert un principal de service Azure qui est affecté au rôle de contributeur. Astra Control Service utilise ce service principal pour faciliter la gestion des données d'applications Kubernetes pour votre compte.

Un entité de service est une identité créée spécifiquement pour une utilisation avec des applications, des services et des outils. L'affectation d'un rôle principal du service restreint l'accès à des ressources Azure spécifiques.

Suivez les étapes ci-dessous pour créer une entité de service à l'aide de l'interface de ligne de commande Azure. Vous devrez enregistrer la sortie dans un fichier JSON et la fournir ultérieurement au service de contrôle Astra. "Pour plus d'informations sur l'utilisation de l'interface de ligne de commandes, consultez la documentation Azure".

Les étapes suivantes supposent que vous êtes autorisé à créer un service principal et que vous disposez du SDK Microsoft Azure (commande az) installé sur votre ordinateur.

De formation

- Le service principal doit utiliser une authentification régulière. Les certificats ne sont pas pris en charge.
- Le responsable de service doit disposer de l'accès du Contributeur ou du propriétaire à votre abonnement Azure.
- L'abonnement ou le groupe de ressources que vous choisissez pour la portée doit contenir les clusters AKS et votre compte Azure NetApp Files.

Étapes

1. Identifiez l'identifiant d'abonnement et de locataire où résident vos clusters AKS (il s'agit des clusters que vous souhaitez gérer dans le service Astra Control).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Effectuez l'une des opérations suivantes, selon que vous utilisez un abonnement complet ou un groupe de ressources :
   - Créez le principal de service, attribuez le rôle Contributor et spécifiez la portée de l'abonnement à l'ensemble de l'abonnement où résident les clusters.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Créez le principal de service, attribuez le rôle Contributor et spécifiez le groupe de ressources où résident les clusters.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. Stockez la sortie de l'interface de ligne de commandes Azure résultante en tant que fichier JSON.

   Vous devez fournir ce fichier pour qu'Astra Control Service puisse détecter vos clusters AKS et gérer les opérations de gestion des données Kubernetes. "Découvrez comment gérer les références dans le service Astra Control".

4. Facultatif : ajoutez l'ID d'abonnement au fichier JSON pour que le service de contrôle Astra renseigne automatiquement l'ID lorsque vous sélectionnez le fichier.

   Sinon, vous devrez entrer l'ID d'abonnement dans le service Astra Control lorsque vous y êtes invité.

Exemple

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facultatif : testez votre service principal. Choisissez parmi les exemples de commandes suivants en fonction du périmètre que vos principales utilisations du service.

Étendue de l'abonnement

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Portée du groupe de ressources

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Configurer les détails du pilote CSI (Container Storage interface)

Pour utiliser des disques gérés Azure avec Astra Control Service, vous devez installer les pilotes CSI requis.

Activez la fonction de pilote CSI dans votre abonnement Azure

Avant d'installer les pilotes CSI, vous devez activer la fonction de pilote CSI dans votre abonnement Azure.

Étapes

1. Ouvrez l'interface de ligne de commande Azure.
2. Exécutez la commande suivante pour enregistrer le pilote :

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. Exécutez la commande suivante pour vous assurer que la modification est propagée :

```
az provider register -n Microsoft.ContainerService
```

Vous devez voir les résultats similaires à ce qui suit :

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Installez les pilotes de disque géré Azure CSI sur votre cluster Azure Kubernetes Service

Vous pouvez installer les pilotes Azure CSI pour terminer votre préparation.

Étape

1. Accédez à "Documentation du pilote Microsoft CSI".
2. Suivez les instructions pour installer les pilotes CSI requis.

Facultatif : configurez la redondance pour les compartiments de sauvegarde Azure

Vous pouvez configurer un niveau de redondance plus durable pour les compartiments de sauvegarde Azure. Par défaut, les compartiments Astra Control Service utilisent pour stocker les sauvegardes Azure Kubernetes Service avec l'option de redondance LRS (local Redundant Storage). Pour utiliser une option de redondance plus durable pour les compartiments Azure, vous devez effectuer les opérations suivantes :

Étapes

1. Créez un compte de stockage Azure qui utilise le niveau de redondance requis "ces instructions".
2. Créez un conteneur Azure dans le nouveau compte de stockage à l'aide de "ces instructions".
3. Ajoutez le conteneur en tant que compartiment au service Astra Control. Reportez-vous à la section "Ajouter un godet supplémentaire".
4. (Facultatif) pour utiliser le compartiment récemment créé comme compartiment par défaut pour les sauvegardes Azure, définissez-le comme compartiment par défaut pour Azure. Reportez-vous à la section "Modifier le compartiment par défaut".

Créez un compte de service Astra Control

Pour utiliser Astra Control Service, vous devez disposer d'un compte Astra Control Service associé à votre compte NetApp BlueXP. Effectuez le processus d'enregistrement d'Astra Control Service, puis, si vous ne possédez pas encore de compte BlueXP, inscrivez-vous à BlueXP pour accéder à Astra Control Service.

Créez un compte Astra Control

Avant de pouvoir vous connecter au service Astra Control, vous devez effectuer un processus d'inscription pour obtenir un compte Astra Control Service.

Lorsque vous utilisez Astra Control Service, vous gérerez vos applications à partir d'un compte. Un compte comprend les utilisateurs qui peuvent afficher et gérer les applications du compte, ainsi que vos détails de facturation.

Étapes

1. "Accédez à la page Astra Control sur BlueXP".
2. Sélectionnez **s'inscrire pour le plan gratuit**.
3. Fournissez les informations requises dans le formulaire.

   Quelques points importants à prendre en compte lorsque vous remplissez le formulaire :

   - Votre nom d'entreprise et votre adresse doivent être précis car nous les vérifions afin de répondre aux exigences de la conformité aux règlements du commerce international.
   - Le **Nom de compte Astra** est le nom du compte de service de contrôle Astra de votre entreprise. Vous verrez ce nom dans l'interface utilisateur du service de contrôle Astra. Notez que vous pouvez créer des comptes supplémentaires (jusqu'à 5), si nécessaire.
   - Dans le champ **adresse e-mail professionnelle**, si vous disposez d'un compte NetApp BlueXP, saisissez ici l'adresse e-mail que vous utilisez pour ce compte. Si vous ne possédez pas encore de compte NetApp BlueXP, utilisez l'adresse e-mail que vous entrez ici lorsque vous vous inscrivez à BlueXP.
4. Sélectionnez **Créer un compte**.

Inscrivez-vous à BlueXP

ASTRA Control Service est intégré au service d'authentification de NetApp BlueXP. Vous pouvez vous connecter à NetApp BlueXP à l'aide de vos identifiants BlueXP ou du site de support NetApp. Si vous ne possédez pas encore de compte NetApp BlueXP ou sur le site de support NetApp, inscrivez-vous à BlueXP pour accéder à Astra Control Service et aux autres services cloud de NetApp. Si vous possédez déjà un compte BlueXP ou sur le site de support NetApp et que vous avez terminé votre inscription, vous pouvez accéder à "Service Astra Control" Directement à l'aide de vos identifiants BlueXP ou du site de support NetApp.

> Vous pouvez également utiliser l'authentification unique pour vous connecter à BlueXP à l'aide d'identifiants de votre annuaire d'entreprise (identité fédérée). Pour en savoir plus, consultez le "Centre d'assistance" Puis sélectionnez **Options de connexion à Cloud Central**.

Étapes

1. Accédez à "NetApp BlueXP".
2. En haut à droite, sélectionnez **commencer**.
3. Sélectionnez **s'inscrire**.
4. Remplissez le formulaire.

   Assurez-vous que le numéro de téléphone et l'adresse e-mail que vous avez saisis sont les mêmes que ceux que vous avez utilisés dans le formulaire d'inscription à Astra Control précédent.

5. Sélectionnez **s'inscrire**.

> L'adresse e-mail que vous saisissez dans ces formulaires est destinée à votre identifiant utilisateur NetApp BlueXP. Utilisez cet ID d'utilisateur BlueXP lorsque vous créez un compte Astra Control ou lorsqu'un administrateur Astra Control vous invite à un compte Astra Control existant.

6. Attendez la réception d'un e-mail depuis NetApp BlueXP. L'e-mail provient de l'adresse saas.support@netapp.com et peut prendre plusieurs minutes. Assurez-vous de vérifier votre dossier de courrier indésirable.
7. Une fois l'e-mail reçu, sélectionnez le lien dans l'e-mail pour vérifier votre adresse e-mail.

Résultat

Vous disposez désormais d'un identifiant BlueXP actif.

Maintenant que vous êtes enregistré, vous pouvez accéder à Astra Control directement à l'aide de vos identifiants BlueXP depuis https://astra.netapp.io.

Ajoutez un cluster à Astra Control Service

Une fois votre environnement configuré, vous êtes prêt à créer un cluster Kubernetes, puis à l'ajouter à Astra Control Service. Vous pouvez ainsi utiliser Astra Control Service pour protéger vos applications sur le cluster.

Selon le type de cluster que vous devez ajouter à Astra Control Service, vous devez suivre différentes étapes pour ajouter le cluster.

- "Ajoutez un cluster géré par un fournisseur public à Astra Control Service": Utilisez ces étapes pour ajouter un cluster qui a une adresse IP publique et qui est géré par un fournisseur de cloud. Vous aurez besoin du compte principal de service, du compte de service ou du compte utilisateur du fournisseur cloud.
- "Ajoutez un cluster géré par un fournisseur privé à Astra Control Service": Procédez comme suit pour ajouter un cluster qui a une adresse IP privée et qui est géré par un fournisseur de cloud. Vous aurez besoin du compte principal de service, du compte de service ou du compte utilisateur du fournisseur cloud.
- "Ajoutez un cluster public autogéré à Astra Control Service": Utilisez ces étapes pour ajouter un cluster qui a une adresse IP publique et qui est géré par votre organisation. Vous devrez créer un fichier kubeconfig pour le cluster que vous souhaitez ajouter.
- "Ajoutez un cluster privé autogéré à Astra Control Service": Utilisez ces étapes pour ajouter un cluster qui a une adresse IP privée et qui est géré par votre organisation. Vous devrez créer un fichier kubeconfig pour le cluster que vous souhaitez ajouter.

Installez Astra Connector pour les clusters privés

ASTRA Control Service utilise Astra Connector pour activer la communication entre Astra Control Service et les clusters privés. Vous devez installer Astra Connector sur les clusters privés que vous souhaitez gérer.

ASTRA Connector prend en charge les types suivants de clusters privés :

- Amazon Elastic Kubernetes Service (EKS)

- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service sur AWS (ROSA)
- ROSA avec AWS PrivateLink
- Red Hat OpenShift Container Platform sur site

Poser le connecteur Astra

Description de la tâche

- Lorsque vous effectuez ces étapes, exécutez ces commandes sur le cluster privé que vous souhaitez gérer avec Astra Control Service.
- Si vous utilisez un hôte bastion, exécutez ces commandes à partir de la ligne de commande de l'hôte bastion.

Avant de commencer

- Vous devez accéder au cluster privé que vous souhaitez gérer avec Astra Control Service.
- Vous devez disposer des autorisations d'administrateur Kubernetes pour installer l'opérateur Astra Connector sur le cluster.

Étapes

1. Installez l'opérateur Astra Connector sur le cluster privé que vous souhaitez gérer avec Astra Control Service. Lorsque vous exécutez cette commande, le namespace `astra-connector-operator` est créé et la configuration est appliquée au namespace :

   ```
   kubectl apply -f https://github.com/NetApp/astra-connector-
   operator/releases/download/23.07.0-
   202310251519/astraconnector_operator.yaml
   ```

2. Vérifiez que l'opérateur est installé et prêt :

   ```
   kubectl get all -n astra-connector-operator
   ```

3. Obtenez un jeton API d'Astra Control. Reportez-vous à la "Documentation relative à l'automatisation d'Astra" pour obtenir des instructions.
4. Créez le namespace astra-Connector :

   ```
   kubectl create ns astra-connector
   ```

5. Créez le fichier CR du connecteur Astra et nommez-le `astra-connector-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - **<ASTRA_CONTROL_SERVICE_URL>** : l'URL de l'interface utilisateur Web d'Astra Control Service. Par exemple :

```
https://astra.netapp.io
```

- **<ASTRA_CONTROL_SERVICE_API_TOKEN>** : jeton API Astra Control que vous avez obtenu à l'étape précédente.
- **<PRIVATE_AKS_CLUSTER_NAME>**: (Clusters AKS uniquement) - le nom du cluster du cluster privé Azure Kubernetes Service. Supprimez le commentaire et remplissez cette ligne uniquement si vous ajoutez un cluster AKS privé.
- **<ASTRA_CONTROL_ACCOUNT_ID>** : obtenu à partir de l'interface utilisateur Web d'Astra Control. Sélectionnez l'icône de figure en haut à droite de la page et sélectionnez **API Access**.

```yaml
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Après avoir renseigné le `astra-connector-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-connector-cr.yaml
```

7. Vérifier que le connecteur Astra est entièrement déployé :

```
kubectl get all -n astra-connector
```

8. Vérifier que le cluster est enregistré avec Astra Control :

```
kubectl get astraconnector -n astra-connector
```

Vous devez voir les résultats similaires à ce qui suit :

```
NAME                REGISTERED   ASTRACONNECTORID
STATUS
astra-connector     true         be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```

Notez l'ASTRACONNECTORID ; vous en aurez besoin lorsque vous ajouterez le cluster à Astra Control.

Et la suite ?

Maintenant que vous avez installé Astra Connector, vous êtes prêt à ajouter votre cluster privé à Astra Control Service.

- "Ajoutez un cluster géré par un fournisseur privé à Astra Control Service": Procédez comme suit pour ajouter un cluster qui a une adresse IP privée et qui est géré par un fournisseur de cloud. Vous aurez besoin du compte principal de service, du compte de service ou du compte utilisateur du fournisseur cloud.
- "Ajoutez un cluster privé autogéré à Astra Control Service": Utilisez ces étapes pour ajouter un cluster qui a une adresse IP privée et qui est géré par votre organisation. Vous devrez créer un fichier kubeconfig pour le cluster que vous souhaitez ajouter.

Pour en savoir plus

- "Ajouter un cluster"

Ajoutez un cluster géré par le fournisseur

Ajoutez un cluster géré par un fournisseur public à Astra Control Service

Une fois que vous avez configuré votre environnement cloud, vous êtes prêt à créer un cluster Kubernetes, puis à l'ajouter à Astra Control Service.

- Créez un cluster Kubernetes
- Ajoutez le cluster à Astra Control Service
- Modifiez la classe de stockage par défaut

Créez un cluster Kubernetes

Si vous ne disposez pas encore d'un cluster, vous pouvez en créer un qui rencontre "Exigences d'Astra Control Service pour Amazon Elastic Kubernetes Service (EKS)". Si vous ne disposez pas encore d'un cluster, vous pouvez en créer un qui rencontre "Exigences d'Astra Control Service pour Google Kubernetes Engine (GKE)". Si vous ne disposez pas encore d'un cluster, vous pouvez en créer un qui rencontre "Astra Control Service exigences pour Azure Kubernetes Service (AKS) avec Azure NetApp Files" ou "Astra Control Service exigences pour Azure Kubernetes Service (AKS) avec des disques gérés Azure".

Astra Control Service prend en charge les clusters AKS qui utilisent Azure Active Directory (Azure AD) pour l'authentification et la gestion des identités. Une fois le cluster créé, suivez les instructions du "documentation officielle" Pour configurer le cluster afin d'utiliser Azure AD. Vous devez vous assurer que vos clusters répondent aux exigences de l'intégration d'Azure AD gérée par AKS.

Ajoutez le cluster à Astra Control Service

Une fois connecté au service Astra Control, la première étape consiste à commencer à gérer vos clusters. Avant d'ajouter un cluster à Astra Control Service, vous devez effectuer des tâches spécifiques et vous assurer qu'il répond à certaines exigences.

Lorsque vous gérez des clusters Azure Kubernetes Service et Google Kubernetes Engine, notez que vous disposez de deux options pour l'installation et la gestion du cycle de vie d'Astra Control Provisioner :

- Vous pouvez utiliser Astra Control Service pour gérer automatiquement le cycle de vie d'Astra Control Provisioner. Pour ce faire, assurez-vous qu'Astra Trident n'est pas installée et que Astra Control Provisioner n'est pas activé sur le cluster que vous souhaitez gérer avec Astra Control Service. Dans ce cas, Astra Control Service active automatiquement Astra Control provisionner lorsque vous commencez à gérer le cluster, et les mises à niveau d'Astra Control provisionner sont gérées automatiquement.
- Vous pouvez gérer vous-même le cycle de vie d'Astra Control Provisioner. Pour ce faire, activez Astra Control Provisioner sur le cluster avant de gérer le cluster avec Astra Control Service. Dans ce cas, Astra Control Service détecte que le mécanisme de provisionnement Astra Control est déjà activé et ne le réinstalle pas et ne gère pas les mises à niveau d'Astra Control Provisioner. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" Pour connaître les étapes à suivre, activez le mécanisme de provisionnement Astra Control.

Lorsque vous gérez des clusters Amazon Web Services avec Astra Control Service, si vous avez besoin de systèmes back-end de stockage qui ne peuvent être utilisés qu'avec Astra Control provisionner, vous devez activer manuellement le mécanisme Astra Control provisionner sur le cluster avant de le gérer avec Astra Control Service. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" Pour connaître les étapes à suivre pour activer le mécanisme de provisionnement Astra Control.

Avant de commencer

Amazon Web Services

- Vous devez disposer du fichier JSON contenant les informations d'identification de l'utilisateur IAM qui a créé le cluster. "Découvrez comment créer un utilisateur IAM".
- ASTRA Control Provisioner est requis pour Amazon FSX pour NetApp ONTAP. Si vous prévoyez d'utiliser Amazon FSX pour NetApp ONTAP en tant que back-end de stockage pour votre cluster EKS, reportez-vous aux informations concernant Astra Control provisionner du "Configuration requise pour le cluster EKS".
- (Facultatif) si vous devez fournir les informations nécessaires `kubectl` L'accès aux commandes d'un cluster à d'autres utilisateurs IAM qui ne sont pas le créateur du cluster, reportez-vous aux instructions de la "Comment puis-je fournir l'accès aux autres utilisateurs IAM et aux rôles après la création du cluster dans Amazon EKS ?".
- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Amazon Web Services. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Microsoft Azure

- Vous devez disposer du fichier JSON qui contient la sortie de l'interface de ligne de commandes Azure lorsque vous avez créé le principal de service. "Découvrez comment configurer un principal de service".

  Vous aurez également besoin de votre ID d'abonnement Azure, si vous n'avez pas ajouté le fichier JSON.

- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Microsoft Azure. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Google Cloud

- Vous devez disposer du fichier de clé de compte de service pour un compte de service disposant des autorisations requises. "Découvrez comment configurer un compte de service".
- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Google Cloud. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Étapes

1. (Facultatif) si vous ajoutez un cluster Amazon EKS ou si vous souhaitez gérer vous-même l'installation et les mises à niveau d'Astra Control Provisioner, activez Astra Control Provisioner sur le cluster. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" des étapes d'accompagnement.
2. Ouvrez l'interface utilisateur web d'Astra Control Service dans un navigateur.
3. Dans le Tableau de bord, sélectionnez **Manage Kubernetes cluster**.

   Suivez les invites pour ajouter le cluster.

4. **Fournisseur** : sélectionnez votre fournisseur de cloud, puis fournissez les informations d'identification requises pour créer une nouvelle instance de cloud ou sélectionnez une instance de cloud existante à utiliser.

5. **Amazon Web Services**: Fournissez des détails sur votre compte utilisateur Amazon Web Services IAM en téléchargeant un fichier JSON ou en collant le contenu de ce fichier JSON à partir de votre presse-papiers.

   Le fichier JSON doit contenir les informations d'identification de l'utilisateur IAM qui a créé le cluster.

6. **Microsoft Azure**: Fournissez des détails sur votre entité de service Azure en téléchargeant un fichier JSON ou en collant le contenu de ce fichier JSON à partir de votre presse-papiers.

   Le fichier JSON doit contenir la sortie de l'interface de ligne de commandes Azure lorsque vous avez créé le principal de service. Il peut également inclure votre identifiant d'abonnement afin qu'il soit automatiquement ajouté à Astra. Sinon, vous devez saisir manuellement l'ID après avoir fourni le fichier JSON.

7. **Google Cloud Platform**: Fournir le fichier de clé de compte de service soit en téléchargeant le fichier ou en collant le contenu à partir de votre presse-papiers.

   Astra Control Service utilise le compte de service pour détecter les clusters qui s'exécutent dans Google Kubernetes Engine.

8. **Autre** : cet onglet est destiné uniquement aux clusters autogérés.
   a. **Nom de l'instance de Cloud** : indiquez un nom pour la nouvelle instance de Cloud qui sera créée lorsque vous ajoutez ce cluster. En savoir plus sur "instances cloud".
   b. Sélectionnez **Suivant**.

      ASTRA Control Service affiche la liste des clusters disponibles.

   c. **Cluster** : sélectionnez un cluster dans la liste à ajouter à Astra Control Service.

      > Lorsque vous sélectionnez dans la liste des groupes, faites attention à la colonne **Eligiblity**. Si un cluster est « inéligible » ou « partiellement éligible », passez la souris sur l'état pour déterminer s'il y a un problème au niveau du cluster. Par exemple, il peut identifier que le cluster ne dispose pas d'un nœud worker.

   d. Sélectionnez **Suivant**.
   e. (Facultatif) **Storage** : si vous le souhaitez, sélectionnez la classe de stockage que les applications Kubernetes déployées sur ce cluster doivent utiliser par défaut.
9. Pour sélectionner une nouvelle classe de stockage par défaut pour le cluster, cochez la case **affecter une nouvelle classe de stockage par défaut**.
10. Sélectionnez une nouvelle classe de stockage par défaut dans la liste.

Chaque fournisseur de service de stockage cloud affiche les informations suivantes en matière de prix, de performance et de résilience :

- Cloud Volumes Service pour Google Cloud : informations sur le prix, la performance et la résilience
- Google persistent Disk : pas d'informations sur le prix, la performance ou la résilience disponibles
- Azure NetApp Files : informations sur les performances et la résilience
- Azure Managed Disks : aucun prix, performances ou résilience disponibles
- Amazon Elastic Block Store : pas d'informations disponibles sur le prix, la performance ou la résilience
- Amazon FSX pour NetApp ONTAP : aucune information disponible concernant le prix, les performances ou la résilience
- NetApp Cloud Volumes ONTAP : aucune information disponible sur le prix, les performances ou la résilience

Chaque classe de stockage peut utiliser l'un des services suivants :

- "Cloud Volumes Service pour Google Cloud"
- "Disque persistant Google"
  - "Azure NetApp Files"
  - "Disques gérés Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX pour NetApp ONTAP"
  - "NetApp Cloud Volumes ONTAP"

  En savoir plus sur "Classes de stockage pour les clusters Amazon Web Services". En savoir plus sur "Classes de stockage pour les clusters AKS". En savoir plus sur "Classes de stockage pour clusters GKE".

  a. Sélectionnez **Suivant**.
  b. **Revoir et approuver** : consultez les détails de la configuration.
  c. Sélectionnez **Ajouter** pour ajouter le cluster à Astra Control Service.

Résultat

S'il s'agit du premier cluster que vous avez ajouté pour ce fournisseur cloud, Astra Control Service crée un magasin d'objets pour le fournisseur cloud pour les sauvegardes d'applications s'exécutant sur les clusters éligibles. (Lorsque vous ajoutez des clusters suivants pour ce fournisseur de cloud, aucun magasin d'objets n'est créé.) Si vous avez spécifié une classe de stockage par défaut, Astra Control Service définit la classe de stockage par défaut que vous avez spécifiée. Pour les clusters gérés dans Amazon Web Services ou Google Cloud Platform, Astra Control Service crée également un compte d'administration sur le cluster. Ces actions peuvent prendre plusieurs minutes.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster.

Modifiez la classe de stockage par défaut avec Astra Control

Vous pouvez modifier la classe de stockage par défaut d'un cluster depuis Astra Control. Si votre cluster utilise un service back-end de stockage installé précédemment, il se peut que vous ne puissiez pas utiliser cette méthode pour modifier la classe de stockage par défaut (l'action **Set as default** n'est pas sélectionnable). Dans ce cas, vous pouvez Modifiez la classe de stockage par défaut à l'aide de la ligne de commande.

Étapes

1. Dans l'interface utilisateur du service de contrôle Astra, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster que vous souhaitez modifier.
3. Sélectionnez l'onglet **stockage**.
4. Sélectionnez la catégorie **classes de stockage**.
5. Sélectionnez le menu **actions** pour la classe de stockage que vous souhaitez définir par défaut.
6. Sélectionnez **définir comme valeur par défaut**.

Modifiez la classe de stockage par défaut à l'aide de la ligne de commande

Vous pouvez modifier la classe de stockage par défaut d'un cluster à l'aide des commandes Kubernetes. Cette méthode fonctionne quelle que soit la configuration du cluster.

Étapes

1. Connectez-vous à votre cluster Kubernetes.
2. Lister les classes de stockage de votre cluster :

```
kubectl get storageclass
```

3. Supprimez la désignation par défaut de la classe de stockage par défaut. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Sélectionnez par défaut une classe de stockage différente. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirmez la nouvelle classe de stockage par défaut :

```
kubectl get storageclass
```

Ajoutez un cluster géré par un fournisseur privé à Astra Control Service

Vous pouvez utiliser Astra Control Service pour gérer les clusters Google Kubernetes Engine (GKE) privés. Ces instructions supposent que vous avez déjà créé un cluster AKS ou OpenShift privé et préparé une méthode sécurisée pour y accéder à distance. Pour plus d'informations sur la création et l'accès à des clusters AKS ou OpenShift privés, reportez-vous à la documentation suivante :

- "Documentation Azure pour clusters AKS privés"
- "Documentation Azure pour les clusters OpenShift privés"

Vous pouvez utiliser Astra Control Service pour gérer des clusters Azure Kubernetes Service (AKS) privés ainsi que des clusters Red Hat OpenShift privés dans AKS. Ces instructions supposent que vous avez déjà créé un cluster AKS ou OpenShift privé et préparé une méthode sécurisée pour y accéder à distance. Pour plus d'informations sur la création et l'accès à des clusters AKS ou OpenShift privés, reportez-vous à la documentation suivante :

- "Documentation Azure pour clusters AKS privés"
- "Documentation Azure pour les clusters OpenShift privés"

Vous pouvez utiliser Astra Control Service pour gérer les clusters Amazon Elastic Kubernetes Service (EKS) privés. Ces instructions supposent que vous avez déjà créé un cluster EKS privé et préparé une méthode sécurisée pour y accéder à distance. Pour plus d'informations sur la création et l'accès à des clusters EKS privés, reportez-vous au "Documentation Amazon EKS".

Pour ajouter votre cluster privé à Astra Control Service, vous devez effectuer les tâches suivantes :

1. Poser le connecteur Astra
2. Configuration du stockage persistant
3. Ajoutez le cluster géré par le fournisseur privé à Astra Control Service

Poser le connecteur Astra

Avant d'ajouter un cluster privé, vous devez installer Astra Connector sur le cluster afin qu'Astra Control puisse communiquer avec lui. Reportez-vous à la section "Installez Astra Connector pour les clusters privés" pour obtenir des instructions.

Configuration du stockage persistant

Configurer le stockage persistant pour le cluster. Pour plus d'informations sur la configuration du stockage persistant, reportez-vous à la documentation de mise en route :

- "Configuration de Microsoft Azure avec Azure NetApp Files"
- "Configuration de Microsoft Azure avec des disques gérés Azure"
- "Configurer Amazon Web Services"
- "Configurez Google Cloud"

Ajoutez le cluster géré par le fournisseur privé à Astra Control Service

Vous pouvez maintenant ajouter le cluster privé à Astra Control Service.

Lorsque vous gérez des clusters Azure Kubernetes Service et Google Kubernetes Engine, notez que vous disposez de deux options pour l'installation et la gestion du cycle de vie d'Astra Control Provisioner :

- Vous pouvez utiliser Astra Control Service pour gérer automatiquement le cycle de vie d'Astra Control Provisioner. Pour ce faire, assurez-vous qu'Astra Trident n'est pas installée et que Astra Control Provisioner n'est pas activé sur le cluster que vous souhaitez gérer avec Astra Control Service. Dans ce cas, Astra Control Service active automatiquement Astra Control provisionner lorsque vous commencez à gérer le cluster, et les mises à niveau d'Astra Control provisionner sont gérées automatiquement.
- Vous pouvez gérer vous-même le cycle de vie d'Astra Control Provisioner. Pour ce faire, activez Astra Control Provisioner sur le cluster avant de gérer le cluster avec Astra Control Service. Dans ce cas, Astra Control Service détecte que le mécanisme de provisionnement Astra Control est déjà activé et ne le réinstalle pas et ne gère pas les mises à niveau d'Astra Control Provisioner. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" Pour connaître les étapes à suivre, activez le mécanisme de provisionnement Astra Control.

Lorsque vous gérez des clusters Amazon Web Services avec Astra Control Service, si vous avez besoin de systèmes back-end de stockage qui ne peuvent être utilisés qu'avec Astra Control provisionner, vous devez activer manuellement le mécanisme Astra Control provisionner sur le cluster avant de le gérer avec Astra Control Service. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" Pour connaître les étapes à suivre pour activer le mécanisme de provisionnement Astra Control.

Avant de commencer

Amazon Web Services

- Vous devez disposer du fichier JSON contenant les informations d'identification de l'utilisateur IAM qui a créé le cluster. "Découvrez comment créer un utilisateur IAM".
- ASTRA Control Provisioner est requis pour Amazon FSX pour NetApp ONTAP. Si vous prévoyez d'utiliser Amazon FSX pour NetApp ONTAP en tant que back-end de stockage pour votre cluster EKS, reportez-vous aux informations concernant Astra Control provisionner du "Configuration requise pour le cluster EKS".
- (Facultatif) si vous devez fournir les informations nécessaires `kubectl` L'accès aux commandes d'un cluster à d'autres utilisateurs IAM qui ne sont pas le créateur du cluster, reportez-vous aux instructions de la "Comment puis-je fournir l'accès aux autres utilisateurs IAM et aux rôles après la création du cluster dans Amazon EKS ?".
- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Amazon Web Services. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Microsoft Azure

- Vous devez disposer du fichier JSON qui contient la sortie de l'interface de ligne de commandes Azure lorsque vous avez créé le principal de service. "Découvrez comment configurer un principal de service".

  Vous aurez également besoin de votre ID d'abonnement Azure, si vous n'avez pas ajouté le fichier JSON.

- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Microsoft Azure. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Google Cloud

- Vous devez disposer du fichier de clé de compte de service pour un compte de service disposant des autorisations requises. "Découvrez comment configurer un compte de service".
- Si le cluster est privé, le "réseaux autorisés" Doit autoriser l'adresse IP du service de contrôle Astra :

  52.188.218.166/32

- Si vous prévoyez d'utiliser NetApp Cloud Volumes ONTAP en tant que système back-end de stockage, vous devez configurer Cloud Volumes ONTAP pour qu'il fonctionne avec Google Cloud. Consultez le Cloud Volumes ONTAP "documentation de configuration".

Étapes

1. (Facultatif) si vous ajoutez un cluster Amazon EKS ou si vous souhaitez gérer vous-même l'installation et les mises à niveau d'Astra Control Provisioner, activez Astra Control Provisioner sur le cluster. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" des étapes d'accompagnement.
2. Ouvrez l'interface utilisateur web d'Astra Control Service dans un navigateur.
3. Dans le Tableau de bord, sélectionnez **Manage Kubernetes cluster**.

   Suivez les invites pour ajouter le cluster.

4. **Fournisseur** : sélectionnez votre fournisseur de cloud, puis fournissez les informations d'identification requises pour créer une nouvelle instance de cloud ou sélectionnez une instance de cloud existante à utiliser.
5. **Amazon Web Services**: Fournissez des détails sur votre compte utilisateur Amazon Web Services IAM en téléchargeant un fichier JSON ou en collant le contenu de ce fichier JSON à partir de votre presse-papiers.

   Le fichier JSON doit contenir les informations d'identification de l'utilisateur IAM qui a créé le cluster.

6. **Microsoft Azure**: Fournissez des détails sur votre entité de service Azure en téléchargeant un fichier JSON ou en collant le contenu de ce fichier JSON à partir de votre presse-papiers.

   Le fichier JSON doit contenir la sortie de l'interface de ligne de commandes Azure lorsque vous avez créé le principal de service. Il peut également inclure votre identifiant d'abonnement afin qu'il soit automatiquement ajouté à Astra. Sinon, vous devez saisir manuellement l'ID après avoir fourni le fichier JSON.

7. **Google Cloud Platform**: Fournir le fichier de clé de compte de service soit en téléchargeant le fichier ou en collant le contenu à partir de votre presse-papiers.

   Astra Control Service utilise le compte de service pour détecter les clusters qui s'exécutent dans Google Kubernetes Engine.

8. **Autre** : cet onglet est destiné uniquement aux clusters autogérés.
   a. **Nom de l'instance de Cloud** : indiquez un nom pour la nouvelle instance de Cloud qui sera créée lorsque vous ajoutez ce cluster. En savoir plus sur "instances cloud".
   b. Sélectionnez **Suivant**.

      ASTRA Control Service affiche la liste des clusters disponibles.

   c. **Cluster** : sélectionnez un cluster dans la liste à ajouter à Astra Control Service.

      > Lorsque vous sélectionnez dans la liste des groupes, faites attention à la colonne **Eligiblity**. Si un cluster est « inéligible » ou « partiellement éligible », passez la souris sur l'état pour déterminer s'il y a un problème au niveau du cluster. Par exemple, il peut identifier que le cluster ne dispose pas d'un nœud worker.

9. Sélectionnez **Suivant**.
10. (Facultatif) **Storage** : si vous le souhaitez, sélectionnez la classe de stockage que les applications Kubernetes déployées sur ce cluster doivent utiliser par défaut.
    a. Pour sélectionner une nouvelle classe de stockage par défaut pour le cluster, cochez la case **affecter une nouvelle classe de stockage par défaut**.
    b. Sélectionnez une nouvelle classe de stockage par défaut dans la liste.

Chaque fournisseur de service de stockage cloud affiche les informations suivantes en matière de prix, de performance et de résilience :

- Cloud Volumes Service pour Google Cloud : informations sur le prix, la performance et la résilience
- Google persistent Disk : pas d'informations sur le prix, la performance ou la résilience disponibles
- Azure NetApp Files : informations sur les performances et la résilience
- Azure Managed Disks : aucun prix, performances ou résilience disponibles
- Amazon Elastic Block Store : pas d'informations disponibles sur le prix, la performance ou la résilience
- Amazon FSX pour NetApp ONTAP : aucune information disponible concernant le prix, les performances ou la résilience
- NetApp Cloud Volumes ONTAP : aucune information disponible sur le prix, les performances ou la résilience

Chaque classe de stockage peut utiliser l'un des services suivants :

- "Cloud Volumes Service pour Google Cloud"
- "Disque persistant Google"
- "Azure NetApp Files"
- "Disques gérés Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX pour NetApp ONTAP"
- "NetApp Cloud Volumes ONTAP"

  En savoir plus sur "Classes de stockage pour les clusters Amazon Web Services". En savoir plus sur "Classes de stockage pour les clusters AKS". En savoir plus sur "Classes de stockage pour clusters GKE".

c. Sélectionnez **Suivant**.

d. **Revoir et approuver** : consultez les détails de la configuration.

e. Sélectionnez **Ajouter** pour ajouter le cluster à Astra Control Service.

Résultat

S'il s'agit du premier cluster que vous avez ajouté pour ce fournisseur cloud, Astra Control Service crée un magasin d'objets pour le fournisseur cloud pour les sauvegardes d'applications s'exécutant sur les clusters éligibles. (Lorsque vous ajoutez des clusters suivants pour ce fournisseur de cloud, aucun magasin d'objets n'est créé.) Si vous avez spécifié une classe de stockage par défaut, Astra Control Service définit la classe de stockage par défaut que vous avez spécifiée. Pour les clusters gérés dans Amazon Web Services ou Google Cloud Platform, Astra Control Service crée également un compte d'administration sur le cluster. Ces actions peuvent prendre plusieurs minutes.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster.

Modifiez la classe de stockage par défaut avec Astra Control

Vous pouvez modifier la classe de stockage par défaut d'un cluster depuis Astra Control. Si votre cluster utilise un service back-end de stockage installé précédemment, il se peut que vous ne puissiez pas utiliser cette méthode pour modifier la classe de stockage par défaut (l'action **Set as default** n'est pas sélectionnable). Dans ce cas, vous pouvez Modifiez la classe de stockage par défaut à l'aide de la ligne de commande.

Étapes

1. Dans l'interface utilisateur du service de contrôle Astra, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster que vous souhaitez modifier.
3. Sélectionnez l'onglet **stockage**.
4. Sélectionnez la catégorie **classes de stockage**.
5. Sélectionnez le menu **actions** pour la classe de stockage que vous souhaitez définir par défaut.
6. Sélectionnez **définir comme valeur par défaut**.

Modifiez la classe de stockage par défaut à l'aide de la ligne de commande

Vous pouvez modifier la classe de stockage par défaut d'un cluster à l'aide des commandes Kubernetes. Cette méthode fonctionne quelle que soit la configuration du cluster.

Étapes

1. Connectez-vous à votre cluster Kubernetes.
2. Lister les classes de stockage de votre cluster :

```
kubectl get storageclass
```

3. Supprimez la désignation par défaut de la classe de stockage par défaut. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Sélectionnez par défaut une classe de stockage différente. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirmez la nouvelle classe de stockage par défaut :

```
kubectl get storageclass
```

Ajoutez un cluster autogéré

Ajoutez un cluster public autogéré à Astra Control Service

Une fois votre environnement configuré, vous êtes prêt à créer un cluster Kubernetes, puis à l'ajouter à Astra Control Service.

Un cluster autogéré est un cluster que vous provisionnez et gérez directement. ASTRA Control Service prend en charge les clusters autogérés qui s'exécutent dans un environnement de cloud public. Vous pouvez ajouter un cluster auto-géré au service Astra Control en téléchargeant un `kubeconfig.yaml` fichier. Vous devez vous assurer que le cluster répond aux exigences décrites ici.

Distributions Kubernetes prises en charge

Vous pouvez utiliser Astra Control Service pour gérer les types suivants de clusters publics et autogérés :

Distribution Kubernetes	Versions prises en charge
Kubernetes (en amont)	1.27 à 1.29
Rancher Kubernetes Engine (RKE)	RKE 1 : versions 1.24.17, 1.25.13, 1.26.8 avec Rancher Manager 2.7.9 RKE 2 : versions 1.23.16 et 1.24.13 avec Rancher Manager 2.6.13 RKE 2 : versions 1.24.17, 1.25.14, 1.26.9 avec Rancher Manager 2.7.9
Plateforme de conteneurs Red Hat OpenShift	4.12 à 4.14

Ces instructions supposent que vous avez déjà créé un cluster autogéré.

- Ajoutez le cluster à Astra Control Service
- Modifiez la classe de stockage par défaut

Ajoutez le cluster à Astra Control Service

Une fois connecté au service Astra Control, la première étape consiste à commencer à gérer vos clusters. Avant d'ajouter un cluster à Astra Control Service, vous devez effectuer des tâches spécifiques et vous assurer qu'il répond à certaines exigences.

Avant de commencer

Un cluster autogéré est un cluster que vous provisionnez et gérez directement. ASTRA Control Service prend en charge les clusters autogérés qui s'exécutent dans un environnement de cloud public. Vos clusters autogérés peuvent utiliser Astra Control Provisioner pour s'interfacer avec les services de stockage NetApp ou des pilotes Container Storage interface (CSI) pour s'interfacer avec Amazon Elastic Block Store (EBS), les disques gérés Azure et le service Google persistent Disk.

ASTRA Control Service prend en charge les clusters autogérés qui utilisent les distributions Kubernetes suivantes :

- Plateforme de conteneurs Red Hat OpenShift
- Moteur rancher Kubernetes
- Kubernetes en amont

Votre cluster autogéré doit répondre aux exigences suivantes :

- Le cluster doit être accessible via Internet.
- Si vous utilisez ou prévoyez d'utiliser le stockage activé avec des pilotes CSI, les pilotes CSI appropriés doivent être installés sur le cluster. Pour plus d'informations sur l'utilisation des pilotes CSI pour intégrer le stockage, reportez-vous à la documentation de votre service de stockage.
- Vous avez accès au fichier kubeconfig du cluster qui ne contient qu'un seul élément de contexte. Suivre "ces instructions" pour générer un fichier kubeconfig.
- Si vous ajoutez le cluster à l'aide d'un fichier kubeconfig qui fait référence à une autorité de certification privée (CA), ajoutez la ligne suivante au `cluster` section du fichier kubeconfig. Cela permet à Astra Control d'ajouter le cluster :

  ```
  insecure-skip-tls-verify: true
  ```

- **Rancher uniquement**: Lorsque vous gérez des clusters d'applications dans un environnement Rancher, modifiez le contexte par défaut du cluster d'applications dans le fichier kubeconfig fourni par Rancher pour utiliser un contexte de plan de contrôle au lieu du contexte du serveur d'API Rancher. La charge est réduite sur le serveur API Rancher et les performances sont améliorées.
- **Exigences du mécanisme de provisionnement Astra Control** : vous devez avoir un mécanisme de provisionnement Astra Control correctement configuré, y compris ses composants Astra Trident, pour gérer les clusters.
  - **Revoir les exigences de l'environnement Astra Trident** : avant d'installer ou de mettre à niveau Astra Control Provisioner, consultez le "systèmes front-end, systèmes back-end et configurations hôte pris en charge".
  - **Activer la fonctionnalité Astra Control Provisioner** : il est fortement recommandé d'installer Astra Trident 23.10 ou version ultérieure et de l'activer "Fonctionnalité de stockage avancée Astra Control Provisioner". Dans les prochaines versions, Astra Control ne prendra pas en charge Astra Trident si le mécanisme de provisionnement Astra Control n'est pas également activé.
  - **Configurer un back-end de stockage** : au moins un back-end de stockage doit l'être "Configuré dans Astra Trident" sur le cluster.
  - **Configurer une classe de stockage** : au moins une classe de stockage doit être "Configuré dans Astra Trident" sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'il s'agit de la classe de stockage **Only** qui possède l'annotation par défaut.

- **Configurer un contrôleur de snapshot de volume et installer une classe de snapshot de volume** : "Installez un contrôleur de snapshot de volume" Il est ainsi possible de créer des snapshots dans Astra Control. "Création" au moins un `VolumeSnapshotClass` Avec Astra Trident.

Étapes

1. Dans le Tableau de bord, sélectionnez **Manage Kubernetes cluster**.

   Suivez les invites pour ajouter le cluster.

2. **Fournisseur** : sélectionnez l'onglet **autre** pour ajouter des détails sur votre cluster auto-géré.
   a. **Autre**: Fournir des détails sur votre cluster auto-géré en téléchargeant un `kubeconfig.yaml` ou en collant le contenu du `kubeconfig.yaml` fichier à partir du presse-papiers.

   > Si vous créez la vôtre `kubeconfig` fichier, vous ne devez définir que **un** élément de contexte dans celui-ci. Reportez-vous à la section "Documentation Kubernetes" pour plus d'informations sur la création `kubeconfig` fichiers.

3. **Nom d'identification** : indiquez un nom pour les informations d'identification de cluster autogérées que vous téléchargez sur Astra Control. Par défaut, le nom des identifiants est automatiquement renseigné comme nom du cluster.
4. **ID de route privée** : ce champ est destiné uniquement aux clusters privés.
5. Sélectionnez **Suivant**.
6. (Facultatif) **Storage** : si vous le souhaitez, sélectionnez la classe de stockage que les applications Kubernetes déployées sur ce cluster doivent utiliser par défaut.
   a. Pour sélectionner une nouvelle classe de stockage par défaut pour le cluster, cochez la case **affecter une nouvelle classe de stockage par défaut**.
   b. Sélectionnez une nouvelle classe de stockage par défaut dans la liste.

   > Chaque fournisseur de service de stockage cloud affiche les informations suivantes en matière de prix, de performance et de résilience :
   >
   > - Cloud Volumes Service pour Google Cloud : informations sur le prix, la performance et la résilience
   > - Google persistent Disk : pas d'informations sur le prix, la performance ou la résilience disponibles
   > - Azure NetApp Files : informations sur les performances et la résilience
   > - Azure Managed Disks : aucun prix, performances ou résilience disponibles
   > - Amazon Elastic Block Store : pas d'informations disponibles sur le prix, la performance ou la résilience
   > - Amazon FSX pour NetApp ONTAP : aucune information disponible concernant le prix, les performances ou la résilience
   > - NetApp Cloud Volumes ONTAP : aucune information disponible sur le prix, les performances ou la résilience

   Chaque classe de stockage peut utiliser l'un des services suivants :

- "Cloud Volumes Service pour Google Cloud"
- "Disque persistant Google"
  - "Azure NetApp Files"
  - "Disques gérés Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX pour NetApp ONTAP"
  - "NetApp Cloud Volumes ONTAP"

    En savoir plus sur "Classes de stockage pour les clusters Amazon Web Services". En savoir plus sur "Classes de stockage pour les clusters AKS". En savoir plus sur "Classes de stockage pour clusters GKE".

c. Sélectionnez **Suivant**.

d. **Revoir et approuver** : consultez les détails de la configuration.

e. Sélectionnez **Ajouter** pour ajouter le cluster à Astra Control Service.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster.

Modifiez la classe de stockage par défaut avec Astra Control

Vous pouvez modifier la classe de stockage par défaut d'un cluster depuis Astra Control. Si votre cluster utilise un service back-end de stockage installé précédemment, il se peut que vous ne puissiez pas utiliser cette méthode pour modifier la classe de stockage par défaut (l'action **Set as default** n'est pas sélectionnable). Dans ce cas, vous pouvez Modifiez la classe de stockage par défaut à l'aide de la ligne de commande.

Étapes

1. Dans l'interface utilisateur du service de contrôle Astra, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster que vous souhaitez modifier.
3. Sélectionnez l'onglet **stockage**.
4. Sélectionnez la catégorie **classes de stockage**.
5. Sélectionnez le menu **actions** pour la classe de stockage que vous souhaitez définir par défaut.
6. Sélectionnez **définir comme valeur par défaut**.

Modifiez la classe de stockage par défaut à l'aide de la ligne de commande

Vous pouvez modifier la classe de stockage par défaut d'un cluster à l'aide des commandes Kubernetes. Cette méthode fonctionne quelle que soit la configuration du cluster.

Étapes

1. Connectez-vous à votre cluster Kubernetes.
2. Lister les classes de stockage de votre cluster :

```
kubectl get storageclass
```

3. Supprimez la désignation par défaut de la classe de stockage par défaut. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Sélectionnez par défaut une classe de stockage différente. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirmez la nouvelle classe de stockage par défaut :

```
kubectl get storageclass
```

Ajoutez un cluster privé autogéré à Astra Control Service

Une fois votre environnement configuré, vous êtes prêt à créer un cluster Kubernetes, puis à l'ajouter à Astra Control Service.

Un cluster autogéré est un cluster que vous provisionnez et gérez directement. ASTRA Control Service prend en charge les clusters autogérés qui s'exécutent dans un environnement de cloud public. Vous pouvez ajouter un cluster auto-géré au service Astra Control en téléchargeant un `kubeconfig.yaml` fichier. Vous devez vous assurer que le cluster répond aux exigences décrites ici.

Distributions Kubernetes prises en charge

Vous pouvez utiliser Astra Control Service pour gérer les types suivants de clusters privés et autogérés :

Distribution Kubernetes	Versions prises en charge
Kubernetes (en amont)	1.27 à 1.29
Rancher Kubernetes Engine (RKE)	RKE 1 : versions 1.24.17, 1.25.13, 1.26.8 avec Rancher Manager 2.7.9 RKE 2 : versions 1.23.16 et 1.24.13 avec Rancher Manager 2.6.13 RKE 2 : versions 1.24.17, 1.25.14, 1.26.9 avec Rancher Manager 2.7.9
Plateforme de conteneurs Red Hat OpenShift	4.12 à 4.14

Ces instructions supposent que vous avez déjà créé un cluster privé et préparé une méthode sécurisée pour y accéder à distance.

Pour ajouter votre cluster privé à Astra Control Service, vous devez effectuer les tâches suivantes :

1. Poser le connecteur Astra
2. Configuration du stockage persistant
3. Ajoutez le cluster privé autogéré à Astra Control Service

Poser le connecteur Astra

Avant d'ajouter un cluster privé, vous devez installer Astra Connector sur le cluster afin qu'Astra Control puisse communiquer avec lui. Reportez-vous à la section "Installez Astra Connector pour les clusters privés" pour obtenir des instructions.

Configuration du stockage persistant

Configurer le stockage persistant pour le cluster. Pour plus d'informations sur la configuration du stockage persistant, reportez-vous à la documentation de mise en route :

- "Configuration de Microsoft Azure avec Azure NetApp Files"
- "Configuration de Microsoft Azure avec des disques gérés Azure"
- "Configurer Amazon Web Services"
- "Configurez Google Cloud"

Ajoutez le cluster privé autogéré à Astra Control Service

Vous pouvez maintenant ajouter le cluster privé à Astra Control Service.

Avant de commencer

Un cluster autogéré est un cluster que vous provisionnez et gérez directement. ASTRA Control Service prend en charge les clusters autogérés qui s'exécutent dans un environnement de cloud public. Vos clusters autogérés peuvent utiliser Astra Control Provisioner pour s'interfacer avec les services de stockage NetApp ou des pilotes Container Storage interface (CSI) pour s'interfacer avec Amazon Elastic Block Store (EBS), les disques gérés Azure et le service Google persistent Disk.

ASTRA Control Service prend en charge les clusters autogérés qui utilisent les distributions Kubernetes suivantes :

- Plateforme de conteneurs Red Hat OpenShift
- Moteur rancher Kubernetes
- Kubernetes en amont

Votre cluster autogéré doit répondre aux exigences suivantes :

- Le cluster doit être accessible via Internet.
- Si vous utilisez ou prévoyez d'utiliser le stockage activé avec des pilotes CSI, les pilotes CSI appropriés doivent être installés sur le cluster. Pour plus d'informations sur l'utilisation des pilotes CSI pour intégrer le stockage, reportez-vous à la documentation de votre service de stockage.
- Vous avez accès au fichier kubeconfig du cluster qui ne contient qu'un seul élément de contexte. Suivre "ces instructions" pour générer un fichier kubeconfig.
- Si vous ajoutez le cluster à l'aide d'un fichier kubeconfig qui fait référence à une autorité de certification privée (CA), ajoutez la ligne suivante au `cluster` section du fichier kubeconfig. Cela permet à Astra Control d'ajouter le cluster :

  ```
  insecure-skip-tls-verify: true
  ```

- **Rancher uniquement**: Lorsque vous gérez des clusters d'applications dans un environnement Rancher, modifiez le contexte par défaut du cluster d'applications dans le fichier kubeconfig fourni par Rancher pour utiliser un contexte de plan de contrôle au lieu du contexte du serveur d'API Rancher. La charge est réduite sur le serveur API Rancher et les performances sont améliorées.
- **Exigences du mécanisme de provisionnement Astra Control** : vous devez avoir un mécanisme de provisionnement Astra Control correctement configuré, y compris ses composants Astra Trident, pour gérer les clusters.
  - **Revoir les exigences de l'environnement Astra Trident** : avant d'installer ou de mettre à niveau Astra Control Provisioner, consultez le "systèmes front-end, systèmes back-end et configurations hôte pris en charge".
  - **Activer la fonctionnalité Astra Control Provisioner** : il est fortement recommandé d'installer Astra Trident 23.10 ou version ultérieure et de l'activer "Fonctionnalité de stockage avancée Astra Control Provisioner". Dans les prochaines versions, Astra Control ne prendra pas en charge Astra Trident si le mécanisme de provisionnement Astra Control n'est pas également activé.
  - **Configurer un back-end de stockage** : au moins un back-end de stockage doit l'être "Configuré dans Astra Trident" sur le cluster.
  - **Configurer une classe de stockage** : au moins une classe de stockage doit être "Configuré dans Astra Trident" sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'il s'agit de la classe de stockage **Only** qui possède l'annotation par défaut.

- **Configurer un contrôleur de snapshot de volume et installer une classe de snapshot de volume** : "Installez un contrôleur de snapshot de volume" Il est ainsi possible de créer des snapshots dans Astra Control. "Création" au moins un `VolumeSnapshotClass` Avec Astra Trident.

Étapes

1. Dans le Tableau de bord, sélectionnez **Manage Kubernetes cluster**.

   Suivez les invites pour ajouter le cluster.

2. **Fournisseur** : sélectionnez l'onglet **autre** pour ajouter des détails sur votre cluster auto-géré.
3. **Autre**: Fournir des détails sur votre cluster auto-géré en téléchargeant un `kubeconfig.yaml` ou en collant le contenu du `kubeconfig.yaml` fichier à partir du presse-papiers.

   > Si vous créez la vôtre `kubeconfig` fichier, vous ne devez définir que **un** élément de contexte dans celui-ci. Reportez-vous à la section "ces instructions" pour plus d'informations sur la création `kubeconfig` fichiers.

4. **Nom d'identification** : indiquez un nom pour les informations d'identification de cluster autogérées que vous téléchargez sur Astra Control. Par défaut, le nom des identifiants est automatiquement renseigné comme nom du cluster.
5. **Identificateur de route privée** : saisissez l'identificateur de route privée que vous pouvez obtenir à partir du connecteur Astra. Si vous interrogez le connecteur Astra via le `kubectl get astraconnector -n astra-connector` l'identificateur de route privée est appelé `ASTRACONNECTORID`.

   > L'identifiant de la route privée est le nom associé à Astra Connector qui permet de gérer un cluster Kubernetes privé par Astra. Dans ce contexte, un cluster privé est un cluster Kubernetes qui n'expose pas son serveur d'API à Internet.

6. Sélectionnez **Suivant**.
7. (Facultatif) **Storage** : si vous le souhaitez, sélectionnez la classe de stockage que les applications Kubernetes déployées sur ce cluster doivent utiliser par défaut.
   a. Pour sélectionner une nouvelle classe de stockage par défaut pour le cluster, cochez la case **affecter une nouvelle classe de stockage par défaut**.
   b. Sélectionnez une nouvelle classe de stockage par défaut dans la liste.

Chaque fournisseur de service de stockage cloud affiche les informations suivantes en matière de prix, de performance et de résilience :

- Cloud Volumes Service pour Google Cloud : informations sur le prix, la performance et la résilience
- Google persistent Disk : pas d'informations sur le prix, la performance ou la résilience disponibles
- Azure NetApp Files : informations sur les performances et la résilience
- Azure Managed Disks : aucun prix, performances ou résilience disponibles
- Amazon Elastic Block Store : pas d'informations disponibles sur le prix, la performance ou la résilience
- Amazon FSX pour NetApp ONTAP : aucune information disponible concernant le prix, les performances ou la résilience
- NetApp Cloud Volumes ONTAP : aucune information disponible sur le prix, les performances ou la résilience

Chaque classe de stockage peut utiliser l'un des services suivants :

- "Cloud Volumes Service pour Google Cloud"
- "Disque persistant Google"
- "Azure NetApp Files"
- "Disques gérés Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX pour NetApp ONTAP"
- "NetApp Cloud Volumes ONTAP"

  En savoir plus sur "Classes de stockage pour les clusters Amazon Web Services". En savoir plus sur "Classes de stockage pour les clusters AKS". En savoir plus sur "Classes de stockage pour clusters GKE".

c. Sélectionnez **Suivant**.

d. **Revoir et approuver** : consultez les détails de la configuration.

e. Sélectionnez **Ajouter** pour ajouter le cluster à Astra Control Service.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster.

Modifiez la classe de stockage par défaut avec Astra Control

Vous pouvez modifier la classe de stockage par défaut d'un cluster depuis Astra Control. Si votre cluster utilise un service back-end de stockage installé précédemment, il se peut que vous ne puissiez pas utiliser cette méthode pour modifier la classe de stockage par défaut (l'action **Set as default** n'est pas sélectionnable). Dans ce cas, vous pouvez Modifiez la classe de stockage par défaut à l'aide de la ligne de commande.

Étapes

1. Dans l'interface utilisateur du service de contrôle Astra, sélectionnez **clusters**.

2. Sur la page **clusters**, sélectionnez le cluster que vous souhaitez modifier.
3. Sélectionnez l'onglet **stockage**.
4. Sélectionnez la catégorie **classes de stockage**.
5. Sélectionnez le menu **actions** pour la classe de stockage que vous souhaitez définir par défaut.
6. Sélectionnez **définir comme valeur par défaut**.

Modifiez la classe de stockage par défaut à l'aide de la ligne de commande

Vous pouvez modifier la classe de stockage par défaut d'un cluster à l'aide des commandes Kubernetes. Cette méthode fonctionne quelle que soit la configuration du cluster.

Étapes

1. Connectez-vous à votre cluster Kubernetes.
2. Lister les classes de stockage de votre cluster :

```
kubectl get storageclass
```

3. Supprimez la désignation par défaut de la classe de stockage par défaut. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Sélectionnez par défaut une classe de stockage différente. Remplacez <SC_NAME> par le nom de la classe de stockage :

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirmez la nouvelle classe de stockage par défaut :

```
kubectl get storageclass
```

Vérifiez la version d'Astra Trident

Pour ajouter un cluster autogéré qui utilise Astra Control Provisioner ou Astra Trident pour les services de stockage, assurez-vous que la version installée d'Astra Trident est la version 23.10 ou la plus récente.

Étapes

1. Déterminez la version d'Astra Trident que vous exécutez :

```
kubectl get tridentversions -n trident
```

Si Astra Trident est installé, le résultat est similaire à ce qui suit :

```
NAME      VERSION
trident   24.02.0
```

Si Astra Trident n'est pas installé, le résultat est similaire à ce qui suit :

```
error: the server doesn't have a resource type "tridentversions"
```

2. Effectuez l'une des opérations suivantes :
   - Si vous exécutez Astra Trident 23.01 ou une version antérieure, utilisez-les "instructions" Pour effectuer une mise à niveau vers une version plus récente d'Astra Trident avant de passer à Astra Control Provisioner. C'est possible "effectuer une mise à niveau directe" Vers Astra Control Provisioner 24.02 si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers Astra Control Provisioner 24.02.
   - Si vous exécutez Astra Trident 23.10 ou version ultérieure, vérifiez que le mécanisme de provisionnement Astra Control a été utilisé "activé". ASTRA Control Provisioner ne fonctionnera pas avec les versions d'Astra Control Center antérieures à 23.10. "Mettez à niveau votre mécanisme de provisionnement Astra Control" De sorte qu'il dispose de la même version que l'Astra Control Center que vous mettez à niveau pour accéder aux dernières fonctionnalités.
3. Assurez-vous que les pods fonctionnent :

```
kubectl get pods -n trident
```

4. Vérifiez si les classes de stockage utilisent les pilotes Trident Astra pris en charge. Le nom de provisionnement doit être `csi.trident.netapp.io`. Reportez-vous à l'exemple suivant :

```
kubectl get sc
```

Exemple de réponse :

```
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
```

Créez un fichier kubeconfig

Vous pouvez ajouter un cluster à Astra Control Service à l'aide d'un fichier kubeconfig. Selon le type de cluster à ajouter, vous devrez peut-être créer manuellement un fichier kubeconfig pour votre cluster en suivant des étapes spécifiques.

- Créez un fichier kubeconfig pour les clusters Amazon EKS
- Créez un fichier kubeconfig pour les clusters Red Hat OpenShift Service sur AWS (ROSA)
- Créez un fichier kubeconfig pour d'autres types de clusters

Créez un fichier kubeconfig pour les clusters Amazon EKS

Suivez ces instructions pour créer un fichier kubeconfig et un code secret de jeton permanent pour les clusters Amazon EKS. Un code secret de jeton permanent est requis pour les clusters hébergés dans EKS.

Étapes

1. Suivez les instructions de la documentation Amazon pour générer un fichier kubeconfig :

   "Création ou mise à jour d'un fichier kubeconfig pour un cluster Amazon EKS"

2. Créer un compte de service comme suit :

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

      Ajustez le nom du compte de service si nécessaire. L'espace de noms `kube-system` est nécessaire pour ces étapes. Si vous modifiez le nom du compte de service ici, vous devez appliquer les mêmes modifications dans les étapes suivantes.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Appliquer le compte de service :

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

4. Créer un `ClusterRoleBinding` fichier appelé `astracontrol-clusterrolebinding.yaml`.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system
```

5. Appliquer la liaison de rôle de cluster :

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

6. Créez un fichier secret de token de compte de service appelé `astracontrol-secret.yaml`.

```
<strong>astracontrol-secret.yaml</strong>
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
type: kubernetes.io/service-account-token
```

7. Appliquer le secret de jeton :

```
kubectl apply -f astracontrol-secret.yaml
```

8. Récupérer le secret de jeton :

```
kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d
```

9. Remplacer l' `user` Section du fichier kubeconfig AWS EKS avec le jeton, comme illustré ci-dessous :

```
user:
    token: k8s-aws-
v1.aHR0cHM6Ly9zdHMudXMtd2VzdC0yLmFtYXpvbmF3cy5jb20vP0FjdGlvbj1HZXRDYWxsZ
XJJZGVudGl0eSZWZXJzaW9uPTIwMTEtMDYtMTUmWC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQ
y1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBM1JEWDdKU0haWU9LSEQ2SyUyRjIwMjMwN
DAzJTJGdXMtd2VzdC0yJTJGc3RzJTJGYXdzNF9yZXF1ZXN0JlgtQW16LURhdGU9MjAyMzA0M
DNUMjA0MzQwWiZYLUFtei1FeHBpcmVzPTYwJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCUzQ
ngtazhzLWF3cy1pZCZYLUFtei1TaWduYXR1cmU9YjU4ZWM0NzdiM2NkZGYxNGRhNzU4MGI2Z
WQ2zY2NzI2YWIwM2UyNThjMjRhNTJjNmVhNjc4MTRlNjJkOTg2Mg
```

Créez un fichier kubeconfig pour les clusters Red Hat OpenShift Service sur AWS (ROSA)

Suivez ces instructions pour créer un fichier kubeconfig pour les clusters Red Hat OpenShift Service sur AWS (ROSA).

Étapes

1. Connectez-vous au cluster ROSA.
2. Créer un compte de service :

```
oc create sa astracontrol-service-account
```

3. Ajouter un rôle de cluster :

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-
service-account
```

4. À l'aide de l'exemple suivant, créez un fichier de configuration secret de compte de service :

```
<strong>secret-astra-sa.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Créez le secret :

```
oc create -f secret-astra-sa.yaml
```

6. Modifiez le compte de service que vous avez créé et ajoutez le nom secret du compte de service Astra Control au `secrets` section :

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

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

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

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

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-dvfcd"},
{ "name": "secret-astracontrol-service-account"}
]
```

Les indices pour chaque élément dans `secrets` la matrice commence par 0. Dans l'exemple ci-dessus, l'index de `astracontrol-service-account-dockercfg-dvfcd` serait 0 et l'index pour `secret-astracontrol-service-account` serait 1. Dans votre sortie, notez le numéro d'index du compte de service secret. Vous aurez besoin de ce numéro d'index à l'étape suivante.

8. Générez le kubeconfig comme suit :

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

```
<strong>create-kubeconfig.sh</strong>
```

```
# 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=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
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
```

9. (Facultatif) Renommer le kubeconfig pour nommer votre cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Créez un fichier kubeconfig pour d'autres types de clusters

Suivez ces instructions pour créer un fichier kubeconfig de rôle limité ou étendu pour les clusters Rancher, Kubernetes en amont et Red Hat OpenShift.

Pour les clusters gérés à l'aide de kubeconfig, vous pouvez éventuellement créer une autorisation limitée ou un rôle d'administrateur d'autorisations étendues pour Astra Control Service.

Cette procédure vous aide à créer un kubeconfig distinct si l'un des scénarios suivants s'applique à votre environnement :

- Vous souhaitez limiter les autorisations Astra Control sur les clusters qu'il gère
- Vous utilisez plusieurs contextes et ne pouvez pas utiliser le kubeconfig Astra Control par défaut configuré lors de l'installation, sinon un rôle limité avec un seul contexte ne fonctionnera pas dans votre environnement

Avant de commencer

Assurez-vous que vous disposez des éléments suivants pour le cluster que vous souhaitez gérer avant

d'effectuer la procédure suivante :

- A "version prise en charge" de kubectl est installé.
- Kubectl accès au cluster que vous envisagez d'ajouter et de gérer avec Astra Control Service

> Pour cette procédure, vous n'avez pas besoin d'un accès kubectl au cluster exécutant Astra Control Service.

- Un kubeconfig actif pour le cluster que vous avez l'intention de gérer avec des droits d'administrateur de cluster pour le contexte actif

Étapes

1. Créer un compte de service :
   a. Créez un fichier de compte de service appelé `astracontrol-service-account.yaml`.

```
<strong>astracontrol-service-account.yaml</strong>
```

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

   b. Appliquer le compte de service :

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

2. Créez l'un des rôles de cluster suivants avec des autorisations suffisantes pour qu'un cluster soit géré par Astra Control :

Rôle limité du cluster

Ce rôle contient les autorisations minimales nécessaires à la gestion d'un cluster par Astra Control :

a. Créer un `ClusterRole` fichier appelé, par exemple, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```
    - horizontalpodautoscalers
    - ingresses
    - jobs
    - namespaces
    - networkpolicies
    - persistentvolumeclaims
    - poddisruptionbudgets
    - pods
    - podtemplates
    - replicasets
    - replicationcontrollers
    - replicationcontrollers/scale
    - rolebindings
    - roles
    - secrets
    - serviceaccounts
    - services
    - statefulsets
    - tridentmirrorrelationships
    - tridentsnapshotinfos
    - volumesnapshots
    - volumesnapshotcontents
    verbs:
    - delete

  # Watch resources
  # Necessary to monitor progress
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    verbs:
    - watch

  # Update resources
  - apiGroups:
    - ""
    - build.openshift.io
    - image.openshift.io
    resources:
    - builds/details
    - replicationcontrollers
    - replicationcontrollers/scale
    - imagestreams/layers
```

```
  - imagestreamtags
  - imagetags
  verbs:
  - update
```

b. (Pour les clusters OpenShift uniquement) Ajouter les éléments suivants à la fin du `astra-admin-account.yaml` fichier :

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

c. Appliquer le rôle de cluster :

```
kubectl apply -f astra-admin-account.yaml
```

Rôle de cluster étendu

Ce rôle contient des autorisations étendues pour qu'un cluster soit géré par Astra Control. Vous pouvez utiliser ce rôle si vous utilisez plusieurs contextes et que vous ne pouvez pas utiliser le kubeconfig Astra Control par défaut configuré lors de l'installation, ou si un rôle limité avec un seul contexte ne fonctionnera pas dans votre environnement :

> Les éléments suivants `ClusterRole` Les étapes constituent un exemple Kubernetes général. Pour des instructions spécifiques à votre environnement, reportez-vous à la documentation de votre distribution Kubernetes.

a. Créer un `ClusterRole` fichier appelé, par exemple, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. Appliquer le rôle de cluster :

```
kubectl apply -f astra-admin-account.yaml
```

3. Créer la liaison de rôle cluster pour le rôle cluster vers le compte de service :

a. Créer un `ClusterRoleBinding` fichier appelé `astracontrol-clusterrolebinding.yaml`.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

b. Appliquer la liaison de rôle de cluster :

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

4. Créez et appliquez le secret de jeton :
   a. Créez un fichier secret de jeton appelé `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

   b. Appliquer le secret de jeton :

```
kubectl apply -f secret-astracontrol-service-account.yaml
```

5. Ajoutez le secret de jeton au compte de service en ajoutant son nom au `secrets` tableau (dernière ligne de l'exemple suivant) :

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

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

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

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

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Les indices pour chaque élément dans `secrets` la matrice commence par 0. Dans l'exemple ci-dessus, l'index de `astracontrol-service-account-dockercfg-48xhx` serait 0 et l'index pour `secret-astracontrol-service-account` serait 1. Dans votre sortie, notez le numéro d'index du compte de service secret. Vous aurez besoin de ce numéro d'index à l'étape suivante.

7. Générez le kubeconfig comme suit :
   a. Créer un `create-kubeconfig.sh` fichier.
   b. Remplacement `TOKEN_INDEX` au début du script suivant avec la valeur correcte.

```
<strong>create-kubeconfig.sh</strong>
```

```
# 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=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
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
```

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

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

8. (Facultatif) Renommer le kubeconfig pour nommer votre cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Et la suite ?

Maintenant que vous vous êtes connecté et que vous avez ajouté un cluster à Astra Control, vous êtes prêt à utiliser les fonctionnalités de gestion des données d'application d'Astra Control.

- "Commencez à gérer les applications"
- "Protégez vos applications"
- "Clonage des applications"
- "Configurez la facturation"
- "Inviter et gérer des utilisateurs"
- "Gérez les identifiants du fournisseur cloud"
- "Gérer les notifications"
- "Déployez une instance autogérée d'Astra Control"

Vidéos sur le service Astra Control

Consultez NetApp TV pour découvrir les dernières vidéos présentant Astra Control Service. NetApp TV inclut des vidéos qui présentent certaines fonctionnalités d'Astra Control Service ou vous montrent comment réaliser certaines tâches courantes.

"Vidéos sur le service Astra Control"

Informations sur le copyright

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

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

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