Commencez

Astra Control Service

NetApp
May 30, 2023

Table des matières

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
- Cloner une application de la phase intermédiaire 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
Quels sont les systèmes back-end pris en charge ?	• 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 ◦ Disque persistant Google ◦ Disques gérés Azure ◦ "Cloud Volumes ONTAP"	• Systèmes NetApp ONTAP AFF et FAS • "Cloud Volumes ONTAP"

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'administrateur pour l'installation "Astra Trident" 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 Trident 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 les clusters Kubernetes avec un système de stockage basé sur Trident avec un système ONTAP 9.5 et supérieur.

Dans un environnement connecté au cloud, Astra Control Center utilise Cloud Insights pour fournir des fonctionnalités avancées de surveillance et de télémétrie. En l'absence de connexion Cloud Insights, un contrôle et une télémétrie limités (7 jours de metrics) sont disponibles dans Astra Control Center, mais aussi exportés vers les outils de surveillance natifs de Kubernetes (comme Prometheus et Grafana) via des points de terminaison ouverts.

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 relative à la gamme de produits NetApp Astra"
- "Documentation relative au service après-vente Astra Control"
- "Documentation Astra Control Center"
- "Documentation Astra Trident"
- "Utilisez l'API de contrôle Astra"
- "Documentation Cloud Insights"
- "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 Cloud Central" compte.
2. Indiquez votre ID d'e-mail NetApp Cloud Central lors de la création de votre compte Astra Control "À partir de la page produit Astra".

"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 1.23 et 1.25.

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.

Astra Trident

Vous devez utiliser Astra Trident et un contrôleur Snapshot externe pour les opérations avec les systèmes back-end. Pour les installer, procédez comme suit :

1. "Installez les CRD de snapshot et le contrôleur de snapshot".
2. "Installez la dernière version d’Astra Trident".
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 1.24 et 1.25.

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 à NetApp Cloud Central's Global régions Maps" 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".

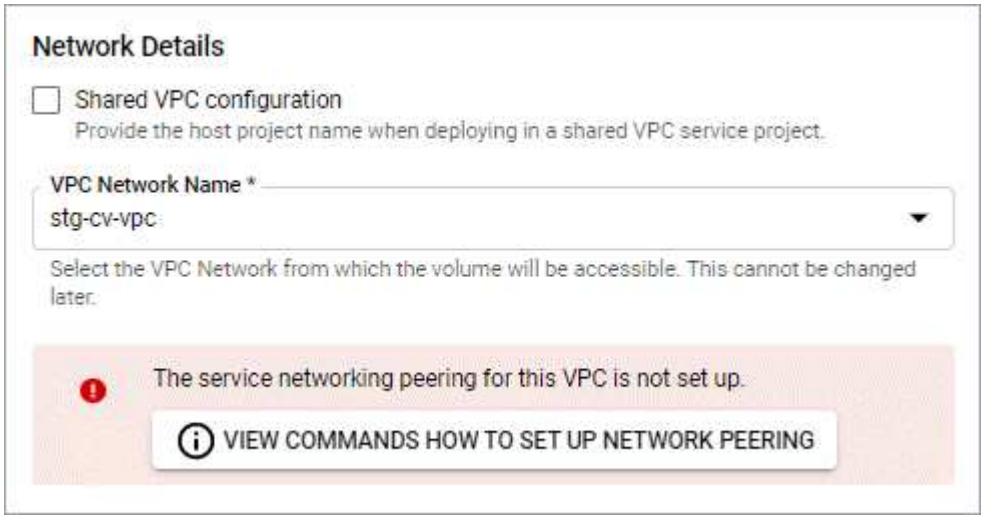
2. "Accédez à Cloud volumes dans Google Cloud Platform".
3. Sur la page **volumes**, sélectionnez **Créer**.
4. Sous **Type de service**, sélectionnez **CVS** ou **CVS-Performance**.

   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 1.23 à 1.25.

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 1.24 à 1.26.

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 Cloud Central. Suivez le processus d'inscription à Astra Control Service et, si vous ne disposez pas déjà d'un compte Cloud Central, inscrivez-vous à Cloud Central pour accéder au service Astra Control.

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 Cloud Central".
2. Sélectionnez **commencez avec Astra Control**.
3. Sélectionnez l'onglet **PLAN LIBRE**.

4. 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 Cloud Central, saisissez l'adresse e-mail que vous utilisez pour ce compte ici. Si vous ne possédez pas encore de compte NetApp Cloud Central, utilisez l'adresse e-mail que vous saisissez ici lorsque vous vous inscrivez à Cloud Central.
5. Sélectionnez **soumettre**.

Inscrivez-vous à Cloud Central

Si vous ne possédez pas encore de compte NetApp Cloud Central, inscrivez-vous sur Cloud Central pour accéder à Astra Control Service et aux autres services cloud de NetApp. Astra Control Service est intégré au service d'authentification de NetApp Cloud Central. Si vous êtes déjà titulaire d'un compte Cloud Central et que vous avez terminé votre inscription, vous pouvez y accéder "Service Astra Control" En utilisant directement vos identifiants Cloud Central.

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

Étapes

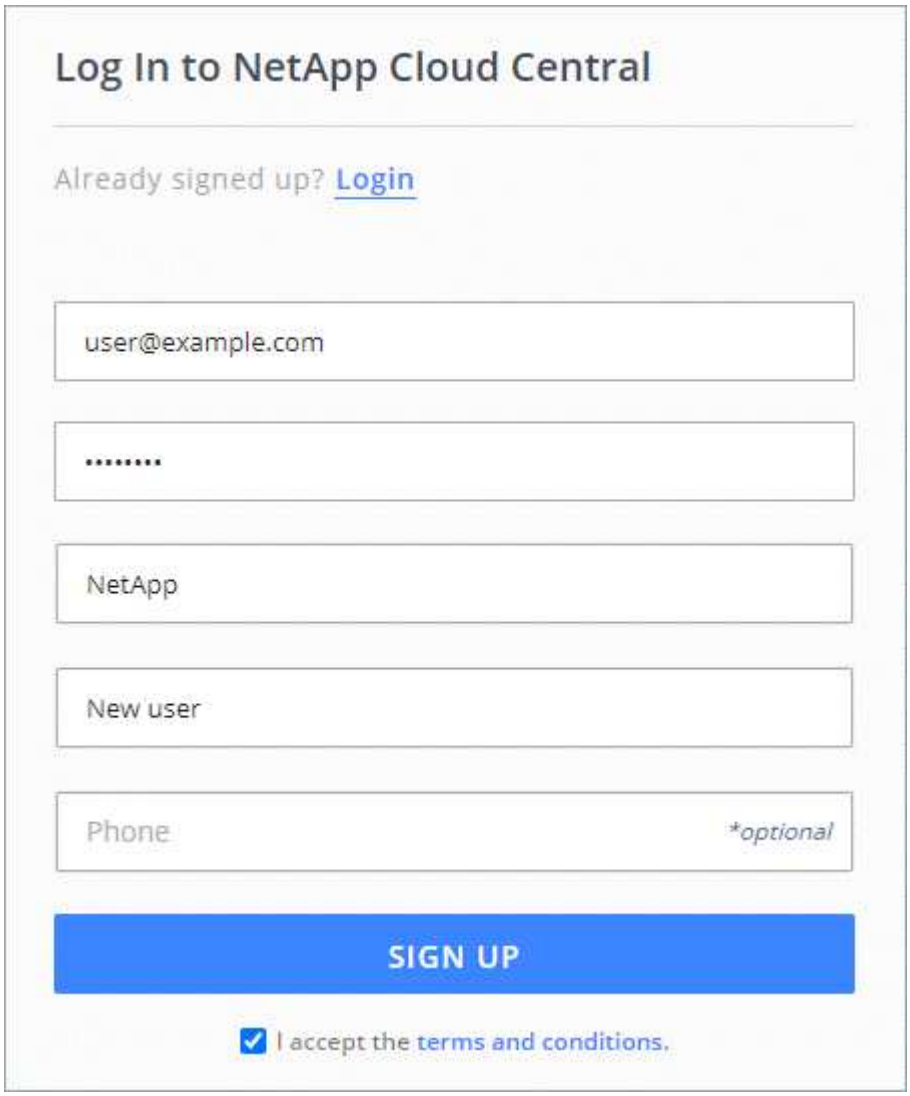
1. Accédez à "NetApp Cloud Central".

2. Dans le coin supérieur droit, sélectionnez **s'inscrire**.
3. Remplissez le formulaire.

   Assurez-vous que le numéro de téléphone et l'adresse e-mail que vous entrez ici sont identiques à ceux que vous avez utilisés dans le formulaire d'inscription au régime gratuit précédent.

4. Sélectionnez **s'inscrire**.

> L'adresse e-mail que vous saisissez dans ces formulaires correspond à votre identifiant d'utilisateur NetApp Cloud Central. Utilisez cet identifiant d'utilisateur Cloud Central lorsque vous vous inscrivez à un nouveau compte de service de contrôle Astra ou lorsqu'un administrateur du service de contrôle Astra vous invite à créer un compte de service Astra Control.



5. Attendez qu'un e-mail soit envoyé par NetApp Cloud Central. 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.
6. 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 utilisateur Cloud Central actif.

Maintenant que vous êtes inscrit, vous pouvez accéder au service Astra Control directement à l'aide de vos identifiants Cloud Central de https://astra.netapp.io.

Commencez à gérer les clusters Kubernetes à partir d'Astra Control Service

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

- Créez un cluster Kubernetes
- Commencez à gérer les clusters Kubernetes
- 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.

Clusters autogérés

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 dans Commencez à gérer les clusters Kubernetes.

Commencez à gérer les clusters Kubernetes

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

Vous devez adopter une nouvelle version du modèle 8217;Il pour la gestion de clusters gérés par un fournisseur de services cloud

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 Trident est requis pour Amazon FSX pour NetApp ONTAP. Si vous prévoyez d'utiliser Amazon FSX pour NetApp ONTAP en tant que backend de stockage de votre cluster EKS, consultez les informations d'Astra Trident dans le "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.

- Pour les clusters AKS privés, reportez-vous à la section "Gérer des clusters privés à partir d'Astra Control 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 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".

Ce que vous'll avez besoin pour les clusters autogérés

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 Trident pour s'interfacer avec les services de stockage NetApp ou les 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.
- Le cluster ne peut pas être hébergé sur votre réseau sur site ; il doit être hébergé dans un environnement de cloud public.
- 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 de rôle de cluster admin.
- **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.
- **Astra Trident** : si vous utilisez ou prévoyez d'utiliser le stockage NetApp, assurez-vous d'avoir installé la dernière version d'Astra Trident. Si Astra Trident est déjà installé, "vérifiez qu'il s'agit de la dernière version".

  > C'est possible "Déployez Astra Trident" Utilisation de l'opérateur Trident (manuellement ou à l'aide du graphique Helm) ou `tridentctl`. Avant d'installer ou de mettre à niveau Astra Trident, consultez le "systèmes front-end, systèmes back-end et configurations hôte pris en charge".

  - **Système back-end de stockage Astra Trident configuré** : au moins un système back-end de stockage Astra Trident doit l'être "configuré" sur le cluster.
  - **Classes de stockage Astra Trident configurées** : au moins une classe de stockage Astra Trident doit être "configuré" sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'une seule classe de stockage possède cette annotation.
  - **Contrôleur de snapshot de volume Astra Trident et classe de snapshot de volume installés et configurés** : le contrôleur de snapshot de volume doit être "installé" Il est ainsi possible de créer des snapshots dans Astra Control. Au moins un Astra Trident `VolumeSnapshotClass` a été "configuration" par un administrateur.

Étapes

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

   Suivez les invites pour ajouter le cluster.

2. **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.
3. **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.

4. **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.

5. **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.

6. **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.

   a. **Nom de l'instance de Cloud** (pour les clusters gérés par le fournisseur) : indiquez un nom pour la nouvelle instance de Cloud qui sera créée lors de l'ajout de ce cluster. En savoir plus sur "instances cloud".

      > Lorsque vous sélectionnez dans la liste des clusters, faites attention à l'onglet éligible. Si un avertissement s'affiche, passez le curseur de la souris sur l'avertissement pour déterminer si un problème est lié au cluster. Par exemple, il peut identifier que le cluster ne dispose pas d'un nœud worker.

   > Si vous sélectionnez un cluster marqué d'une icône « privé », il utilise des adresses IP privées et le connecteur Astra est nécessaire pour que Astra Control gère le cluster. Si vous voyez un message indiquant que vous devez installer le connecteur Astra, "reportez-vous à ces instructions" Pour installer le connecteur Astra et permettre la gestion du cluster. Après avoir installé le connecteur Astra, le cluster doit être admissible et vous pouvez procéder à l'ajout du cluster.

1. **Credential name** (pour les clusters autogérés) : indiquez un nom pour les informations d'identification du cluster autogérées que vous téléchargez sur Astra Control. Par défaut, le nom des identifiants est automatiquement renseigné comme nom du cluster.

2. (Facultatif) **ID de route privée** : saisissez l'identifiant de route privée que vous pouvez obtenir à partir du connecteur Astra.

   L'ID de 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.

3. (Facultatif) **stockage** : sélectionnez la classe de stockage que vous souhaitez déployer par défaut pour les applications Kubernetes sur ce cluster.

   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. **Review & Approve** : consultez les détails de la configuration et sélectionnez **Add cluster**.

Résultat

Pour les clusters gérés par le fournisseur : s'il s'agit du premier cluster que vous avez ajouté pour ce fournisseur de cloud, Astra Control Service crée un magasin d'objets pour le fournisseur de cloud pour les sauvegardes des applications exécutées sur des 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
```

Pour en savoir plus

- "Gérer un cluster privé"

Vérifiez la version d'Astra Trident

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

Étapes

1. Vérifiez la version d'Astra Trident.

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

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

```
NAME      VERSION
trident   22.10.0
```

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"
```

> Si Astra Trident n'est pas installé ou n'est pas à jour et que vous souhaitez que votre cluster utilise Astra Trident pour les services de stockage, vous devez installer la dernière version d'Astra Trident avant de poursuivre. Reportez-vous à la "Documentation Astra Trident" pour obtenir des instructions.

2. Assurez-vous que les pods fonctionnent :

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

3. 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 de rôle de cluster d'administration

Pour ajouter un cluster autogéré, vous devez créer un fichier kubeconfig de rôle de cluster d'administration.

Créez un fichier kubeconfig pour les clusters Rancher, Kubernetes en amont et Red Hat OpenShift

Avant d'effectuer les étapes suivantes, assurez-vous que vous disposez des éléments suivants sur votre machine :

- kubectl v1.19 ou version ultérieure installé
- Un kubeconfig actif avec des droits d'administrateur de cluster pour le contexte actif

Étapes

1. Créer un compte de service comme suit :

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

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

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

   +

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

   a. Appliquer le compte de service :

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

2. Accordez des autorisations d'administration du cluster comme suit :

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

   Ajustez les noms et espaces de noms modifiés lors de la création du compte de service, le cas échéant.

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

+

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

a. Appliquer la liaison de rôle de cluster :

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

3. 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-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

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

4. 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
```

5. (Facultatif) Renommer le kubeconfig pour nommer votre cluster. Protéger les informations d'identification du cluster.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Créez un fichier kubeconfig pour les clusters Amazon EKS

Pour créer un fichier kubeconfig pour les clusters Amazon EKS, suivez les instructions de la documentation Amazon :

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

Gérer des clusters privés à partir d'Astra Control Service

Vous pouvez utiliser Astra Control Service pour gérer des clusters Azure Kubernetes Service (AKS) privés et Red Hat OpenShift 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 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".

Poser le conducteur du connecteur Astra

Vous devez installer l'opérateur Astra Connector sur le cluster privé. Si vous utilisez un hôte bastion, exécutez ces commandes à partir de la ligne de commande de l'hôte bastion.

Étapes

1. Cloner le référentiel de l'opérateur de connecteur Astra GitHub :

```
git clone https://github.com/NetApp/astra-connector-operator.git
```

2. Modifiez les répertoires au niveau supérieur du package opérateur non compressé, afin que vous puissiez voir le `astraconnector_operator.yaml` fichier avec le `ls` commande.
3. Créez un espace de noms pour l'opérateur de connecteur Astra.

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

4. Appliquez le `astraconnector_operator.yaml` fichier dans l'espace de noms de l'opérateur.

```
kubectl apply -f astraconnector_operator.yaml -n astra-connector-
operator
```

5. Créez un namespace pour les composants du cluster privé.

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

6. Générez un jeton API de contrôle Astra en suivant les instructions de la section "Documentation relative à l'automatisation d'Astra".
7. Modifiez l'exemple de fichier de configuration dans le répertoire config/samples du référentiel opérateur du connecteur Astra afin d'inclure des valeurs spécifiques à votre environnement pour les clés suivantes :

   - `spec.natssync-client.cloud-bridge-url`
   - `spec.astra.token`
   - `spec.astra.clusterName`
   - `spec.astra.accountId`

   Par exemple :

```
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
spec:
  natssync-client:
    image: natssync-client:2.0
    cloud-bridge-url: https://<your.astra.control.service.url>
  nats:
    image: nats:2.6.1-alpine3.14
  httpproxy-client:
    image: httpproxylet:2.0
  echo-client:
    image: echo-proxylet:2.0
  imageRegistry:
    name: theotw
  astra:
    token: <Astra Control API token>
    clusterName: <your-cluster-name>
    accountId: <Astra Control account id>
    acceptEULA: yes
```

8. Appliquer la définition de ressource personnalisée (CRD) du connecteur Astra.

```
kubectl apply -f config/samples/astraconnector_v1.yaml -n astra-
connector
```

9. Vérifier l'état du connecteur Astra.

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

Vous devez voir les résultats similaires à ce qui suit :

```
NAME              REGISTERED   ASTRACONNECTORID
astra-connector   true         22b839aa-8b85-445a-85dd-0b1f53b5ea19
```

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 :

Ajoutez le cluster privé au service Astra Control

Vous pouvez maintenant ajouter le cluster privé à Astra Control Service. Suivez le workflow standard pour ajouter un cluster au service Astra Control : "Commencez à gérer les clusters Kubernetes à partir d'Astra Control Service".

Et la suite ?

Maintenant que vous vous êtes connecté et que vous avez ajouté un cluster à Astra Control, vous pouvez commencer à utiliser les fonctions de gestion des données applicatives 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"

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"

Foire aux questions concernant le service Astra Control

Cette FAQ peut vous aider si vous cherchez juste une réponse rapide à une question.

Présentation

Astra Control a pour objectif de simplifier les opérations de gestion du cycle de vie des données d'application

pour les applications natives Kubernetes. Astra Control Service prend en charge les clusters Kubernetes qui s'exécutent sur plusieurs environnements de fournisseurs cloud.

Les sections suivantes fournissent des réponses à des questions supplémentaires que vous pourriez vous poser lorsque vous utilisez Astra Control. Pour plus de précisions, veuillez contacter astra.feedback@netapp.com

Accès à Astra Control

Pourquoi dois-je fournir autant de détails lors de l'inscription à Astra Control?

Astra Control exige des renseignements précis sur le client lors de l'enregistrement. Cette information est requise pour passer par une vérification de la conformité aux règlements du commerce international (GTC, Global Trade Compliance).

Pourquoi suis-je en train d'obtenir une erreur "échec de l'enregistrement" lors de l'enregistrement pour Astra Control?

Astra Control exige que vous fournissez des renseignements précis sur le client dans la section d'intégration. Si vous avez fourni des informations incorrectes, une erreur d'enregistrement a été détectée. Les autres comptes dont vous êtes membre sont également verrouillés.

Qu'est-ce que l'URL du service de contrôle Astra?

Vous pouvez accéder au service Astra Control à l'adresse https://astra.netapp.io.

J'ai envoyé une invitation par e-mail à un collègue, mais ils ne l'ont pas reçue. Que dois-je faire?

Demandez-leur de vérifier leur dossier de courrier indésirable à partir de do-not-reply@netapp.com, ou de rechercher une "invitation" dans leur boîte de réception. Vous pouvez également supprimer l'utilisateur et tenter de les ajouter à nouveau.

J'ai mis à niveau le Plan Premium PayGo à partir du Plan gratuit. Est-ce que je serai chargé pour les 10 premiers espaces de noms?

Oui. Après la mise à niveau vers le plan Premium, Astra Control commence à vous facturer pour tous les espaces de noms gérés de votre compte.

J'ai mis à niveau le Plan Premium PayGo au milieu d'un mois. Est-ce que je serai facturé pour tout le mois?

Non, la facturation commence à partir du moment où vous avez effectué la mise à niveau vers le plan Premium.

J'utilise le Plan libre, vais-je être facturé pour les demandes de remboursement de volume persistant?

Oui, vous serez facturé pour les volumes persistants utilisés par les clusters de votre fournisseur cloud.

Enregistrement des clusters Kubernetes

Dois-je installer des pilotes CSI sur mon cluster avant de l'ajouter à Astra Control Service?

Non Une fois votre cluster ajouté à Astra Control, le service installe automatiquement le pilote Trident Container Storage interface (CSI) de NetApp sur le cluster Kubernetes. Ce pilote CSI est utilisé pour provisionner des volumes persistants pour les clusters sauvegardés par votre fournisseur cloud.

J'ai besoin d'ajouter des nœuds de travail à mon cluster après avoir ajouté à Astra Control Service. Que dois-je faire?

Il est possible d'ajouter de nouveaux nœuds workers aux pools existants ou de créer de nouveaux pools tant qu'ils ne le sont pas `COS_CONTAINERD` type d'image. Elles seront automatiquement découvertes par Astra Control. Si les nouveaux nœuds ne sont pas visibles dans Astra Control, vérifiez si les nouveaux nœuds de travail exécutent le type d'image pris en charge. Vous pouvez également vérifier l'état de santé des nouveaux nœuds workers à l'aide de la `kubectl get nodes` commande.

Enregistrement des clusters Elastic Kubernetes Service (EKS)

Puis-je ajouter un cluster privé EKS au service Astra Control?

Les clusters EKS privés ne sont pas pris en charge dans Astra Control Service pour le moment.

Enregistrement des clusters Azure Kubernetes Service (AKS)

Puis-je ajouter un cluster AKS privé au service Astra Control?

Oui, vous pouvez ajouter des clusters AKS privés au service Astra Control. Pour ajouter un cluster AKS privé, reportez-vous à la section "Commencez à gérer les clusters Kubernetes à partir d'Astra Control Service".

Puis-je utiliser Active Directory pour gérer l'authentification pour mes clusters AKS?

Oui, vous pouvez configurer vos clusters AKS pour utiliser 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.

Enregistrement des clusters Google Kubernetes Engine (GKE)

Mon cluster GKE peut-il résider sur un VPC partagé ?

Oui, Astra Control peut gérer les clusters qui résident dans un VPC partagé. "Découvrez comment configurer le compte de service Astra pour une configuration VPC partagée".

Où puis-je trouver les informations d'identification de mon compte de service sur GCP?

Une fois que vous êtes connecté au "Console Google Cloud", Les détails de votre compte de service seront dans la section **IAM et Admin**. Pour plus de détails, reportez-vous à "Comment configurer Google Cloud pour Astra Control".

Je voudrais ajouter différents clusters GKE de différents projets GCP. Est-ce pris en charge dans Astra Control?

Non, cette configuration n'est pas prise en charge. Seul un projet GCP unique est pris en charge.

Supprimer les clusters

Comment puis-je annuler correctement l'enregistrement, arrêter un cluster et supprimer les volumes associés?

1. "Gérez les applications avec Astra Control".

2. "Désenregistrer le cluster d'Astra Control".
3. "Supprimez les demandes de volume persistant".
4. Supprime le cluster.

Qu'arrive-t-il à mes applications et données après avoir retiré le cluster d'Astra Control?

La suppression d'un cluster d'Astra Control ne modifie pas la configuration du cluster (applications et stockage persistant). Toute restauration de snapshots ou de sauvegardes Astra Control effectuée sur ce cluster sera indisponible. Les données snapshot de volume stockées sur le système back-end ne seront pas supprimées. Les sauvegardes de stockage persistant créées par Astra Control resteront dans le magasin d'objets de votre fournisseur cloud, mais elles sont indisponibles pour la restauration.

Supprimez toujours un cluster d'Astra Control avant de le supprimer via GCP. La suppression d'un cluster depuis GCP alors qu'il est toujours géré par Astra Control peut générer des problèmes pour votre compte Astra Control.

Est-ce qu'Astra Trident sera désinstallé lorsque je retire un cluster d'Astra Control?

Astra Trident ne sera pas désinstallé d'un cluster lorsque vous retirez le cluster d'Astra Control.

La gestion des applications

Astra Control peut-il déployer une application?

Astra Control ne déploie pas d'applications. Les applications doivent être déployées en dehors d'Astra Control.

Je ne vois aucune des ESV de mon application liées à GCP CVS de GCP. Qu'est-ce qui ne va pas ?

L'opérateur Astra Trident définit la classe de stockage par défaut sur `netapp-cvs-perf-premium` Une fois qu'il a été ajouté à Astra Control. Lorsque les demandes de volume persistant d'une application ne sont pas liées à Cloud Volumes Service pour Google Cloud, vous pouvez effectuer plusieurs opérations :

- Courez `kubectl get sc` et vérifiez la classe de stockage par défaut.
- Vérifiez le fichier yaml ou le graphique Helm utilisé pour déployer l'application et voir si une classe de stockage différente est définie.
- GKE version 1.24 et ultérieure ne prend pas en charge les images de nœud basées sur Docker. Assurez-vous que le type d'image du nœud de travail dans GKE est `COS_CONTAINERD` Et que le montage NFS a réussi.

Que se passe-t-il pour les applications après que je les ai cessent de les gérer à partir d'Astra Control?

Toutes les sauvegardes ou tous les instantanés existants seront supprimés. Les applications et les données restent disponibles. Les opérations de gestion des données ne seront pas disponibles pour les applications non gérées ni pour les sauvegardes ou snapshots qui y appartiennent.

Les opérations de gestion des données

Où est créé Astra Control le compartiment de magasin d'objets?

Le lieu géographique du premier cluster géré détermine l'emplacement du magasin d'objets. Par exemple, si le premier cluster que vous ajoutez se trouve dans une zone européenne, le compartiment est créé dans ce même emplacement. Si nécessaire, vous pouvez "ajoutez des compartiments supplémentaires".

Il y a des instantanés dans mon compte que je n'ai pas créés. D'où viennent-ils?

Dans certains cas, Astra Control crée automatiquement un instantané dans le cadre d'un autre processus. Si ces instantanés ont plus de quelques minutes, vous pouvez les supprimer en toute sécurité.

Mon application utilise plusieurs PVS. ASTRA Control prendra-t-il des instantanés et des sauvegardes de toutes ces ESV?

Oui. Une opération d'instantané sur une application par Astra Control inclut un instantané de tous les volumes persistants liés aux demandes de volume persistant de l'application.

Puis-je gérer les instantanés pris par Astra Control directement par l'intermédiaire de mon fournisseur de cloud?

Non Les copies Snapshot et les sauvegardes effectuées par Astra Control ne peuvent être gérées qu'avec Astra Control.

Informations sur le copyright

Informations sur les marques commerciales