Configurez votre fournisseur cloud

Astra Control Service

NetApp
May 30, 2023

Table des matières

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".

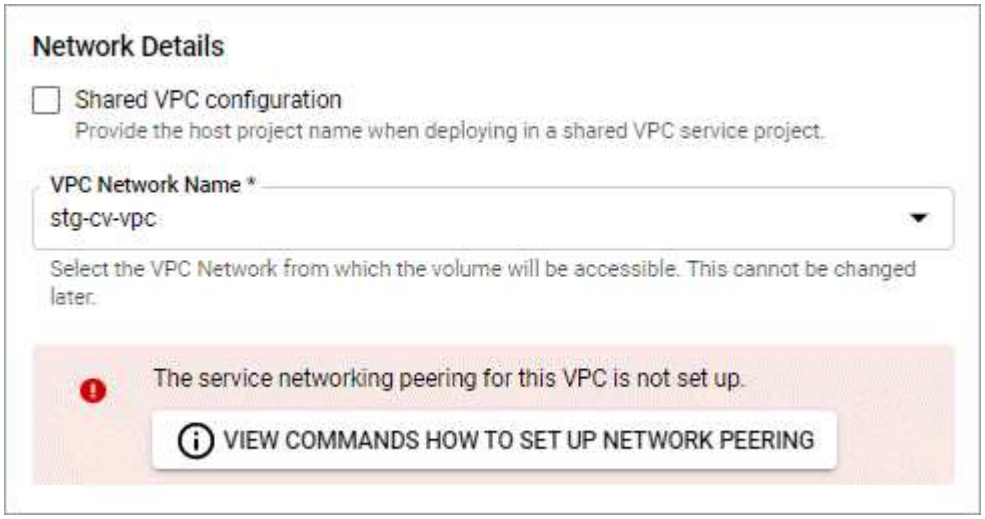
2. "Accédez à Cloud volumes dans Google Cloud Platform".
3. Sur la page **volumes**, sélectionnez **Créer**.
4. Sous **Type de service**, sélectionnez **CVS** ou **CVS-Performance**.

   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".

Informations sur le copyright

Informations sur les marques commerciales