



Commencez

Astra Control Center

NetApp
February 20, 2023

Table des matières

- Commencez 1
- Exigences du centre de contrôle Astra 1
- Démarrage rapide pour Astra Control Center 4
- Poser le centre de contrôle Astra 5
- Configurer le centre de contrôle Astra 17
- Foire aux questions pour Astra Control Center 32

Commencez

Exigences du centre de contrôle Astra

Commencez par vérifier le support de vos clusters Kubernetes, applications, licences et navigateurs Web.

Configuration générale du cluster Kubernetes

Un cluster Kubernetes doit satisfaire aux exigences générales suivantes pour que vous puissiez la découvrir et la gérer à partir d'Astra Control Center.

- **Registre d'images:** Vous devez avoir un registre d'images privé Docker existant à laquelle vous pouvez pousser les images de construction d'Astra Control Center. Vous devez avoir l'URL du registre d'images où vous allez télécharger les images, et vous devez avoir marqué les images pour le registre du conteneur privé.
- **Configuration du stockage ONTAP/Trident :** Astra Control Center requiert que la version 21.01 ou 21.04 de Trident soit déjà installée et configurée pour fonctionner avec NetApp ONTAP version 9.5 ou plus récente en tant que système back-end. Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Trident :
 - ontap-nas
 - ontap-nas-flexgroup
 - ontap-san
 - ontap-san-économie

Si vous prévoyez de gérer le cluster Kubernetes à partir d'Astra Control Center et d'utiliser le cluster pour héberger l'installation d'Astra Control Center, le cluster doit satisfaire les exigences supplémentaires suivantes :

- La version la plus récente de Kubernetes "[composant de snapshot-controller](#)" est installé
- Un Trident "[objet volumessnapshotclass](#)" a été défini par un administrateur
- Une classe de stockage Kubernetes par défaut existe sur le cluster
- Au moins une classe de stockage est configurée pour utiliser Trident
- Méthode de pointage du FQDN de Astra Control Center vers l'adresse IP externe du service Astra Control Center

Clusters OpenShift

L'Astra Control Center requiert un cluster Red Hat OpenShift Container Platform 4.6.8 ou 4.7 qui possède des classes de stockage Trident basées sur ONTAP 9.5 ou version ultérieure. Il inclut les attributs suivants :

- Au moins 300 Go de capacité de stockage ONTAP disponible
- 3 nœuds de contrôleur avec 4 cœurs de CPU, 16 Go de RAM et 120 Go de stockage disponibles chacun
- 3 nœuds workers avec au moins 12 cœurs CPU, 32 Go de RAM et 50 Go de stockage disponibles chacun
- Kubernetes version 1.19 ou 1.20
- Type de service « LoadBalancer » disponible pour le trafic d'entrée qui sera envoyé aux services du cluster OpenShift

- Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée



Ces exigences minimales supposent que Astra Control Center est la seule application qui s'exécute sur le cluster OpenShift. Si le cluster exécute des applications supplémentaires, vous devez ajuster ces exigences minimales en conséquence.

Assurez-vous que votre cluster répond au minimum requis et que vous suivez les bonnes pratiques de Kubernetes de sorte qu'Astra Control Center est hautement disponible dans votre cluster Kubernetes.



OpenShift 4.8 n'est pas pris en charge.

Lors du clonage d'applications, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Par conséquent, ONTAP doit être configuré pour permettre aux opérations de volume d'être correctement effectuées à l'aide des commandes suivantes :



1. `export-policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
2. `export-policy rule modify -policyname default -ruleindex 1 -anon 65534`



Si vous prévoyez d'ajouter un second cluster OpenShift 4.6 ou 4.7 en tant que ressource de calcul gérée, vous devez vous assurer que la fonctionnalité Snapshot des volumes Trident est activée. Voir le Trident officiel "[instructions](#)" Pour activer et tester des snapshots de volume avec Trident.

Besoins en termes de gestion des applications

Astra Control Center a les exigences suivantes en matière de gestion des applications :

- **Licensing:** Vous avez besoin d'une licence Astra Control Center pour gérer les applications à l'aide d'Astra Control Center.
- **Helm 3 :** si vous utilisez Helm pour déployer des applications, Astra Control Center requiert Helm version 3. La gestion et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.
- **Operator Management:** Astra Control Center ne prend pas en charge les applications déployées avec les opérateurs Operator Lifecycle Manager (OLM) ou les opérateurs cluster-scoped.

Accès à Internet

Vous devez déterminer si vous avez un accès externe à Internet. Par ailleurs, certaines fonctionnalités sont limitées, comme la réception de données de surveillance et de metrics depuis NetApp Cloud Insights ou l'envoi de packs de support vers le site de support NetApp.

Licence

Astra Control Center requiert une licence Astra Control Center pour bénéficier de toutes les fonctionnalités. Obtenez une licence d'évaluation ou une licence complète auprès de NetApp. Sans licence, vous ne pourrez pas :

- Définir des applications personnalisées
- Créer des snapshots ou des clones d'applications existantes
- Configuration des règles de protection des données

Si vous voulez essayer Astra Control Center, vous pouvez ["utilisez une licence d'essai gratuite de 90 jours"](#).

Type de service « LoadBalancer » pour les clusters Kubernetes sur site

Astra Control Center utilise un service de type "LoadBalancer" (svc/trafik dans l'espace de noms du Centre de contrôle Astra), et exige qu'il se voit attribuer une adresse IP externe accessible. Pour les clusters OpenShift sur site, vous pouvez utiliser ["MetalLB"](#) Pour attribuer automatiquement une adresse IP externe au service. Dans la configuration du serveur DNS interne, pointez le nom DNS choisi pour Astra Control Center vers l'adresse IP à équilibrage de charge.

Configuration réseau requise

Le cluster qui héberge Astra Control Center communique avec les ports TCP suivants. Veillez à ce que ces ports soient autorisés par le biais de pare-feu et configurez des pare-feu pour autoriser tout trafic de sortie HTTPS provenant du réseau Astra. Certains ports nécessitent une connectivité entre le cluster hébergeant le centre de contrôle Astra et chaque cluster géré (le cas échéant).

| Solution NetApp | Port | Protocole | Direction | Objectif |
|--------------------------|-------|-----------|---|---|
| Centre de contrôle Astra | 443 | HTTPS | Entrée | Accès à l'interface utilisateur/à l'API : assurez-vous que ce port est ouvert à la fois entre le cluster hébergeant Astra Control Center et chaque cluster géré |
| Centre de contrôle Astra | 9090 | HTTPS | <ul style="list-style-type: none"> • Entrée (vers le cluster hébergeant le centre de contrôle Astra) • Sortie (port aléatoire de l'adresse IP de nœud de chaque nœud worker de chaque cluster géré) | Données de mesure destinées aux consommateurs de metrics : assurez-vous que chaque cluster géré peut accéder à ce port sur le cluster hébergeant Astra Control Center |
| Trident | 34571 | HTTPS | Entrée | Communication avec le pod de nœuds |
| Trident | 9220 | HTTP | Entrée | Terminal de metrics |

Navigateurs Web pris en charge

Astra Control Center prend en charge les versions récentes de Firefox, Safari et Chrome avec une résolution minimale de 1280 x 720.

Et la suite

Afficher le ["démarrage rapide"](#) présentation.

Démarrage rapide pour Astra Control Center

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

Essayez-le ! Si vous voulez essayer Astra Control Center, vous pouvez utiliser une licence d'évaluation de 90 jours. Voir ["informations de licence"](#) pour plus d'informations.

1

Vérifiez la configuration des clusters Kubernetes

- Astra fonctionne avec les clusters Kubernetes avec un système back-end de stockage ONTAP configuré avec Trident.
- Les clusters doivent fonctionner correctement, avec au moins trois nœuds de travail en ligne.
- Le cluster doit exécuter Kubernetes.

["En savoir plus sur les exigences du centre de contrôle Astra"](#).

2

Téléchargez et installez Astra Control Center

- Téléchargez le centre de contrôle Astra sur le site de support NetApp.
- Installez Astra Control Center dans votre environnement local.
- Découvrez votre configuration Trident sur le système back-end de stockage ONTAP.

Dans notre première version, vous installez les images sur un registre OpenShift ou utilisez votre registre local.

["En savoir plus sur l'installation d'Astra Control Center"](#).

3

Effectuez certaines tâches de configuration initiales

- Ajouter une licence.
- Ajoutez un cluster Kubernetes et Astra Control Center découverte des détails.
- Ajouter un système back-end de stockage ONTAP.
- Vous pouvez également ajouter un compartiment de magasin d'objets qui stockera les sauvegardes de vos applications.

["En savoir plus sur le processus de configuration initiale"](#).

4

Utilisez Astra Control Center

Après avoir terminé la configuration du centre de contrôle Astra, voici ce que vous pourriez faire :

- Gérer une application. "[En savoir plus sur la gestion des applications](#)".
- Vous pouvez également vous connecter à NetApp Cloud Insights pour afficher des mesures sur l'état de santé de votre système, la capacité et le débit dans l'interface utilisateur de l'Astra Control Center. "[En savoir plus sur la connexion à Cloud Insights](#)".

5

Continuez à partir de ce démarrage rapide

["Poser le centre de contrôle Astra"](#).

Trouvez plus d'informations

- "[Utilisez l'API Astra](#)"

Poser le centre de contrôle Astra

Pour installer le centre de contrôle Astra, procédez comme suit :

- [Poser le centre de contrôle Astra](#)
- <https://docs.netapp.com/fr-fr/astra-control-center-2108/Connectez-vous-à-l&.html#8217;interface-utilisateur-du-centre-de-contrôle-Astra>

Poser le centre de contrôle Astra

Pour installer Astra Control Center, téléchargez le bundle d'installation sur le site de support NetApp et exécutez une série de commandes pour installer l'opérateur d'Astra Control Center et le centre de contrôle d'Astra dans votre environnement. Vous pouvez utiliser cette procédure pour installer Astra Control Center dans des environnements connectés à Internet ou équipés d'un filtre à air.

Ce dont vous avez besoin

- "[Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center](#)".
- Depuis votre cluster OpenShift, assurez-vous que tous les opérateurs de clusters sont en état sain (`available est true`) :

```
oc get clusteroperators
```

- Depuis votre cluster OpenShift, assurez-vous que tous les services d'API sont en état sain (`available est true`) :

```
oc get apiservices
```

Description de la tâche

La procédure d'installation d'Astra Control Center est la suivante :

- Installe les composants Astra dans le `netapp-acc` (ou espace de nom personnalisé).
- Crée un compte par défaut.
- Définit une adresse e-mail d'utilisateur administratif par défaut et un mot de passe unique par défaut de `ACC-<UUID_of_installation>` Pour cet exemple de centre de contrôle Astra. Ce rôle est attribué à cet utilisateur dans le système et est nécessaire pour la première connexion à l'interface utilisateur.
- Vous aide à déterminer que toutes les POD Astra Control Center sont en cours d'exécution.
- Installe l'interface utilisateur Astra.



Les commandes Podman peuvent être utilisées à la place des commandes Docker si vous utilisez le référentiel Podman de Red Hat.

Étapes

1. Téléchargez le pack Astra Control Center (`astra-control-center-[version].tar.gz`) du "[Site de support NetApp](#)".
2. Téléchargez le code postal des certificats et clés Astra Control Center à l'adresse "[Site de support NetApp](#)".
3. (Facultatif) utilisez la commande suivante pour vérifier la signature du pack :

```
openssl dgst -sha256 -verify astra-control-center[version].pub  
-signature <astra-control-center[version].sig astra-control-  
center[version].tar.gz
```

4. Extraire les images :

```
tar -vzxzf astra-control-center-[version].tar.gz
```

5. Passez au répertoire Astra.

```
cd astra-control-center-[version]
```

6. Ajoutez les fichiers du répertoire d'images de l'Astra Control Center à votre registre local.



Voir un exemple de script pour le chargement automatique des images ci-dessous.

- a. Connectez-vous à votre registre Docker :

```
docker login [Docker_registry_path]
```

- b. Chargez les images dans Docker.

c. Marquez les images.

d. Envoyez les images dans votre registre local.

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
  the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
  image: //'')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

7. (Pour les registres avec des exigences d'authentification uniquement) si vous utilisez un registre qui nécessite une authentification, vous devez procéder comme suit :

a. Créer le `netapp-acc-operator` espace de noms :

```
kubectl create ns netapp-acc-operator
```

Réponse :

```
namespace/netapp-acc-operator created
```

b. Créez un secret pour le `netapp-acc-operator` espace de noms. Ajoutez des informations sur Docker et exécutez la commande suivante :

```
kubectl create secret docker-registry astra-registry-cred -n netapp-
acc-operator --docker-server=[Docker_registry_path] --docker
-username=[username] --docker-password=[token]
```

Exemple de réponse :

```
secret/astra-registry-cred created
```

c. Créer le `netapp-acc` (ou espace de nom personnalisé).

```
kubectl create ns [netapp-acc or custom]
```

Exemple de réponse :

```
namespace/netapp-acc created
```

- d. Créez un secret pour le netapp-acc (ou espace de nom personnalisé). Ajoutez des informations sur Docker et exécutez la commande suivante :

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom] --docker-server=[Docker_registry_path] --docker-username=[username] --docker-password=[token]
```

Réponse

```
secret/astra-registry-cred created
```

8. Modifiez le yaml de déploiement de l'opérateur Astra Control Center (`astra_control_center_operator_deploy.yaml`) pour faire référence à votre registre local et à votre secret.

```
vim astra_control_center_operator_deploy.yaml
```

- a. Si vous utilisez un registre qui nécessite une authentification, remplacez la ligne par défaut de `imagePullSecrets: []` avec les éléments suivants :

```
imagePullSecrets:  
- name: astra-registry-cred
```

- b. Changer `[Docker_registry_path]` pour le `kube-rbac-prox` image dans le chemin du registre où vous avez poussé les images à l'étape précédente.
- c. Changer `[Docker_registry_path]` pour le `acc-operator-controller-manager` image dans le chemin du registre où vous avez poussé les images à l'étape précédente.

```

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: [Docker_registry_path]/kube-rbac-proxy:v0.5.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          command:
            - /manager
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
          image: [Docker_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
      imagePullSecrets: []

```

9. Modifiez le fichier de ressources personnalisées (CR) Astra Control Center (astra_control_center_min.yaml):

```
vim astra_control_center_min.yaml
```



Si d'autres personnalisations sont nécessaires pour votre environnement, vous pouvez l'utiliser `astra_control_center.yaml` En tant que CR alternatif. `astra_control_center_min.yaml` Est le CR par défaut et convient à la plupart des installations.



Les propriétés configurées par le CR ne peuvent pas être modifiées après le déploiement initial du centre de contrôle Astra.

- a. Changer `[Docker_registry_path]` vers le chemin du registre où vous avez poussé les images à l'étape précédente.
- b. Modifiez le `accountName` chaîne du nom que vous souhaitez associer au compte.
- c. Modifiez le `astraAddress` Chaîne du FQDN que vous souhaitez utiliser dans votre navigateur pour accéder à Astra. Ne pas utiliser `http://` ou `https://` dans l'adresse. Copier ce FQDN pour l'utiliser dans un [plus tard](#).
- d. Modifiez le `email` chaîne à l'adresse d'administrateur initiale par défaut. Copiez cette adresse e-mail pour l'utiliser dans un [plus tard](#).
- e. Changer `enrolled` Pour AutoSupport à `false` pour les sites sans connexion internet ou sans conservation `true` pour les sites connectés.
- f. (Facultatif) Ajouter un prénom `firstName` et nom `lastName` de l'utilisateur associé au compte. Vous pouvez effectuer cette étape maintenant ou plus tard dans l'interface utilisateur.
- g. (Facultatif) modifiez le `storageClass` Valeur ajoutée pour une autre ressource de stockage Trident si votre installation l'exige.
- h. Si vous n'utilisez pas de registre nécessitant une autorisation, supprimez le `secret` ligne.

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[Docker_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

10. Poser le conducteur du centre de commande Astra :

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Exemple de réponse :

```
namespace/netapp-acc-operator created
customresourcedefinition.apixtensions.k8s.io/astracontrolcenters.astra.
netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

11. Si vous ne l'avez pas déjà fait dans une étape précédente, créez le netapp-acc (ou personnalisée) espace de noms :

```
kubectl create ns [netapp-acc or custom]
```

Exemple de réponse :

```
namespace/netapp-acc created
```

12. Exécutez le correctif suivant pour corriger le problème "[liaison de rôle de cluster](#)".

13. Poser le centre de contrôle Astra dans le netapp-acc (ou votre espace de noms personnalisé) :

```
kubectl apply -f astra_control_center_min.yaml -n [netapp-acc or custom]
```

Exemple de réponse :

```
astracontrolcenter.astra.netapp.io/astra created
```

14. Vérifiez que tous les composants du système sont correctement installés.

```
kubectl get pods -n [netapp-acc or custom]
```

Chaque pod doit avoir un statut de `Running`. Le déploiement des modules du système peut prendre plusieurs minutes.

Exemple de réponse :

| NAME | READY | STATUS | RESTARTS |
|--|-------|---------|----------|
| AGE | | | |
| acc-helm-repo-5fdfff786f-gkv6z 4m58s | 1/1 | Running | 0 |
| activity-649f869bf7-jn5gs 3m14s | 1/1 | Running | 0 |
| asup-79846b5fdc-s9s97 3m10s | 1/1 | Running | 0 |
| authentication-84c78f5cf4-qhx9t 118s | 1/1 | Running | 0 |
| billing-9b8496787-v8rzv 2m54s | 1/1 | Running | 0 |
| bucket-service-5fb876d9d5-wkfvz 3m26s | 1/1 | Running | 0 |
| cloud-extension-f9f4f59c6-dz6s6 3m | 1/1 | Running | 0 |
| cloud-insights-service-5676b8c6d4-6q7lv 2m52s | 1/1 | Running | 0 |
| composite-compute-7dcc9c6d6c-lxdr6 2m50s | 1/1 | Running | 0 |
| composite-volume-74dbfd7577-cd42b 3m2s | 1/1 | Running | 0 |
| credentials-75dbf46f9d-5qm2b 3m32s | 1/1 | Running | 0 |
| entitlement-6cf875cb48-gkvhp 3m12s | 1/1 | Running | 0 |
| features-74fd97bb46-vss2n 3m6s | 1/1 | Running | 0 |
| fluent-bit-ds-2g9jb 113s | 1/1 | Running | 0 |
| fluent-bit-ds-5tg5h 113s | 1/1 | Running | 0 |
| fluent-bit-ds-qfxb8 | 1/1 | Running | 0 |

| | | | |
|--|-----|---------|---|
| 113s | | | |
| graphql-server-7769f98b86-p4qrv | 1/1 | Running | 0 |
| 90s | | | |
| identity-566c566cd5-ntfj6 | 1/1 | Running | 0 |
| 3m16s | | | |
| influxdb2-0 | 1/1 | Running | 0 |
| 4m43s | | | |
| krakend-5cb8d56978-44q66 | 1/1 | Running | 0 |
| 93s | | | |
| license-66cbbc6f48-27kgf | 1/1 | Running | 0 |
| 3m4s | | | |
| login-ui-584f7fd84b-dmdrp | 1/1 | Running | 0 |
| 87s | | | |
| loki-0 | 1/1 | Running | 0 |
| 4m44s | | | |
| metrics-ingestion-service-6dcfddf45f-mhnhv | 1/1 | Running | 0 |
| 3m8s | | | |
| monitoring-operator-78d67b4d4-nxs6v | 2/2 | Running | 0 |
| 116s | | | |
| nats-0 | 1/1 | Running | 0 |
| 4m40s | | | |
| nats-1 | 1/1 | Running | 0 |
| 4m26s | | | |
| nats-2 | 1/1 | Running | 0 |
| 4m15s | | | |
| nautilus-9b664bc55-rn9t8 | 1/1 | Running | 0 |
| 2m56s | | | |
| openapi-dc5ddfb7d-6q8vh | 1/1 | Running | 0 |
| 3m20s | | | |
| polaris-consul-consul-5tjs7 | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-consul-consul-5wbnx | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-consul-consul-bfv17 | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-consul-consul-server-0 | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-consul-consul-server-1 | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-consul-consul-server-2 | 1/1 | Running | 0 |
| 4m43s | | | |
| polaris-mongodb-0 | 2/2 | Running | 0 |
| 4m49s | | | |
| polaris-mongodb-1 | 2/2 | Running | 0 |
| 4m22s | | | |
| polaris-mongodb-arbiter-0 | 1/1 | Running | 0 |

```

4m49s
polaris-ui-6648875998-75d98          1/1      Running  0
92s
polaris-vault-0                      1/1      Running  0
4m41s
polaris-vault-1                      1/1      Running  0
4m41s
polaris-vault-2                      1/1      Running  0
4m41s
storage-backend-metrics-69546f4fc8-m71fj 1/1      Running  0
3m22s
storage-provider-5d46f755b-qfv89     1/1      Running  0
3m30s
support-5dc579865c-z4pwq            1/1      Running  0
3m18s
telegraf-ds-4452f                   1/1      Running  0
113s
telegraf-ds-gnqxl                    1/1      Running  0
113s
telegraf-ds-jhw74                    1/1      Running  0
113s
telegraf-rs-gg6m4                    1/1      Running  0
113s
telemetry-service-6dcc875f98-zft26   1/1      Running  0
3m24s
tenancy-7f7f77f699-q716w            1/1      Running  0
3m28s
traefik-769d846f9b-c9crt             1/1      Running  0
83s
traefik-769d846f9b-l9n4k             1/1      Running  0
67s
trident-svc-8649c8bfc5-pdj79         1/1      Running  0
2m57s
vault-controller-745879f98b-49c5v    1/1      Running  0
4m51s

```

15. (Facultatif) pour vous assurer que l'installation est terminée, vous pouvez regarder le `acc-operator` journaux utilisant la commande suivante.

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```

16. Lorsque tous les pods s'exécutent, vérifiez que l'installation est réussie en récupérant l'instance `AstrakControlCenter` installée par l'opérateur ACC.


```
kubectl get acc -o yaml -n netapp-acc
```

17. Vérifier le `status.deploymentState` dans le champ de réponse pour le `Deployed` valeur. Si le déploiement a échoué, un message d'erreur s'affiche à la place.



Vous utiliserez le `uuid` à l'étape suivante.

```

apiVersion: v1
items:
- apiVersion: astra.netapp.io/v1
  kind: AstraControlCenter
  metadata:
    creationTimestamp: "2021-07-28T21:36:49Z"
    finalizers:
    - astracontrolcenter.netapp.io/finalizer
  generation: 1
  name: astra
  namespace: netapp-acc
  resourceVersion: "27797604"
  selfLink: /apis/astra.netapp.io/v1/namespaces/netapp-
acc/astracontrolcenters/astra
  uid: 61cd8b65-047b-431a-ba35-510afcb845f1
  spec:
    accountName: Example
    astraAddress: astra.example.com
    astraResourcesScaler: "Off"
    astraVersion: 21.08.52
    autoSupport:
      enrolled: false
    email: admin@example.com
    firstName: SRE
    lastName: Admin
    imageRegistry:
      name: registry_name/astra
  status:
    certManager: deploy
    deploymentState: Deployed
    observedGeneration: 1
    observedVersion: 21.08.52
    postInstall: Complete
    uuid: c49008a5-4ef1-4c5d-a53e-830daf994116
  kind: List
  metadata:
    resourceVersion: ""
    selfLink: ""

```

18. Pour obtenir le mot de passe unique que vous utiliserez lorsque vous vous connecterez à Astra Control Center, copiez le `status.uuid` valeur de la réponse à l'étape précédente. Le mot de passe est ACC- Suivi de la valeur UUID (ACC- [UUID] ou, dans cet exemple, ACC-c49008a5-4ef1-4c5d-a53e-830daf994116).

Connectez-vous à l'interface utilisateur du centre de contrôle Astra

Après avoir installé ACC, vous modifierez le mot de passe de l'administrateur par défaut et vous connecterez au tableau de bord de l'interface utilisateur ACC.

Étapes

1. Dans un navigateur, entrez le FQDN que vous avez utilisé dans le `astraAddress` dans le `astra_control_center_min.yaml` CR quand [Vous avez installé ACC](#).
2. Acceptez les certificats auto-signés lorsque vous y êtes invité.



Vous pouvez créer un certificat personnalisé après la connexion.

3. Dans la page de connexion à Astra Control Center, entrez la valeur que vous avez utilisée `email` dans `astra_control_center_min.yaml` CR quand [Vous avez installé ACC](#), suivi du mot de passe à usage unique (`ACC-[UUID]`).



Si vous saisissez trois fois un mot de passe incorrect, le compte admin est verrouillé pendant 15 minutes.

4. Sélectionnez **connexion**.
5. Modifiez le mot de passe lorsque vous y êtes invité.



Si c'est votre premier login et que vous oubliez le mot de passe et qu'aucun autre compte utilisateur administratif n'a encore été créé, contactez le support NetApp pour obtenir de l'aide pour la récupération de mot de passe.

6. (Facultatif) supprimez le certificat TLS auto-signé existant et remplacez-le par un ["Certificat TLS personnalisé signé par une autorité de certification"](#).

Dépanner l'installation

Si l'un des services est dans `Error` état, vous pouvez inspecter les journaux. Recherchez les codes de réponse API dans la plage 400 à 500. Ceux-ci indiquent l'endroit où un échec s'est produit.

Étapes

1. Pour inspecter les journaux de l'opérateur de l'Astra Control Center, entrez ce qui suit :

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n netapp-acc-operator -o name) -c manager
```

Et la suite

Terminez le déploiement en effectuant le processus ["tâches de configuration"](#).

Configurer le centre de contrôle Astra

Après avoir installé Astra Control Center, connectez-vous à l'interface utilisateur et modifiez votre mot de passe, vous devez configurer une licence, ajouter des clusters, gérer le stockage et ajouter des

compartiments.

Tâches

- [Ajoutez une licence pour Astra Control Center](#)
- [Ajouter un cluster](#)
- [- \[Ajouter un godet\]\(#\)](https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout d&.html#8217;un système back-end)

Ajoutez une licence pour Astra Control Center

Vous pouvez ajouter une nouvelle licence à l'aide de l'interface utilisateur ou de "API" Pour bénéficier de toutes les fonctionnalités de l'Astra Control Center. Sans licence, votre utilisation d'Astra Control Center se limite à la gestion des utilisateurs et à l'ajout de nouveaux clusters.

Ce dont vous avez besoin

Lorsque vous avez téléchargé Astra Control Center à partir du "[Site de support NetApp](#)", Vous avez également téléchargé le fichier de licence NetApp (NLF). Assurez-vous d'avoir accès à ce fichier de licence.



Pour mettre à jour une évaluation existante ou une licence complète, voir "[Mettre à jour une licence existante](#)".

Ajoutez une licence d'évaluation ou complète

Les licences Astra Control Center mesurent les ressources CPU avec des unités de processeur Kubernetes. La licence doit tenir compte des ressources CPU attribuées aux nœuds workers de tous les clusters Kubernetes gérés. Avant d'ajouter une licence, vous devez obtenir le fichier de licence (NLF) du "[Site de support NetApp](#)".

Vous pouvez également essayer Astra Control Center avec une licence d'évaluation qui vous permet d'utiliser Astra Control Center pendant 90 jours à compter de la date de téléchargement de la licence. Vous pouvez vous inscrire pour une version d'évaluation gratuite en vous inscrivant "[ici](#)".



Si votre installation dépasse le nombre de processeurs sous licence, Astra Control Center vous empêche de gérer de nouvelles applications. Une alerte s'affiche lorsque la capacité est dépassée.

Étapes

1. Connectez-vous à l'interface utilisateur du centre de contrôle Astra.
2. Sélectionnez **compte > Licence**.
3. Sélectionnez **Ajouter licence**.
4. Accédez au fichier de licence (NLF) que vous avez téléchargé.
5. Sélectionnez **Ajouter licence**.

La page **Account > License** affiche les informations de licence, la date d'expiration, le numéro de série de licence, l'ID de compte et les unités UC utilisées.



Si vous disposez d'une licence d'évaluation, veillez à stocker votre identifiant de compte afin d'éviter toute perte de données en cas d'échec du Centre de contrôle Astra si vous n'envoyez pas d'ASUP.

Ajouter un cluster

Pour commencer à gérer vos applications, ajoutez un cluster Kubernetes et gérez-le comme une ressource de calcul. Il faut ajouter un cluster pour découvrir vos applications Kubernetes pour Astra Control Center.



Nous vous recommandons de gérer le cluster qu'Astra Control Center déploie en premier avant d'ajouter d'autres clusters à Astra Control Center. La gestion du cluster initial est nécessaire pour envoyer les données Kubemetrics et les données associées au cluster pour les mesures et le dépannage. Vous pouvez utiliser la fonction **Ajouter un cluster** pour gérer un cluster avec Astra Control Center.



Ce dont vous avez besoin, 8217;II

Avant d'ajouter un cluster, vérifiez et effectuez les opérations nécessaires "[tâches préalables](#)".

Étapes

1. Dans **Dashboard** de l'interface utilisateur du Centre de contrôle Astra, sélectionnez **Add** dans la section clusters.
2. Dans la fenêtre **Ajouter un cluster** qui s'ouvre, chargez un `kubeconfig.yaml` classez le contenu d'un `kubeconfig.yaml` fichier.



Le `kubeconfig.yaml` le fichier doit inclure **uniquement les informations d'identification du cluster pour un cluster**.



Add cluster

STEP 1/3: CREDENTIALS

CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

Upload file

Paste from clipboard

Kubeconfig YAML file
No file selected



Credential name



Si vous créez la vôtre `kubeconfig` fichier, vous ne devez définir que **un** élément de contexte dans celui-ci. Voir "[Documentation Kubernetes](#)" pour plus d'informations sur la création `kubeconfig` fichiers.

3. Indiquez un nom d'identification. Par défaut, le nom des identifiants est automatiquement renseigné comme nom du cluster.

- Sélectionnez **configurer le stockage**.
- Sélectionnez la classe de stockage à utiliser pour ce cluster Kubernetes et sélectionnez **Review**.



Vous devez sélectionner une classe de stockage Trident soutenue par le stockage ONTAP.

Add cluster
STEP 2/3: STORAGE

CONFIGURE STORAGE

Existing storage classes are discovered and verified as eligible for use with Astra. You can use your existing default, or choose to set a new default at this time.
Applications with persistent volumes on eligible storage classes are validated for use with Astra.

| Default | Storage class | Storage provisioner | Reclaim policy | Binding mode | Eligible |
|----------------------------------|---------------|------------------------------|----------------|--------------|----------|
| <input checked="" type="radio"/> | basic-csi | csi.trident.netapp.io | Delete | | |
| <input type="radio"/> | thin | kubernetes.io/vsphere-volume | Delete | | |

- Vérifiez les informations, et si tout semble bien, sélectionnez **Ajouter cluster**.

Résultat

Le cluster passe à l'état **découverte**, puis à **en cours d'exécution**. Vous avez ajouté un cluster Kubernetes et gérez-le dans Astra Control Center.



Une fois que vous avez ajouté un cluster à gérer dans Astra Control Center, le déploiement de l'opérateur de surveillance peut prendre quelques minutes. En attendant, l'icône notification devient rouge et consigne un événement **échec de la vérification de l'état de l'agent de surveillance**. Vous pouvez ignorer cela car le problème résout lorsque le centre de contrôle Astra obtient le statut correct. Si le problème ne résout pas le problème en quelques minutes, accédez au cluster, puis exécutez-le `oc get pods -n netapp-monitoring` comme point de départ. Vous devrez consulter les journaux de l'opérateur de surveillance pour déboguer le problème.

Ajout d'un système back-end

Vous pouvez ajouter un système de stockage back-end pour qu'Astra Control puisse gérer ses ressources. La gestion des clusters de stockage d'Astra Control en tant que backend de stockage vous permet d'obtenir des liens entre les volumes persistants (PVS) et le back-end de stockage, ainsi que des metrics de stockage supplémentaires.

Vous pouvez ajouter un système back-end de l'une des manières suivantes :

- Configurer le stockage lorsque vous ajoutez un cluster. Voir "[Ajouter un cluster](#)".
- Ajoutez un stockage back-end découvert à l'aide de l'option Dashboard ou Backends.

Vous pouvez ajouter un back-end de stockage déjà découvert à l'aide des options suivantes :

- [https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout du stockage back-end à l&.html#8217;aide du tableau de bord](https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout%20du%20stockage%20back-end%20à%20l%27aide%20du%20tableau%20de%20bord)><https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout du stockage back-end à l&.html#8217;aide du tableau de bord>
- [https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout du stockage back-end à l&.html#8217;aide de l’option Backends](https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout%20du%20stockage%20back-end%20à%20l%27aide%20de%20l%27option%20Backends)><https://docs.netapp.com/fr-fr/astra-control-center-2108/Ajout du stockage back-end à l&.html#8217;aide de l’option Backends>

Ajout du stockage back-end à l'aide du tableau de bord

1. Dans le tableau de bord, effectuez l'une des opérations suivantes :
 - a. Dans la section backend de stockage du tableau de bord, sélectionnez **gérer**.
 - b. Dans la section Dashboard Resource Summary > Storage backend, sélectionnez **Add**.
2. Entrez les informations d'identification administrateur ONTAP et sélectionnez **Revue**.
3. Confirmez les détails du back-end et sélectionnez **gérer**.

Le back-end s'affiche dans la liste avec des informations récapitulatives.

Ajout du stockage back-end à l'aide de l'option Backends

1. Dans la zone de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez **gérer**.
3. Entrez les informations d'identification administrateur ONTAP et sélectionnez **Revue**.
4. Confirmez les détails du back-end et sélectionnez **gérer**.

Le back-end s'affiche dans la liste avec des informations récapitulatives.

5. Pour afficher les détails du stockage principal, sélectionnez-le.



Les volumes persistants utilisés par les applications dans le cluster de calcul géré sont également affichés.

Ajouter un godet

Il est essentiel d'ajouter des fournisseurs de compartiments de stockage objet pour sauvegarder les applications et le stockage persistant ou pour cloner les applications entre les clusters. Astra Control stocke les sauvegardes ou les clones dans les compartiments de magasin d'objets que vous définissez.

Lorsque vous ajoutez un godet, Astra Control marque un godet comme indicateur de compartiment par défaut. Le premier compartiment que vous créez devient le compartiment par défaut.

Il n'est pas nécessaire de cloner la configuration de vos applications et le stockage persistant vers le même cluster.

Utiliser l'un des types de godet suivants :

- NetApp ONTAP S3
- NetApp StorageGRID S3
- S3 générique



Bien qu'Astra Control Center prenne en charge Amazon S3 en tant que fournisseur de compartiments S3 génériques, Astra Control Center peut ne pas prendre en charge tous les fournisseurs de magasins d'objets qui affirment la prise en charge d'Amazon S3.

Pour plus d'informations sur l'ajout de compartiments à l'aide de l'API Astra, reportez-vous à la section ["Informations sur l'automatisation et les API d'Astra"](#).

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **godets**.
 - a. Sélectionnez **Ajouter**.
 - b. Sélectionner le type de godet.



Lorsque vous ajoutez un compartiment, sélectionnez le type de fournisseur de compartiment approprié avec les identifiants appropriés pour ce fournisseur. Par exemple, l'interface utilisateur accepte NetApp ONTAP S3 comme type avec les identifiants StorageGRID. Toutefois, toutes les futures sauvegardes et restaurations des applications à l'aide de ce compartiment échoueront.

- c. Créer un nouveau nom de compartiment ou saisir un nom de compartiment existant et une description facultative.



Le nom et la description du compartiment apparaissent comme un emplacement de sauvegarde que vous pouvez choisir ultérieurement lors de la création d'une sauvegarde. Ce nom apparaît également lors de la configuration de la règle de protection.

- d. Entrez le nom ou l'adresse IP du serveur S3.
 - e. Si vous souhaitez que ce compartiment soit utilisé comme compartiment par défaut pour toutes les sauvegardes, vérifiez le `Make this bucket the default bucket for this private cloud option`.



Cette option n'apparaît pas pour le premier compartiment que vous créez.

- f. Continuez en ajoutant [informations d'identification](#).

Ajoutez des identifiants d'accès S3

Ajoutez les identifiants d'accès S3 à tout moment.

Étapes

1. Dans la boîte de dialogue compartiments, sélectionnez l'onglet **Ajouter** ou **utiliser existant**.
 - a. Saisissez un nom pour l'identifiant qui le distingue des autres identifiants dans Astra Control.
 - b. Saisissez l'ID d'accès et la clé secrète en collant le contenu dans le presse-papiers.

Et la suite ?

Maintenant que vous vous êtes connecté et que vous avez ajouté des clusters à Astra Control Center, vous pouvez commencer à utiliser les fonctions de gestion des données applicatives d'Astra Control Center.

- ["Gérer les utilisateurs"](#)
- ["Commencez à gérer les applications"](#)
- ["Protégez vos applications"](#)
- ["Clonage des applications"](#)
- ["Gérer les notifications"](#)
- ["Connectez-vous à Cloud Insights"](#)

- ["Ajouter un certificat TLS personnalisé"](#)

Trouvez plus d'informations

- ["Utilisez l'API Astra"](#)
- ["Problèmes connus"](#)

Conditions préalables à l'ajout d'un cluster

Assurez-vous que les conditions préalables sont remplies avant d'ajouter un cluster. Vous devez également effectuer les vérifications d'admissibilité pour vous assurer que votre grappe est prête à être ajoutée au Centre de contrôle Astra.

Ce dont vous avez besoin avant d'ajouter un cluster

- Cluster OpenShift 4.6 ou 4.7 avec des classes de stockage Trident combinées à ONTAP 9.5 ou une version ultérieure.
 - Un ou plusieurs nœuds de travail avec au moins 1 Go de RAM disponible pour l'exécution des services de télémétrie.



Si vous prévoyez d'ajouter un second cluster OpenShift 4.6 ou 4.7 comme ressource de calcul gérée, assurez-vous que la fonctionnalité Snapshot des volumes Trident est activée. Voir le Trident officiel ["instructions"](#) Pour activer et tester des snapshots de volume avec Trident.

- Le superutilisateur et l'ID utilisateur définis sur le système ONTAP de sauvegarde pour sauvegarder et restaurer des applications avec le Centre de contrôle Astra (ACC). Exécutez les commandes suivantes dans la ligne de commande ONTAP :

```
export policy rule modify -vserver svm0 -policyname default -ruleindex 1
-superuser sys
export-policy rule modify -policyname default -ruleindex 1 -anon 65534 (il s'agit de la valeur par défaut)
```

Effectuer des vérifications d'éligibilité

Effectuez les contrôles d'éligibilité suivants pour vous assurer que votre grappe est prête à être ajoutée au Centre de contrôle Astra.

Étapes

1. Vérifiez la version de Trident.

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

Si Trident est présent, vous voyez des valeurs de sortie similaires à celles illustrées dans l'exemple suivant :

```
NAME          VERSION
trident       21.04.0
```

Si Trident n'existe pas, vous voyez des résultats similaires à ce qui suit :

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



Si Trident n'est pas installé ou si la version installée n'est pas la dernière, vous devez installer la dernière version de Trident avant de continuer. Voir la "[Documentation Trident](#)" pour obtenir des instructions.

2. Vérifiez si les classes de stockage utilisent les pilotes Trident pris en charge. Le nom de provisionnement doit être `csi.trident.netapp.io`. Voir l'exemple suivant :

```
kubectl get storageClass -A
NAME                                PROVISIONER                                RECLAIMPOLICY
VOLUMEBINDINGMODE  ALLOWVOLUMEEXPANSION  AGE
ontap-gold (default)  csi.trident.netapp.io  Delete
Immediate          true                  5d23h
thin                kubernetes.io/vsphere-volume  Delete
Immediate          false                 6d
```

Créez un kubeconfig. Rôle admin

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 `astraccontrol-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>astraccontrol-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. Si l'index de jeton que vous avez noté dans l'étape précédente n'était pas 0, remplacez la valeur pour `TOKEN_INDEX` au début du script suivant avec la valeur correcte.

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

```
# Update these to match your environment. Replace the value for
TOKEN_INDEX from
# the output in the previous step if it was not 0. 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'
TOKEN_INDEX=0

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 en un nom significatif pour votre grappe. Protéger les informations d'identification du cluster.

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

Et la suite ?

Maintenant que vous avez vérifié que les conditions préalables sont remplies, vous êtes prêt à "[ajouter un cluster](#)".

Trouvez plus d'informations

- "[Documentation Trident](#)"
- "[Utilisez l'API Astra](#)"

Ajouter un certificat TLS personnalisé

Vous pouvez supprimer le certificat TLS auto-signé existant et le remplacer par un certificat TLS signé par une autorité de certification (AC).

Ce dont vous avez besoin

- Cluster Kubernetes avec Astra Control Center installé
- Accès administratif à un shell de commande sur le cluster à exécuter `kubectl` commandes
- Clé privée et fichiers de certificat de l'autorité de certification

Supprimez le certificat auto-signé

1. Avec SSH, connectez-vous au cluster Kubernetes qui héberge Astra Control Center en tant qu'utilisateur administratif.
2. Recherchez le code secret TLS associé au certificat en cours à l'aide de la commande suivante, remplacement `<ACC-deployment-namespace>` Avec l'espace de noms de déploiement d'Astra Control Center :

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Supprimez le certificat et le secret actuellement installés à l'aide des commandes suivantes :

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Ajoutez un nouveau certificat

1. Utilisez la commande suivante pour créer le nouveau secret TLS avec la clé privée et les fichiers de certificat de l'autorité de certification, en remplaçant les arguments entre parenthèses `<>` par les informations appropriées :

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Utilisez la commande et l'exemple suivants pour modifier le fichier CRD (Custom Resource Definition) du cluster et modifier `spec.selfSigned` valeur à `spec.ca.secretName` Pour consulter le secret TLS créé précédemment :

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Utilisez la commande suivante et exemple de résultat pour vérifier que les modifications sont correctes et le cluster est prêt à valider les certificats, en remplaçant `<ACC-deployment-namespace>` Avec l'espace de noms de déploiement d'Astra Control Center :

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time: 2021-07-01T23:50:27Z
    Message:             Signing CA verified
    Reason:              KeyPairVerified
    Status:              True
    Type:                Ready
  Events:               <none>
```

4. Créer le `certificate.yaml` fichier avec l'exemple suivant, en remplaçant les valeurs de paramètre fictif entre parenthèses `<>` par les informations appropriées :

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
    - <astra.dnsname.example.com> #Replace with the correct Astra Control
      Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Créez le certificat à l'aide de la commande suivante :

```
kubectl apply -f certificate.yaml
```

6. À l'aide de la commande et de l'exemple de sortie suivants, vérifiez que le certificat a été créé correctement et avec les arguments que vous avez spécifiés lors de la création (tels que le nom, la durée, la date limite de renouvellement et les noms DNS).


```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration: 125h0m0s
  Issuer Ref:
    Kind:      ClusterIssuer
    Name:      cert-manager-certificates
  Renew Before: 61h0m0s
  Secret Name: <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time: 2021-07-02T00:45:41Z
    Message:             Certificate is up to date and has not expired
    Reason:              Ready
    Status:              True
    Type:               Ready
  Not After: 2021-07-07T05:45:41Z
  Not Before: 2021-07-02T00:45:41Z
  Renewal Time: 2021-07-04T16:45:41Z
  Revision: 1
  Events: <none>
```

7. Modifiez l'option Ingress CRD TLS pour pointer vers votre nouveau secret de certificat à l'aide de la commande suivante et de l'exemple, en remplaçant les valeurs de paramètre fictif entre parenthèses <> par les informations appropriées :

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-namespace>
....

# tls:
#   options:
#     name: default
#     secretName: secure-testing-cert
#     store:
#       name: default

tls:
  options:
    name: default
  secretName: <certificate-secret-name>
  store:
    name: default
```

8. À l'aide d'un navigateur Web, accédez à l'adresse IP de déploiement d'Astra Control Center.
9. Vérifiez que les détails du certificat correspondent aux détails du certificat que vous avez installé.
10. Exportez le certificat et importez le résultat dans le gestionnaire de certificats de votre navigateur Web.

Foire aux questions pour Astra Control Center

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

Présentation

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

Accès au centre de contrôle Astra

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

Astra Control Center utilise l'authentification locale et une URL spécifique à chaque environnement.

Pour l'URL, dans un navigateur, entrez le nom de domaine complet (FQDN) que vous avez défini dans le champ `spec.astraAddress` dans le fichier `astra_control_Center_min.yaml` personnalisé Resource definition (CRD) lorsque vous avez installé Astra Control Center. L'e-mail est la valeur que vous avez définie dans le champ `spec.email` de l'`astra_Control_Center_min.yaml` CRD.

J'utilise la licence d'évaluation. Comment puis-je passer à la licence complète?

Vous pouvez facilement passer à une licence complète en obtenant le fichier de licence NetApp (NLF).

Étapes

- Dans le menu de navigation de gauche, sélectionnez **compte > Licence**.
- Sélectionnez **Ajouter licence**.
- Naviguez jusqu'au fichier de licence que vous avez téléchargé et sélectionnez **Ajouter**.

J'utilise la licence d'évaluation. Puis-je toujours gérer les applications ?

Oui, vous pouvez tester la fonctionnalité de gestion des applications avec la licence d'évaluation.

Enregistrement des clusters Kubernetes

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

De nouveaux nœuds workers peuvent être ajoutés aux pools existants. 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 `kubect1 get nodes` commande.

Comment puis-je dégérer correctement un cluster?

1. "[Gérez les applications avec Astra Control](#)".
2. "[Dégérer le cluster à partir d'Astra Control](#)".

Que se passe-t-il pour mes applications et données après avoir retiré le cluster Kubernetes 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 sauvegardes de stockage persistant créées par Astra Control restent dans le contrôle d'Astra, mais elles sont indisponibles pour les restaurations.



Retirez toujours un cluster d'Astra Control avant de le supprimer par d'autres méthodes. La suppression d'un cluster à l'aide d'un autre outil alors qu'il est toujours géré par Astra Control peut causer des problèmes pour votre compte Astra Control.

NetApp Trident sera-t-il désinstallé lorsque je retire un cluster Kubernetes d'Astra Control ?

Trident ne sera pas désinstallé d'un cluster lorsque vous le supprimez 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.

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.

Astra Control peut-il gérer une application qui se trouve sur un système de stockage autre que NetApp?

Non Astra Control peut découvrir des applications qui utilisent un stockage autre que NetApp, mais il ne peut pas gérer une application qui utilise un stockage non NetApp.

Devrais-je gérer Astra Control lui-même? non, vous ne devriez pas gérer Astra Control lui-même parce qu'il s'agit d'une "application système".

Les opérations de gestion des données

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 snapshot dans le cadre d'un processus de sauvegarde, de clonage ou de restauration.

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 via une interface ou un stockage objet différent?

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

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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