



Documentation Astra Control Center 22.11

Astra Control Center

NetApp
November 21, 2023

Sommaire

Documentation Astra Control Center 22.11	1
Notes de mise à jour	2
Nouveautés de cette version d'Astra Control Center	2
Problèmes connus	4
Limites connues	7
Commencez	12
Exigences du centre de contrôle Astra	12
Démarrage rapide pour Astra Control Center	16
Présentation de l'installation	18
Configurer le centre de contrôle Astra	73
Foire aux questions pour Astra Control Center	87
Concepts	90
Architecture et composants	90
Protection des données	91
Licences	95
Classes de stockage et taille de volume persistant	96
Rôles et espaces de noms d'utilisateur	96
Utilisez Astra Control Center	98
Commencez à gérer les applications	98
Protégez vos applications	104
Surveillez l'état des applications et des clusters	127
Gérez votre compte	130
Gestion des compartiments	140
Gérer le stockage back-end	143
Surveillez les tâches en cours d'exécution	146
Surveillez l'infrastructure avec des connexions Cloud Insights, Prometheus ou Fluentd	147
Annuler la gestion des applications et des clusters	156
Mettez à niveau Astra Control Center	157
Désinstaller Astra Control Center	166
Automatisez avec l'API REST d'Astra Control	170
Automatisation avec l'API REST Astra Control	170
Connaissances et support	171
Dépannage	171
Obtenez de l'aide	171
Versions antérieures de la documentation Astra Control Center	174
Mentions légales	175
Droits d'auteur	175
Marques déposées	175
Brevets	175
Politique de confidentialité	175
Source ouverte	175
Licence API Astra Control	175

Documentation Astra Control Center 22.11

Notes de mise à jour

Nous sommes heureux d'annoncer la dernière version d'Astra Control Center.

- ["Dans cette version d'Astra Control Center"](#)
- ["Problèmes connus"](#)
- ["Limites connues"](#)

Suivez-nous sur Twitter [@NetAppDoc](#). Envoyez vos commentaires sur la documentation en devenant un ["Contributeur GitHub"](#) ou en envoyant un e-mail à doccomments@netapp.com.

Nouveautés de cette version d'Astra Control Center

Nous sommes heureux d'annoncer la dernière version d'Astra Control Center.

22 novembre 2022 (22.11.0)

Nouvelles fonctionnalités et prises en charge

- ["Prise en charge des applications réparties sur plusieurs espaces de noms"](#)
- ["La prise en charge de l'inclusion des ressources de cluster dans une définition d'application"](#)
- ["L'authentification LDAP optimisée avec l'intégration du contrôle d'accès basé sur des rôles \(RBAC\)"](#)
- ["Ajout de la prise en charge de Kubernetes 1.25 et de Pod Security admission \(PSA\)"](#)
- ["Création de rapports d'avancement pour les opérations de sauvegarde, de restauration et de clonage"](#)

Problèmes et limites connus

- ["Problèmes connus pour cette version"](#)
- ["Restrictions connues pour cette version"](#)

8 septembre 2022 (22.08.1)

Cette version (22.08.1) pour Astra Control Center (22.08.0) corrige les bugs mineurs dans la réplication d'applications à l'aide de NetApp SnapMirror.

10 août 2022 (22.08.0)

Détails

Nouvelles fonctionnalités et prises en charge

- ["Réplication d'applications à l'aide de la technologie NetApp SnapMirror"](#)
- ["Workflow de gestion des applications amélioré"](#)
- ["Fonctionnalité améliorée de crochets d'exécution"](#)



Les crochets d'exécution par défaut avant ou après snapshot de NetApp ont été retirés pour des applications spécifiques dans cette version. Si vous effectuez une mise à niveau vers cette version et que vous ne fournissez pas vos propres crochets d'exécution pour les instantanés, Astra Control ne prendra que des instantanés cohérents avec les collisions. Consultez le ["NetApp Verda" Référentiel GitHub](#) pour des exemples de scripts de hook d'exécution que vous pouvez modifier en fonction de votre environnement.

- ["Prise en charge de VMware Tanzu Kubernetes Grid Integrated Edition \(TKGI\)"](#)
- ["Prise en charge de Google Anthos"](#)
- ["Configuration LDAP \(via l'API de contrôle Astra\)"](#)

Problèmes et limites connus

- ["Problèmes connus pour cette version"](#)
- ["Restrictions connues pour cette version"](#)

26 avril 2022 (22.04.0)

Détails

Nouvelles fonctionnalités et prises en charge

- ["Contrôle d'accès basé sur des rôles \(RBAC\) dans un espace de noms"](#)
- ["Prise en charge de Cloud Volumes ONTAP"](#)
- ["Activation d'entrée générique pour le centre de contrôle Astra"](#)
- ["Dépose du godet de l'Astra Control"](#)
- ["Prise en charge de la gamme VMware Tanzu"](#)

Problèmes et limites connus

- ["Problèmes connus pour cette version"](#)
- ["Restrictions connues pour cette version"](#)

14 décembre 2021 (21.12)

Détails

Nouvelles fonctionnalités et prises en charge

- ["Restauration des applications"](#)
- ["Crochets d'exécution"](#)
- ["Prise en charge des applications déployées avec des opérateurs du système namespace"](#)
- ["Prise en charge supplémentaire de Kubernetes et Rancher en amont"](#)
- ["Mises à niveau d'Astra Control Center"](#)
- ["Option Red Hat OperatorHub pour l'installation"](#)

Résolution des problèmes

- ["Problèmes résolus pour cette version"](#)

Problèmes et limites connus

- ["Problèmes connus pour cette version"](#)
- ["Restrictions connues pour cette version"](#)

5 août 2021 (21.08)

Détails

Lancement initial du centre de contrôle Astra.

- ["Ce qu'il est"](#)
- ["Analysez l'architecture et les composants"](#)
- ["Commencez dès maintenant"](#)
- ["Installer" et "configuration"](#)
- ["Gérez" et "protéger" en applications](#)
- ["Gestion des compartiments" et "systèmes back-end"](#)
- ["Gestion des comptes"](#)
- ["Automatisez votre système avec des API"](#)

Trouvez plus d'informations

- ["Problèmes connus pour cette version"](#)
- ["Restrictions connues pour cette version"](#)
- ["Versions antérieures de la documentation Astra Control Center"](#)

Problèmes connus

Les problèmes connus identifient les problèmes susceptibles de vous empêcher d'utiliser cette version du produit avec succès.

Les problèmes connus suivants ont une incidence sur la version actuelle :

En applications

- La restauration d'une application entraîne une taille de volume persistant supérieure à celle de l'application initiale
- Les clones d'applications échouent à l'aide d'une version spécifique de PostgreSQL
- Les clones d'application échouent lors de l'utilisation des contraintes de contexte de sécurité OCP au niveau du compte de service (SCC)
- Les clones d'application échouent après le déploiement d'une application avec une classe de stockage définie
- Les sauvegardes d'applications et les snapshots échouent si la classe `volumesnapshotclass` est ajoutée après la gestion d'un cluster

Clusters

- La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier `kubeconfig` par défaut contient plusieurs contextes

Autres questions

- Les clusters gérés n'apparaissent pas dans NetApp Cloud Insights lors de la connexion via un proxy
- Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne

La restauration d'une application entraîne une taille de volume persistant supérieure à celle de l'application initiale

Si vous redimensionnez un volume persistant après avoir créé une sauvegarde puis restauré à partir de cette sauvegarde, la taille du volume persistant correspond à la nouvelle taille du volume persistant, et non à la taille de la sauvegarde.

Les clones d'applications échouent à l'aide d'une version spécifique de PostgreSQL

Les clones d'applications au sein du même cluster échouent systématiquement avec le graphique Bitnami PostgreSQL 11.5.0. Pour effectuer un clonage réussi, utilisez une version antérieure ou ultérieure du graphique.

Les clones d'application échouent lors de l'utilisation des contraintes de contexte de sécurité OCP au niveau du compte de service (SCC)

Un clone d'application peut échouer si les contraintes de contexte de sécurité d'origine sont configurées au niveau du compte de service dans l'espace de noms du cluster OpenShift Container Platform. Lorsque le clone de l'application échoue, il apparaît dans la zone applications gérées du Centre de contrôle Astra avec l'état `Removed`. Voir la ["article de la base de connaissances"](#) pour en savoir plus.

Les sauvegardes d'applications et les snapshots échouent si la classe `volumesnapshotclass` est ajoutée après la gestion d'un cluster

Les sauvegardes et les snapshots échouent avec un `UI 500 error` dans ce scénario. Pour contourner ce problème, actualisez la liste des applications.

Les clones d'application échouent après le déploiement d'une application avec une classe de stockage définie

Après le déploiement d'une application avec une classe de stockage définie explicitement (par exemple, `helm install ...-set global.storageClass=netapp-cvs-perf-extreme`), les tentatives ultérieures de clonage de l'application nécessitent que le cluster cible ait la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera. Il n'y a pas d'étapes de récupération dans ce scénario.

La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig par défaut contient plusieurs contextes

Vous ne pouvez pas utiliser un kubeconfig avec plus d'un cluster et un contexte. Voir la ["article de la base de connaissances"](#) pour en savoir plus.

Les clusters gérés n'apparaissent pas dans NetApp Cloud Insights lors de la connexion via un proxy

Lorsque le centre de contrôle Astra se connecte à NetApp Cloud Insights par le biais d'un proxy, il se peut que les clusters gérés n'apparaissent pas dans Cloud Insights. Pour contourner ce problème, exécutez les commandes suivantes sur chaque cluster géré :

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[outputs.http\]/c\ [[outputs.http]]\n use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[outputs.http\]/c\ [[outputs.http]]\n use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-
ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-
monitoring pod
```

Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne

Si Astra Trident sur un cluster d'application est mis hors ligne (et reconnecté) et 500 erreurs de service internes sont rencontrées lors de la tentative de gestion des données d'application, redémarrez tous les nœuds Kubernetes du cluster d'application pour restaurer la fonctionnalité.

Trouvez plus d'informations

- ["Limites connues"](#)

Limites connues

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Limites de gestion du cluster

- Le même cluster ne peut pas être géré par deux instances Astra Control Center
- Astra Control Center ne peut pas gérer deux clusters nommés de manière identique

Limites du contrôle d'accès basé sur des rôles (RBAC)

- Un utilisateur doté de contraintes RBAC d'espace de noms peut ajouter et annuler la gestion d'un cluster
- Un membre avec des contraintes d'espace de noms ne peut pas accéder aux applications clonées ou restaurées tant que admin n'ajoute pas l'espace de noms à la contrainte

Limites de gestion des applications

- vous ne pouvez pas restaurer collectivement plusieurs applications dans un autre espace de noms
- Astra Control n'attribue pas automatiquement de compartiments par défaut pour les instances de cloud
- Les clones des applications installées à l'aide d'opérateurs pass-by-Reference peuvent échouer
- Les opérations de restauration sur place des applications qui utilisent un gestionnaire de certificats ne sont pas prises en charge
- Applications activées par OLM et déployées par l'opérateur à étendue de cluster non prises en charge
- Les applications déployées avec Helm 2 ne sont pas prises en charge

Limitations générales

- Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible
- Astra Control Center ne valide pas les détails que vous entrez pour votre serveur proxy
- Les connexions existantes à un pod Postgres provoquent des défaillances
- Il est possible que les sauvegardes et les snapshots ne soient pas conservés lors du retrait d'une instance Astra Control Center
- Limitations de l'utilisateur et du groupe LDAP

Le même cluster ne peut pas être géré par deux instances Astra Control Center

Si vous souhaitez gérer un cluster sur une autre instance Astra Control Center, vous devez d'abord ["annuler la gestion du cluster"](#) à partir de l'instance sur laquelle elle est gérée avant de la gérer sur une autre instance. Une fois le cluster supprimé de la gestion, vérifiez que le cluster n'est pas géré en exécutant la commande suivante :

```
oc get pods n -netapp-monitoring
```

Il ne doit y avoir aucun pod en cours d'exécution dans cet espace de nom, sinon l'espace de noms ne doit pas exister. Si l'un de ces deux éléments est vrai, le cluster n'est pas géré.

Astra Control Center ne peut pas gérer deux clusters nommés de manière identique

Si vous tentez d'ajouter un cluster portant le même nom qu'un cluster existant, l'opération échoue. Ce problème se produit le plus souvent dans un environnement Kubernetes standard si vous n'avez pas modifié le nom de cluster par défaut dans les fichiers de configuration Kubernetes.

Pour résoudre ce problème, procédez comme suit :

1. Modifiez votre `kubeadm-config` ConfigMap :

```
kubectl edit configmaps -n kube-system kubeadm-config
```

2. Modifiez le `clusterName` valeur de champ de `kubernetes` (Nom par défaut de Kubernetes) vers un nom personnalisé unique.
3. Modifiez `kubeconfig` (`.kube/config`).
4. Mettre à jour le nom de cluster depuis `kubernetes` à un nom personnalisé unique (`xyz-cluster` est utilisé dans les exemples ci-dessous). Effectuez la mise à jour dans les deux `clusters` et `contexts` sections comme indiqué dans cet exemple :

```
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
  ExAmPLERb2tCcJZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
  server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
  cluster: xyz-cluster
  namespace: default
  user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

Un utilisateur doté de contraintes RBAC d'espace de noms peut ajouter et annuler la gestion d'un cluster

Un utilisateur doté de contraintes RBAC d'espace de noms ne doit pas être autorisé à ajouter ou annuler la gestion des clusters. En raison d'une limitation actuelle, Astra n'empêche pas ces utilisateurs de déléguer les clusters.

Un membre avec des contraintes d'espace de noms ne peut pas accéder aux applications clonées ou restaurées tant que admin n'ajoute pas l'espace de noms à la contrainte

Toutes `member` Les utilisateurs ayant des contraintes RBAC en fonction du nom/ID de l'espace de noms peuvent cloner ou restaurer une application vers un nouvel espace de noms sur le même cluster ou vers tout autre cluster du compte de leur entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, le compte admin/propriétaire peut modifier le `member` contraintes de compte d'utilisateur et de rôle de mise à jour pour l'utilisateur affecté pour accorder l'accès au nouvel espace de noms.

De même, vous ne pouvez pas restaurer collectivement plusieurs applications dans un autre espace de noms

Si vous gérez plusieurs applications dans un seul espace de noms (en créant plusieurs définitions d'applications dans Astra Control), vous ne pouvez pas restaurer toutes les applications dans un espace de noms différent. Chaque application doit être restaurée dans son propre espace de noms distinct.

Astra Control n'attribue pas automatiquement de compartiments par défaut pour les instances de cloud

Astra Control n'attribue pas automatiquement de compartiment par défaut à une instance de cloud. Vous devez définir manuellement un compartiment par défaut pour une instance de cloud. Si un compartiment par défaut n'est pas défini, vous ne pourrez pas effectuer les opérations de clonage d'applications entre les deux clusters.

Les clones des applications installées à l'aide d'opérateurs pass-by-Reference peuvent échouer

Astra Control prend en charge les applications installées avec des opérateurs à espace de noms. Ces opérateurs sont généralement conçus avec une architecture « pass-by-value » plutôt qu'une architecture « pass-by-Reference ». Voici quelques applications opérateur qui suivent ces modèles :

- ["Apache K8ssandra"](#)



Pour K8ssandra, les opérations de restauration sur place sont prises en charge. Pour effectuer une opération de restauration vers un nouvel espace de noms ou un cluster, l'instance d'origine de l'application doit être arrêté. Cela permet de s'assurer que les informations du groupe de pairs transmises ne conduisent pas à une communication entre les instances. Le clonage de l'application n'est pas pris en charge.

- ["IC Jenkins"](#)
- ["Cluster Percona XtraDB"](#)

Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture « pass-by-Reference » (par exemple, l'opérateur CockroachDB). Lors de ces types d'opérations de clonage, l'opérateur cloné tente de référencer les secrets de Kubernetes de l'opérateur source malgré avoir son propre nouveau secret dans le cadre du processus de clonage. Il est possible que le clonage échoue, car Astra Control ne connaît pas les secrets de Kubernetes qui sont présents dans l'opérateur source.



Lors des opérations de clonage, les applications nécessitant une ressource IngressClass ou des crochets Web ne doivent pas avoir ces ressources déjà définies sur le cluster de destination.

Les opérations de restauration sur place des applications qui utilisent un gestionnaire de certificats ne sont pas prises en charge

Cette version d'Astra Control Center ne prend pas en charge la restauration sur place des applications avec des gestionnaires de certificats. Les opérations de restauration vers un espace de noms et des clones différents sont prises en charge.

Applications activées par OLM et déployées par l'opérateur à étendue de cluster non prises en charge

Astra Control Center ne prend pas en charge les activités de gestion d'applications avec des opérateurs à périmètre de cluster.

Les applications déployées avec Helm 2 ne sont pas prises en charge

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. Pour plus d'informations, voir "[Exigences du centre de contrôle Astra](#)".

Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible

Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.

Astra Control Center ne valide pas les détails que vous entrez pour votre serveur proxy

Assurez-vous que vous "[entrez les valeurs correctes](#)" lors de l'établissement d'une connexion.

Les connexions existantes à un pod Postgres provoquent des défaillances

Lorsque vous exécutez des opérations sur les modules Postgres, vous ne devez pas vous connecter directement dans le pod pour utiliser la commande psql. Astra Control nécessite un accès psql pour geler et dégeler les bases de données. S'il existe une connexion existante, le snapshot, la sauvegarde ou le clone échoueront.

Il est possible que les sauvegardes et les snapshots ne soient pas conservés lors du retrait d'une instance Astra Control Center

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.

Limitations de l'utilisateur et du groupe LDAP

Astra Control Center prend en charge jusqu'à 5,000 groupes distants et 10,000 utilisateurs distants.

Trouvez plus d'informations

- ["Problèmes connus"](#)

Commencez

=
:allow-uri-read:

Exigences du centre de contrôle Astra

Commencez par vérifier que votre environnement opérationnel, vos clusters d'applications, vos applications, vos licences et votre navigateur Web sont prêts.

- [De l'environnement opérationnel](#)
- [Systèmes back-end de stockage pris en charge](#)
- [Accès à Internet](#)
- [Licence](#)
- [Entrée pour les clusters Kubernetes sur site](#)
- [Configuration réseau requise](#)
- [Navigateurs Web pris en charge](#)
- [Exigences supplémentaires relatives aux clusters d'applications](#)
- [Exigences des clusters Google Anthos](#)
- [Configuration requise pour le cluster VMware Tanzu Kubernetes Grid](#)

De l'environnement opérationnel

Le centre de contrôle Astra a été validé pour les types d'environnements opérationnels suivants :

- Cisco IKS avec Kubernetes 1.22
- Google Anthos 1.11 ou 1.12 (voir [Exigences des clusters Google Anthos](#))
- Rancher Kubernetes Engine (RKE) :
 - RKE 1.3.12 avec Rancher 2.6.5 et 2.6.6
 - RKE 1.3.13 avec Rancher 2.6.8
 - RKE 2 (v1.23,6+rke2r1) avec Rancher 2.6.5 et 2.6.6
 - RKE 2 (v1.24.x) avec Rancher 2.6.8
- Red Hat OpenShift Container Platform 4.8 à 4.11
- Kubernetes 1.23 vers 1.25 en amont (Astra Trident 22.10 ou version ultérieure requise pour Kubernetes 1.25)
- VMware Tanzu Kubernetes Grid : (voir [Configuration requise pour le cluster VMware Tanzu Kubernetes Grid](#))
 - VMware Tanzu Kubernetes Grid 1.5
 - VMware Tanzu Kubernetes Grid Integrated Edition 1.13 et 1.14

Assurez-vous que l'environnement d'exploitation que vous choisissez d'héberger est conforme aux exigences de base en matière de ressources décrites dans la documentation officielle de l'environnement. Outre les exigences de l'environnement en matière de ressources, Astra Control Center requiert les ressources

suivantes :

Composant	Conditions requises
Extensions de processeur	Les processeurs de tous les nœuds de l'environnement d'hébergement doivent avoir des extensions AVX activées.
Capacité du système back-end	Au moins 500 Go disponibles
Nœuds worker	Au moins 3 nœuds workers au total, avec 4 cœurs de processeurs et 12 Go de RAM chacun
Adresse FQDN	Une adresse FQDN pour Astra Control Center
Astra Trident	Astra Trident 22.01 ou version ultérieure installé et configuré avec Astra Trident 22.07 ou plus récent installé pour la réplication d'applications basée sur SnapMirror Astra Trident 22.10 ou version ultérieure installée pour les clusters Kubernetes 1.25 (vous devez effectuer une mise à niveau vers Astra Trident 22.10 avant la mise à niveau vers Kubernetes 1.25).



De telles exigences supposent que Astra Control Center est la seule application qui s'exécute dans l'environnement opérationnel. Si l'environnement exécute des applications supplémentaires, ajustez ces exigences minimales en conséquence.

- **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 fournir l'URL du registre d'images où vous allez télécharger les images.
- **Configuration de l'Astra Trident / ONTAP :**
 - Vous devez configurer au moins une classe de stockage Astra Trident sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'elle est la seule classe de stockage avec la désignation par défaut.
 - Assurez-vous que les nœuds workers de votre cluster sont configurés avec les pilotes de stockage appropriés afin que les pods puissent interagir avec le système de stockage back-end. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Astra Trident :
 - ontap-nas
 - ontap-san
 - ontap-san-économie (non pris en charge pour la réplication d'applications)

Systemes back-end de stockage pris en charge

Astra Control Center prend en charge les systèmes back-end de stockage suivants.

- NetApp ONTAP 9.5 ou version ultérieure des systèmes AFF, FAS et ASA
- Systèmes NetApp ONTAP 9.8 ou plus récents AFF, FAS et ASA pour la réplication d'applications basée sur SnapMirror
- NetApp ONTAP Select 9.5 ou version ultérieure

- NetApp ONTAP Select 9.8 ou version ultérieure pour la réplication d'applications basée sur SnapMirror
- NetApp Cloud Volumes ONTAP 9.5 ou version ultérieure

Pour utiliser Astra Control Center, vérifiez que vous disposez des licences ONTAP suivantes, en fonction de ce que vous devez accomplir :

- FlexClone
- SnapMirror : en option. Elle est nécessaire uniquement pour la réplication vers des systèmes distants à l'aide de la technologie SnapMirror. Reportez-vous à la section "[Informations sur la licence SnapMirror](#)".
- Licence S3 : en option. Nécessaire uniquement pour les compartiments ONTAP S3

Pour vérifier si votre système ONTAP dispose des licences requises, reportez-vous à la section "[Gérer les licences ONTAP](#)".

Accès à Internet

Vous devez déterminer si vous avez un accès externe à Internet. Si ce n'est pas le cas, certaines fonctionnalités peuvent être limitées, comme la réception de données de surveillance et de metrics depuis NetApp Cloud Insights ou l'envoi de packs de support au "[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. Vous devez disposer d'une licence pour protéger vos applications et vos données. Reportez-vous à la section "[Caractéristiques du centre de contrôle Astra](#)" pour plus d'informations.

Vous pouvez 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](#)".

Pour configurer la licence, reportez-vous à la section "[utilisez une licence d'essai gratuite de 90 jours](#)".

Pour en savoir plus sur le fonctionnement des licences, reportez-vous à la section "[Licences](#)".

Pour plus d'informations sur les licences requises pour les systèmes de stockage back-end ONTAP, reportez-vous à la "[Systèmes back-end de stockage pris en charge](#)".

Entrée pour les clusters Kubernetes sur site

Vous pouvez choisir le type d'entrée de réseau utilisé par le centre de contrôle Astra. Par défaut, Astra Control Center déploie la passerelle Astra Control Center (service/trafik) comme ressource à l'échelle du cluster. Astra Control Center prend également en charge l'utilisation d'un équilibreur de charge de service, s'ils sont autorisés dans votre environnement. Si vous préférez utiliser un équilibreur de charge de service et que vous n'avez pas encore configuré, vous pouvez utiliser l'équilibreur de charge 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.



L'équilibreur de charge doit utiliser une adresse IP située dans le même sous-réseau que les adresses IP du nœud de travail de l'Astra Control Center.



Si vous hébergez Astra Control Center sur un cluster Kubernetes Grid de Tanzu, utilisez le `kubectl get nsxlbmonitors -A` commande pour voir si un moniteur de service est déjà configuré pour accepter le trafic d'entrée. S'il en existe un, vous ne devez pas installer MetalLB, car le moniteur de service existant remplacera toute nouvelle configuration d'équilibreur de charge.

Pour plus d'informations, voir ["Configurer l'entrée pour l'équilibrage de charge"](#).

Configuration réseau requise

L'environnement opérationnel qui héberge le centre de contrôle Astra 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 l'environnement hébergeant le centre de contrôle Astra et chaque cluster géré (le cas échéant).



Vous pouvez déployer Astra Control Center dans un cluster Kubernetes à double pile, et Astra Control Center peut gérer les applications et les systèmes back-end de stockage qui ont été configurés pour un fonctionnement à double pile. Pour plus d'informations sur la configuration requise pour les clusters à double pile, consultez le ["Documentation Kubernetes"](#).

Source	Destination	Port	Protocole	Objectif
PC client	Centre de contrôle Astra	443	HTTPS	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
Consommateurs de metrics	Nœud de travail Astra Control Center	9090	HTTPS	Communication de données de metrics : assurez-vous que chaque cluster géré peut accéder à ce port sur le cluster hébergeant Astra Control Center (communication bidirectionnelle requise).
Centre de contrôle Astra	Service Cloud Insights hébergé	443	HTTPS	Communication avec Cloud Insights
Centre de contrôle Astra	Fournisseur de compartiments de stockage Amazon S3	443	HTTPS	Communications de stockage Amazon S3
Centre de contrôle Astra	NetApp AutoSupport	443	HTTPS	Communication avec NetApp AutoSupport

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.

Exigences supplémentaires relatives aux clusters d'applications

Gardez à l'esprit ces exigences si vous prévoyez d'utiliser ces caractéristiques du centre de contrôle Astra :

- **Configuration requise pour le cluster d'applications** : ["Exigences de gestion du cluster"](#)
 - * Exigences des applications gérées* : ["De gestion des applications"](#)
 - **Exigences supplémentaires pour la réplication d'applications** : ["Conditions préalables à la réplication"](#)

Exigences des clusters Google Anthos

Lorsque vous hébergez Astra Control Center sur un cluster Google Anthos, notez que Google Anthos inclut par défaut l'équilibreur de charge MetalLB et le service de passerelle d'entrée Istio, vous permettant d'utiliser simplement les fonctionnalités d'entrée génériques d'Astra Control Center pendant l'installation. Voir ["Configurer le centre de contrôle Astra"](#) pour plus d'informations.

Configuration requise pour le cluster VMware Tanzu Kubernetes Grid

Lorsque vous hébergez Astra Control Center sur un cluster VMware Tanzu Kubernetes Grid (TKG) ou Tanzu Kubernetes Grid Integrated Edition (TKGi), gardez à l'esprit les considérations suivantes.

- Désactivez la mise en œuvre par défaut des classes de stockage TKG ou TKGi sur les clusters d'applications devant être gérés par Astra Control. Vous pouvez le faire en modifiant le `TanzuKubernetesCluster` ressource sur le cluster d'espace de noms.
- Tenez compte des exigences spécifiques de l'Astra Trident lorsque vous déployez le centre de contrôle Astra dans un environnement TKG ou TKGi. Pour plus d'informations, reportez-vous à la section ["Documentation Astra Trident"](#).



Le token de fichier de configuration VMware TKG et TKGi par défaut expire dix heures après le déploiement. Si vous utilisez des produits de la gamme Tanzu, vous devez générer un fichier de configuration de cluster Kubernetes Tanzu avec un jeton non expirant pour éviter les problèmes de connexion entre Astra Control Center et les clusters d'applications gérés. Pour obtenir des instructions, rendez-vous sur ["Documentation produit relative au data Center VMware NSX-T"](#)

Et la suite

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

Démarrage rapide pour Astra Control Center

Voici un aperçu 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.



Vérifiez la configuration des clusters Kubernetes

Assurez-vous que votre environnement répond à ces exigences.

Cluster Kubernetes

- "Assurez-vous que votre environnement répond aux exigences de votre environnement opérationnel"
- "Configuration de la détection d'entrée pour l'équilibrage de la charge sur les clusters Kubernetes sur site"

Intégration du stockage

- "Vérifiez que votre environnement inclut la version prise en charge d'Astra Trident"
- "Préparez les nœuds worker"
- "Configurer le système back-end de stockage Astra Trident"
- "Configurez des classes de stockage Astra Trident"
- "Installation du contrôleur de snapshot de volume Astra Trident"
- "Créer une classe de snapshot de volume"

Informations d'identification ONTAP

- "Configurez les identifiants ONTAP"

2

Téléchargez et installez Astra Control Center

Effectuez ces tâches d'installation.

- "Téléchargez Astra Control Center à partir de la page de téléchargement du site de support NetApp"
- Obtenez le fichier de licence NetApp :
 - "Si vous évaluez Astra Control Center, téléchargez le fichier de licence d'évaluation"
 - "Si vous avez déjà acheté Astra Control Center, générez votre fichier de licence"
- "Poser le centre de contrôle Astra"
- "Effectuez d'autres étapes de configuration facultatives"

3

Effectuez certaines tâches de configuration initiales

Réalisez certaines tâches de base pour démarrer.

- "Ajouter une licence"
- "Préparez votre environnement à la gestion du cluster"
- "Ajouter un cluster"
- "Ajout d'un système back-end"
- "Ajouter un godet"

4

Utilisez Astra Control Center

Après avoir terminé la configuration du centre de contrôle Astra, voici ce que vous pourriez faire ensuite. Vous pouvez utiliser l'interface utilisateur Astra Control (UI) ou le "[API de contrôle Astra](#)".

- ["Gérer des applications"](#)
- ["Protégez vos applications"](#): Configurer des stratégies de protection et répliquer, cloner et migrer des applications.
- ["Gestion des comptes"](#): Utilisateurs, rôles, LDAP, informations d'identification, etc
- ["Vous pouvez également vous connecter à Cloud Insights"](#): Permet d'afficher des mesures sur l'état de santé de votre système.

Pour en savoir plus

- ["API de contrôle Astra"](#)
- ["Mettez à niveau Astra Control Center"](#)
- ["Aidez-vous d'Astra Control"](#)

Présentation de l'installation

Choisissez l'une des procédures d'installation suivantes du centre de contrôle Astra :

- ["Installer le centre de contrôle Astra en suivant la procédure standard"](#)
- ["\(Si vous utilisez Red Hat OpenShift\) installez Astra Control Center à l'aide d'OpenShift OperatorHub"](#)
- ["Installer le centre de contrôle Astra avec un système de stockage back-end Cloud Volumes ONTAP"](#)

Selon votre environnement, une configuration supplémentaire peut être nécessaire après l'installation d'Astra Control Center :

- ["Configurer le centre de contrôle Astra après l'installation"](#)

Installer le centre de contrôle Astra en suivant la procédure standard

Pour installer Astra Control Center, téléchargez le bundle d'installation depuis le site de support NetApp et effectuez les opérations suivantes. Vous pouvez utiliser cette procédure pour installer Astra Control Center dans des environnements connectés à Internet ou équipés d'un filtre à air.

Autres procédures d'installation

- **Installer avec RedHat OpenShift OperatorHub**: Utilisez ceci ["autre procédure"](#) Pour installer Astra Control Center sur OpenShift à l'aide d'OperatorHub.
- **Installer dans le Cloud public avec Cloud Volumes ONTAP backend**: Utilisez ["ces procédures"](#) Pour installer Astra Control Center dans Amazon Web Services (AWS), Google Cloud Platform (GCP) ou Microsoft Azure avec un système de stockage principal Cloud Volumes ONTAP.

Pour une démonstration du processus d'installation d'Astra Control Center, reportez-vous à la section ["vidéo"](#).

Ce dont vous avez besoin

- ["Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center"](#).
- Si vous avez configuré ou que vous souhaitez configurer des stratégies de sécurité de pod dans votre

environnement, familiarisez-vous avec les stratégies de sécurité de pod et leur incidence sur l'installation d'Astra Control Center. Voir "[Comprendre les restrictions de la stratégie de sécurité du pod](#)".

- Assurez-vous que tous les services API sont en état de santé et disponibles :

```
kubectl get apiservices
```

- Assurez-vous que le FQDN Astra que vous prévoyez d'utiliser est routable vers ce cluster. Cela signifie que vous avez une entrée DNS dans votre serveur DNS interne ou que vous utilisez une route URL de base déjà enregistrée.
- Si un cert Manager existe déjà dans le cluster, vous devez en effectuer certaines "[étapes préalables](#)" Pour qu'Astra Control Center ne tente pas d'installer son propre gestionnaire de certificat. Par défaut, Astra Control Center installe son propre gestionnaire de certificats lors de l'installation.

Description de la tâche

Le processus d'installation d'Astra Control Center vous aide à :

- Poser les composants Astra dans le `netapp-acc` (ou espace de nom personnalisé).
- Créez un compte d'administrateur propriétaire Astra Control par défaut.
- Définissez une adresse e-mail d'utilisateur administratif et un mot de passe de configuration initiale par défaut. Ce rôle de propriétaire est attribué à cet utilisateur pour la première connexion à l'interface utilisateur.
- Vérifiez que toutes les POD Astra Control Center sont en cours d'exécution.
- Installez l'interface utilisateur du centre de contrôle Astra.



Ne supprimez pas l'opérateur du centre de contrôle Astra (par exemple, `kubectl delete -f astra_control_center_operator_deploy.yaml`) À tout moment pendant l'installation ou le fonctionnement d'Astra Control Center pour éviter de supprimer les modules.

Étapes

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

- [Téléchargez et extrayez Astra Control Center](#)
- [Installez le plug-in NetApp Astra kubectl](#)
- [Ajoutez les images à votre registre local](#)
- [Configurez l'espace de noms et le secret pour les registres avec les exigences d'authentification](#)
- [Poser le conducteur du centre de commande Astra](#)
- [Configurer le centre de contrôle Astra](#)
- [Installation complète du centre de contrôle Astra et du conducteur](#)
- [Vérifiez l'état du système](#)
- [Configurer l'entrée pour l'équilibrage de charge](#)
- [Connectez-vous à l'interface utilisateur du centre de contrôle Astra](#)

Téléchargez et extrayez Astra Control Center

1. Accédez au "[Page de téléchargement de l'évaluation Astra Control Center](#)" Sur le site de support NetApp.
2. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recommandé mais facultatif) Téléchargez le lot de certificats et de signatures pour Astra Control Center (`astra-control-center-certs-[version].tar.gz`) pour vérifier la signature du paquet :

```
tar -vxf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

La sortie s'affiche `Verified OK` une fois la vérification terminée.

4. Extraire les images du pack Astra Control Center :

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

Installez le plug-in NetApp Astra kubectl

Le plug-in de ligne de commande NetApp Astra kubectl permet de gagner du temps lors de l'exécution des tâches courantes associées au déploiement et à la mise à niveau d'Astra Control Center.

Ce dont vous avez besoin

NetApp fournit des binaires de plug-ins pour différentes architectures CPU et systèmes d'exploitation. Avant d'effectuer cette tâche, vous devez savoir quelle unité centrale et quel système d'exploitation vous possédez.

Étapes

1. Répertoriez les binaires NetApp Astra kubectl disponibles et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et votre architecture de processeur :



La bibliothèque de plug-ins kubectl fait partie du bundle tar et est extraite dans le dossier `kubectl-astra`.

```
ls kubectl-astra/
```

2. Déplacez le bon binaire dans le chemin actuel et renommez-le `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Ajoutez les images à votre registre local

1. Suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Envoyez les images du package dans le répertoire d'images Astra Control Center vers votre registre local. Effectuez les remplacements suivants avant d'exécuter le `push-images` commande :

- Remplacez `<BUNDLE_FILE>` par le nom du fichier bundle Astra Control (`acc.manifest.bundle.yaml`).
- Remplacer `<MY_FULL_REGISTRY_PATH>` par l'URL du référentiel Docker, par exemple `"<a href="https://<docker-registry>" class="bare">https://<docker-registry>"`.
- Remplacez `<MY_REGISTRY_USER>` par le nom d'utilisateur.
- Remplacez `<MY_REGISTRY_TOKEN>` par un jeton autorisé pour le registre.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

3. Préparez et exécutez l'un des scripts suivants qui est personnalisé pour la version de Podman que vous utilisez. Remplacez `<MY_FULL_REGISTRY_PATH>` par l'URL de votre référentiel qui inclut tous les sous-répertoires.

```
<strong>Podman 4</strong>
```



```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



Le chemin d'accès à l'image que le script crée doit ressembler aux éléments suivants, selon la configuration de votre registre : <https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

Configurez l'espace de noms et le secret pour les registres avec les exigences d'authentification

1. Exporter le KUBECONFIG pour le groupe hôte du centre de contrôle Astra :

```
export KUBECONFIG=[file path]
```



Avant de terminer l'installation, assurez-vous que votre KUBECONFIG pointe vers le groupe d'instruments où vous souhaitez installer le centre de contrôle Astra. Le KUBECONFIG ne peut contenir qu'un seul contexte.

2. 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 :



Le paramètre fictif `your_registry_path` doit correspondre à l'emplacement des images que vous avez téléchargées précédemment (par exemple, `[Registry_URL]/netapp/astra/astracc/22.11.0-82`).

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

Exemple de réponse :

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



Si vous supprimez l'espace de noms après la génération du secret, recréez l'espace de noms, puis régénérez le secret pour l'espace de noms.

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

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

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 namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

Réponse

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

Poser le conducteur du centre de commande Astra

1. Modifier le répertoire :

```
cd manifests
```

2. 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
```



Un échantillon annoté YAML suit ces étapes.

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. Changez `[your_registry_path]` pour le kube-rbac-proxy image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).

c. Changez `[your_registry_path]` pour le acc-operator-controller-manager image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).

```
<strong>astra_control_center_operator_deploy.yaml</strong>
```

```
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
  strategy:
    type: Recreate
  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: [your_registry_path]/kube-rbac-proxy:v4.8.0
          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
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_INSTALLTIMEOUT
              value: 5m
          image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
              port: 8081
              initialDelaySeconds: 15
              periodSeconds: 20
          name: manager
          readinessProbe:

```

```

    httpGet:
      path: /readyz
      port: 8081
      initialDelaySeconds: 5
      periodSeconds: 10
    resources:
      limits:
        cpu: 300m
        memory: 750Mi
      requests:
        cpu: 100m
        memory: 75Mi
    securityContext:
      allowPrivilegeEscalation: false
imagePullSecrets: []
    securityContext:
      runAsUser: 65532
    terminationGracePeriodSeconds: 10

```

3. 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.apiextensions.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

```

4. Vérifiez que les pods sont en cours d'exécution :

```
kubectl get pods -n netapp-acc-operator
```

Configurer le centre de contrôle Astra

1. Modifiez le fichier de ressources personnalisées (CR) Astra Control Center (`astra_control_center.yaml`) pour créer des comptes, un support, un registre et d'autres configurations nécessaires :

```
vim astra_control_center.yaml
```



Un échantillon annoté YAML suit ces étapes.

2. Modifiez ou confirmez les paramètres suivants :

`<code>accountName</code>`

Réglage	Guidage	Type	Exemple
<code>accountName</code>	Modifiez le <code>accountName</code> Chaîne du nom que vous souhaitez associer au compte Astra Control Center. Il ne peut y avoir qu'un seul nom de compte.	chaîne	Exemple

`<code>astraVersion</code>`

Réglage	Guidage	Type	Exemple
<code>astraVersion</code>	La version d'Astra Control Center à déployer. Aucune action n'est nécessaire pour ce paramètre car la valeur sera pré-remplie.	chaîne	22.11.0-82

`<code>astraAddress</code>`

Réglage	Guidage	Type	Exemple
<code>astraAddress</code>	<p>Modifiez le <code>astraAddress</code> Chaîne sur le FQDN (recommandé) ou l'adresse IP que vous souhaitez utiliser dans votre navigateur pour accéder à Astra Control Center. Cette adresse définit la façon dont Astra Control Center se trouve dans votre centre de données et est le même FQDN ou l'adresse IP que vous avez fournie à partir de votre équilibreur de charge une fois que vous avez terminé "Exigences du centre de contrôle Astra". REMARQUE : ne pas utiliser <code>http://</code> ou <code>https://</code> dans l'adresse. Copier ce FQDN pour l'utiliser dans un plus tard.</p>	chaîne	<code>astra.example.com</code>

<code>autoSupport</code>

Vos sélections dans cette section déterminent si vous allez participer à l'application de support proactif de NetApp, à NetApp Active IQ et à l'endroit où les données seront envoyées. Une connexion Internet est requise (port 442) et toutes les données de support sont anonymisées.

Réglage	Utiliser	Guidage	Type	Exemple
<code>autoSupport.enrolled</code>	Soit <code>enrolled</code> ou <code>url</code> les champs doivent être sélectionnés	Changer <code>enrolled</code> Pour AutoSupport à <code>false</code> pour les sites sans connexion internet ou sans conservation <code>true</code> pour les sites connectés. Un réglage de <code>true</code> Les données anonymes peuvent être envoyées à NetApp pour bénéficier d'un support. La sélection par défaut est <code>false</code> Aucune donnée de support n'est envoyée à NetApp.	Booléen	<code>false</code> (cette valeur est la valeur par défaut)
<code>autoSupport.url</code>	Soit <code>enrolled</code> ou <code>url</code> les champs doivent être sélectionnés	Cette URL détermine l'emplacement d'envoi des données anonymes.	chaîne	https://support.netapp.com/asupprod/post/1.0/postAsup

`<code>email</code>`

Réglage	Guidage	Type	Exemple
email	Modifiez le email chaîne à l'adresse d'administrateur initiale par défaut. Copiez cette adresse e-mail pour l'utiliser dans un plus tard . Cette adresse e-mail sera utilisée comme nom d'utilisateur du compte initial pour se connecter à l'interface utilisateur et sera informée des événements dans Astra Control.	chaîne	admin@example.com

`<code>firstName</code>`

Réglage	Guidage	Type	Exemple
firstName	Prénom de l'administrateur initial par défaut associé au compte Astra. Le nom utilisé ici sera visible dans un en-tête de l'interface utilisateur après votre première connexion.	chaîne	SRE

`<code>lastName</code>`

Réglage	Guidage	Type	Exemple
lastName	Nom de l'administrateur initial par défaut associé au compte Astra. Le nom utilisé ici sera visible dans un en-tête de l'interface utilisateur après votre première connexion.	chaîne	Admin

<code>imageRegistry</code>

Vos sélections dans cette section définissent le registre d'images du conteneur qui héberge les images d'application Astra, l'opérateur du centre de contrôle Astra et le référentiel Helm d'Astra Control Center.

Réglage	Utiliser	Guidage	Type	Exemple
<code>imageRegistry.name</code>	Obligatoire	Nom du registre d'images dans lequel vous avez poussé les images dans le étape précédente . Ne pas utiliser <code>http://</code> ou <code>https://</code> dans le nom du registre.	chaîne	<code>example.registry.com/astra</code>
<code>imageRegistry.secret</code>	Obligatoire si la chaîne que vous avez entrée pour <code>imageRegistry.name</code> requires a secret. IMPORTANT: If you are using a registry that does not require authorization, you must delete this <code>secret</code> ligne comprise entre <code>imageRegistry</code> sinon, l'installation échouera.	Nom du secret Kubernetes utilisé pour s'authentifier auprès du registre d'images.	chaîne	<code>astra-registry-cred</code>

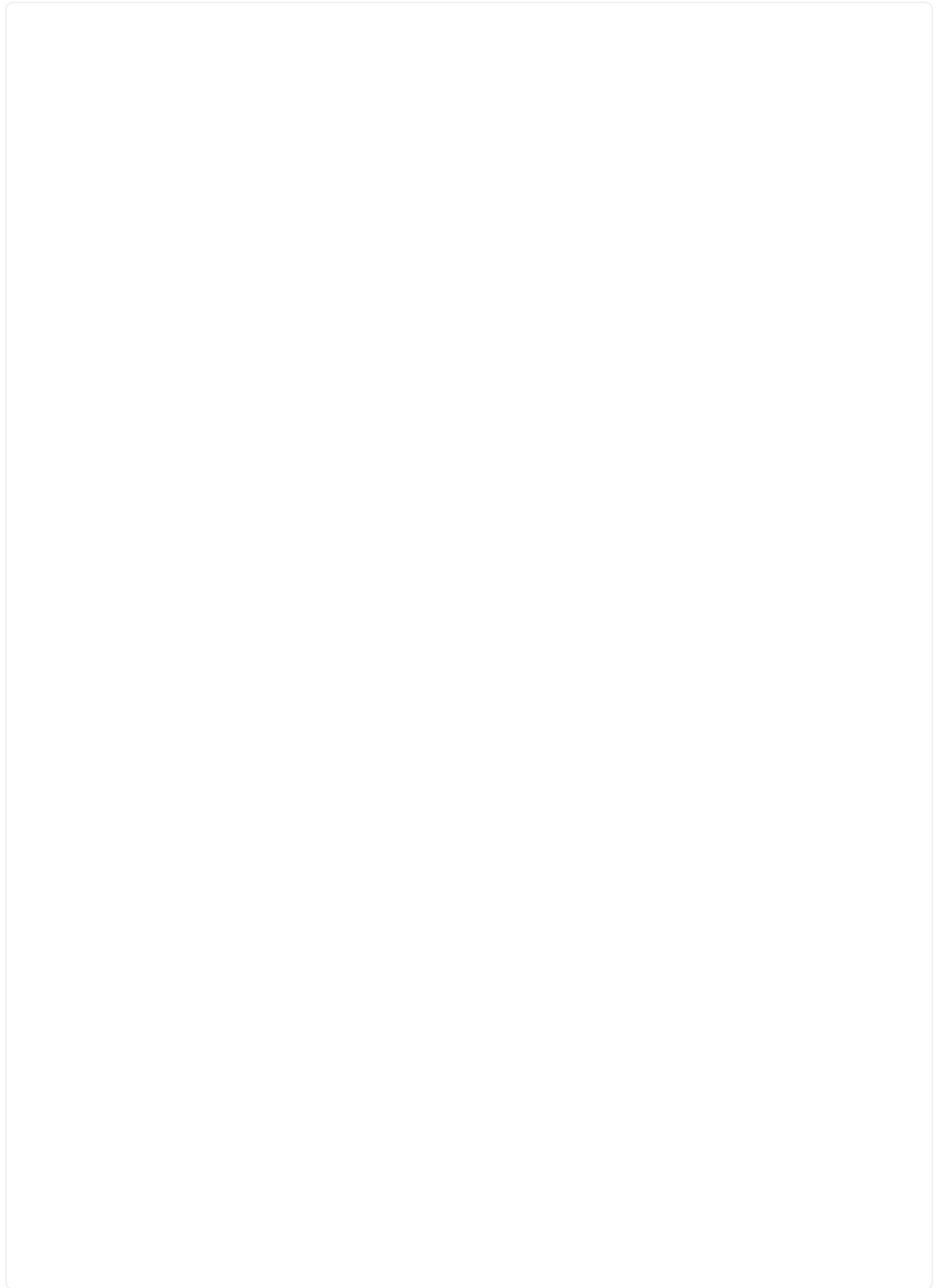
`<code>storageClass</code>`

Réglage	Guidage	Type	Exemple
<code>storageClass</code>	<p>Modifiez le <code>storageClass</code> valeur à partir de <code>ontap-gold</code> Sur une autre ressource de stockage Trident, tel que requis par votre installation. Lancer la commande <code>kubectl get sc</code> pour déterminer vos classes de stockage configurées existantes. L'une des classes de stockage basées sur Trident doit être saisie dans le fichier manifeste (<code>astra-control-center-<version>.manifest</code>) Et sera utilisé pour ASTRA PVS. Si elle n'est pas définie, la classe de stockage par défaut sera utilisée. REMARQUE : si une classe de stockage par défaut est configurée, assurez-vous qu'elle est la seule classe de stockage à avoir l'annotation par défaut.</p>	chaîne	<code>ontap-gold</code>

`<code>volumeReclaimPolicy</code>`

Réglage	Guidage	Type	Options
<code>volumeReclaimPolicy</code>	Cette règle définit la règle de récupération pour les volumes persistants d'Astra. Définition de cette règle sur <code>Retain</code> Conserve les volumes persistants après la suppression d'Astra. Définition de cette règle sur <code>Delete</code> supprime les volumes persistants après la suppression d'astra. Si cette valeur n'est pas définie, les PV sont conservés.	chaîne	<ul style="list-style-type: none">• <code>Retain</code> (Il s'agit de la valeur par défaut)• <code>Delete</code>

`<code>ingressType</code>`





Réglage	Guidage	Type	Options
ingressType	<p>Utilisez l'un des types d'entrées suivants</p> <pre>:*Generic*</pre> <p>(ingressType: "Generic") (Par défaut) utilisez cette option lorsque vous avez un autre contrôleur d'entrée en service ou que vous préférez utiliser votre propre contrôleur d'entrée. Après le déploiement du centre de contrôle Astra, vous devez configurer le "contrôleur d'entrée" Pour exposer Astra Control Center avec une URL AccTraefik</p> <pre>(ingressType: "AccTraefik")</pre> <p>Utilisez cette option si vous préférez ne pas configurer un contrôleur d'entrée. Ceci déploie le centre de contrôle Astra traefik Passerelle en tant que service de type Kubernetes LoadBalancer. Le centre de contrôle Astra utilise un service de type « équilibreur de charge »</p> <p>(svc/traefik Dans l'espace de noms du centre de contrôle Astra), et exige qu'il se voit attribuer une adresse IP externe accessible. Si des équilibreurs de charge sont autorisés dans votre environnement et que vous n'en avez pas encore configuré, vous pouvez utiliser MetalLB ou un autre équilibreur de charge de service externe pour attribuer une adresse IP externe au service. Dans la configuration du serveur</p>	chaîne	<ul style="list-style-type: none"> • Generic (il s'agit de la valeur par défaut) • AccTraefik

`<code>astraResourcesScaler</code>`

Réglage	Guidage	Type	Options
<code>astraResourcesScaler</code>	<p>Options d'évolutivité pour les limites de ressources AstrakControlCenter. Par défaut, Astra Control Center se déploie avec des demandes de ressources définies pour la plupart des composants d'Astra. Avec cette configuration, la pile logicielle Astra Control Center est plus performante dans les environnements soumis à une charge et à une évolutivité accrues des applications. Cependant, dans les scénarios utilisant des grappes de développement ou de test plus petites, le champ CR <code>astraResourcesScaler</code> peut être réglé sur <code>Off</code>. Cela désactive les demandes de ressources et permet un déploiement sur les clusters plus petits.</p>	chaîne	<ul style="list-style-type: none">• Default (Il s'agit de la valeur par défaut)• Off

`<code>crds</code>`

Vos sélections dans cette section déterminent comment Astra Control Center doit traiter les CRD.

Réglage	Guidage	Type	Exemple
<code>crds.externalCertManager</code>	Si vous utilisez un gestionnaire de certificats externe, modifiez-le <code>externalCertManager</code> à <code>true</code> . La valeur par défaut <code>false</code> Provoque l'installation d'Astra Control Center de ses propres CRD de <code>cert Manager</code> lors de l'installation. Les CRDS sont des objets à l'échelle du cluster et leur installation peut avoir un impact sur d'autres parties du cluster. Vous pouvez utiliser cet indicateur pour signaler à Astra Control Center que ces CRD seront installés et gérés par l'administrateur de cluster en dehors du centre de contrôle Astra.	Booléen	<code>False</code> (cette valeur est la valeur par défaut)
<code>crds.externalTraefik</code>	Par défaut, Astra Control Center installe les CRD Traefik requis. Les CRDS sont des objets à l'échelle du cluster et leur installation peut avoir un impact sur d'autres parties du cluster. Vous pouvez utiliser cet indicateur pour signaler à Astra Control Center que ces CRD seront installés et gérés par l'administrateur de cluster en dehors du centre de contrôle Astra.	Booléen	<code>False</code> (cette valeur est la valeur par défaut)

```
<strong>astra_control_center.yaml</strong>
```

```
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: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  astraResourcesScaler: "Default"
  additionalValues: {}
  crds:
    externalTraefik: false
    externalCertManager: false
```

Installation complète du centre de contrôle Astra et du conducteur

1. 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 namespace]
```

Exemple de réponse :

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

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

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

Exemple de réponse :

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

Vérifiez l'état du système

Vous pouvez vérifier l'état du système à l'aide des commandes kubectl. Si vous préférez utiliser OpenShift, vous pouvez utiliser des commandes oc comparables pour les étapes de vérification.

Étapes

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

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

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-76d8d845c9-ggds2 14m	1/1	Running	0
activity-6cc67ff9f4-z48mr (8m32s ago) 9m	1/1	Running	2
api-token-authentication-7s67v 8m56s	1/1	Running	0
api-token-authentication-bplb4 8m56s	1/1	Running	0
api-token-authentication-p2c9z 8m56s	1/1	Running	0
asup-6cdfbc6795-md8vn 9m14s	1/1	Running	0
authentication-9477567db-8hnc9 7m4s	1/1	Running	0
bucket-service-f4dbdfcd6-wqzkw 8m48s	1/1	Running	0
cert-manager-bb756c7c4-wm2cv 14m	1/1	Running	0
cert-manager-cainjector-c9bb86786-8wrf5 14m	1/1	Running	0
cert-manager-webhook-dd465db99-j2w4x 14m	1/1	Running	0
certificates-68dff9cdd6-kcvml (8m43s ago) 9m2s	1/1	Running	2
certificates-68dff9cdd6-rsnsb 9m2s	1/1	Running	0
cloud-extension-69d48c956c-2s8dt (8m43s ago) 9m24s	1/1	Running	3
cloud-insights-service-7c4f48b978-7gvlh (8m50s ago) 9m28s	1/1	Running	3
composite-compute-7d9ff5f68-nxbhl 8m51s	1/1	Running	0
composite-volume-57b4756d64-nl66d 9m13s	1/1	Running	0
credentials-6dbc55f89f-qpzff 11m	1/1	Running	0
entitlement-67bfb6d7-gl6kp (8m33s ago) 9m38s	1/1	Running	4
features-856cc4dccc-mxbdb 9m20s	1/1	Running	0
fluent-bit-ds-4rtsp 6m54s	1/1	Running	0

fluent-bit-ds-9rql1	1/1	Running	0
6m54s			
fluent-bit-ds-w5mp7	1/1	Running	0
6m54s			
graphql-server-7c7cc49776-jz2kn	1/1	Running	0
2m29s			
identity-87c59c975-9jpnf	1/1	Running	0
9m6s			
influxdb2-0	1/1	Running	0
13m			
keycloak-operator-84ff6d59d4-qcnmc	1/1	Running	0
7m1s			
krakend-cbf6c7df9-mdtzv	1/1	Running	0
2m30s			
license-5b888b78bf-plj6j	1/1	Running	0
9m32s			
login-ui-846b4664dd-fz8hv	1/1	Running	0
2m24s			
loki-0	1/1	Running	0
13m			
metrics-facade-779cc9774-n26rw	1/1	Running	0
9m18s			
monitoring-operator-974db78f-pkspq	2/2	Running	0
6m58s			
nats-0	1/1	Running	0
13m			
nats-1	1/1	Running	0
13m			
nats-2	1/1	Running	0
13m			
nautilus-7bdc7ddc54-49tfn	1/1	Running	0
7m50s			
nautilus-7bdc7ddc54-cwc79	1/1	Running	0
9m36s			
openapi-5584ff9f46-gbrdj	1/1	Running	0
9m17s			
openapi-5584ff9f46-z9mzk	1/1	Running	0
9m17s			
packages-bfc58cc98-lpxq9	1/1	Running	0
8m58s			
polaris-consul-consul-server-0	1/1	Running	0
13m			
polaris-consul-consul-server-1	1/1	Running	0
13m			
polaris-consul-consul-server-2	1/1	Running	0
13m			

polaris-keycloak-0 (6m15s ago) 6m56s	1/1	Running	3
polaris-keycloak-1 4m22s	1/1	Running	0
polaris-keycloak-2 3m41s	1/1	Running	0
polaris-keycloak-db-0 6m56s	1/1	Running	0
polaris-keycloak-db-1 4m23s	1/1	Running	0
polaris-keycloak-db-2 3m36s	1/1	Running	0
polaris-mongodb-0 13m	2/2	Running	0
polaris-mongodb-1 13m	2/2	Running	0
polaris-mongodb-2 12m	2/2	Running	0
polaris-ui-5ccff47897-8rzgh 2m33s	1/1	Running	0
polaris-vault-0 13m	1/1	Running	0
polaris-vault-1 13m	1/1	Running	0
polaris-vault-2 13m	1/1	Running	0
public-metrics-6cb7bfc49b-p54xm (8m29s ago) 9m31s	1/1	Running	1
storage-backend-metrics-5c77994586-kjn48 8m52s	1/1	Running	0
storage-provider-769fdc858c-62w54 8m54s	1/1	Running	0
task-service-9ffc484c5-kx9f4 (8m44s ago) 9m34s	1/1	Running	3
telegraf-ds-bphb9 6m54s	1/1	Running	0
telegraf-ds-rtsm2 6m54s	1/1	Running	0
telegraf-ds-s9h5h 6m54s	1/1	Running	0
telegraf-rs-lbpv7 6m54s	1/1	Running	0
telemetry-service-57cfb998db-zjx78 (8m40s ago) 9m26s	1/1	Running	1
tenancy-5d5dfbcf9f-vmbxh 9m5s	1/1	Running	0

```

traefik-7b87c4c474-jmcp2      1/1      Running   0
2m24s
traefik-7b87c4c474-t9k8x     1/1      Running   0
2m24s
trident-svc-c78f5b6bd-nwdsq  1/1      Running   0
9m22s
vault-controller-55bbc96668-c6425 1/1      Running   0
11m
vault-controller-55bbc96668-lq9n9 1/1      Running   0
11m
vault-controller-55bbc96668-rfkgg 1/1      Running   0
11m

```

2. (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
```



`accHost` l'enregistrement du cluster est l'une des dernières opérations. en cas de défaillance, le déploiement ne pourra pas échouer. Dans l'éventualité où un échec d'enregistrement du cluster était indiqué dans les journaux, vous pouvez essayer de nouveau l'enregistrement via le ["Ajout du flux de travail du cluster dans l'interface utilisateur"](#) Ou API.

3. Lorsque tous les modules sont en cours d'exécution, vérifiez que l'installation a réussi (`READY` est `True`) Et obtenez le mot de passe de configuration initial que vous utiliserez lorsque vous vous connectez à Astra Control Center :

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Réponse :

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.11.0-82	10.111.111.111
True			



Copiez la valeur UUID. Le mot de passe est `ACC-` Suivi de la valeur UUID (`ACC-[UUID]` ou, dans cet exemple, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Configurer l'entrée pour l'équilibrage de charge

Vous pouvez configurer un contrôleur d'entrée Kubernetes qui gère l'accès externe aux services. Ces procédures fournissent des exemples de configuration pour un contrôleur d'entrée si vous avez utilisé la valeur par défaut de `ingressType: "Generic"` Dans la ressource personnalisée Astra Control Center (`astra_control_center.yaml`). Vous n'avez pas besoin d'utiliser cette procédure si vous avez spécifié `ingressType: "AccTraefik"` Dans la ressource personnalisée Astra Control Center (`astra_control_center.yaml`).

Après le déploiement du centre de contrôle Astra, vous devrez configurer le contrôleur d'entrée pour exposer le centre de contrôle Astra à une URL.

Les étapes de configuration varient en fonction du type de contrôleur d'entrée utilisé. Le centre de contrôle Astra prend en charge de nombreux types de contrôleurs d'entrée. Ces procédures de configuration fournissent des exemples pour les types de contrôleurs d'entrée suivants :

- Entrée Istio
- Contrôleur d'entrée Nginx
- Contrôleur d'entrée OpenShift

Ce dont vous avez besoin

- Le requis "[contrôleur d'entrée](#)" doit déjà être déployé.
- Le "[classe d'entrée](#)" correspondant au contrôleur d'entrée doit déjà être créé.

Étapes pour l'entrée Istio

1. Configurer l'entrée Istio.



Cette procédure suppose que Istio est déployé à l'aide du profil de configuration par défaut.

2. Rassemblez ou créez le certificat et le fichier de clé privée souhaités pour la passerelle d'entrée.

Vous pouvez utiliser un certificat signé par une autorité de certification ou auto-signé. Le nom commun doit être l'adresse Astra (FQDN).

Exemple de commande :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

3. Créez un secret `tls secret name` de type `kubernetes.io/tls` Pour une clé privée TLS et un certificat dans `istio-system namespace` Comme décrit dans les secrets TLS.

Exemple de commande :

```
kubectl create secret tls [tls secret name] --key="tls.key"
--cert="tls.crt" -n istio-system
```




Le nom du secret doit correspondre au `spec.tls.secretName` fourni dans `istio-ingress.yaml` fichier.

4. Déployer une ressource d'entrée dans le `netapp-acc` (ou nom personnalisé) de l'espace de noms utilisant le type de ressource `v1` pour un schéma (`istio-Ingress.yaml` est utilisé dans cet exemple) :

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Appliquer les modifications :

```
kubectl apply -f istio-Ingress.yaml
```

6. Vérifier l'état de l'entrée :

```
kubectl get ingress -n [netapp-acc or custom namespace]
```

Réponse :

```
NAME      CLASS HOSTS                ADDRESS          PORTS   AGE
ingress   istio astra.example.com 172.16.103.248 80, 443 1h
```

7. Terminer l'installation du centre de contrôle Astra.

Étapes du contrôleur d'entrée Nginx

1. Créer un secret de type `kubernetes.io/tls` Pour une clé privée TLS et un certificat dans `netapp-acc` (ou espace de noms personnalisé) comme décrit dans "[Secrets TLS](#)".
2. Déployez une ressource entrée dans `netapp-acc` (ou nom personnalisé) de l'espace de noms utilisant le type de ressource `v1` pour un schéma (`nginx-Ingress.yaml` est utilisé dans cet exemple) :

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
      - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

3. Appliquer les modifications :

```
kubectl apply -f nginx-Ingress.yaml
```



NetApp recommande d'installer le contrôleur nginx en tant que déploiement plutôt qu'en tant que `daemonSet`.

Étapes du contrôleur d'entrée OpenShift

1. Procurez-vous votre certificat et obtenez les fichiers de clé, de certificat et d'autorité de certification prêts à l'emploi par la route OpenShift.
2. Création de la route OpenShift :

```
oc create route edge --service=traefik --port=web -n [netapp-acc or custom namespace] --insecure-policy=Redirect --hostname=<ACC address> --cert=cert.pem --key=key.pem
```

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

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

Étapes

1. Dans un navigateur, saisissez le nom de domaine complet (y compris le `https://` prefix) que vous avez utilisé dans `astraAddress` dans le `astra_control_center.yaml` CR quand [Vous avez installé Astra Control Center](#).
2. Acceptez les certificats auto-signés si 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.yaml` CR quand [Vous avez installé Astra Control Center](#), suivi du mot de passe de configuration initiale (`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.



S'il s'agit de votre première connexion et que vous oubliez le mot de passe et qu'aucun autre compte d'utilisateur administratif n'a encore été créé, contactez "[Support NetApp](#)" pour obtenir de l'aide sur la récupération des mots de

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

Et la suite

- (Facultatif) en fonction de votre environnement, effectuez l'installation complète après l'installation "[étapes de configuration](#)".
- Terminez le déploiement en effectuant le processus "[tâches de configuration](#)".

=
:allow-uri-read:

Installez Astra Control Center à l'aide d'OpenShift OperatorHub

Si vous utilisez Red Hat OpenShift, vous pouvez installer Astra Control Center à l'aide de l'opérateur certifié Red Hat. Utilisez cette procédure pour installer le centre de contrôle Astra à partir du "[Catalogue de l'écosystème Red Hat](#)" Ou utilisez Red Hat OpenShift Container Platform.

Une fois cette procédure terminée, vous devez revenir à la procédure d'installation pour terminer le "[les étapes restantes](#)" pour vérifier que l'installation a réussi et ouvrir une session.

Ce dont vous avez besoin

- * Conditions préalables à l'environnement remplies* : "[Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center](#)".
- **Opérateurs de grappe et services API sains** :
 - Depuis votre cluster OpenShift, assurez-vous que tous les opérateurs de clusters sont en état sain :

```
oc get clusteroperators
```

- Depuis votre cluster OpenShift, assurez-vous que tous les services d'API sont en état sain :

```
oc get apiservices
```

- **Adresse FQDN** : obtention d'une adresse FQDN pour Astra Control Center dans votre centre de données.
- **Autorisations OpenShift** : obtenez les autorisations nécessaires et l'accès à Red Hat OpenShift Container Platform pour effectuer les étapes d'installation décrites.
- **Cert Manager configuré** : si un cert Manager existe déjà dans le cluster, vous devez en effectuer certaines "[étapes préalables](#)" Pour qu'Astra Control Center n'installe pas son propre gestionnaire de certificat. Par défaut, Astra Control Center installe son propre gestionnaire de certificats lors de l'installation.
- **Contrôleur d'entrée Kubernetes** : si vous disposez d'un contrôleur d'entrée Kubernetes qui gère l'accès externe aux services, comme l'équilibrage de charge dans un cluster, vous devez le configurer pour l'utiliser avec Astra Control Center :

- a. Créer l'espace de noms de l'opérateur :

```
oc create namespace netapp-acc-operator
```

- b. "[Terminez l'installation](#)" pour votre type de contrôleur d'entrée.

Étapes

- [Téléchargez et extrayez Astra Control Center](#)
- [Installez le plug-in NetApp Astra kubectI](#)
- [Ajoutez les images à votre registre local](#)
- [Recherchez la page d'installation de l'opérateur](#)
- [Poser l'opérateur](#)
- [Poser le centre de contrôle Astra](#)

Téléchargez et extrayez Astra Control Center

1. Accédez au "[Page de téléchargement de l'évaluation Astra Control Center](#)" Sur le site de support NetApp.
2. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recommandé mais facultatif) Téléchargez le lot de certificats et de signatures pour Astra Control Center (`astra-control-center-certs-[version].tar.gz`) pour vérifier la signature du paquet :

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

La sortie s'affiche `Verified OK` une fois la vérification terminée.

4. Extraire les images du pack Astra Control Center :

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

Installez le plug-in NetApp Astra kubectI

Le plug-in de ligne de commande NetApp Astra kubectI permet de gagner du temps lors de l'exécution des tâches courantes associées au déploiement et à la mise à niveau d'Astra Control Center.

Ce dont vous avez besoin

NetApp fournit des binaires de plug-ins pour différentes architectures CPU et systèmes d'exploitation. Avant d'effectuer cette tâche, vous devez savoir quelle unité centrale et quel système d'exploitation vous possédez.

Étapes

1. Répertoriez les binaires NetApp Astra kubectl disponibles et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et votre architecture de processeur :



La bibliothèque de plug-ins kubectl fait partie du bundle tar et est extraite dans le dossier kubectl-astra.

```
ls kubectl-astra/
```

2. Déplacez le bon binaire dans le chemin actuel et renommez-le kubectl-astra:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Ajoutez les images à votre registre local

1. Suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Envoyez les images du package dans le répertoire d'images Astra Control Center vers votre registre local. Effectuez les remplacements suivants avant d'exécuter le `push-images` commande :

- Remplacez `<BUNDLE_FILE>` par le nom du fichier bundle Astra Control (`acc.manifest.bundle.yaml`).
- Remplacer `<MY_FULL_REGISTRY_PATH>` par l'URL du référentiel Docker, par exemple `<a href="https://<docker-registry>" class="bare">https://<docker-registry>"`.
- Remplacez `<MY_REGISTRY_USER>` par le nom d'utilisateur.
- Remplacez `<MY_REGISTRY_TOKEN>` par un jeton autorisé pour le registre.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

3. Préparez et exécutez l'un des scripts suivants qui est personnalisé pour la version de Podman que vous utilisez. Remplacez `<MY_FULL_REGISTRY_PATH>` par l'URL de votre référentiel qui inclut tous les sous-répertoires.

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



Le chemin d'accès à l'image que le script crée doit ressembler aux éléments suivants, selon la configuration de votre registre : <https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

Recherchez la page d'installation de l'opérateur

1. Effectuez l'une des procédures suivantes pour accéder à la page d'installation de l'opérateur :

- Depuis la console Web Red Hat OpenShift :
 - i. Connectez-vous à l'interface utilisateur de OpenShift Container Platform.

ii. Dans le menu latéral, sélectionnez **Operators > OperatorHub**.

iii. Recherchez et sélectionnez l'opérateur NetApp Astra Control Center.

◦ À partir du catalogue de l'écosystème Red Hat :

i. Sélectionnez le centre de contrôle NetApp Astra "opérateur".

ii. Sélectionnez **déployer et utiliser**.

Overview

Poser l'opérateur

1. Complétez la page **Install Operator** et installez l'opérateur :



L'opérateur sera disponible dans tous les namespaces du cluster.

a. Sélectionnez l'espace de noms de l'opérateur ou `netapp-acc-operator` l'espace de noms sera créé automatiquement dans le cadre de l'installation de l'opérateur.

b. Sélectionnez une stratégie d'approbation manuelle ou automatique.



L'approbation manuelle est recommandée. Une seule instance d'opérateur doit s'exécuter par cluster.

c. Sélectionnez **installer**.

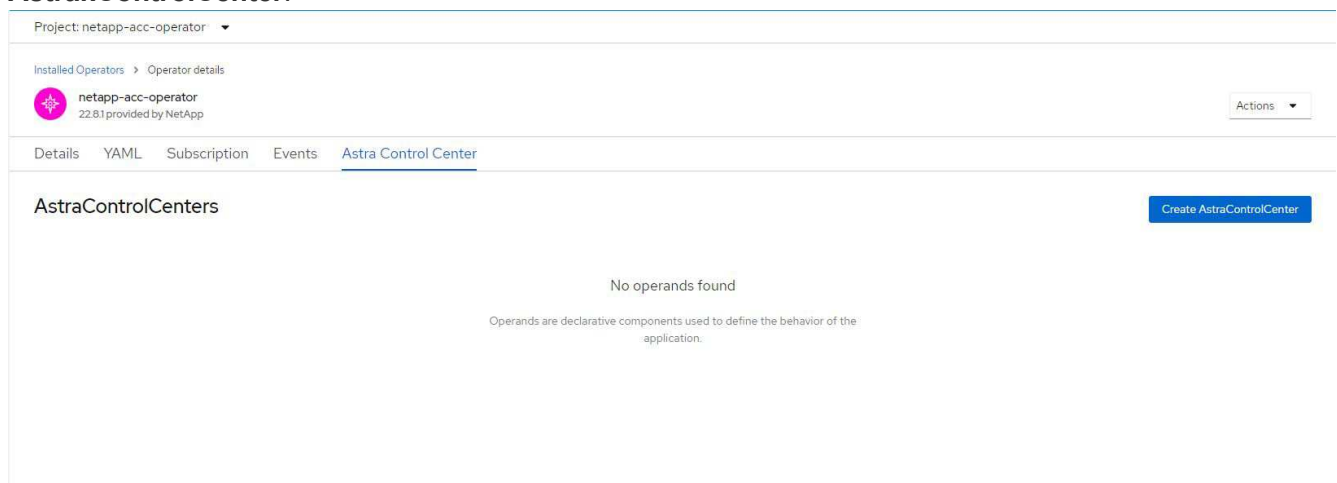


Si vous avez sélectionné une stratégie d'approbation manuelle, vous serez invité à approuver le plan d'installation manuelle pour cet opérateur.

2. Depuis la console, accéder au menu OperatorHub et vérifier que l'opérateur a bien installé.

Poser le centre de contrôle Astra

1. Dans la console de l'onglet **Astra Control Center** de l'opérateur Astra Control Center, sélectionnez **Create AstrakControlCenter**.



2. Complétez le `Create AstraControlCenter` champ de formulaire :

- Conservez ou ajustez le nom du centre de contrôle Astra.
- Ajouter des étiquettes pour le centre de contrôle Astra.
- Activez ou désactivez Auto support. Il est recommandé de conserver la fonctionnalité Auto support.
- Saisissez le nom de domaine complet ou l'adresse IP d'Astra Control Center. N'entrez pas `http://` ou `https://` dans le champ d'adresse.
- Entrez la version Astra Control Center, par exemple 22.04.1.
- Entrez un nom de compte, une adresse e-mail et un nom d'administrateur.
- Choisir une règle de récupération de volume de `Retain`, `Recycle`, ou `Delete`. La valeur par défaut est `Retain`.
- Sélectionnez le type d'entrée :

▪ **Generic** (`ingressType: "Generic"`) (Par défaut)

Utilisez cette option si vous avez un autre contrôleur d'entrée en service ou si vous préférez utiliser votre propre contrôleur d'entrée. Après le déploiement du centre de contrôle Astra, vous devez configurer le "contrôleur d'entrée" Pour exposer Astra Control Center avec une URL.

- **AccTraefik** (ingressType: "AccTraefik")

Utilisez cette option lorsque vous préférez ne pas configurer de contrôleur d'entrée. Ceci déploie le centre de contrôle Astra traefik Passerelle en tant que service de type Kubernetes « LoadBalancer ».

Le centre de contrôle Astra utilise un service de type « équilibreur de charge » (svc/traefik Dans l'espace de noms du centre de contrôle Astra), et exige qu'il se voit attribuer une adresse IP externe accessible. Si des équilibreurs de charge sont autorisés dans votre environnement et que vous n'en avez pas encore configuré, vous pouvez utiliser MetalLB ou un autre équilibreur de charge de service externe pour attribuer 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.



Pour plus de détails sur le type de service « LoadBalancer » et l'entrée, voir ["De formation"](#).

- a. Dans **image Registry**, entrez le chemin d'accès au registre d'images du conteneur local. N'entrez pas `http://` ou `https://` dans le champ d'adresse.
- b. Si vous utilisez un registre d'images qui nécessite une authentification, saisissez le secret d'image.



Si vous utilisez un registre qui nécessite une authentification, [créez un secret sur le cluster](#).

- c. Entrez le prénom de l'administrateur.
- d. Configurer l'évolutivité des ressources.
- e. Indiquez la classe de stockage par défaut.



Si une classe de stockage par défaut est configurée, assurez-vous qu'elle est la seule classe de stockage qui possède l'annotation par défaut.

- f. Définissez les préférences de gestion de CRD.

3. Sélectionnez la vue YAML pour vérifier les paramètres sélectionnés.
4. Sélectionnez `Create`.

Créer un secret de registre

Si vous utilisez un registre qui nécessite une authentification, créez un secret sur le cluster OpenShift et entrez le nom secret dans le `Create AstraControlCenter` champ de formulaire.

1. Créez un espace de noms pour l'opérateur du centre de contrôle Astra :

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. Créez un secret dans ce namespace :

```
oc create secret docker-registry astra-registry-cred n [netapp-acc-operator or custom namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```



Astra Control prend uniquement en charge les secrets de registre Docker.

3. Renseignez les champs restants dans [Le champ de formulaire Create AstrakControlCenter](#).

Et la suite

Complétez le "[les étapes restantes](#)" Pour vérifier que le centre de contrôle Astra est correctement installé, configurez un contrôleur d'entrée (en option) et connectez-vous à l'interface utilisateur. De plus, vous devez effectuer cette opération "[tâches de configuration](#)" une fois l'installation terminée.

Installer le centre de contrôle Astra avec un système de stockage back-end Cloud Volumes ONTAP

Avec Astra Control Center, vous pouvez gérer les applications dans un environnement de cloud hybride avec des clusters Kubernetes et des instances Cloud Volumes ONTAP autogérés. Vous pouvez déployer Astra Control Center dans vos clusters Kubernetes sur site ou dans l'un des clusters Kubernetes autogéré dans l'environnement cloud.

Dans l'un de ces déploiements, vous pouvez effectuer des opérations de gestion des données d'application en utilisant Cloud Volumes ONTAP comme système back-end. Vous pouvez également configurer un compartiment S3 en tant que cible de sauvegarde.

Pour installer Astra Control Center dans Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure avec un système back-end de stockage Cloud Volumes ONTAP, effectuez les opérations suivantes en fonction de votre environnement cloud.

- [Déploiement d'Astra Control Center dans Amazon Web Services](#)
- [Déployez Astra Control Center dans Google Cloud Platform](#)
- [Déploiement d'Astra Control Center dans Microsoft Azure](#)

Vous pouvez gérer vos applications dans des distributions avec des clusters Kubernetes autogérés, tels qu'OpenShift Container Platform (OCP). Seuls les clusters OCP autogérés sont validés pour le déploiement d'Astra Control Center.

Déploiement d'Astra Control Center dans Amazon Web Services

Vous pouvez déployer Astra Control Center sur un cluster Kubernetes autogéré, hébergé dans un cloud public Amazon Web Services (AWS).

Ce dont vous avez besoin pour AWS

Avant de déployer Astra Control Center dans AWS, vous aurez besoin des éléments suivants :

- Licence Astra Control Center. Voir "[Exigences de licence d'Astra Control Center](#)".
- "[Découvrez les exigences d'Astra Control Center](#)".

- Compte NetApp Cloud Central
- En cas d'utilisation des autorisations OCP, Red Hat OpenShift Container Platform (OCP) (au niveau de l'espace de noms pour créer des pods)
- Les identifiants AWS, l'ID d'accès et la clé secrète avec des autorisations qui vous permettent de créer des compartiments et des connecteurs
- Accès et connexion au registre d'instance de conteneur souple (ECR) du compte AWS
- Zone hébergée sur AWS et entrée route 53 nécessaires pour accéder à l'interface utilisateur de contrôle Astra

Exigences de l'environnement opérationnel pour AWS

Astra Control Center requiert l'environnement opérationnel suivant pour AWS :

- Red Hat OpenShift Container Platform 4.8



Assurez-vous que l'environnement d'exploitation que vous choisissez d'héberger est conforme aux exigences de base en matière de ressources décrites dans la documentation officielle de l'environnement.

Outre les exigences de l'environnement en matière de ressources, Astra Control Center requiert les ressources suivantes :

Composant	Conditions requises
Backend la capacité de stockage Cloud Volumes ONTAP	300 Go au moins disponibles
Nœuds workers (exigence AWS EC2)	Au moins 3 nœuds workers au total, avec 4 cœurs de vCPU et 12 Go de RAM chacun
Équilibrage de la charge	Type de service « LoadBalancer » disponible pour que le trafic d'entrée soit envoyé aux services du cluster d'environnement opérationnel
FQDN	Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée
Astra Trident (installé dans le cadre de la découverte du cluster Kubernetes dans NetApp BlueXP, anciennement Cloud Manager)	Astra Trident 21.04 ou version ultérieure installé et configuré et NetApp ONTAP 9.5 ou version ultérieure en tant que système de stockage back-end
Registre d'images	<p>Vous devez disposer d'un registre privé existant, comme AWS Elastic Container Registry, auquel vous pouvez pousser les images de création Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p>Le cluster hébergé par Astra Control Center et le cluster géré doivent avoir accès au même registre d'images pour pouvoir sauvegarder et restaurer des applications à l'aide de l'image Restic.</p> </div>

Composant	Conditions requises
Configuration d'Astra Trident et ONTAP	<p>Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. L'Astra Control Center prend en charge les classes de stockage Kubernetes ONTAP suivantes qui sont créées lorsque vous importez votre cluster Kubernetes dans NetApp BlueXP (anciennement Cloud Manager). Découvrez Astra Trident :</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



De telles exigences supposent que Astra Control Center est la seule application qui s'exécute dans l'environnement opérationnel. Si l'environnement exécute des applications supplémentaires, ajustez ces exigences minimales en conséquence.



Le jeton de Registre AWS expire dans 12 heures. Après cela, vous devrez renouveler le code secret de Registre d'images Docker.

Présentation du déploiement pour AWS

Voici un aperçu du processus d'installation d'Astra Control Center pour AWS avec Cloud Volumes ONTAP en tant que système de stockage back-end.

Chacune de ces étapes est expliquée en détail ci-dessous.

1. [Assurez-vous que vous disposez de suffisamment d'autorisations IAM.](#)
2. [Installez un cluster Red Hat OpenShift sur AWS.](#)
3. [Configurez AWS.](#)
4. [Configuration de NetApp BlueXP pour AWS.](#)
5. [Installer Astra Control Center pour AWS.](#)

Assurez-vous que vous disposez de suffisamment d'autorisations IAM

Assurez-vous de disposer de suffisamment de rôles et d'autorisations IAM pour installer un cluster RedHat OpenShift et un connecteur NetApp BlueXP (anciennement Cloud Manager).

Voir "[Identifiants AWS initiaux](#)".

Installez un cluster Red Hat OpenShift sur AWS

Installez un cluster Red Hat OpenShift Container Platform sur AWS.

Pour obtenir des instructions d'installation, reportez-vous à la section "[Installation d'un cluster sur AWS dans OpenShift Container Platform](#)".

Configurez AWS

Configurez ensuite AWS pour créer un réseau virtuel, configurez les instances de calcul EC2, créez un compartiment AWS S3, créez un registre d'objets élastiques (ECR) pour héberger les images d'Astra Control Center et envoyez les images dans ce registre.

Suivez la documentation AWS pour suivre la procédure ci-dessous. Voir "[Documentation d'installation d'AWS](#)".

1. Créez un réseau virtuel AWS.
2. Vérifiez les instances de calcul EC2. Il peut s'agir d'un serveur bare Metal ou de machines virtuelles dans AWS.
3. Si le type d'instance ne correspond pas déjà aux exigences de ressources minimales Astra pour les nœuds maîtres et workers, modifiez le type d'instance dans AWS afin qu'il réponde aux exigences de l'Astra. Voir "[Exigences du centre de contrôle Astra](#)".
4. Créez au moins un compartiment AWS S3 pour stocker vos sauvegardes.
5. Créez un registre AWS Elastic Container (ECR) pour héberger toutes les images ACC.



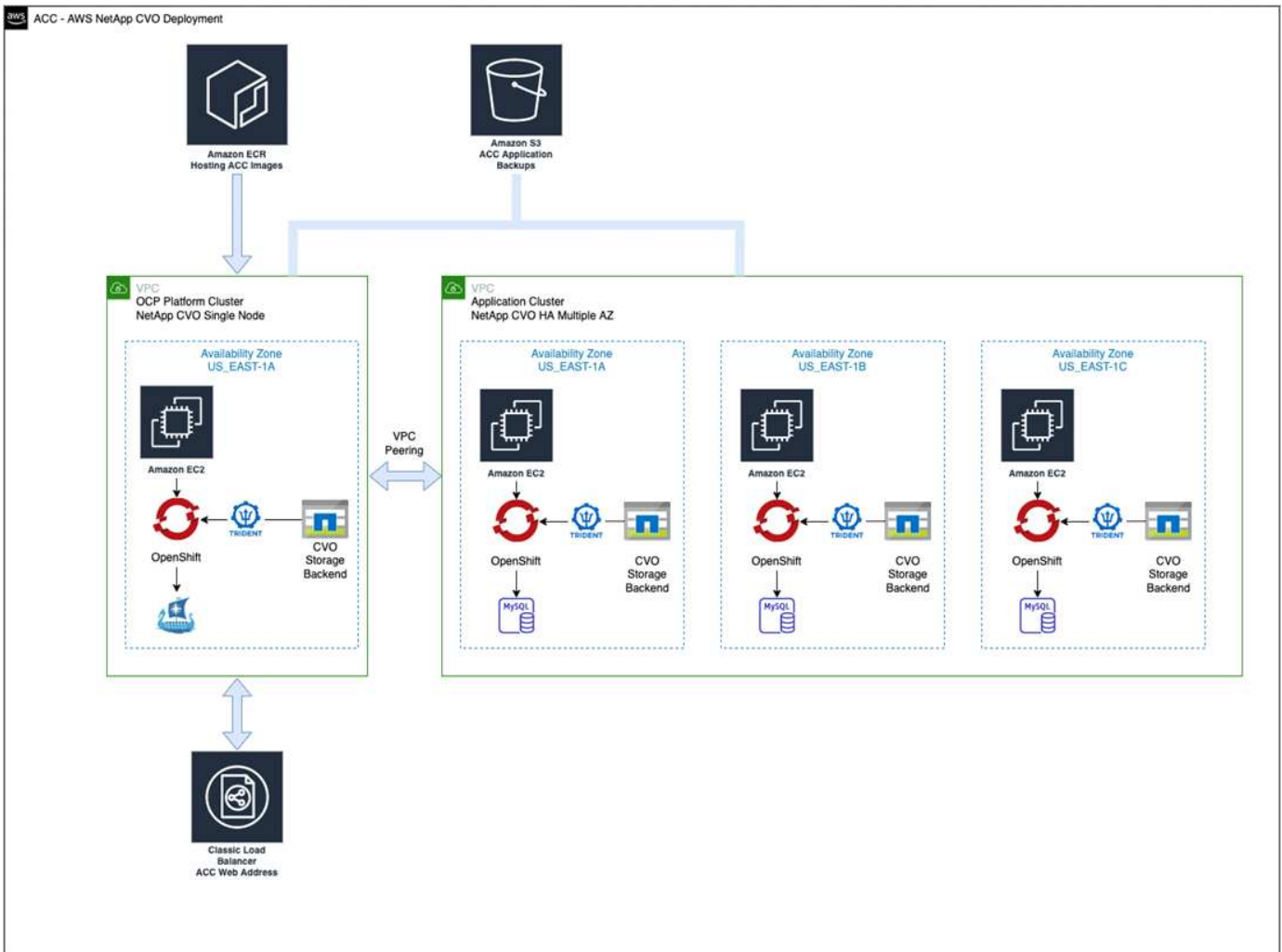
Si vous ne créez pas d'ECR, le centre de contrôle Astra ne peut pas accéder aux données de surveillance à partir d'un cluster contenant Cloud Volumes ONTAP avec un back-end AWS. Le problème survient lorsque le cluster que vous essayez de découvrir et de gérer à l'aide d'Astra Control Center n'a pas accès à AWS ECR.

6. Poussez les images ACC dans le registre défini.



Le token AWS Elastic Container Registry (ECR) expire au bout de 12 heures et provoque l'échec des opérations de clonage inter-cluster. Ce problème survient lors de la gestion d'un système back-end à partir d'Cloud Volumes ONTAP configuré pour AWS. Pour corriger ce problème, authentifiez-vous à nouveau avec l'ECR et générez un nouveau secret pour que les opérations de clonage puissent reprendre avec succès.

Voici un exemple de déploiement AWS :



Configuration de NetApp BlueXP pour AWS

Avec NetApp BlueXP (anciennement Cloud Manager), créez un espace de travail, ajoutez un connecteur à AWS, créez un environnement de travail et importez le cluster.

Suivez la documentation BlueXP pour effectuer les étapes suivantes. Voir les éléments suivants :

- ["Mise en route de Cloud Volumes ONTAP dans AWS"](#).
- ["Créez un connecteur dans AWS à l'aide de BlueXP"](#)

Étapes

1. Ajoutez vos informations d'identification à BlueXP.
2. Créez un espace de travail.
3. Ajoutez un connecteur pour AWS. Choisissez AWS en tant que fournisseur.
4. Créez un environnement de travail pour votre environnement cloud.
 - a. Emplacement : « Amazon Web Services (AWS) »
 - b. Type : « Cloud Volumes ONTAP HA »
5. Importer le cluster OpenShift Le cluster se connecte à l'environnement de travail que vous venez de créer.
 - a. Pour en savoir plus sur le cluster NetApp, sélectionnez **K8s > liste des clusters > Détails du cluster**.

- b. Notez la version Trident dans le coin supérieur droit.
- c. Notez les classes de stockage du cluster Cloud Volumes ONTAP indiquant NetApp comme provisionneur.

Cela importe votre cluster Red Hat OpenShift et lui attribue une classe de stockage par défaut. Vous sélectionnez la classe de stockage. Trident est automatiquement installé dans le cadre du processus d'importation et de détection.

6. Noter tous les volumes et volumes persistants sur ce déploiement Cloud Volumes ONTAP



Cloud Volumes ONTAP peut fonctionner comme un seul nœud ou en mode haute disponibilité. Si la HA est activée, noter l'état de la HA et l'état du déploiement du nœud en cours dans AWS.

Installer Astra Control Center pour AWS

Respectez la norme "[Instructions d'installation du centre de contrôle Astra](#)".



AWS utilise le type de compartiment S3 générique.

Déployez Astra Control Center dans Google Cloud Platform

Vous pouvez déployer Astra Control Center sur un cluster Kubernetes autogéré, hébergé dans un cloud public Google Cloud Platform (GCP).

Éléments requis pour GCP

Avant de déployer Astra Control Center dans GCP, vous aurez besoin des éléments suivants :

- Licence Astra Control Center. Voir "[Exigences de licence d'Astra Control Center](#)".
- "[Découvrez les exigences d'Astra Control Center](#)".
- Compte NetApp Cloud Central
- Si vous utilisez OCP, Red Hat OpenShift Container Platform (OCP) 4.10
- En cas d'utilisation des autorisations OCP, Red Hat OpenShift Container Platform (OCP) (au niveau de l'espace de noms pour créer des pods)
- Compte de service GCP avec les autorisations qui vous permettent de créer des compartiments et des connecteurs


Exigences de l'environnement opérationnel pour GCP



Assurez-vous que l'environnement d'exploitation que vous choisissez d'héberger est conforme aux exigences de base en matière de ressources décrites dans la documentation officielle de l'environnement.

Outre les exigences de l'environnement en matière de ressources, Astra Control Center requiert les ressources suivantes :

Composant	Conditions requises
Backend la capacité de stockage Cloud Volumes ONTAP	300 Go au moins disponibles

Composant	Conditions requises
Nœuds workers (exigences de calcul GCP)	Au moins 3 nœuds workers au total, avec 4 cœurs de vCPU et 12 Go de RAM chacun
Équilibrage de la charge	Type de service « LoadBalancer » disponible pour que le trafic d'entrée soit envoyé aux services du cluster d'environnement opérationnel
FQDN (ZONE DNS GCP)	Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée
Astra Trident (installé dans le cadre de la découverte du cluster Kubernetes dans NetApp BlueXP, anciennement Cloud Manager)	Astra Trident 21.04 ou version ultérieure installé et configuré et NetApp ONTAP 9.5 ou version ultérieure en tant que système de stockage backend
Registre d'images	<p>Vous devez disposer d'un registre privé existant, tel que le registre de conteneurs Google, auquel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Vous devez activer l'accès anonyme pour extraire les images Restic pour les sauvegardes.</p> </div>
Configuration d'Astra Trident et ONTAP	<p>Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Astra Control Center prend en charge les classes de stockage Kubernetes ONTAP suivantes qui sont créées lorsque vous importez votre cluster Kubernetes dans NetApp BlueXP. Découvrez Astra Trident :</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



De telles exigences supposent que Astra Control Center est la seule application qui s'exécute dans l'environnement opérationnel. Si l'environnement exécute des applications supplémentaires, ajustez ces exigences minimales en conséquence.

Présentation du déploiement pour GCP

Voici un aperçu du processus d'installation d'Astra Control Center sur un cluster OCP autogéré dans GCP avec Cloud Volumes ONTAP comme système de stockage principal.

Chacune de ces étapes est expliquée en détail ci-dessous.

1. [Installez un cluster Red Hat OpenShift sur GCP.](#)
2. [Création d'un projet GCP et d'un cloud privé virtuel.](#)
3. [Assurez-vous que vous disposez de suffisamment d'autorisations IAM.](#)
4. [Configurez GCP.](#)
5. [Configuration de NetApp BlueXP pour GCP.](#)
6. [Installer Astra Control Center pour GCP.](#)

Installez un cluster Red Hat OpenShift sur GCP

La première étape consiste à installer un cluster Red Hat OpenShift sur GCP.

Pour les instructions d'installation, reportez-vous aux sections suivantes :

- ["Installation d'un cluster OpenShift dans GCP"](#)
- ["Création d'un compte de service GCP"](#)

Création d'un projet GCP et d'un cloud privé virtuel

Créez au moins un projet GCP et un cloud privé virtuel (VPC).



OpenShift peut créer ses propres groupes de ressources. En plus de ces VPC, vous devez également définir un VPC GCP. Voir la documentation OpenShift.

Vous pouvez créer un groupe de ressources de cluster de plate-forme et un groupe de ressources de cluster OpenShift d'application cible.

Assurez-vous que vous disposez de suffisamment d'autorisations IAM

Assurez-vous de disposer de suffisamment de rôles et d'autorisations IAM pour installer un cluster RedHat OpenShift et un connecteur NetApp BlueXP (anciennement Cloud Manager).

Voir ["Identifiants et autorisations GCP initiaux"](#).

Configurez GCP

Configurez ensuite GCP pour créer un VPC, configurez des instances de calcul, créez un stockage objet Google Cloud, créez un registre de conteneurs Google pour héberger les images d'Astra Control Center et envoyez les images vers ce registre.

Suivez la documentation GCP pour effectuer les étapes suivantes. Voir installation du cluster OpenShift dans GCP.

1. Créez un projet GCP et un VPC dans le GCP que vous prévoyez d'utiliser pour le cluster OCP avec le backend CVO.
2. Vérifiez les instances de calcul. Il peut s'agir d'un serveur bare Metal ou de machines virtuelles dans GCP.
3. Si le type d'instance ne correspond pas déjà aux exigences de ressources minimales Astra pour les nœuds maîtres et workers, modifiez le type d'instance dans GCP afin qu'il réponde aux exigences de l'Astra. Voir ["Exigences du centre de contrôle Astra"](#).
4. Créez au moins un compartiment de stockage cloud GCP pour stocker vos sauvegardes.
5. Créez un secret, requis pour l'accès au compartiment.

6. Créez un registre de conteneurs Google pour héberger toutes les images du centre de contrôle Astra.
7. Configurez l'accès du registre de conteneurs Google pour le transfert/transfert de Docker pour toutes les images du centre de contrôle Astra.

Exemple : les images ACC peuvent être transmises à ce registre en entrant le script suivant :

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

Ce script nécessite un fichier manifeste Astra Control Center et votre emplacement dans le registre d'images Google.

Exemple :

```
manifestfile=astra-control-center-<version>.manifest
GCP_CR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

8. Configurer les zones DNS.

Configuration de NetApp BlueXP pour GCP

À l'aide de NetApp BlueXP (anciennement Cloud Manager), créez un espace de travail, ajoutez un connecteur à GCP, créez un environnement de travail et importez le cluster.

Suivez la documentation BlueXP pour effectuer les étapes suivantes. Voir "[Mise en route de Cloud Volumes ONTAP dans GCP](#)".

Ce dont vous avez besoin

- Accès au compte de services GCP avec les autorisations IAM et les rôles requis

Étapes

1. Ajoutez vos informations d'identification à BlueXP. Voir "[Ajout de comptes GCP](#)".
2. Ajoutez un connecteur pour GCP.
 - a. Choisissez GCP comme fournisseur.
 - b. Entrez les identifiants GCP. Voir "[Création d'un connecteur dans GCP à partir de BlueXP](#)".
 - c. S'assurer que le connecteur est en marche et basculer vers ce connecteur.

3. Créez un environnement de travail pour votre environnement cloud.
 - a. Emplacement : « GCP »
 - b. Type : « Cloud Volumes ONTAP HA »
4. Importer le cluster OpenShift Le cluster se connecte à l'environnement de travail que vous venez de créer.
 - a. Pour en savoir plus sur le cluster NetApp, sélectionnez **K8s > liste des clusters > Détails du cluster**.
 - b. Notez la version Trident dans le coin supérieur droit.
 - c. Notez les classes de stockage du cluster Cloud Volumes ONTAP indiquant « NetApp » comme provisionneur.

Cela importe votre cluster Red Hat OpenShift et lui attribue une classe de stockage par défaut. Vous sélectionnez la classe de stockage. Trident est automatiquement installé dans le cadre du processus d'importation et de détection.

5. Noter tous les volumes et volumes persistants sur ce déploiement Cloud Volumes ONTAP



Cloud Volumes ONTAP peut fonctionner comme un seul nœud ou en haute disponibilité. Si la haute disponibilité est activée, notez l'état de la haute disponibilité et l'état du déploiement des nœuds exécutés dans GCP.

Installer Astra Control Center pour GCP

Respectez la norme "[Instructions d'installation du centre de contrôle Astra](#)".



GCP utilise le type de compartiment S3 générique.

1. Générez le secret Docker pour extraire des images pour l'installation du centre de contrôle Astra :

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

Déploiement d'Astra Control Center dans Microsoft Azure

Vous pouvez déployer Astra Control Center sur un cluster Kubernetes autogéré, hébergé dans un cloud public Microsoft Azure.

Ce dont vous avez besoin pour Azure

Avant de déployer Astra Control Center dans Azure, vous aurez besoin des éléments suivants :

- Licence Astra Control Center. Voir "[Exigences de licence d'Astra Control Center](#)".
- "[Découvrez les exigences d'Astra Control Center](#)".
- Compte NetApp Cloud Central
- Si vous utilisez OCP, Red Hat OpenShift Container Platform (OCP) 4.8
- En cas d'utilisation des autorisations OCP, Red Hat OpenShift Container Platform (OCP) (au niveau de l'espace de noms pour créer des pods)


- Les identifiants Azure avec autorisations qui vous permettent de créer des compartiments et des connecteurs

Exigences de l'environnement opérationnel pour Azure

Assurez-vous que l'environnement d'exploitation que vous choisissez d'héberger est conforme aux exigences de base en matière de ressources décrites dans la documentation officielle de l'environnement.

Outre les exigences de l'environnement en matière de ressources, Astra Control Center requiert les ressources suivantes :

Voir "[Exigences relatives à l'environnement opérationnel d'Astra Control Center](#)".

Composant	Conditions requises
Backend la capacité de stockage Cloud Volumes ONTAP	300 Go au moins disponibles
Nœuds worker (exigences de calcul Azure)	Au moins 3 nœuds workers au total, avec 4 cœurs de vCPU et 12 Go de RAM chacun
Équilibrage de la charge	Type de service « LoadBalancer » disponible pour que le trafic d'entrée soit envoyé aux services du cluster d'environnement opérationnel
FQDN (zone Azure DNS)	Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée
Astra Trident (installé dans le cadre de la découverte du cluster Kubernetes dans NetApp BlueXP)	Astra Trident 21.04 ou version ultérieure installé et configuré et NetApp ONTAP version 9.5 ou ultérieure sera utilisé comme système de stockage back-end
Registre d'images	<p>Vous devez disposer d'un registre privé existant, tel que le registre de conteneur Azure (ACR), auquel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images.</p> <div style="display: flex; align-items: center;">  <p>Vous devez activer l'accès anonyme pour extraire les images Restic pour les sauvegardes.</p> </div>

Composant	Conditions requises
Configuration d'Astra Trident et ONTAP	<p>Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Astra Control Center prend en charge les classes de stockage Kubernetes ONTAP suivantes qui sont créées lorsque vous importez votre cluster Kubernetes dans NetApp BlueXP. Découvrez Astra Trident :</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



De telles exigences supposent que Astra Control Center est la seule application qui s'exécute dans l'environnement opérationnel. Si l'environnement exécute des applications supplémentaires, ajustez ces exigences minimales en conséquence.

Présentation du déploiement pour Azure

Voici un aperçu du processus d'installation d'Astra Control Center pour Azure.

Chacune de ces étapes est expliquée en détail ci-dessous.

1. [Installez un cluster Red Hat OpenShift sur Azure.](#)
2. [Créez des groupes de ressources Azure.](#)
3. [Assurez-vous que vous disposez de suffisamment d'autorisations IAM.](#)
4. [Configurez Azure.](#)
5. [Configuration de NetApp BlueXP \(anciennement Cloud Manager\) pour Azure.](#)
6. [Installer et configurer Astra Control Center pour Azure.](#)

Installez un cluster Red Hat OpenShift sur Azure

La première étape consiste à installer un cluster Red Hat OpenShift sur Azure.

Pour les instructions d'installation, reportez-vous aux sections suivantes :

- ["Installation du cluster OpenShift sur Azure"](#).
- ["Installation d'un compte Azure"](#).

Créez des groupes de ressources Azure

Créez au moins un groupe de ressources Azure.



OpenShift peut créer ses propres groupes de ressources. En plus de ces groupes, vous devez également définir des groupes de ressources Azure. Voir la documentation OpenShift.

Vous pouvez créer un groupe de ressources de cluster de plate-forme et un groupe de ressources de cluster OpenShift d'application cible.

Assurez-vous que vous disposez de suffisamment d'autorisations IAM

Assurez-vous de disposer de suffisamment de rôles et d'autorisations IAM pour installer un cluster RedHat OpenShift et un connecteur NetApp BlueXP.

Voir "[Identifiants et autorisations Azure](#)".

Configurez Azure

Configurez ensuite Azure pour créer un réseau virtuel, configurez des instances de calcul, créez un conteneur Azure Blob Container Register, créez un ACR (Azure Container Register) pour héberger les images d'Astra Control Center et envoyez les images dans ce registre.

Suivez la documentation Azure pour suivre les étapes ci-dessous. Voir "[Installation du cluster OpenShift sur Azure](#)".

1. Créez un réseau virtuel Azure.
2. Vérifiez les instances de calcul. Il peut s'agir d'un serveur bare Metal ou de machines virtuelles dans Azure.
3. Si le type d'instance ne correspond pas déjà aux exigences de ressources minimales Astra pour les nœuds maîtres et workers, modifiez le type d'instance dans Azure afin qu'il réponde aux exigences de l'Astra. Voir "[Exigences du centre de contrôle Astra](#)".
4. Créez au moins un conteneur Azure Blob pour stocker vos sauvegardes.
5. Créez un compte de stockage. Vous aurez besoin d'un compte de stockage pour créer un conteneur à utiliser comme compartiment dans Astra Control Center.
6. Créez un secret, requis pour l'accès au compartiment.
7. Créez un registre de conteneurs Azure (ACR) pour héberger toutes les images du centre de contrôle Astra.
8. Configurez l'accès ACR pour Docker pousser/extraire toutes les images du centre de contrôle Astra.
9. Envoyez les images ACC dans ce registre en entrant le script suivant :

```
az acr login -n <AZ ACR URL/Location>  
This script requires ACC manifest file and your Azure ACR location.
```

Exemple :


```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Configurer les zones DNS.

Configuration de NetApp BlueXP (anciennement Cloud Manager) pour Azure

À l'aide de BlueXP (anciennement Cloud Manager), créez un espace de travail, ajoutez un connecteur à Azure, créez un environnement de travail et importez le cluster.

Suivez la documentation BlueXP pour effectuer les étapes suivantes. Voir "[Mise en route de BlueXP dans Azure](#)".

Ce dont vous avez besoin

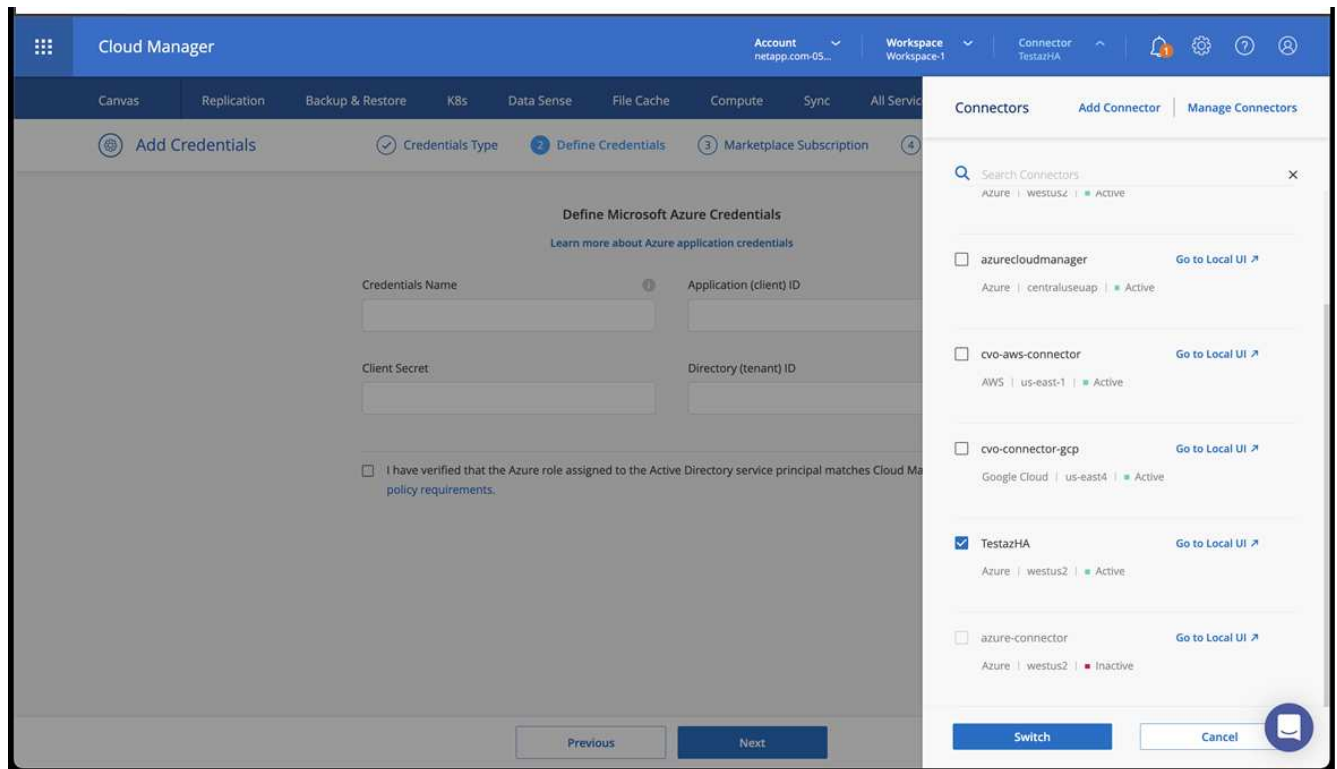
Accès au compte Azure avec les autorisations IAM et les rôles requis

Étapes

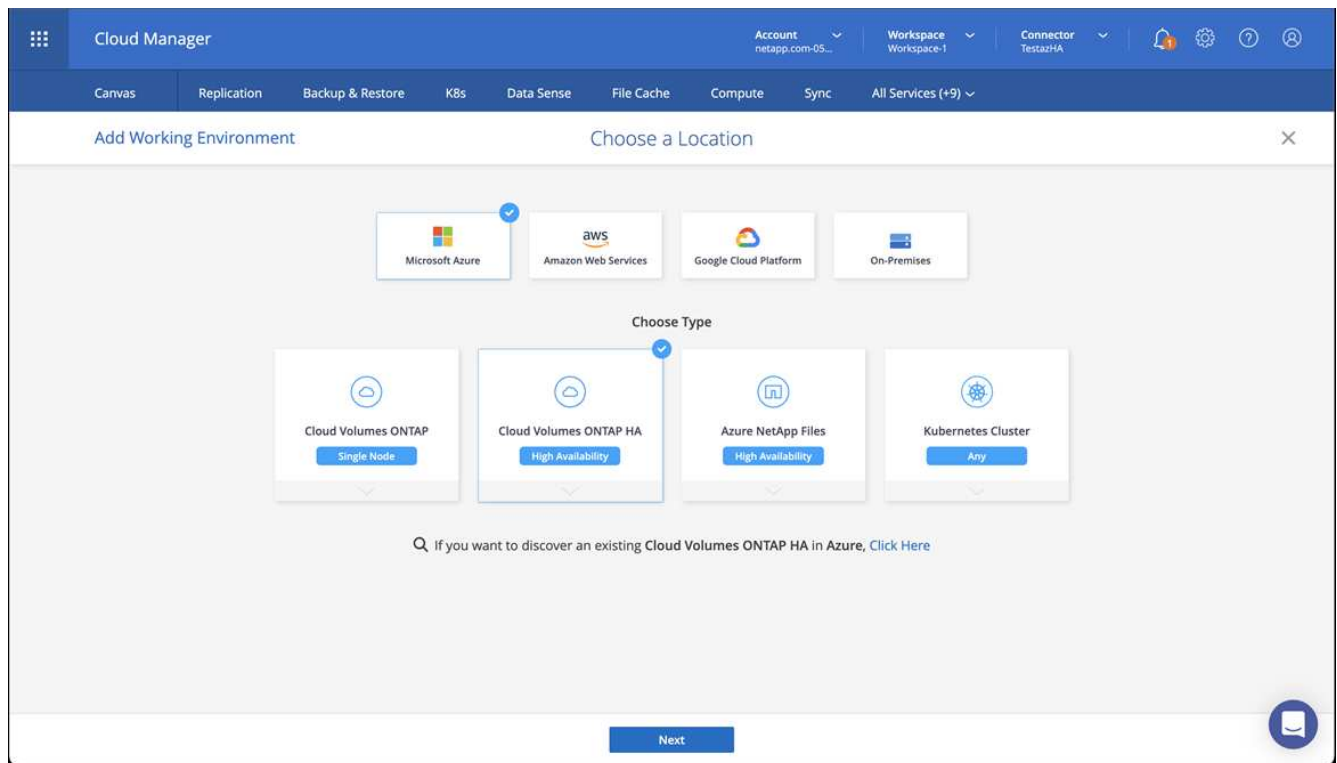
1. Ajoutez vos informations d'identification à BlueXP.
2. Ajoutez un connecteur pour Azure. Voir "[Politiques BlueXP](#)".
 - a. Choisissez **Azure** comme fournisseur.
 - b. Vous pouvez entrer les identifiants Azure, notamment l'ID de l'application, le secret client et l'ID du répertoire (locataire).

Voir "[Création d'un connecteur dans Azure à partir de BlueXP](#)".

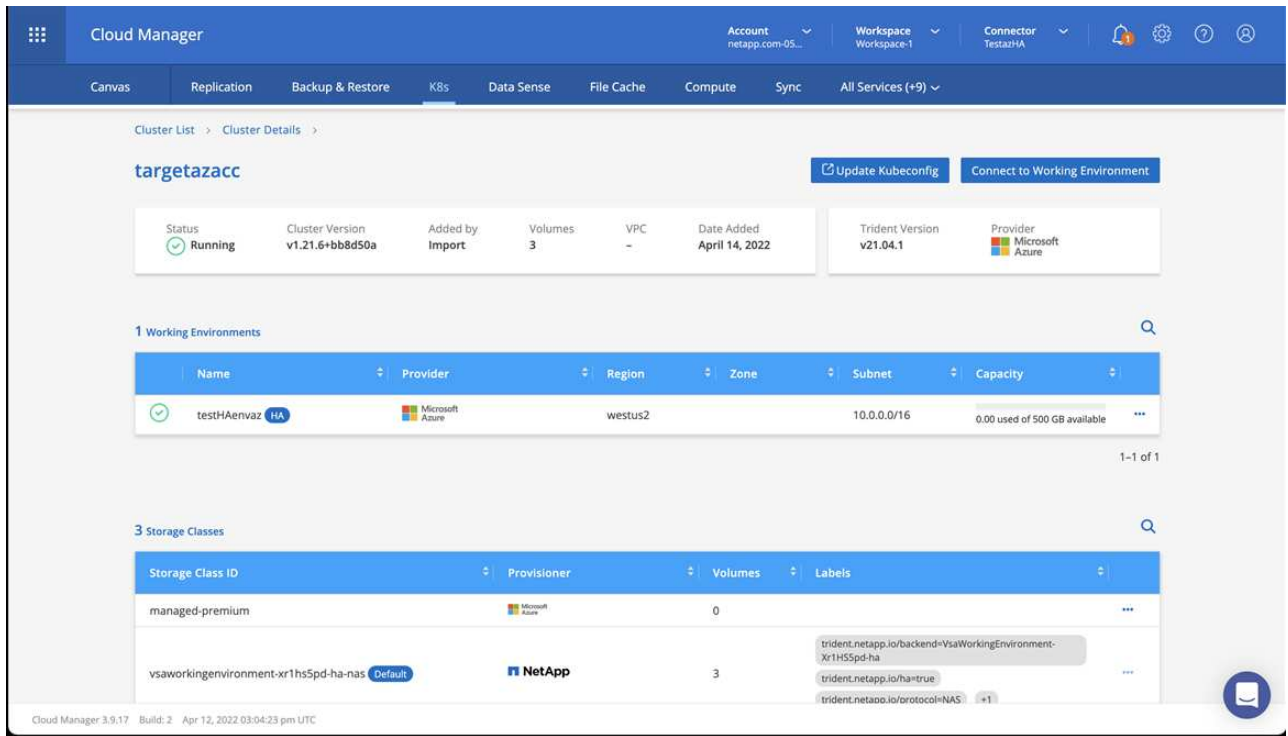
3. S'assurer que le connecteur est en marche et basculer vers ce connecteur.



4. Créez un environnement de travail pour votre environnement cloud.
 - a. Emplacement : « Microsoft Azure ».
 - b. Type : « Cloud Volumes ONTAP HA ».



5. Importer le cluster OpenShift Le cluster se connecte à l'environnement de travail que vous venez de créer.
 - a. Pour en savoir plus sur le cluster NetApp, sélectionnez **K8s > liste des clusters > Détails du cluster**.



- b. Notez la version Trident dans le coin supérieur droit.
- c. Notez les classes de stockage du cluster Cloud Volumes ONTAP indiquant NetApp comme provisionneur.

Cela importe votre cluster Red Hat OpenShift et attribue une classe de stockage par défaut. Vous sélectionnez la classe de stockage. Trident est automatiquement installé dans le cadre du processus d'importation et de détection.

6. Noter tous les volumes et volumes persistants sur ce déploiement Cloud Volumes ONTAP
7. Cloud Volumes ONTAP peut fonctionner comme un seul nœud ou en mode haute disponibilité. Si la HA est activée, noter l'état de la HA et l'état du déploiement du nœud en cours d'exécution dans Azure.

Installer et configurer Astra Control Center pour Azure

Installer le centre de contrôle Astra de série "[instructions d'installation](#)".

Avec Astra Control Center, ajoutez un compartiment Azure. Voir "[Configurer le centre de contrôle Astra et ajouter des seaux](#)".

=

:allow-uri-read:

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](#)

- [Préparez votre environnement à la gestion des clusters avec Astra Control](#)
- [Ajouter un cluster](#)
- [Ajout d'un système back-end](#)
- [Ajouter un godet](#)

Ajoutez une licence pour Astra Control Center

Vous pouvez ajouter une nouvelle licence à l'aide de l'interface utilisateur Astra Control ou ["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.

Les licences Astra Control Center mesurent les ressources CPU avec des unités de processeur Kubernetes et représentent les ressources de processeur attribuées aux nœuds de travail de tous les clusters Kubernetes gérés. Les licences dépendent de l'utilisation des processeurs virtuels. Pour plus d'informations sur le calcul des licences, reportez-vous à la section ["Licences"](#).



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.



Pour mettre à jour une évaluation existante ou une licence complète, reportez-vous à la section ["Mettre à jour une licence existante"](#).

Ce dont vous avez besoin

- Accès à une instance Astra Control Center récemment installée.
- Autorisations de rôle d'administrateur.
- A ["Fichier de licence NetApp"](#) (NLF).

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 et que vous n'envoyez pas de données à AutoSupport, assurez-vous de stocker votre identifiant de compte pour éviter toute perte de données en cas de défaillance d'Astra Control Center.

Préparez votre environnement à la gestion des clusters avec Astra Control

Avant d'ajouter un cluster, assurez-vous que les conditions préalables suivantes sont remplies. Vous devez également effectuer des vérifications d'admissibilité pour vous assurer que votre cluster est prêt à être ajouté au Centre de contrôle Astra et créer des rôles pour la gestion du cluster.

Ce dont vous avez besoin

- Assurez-vous que les nœuds workers de votre cluster sont configurés avec les pilotes de stockage appropriés afin que les pods puissent interagir avec le système de stockage back-end.
- Votre environnement répond au "de l'environnement opérationnel" Pour Astra Trident et Astra Control Center.
- Une version d'Astra Trident "Pris en charge par Astra Control Center" est installé :



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

- **Système back-end de stockage Trident configuré** : au moins un système back-end de stockage Trident Astra doit être configuré "configuré" sur le cluster.
 - **Classes de stockage Trident configurées** : au moins une classe de stockage Astra Trident doit être "configuré" sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'elle est la seule classe de stockage qui possède l'annotation par défaut.
 - **Contrôleur de snapshot de volume Astra Trident et classe de snapshot de volume installés et configurés** : le contrôleur de snapshot de volume doit être "installé" Il est ainsi possible de créer des snapshots dans Astra Control. Au moins un Astra Trident `VolumeSnapshotClass` a été "configuration" par un administrateur.
- **Kubeconfig accessible**: Vous avez accès au "cluster kubeconfig" qui ne comprend qu'un seul élément de contexte.
 - **Informations d'identification ONTAP** : vous avez besoin d'informations d'identification ONTAP et d'un superutilisateur et d'un ID utilisateur définis sur le système ONTAP de sauvegarde pour sauvegarder et restaurer des applications avec le Centre de contrôle Astra.

Exécutez les commandes suivantes dans la ligne de commande ONTAP :

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

- **Rancher uniquement**: Lorsque vous gérez des clusters d'applications dans un environnement Rancher, modifiez le contexte par défaut du cluster d'applications dans le fichier kubeconfig fourni par Rancher pour utiliser un contexte de plan de contrôle au lieu du contexte du serveur d'API Rancher. La charge est réduite sur le serveur API Rancher et les performances sont améliorées.

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       22.10.0
```

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. Reportez-vous à la ["Documentation Trident"](#) pour obtenir des instructions.

2. Assurez-vous que les pods fonctionnent :

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

3. Déterminez 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 sc
```

Exemple de réponse :

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

Créez un nombre limité de rôles de cluster kubeconfig

Vous pouvez éventuellement créer un rôle d'administrateur limité pour Astra Control Center. Il ne s'agit pas d'une procédure requise pour la configuration du centre de contrôle Astra. Cette procédure permet de créer un kubeconfig distinct qui limite les autorisations de contrôle Astra sur les clusters qu'il gère.

Ce dont vous avez besoin

Assurez-vous que vous disposez des éléments suivants pour le cluster que vous souhaitez gérer avant d'effectuer la procédure suivante :

- kubectl v1.23 ou version ultérieure installée
- Accès kubectl au cluster que vous souhaitez ajouter et gérer avec Astra Control Center



Pour cette procédure, il n'est pas nécessaire d'avoir un accès kubectl au cluster qui exécute Astra Control Center.

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

Étapes

1. Créer un compte de service :

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

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

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

+

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

- a. Appliquer le compte de service :

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

2. Créez un rôle de cluster limité avec le minimum d'autorisations nécessaires à la gestion d'un cluster par Astra Control :

- a. Créer un `ClusterRole` fichier appelé `astra-admin-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>astra-admin-account.yaml</strong>
```

+

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

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
```



```
- '*'
resources:
- '*'
verbs:
- get
- list
- create
- patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
- ""
- apps
- autoscaling
- batch
- crd.projectcalico.org
- extensions
- networking.k8s.io
- policy
- rbac.authorization.k8s.io
- snapshot.storage.k8s.io
- trident.netapp.io
resources:
- configmaps
- cronjobs
- daemonsets
- deployments
- horizontalpodautoscalers
- ingresses
- jobs
- namespaces
- networkpolicies
- persistentvolumeclaims
- poddisruptionbudgets
- pods
- podtemplates
- podsecuritypolicies
- replicaset
- replicationcontrollers
- replicationcontrollers/scale
- rolebindings
- roles
- secrets
- serviceaccounts
- services
```

```

- statefulsets
- tridentmirrorrelationships
- tridentnapshotinfos
- volumesnapshots
- volumesnapshotcontents
verbs:
- delete

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

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagetags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use

```

a. Appliquer le rôle de cluster :

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

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

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

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: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

- a. Appliquer la liaison de rôle de cluster :

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

4. 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".

5. Générez le kubeconfig comme suit :

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

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

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
\
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
\
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp
```

```

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-
context ${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp

```

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

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

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

```
mv kubeconfig-sa 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](#).

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.

Ce dont vous avez besoin

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

Étapes

1. Naviguer à partir du menu Tableau de bord ou clusters :
 - Dans **Dashboard**, sélectionnez **Add** dans le volet clusters.
 - Dans la zone de navigation de gauche, sélectionnez **clusters**, puis **Ajouter un cluster** à partir de la page 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**.



Si vous créez la vôtre `kubeconfig` fichier, vous ne devez définir que **un** élément de contexte dans celui-ci. Reportez-vous à la section "[Documentation Kubernetes](#)" pour plus d'informations sur la création `kubeconfig` fichiers. Si vous avez créé un `kubeconfig` pour un rôle de cluster limité à l'aide de [le processus ci-dessus](#), assurez-vous de télécharger ou de coller ce `kubeconfig` dans cette étape.

3. Indiquez un nom d'identification. Par défaut, le nom des identifiants est automatiquement renseigné comme nom du cluster.
4. Sélectionnez **Suivant**.
5. Sélectionnez la classe de stockage par défaut à utiliser pour ce cluster Kubernetes et sélectionnez **Suivant**.



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

6. Passez en revue les informations, et si tout semble bien, sélectionnez **Ajouter**.

Résultat

Le cluster passe à l'état **découverte**, puis passe à **sain**. Vous gérez maintenant le cluster avec 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 ONTAP à Astra Control Center pour 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.

Étapes

1. Dans la zone de navigation gauche du tableau de bord, sélectionnez **Backends**.
2. Effectuez l'une des opérations suivantes :
 - **Nouveaux systèmes back-end** : sélectionnez **Ajouter** pour gérer un back-end existant, sélectionnez **ONTAP**, puis **Suivant**.
 - **Backends découverts** : dans le menu actions, sélectionnez **Manage** sur un back-end découvert à partir du cluster géré.
3. Saisissez l'adresse IP de gestion du cluster ONTAP et les identifiants d'administrateur. Les identifiants doivent être identifiants au niveau du cluster.



L'utilisateur dont vous saisissez ici les informations d'identification doit disposer du `ontapi` Méthode d'accès de connexion utilisateur activée dans ONTAP System Manager sur le cluster ONTAP. Si vous prévoyez d'utiliser la réplication SnapMirror, appliquez les identifiants de l'utilisateur au rôle « admin », qui dispose des méthodes d'accès `ontapi` et `http`, Sur les clusters ONTAP source et destination. Reportez-vous à la section "[Gérer les comptes utilisateur dans la documentation ONTAP](#)" pour en savoir plus.

4. Sélectionnez **Suivant**.
5. Confirmez les détails du back-end et sélectionnez **gérer**.

Résultat

Le back-end s'affiche dans le `Healthy` état dans la liste avec des informations récapitulatives.



Vous devrez peut-être actualiser la page pour que le back-end apparaisse.

Ajouter un godet

Vous pouvez ajouter un compartiment à l'aide de l'interface utilisateur Astra Control ou "API". 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.

Si vous clonez la configuration de vos applications et le stockage persistant vers le même cluster, il n'est pas nécessaire d'utiliser un compartiment dans Astra Control. La fonctionnalité de copie Snapshot des applications ne nécessite pas de compartiment.

Ce dont vous avez besoin

- Compartiment accessible depuis vos clusters gérés par Astra Control Center.
- Identifiants pour le compartiment.
- Un godet des types suivants :
 - NetApp ONTAP S3
 - NetApp StorageGRID S3
 - Microsoft Azure
 - S3 générique



Amazon Web Services (AWS) et Google Cloud Platform (GCP) utilisent le type de compartiment S3 générique.



Bien qu'Astra Control Center prenne en charge Amazon S3 en tant que fournisseur de compartiments 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.

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **godets**.
2. Sélectionnez **Ajouter**.
3. Sélectionner le type de godet.



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

4. Saisissez 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 plus tard lors de la création d'une sauvegarde. Ce nom apparaît également lors de la configuration de la règle de protection.

5. Entrez le nom ou l'adresse IP du terminal S3.
6. Sous **Sélectionner les informations d'identification**, choisissez l'onglet **Ajouter** ou **utiliser l'onglet existant**.
 - Si vous avez choisi **Ajouter**:
 - i. Saisissez un nom pour l'identifiant qui le distingue des autres identifiants dans Astra Control.
 - ii. Saisissez l'ID d'accès et la clé secrète en collant le contenu dans le presse-papiers.
 - Si vous avez choisi **utiliser existant**:
 - i. Sélectionnez les informations d'identification existantes à utiliser avec le compartiment.

7. Sélectionnez Add.



Lorsque vous ajoutez un godet, Astra Control marque un godet avec l'indicateur de compartiment par défaut. Le premier compartiment que vous créez devient le compartiment par défaut. Au fur et à mesure que vous ajoutez des compartiments, vous pourrez décider plus tard "[définir un autre compartiment par défaut](#)".

Et la suite ?

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

- "[Gérez les utilisateurs et les rôles locaux](#)"
- "[Commencez à gérer les applications](#)"
- "[Protégez vos applications](#)"
- "[Gérer les notifications](#)"
- "[Connectez-vous à Cloud Insights](#)"
- "[Ajouter un certificat TLS personnalisé](#)"
- "[Modifiez la classe de stockage par défaut](#)"

Trouvez plus d'informations

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

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` du fichier de ressource personnalisée `astra_control_Center.yaml` 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.yaml` CR.

Licences

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

1. Dans le menu de navigation de gauche, sélectionnez **compte > Licence**.
2. Sélectionnez **Ajouter licence**.
3. 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 `kubectl 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 est-il automatiquement désinstallé d'un cluster lorsque je le dégère ? lorsque vous dégèrez un cluster depuis Astra Control Center, Trident n'est pas automatiquement désinstallé du cluster. Pour désinstaller Trident, vous devez procéder comme ça "[Suivez ces étapes dans la documentation Trident](#)".

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 pods malsains affectent-ils la gestion des applications? si une application gérée possède des pods dans un état malsain, Astra Control ne peut pas créer de nouvelles sauvegardes et de nouveaux clones.

Les opérations de gestion des données

Mon application utilise plusieurs PVS. ASTRA Control prendra-t-il des snapshots et des sauvegardes de ces volumes persistants ?

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.

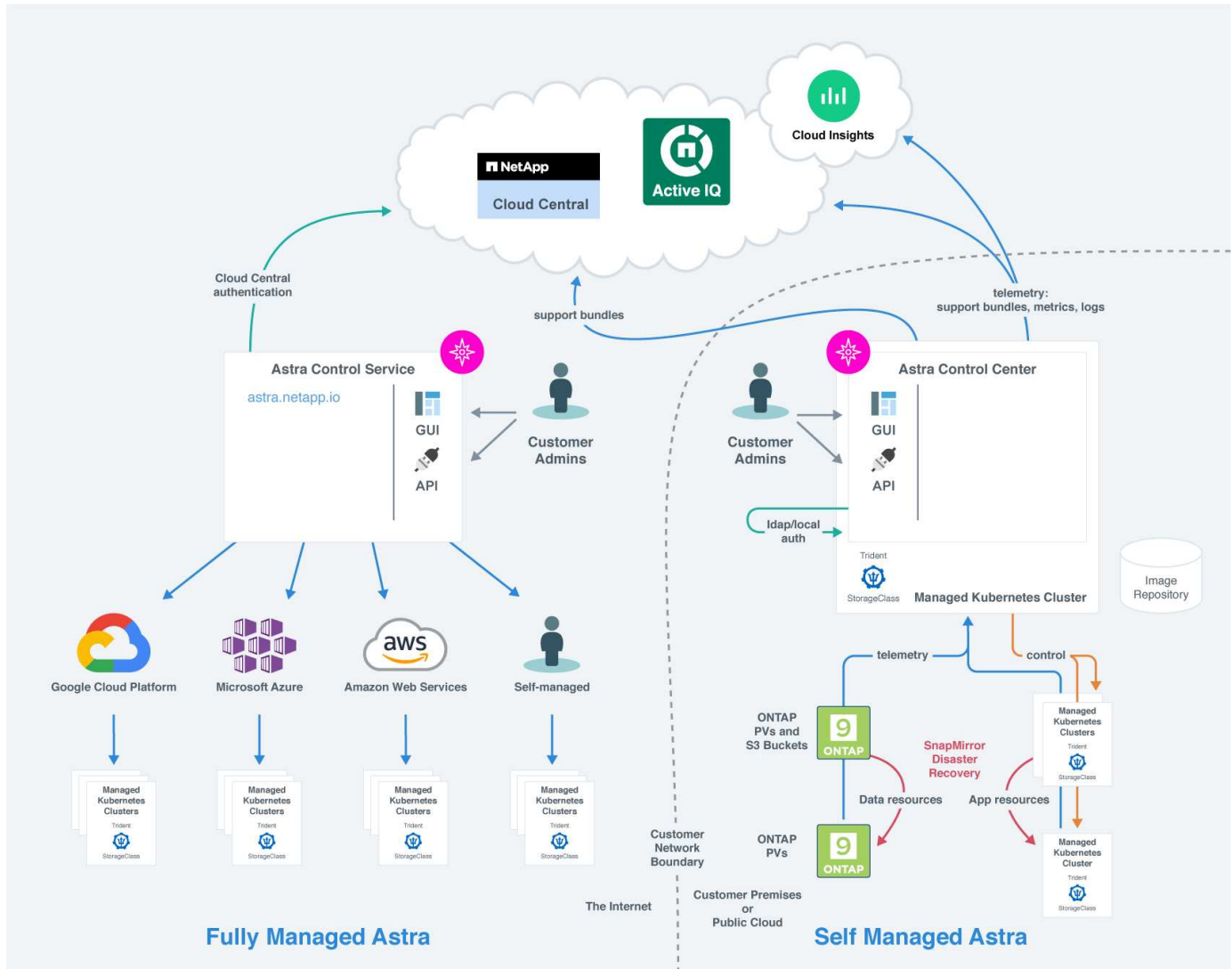
Puis-je gérer les instantanés pris par Astra Control directement via une interface ou un stockage objet différent?

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

Concepts

Architecture et composants

Voici un aperçu des divers composants de l'environnement Astra Control.



Composants d'Astra Control

- **Clusters Kubernetes** : Kubernetes est une plateforme portable, extensible et open source pour la gestion des workloads et des services conteneurisés, qui facilite à la fois la configuration déclarative et l'automatisation. Astra propose des services de gestion pour les applications hébergées dans un cluster Kubernetes.
- **Astra Trident** : en tant que fournisseur de stockage open source entièrement pris en charge et orchestrateur géré par NetApp, Trident vous permet de créer des volumes de stockage pour les applications conteneurisées gérées par Docker et Kubernetes. Lorsqu'il est déployé avec Astra Control Center, Trident inclut un système back-end de stockage ONTAP configuré.
- **Back-end de stockage** :
 - Le service Astra Control utilise les systèmes de stockage back-end suivants :

- ["NetApp Cloud Volumes Service pour Google Cloud"](#) Ou Google persistent Disk en tant que backend de stockage pour les clusters GKE
 - ["Azure NetApp Files"](#) Ou des disques gérés Azure en tant que système de stockage back-end pour les clusters AKS.
 - ["Amazon Elastic Block Store \(EBS\)"](#) ou ["Amazon FSX pour NetApp ONTAP"](#) En tant qu'options de stockage back-end pour les clusters EKS.
- Astra Control Center utilise les systèmes back-end de stockage suivants :
 - ONTAP AFF, FAS et ASA. En tant que plateforme matérielle et logicielle de stockage, ONTAP fournit des services de stockage de base, la prise en charge de plusieurs protocoles d'accès au stockage et des fonctionnalités de gestion du stockage, telles que les snapshots et la mise en miroir.
 - Cloud Volumes ONTAP
- **Cloud Insights** : un outil NetApp de surveillance de l'infrastructure cloud, Cloud Insights vous permet de surveiller les performances et l'utilisation de vos clusters Kubernetes gérés par Astra Control Center. Cloud Insights met en corrélation l'utilisation du stockage avec les charges de travail. Lorsque vous activez la connexion Cloud Insights dans le centre de contrôle Astra, les informations de télémétrie s'affichent dans les pages de l'interface utilisateur du centre de contrôle Astra.

Interfaces de contrôle Astra

Vous pouvez effectuer des tâches à l'aide de différentes interfaces :

- **Interface utilisateur Web (UI)** : Astra Control Service et Astra Control Center utilisent la même interface utilisateur Web où vous pouvez gérer, migrer et protéger des applications. Utilisez également l'interface utilisateur pour gérer les comptes utilisateur et les paramètres de configuration.
- **API** : le service de contrôle Astra et le centre de contrôle Astra utilisent la même API de contrôle Astra. L'API vous permet d'effectuer les mêmes tâches que l'interface utilisateur.

Astra Control Center vous permet également de gérer, de migrer et de protéger les clusters Kubernetes qui s'exécutent dans des environnements de machines virtuelles.

Pour en savoir plus

- ["Documentation relative au service après-vente Astra Control"](#)
- ["Documentation Astra Control Center"](#)
- ["Documentation Astra Trident"](#)
- ["Utilisez l'API de contrôle Astra"](#)
- ["Documentation Cloud Insights"](#)
- ["Documentation ONTAP"](#)

Protection des données

Découvrez les types de protection des données disponibles dans Astra Control Center, et comment il est préférable de les utiliser pour protéger vos applications.

Snapshots, sauvegardes et règles de protection

Les snapshots et les sauvegardes protègent les types de données suivants :

- L'application elle-même
- Tout volume de données persistant associé à l'application
- Tous les artefacts de ressource appartenant à l'application

Un *snapshot* est une copie ponctuelle d'une application stockée sur le même volume provisionné que l'application. Ils sont généralement rapides. Vous pouvez utiliser les snapshots locaux pour restaurer l'application à un point antérieur dans le temps. Les copies Snapshot sont utiles pour les clones rapides. Les snapshots incluent tous les objets Kubernetes de l'application, y compris les fichiers de configuration. Les snapshots sont utiles pour le clonage ou la restauration d'une application au sein du même cluster.

Une *sauvegarde* est basée sur un snapshot. Il est stocké dans le magasin d'objets externe et, par conséquent, peut être plus lent à prendre par rapport aux snapshots locaux. Vous pouvez restaurer une sauvegarde d'application sur le même cluster ou migrer une application en restaurant sa sauvegarde sur un autre cluster. Vous pouvez également choisir une période de conservation plus longue pour les sauvegardes. Les sauvegardes étant stockées dans un référentiel de stockage objet externe, il est généralement plus efficace que les copies Snapshot en cas de panne serveur ou de perte de données.

Une *stratégie de protection* est un moyen de protéger une application en créant automatiquement des snapshots, des sauvegardes ou les deux en fonction d'un planning que vous définissez pour cette application. Une règle de protection vous permet également de choisir le nombre de snapshots et de sauvegardes à conserver dans la planification, et de définir différents niveaux de granularité de planification. L'automatisation de vos sauvegardes et de vos snapshots à l'aide d'une règle de protection est la meilleure façon de garantir que chaque application est protégée en fonction des besoins de votre organisation et des exigences de votre contrat de niveau de service.



Vous ne pouvez pas être entièrement protégé tant que vous n'avez pas une sauvegarde récente. Ceci est important, car les sauvegardes sont stockées dans un magasin d'objets à distance des volumes persistants. En cas de défaillance ou d'accident, le cluster et le stockage persistant qui lui est associé doivent être sauvegardés pour être restaurés. Un snapshot ne vous permettrait pas de restaurer.

Clones

Un *clone* est un doublon exact d'une application, de sa configuration et de ses volumes de données persistants. Vous pouvez créer manuellement un clone sur le même cluster Kubernetes ou sur un autre cluster. Le clonage d'une application peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre.

Réplication sur un cluster distant

Avec Astra Control, vous pouvez assurer la continuité de l'activité de vos applications avec un objectif de point de récupération (RPO) et un objectif de délai de restauration (RTO) faible grâce aux fonctionnalités de réplication asynchrone de la technologie NetApp SnapMirror. Une fois configurée, cela permet à vos applications de répliquer les modifications apportées aux données et aux applications d'un cluster à un autre.

Astra Control réplique de façon asynchrone les copies Snapshot d'application vers un cluster distant. Le processus de réplication inclut les données des volumes persistants répliqués par SnapMirror et les métadonnées d'application protégées par Astra Control.

La réplication d'application est différente de la sauvegarde et de la restauration de l'application de la manière suivante :

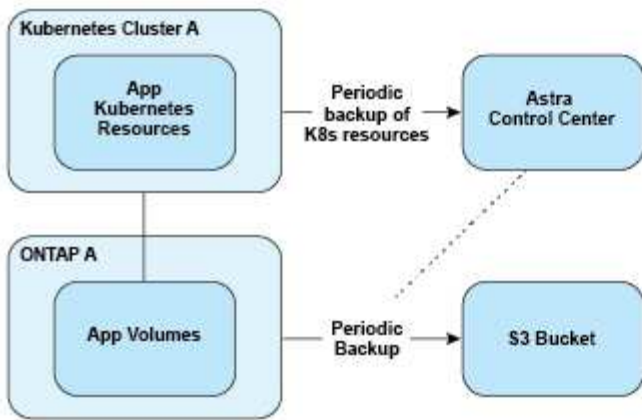
- **Réplication d'application** : Astra Control requiert la disponibilité et la gestion des clusters Kubernetes source et de destination avec leur système back-end de stockage ONTAP respectif configuré pour activer NetApp SnapMirror. Astra Control transfère la copie Snapshot de l'application pilotée par des règles vers le cluster distant. La technologie NetApp SnapMirror est utilisée pour répliquer les données de volume persistant. Pour basculer, Astra Control peut rendre l'application répliquée en ligne en recréant les objets d'application sur le cluster Kubernetes de destination avec les volumes répliqués sur le cluster ONTAP de destination. Comme les données de volume persistant sont déjà présentes sur le cluster ONTAP de destination, Astra Control peut bénéficier d'un temps de récupération rapide pour le basculement.
- **Sauvegarde et restauration d'applications** : lors de la sauvegarde d'applications, Astra Control crée un instantané des données d'application et le stocke dans un compartiment de stockage objet. Lorsqu'une restauration est nécessaire, les données du compartiment doivent être copiées sur un volume persistant du cluster ONTAP. Pour réaliser l'opération de sauvegarde et de restauration, le cluster Kubernetes/ONTAP secondaire ne doit pas être disponible et géré, mais la copie de données supplémentaire peut générer des délais de restauration plus longs.

Pour savoir comment répliquer des applications, voir ["Répliquez vos applications sur un système distant grâce à la technologie SnapMirror"](#).

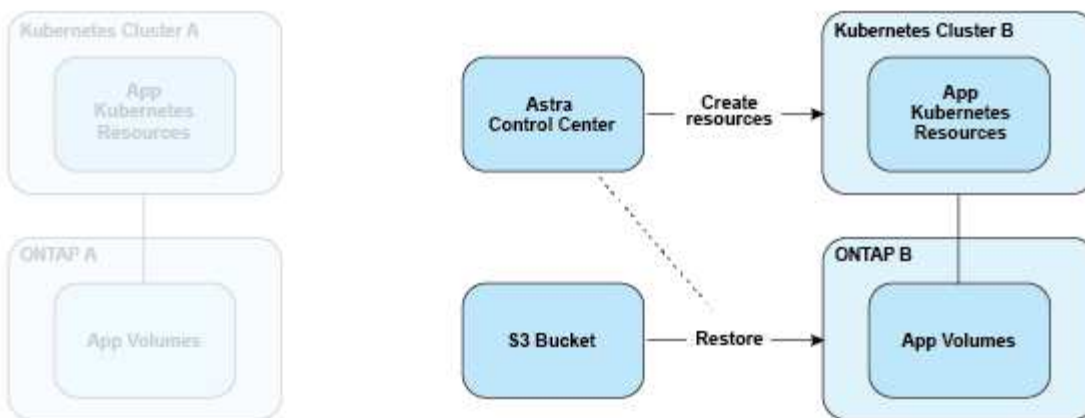
Les images suivantes présentent le processus de sauvegarde et de restauration planifié par rapport au processus de réplication.

Le processus de sauvegarde copie les données dans des compartiments S3 et les restaure à partir de compartiments S3 :

Scheduled Backup

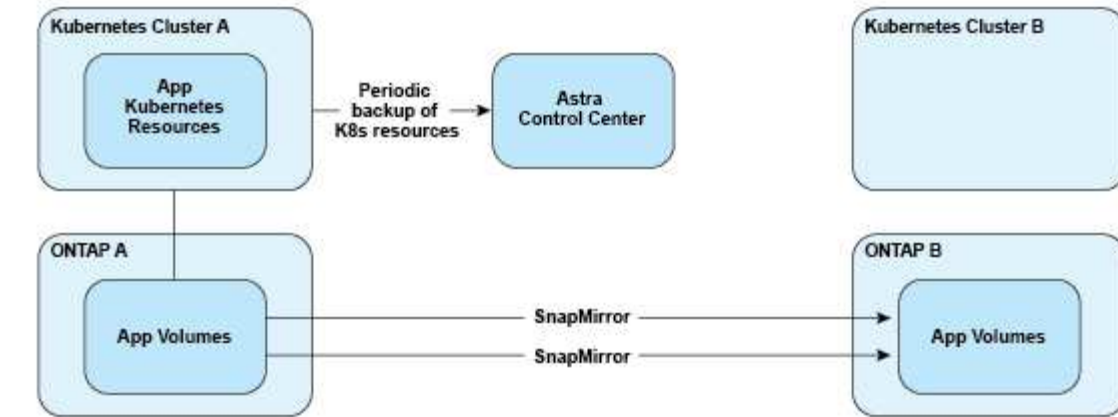


Restore

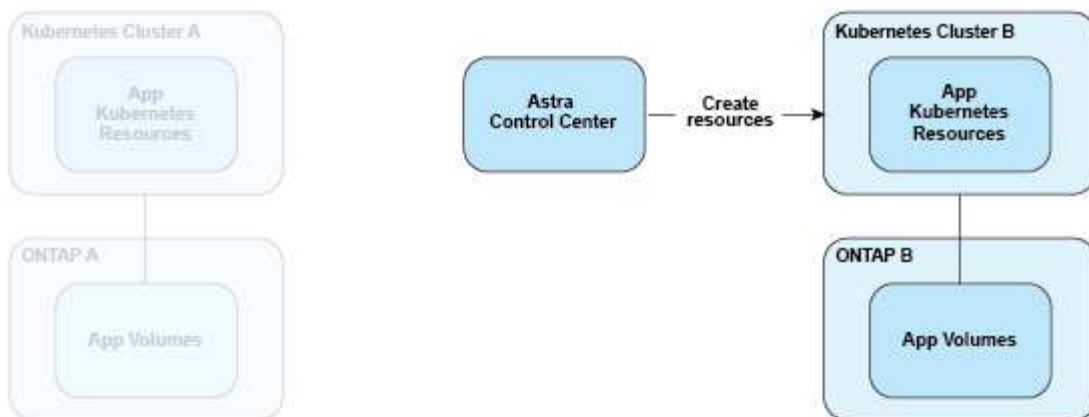


Par contre, la réplication est effectuée par réplication vers ONTAP, puis un basculement crée les ressources Kubernetes :

Replication Relationship



Fail over



Licences

Astra Control Center requiert l'installation d'une licence qui permet la mise en œuvre de la fonctionnalité complète de gestion des données d'application. Lorsque vous déployez Astra Control Center sans licence, une bannière s'affiche dans l'interface utilisateur Web, vous avertissant que la fonctionnalité du système est limitée.

Vous obtenez une licence de l'une des manières suivantes :

- ["Si vous évaluez Astra Control Center, téléchargez le fichier de licence d'évaluation"](#). Une licence d'évaluation vous permet d'utiliser Astra Control Center pendant 90 jours à compter de la date de téléchargement de la licence.
- ["Si vous avez déjà acheté Astra Control Center, générez votre fichier de licence NetApp \(NLF\)"](#) Sur le site de support NetApp. Après avoir acheté le produit, vous recevez un numéro de série et une licence que vous utilisez sur le site de support.

Pour plus d'informations sur les licences requises pour les systèmes de stockage back-end ONTAP, reportez-vous à la ["systèmes back-end de stockage pris en charge"](#).



Il est possible d'ajouter un cluster, d'ajouter un compartiment et de gérer un système back-end sans licence.

Mode de calcul de la consommation des licences

Lorsque vous ajoutez un nouveau cluster à Astra Control Center, il ne prend pas en compte les licences consommées tant qu'au moins une application exécutée sur le cluster est gérée par Astra Control Center.

Lorsque vous commencez à gérer une application sur un cluster, toutes les unités CPU de ce cluster sont incluses dans la consommation de licence Astra Control Center.

Trouvez plus d'informations

- ["Ajoutez une licence lorsque vous configurez Astra Control Center pour la première fois"](#)
- ["Mettre à jour une licence existante"](#)

=
:allow-uri-read:

Classes de stockage et taille de volume persistant

Astra Control Center prend en charge ONTAP en tant que système de stockage back-end.

Présentation

Le centre de contrôle Astra est compatible avec les éléments suivants :

- **Classes de stockage Trident soutenues par ONTAP Storage** : si vous utilisez un back-end ONTAP, Astra Control Center permet d'importer le back-end ONTAP pour signaler diverses informations de surveillance.



Les classes de stockage Trident doivent être préconfigurées en dehors du centre de contrôle Astra.

Classes de stockage

Lorsque vous ajoutez un cluster à Astra Control Center, vous êtes invité à sélectionner une classe de stockage précédemment configurée sur ce cluster comme classe de stockage par défaut. Cette classe de stockage sera utilisée lorsqu'aucune classe de stockage n'est spécifiée dans une demande de volume persistant. La classe de stockage par défaut peut être modifiée à tout moment dans Astra Control Center et toute classe de stockage peut être utilisée à tout moment en spécifiant le nom de la classe de stockage dans le graphique ESV ou Helm. Assurez-vous de n'avoir qu'une seule classe de stockage par défaut définie pour votre cluster Kubernetes.

Pour en savoir plus

- ["Documentation Astra Trident"](#)

Rôles et espaces de noms d'utilisateur

Apprenez-en plus sur les rôles d'utilisateur et les espaces de noms d'Astra Control, et découvrez comment vous pouvez les utiliser pour contrôler l'accès aux ressources de

votre entreprise.

Rôles utilisateur

Vous pouvez utiliser des rôles pour contrôler l'accès des utilisateurs aux ressources ou aux fonctionnalités d'Astra Control. Les rôles d'utilisateur dans Astra Control sont les suivants :

- Un **Viewer** peut afficher les ressources.
- Un **membre** dispose des autorisations de rôle Viewer et peut gérer les applications et les clusters, annuler la gestion des applications et supprimer des instantanés et des sauvegardes.
- Un **Admin** dispose des autorisations de rôle de membre et peut ajouter et supprimer d'autres utilisateurs, à l'exception du propriétaire.
- Un **propriétaire** possède des autorisations de rôle d'administrateur et peut ajouter et supprimer des comptes d'utilisateur.

Vous pouvez ajouter des contraintes à un membre ou à un visualiseur pour limiter l'utilisateur à un ou plusieurs [Espaces de noms](#).

Espaces de noms

Un espace de noms est une portée que vous pouvez attribuer à des ressources spécifiques au sein d'un cluster géré par Astra Control. Astra Control détecte les espaces de noms d'un cluster lorsque vous ajoutez le cluster à Astra Control. Une fois découverts, les espaces de noms sont disponibles pour leur attribuer en tant que contraintes. Seuls les membres ayant accès à cet espace de noms peuvent utiliser cette ressource. Vous pouvez utiliser les espaces de noms pour contrôler l'accès aux ressources à l'aide d'un paradigme adapté à votre entreprise (par exemple, par régions physiques ou par divisions au sein d'une entreprise). Lorsque vous ajoutez des contraintes à un utilisateur, vous pouvez configurer cet utilisateur pour qu'il ait accès à tous les espaces de noms ou seulement à un ensemble spécifique d'espaces de noms. Vous pouvez également affecter des contraintes d'espace de noms à l'aide d'étiquettes d'espace de noms.

Trouvez plus d'informations

["Gérez les utilisateurs et les rôles locaux"](#)

=

:allow-uri-read:

Utilisez Astra Control Center

Commencez à gérer les applications

Après vous "[Ajoutez un cluster à la gestion Astra Control](#)", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour définir les applications et leurs ressources.

De gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer des applications à l'aide d'Astra Control Center, vous devez disposer d'une licence Astra Control Center.
- **Espaces de noms** : les applications peuvent être définies au sein d'un ou plusieurs espaces de noms spécifiés sur un même cluster à l'aide d'Astra Control. Une application peut contenir des ressources couvrant plusieurs espaces de noms au sein d'un même cluster. Astra Control ne prend pas en charge la possibilité de définir des applications entre plusieurs clusters.
- **Classe de stockage** : si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Ressources Kubernetes** : les applications qui utilisent des ressources Kubernetes non collectées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control collecte les ressources Kubernetes suivantes :

ClusterRole	ClusterRoleBinding	ConfigMap
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

Méthodes d'installation d'applications prises en charge

Astra Control prend en charge les méthodes d'installation d'application suivantes :

- **Fichier manifeste** : Astra Control prend en charge les applications installées à partir d'un fichier manifeste utilisant kubectl. Par exemple :

```
kubectl apply -f myapp.yaml
```

- **Helm 3** : si vous utilisez Helm pour installer des applications, Astra Control nécessite Helm version 3. La gestion et le clonage des applications installées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. La gestion des applications installées avec Helm 2 n'est pas prise en charge.
- **Applications déployées par l'opérateur** : Astra Control prend en charge les applications installées avec des opérateurs situés à l'étendue de l'espace de noms qui sont, en général, conçus avec une architecture « valeur par passe » plutôt que « par référence ». Un opérateur et l'application qu'il installe doivent utiliser le même espace de noms ; vous devrez peut-être modifier le fichier .yaml de déploiement pour que l'opérateur s'assure que c'est le cas.

Voici quelques applications opérateur qui suivent ces modèles :

- ["Apache K8ssandra"](#)



Pour K8ssandra, les opérations de restauration sur place sont prises en charge. Pour effectuer une opération de restauration vers un nouvel espace de noms ou un cluster, l'instance d'origine de l'application doit être arrêté. Cela permet de s'assurer que les informations du groupe de pairs transmises ne conduisent pas à une communication entre les instances. Le clonage de l'application n'est pas pris en charge.

- ["IC Jenkins"](#)
- ["Cluster Percona XtraDB"](#)

Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture « pass-by-Reference » (par exemple, l'opérateur CockroachDB). Lors de ces types d'opérations de clonage, l'opérateur cloné tente de référencer les secrets de Kubernetes de l'opérateur source malgré avoir son propre nouveau secret dans le cadre du processus de clonage. Il est possible que le clonage échoue, car Astra Control ne connaît pas les secrets de Kubernetes qui sont présents dans l'opérateur source.

Installez les applications sur votre cluster

Après vous l'avez ["a ajouté votre cluster"](#) Avec Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application dont la portée est étendue à un ou plusieurs espaces de noms peut être gérée.

Définir les applications

Une fois qu'Astra Control détecte les espaces de noms sur vos clusters, vous pouvez définir les applications que vous souhaitez gérer. Vous pouvez choisir [gérer une application couvrant un ou plusieurs espaces de noms](#) ou [gérer la totalité d'un namespace comme une seule application](#). La granularité est en effet au niveau de granularité requis pour les opérations de protection des données.

Bien qu'Astra Control vous permet de gérer séparément les deux niveaux de la hiérarchie (l'espace de noms et les applications dans cet espace de noms ou les espaces de noms d'extension), il est recommandé de choisir l'un ou l'autre. Les actions que vous prenez dans Astra Control peuvent échouer si les actions ont lieu en même temps au niveau de l'espace de noms et de l'application.



Par exemple, vous pouvez définir une stratégie de sauvegarde pour « maria » avec une fréquence hebdomadaire, mais vous devrez peut-être sauvegarder « mariadb » (qui se trouve dans le même espace de noms) plus fréquemment que cela. En fonction de ces besoins, vous devrez gérer les applications séparément et non sous la forme d'une application à espace de noms unique.

Ce dont vous avez besoin

- Un cluster Kubernetes ajouté à Astra Control.
- Une ou plusieurs applications installées sur le cluster. [En savoir plus sur les méthodes d'installation d'applications prises en charge.](#)
- Un ou plusieurs pods actifs.
- Espaces de noms existants sur le cluster Kubernetes que vous avez ajouté à Astra Control.
- (Facultatif) Etiquette Kubernetes de toute ["Ressources Kubernetes prises en charge"](#).



Une étiquette est une paire clé/valeur que vous pouvez attribuer aux objets Kubernetes pour identification. Elles facilitent le tri, l'organisation et la recherche des objets Kubernetes. Pour en savoir plus sur les étiquettes Kubernetes, ["Consultez la documentation officielle Kubernetes"](#).

Description de la tâche

- Avant de commencer, vous devez également comprendre ["gestion des espaces de noms standard et système"](#).
- Si vous prévoyez d'utiliser plusieurs espaces de noms avec vos applications dans Astra Control, ["modifier les rôles utilisateur avec des contraintes d'espace de noms"](#) Après la mise à niveau vers une version Astra Control Center avec prise en charge de plusieurs espaces de noms.
- Pour obtenir des instructions sur la gestion des applications à l'aide de l'API Astra Control, reportez-vous au ["Informations sur l'automatisation et les API d'Astra"](#).

Options de gestion des applications

- [Définissez les ressources à gérer en tant qu'application](#)
- [Définissez un espace de noms à gérer en tant qu'application](#)

Définissez les ressources à gérer en tant qu'application

Vous pouvez spécifier le ["Ressources Kubernetes qui constituent une application"](#) Que vous voulez gérer avec Astra Control. La définition d'une application vous permet de regrouper des éléments de votre cluster Kubernetes dans une seule application. Cette collection de ressources Kubernetes est organisée par critères d'espace de noms et de sélecteur d'étiquettes.

La définition d'une application vous offre un contrôle plus granulaire sur les éléments à inclure dans une opération Astra Control, notamment le clonage, les snapshots et les sauvegardes.



Lors de la définition d'applications, assurez-vous de ne pas inclure de ressource Kubernetes dans plusieurs applications avec des règles de protection. Le chevauchement des règles de protection sur les ressources Kubernetes peut entraîner des conflits de données. [En savoir plus dans un exemple.](#)

L'exécution d'une opération de restauration sur place sur une application qui partage des ressources avec une autre application peut avoir des résultats inattendus. Toutes les ressources partagées entre les applications sont remplacées lorsqu'une restauration sur place est effectuée sur l'une des applications. Par exemple, le scénario suivant génère une situation indésirable lors de l'utilisation de la réplication NetApp SnapMirror :



1. Vous définissez l'application `app1` utilisation de l'espace de noms `ns1`.
2. Vous configurez une relation de réplication pour `app1`.
3. Vous définissez l'application `app2` (sur le même cluster) utilisant les namespaces `ns1` et `ns2`.
4. Vous configurez une relation de réplication pour `app2`.
5. La réplication est inversée pour `app2`. Ceci provoque le `app1` l'application sur le cluster source à désactiver.

** a propos de l'ajout de ressources cluster-scoped à vos espaces de noms d'applications.**

Vous pouvez importer des ressources de cluster associées aux ressources d'espace de noms en plus de celles incluses automatiquement dans Astra Control. Vous pouvez ajouter une règle qui inclura des ressources d'un groupe, un type, une version et, éventuellement, une étiquette. Vous voudrez peut-être le faire si certaines ressources qu'Astra Control n'incluent pas automatiquement.

Vous ne pouvez exclure aucune des ressources à périmètre de cluster qui sont automatiquement incluses par Astra Control.

Vous pouvez ajouter les éléments suivants `apiVersions` (Qui sont les groupes combinés avec la version API) :

Type de ressource	ApiVersions (groupe + version)
ClusterRole	rbac.authorization.k8s.io/v1
ClusterRoleBinding	rbac.authorization.k8s.io/v1
CustomResource	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
CustomResourceDefinition	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
MutatingWebhookConfiguration	admissionregistration.k8s.io/v1
ValidatingWebhookConfiguration	admissionregistration.k8s.io/v1

Étapes

1. Dans la page applications, sélectionnez **définir**.
2. Dans la fenêtre **define application**, entrez le nom de l'application.
3. Choisissez le cluster sur lequel votre application s'exécute dans la liste déroulante **Cluster**.
4. Choisissez un espace de nom pour votre application dans la liste déroulante **namespace**.



Les applications peuvent être définies au sein d'un ou plusieurs espaces de noms spécifiés sur un même cluster à l'aide d'Astra Control. Une application peut contenir des ressources couvrant plusieurs espaces de noms au sein d'un même cluster. Astra Control ne prend pas en charge la possibilité de définir des applications entre plusieurs clusters.

- (Facultatif) Indiquez une étiquette pour les ressources Kubernetes dans chaque espace de noms. Vous pouvez spécifier un seul libellé ou un seul critère de sélection d'étiquette (requête).



Pour en savoir plus sur les étiquettes Kubernetes, "[Consultez la documentation officielle Kubernetes](#)".

- (Facultatif) Ajouter des espaces de noms supplémentaires pour l'application en sélectionnant **Ajouter un espace de noms** et en choisissant l'espace de noms dans la liste déroulante.
- (Facultatif) Entrez des critères de sélection d'étiquette ou d'étiquette pour tout espace de noms supplémentaire que vous ajoutez.
- (Facultatif) pour inclure des ressources à périmètre de cluster en plus de celles qu'Astra Control inclut automatiquement, cochez **inclure des ressources supplémentaires à périmètre de cluster** et complétez les éléments suivants :
 - Sélectionnez **Ajouter inclure règle**.
 - Groupe** : dans la liste déroulante, sélectionnez le groupe de ressources API.
 - Type** : dans la liste déroulante, sélectionnez le nom du schéma d'objet.
 - Versión** : saisissez la version de l'API.
 - Sélecteur d'étiquettes** : si vous le souhaitez, incluez un libellé à ajouter à la règle. Cette étiquette est utilisée pour récupérer uniquement les ressources correspondant à cette étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe.
 - Vérifiez la règle créée en fonction de vos entrées.
 - Sélectionnez **Ajouter**.



Vous pouvez créer autant de règles de ressources à périmètre cluster que vous le souhaitez. Les règles apparaissent dans le Résumé de l'application définir.

- Sélectionnez **définir**.
- Après avoir sélectionné **définir**, répétez le processus pour les autres applications, selon les besoins.

Une fois que vous avez terminé de définir une application, celle-ci s'affiche dans **Healthy** Dans la liste des applications de la page applications. Vous pouvez désormais le cloner et créer des sauvegardes et des snapshots.



Il se peut que l'application que vous venez d'ajouter comporte une icône d'avertissement sous la colonne protégé, indiquant qu'elle n'est pas encore sauvegardée et qu'elle n'est pas planifiée pour les sauvegardes.



Pour afficher les détails d'une application particulière, sélectionnez le nom de l'application.

Pour afficher les ressources ajoutées à cette application, sélectionnez l'onglet **Ressources**. Sélectionnez le numéro après le nom de la ressource dans la colonne ressource ou entrez le nom de la ressource dans la

recherche pour voir les ressources supplémentaires comprises dans la portée du cluster.

Définissez un espace de noms à gérer en tant qu'application

Vous pouvez ajouter toutes les ressources Kubernetes dans un namespace à la gestion d'Astra Control en définissant les ressources de ce namespace comme une application. Cette méthode est préférable à définir des applications individuellement si vous avez l'intention de gérer et de protéger toutes les ressources d'un espace de noms particulier de la même manière et à intervalles communs.

Étapes

1. Sur la page clusters, sélectionnez un cluster.
2. Sélectionnez l'onglet **espaces de noms**.
3. Sélectionnez le menu actions de l'espace de noms contenant les ressources d'application que vous souhaitez gérer et sélectionnez **définir comme application**.



Si vous souhaitez définir plusieurs applications, sélectionnez dans la liste Namespaces et sélectionnez le bouton **actions** dans le coin supérieur gauche et sélectionnez **définir comme application**. Cela définira plusieurs applications individuelles dans leurs espaces de noms individuels. Pour les applications à espace de noms multiples, voir [Définissez les ressources à gérer en tant qu'application](#).



Cochez la case **Afficher les espaces de noms système** pour afficher les espaces de noms système qui ne sont généralement pas utilisés dans la gestion des applications par défaut. Show system namespaces ["En savoir plus"](#).

Une fois le processus terminé, les applications associées à l'espace de noms apparaissent dans le Associated applications colonne.

Qu'en est-il des espaces de noms système

Astra Control détecte également les espaces de noms système sur un cluster Kubernetes. Nous ne vous montrons pas ces espaces de noms système par défaut, car il est rare qu'il soit nécessaire de sauvegarder les ressources d'applications système.

Vous pouvez afficher les espaces de noms système à partir de l'onglet espaces de noms d'un cluster sélectionné en cochant la case **Afficher les espaces de noms système**.

Show system namespaces



Astra Control en soi n'est pas une application standard. Il s'agit d'une « application système ». Vous ne devriez pas essayer de gérer Astra Control lui-même. Le contrôle Astra lui-même n'est pas indiqué par défaut pour la direction.

Exemple : politique de protection distincte pour différentes versions

Dans cet exemple, l'équipe devops gère un déploiement de version « canary ». Le cluster de l'équipe a trois modules exécutant Nginx. Deux des modules sont dédiés à la version stable. Le troisième pod est pour la libération des canaris.

L'administrateur Kubernetes de l'équipe devops ajoute ce label `deployment=stable` aux boîtiers de déverrouillage stables. L'équipe ajoute l'étiquette `deployment=canary` à la canary release pod.

La version stable de l'équipe inclut des snapshots horaires et des sauvegardes quotidiennes. La libération des canaris est plus éphémère, ils veulent donc créer une politique de protection moins agressive à court terme pour tout ce qui est étiqueté `deployment=canary`.

Afin d'éviter d'éventuels conflits de données, l'administrateur va créer deux apps: Une pour la version "canary", et une pour la version "stable". Les sauvegardes, snapshots et opérations de clonage sont donc séparés pour les deux groupes d'objets Kubernetes.

Trouvez plus d'informations

- ["Utilisez l'API de contrôle Astra"](#)
- ["Annuler la gestion d'une application"](#)

Protégez vos applications

Présentation de la protection

Vous pouvez créer des sauvegardes, des clones, des copies Snapshot et des règles de protection pour vos applications à l'aide d'Astra Control Center. La sauvegarde de vos applications aide vos services et vos données associées à être aussi disponibles que possible. En cas d'incident, la restauration à partir d'une sauvegarde permet une restauration complète d'une application et de ses données, avec une interruption minimale. Les sauvegardes, les clones et les snapshots contribuent à vous protéger contre les menaces classiques, comme les ransomwares, la perte accidentelle de données et les incidents environnementaux. ["Découvrez les types de protection des données disponibles dans Astra Control Center et le moment de les utiliser"](#).

En outre, vous pouvez répliquer des applications sur un cluster distant en préparation de la reprise après incident.

Workflow de protection des applications

Vous pouvez utiliser l'exemple de flux de travail suivant pour commencer à protéger vos applications.

[Une seule] Protégez toutes vos applications

Pour être sûr que vos applications sont immédiatement protégées, ["créez une sauvegarde manuelle de toutes les applications"](#).

[Deux] Configurez une stratégie de protection pour chaque application

Pour automatiser les sauvegardes et snapshots futurs, ["configurez une stratégie de protection pour chaque application"](#). Par exemple, vous pouvez commencer avec des sauvegardes hebdomadaires et des snapshots quotidiens, et en conserver un mois pour les deux. Il est fortement recommandé d'automatiser les sauvegardes et les snapshots avec une règle de protection par rapport aux sauvegardes et snapshots manuels.

[Trois] Ajuster les règles de protection

À mesure que les applications et leurs modèles d'utilisation évoluent, ajustez les règles de protection selon les besoins pour bénéficier d'une protection optimale.

[Quatre] Répliquer les applications sur un cluster distant

"[Réplication d'applications](#)" Sur un cluster distant avec la technologie NetApp SnapMirror. Astra Control réplique les copies Snapshot sur un cluster distant, offrant une fonctionnalité de reprise après incident asynchrone.

[Cinq] En cas d'incident, restaurez vos applications avec la dernière sauvegarde ou réplication sur un système distant

En cas de perte de données, vous pouvez effectuer une restauration par "[restauration de la dernière sauvegarde](#)" d'abord pour chaque application. Vous pouvez alors restaurer le dernier snapshot (si disponible). Vous pouvez également utiliser la réplication sur un système distant.

Protéger les applications avec les snapshots et les sauvegardes

Protégez toutes les applications en effectuant des copies Snapshot et des sauvegardes à l'aide d'une stratégie de protection automatisée ou ad hoc. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou "[API de contrôle Astra](#)" pour protéger les applications.

Description de la tâche

- **Helm Deployed apps** : si vous utilisez Helm pour déployer des applications, Astra Control Center nécessite 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.
- **(clusters OpenShift uniquement) Ajouter des règles** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Vous pouvez effectuer les tâches suivantes liées à la protection de vos données applicatives :

- [Configurer une règle de protection](#)
- [Créer un snapshot](#)
- [Créer une sauvegarde](#)
- [Afficher les snapshots et les sauvegardes](#)
- [Supprimer les instantanés](#)
- [Annuler les sauvegardes](#)
- [Supprimer les sauvegardes](#)

Configurer une règle de protection

Une règle de protection protège une application en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Vous pouvez choisir de créer des snapshots et des sauvegardes toutes les heures, tous les jours, toutes les semaines et tous les mois, et vous pouvez spécifier le nombre de copies à conserver.

Si vous avez besoin de sauvegardes ou de snapshots pour qu'ils s'exécutent plus fréquemment qu'une fois par heure, vous pouvez "[Utilisez l'API REST Astra Control pour créer des snapshots et des sauvegardes](#)".

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Sélectionnez **configurer la stratégie de protection**.
4. Définissez un planning de protection en choisissant le nombre de snapshots et de sauvegardes pour conserver toutes les heures, tous les jours, toutes les semaines et tous les mois.

Vous pouvez définir les horaires horaires, quotidiens, hebdomadaires et mensuels simultanément. Un programme ne s'active pas tant que vous n'avez pas défini de niveau de rétention.

Lorsque vous définissez un niveau de conservation pour les sauvegardes, vous pouvez choisir le compartiment dans lequel vous souhaitez stocker les sauvegardes.

L'exemple suivant illustre quatre planifications de protection : toutes les heures, tous les jours, toutes les semaines et tous les mois pour les snapshots et les sauvegardes.

Configure protection policy STEP 1/2: DETAILS

PROTECTION SCHEDULE

Hourly: Every hour on the 0th minute, keep the last 4 snapshots

Daily: Daily at 02:00 (UTC), keep the last 15 snapshots

Weekly: Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots

Monthly: Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly ● Daily ● **Weekly** ● Monthly

Select Weekday(s) (optional): Monday X

Time (UTC) (optional): 02:00

Snapshots to keep: 26

Backups to keep: 0

BACKUP DESTINATION

Bucket: ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10 (Default)

OVERVIEW

Schedule and retention

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application cattle-logging

Namespace cattle-logging

Cluster se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel Review ->

5. Sélectionnez **Revue**.
6. Sélectionnez **définir la stratégie de protection**.

Résultat

Astra Control implémente la règle de protection des données en créant et en conservant des snapshots et des sauvegardes à l'aide du calendrier et de la règle de conservation que vous avez définis.

Créer un snapshot

Vous pouvez créer un snapshot à la demande à tout moment.

Étapes

1. Sélectionnez **applications**.
2. Dans le menu Options de la colonne **actions** de l'application souhaitée, sélectionnez **instantané**.
3. Personnalisez le nom du snapshot, puis sélectionnez **Suivant**.
4. Examinez le résumé de l'instantané et sélectionnez **instantané**.

Résultat

Le processus d'instantané commence. Un instantané a réussi lorsque l'état est **Healthy** dans la colonne **State** de la page **Data protection > snapshots**.

Créer une sauvegarde

Vous pouvez également sauvegarder une application à tout moment.



Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.

Étapes

1. Sélectionnez **applications**.
2. Dans le menu Options de la colonne **actions** de l'application souhaitée, sélectionnez **Sauvegarder**.
3. Personnaliser le nom de la sauvegarde.
4. Choisissez de sauvegarder l'application à partir d'un snapshot existant. Si vous sélectionnez cette option, vous pouvez choisir parmi une liste de snapshots existants.
5. Choisir un compartiment de destination pour la sauvegarde dans la liste des compartiments de stockage.
6. Sélectionnez **Suivant**.
7. Passez en revue le résumé des sauvegardes et sélectionnez **Sauvegarder**.

Résultat

Astra Control crée une sauvegarde de l'application.



Si votre réseau est en panne ou anormalement lent, une opération de sauvegarde risque d'être terminée. Ceci entraîne l'échec de la sauvegarde.



Si vous devez annuler une sauvegarde en cours d'exécution, suivez les instructions de la section [Annuler les sauvegardes](#). Pour supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez les instructions de la section [Supprimer les sauvegardes](#).



Après une opération de protection des données (clonage, sauvegarde, restauration) et après le redimensionnement du volume persistant, il y a vingt minutes de retard avant que la nouvelle taille du volume ne s'affiche dans l'interface utilisateur. La protection des données fonctionne avec succès en quelques minutes et vous pouvez utiliser le logiciel de gestion pour le système back-end pour confirmer la modification de la taille du volume.

Afficher les snapshots et les sauvegardes

Vous pouvez afficher les instantanés et les sauvegardes d'une application à partir de l'onglet protection des données.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.

Les snapshots s'affichent par défaut.

3. Sélectionnez **backups** pour afficher la liste des sauvegardes.

Supprimer les instantanés

Supprimez les snapshots programmés ou à la demande dont vous n'avez plus besoin.



Vous ne pouvez pas supprimer un snapshot en cours de réplication.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez **protection des données**.
3. Dans le menu Options de la colonne **actions** pour l'instantané souhaité, sélectionnez **Supprimer instantané**.
4. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer l'instantané**.

Résultat

Astra Control supprime le snapshot.

Annuler les sauvegardes

Vous pouvez annuler une sauvegarde en cours.



Pour annuler une sauvegarde, la sauvegarde doit être dans `Running` état. Vous ne pouvez pas annuler une sauvegarde dans `Pending` état.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Sélectionnez **backups**.
4. Dans le menu Options de la colonne **actions** pour la sauvegarde souhaitée, sélectionnez **Annuler**.
5. Tapez le mot "annuler" pour confirmer l'opération, puis sélectionnez **Oui, annuler la sauvegarde**.

Supprimer les sauvegardes

Supprimez les sauvegardes planifiées ou à la demande qui ne vous sont plus nécessaires.



Si vous devez annuler une sauvegarde en cours d'exécution, suivez les instructions de la section [Annuler les sauvegardes](#). Pour supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez ces instructions.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Sélectionnez **backups**.
4. Dans le menu Options de la colonne **actions** pour la sauvegarde souhaitée, sélectionnez **Supprimer sauvegarde**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer sauvegarde**.

Résultat

Astra Control supprime la sauvegarde.

Restaurez les applications

Astra Control peut restaurer votre application à partir d'un snapshot ou d'une sauvegarde. La restauration d'un snapshot existant est plus rapide lors de la restauration d'une application sur le même cluster. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "[API de contrôle Astra](#)" pour restaurer des applications.



Lorsque vous effectuez une restauration sur place d'une application qui utilise un stockage NetApp ONTAP, l'espace utilisé par cette application peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.

Description de la tâche

- **Protéger vos applications d'abord**: Il est fortement recommandé de prendre un instantané de ou de sauvegarder votre application avant de la restaurer. Cela vous permettra de cloner à partir du snapshot ou de la sauvegarde en cas d'échec de la restauration.
- **Vérifiez les volumes de destination** : si vous restaurez sur un autre cluster, assurez-vous que le cluster utilise le même mode d'accès aux volumes persistants (par exemple, ReadWriteMany). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent.
- **(clusters OpenShift uniquement) Ajouter des règles** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- **Helm Deployed apps** : le clonage des applications déployées avec Helm 3 (ou mis à niveau de Helm 2 vers Helm 3) est entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Si vous souhaitez effectuer une restauration à partir d'un instantané, conservez l'icône **snapshots** sélectionnée. Sinon, sélectionnez l'icône **backups** pour restaurer à partir d'une sauvegarde.
4. Dans le menu Options de la colonne **actions** pour l'instantané ou la sauvegarde à partir duquel vous souhaitez restaurer, sélectionnez **Restaurer l'application**.
5. Choisissez le type de restauration :
 - **Restaurer les espaces de noms d'origine** : utilisez cette procédure pour restaurer l'app sur place dans le cluster d'origine.

L'exécution d'une opération de restauration sur place sur une application qui partage des ressources avec une autre application peut avoir des résultats inattendus. Toutes les ressources partagées entre les applications sont remplacées lorsqu'une restauration sur place est effectuée sur l'une des applications. Par exemple, le scénario suivant génère une situation indésirable lors de l'utilisation de la réplication NetApp SnapMirror :



- i. Vous définissez l'application `app1` utilisation de l'espace de noms `ns1`.
- ii. Vous configurez une relation de réplication pour `app1`.
- iii. Vous définissez l'application `app2` (sur le même cluster) utilisant les namespaces `ns1` et `ns2`.
- iv. Vous configurez une relation de réplication pour `app2`.
- v. La réplication est inversée pour `app2`. Ceci provoque le `app1` l'application sur le cluster source à désactiver.

- i. Sélectionnez le snapshot à utiliser pour restaurer l'application sur place, qui restaure l'application vers une version antérieure de lui-même.
- ii. Sélectionnez **Suivant**.



Si vous restaurez vers un espace de nom qui a déjà été supprimé, un nouvel espace de nom avec le même nom est créé dans le cadre du processus de restauration. Tous les utilisateurs disposant des droits de gestion des applications dans l'espace de noms précédemment supprimé doivent restaurer manuellement les droits sur l'espace de noms nouvellement créé.

- iii. Consultez les détails de l'action de restauration, saisissez "restaurer" et sélectionnez **Restaurer**.
- **Restaurer vers de nouveaux espaces de noms** : utilisez cette procédure pour restaurer l'application vers un autre cluster ou avec des espaces de noms différents de la source.
 - i. Choisissez le cluster de destination pour l'application que vous souhaitez restaurer.
 - ii. Entrez un espace de noms de destination pour chaque espace de noms source associé à l'application.



Astra Control crée de nouveaux espaces de noms de destination dans le cadre de cette option de restauration. Les espaces de noms de destination que vous spécifiez ne doivent pas être déjà présents sur le cluster de destination.

- iii. Sélectionnez **Suivant**.
- iv. Sélectionnez le snapshot à utiliser pour restaurer l'application.
- v. Sélectionnez **Suivant**.
- vi. Consultez les détails de l'action de restauration et sélectionnez **Restaurer**.

Résultat

Astra Control restaure l'application en fonction des informations que vous avez fournies. Si vous avez restauré l'application sur place, le contenu des volumes persistants existants est remplacé par le contenu des volumes persistants de l'application restaurée.



Après une opération de protection des données (clonage, sauvegarde ou restauration) et après le redimensionnement du volume persistant, la nouvelle taille du volume s'affiche dans l'interface utilisateur Web pendant vingt minutes. La protection des données fonctionne avec succès en quelques minutes et vous pouvez utiliser le logiciel de gestion pour le système back-end pour confirmer la modification de la taille du volume.



Tout utilisateur membre aux contraintes de namespace par nom/ID d'espace de noms ou par libellés de namespace peut cloner ou restaurer une application vers un nouvel espace de noms sur le même cluster ou vers tout autre cluster du compte de son entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

Répliquez vos applications sur un système distant grâce à la technologie SnapMirror

Avec Astra Control, vous pouvez assurer la continuité de l'activité de vos applications avec un objectif de point de récupération (RPO) et un objectif de délai de restauration (RTO) faible grâce aux fonctionnalités de réplication asynchrone de la technologie NetApp SnapMirror. Une fois configurée, cela permet à vos applications de répliquer les modifications apportées aux données et aux applications d'un cluster à un autre.

Pour une comparaison entre les sauvegardes/restaurations et la réplication, voir "[Concepts de protection des données](#)".

Vous pouvez répliquer des applications dans différents scénarios, comme : uniquement sur site, environnements hybrides et multicloud :

- Du site A au site B sur site
- Du site au cloud avec Cloud Volumes ONTAP
- Cloud avec Cloud Volumes ONTAP vers une infrastructure sur site
- Cloud avec Cloud Volumes ONTAP vers le cloud (entre différentes régions du même fournisseur cloud ou

vers des fournisseurs de cloud différents)

Astra Control peut répliquer les applications entre les clusters sur site, le stockage sur site vers le cloud (avec Cloud Volumes ONTAP) ou entre les clouds (Cloud Volumes ONTAP vers Cloud Volumes ONTAP).



Vous pouvez répliquer simultanément une autre application (exécutée sur l'autre cluster ou site) dans la direction opposée. Par exemple, les applications A, B, C peuvent être répliquées depuis Datacenter 1 vers Datacenter 2. Et les applications X, y, Z peuvent être répliquées depuis Datacenter 2 vers Datacenter 1.

Avec Astra Control, vous pouvez effectuer les tâches suivantes relatives aux applications de réplication :

- [Configuration d'une relation de réplication](#)
- [Mettre une application répliquée en ligne sur le cluster de destination \(basculement\)](#)
- [Resynchroniser un basculement de réplication impossible](#)
- [Réplication inverse des applications](#)
- [Rétablir le fonctionnement des applications sur le cluster source d'origine](#)
- [Supprime une relation de réplication d'application](#)

Conditions préalables à la réplication

La réplication de l'application Astra Control exige que les conditions préalables suivantes soient respectées avant de commencer :

- Pour assurer une reprise après incident transparente, nous vous recommandons de déployer Astra Control Center dans un troisième domaine de pannes ou un troisième site secondaire.
- Le cluster Kubernetes hôte de l'application et un cluster Kubernetes de destination doivent être gérés avec leurs clusters ONTAP, dans l'idéal dans différents domaines ou sites de défaillance.
- Les clusters ONTAP et le SVM hôte doivent être associés. Voir "[Présentation du cluster et de SVM peering](#)".
- Le SVM distant couplé doit être disponible avec Astra Trident sur le cluster de destination.
- La version 22.07 ou ultérieure d'Astra Trident doit exister sur les clusters ONTAP source et de destination.
- Les licences asynchrones ONTAP SnapMirror via le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Voir "[Présentation des licences SnapMirror dans ONTAP](#)".
- Lorsque vous ajoutez un système de stockage back-end ONTAP à Astra Control Center, appliquez les identifiants de l'utilisateur avec le rôle « admin » qui possède des méthodes d'accès `http` et `ontapi` Activation sur les clusters ONTAP source et de destination Voir "[Gérer les comptes utilisateur dans la documentation ONTAP](#)" pour en savoir plus.
- Les clusters Kubernetes source et destination et les clusters ONTAP doivent être gérés par Astra Control.



Vous pouvez répliquer simultanément une autre application (exécutée sur l'autre cluster ou site) dans la direction opposée. Par exemple, les applications A, B, C peuvent être répliquées depuis Datacenter 1 vers Datacenter 2. Et les applications X, y, Z peuvent être répliquées depuis Datacenter 2 vers Datacenter 1.

- **Configuration de l'Astra Trident / ONTAP** : le Centre de contrôle Astra requiert la création et la définition d'une classe de stockage comme classe de stockage par défaut. Astra Control Center prend en charge les pilotes ONTAP suivants fournis par Astra Trident pour la réplication :

- ontap-nas
- ontap-nas-flexgroup
- ontap-san

Découvrez comment ["Répliquez vos applications sur un système distant grâce à la technologie SnapMirror"](#).

Configuration d'une relation de réplication

La configuration d'une relation de réplication implique les éléments suivants qui constituent la règle de réplication ;

- Choix de la fréquence à laquelle vous souhaitez qu'Astra Control prenne un snapshot d'application (qui inclut les ressources Kubernetes de l'application ainsi que les copies de volume Snapshot pour chacun des volumes de l'application)
- Choix de la planification de réplication (ressources Kubernetes incluses ainsi que données de volume persistant)
- Réglage de l'heure de prise de vue

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, sélectionnez **configurer la stratégie de réplication**. Ou, dans la zone protection des applications, sélectionnez l'option actions et sélectionnez **configurer la stratégie de réplication**.
4. Entrez ou sélectionnez les informations suivantes :
 - **Grappe de destination** : saisissez un cluster de destination différent de la source.
 - **Classe de stockage de destination** : sélectionnez ou entrez la classe de stockage qui utilise le SVM apparié sur le cluster ONTAP de destination.
 - **Type de réplication**: "Asynchrone" est actuellement le seul type de réplication disponible.
 - **Espace de noms de destination** : saisissez des espaces de noms de destination nouveaux ou existants pour le cluster de destination.
 - (Facultatif) Ajouter des espaces de noms supplémentaires en sélectionnant **Ajouter espace de noms** et en choisissant l'espace de noms dans la liste déroulante.
 - **Fréquence de réplication**: Définissez la fréquence à laquelle vous souhaitez qu'Astra Control prenne un instantané et le réplique à sa destination.
 - **Décalage**: Définissez le nombre de minutes à partir du haut de l'heure que vous voulez que le contrôle Astra prenne un instantané. Vous pouvez utiliser un décalage afin qu'il ne coïncide pas avec d'autres opérations planifiées. Par exemple, si vous voulez prendre l'instantané toutes les 5 minutes à partir de 10:02, entrez "02" comme minutes de décalage. Le résultat serait 10:02, 10:07, 10:12, etc
5. Sélectionnez **Suivant**, examinez le résumé et sélectionnez **Enregistrer**.



Au début, l'état affiche « APP-mirror » avant que le premier programme ne se produise.

Astra Control crée un Snapshot d'application utilisé pour la réplication.

6. Pour afficher l'état de l'instantané de l'application, sélectionnez l'onglet **applications > snapshots**.

Le nom d'un snapshot utilise le format « Replication-schedule-<chaîne> ». Astra Control conserve le dernier snapshot utilisé pour la réplication. Tous les snapshots de réplication plus anciens sont supprimés après la réussite de la réplication.

Résultat

Cela crée la relation de réplication.

Astra Control effectue les actions suivantes à la suite de l'établissement de la relation :

- Crée un espace de noms sur la destination (s'il n'existe pas)
- Crée une demande de volume persistant sur l'espace de noms de destination correspondant aux demandes de volume virtuel de l'application source.
- Utilise une copie Snapshot initiale cohérente avec les applications.
- Établit la relation SnapMirror pour les volumes persistants à l'aide de la copie Snapshot initiale.

La page protection des données indique l'état et le statut de la relation de réplication : <Health status> | <Relationship cycle State>

Par exemple : normal | établi

Pour en savoir plus sur l'état et l'état de la réplication, consultez cette rubrique.

Mettre une application répliquée en ligne sur le cluster de destination (basculement)

Avec Astra Control, vous pouvez basculer les applications répliquées vers un cluster de destination. Cette procédure arrête la relation de réplication et met l'application en ligne sur le cluster de destination. Cette procédure n'arrête pas l'application sur le cluster source s'il était opérationnel.

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **basculer**.
4. Dans la page basculement, consultez les informations et sélectionnez **basculer**.

Résultat

Les actions suivantes se produisent suite à la procédure de basculement :

- Sur le cluster de destination, l'application démarre en fonction du dernier snapshot répliqué.
- Le cluster source et l'app (si opérationnel) ne sont pas arrêtés et continuent à fonctionner.
- L'état de réplication passe à « basculement » puis à « basculement » une fois terminé.
- La stratégie de protection de l'application source est copiée vers l'application de destination en fonction des planifications présentes sur l'application source au moment du basculement.
- Astra Control affiche l'application sur les clusters source et de destination et son état de santé respectif.

Resynchroniser un basculement de réplication impossible

L'opération de resynchronisation rétablit la relation de réplication. Vous pouvez choisir la source de la relation pour conserver les données sur le cluster source ou destination. Cette opération rétablit les relations SnapMirror pour démarrer la réplication du volume dans le sens de votre choix.

Le processus arrête l'application sur le nouveau cluster de destination avant de rétablir la réplication.



Pendant le processus de resynchronisation, l'état du cycle de vie apparaît comme « établissement ».

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **Resync**.
4. Dans la page Resync, sélectionnez l'instance d'application source ou de destination contenant les données que vous souhaitez conserver.



Choisissez soigneusement la source de resynchronisation, car les données de la destination sont écrasées.

5. Sélectionnez **Resync** pour continuer.
6. Tapez « resynchroniser » pour confirmer.
7. Sélectionnez **Oui, resynchronisation** pour terminer.

Résultat

- La page réplication affiche « établissement » comme état de réplication.
- Astra Control arrête l'application sur le nouveau cluster de destination.
- Astra Control rétablit le processus de réplication du volume persistant dans la direction sélectionnée à l'aide de la resynchronisation de SnapMirror.
- La page réplication affiche la relation mise à jour.

Réplication inverse des applications

Il s'agit de l'opération planifiée pour déplacer l'application vers le cluster de destination tout en conservant la réplication arrière vers le cluster source d'origine. Astra Control arrête l'application du cluster source et réplique les données vers la destination avant de basculer l'application vers le cluster de destination.

Dans ce cas, vous permutez la source et la destination. Le cluster source d'origine devient le nouveau cluster cible, et le cluster destination d'origine devient le nouveau cluster source.

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **réplication inverse**.
4. Dans la page réplication inverse, vérifiez les informations et sélectionnez **réplication inverse** pour continuer.

Résultat

Les actions suivantes se produisent suite à la réplication inverse :

- Une copie Snapshot est réalisée des ressources Kubernetes de l'application source d'origine.

- Les pods de l'application source d'origine sont « interrompus » en supprimant les ressources Kubernetes de l'application (laissant les demandes de volume persistant et les volumes persistants en place).
- Une fois les pods arrêtés, des snapshots des volumes de l'application sont pris et répliqués.
- Les relations SnapMirror sont rompues, les volumes de destination étant prêts pour la lecture/l'écriture.
- Les ressources Kubernetes de l'application sont restaurées à partir d'un snapshot pré-arrêt, en utilisant les données de volume répliquées après l'arrêt de l'application source d'origine.
- La réplication est rétablie dans la direction inverse.

Rétablir le fonctionnement des applications sur le cluster source d'origine

Avec Astra Control, vous pouvez obtenir un retour après une opération de basculement en utilisant la séquence d'opérations suivante. Dans ce flux de production, pour restaurer la direction de réplication d'origine, Astra Control réplique (resynchronise) toute application redevient le cluster source d'origine avant d'inverser la direction de réplication.

Ce processus commence par une relation qui a terminé un basculement vers une destination et implique les étapes suivantes :

- Commencer par un état de basculement défaillant.
- Resynchroniser la relation.
- Inverser la réplication.

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **Resync**.
4. Pour permettre un basculement en arrière, choisissez l'application défaillante comme source de l'opération de resynchronisation (qui préserve toutes les données écrites après le basculement).
5. Tapez « resynchroniser » pour confirmer.
6. Sélectionnez **Oui, resynchronisation** pour terminer.
7. Une fois la resynchronisation terminée, dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **réplication inverse**.
8. Dans la page réplication inverse, vérifiez les informations et sélectionnez **réplication inverse**.

Résultat

Cette action associe les résultats des opérations de resynchronisation et de « relation inversée » pour que l'application soit en ligne sur le cluster source d'origine et que la réplication reprend au cluster de destination d'origine.

Supprime une relation de réplication d'application

La suppression de la relation se traduit par deux applications distinctes sans relation entre elles.

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection > Replication**.
3. Dans l'onglet protection des données > réplication, dans la zone protection des applications ou dans le

diagramme de relations, sélectionnez **Supprimer la relation de réplication**.

Résultat

Les actions suivantes se produisent suite à la suppression d'une relation de réplication :

- Si la relation est établie mais que l'application n'a pas encore été mise en ligne sur le cluster de destination (échec), Astra Control conserve les demandes de volume persistant créées lors de l'initialisation, laisse une application gérée « vide » sur le cluster de destination et conserve l'application de destination pour conserver les sauvegardes qui pourraient avoir été créées.
- Si l'application a été mise en ligne sur le cluster de destination (avec échec), Astra Control conserve les demandes de volume persistant et les applications de destination. Les applications source et de destination sont désormais traitées comme des applications indépendantes. Les planifications de sauvegarde restent sur les deux applications mais ne sont pas associées les unes aux autres.

État de santé des relations de réplication et état du cycle de vie des relations

Astra Control affiche l'état de santé de la relation et les États du cycle de vie de la relation de réplication.

États d'intégrité des relations de réplication

Les États suivants indiquent l'état de santé de la relation de réplication :

- **Normal** : la relation est établie ou a été établie, et le snapshot le plus récent a été transféré avec succès.
- **Avertissement** : la relation est soit basculée, soit a échoué (et donc ne protège plus l'app source).
- **Critique**
 - La relation est établie ou a échoué et la dernière tentative de réconciliation a échoué.
 - La relation est établie, et la dernière tentative de concilier l'ajout d'un nouveau PVC est un échec.
 - La relation est établie (un snapshot réussi a été répliqué, et le basculement est possible), mais le Snapshot le plus récent a échoué ou a échoué à répliquer.

États du cycle de vie de la réplication

Les États suivants reflètent les différentes étapes du cycle de vie de la réplication :

- **Établissement**: Une nouvelle relation de réplication est en cours de création. Astra Control crée un espace de noms si nécessaire, crée des demandes de volume persistant sur les nouveaux volumes du cluster de destination et crée des relations SnapMirror. Cet état peut également indiquer que la réplication est resynchronisée ou inversée.
- **Créé** : il existe une relation de réplication. Astra Control vérifie régulièrement la disponibilité des ESV, vérifie la relation de réplication, crée régulièrement des instantanés de l'application et identifie les nouveaux ESV source dans l'application. Si c'est le cas, Astra Control crée les ressources qui les incluent dans la réplication.
- **Basculement** : Astra Control rompt les relations SnapMirror et restaure les ressources Kubernetes de l'application à partir du dernier instantané de l'application répliqué avec succès.
- **Failed over**: Astra Control arrête la réplication à partir du cluster source, utilise l'instantané d'application répliqué le plus récent (réussi) sur la destination et restaure les ressources Kubernetes.
- **Resynchronisation** : le contrôle Astra resynchronise les nouvelles données de la source de resynchronisation vers la destination de resynchronisation à l'aide de la resynchronisation SnapMirror. Cette opération peut écraser certaines données de la destination en fonction de la direction de la synchronisation. Astra Control arrête l'application exécutée sur l'espace de noms de destination et

supprime l'application Kubernetes. Pendant le processus de resynchronisation, l'état indique « établissement ».

- **Reversing** : l'opération planifiée pour déplacer l'application vers le cluster de destination tout en continuant à effectuer la réplication vers le cluster source d'origine. Astra Control arrête l'application du cluster source. Il réplique les données vers la destination avant de basculer l'application vers le cluster de destination. Pendant la réplication inverse, l'état indique « établissement ».
- **Suppression** :
 - Si la relation de réplication a été établie mais n'a pas encore été rétablie, Astra Control supprime les demandes de volume persistant qui ont été créées pendant la réplication et supprime l'application gérée de destination.
 - Si la réplication a déjà échoué, Astra Control conserve les ESV et l'application de destination.

Cloner et migrer les applications

Vous pouvez cloner une application existante pour créer une application dupliquée sur le même cluster Kubernetes ou sur un autre cluster. Lorsque vous clonez une application Astra Control, il crée un clone de la configuration des applications et du stockage persistant.

Le clonage peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre. Par exemple, il peut être intéressant de déplacer les workloads dans un pipeline ci/CD et entre les espaces de noms Kubernetes. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou ["API de contrôle Astra"](#) clonage et migration des applications.

Ce dont vous avez besoin

- Pour cloner les applications sur un autre cluster, vous devez vérifier que les instances cloud contenant les clusters source et de destination (le cas échéant) disposent d'un compartiment par défaut. Vous devez attribuer un compartiment par défaut à chaque instance de cloud.
- Lors des opérations de clonage, les applications nécessitant une ressource IngressClass ou des crochets Web ne doivent pas avoir ces ressources déjà définies sur le cluster de destination.

Lors du clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour cela, il faut configurer une policy d'exportation de volume ONTAP afin de permettre ces opérations. Pour ce faire, utilisez les commandes suivantes :



1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limites des clones

- **Classes de stockage explicites** : si vous déployez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Clones et contraintes utilisateur** : tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par étiquette d'espace de noms peut cloner ou restaurer une application dans un nouvel espace de noms sur le même cluster ou sur tout autre cluster du compte de son

organisation. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

- **Les clones utilisent des compartiments par défaut** : lors d'une sauvegarde d'application ou d'une restauration d'application, vous pouvez éventuellement spécifier un ID de compartiment. Cependant, une opération de clonage d'application utilise toujours le compartiment par défaut défini. Il n'existe aucune option pour modifier les compartiments d'un clone. Si vous souhaitez contrôler le godet utilisé, vous pouvez l'un des deux "[modifiez les paramètres par défaut du compartiment](#)" ou faites un "[sauvegarde](#)" suivi d'un "[restaurer](#)" séparément.
- **Avec Jenkins ci** : si vous clonez une instance déployée par l'opérateur de Jenkins ci, vous devez restaurer manuellement les données persistantes. Il s'agit d'une limitation du modèle de déploiement de l'application.
- **Avec les compartiments S3**: Les compartiments S3 dans Astra Control Center n'indiquent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.

Considérations d'OpenShift

- **Clusters et versions OpenShift** : si vous clonez une application entre les clusters, les clusters source et cible doivent être de la même distribution qu'OpenShift. Par exemple, si vous clonez une application depuis un cluster OpenShift 4.7, utilisez un cluster de destination qui est également OpenShift 4.7.
- **Projets et UID** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, le projet (ou l'espace de noms Kubernetes) est affecté à un UID SecurityContext. Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Étapes

1. Sélectionnez **applications**.
2. Effectuez l'une des opérations suivantes :
 - Sélectionnez le menu Options dans la colonne **actions** pour l'application souhaitée.
 - Sélectionnez le nom de l'application souhaitée et sélectionnez la liste déroulante d'état en haut à droite de la page.
3. Sélectionnez **Clone**.
4. Spécifiez les détails du clone :
 - Entrez un nom.
 - Choisissez un cluster de destination pour le clone.
 - Entrez les espaces de noms de destination du clone. Chaque espace de noms source associé à l'application est mappé à l'espace de noms de destination que vous définissez.



Astra Control crée de nouveaux espaces de noms de destination dans le cadre de l'opération de clonage. Les espaces de noms de destination que vous spécifiez ne doivent pas être déjà présents sur le cluster de destination.

- Sélectionnez **Suivant**.
 - Indiquez si vous souhaitez créer le clone à partir d'un snapshot ou d'une sauvegarde existant. Si vous ne sélectionnez pas cette option, Astra Control Center crée le clone à partir de l'état actuel de l'application.
 - Si vous avez choisi de cloner à partir d'un snapshot ou d'une sauvegarde existant, choisissez le snapshot ou la sauvegarde que vous souhaitez utiliser.
5. Sélectionnez **Suivant**.
 6. Vérifiez les informations sur le clone et sélectionnez **Clone**.

Résultat

Astra Control clone l'application en fonction des informations que vous avez fournies. L'opération de clonage a réussi lorsque le nouveau clone d'application est dans `Healthy` Indiquez la page **applications**.

Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.



Après une opération de protection des données (clonage, sauvegarde ou restauration) et après le redimensionnement du volume persistant, la nouvelle taille du volume s'affiche dans l'interface utilisateur avec un délai de vingt minutes. La protection des données fonctionne avec succès en quelques minutes et vous pouvez utiliser le logiciel de gestion pour le système back-end pour confirmer la modification de la taille du volume.

Gérer les crochets d'exécution de l'application

Un crochet d'exécution est une action personnalisée que vous pouvez configurer pour s'exécuter conjointement avec une opération de protection des données d'une application gérée. Par exemple, si vous disposez d'une application de base de données, vous pouvez utiliser des crochets d'exécution pour interrompre toutes les transactions de base de données avant un instantané et reprendre les transactions une fois l'instantané terminé. Les snapshots sont ainsi cohérents au niveau des applications.

Types de crochets d'exécution

Astra Control prend en charge les types de crochets d'exécution suivants, en fonction du moment où ils peuvent être exécutés :

- Pré-instantané
- Post-snapshot
- Avant sauvegarde
- Post-sauvegarde
- Post-restauration

Remarques importantes sur les crochets d'exécution personnalisés

Lors de la planification de crochets d'exécution pour vos applications, tenez compte des points suivants.

- Un crochet d'exécution doit utiliser un script pour effectuer des actions. De nombreux crochets d'exécution peuvent référencer le même script.
 - Astra Control exige que les scripts utilisés par les crochets d'exécution soient écrits au format de scripts shell exécutables.
 - La taille du script est limitée à 96 Ko.
 - Astra Control utilise les paramètres de crochet d'exécution et tout critère de correspondance pour déterminer quels crochets s'appliquent à une opération de snapshot, de sauvegarde ou de restauration.
 - Toutes les défaillances de crochet d'exécution sont des pannes logicielles ; d'autres crochets et l'opération de protection des données sont toujours tentées même en cas de défaillance d'un crochet. Cependant, lorsqu'un crochet échoue, un événement d'avertissement est enregistré dans le journal des événements de la page **activité**.
 - Pour créer, modifier ou supprimer des crochets d'exécution, vous devez être un utilisateur disposant des autorisations propriétaire, administrateur ou membre.
 - Si l'exécution d'un crochet d'exécution prend plus de 25 minutes, le crochet échoue, créant une entrée de journal d'événements avec un code retour « N/A ». Tout instantané affecté expire et sera marqué comme ayant échoué, avec une entrée du journal des événements qui en résulte indiquant le délai d'attente.
 - Pour les opérations de protection de données ad hoc, tous les événements hook sont générés et enregistrés dans le journal des événements de la page **Activity**. Cependant, pour les opérations planifiées de protection des données, seuls les événements de défaillance de type « hook » sont enregistrés dans le journal des événements (les événements générés par les opérations de protection des données planifiées sont toujours enregistrés).
-
- Si vous créez un crochet d'exécution pour une application qui participe à un maillage de service Istio, assurez-vous que le crochet s'exécute contre le conteneur d'application d'origine, et non pas le conteneur de maillage de service. Vous pouvez exclure les conteneurs de maillage de service Istio en appliquant un filtre regex à chaque crochet d'exécution qui s'exécute pour les applications qui utilisent un maillage de service Istio.
 - Puisque les crochets d'exécution réduisent souvent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils sont en cours d'exécution, vous devez toujours essayer de réduire le temps d'exécution de vos crochets d'exécution personnalisés.
 - Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée.

Ordre d'exécution

Lors de l'exécution d'une opération de protection des données, les événements de hook d'exécution ont lieu dans l'ordre suivant :

1. Tous les crochets d'exécution de pré-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets de pré-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets avant que l'opération ne soit ni garantie ni configurable.
2. L'opération de protection des données est effectuée.

3. Tous les crochets d'exécution de post-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets post-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets après l'opération n'est ni garanti ni configurable.

Si vous créez plusieurs crochets d'exécution du même type (par exemple, pré-instantané), l'ordre d'exécution de ces crochets n'est pas garanti. Cependant, l'ordre d'exécution des crochets de différents types est garanti. Par exemple, l'ordre d'exécution d'une configuration comportant les cinq types différents de crochets se présente comme suit :

1. Crochets de pré-secours exécutés
2. Crochets pré-instantanés exécutés
3. Crochets post-snapshot exécutés
4. Crochets post-secours exécutés
5. Crochets post-restauration exécutés

Vous pouvez voir un exemple de cette configuration dans le scénario numéro 2 dans le tableau de la [Déterminez si un crochet va courir](#).



Vous devez toujours tester vos scripts d'exécution avant de les activer dans un environnement de production. Vous pouvez utiliser la commande 'kubectl exec' pour tester aisément les scripts. Une fois que vous avez activé les crochets d'exécution dans un environnement de production, testez les snapshots et les sauvegardes obtenus pour vous assurer qu'ils sont cohérents. Pour ce faire, vous pouvez cloner l'application dans un espace de noms temporaire, restaurer le snapshot ou la sauvegarde, puis tester l'application.

Déterminez si un crochet va courir

Utilisez le tableau suivant pour déterminer si un crochet d'exécution personnalisé sera exécuté pour votre application.

Notez que toutes les opérations générales liées aux applications consistent à exécuter l'une des opérations de base de la copie Snapshot, de la sauvegarde ou de la restauration. Selon le scénario, une opération de clonage peut se composer de différentes combinaisons de ces opérations, de sorte que les crochets d'exécution d'une opération de clonage varient.

Les opérations de restauration sur place requièrent un snapshot ou une sauvegarde existante. Elles n'exécutent donc pas de snapshot ni de crochets de sauvegarde.



Si vous démarrez mais annulez ensuite une sauvegarde qui inclut un instantané et qu'il y a des crochets d'exécution associés, certains crochets peuvent s'exécuter, et d'autres peuvent ne pas. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée. Gardez à l'esprit les points suivants pour les sauvegardes annulées avec les crochets d'exécution associés :

- Les crochets de pré-secours et post-secours sont toujours exécutés.
- Si la sauvegarde inclut un nouvel instantané et que l'instantané a démarré, les crochets pré-instantané et post-instantané sont exécutés.
- Si la sauvegarde est annulée avant le démarrage de l'instantané, les crochets pré-instantané et post-instantané ne sont pas exécutés.

Scénario	Fonctionnement	Snapshot existant	Sauvegarder de existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets
1	Clonage	N	N	Nouveau	Identique	Y	N	Y
2	Clonage	N	N	Nouveau	Différente	Y	Y	Y
3	Cloner ou restaurer	Y	N	Nouveau	Identique	N	N	Y
4	Cloner ou restaurer	N	Y	Nouveau	Identique	N	N	Y
5	Cloner ou restaurer	Y	N	Nouveau	Différente	N	Y	Y
6	Cloner ou restaurer	N	Y	Nouveau	Différente	N	N	Y
7	Restaurer	Y	N	Existant	Identique	N	N	Y
8	Restaurer	N	Y	Existant	Identique	N	N	Y
9	Snapshot	S/O	S/O	S/O	S/O	Y	S/O	S/O
10	Sauvegarde	N	S/O	S/O	S/O	Y	Y	S/O
11	Sauvegarde	Y	S/O	S/O	S/O	N	Y	S/O

Exemples de crochet d'exécution

Consultez le "[Projet GitHub NetApp Verda](#)" pour voir des exemples et obtenir une idée de la façon de structurer vos crochets d'exécution. Vous pouvez utiliser ces exemples comme modèles ou scripts de test.

Afficher les crochets d'exécution existants

Vous pouvez afficher les crochets d'exécution personnalisés existants pour une application.

Étapes

1. Accédez à **applications**, puis sélectionnez le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.

Vous pouvez afficher tous les crochets d'exécution activés ou désactivés dans la liste résultante. Vous pouvez voir l'état d'un crochet, sa source et le moment où il est exécuté (pré ou post-opération). Pour afficher les journaux d'événements entourant les crochets d'exécution, accédez à la page **activité** dans la zone de navigation de gauche.

Afficher les scripts existants

Vous pouvez afficher les scripts chargés existants. Vous pouvez également voir quels scripts sont en cours d'utilisation, et quels crochets les utilisent, sur cette page.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **scripts**.

Cette page affiche la liste des scripts chargés existants. La colonne **utilisé par** indique les crochets d'exécution qui utilisent chaque script.

Ajouter un script

Vous pouvez ajouter un ou plusieurs scripts que les crochets d'exécution peuvent référencer. De nombreux crochets d'exécution peuvent référencer le même script ; cela vous permet de mettre à jour de nombreux crochets d'exécution en ne changeant qu'un seul script.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **scripts**.
3. Sélectionnez **Ajouter**.
4. Effectuez l'une des opérations suivantes :
 - Charger un script personnalisé.
 - i. Sélectionnez l'option **Télécharger le fichier**.
 - ii. Accédez à un fichier et téléchargez-le.
 - iii. Donnez un nom unique au script.
 - iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
 - v. Sélectionnez **Enregistrer le script**.
 - Coller dans un script personnalisé à partir du presse-papiers.
 - i. Sélectionnez l'option **Coller ou type**.
 - ii. Sélectionnez le champ de texte et collez le texte du script dans le champ.
 - iii. Donnez un nom unique au script.
 - iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
5. Sélectionnez **Enregistrer le script**.

Résultat

Le nouveau script apparaît dans la liste de l'onglet **scripts**.

Supprimer un script

Vous pouvez supprimer un script du système s'il n'est plus nécessaire et s'il n'est pas utilisé par les crochets d'exécution.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **scripts**.

3. Choisissez un script à supprimer et sélectionnez le menu dans la colonne **actions**.
4. Sélectionnez **Supprimer**.



Si le script est associé à un ou plusieurs crochets d'exécution, l'action **Delete** n'est pas disponible. Pour supprimer le script, modifiez d'abord les crochets d'exécution associés et associez-les à un autre script.

Créer un crochet d'exécution personnalisé

Vous pouvez créer un crochet d'exécution personnalisé pour une application. Voir [Exemples de crochet d'exécution](#) pour des exemples de crochet. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour créer des crochets d'exécution.



Lorsque vous créez un script de shell personnalisé à utiliser comme crochet d'exécution, n'oubliez pas de spécifier le shell approprié au début du fichier, sauf si vous exécutez des commandes spécifiques ou fournissez le chemin complet à un exécutable.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez **Ajouter**.
4. Dans la zone **Détails du crochet**, déterminez quand le crochet doit fonctionner en sélectionnant un type d'opération dans le menu déroulant **opération**.
5. Saisissez un nom unique pour le crochet.
6. (Facultatif) saisissez les arguments à transmettre au crochet pendant l'exécution, en appuyant sur la touche entrée après chaque argument que vous entrez pour enregistrer chacun.
7. Dans la zone **Images conteneur**, si le crochet doit être exécuté sur toutes les images de conteneur contenues dans l'application, activez la case à cocher **appliquer à toutes les images de conteneur**. Si, à la place, le crochet ne doit agir que sur une ou plusieurs images de conteneur spécifiées, entrez les noms d'image de conteneur dans le champ **noms d'image de conteneur à associer**.
8. Dans la zone **script**, effectuez l'une des opérations suivantes :
 - Ajouter un nouveau script.
 - i. Sélectionnez **Ajouter**.
 - ii. Effectuez l'une des opérations suivantes :
 - Charger un script personnalisé.
 - I. Sélectionnez l'option **Télécharger le fichier**.
 - II. Accédez à un fichier et téléchargez-le.
 - III. Donnez un nom unique au script.
 - IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
 - V. Sélectionnez **Enregistrer le script**.
 - Coller dans un script personnalisé à partir du presse-papiers.
 - I. Sélectionnez l'option **Coller ou type**.

- II. Sélectionnez le champ de texte et collez le texte du script dans le champ.
- III. Donnez un nom unique au script.
- IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
 - Sélectionnez un script existant dans la liste.

Cela indique au crochet d'exécution d'utiliser ce script.

9. Sélectionnez **Ajouter crochet**.

Vérifier l'état d'un crochet d'exécution

Une fois qu'une opération de snapshot, de sauvegarde ou de restauration a terminé, vous pouvez vérifier l'état des crochets d'exécution qui ont été exécutés dans le cadre de l'opération. Vous pouvez utiliser ces informations d'état pour déterminer si vous souhaitez maintenir le crochet d'exécution, le modifier ou le supprimer.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **protection des données**.
3. Sélectionnez **snapshots** pour voir exécution de snapshots ou **sauvegardes** pour voir exécution de sauvegardes.

L'état **Hook** indique l'état de la séquence de crochet d'exécution une fois l'opération terminée. Vous pouvez passer le curseur de la souris sur l'état pour plus de détails. Par exemple, si des échecs de crochet d'exécution se produisent au cours d'un snapshot, le fait de passer le curseur sur l'état de crochet pour ce snapshot donne une liste des crochets d'exécution ayant échoué. Pour voir les raisons de chaque échec, vous pouvez consulter la page **activité** dans la zone de navigation de gauche.

Afficher l'utilisation du script

Vous pouvez voir quels crochets d'exécution utilisent un script particulier dans l'interface utilisateur Web Astra Control.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **scripts**.

La colonne **utilisé par** de la liste des scripts contient des détails sur les crochets qui utilisent chaque script de la liste.

3. Sélectionnez les informations de la colonne **utilisé par** pour un script qui vous intéresse.

Une liste plus détaillée s'affiche, avec les noms des crochets qui utilisent le script et le type d'opération avec lesquels ils sont configurés pour s'exécuter.

Désactivez un crochet d'exécution

Vous pouvez désactiver un crochet d'exécution si vous souhaitez l'empêcher temporairement de s'exécuter avant ou après un instantané d'une application. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour désactiver les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez désactiver.
4. Sélectionnez **Désactiver**.

Supprimer un crochet d'exécution

Vous pouvez supprimer entièrement un crochet d'exécution si vous n'en avez plus besoin. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour supprimer les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.

Pour en savoir plus

- ["Projet GitHub NetApp Verda"](#)

Surveillez l'état des applications et des clusters

Affichez un récapitulatif de l'état des applications et du cluster

Sélectionnez **Dashboard** pour afficher une vue de haut niveau de vos applications, clusters, systèmes back-end de stockage et leur état de santé.

Il ne s'agit pas seulement de numéros statiques ou d'États, mais vous pouvez explorer les données à partir de chacun d'entre eux. Par exemple, si les applications ne sont pas totalement protégées, vous pouvez passer le curseur de la souris sur l'icône pour identifier les applications qui ne sont pas totalement protégées, ce qui explique pourquoi.

Mosaïque applications

La mosaïque **applications** vous aide à identifier les éléments suivants :

- Combien d'applications gérez-vous actuellement avec Astra ?
- Si ces applications gérées sont en bon état.
- Que les applications soient entièrement protégées (elles sont protégées si des sauvegardes récentes sont disponibles).
- Le nombre d'applications découvertes, mais non gérées.

Dans l'idéal, ce nombre est égal à zéro, car vous pouvez gérer ou ignorer les applications après leur découverte. Vous devez ensuite surveiller le nombre d'applications découvertes dans le tableau de bord pour déterminer quand les développeurs ajoutent de nouvelles applications à un cluster.

Mosaïque de groupes

La mosaïque **clusters** fournit des détails similaires sur l'état de santé des clusters que vous gérez en utilisant Astra Control Center, et vous pouvez explorer vers le bas pour obtenir plus de détails comme vous pouvez avec une application.

Mosaïque des systèmes back-end de stockage

La mosaïque **Storage backend** fournit des informations pour vous aider à identifier la santé des systèmes back-end :

- Nombre de systèmes back-end gérés
- Que ces systèmes back-end gérés soient en bon état
- Que les systèmes back-end soient entièrement protégés
- Le nombre de systèmes back-end découverts et ne sont pas encore gérés.

Afficher l'état de santé des clusters et gérer les classes de stockage

Une fois que vous avez ajouté des clusters à gérer par Astra Control Center, vous pouvez afficher des informations détaillées sur le cluster, notamment son emplacement, les nœuds de travail, les volumes persistants et les classes de stockage. Vous pouvez également modifier la classe de stockage par défaut des clusters gérés.

Afficher les détails et l'état de santé des clusters

Vous pouvez afficher des informations détaillées sur le cluster, telles que son emplacement, les nœuds de travail, les volumes persistants et les classes de stockage.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster dont vous souhaitez afficher les détails.



Si un cluster se trouve dans le `removed` État et pourtant, la connectivité cluster et réseau semble saine (les tentatives externes d'accès au cluster via les API Kubernetes sont réussies). Le kubeconfig que vous avez fourni au contrôle Astra pourrait ne plus être valide. Cela peut être dû à une rotation ou à une expiration du certificat sur le cluster. Pour corriger ce problème, mettez à jour les informations d'identification associées au cluster dans Astra Control à l'aide du "[API de contrôle Astra](#)".

3. Consultez les informations sur les onglets **Présentation**, **stockage** et **activité** pour trouver les informations que vous recherchez.
 - **Présentation** : détails sur les nœuds de travail, y compris leur état.
 - **Stockage** : volumes persistants associés au calcul, y compris la classe et l'état du stockage.
 - **Activité** : affiche les activités liées au cluster.



Vous pouvez également afficher les informations du groupe d'instruments à partir du Centre de contrôle Astra **Tableau de bord**. Dans l'onglet **clusters** sous **Résumé des ressources**, vous pouvez sélectionner les clusters gérés, qui vous permettent d'accéder à la page **clusters**. Après avoir accédé à la page **clusters**, suivez les étapes décrites ci-dessus.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster. Lorsque Astra Control gère un cluster, il conserve le suivi de la classe de stockage par défaut du cluster.



Ne modifiez pas la classe de stockage à l'aide des commandes kubectl. Utilisez plutôt cette procédure. Astra Control va rétablir les modifications si elles ont été effectuées à l'aide de kubectl.

Étapes

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

Afficher l'état de santé et les détails d'une application

Une fois que vous avez commencé à gérer une application, Astra Control fournit des informations détaillées sur l'application qui vous permet d'identifier son état (qu'il s'agisse d'une application en bon état), son état de protection (qu'il soit entièrement protégé en cas de défaillance), les pods, le stockage persistant, et bien plus encore.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **applications**, puis le nom d'une application.
2. Vérifiez les informations.
 - **App Status** : fournit un état qui reflète l'état de l'application dans Kubernetes. Par exemple, les pods et les volumes persistants sont-ils en ligne ? Si une application est défectueuse, vous devez chercher à résoudre le problème sur le cluster en consultant les journaux Kubernetes. Astra ne fournit pas d'informations pour vous aider à réparer une application défaillante.
 - **App protection Status** : indique l'état de protection de l'application :
 - **Entièrement protégé** : l'application dispose d'un programme de sauvegarde actif et d'une sauvegarde réussie qui a moins d'une semaine
 - **Partiellement protégé** : l'application dispose d'un programme de sauvegarde actif, d'un programme de snapshots actif ou d'une sauvegarde ou d'un snapshot réussi
 - **Non protégé** : Les applications qui ne sont ni totalement protégées ni partiellement protégées.

Vous ne pouvez pas être entièrement protégé tant que vous n'avez pas une sauvegarde récente. Ceci est important, car les sauvegardes sont stockées dans un magasin d'objets à distance des volumes persistants. En cas de défaillance ou d'accident, le cluster doit être doté d'un stockage persistant, alors vous devez effectuer une sauvegarde pour effectuer une restauration. Un snapshot ne vous permettrait pas de restaurer votre système.

- **Présentation** : informations sur l'état des modules associés à l'application.
- **Protection des données** : permet de configurer une stratégie de protection des données et d'afficher

les snapshots et sauvegardes existants.

- **Storage** : affiche les volumes persistants au niveau de l'application. L'état d'un volume persistant est du point de vue du cluster Kubernetes.
- **Ressources** : vous permet de vérifier quelles ressources sont sauvegardées et gérées.
- **Activité** : affiche les activités associées à l'application.



Vous pouvez également afficher les informations de l'application à partir du Centre de contrôle Astra **Tableau de bord**. Dans l'onglet **applications** sous **Résumé des ressources**, vous pouvez sélectionner les applications gérées, qui vous permettent d'accéder à la page **applications**. Après avoir accédé à la page **applications**, suivez les étapes décrites ci-dessus.

Gérez votre compte

Gérez les utilisateurs et les rôles locaux

Vous pouvez ajouter, supprimer et modifier les utilisateurs de votre installation Astra Control Center à l'aide de l'interface utilisateur Astra Control. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "[API de contrôle Astra](#)" pour gérer les utilisateurs.

Vous pouvez également utiliser LDAP pour effectuer l'authentification pour certains utilisateurs.

Utiliser LDAP

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control. À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP. Pour plus d'informations, reportez-vous à la documentation suivante :

- "[Utilisez l'API de contrôle Astra pour gérer l'authentification à distance et les utilisateurs](#)"
- "[Utilisez l'interface utilisateur Astra Control pour gérer les utilisateurs et les groupes distants](#)"
- "[Utilisez l'interface utilisateur Astra Control pour gérer l'authentification à distance](#)"

Ajouter des utilisateurs

Les propriétaires et administrateurs de comptes peuvent ajouter d'autres utilisateurs à l'installation d'Astra Control Center.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Sélectionnez **Ajouter utilisateur**.
4. Entrez le nom de l'utilisateur, son adresse e-mail et son mot de passe temporaire.

L'utilisateur doit modifier le mot de passe lors de sa première connexion.

5. Sélectionnez un rôle d'utilisateur avec les autorisations système appropriées.

Chaque rôle offre les autorisations suivantes :

- Un **Viewer** peut afficher les ressources.
- Un **membre** dispose des autorisations de rôle Viewer et peut gérer les applications et les clusters, annuler la gestion des applications et supprimer des instantanés et des sauvegardes.
- Un **Admin** dispose des autorisations de rôle de membre et peut ajouter et supprimer d'autres utilisateurs, à l'exception du propriétaire.
- Un **propriétaire** possède des autorisations de rôle d'administrateur et peut ajouter et supprimer des comptes d'utilisateur.

6. Pour ajouter des contraintes à un utilisateur avec un rôle membre ou visualiseur, activez la case à cocher **restreindre le rôle aux contraintes**.

Pour plus d'informations sur l'ajout de contraintes, voir "[Gérez les utilisateurs et les rôles locaux](#)".

7. Sélectionnez **Ajouter**.

Gérer les mots de passe

Vous pouvez gérer les mots de passe des comptes utilisateur dans Astra Control Center.

Changer votre mot de passe

Vous pouvez modifier le mot de passe de votre compte utilisateur à tout moment.

Étapes

1. Sélectionnez l'icône utilisateur en haut à droite de l'écran.
2. Sélectionnez **Profile**.
3. Dans le menu Options de la colonne **actions**, sélectionnez **changer mot de passe**.
4. Saisissez un mot de passe conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.
6. Sélectionnez **changer mot de passe**.

Réinitialiser le mot de passe d'un autre utilisateur

Si votre compte dispose des autorisations de rôle Administrateur ou propriétaire, vous pouvez réinitialiser les mots de passe des autres comptes utilisateur ainsi que les vôtres. Lorsque vous réinitialisez un mot de passe, vous attribuez un mot de passe temporaire que l'utilisateur devra modifier lors de la connexion.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez la liste déroulante **actions**.
3. Sélectionnez **Réinitialiser le mot de passe**.
4. Saisissez un mot de passe temporaire conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.



Lors de la prochaine connexion de l'utilisateur, l'utilisateur est invité à modifier le mot de passe.

6. Sélectionnez **Réinitialiser le mot de passe**.

Supprimer des utilisateurs

Les utilisateurs disposant du rôle propriétaire ou administrateur peuvent à tout moment supprimer d'autres utilisateurs du compte.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Dans l'onglet **Users**, cochez la case de la ligne de chaque utilisateur que vous souhaitez supprimer.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Supprimer utilisateur/s**.
4. Lorsque vous y êtes invité, confirmez la suppression en saisissant le mot "supprimer", puis sélectionnez **Oui, Supprimer l'utilisateur**.

Résultat

Astra Control Center supprime l'utilisateur du compte.

Gérez les rôles

Vous pouvez gérer les rôles en ajoutant des contraintes d'espace de noms et en restreignant les rôles des utilisateurs à ces contraintes. Cela vous permet de contrôler l'accès aux ressources de votre organisation. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "[API de contrôle Astra](#)" pour gérer les rôles.

Ajoutez une contrainte d'espace de noms à un rôle

Un administrateur ou un propriétaire peut ajouter des contraintes d'espace de noms aux rôles de membre ou de visualiseur.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur.
4. Sélectionnez **Modifier le rôle**.
5. Activez la case à cocher **restreindre le rôle aux contraintes**.

La case à cocher n'est disponible que pour les rôles de membre ou de visualiseur. Vous pouvez sélectionner un autre rôle dans la liste déroulante **role**.

6. Sélectionnez **Ajouter une contrainte**.

Vous pouvez afficher la liste des contraintes disponibles par espace de noms ou par étiquette d'espace de noms.

7. Dans la liste déroulante **Type de contrainte**, sélectionnez **espace de noms Kubernetes** ou **étiquette d'espace de noms Kubernetes** selon la configuration de vos espaces de noms.
8. Sélectionnez un ou plusieurs espaces de noms ou étiquettes dans la liste pour composer une contrainte

qui restreint les rôles à ces espaces de noms.

9. Sélectionnez **confirmer**.

La page **Modifier rôle** affiche la liste des contraintes que vous avez choisies pour ce rôle.

10. Sélectionnez **confirmer**.

Sur la page **compte**, vous pouvez afficher les contraintes pour n'importe quel rôle de membre ou de visualiseur dans la colonne **rôle**.



Si vous activez des contraintes pour un rôle et que vous sélectionnez **confirmer** sans ajouter de contraintes, le rôle est considéré comme étant soumis à des restrictions complètes (le rôle est refusé l'accès aux ressources affectées aux espaces de noms).

Supprime une contrainte d'espace de noms d'un rôle

Un utilisateur Admin ou propriétaire peut supprimer une contrainte d'espace de noms d'un rôle.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur ayant des contraintes actives.
4. Sélectionnez **Modifier le rôle**.

La boîte de dialogue **Modifier le rôle** affiche les contraintes actives du rôle.

5. Sélectionnez **X** à droite de la contrainte à supprimer.
6. Sélectionnez **confirmer**.

Pour en savoir plus

- ["Rôles et espaces de noms d'utilisateur"](#)

Gérer l'authentification à distance

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control.

À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP.



Astra Control Center utilise l'adresse e-mail de l'attribut LDAP "mail" pour rechercher et garder le suivi des utilisateurs distants. Cet attribut peut être un champ facultatif ou vide dans votre répertoire. Une adresse électronique doit exister dans ce champ pour tous les utilisateurs distants que vous souhaitez afficher dans Astra Control Center. Cette adresse e-mail est utilisée comme nom d'utilisateur dans Astra Control Center pour l'authentification.

Ajoutez un certificat pour l'authentification LDAPS

Ajoutez le certificat TLS privé pour le serveur LDAP afin que Astra Control Center puisse s'authentifier auprès du serveur LDAP lorsque vous utilisez une connexion LDAPS. Vous ne devez le faire qu'une seule fois, ou lorsque le certificat que vous avez installé expire.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **certificats**.
3. Sélectionnez **Ajouter**.
4. Téléchargez le `.pem` importez ou collez le contenu du fichier à partir du presse-papiers.
5. Cochez la case **approuvé**.
6. Sélectionnez **Ajouter un certificat**.

Activez l'authentification à distance

Vous pouvez activer l'authentification LDAP et configurer la connexion entre Astra Control et le serveur LDAP distant.

Ce dont vous avez besoin

Si vous prévoyez d'utiliser LDAPS, assurez-vous que le certificat TLS privé pour le serveur LDAP est installé dans Astra Control Center afin que le centre de contrôle Astra puisse s'authentifier auprès du serveur LDAP. Voir [Ajoutez un certificat pour l'authentification LDAPS](#) pour obtenir des instructions.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **connexion**.
4. Entrez l'adresse IP du serveur, le port et le protocole de connexion préféré (LDAP ou LDAPS).



Il est recommandé d'utiliser LDAPS lors de la connexion au serveur LDAP. Vous devez installer le certificat TLS privé du serveur LDAP dans Astra Control Center avant de vous connecter avec LDAPS.

5. Saisissez les informations d'identification du compte de service au format e-mail (`administrator@example.com`). Astra Control utilisera ces informations d'identification lors de la connexion au serveur LDAP.
6. Dans la section **User Match**, entrez le nom unique de base et un filtre de recherche d'utilisateur approprié à utiliser lors de la récupération des informations utilisateur à partir du serveur LDAP.
7. Dans la section **correspondance de groupe**, entrez le nom unique de base de recherche de groupe et un filtre de recherche de groupe personnalisé approprié.



Veillez à utiliser le nom unique de base (DN) correct et un filtre de recherche approprié pour **User Match** et **Group Match**. Le DN de base indique à Astra Control à quel niveau de l'arborescence de répertoire démarrer la recherche, et le filtre de recherche limite les parties de l'arborescence de répertoires Astra Control à partir de.

8. Sélectionnez **soumettre**.

Résultat

L'état du volet **authentification à distance** passe à **en attente**, puis à **connecté** lorsque la connexion au serveur LDAP est établie.

Désactiver l'authentification à distance

Vous pouvez désactiver temporairement une connexion active au serveur LDAP.



Lorsque vous désactivez une connexion à un serveur LDAP, tous les paramètres sont enregistrés et tous les utilisateurs et groupes distants ajoutés à Astra Control à partir de ce serveur LDAP sont conservés. Vous pouvez vous reconnecter à ce serveur LDAP à tout moment.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Désactiver**.

Résultat

L'état du volet **authentification à distance** passe à **Désactivé**. Tous les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont conservés et vous pouvez réactiver la connexion à tout moment.

Modifier les paramètres d'authentification à distance

Si vous avez désactivé la connexion au serveur LDAP ou si le volet **authentification à distance** est à l'état "erreur de connexion", vous pouvez modifier les paramètres de configuration.



Vous ne pouvez pas modifier l'adresse IP ou l'URL du serveur LDAP lorsque le volet **authentification distante** est à l'état "Désactivé". Vous devez le faire [Déconnectez l'authentification à distance](#) tout d'abord.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Modifier**.
4. Apportez les modifications nécessaires et sélectionnez **Modifier**.

Déconnectez l'authentification à distance

Vous pouvez vous déconnecter d'un serveur LDAP et supprimer les paramètres de configuration d'Astra Control.



Lorsque vous vous déconnectez du serveur LDAP, tous les paramètres de configuration de ce serveur LDAP sont supprimés d'Astra Control, ainsi que tous les utilisateurs et groupes distants ajoutés à partir de ce serveur LDAP.

Étapes

1. Accédez à **compte > connexions**.

2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **déconnecter**.

Résultat

L'état du volet **authentification à distance** passe à **déconnecté**. Les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont supprimés d'Astra Control.

Gérez des utilisateurs et des groupes distants

Si vous avez activé l'authentification LDAP sur votre système Astra Control, vous pouvez rechercher des utilisateurs et des groupes LDAP et les inclure dans les utilisateurs approuvés du système.

Ajouter un utilisateur distant

Les propriétaires et administrateurs de comptes peuvent ajouter des utilisateurs distants à Astra Control.



Vous ne pouvez pas ajouter un utilisateur distant si un utilisateur local avec la même adresse e-mail existe déjà sur le système. Pour ajouter l'utilisateur en tant qu'utilisateur distant, supprimez d'abord l'utilisateur local du système.



Astra Control Center utilise l'adresse e-mail de l'attribut LDAP "mail" pour rechercher et garder le suivi des utilisateurs distants. Cet attribut peut être un champ facultatif ou vide dans votre répertoire. Une adresse électronique doit exister dans ce champ pour tous les utilisateurs distants que vous souhaitez afficher dans Astra Control Center. Cette adresse e-mail est utilisée comme nom d'utilisateur dans Astra Control Center pour l'authentification.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **utilisateurs distants**.
4. Sélectionnez **Ajouter**.
5. Vous pouvez également rechercher un utilisateur LDAP en saisissant l'adresse e-mail de l'utilisateur dans le champ **Filter by email**.
6. Sélectionnez un ou plusieurs utilisateurs dans la liste.
7. Attribuez un rôle à l'utilisateur.



Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à cet utilisateur et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.



Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouvel utilisateur apparaît dans la liste des utilisateurs distants. Dans cette liste, vous pouvez voir les contraintes actives sur l'utilisateur et gérer l'utilisateur à partir du menu **actions**.

Ajouter un groupe distant

Pour ajouter plusieurs utilisateurs distants à la fois, les propriétaires et administrateurs de comptes peuvent ajouter des groupes distants à Astra Control. Lorsque vous ajoutez un groupe distant, tous les utilisateurs distants de ce groupe sont ajoutés à Astra Control et héritent du même rôle.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **Remote Groups**.
4. Sélectionnez **Ajouter**.

Dans cette fenêtre, vous pouvez voir une liste des noms communs et des noms distinctifs des groupes LDAP récupérés par Astra Control à partir du répertoire.

5. Vous pouvez également rechercher un groupe LDAP en saisissant le nom commun du groupe dans le champ **Filter by common name**.
6. Sélectionnez un ou plusieurs groupes dans la liste.
7. Attribuez un rôle aux groupes.



Le rôle que vous sélectionnez est attribué à tous les utilisateurs de ce groupe. Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle le plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à ce groupe et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.



Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouveau groupe apparaît dans la liste des groupes distants et tous les utilisateurs distants de ce groupe

apparaissent dans la liste des utilisateurs distants. Dans cette liste, vous pouvez afficher les détails du groupe et gérer le groupe à partir du menu **actions**.

Afficher et gérer les notifications

Astra vous avertit lorsque les actions sont terminées ou en échec. Par exemple, vous verrez une notification si une sauvegarde d'une application a réussi.

Vous pouvez gérer ces notifications en haut à droite de l'interface :



Étapes

1. Sélectionnez le nombre de notifications non lues en haut à droite.
2. Examinez les notifications, puis sélectionnez **Marquer comme lu** ou **Afficher toutes les notifications**.

Si vous avez sélectionné **Afficher toutes les notifications**, la page Notifications se charge.

3. Sur la page **Notifications**, affichez les notifications, sélectionnez celles que vous souhaitez marquer comme lu, sélectionnez **action** et **Marquer comme lu**.

Ajouter et supprimer des informations d'identification

Ajoutez et supprimez des identifiants pour les fournisseurs de cloud privé local, comme ONTAP S3, les clusters Kubernetes gérés avec OpenShift ou les clusters Kubernetes non gérés depuis votre compte à tout moment. Astra Control Center utilise ces identifiants pour détecter les clusters Kubernetes et les applications sur les clusters et provisionner les ressources en votre nom.

Notez que tous les utilisateurs d'Astra Control Center partagent les mêmes informations d'identification.

Ajouter des informations d'identification

Vous pouvez ajouter des informations d'identification à Astra Control Center lorsque vous gérez des clusters. Pour ajouter des informations d'identification en ajoutant un nouveau cluster, reportez-vous à la section "[Ajouter un cluster Kubernetes](#)".



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.

Supprimer les informations d'identification

Supprimez les informations d'identification d'un compte à tout moment. Vous ne devez supprimer les informations d'identification qu'après "[annuler la gestion de tous les clusters associés](#)".



Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control Center est toujours utilisé car Astra Control Center utilise les informations d'identification pour s'authentifier auprès du compartiment de secours. Il est préférable de ne pas supprimer ces informations d'identification.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **informations d'identification**.
3. Sélectionnez le menu Options dans la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer les informations d'identification**.

Résultat

Astra Control Center supprime les informations d'identification du compte.

Surveillez l'activité des comptes

Vous pouvez consulter les détails des activités de votre compte Astra Control. Par exemple, lorsque de nouveaux utilisateurs ont été invités, lorsqu'un cluster a été ajouté ou lorsqu'un snapshot a été créé. Vous pouvez également exporter votre activité de compte vers un fichier CSV.



Si vous gérez des clusters Kubernetes à partir d'Astra Control et qu'Astra Control est connecté à Cloud Insights, Astra Control envoie des journaux d'événements à Cloud Insights. Les informations du journal, y compris les informations sur le déploiement du pod et les pièces jointes en PVC, apparaissent dans le journal des activités de contrôle Astra. Utilisez ces informations pour identifier les problèmes éventuels sur les clusters Kubernetes que vous gérez.

Afficher toutes les activités du compte dans Astra Control

1. Sélectionnez **activité**.
2. Utilisez les filtres pour réduire la liste des activités ou utilisez la zone de recherche pour trouver exactement ce que vous recherchez.
3. Sélectionnez **Exporter au format CSV** pour télécharger l'activité de votre compte dans un fichier CSV.

Afficher l'activité d'un compte pour une application spécifique

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **activité**.

Afficher l'activité des comptes pour les clusters

1. Sélectionnez **clusters**, puis le nom du cluster.
2. Sélectionnez **activité**.

Prenez des mesures pour résoudre les événements qui nécessitent votre attention

1. Sélectionnez **activité**.

2. Sélectionnez un événement qui nécessite une attention particulière.
3. Sélectionnez l'option de liste déroulante **prendre une action**.

Dans cette liste, vous pouvez consulter les actions correctives possibles, consulter la documentation associée au problème et obtenir de l'aide pour résoudre ce dernier.

Mettre à jour une licence existante

Vous pouvez convertir une licence d'évaluation en licence complète, ou mettre à jour une évaluation existante ou une licence complète avec une nouvelle licence. Si vous ne disposez pas d'une licence complète, contactez votre contact commercial NetApp pour obtenir une licence complète et un numéro de série. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou "[API de contrôle Astra](#)" pour mettre à jour une licence existante.

Étapes

1. Connectez-vous au "[Site de support NetApp](#)".
2. Accédez à la page de téléchargement d'Astra Control Center, entrez le numéro de série et téléchargez le fichier de licence NetApp complet (NLF).
3. Connectez-vous à l'interface utilisateur du centre de contrôle Astra.
4. Dans le menu de navigation de gauche, sélectionnez **compte > Licence**.
5. Dans la page **compte > Licence**, sélectionnez le menu déroulant d'état de la licence existante et sélectionnez **remplacer**.
6. Accédez au fichier de licence que vous avez téléchargé.
7. Sélectionnez **Ajouter**.

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

Pour en savoir plus

- "[Licence Astra Control Center](#)"

Gestion des compartiments

Un fournisseur de compartiments de stockage est essentiel pour la sauvegarde de vos applications et du stockage persistant, ou pour le clonage d'applications entre les clusters. Avec Astra Control Center, ajoutez un fournisseur de magasin d'objets comme destination de sauvegarde externe pour vos applications.

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

Utilisez l'un des fournisseurs de compartiments Amazon simple Storage Service (S3) suivants :

- NetApp ONTAP S3
- NetApp StorageGRID S3

- Microsoft Azure
- S3 générique



Amazon Web Services (AWS) et Google Cloud Platform (GCP) utilisent le type de compartiment S3 générique.



Bien qu'Astra Control Center prenne en charge Amazon S3 en tant que fournisseur de compartiments 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.

Un godet peut être dans l'un des États suivants :

- En attente : le compartiment est planifié pour la découverte.
- Disponible : le godet est disponible.
- Retiré : le godet n'est pas accessible actuellement.

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

Vous pouvez effectuer les tâches suivantes liées à la gestion des compartiments :

- ["Ajouter un godet"](#)
- [Modifier un godet](#)
- [Définir le compartiment par défaut](#)
- [Faire pivoter ou supprimer les identifiants de compartiment](#)
- [Déposer un godet](#)



Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.

Modifier un godet

Vous pouvez modifier les informations d'identification d'accès pour un compartiment et modifier si un compartiment sélectionné est le compartiment par défaut.



Lorsque vous ajoutez un compartiment, sélectionnez le fournisseur approprié et fournissez les identifiants appropriés pour ce fournisseur. Par exemple, l'interface utilisateur accepte NetApp ONTAP S3 comme type et accepte les identifiants StorageGRID. Toutefois, toutes les futures sauvegardes et restaurations des applications à l'aide de ce compartiment échoueront. Voir la ["Notes de version"](#).

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu de la colonne **actions**, sélectionnez **Modifier**.
3. Modifier toute information autre que le type de godet.



Vous ne pouvez pas modifier le type de compartiment.

4. Sélectionnez **mettre à jour**.

Définir le compartiment par défaut

Lorsque vous effectuez un clone entre les clusters, Astra Control requiert un compartiment par défaut. La procédure suivante permet de définir un compartiment par défaut pour l'ensemble des clusters.

Étapes

1. Accédez à **Cloud instances**.
2. Sélectionnez le menu dans la colonne **actions** pour l'instance de Cloud dans la liste.
3. Sélectionnez **Modifier**.
4. Dans la liste **godet**, sélectionnez le compartiment par défaut.
5. Sélectionnez **Enregistrer**.

Faire pivoter ou supprimer les identifiants de compartiment

Astra Control utilise des identifiants de compartiment pour accéder à ce compartiment et fournit des clés secrètes pour le compartiment S3 afin qu'Astra Control Center puisse communiquer avec le compartiment.

Faire pivoter les identifiants du godet

Si vous faites pivoter les informations d'identification, faites-les pivoter pendant une fenêtre de maintenance lorsqu'aucune sauvegarde n'est en cours (planifiée ou à la demande).

Procédure de modification et de rotation des informations d'identification

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu Options de la colonne **actions**, sélectionnez **Modifier**.
3. Créer les nouvelles informations d'identification.
4. Sélectionnez **mettre à jour**.

Supprimer les identifiants du compartiment

Le retrait des identifiants de compartiment est uniquement possible si de nouvelles informations d'identification ont été appliquées à un compartiment ou si ce dernier n'est plus utilisé activement.



Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control est toujours utilisé car Astra Control utilise les informations d'identification pour authentifier le compartiment de secours. Ne pas supprimer ces identifiants si le compartiment est en cours d'utilisation, car cela entraînera des défaillances de sauvegarde et des problèmes d'indisponibilité des sauvegardes.



Si vous supprimez les identifiants de compartiment actifs, reportez-vous à la section "[dépannage de la dépose des informations d'identification du godet](#)".

Pour obtenir des instructions sur la suppression des informations d'identification S3 à l'aide de l'API de contrôle Astra, reportez-vous au "[Informations sur l'automatisation et les API d'Astra](#)".

Déposer un godet

Il est possible de retirer un godet qui n'est plus utilisé ou qui n'est pas en bon état. Pour simplifier et à jour la configuration du magasin d'objets,



Vous ne pouvez pas supprimer un compartiment par défaut. Si vous souhaitez retirer ce compartiment, sélectionnez tout d'abord un autre compartiment comme valeur par défaut.

Ce dont vous avez besoin

- Avant de commencer, assurez-vous qu'aucune sauvegarde n'est en cours d'exécution ou terminée pour ce compartiment.
- Vérifiez que le godet n'est pas utilisé dans le cadre d'une politique de protection active.

Si c'est le cas, vous ne pourrez pas continuer.

Étapes

1. Dans la navigation à gauche, sélectionnez **seaux**.
2. Dans le menu **actions**, sélectionnez **Supprimer**.



Astra Control veille à l'absence de règles de planification qui utilise le compartiment pour les sauvegardes et à l'absence de sauvegardes actives dans le compartiment.

3. Tapez « Supprimer » pour confirmer l'action.
4. Sélectionnez **Oui, retirez le godet**.

Trouvez plus d'informations

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

Gérer le stockage back-end

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. Il est possible de surveiller la capacité du stockage et les informations concernant son état, y compris les performances si le centre de contrôle Astra est connecté à Cloud Insights.

Pour obtenir des instructions sur la gestion des systèmes back-end avec l'API Astra Control, consultez le ["Informations sur l'automatisation et les API d'Astra"](#).

Vous pouvez effectuer les tâches suivantes liées à la gestion d'un système back-end :

- ["Ajout d'un système back-end"](#)
- [Afficher les détails du système back-end](#)
- [Annuler la gestion d'un système back-end](#)
- [Retirer un système back-end](#)

Afficher les détails du système back-end

Vous pouvez afficher les informations de stockage back-end à partir du tableau de bord ou de l'option Backends.

Affichez les détails du système de stockage back-end à partir du tableau de bord

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Tableau de bord**.
2. Vérifiez le panneau Storage backend du tableau de bord indiquant l'état :
 - **Malsain**: Le stockage n'est pas dans un état optimal. Cela peut être dû à un problème de latence ou à une application dégradée en raison d'un problème de conteneur, par exemple.
 - **Tout en bonne santé**: Le stockage a été géré et est dans un état optimal.
 - **Découvert**: Le stockage a été découvert, mais pas géré par Astra Control.

Afficher les détails du système de stockage back-end à partir de l'option Backends

Affichez des informations sur l'état du système back-end, la capacité et les performances (débit et/ou latence des IOPS).

Vous pouvez voir les volumes utilisés par les applications Kubernetes, qui sont stockés sur un back-end de stockage sélectionné. Avec Cloud Insights, des informations supplémentaires s'affichent. Voir "[Documentation Cloud Insights](#)".

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.



Si vous êtes connecté à NetApp Cloud Insights, des extraits de données de Cloud Insights s'affichent sur la page Backends.

Name	Persistent volume	Capacity	App/s	Cluster/s	Cloud
trident_pvc_...	pvc-...	0.04/46.57 GiB: 0.1%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc-...	0.34/23.28 GiB: 1.44%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc-...	0.02/0.93 GiB: 2.33%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc-...	3.02/50.00 GiB: 6.04%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc-...	0.19/8.00 GiB: 2.39%	apps-mysql mysql-mysql	openshift-cluster010	private
trident_pvc_...	pvc-...	0.41/50.00 GiB: 0.81%	netapp-acc polaris-influxdb2-polaris-influxdb2	openshift-cluster010	private
trident_pvc_...	pvc-...	2.93/50.00 GiB: 5.87%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc-...	0.03/10.00 GiB: 0.26%	netapp-acc polaris-consul-consul	openshift-cluster010	private

3. Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Annuler la gestion d'un système back-end

Vous pouvez annuler la gestion du système back-end.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Unmanage**.
4. Saisissez « Unmanage » pour confirmer l'action.
5. Sélectionnez **Oui, annulez la gestion du stockage back-end**.

Retirer un système back-end

Vous pouvez supprimer un système back-end de stockage qui n'est plus utilisé. Pour que votre configuration reste simple et à jour, nous vous le souhaitons.

Ce dont vous avez besoin

- Assurez-vous que le système de stockage back-end n'est pas géré.
- Assurez-vous que le système back-end ne dispose d'aucun volume associé au cluster.

Étapes

1. Dans le menu de navigation gauche, sélectionnez **Backends**.
2. Si le système back-end est géré, le annuler sa gestion.
 - a. Sélectionnez **géré**.
 - b. Sélectionnez le système back-end.
 - c. Dans l'option **actions**, sélectionnez **Unmanage**.
 - d. Saisissez « Unmanage » pour confirmer l'action.
 - e. Sélectionnez **Oui, annulez la gestion du stockage back-end**.
3. Sélectionnez **découvert**.
 - a. Sélectionnez le système back-end.
 - b. Dans l'option **actions**, sélectionnez **Supprimer**.
 - c. Tapez « Supprimer » pour confirmer l'action.
 - d. Sélectionnez **Oui, retirez le back-end de stockage**.

Trouvez plus d'informations

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

Surveillez les tâches en cours d'exécution

Vous pouvez afficher des détails sur l'exécution des tâches et des tâches qui ont terminé, échoué ou ont été annulées au cours des 24 dernières heures dans Astra Control. Par exemple, vous pouvez afficher l'état d'une opération de sauvegarde, de restauration ou de clonage. Pour plus d'informations, reportez-vous aux pourcentages terminés et au temps restant estimé. Vous pouvez afficher l'état d'une opération planifiée exécutée ou d'une opération que vous avez démarrée manuellement.

Lors de l'affichage d'une tâche en cours d'exécution ou terminée, vous pouvez développer les détails de la tâche pour afficher l'état de chacune des sous-tâches. La barre de progression de la tâche est verte pour les tâches en cours ou terminées, bleue pour les tâches annulées et rouge pour les tâches ayant échoué en raison d'une erreur.



Pour les opérations de clonage, les sous-tâches se composent d'un snapshot et d'une opération de restauration de snapshot.

Pour plus d'informations sur les tâches ayant échoué, reportez-vous à la section ["Surveillez l'activité des comptes"](#).

Étapes

1. Pendant qu'une tâche est en cours d'exécution, accédez à **applications**.
2. Sélectionnez le nom d'une application dans la liste.
3. Dans les détails de l'application, sélectionnez l'onglet **tâches**.

Vous pouvez afficher les détails des tâches actuelles ou passées et filtrer par état de tâche.



Les tâches sont conservées dans la liste **tâches** pour un maximum de 24 heures. Vous pouvez configurer cette limite et d'autres paramètres du moniteur de tâches à l'aide de l' "[API de contrôle Astra](#)".

Surveillez l'infrastructure avec des connexions Cloud Insights, Prometheus ou Fluentd

Vous pouvez configurer plusieurs paramètres en option pour améliorer votre expérience avec Astra Control Center. Pour contrôler l'ensemble de votre infrastructure et obtenir des informations exploitables, créez une connexion à NetApp Cloud Insights, configurez Prometheus ou ajoutez une connexion Fluentd.

Si le réseau sur lequel vous exécutez Astra Control Center requiert un proxy pour vous connecter à Internet (pour télécharger des bundles de support vers le site de support NetApp ou établir une connexion avec Cloud Insights), vous devez configurer un serveur proxy dans le centre de contrôle Astra.

- [Connectez-vous à Cloud Insights](#)
- [Connectez-vous à Prometheus](#)
- [Connectez-vous à Fluentd](#)

Ajoutez un serveur proxy pour les connexions à Cloud Insights ou au site de support NetApp

Si le réseau sur lequel vous exécutez Astra Control Center requiert un proxy pour vous connecter à Internet (pour télécharger des bundles de support vers le site de support NetApp ou établir une connexion avec Cloud Insights), vous devez configurer un serveur proxy dans le centre de contrôle Astra.



Astra Control Center ne valide pas les détails que vous entrez pour votre serveur proxy. Assurez-vous de saisir les valeurs correctes.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Connect** dans la liste déroulante pour ajouter un serveur proxy.



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected

Connect

4. Entrez le nom du serveur proxy ou l'adresse IP et le numéro du port proxy.
5. Si votre serveur proxy nécessite une authentification, cochez la case et saisissez le nom d'utilisateur et le mot de passe.
6. Sélectionnez **connexion**.

Résultat

Si les informations de proxy que vous avez saisies ont été enregistrées, la section **HTTP Proxy** de la page **Account > Connections** indique qu'elle est connectée et affiche le nom du serveur.



Connected



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Modifier les paramètres du serveur proxy

Vous pouvez modifier les paramètres du serveur proxy.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les détails du serveur et les informations d'authentification.
5. Sélectionnez **Enregistrer**.

Désactiver la connexion au serveur proxy

Vous pouvez désactiver la connexion au serveur proxy. Vous serez averti avant de désactiver cette interruption potentielle à d'autres connexions.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération.

Connectez-vous à Cloud Insights

Pour surveiller et obtenir des informations exploitables sur l'ensemble de votre infrastructure, connectez NetApp Cloud Insights à votre instance Astra Control Center. Cloud Insights est inclus dans votre licence Astra Control Center.

Cloud Insights doit être accessible à partir du réseau utilisé par Astra Control Center, ou indirectement via un serveur proxy.

Lorsque le centre de contrôle Astra est connecté à Cloud Insights, un pod d'unité d'acquisition est créé. Ce pod collecte les données des systèmes back-end gérés par Astra Control Center et les pousse dans Cloud Insights. Ce pod requiert 8 Go de RAM et 2 cœurs de CPU.



Après avoir activé la connexion Cloud Insights, vous pouvez afficher les informations de débit sur la page **Backends** et vous connecter à Cloud Insights à partir de là après avoir sélectionné un back-end de stockage. Vous trouverez également des informations sur le **Tableau de bord** dans la section Cluster et vous y connectez également à Cloud Insights.

Ce dont vous avez besoin

- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Licence Astra Control Center valide.
- Un serveur proxy si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour se connecter à Internet.



Si vous découvrez Cloud Insights, familiarisez-vous avec les fonctions et les fonctionnalités. Voir "[Documentation Cloud Insights](#)".

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Connect** où apparaît **déconnecté** dans la liste déroulante pour ajouter la connexion.



4. Entrez les jetons de l'API Cloud Insights et l'URL du locataire. L'URL du locataire a le format suivant, par exemple :

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Vous obtenez l'URL du locataire lorsque vous obtenez la licence Cloud Insights. Si vous ne disposez pas de l'URL du locataire, reportez-vous à la section "[Documentation Cloud Insights](#)".

- a. Pour obtenir le "[Jeton API](#)", Connectez-vous à l'URL de votre locataire Cloud Insights.
- b. Dans Cloud Insights, générez un jeton d'accès à l'API **lecture/écriture** et un jeton d'accès à l'API **lecture seule** en cliquant sur **Admin > API Access**.

Cloud Insights (Trial) Tutorial 0% Complete Getting Started

MONITOR & OPTIMIZE

nmm95sx / Admin / API Access

API Access Tokens (4)

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission
<input type="checkbox"/>	astra_...		...zBskB1	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...xKOel_	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...2_A6HP	All Categories	Read Only
<input type="checkbox"/>	astra_...		...8BTKYY	All Categories	Read/Write

+ API Access Token Bulk Actions

- c. Copiez la clé **lecture seule**. Vous devrez la coller dans la fenêtre du centre de contrôle Astra pour activer la connexion Cloud Insights. Pour les autorisations de clé de token d'accès à l'API de lecture, sélectionnez : actifs, alertes, unité d'acquisition et collecte de données.
- d. Copiez la clé **lecture/écriture**. Vous devrez le coller dans la fenêtre Centre de contrôle Astra **connexion Cloud Insights**. Pour les autorisations de clé de token d'accès à l'API Read/Write, sélectionnez : data ingestion, gestion des journaux, unité d'acquisition et collecte de données.



Nous vous recommandons de générer une clé **lecture seule** et une clé **lecture/écriture**, et de ne pas utiliser la même clé à ces deux fins. Par défaut, la période d'expiration du token est définie sur un an. Nous vous recommandons de conserver la sélection par défaut pour donner au token la durée maximale avant son expiration. Si votre jeton expire, la télémétrie s'arrête.

- e. Collez les clés que vous avez copiées de Cloud Insights dans le centre de contrôle Astra.

5. Sélectionnez **connexion**.



Après avoir sélectionné **connexion**, l'état de la connexion devient **en attente** dans la section **Cloud Insights** de la page **compte > connexions**. Il peut y avoir quelques minutes pour que la connexion soit activée et que l'état passe à **Connected**.



Pour passer facilement entre le centre de contrôle Astra et les interfaces utilisateur Cloud Insights, assurez-vous d'être connecté aux deux.

Afficher les données dans Cloud Insights

Si la connexion a réussi, la section **Cloud Insights** de la page **compte > connexions** indique qu'elle est connectée et affiche l'URL du locataire. Vous pouvez accéder à Cloud Insights pour consulter les données reçues et affichées avec succès.

EXTERNAL ?

The screenshot shows two connection cards. The first card, titled 'HTTP PROXY', has a server icon and a 'Connected' status with a dropdown arrow. Below the title, it lists 'Server: proxy.example.com:8888' and 'Authentication: Enabled'. The second card, titled 'CLOUD INSIGHTS', has a bar chart icon and a 'Connected' status with a dropdown arrow. Below the title, it lists 'Tenant: Cloud Insights'.

Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.

The screenshot shows a 'Notifications' panel with a 'Mark All as Read' button. A notification is displayed with a red warning icon: 'Unable to connect to Cloud Insights an hour ago'. The message states: 'The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.'

Vous pouvez également trouver les mêmes informations sous **compte > Notifications**.

À partir du Centre de contrôle Astra, vous pouvez afficher les informations sur le débit sur la page **Backends** et vous connecter à Cloud Insights à partir d'ici après avoir sélectionné un back-end de stockage.

The screenshot shows the 'Backends' page with a table of storage backends. A popup window titled 'Throughput' is open over the first row. The table has columns for Name, Status, Capacity, Type, and Actions. The first row shows a backend with Name '.06', Status 'OK', Capacity '7.67/21.28 TiB: 36%', Type 'ONTAP 9.7.0', and Actions 'Available'. The popup shows a line graph for 'Throughput Last 24 hrs' with a current value of 8.00 MB/s. It also lists '5m ago: 8.00 MB/s', 'Min: 4.00 MB/s', and 'Max: 11.00 MB/s'. A 'View in Cloud Insights' link is at the bottom of the popup.

Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Vous pouvez également trouver les informations sur le **Dashboard**.

Reminder: Before you back up your applications, you need to add at least one object store bucket as a destination to hold your backups.

Add →

Resource summary

The screenshot shows the 'Resource summary' page in Astra Control Center. It features three main panels: 'Apps' (no managed apps), 'Clusters' (with a 'Let's get started' prompt and an 'Add' button), and 'Storage backends' (showing 1 managed and 0 discovered items). A 'View in cloud insights' button is highlighted in the Clusters panel.



Après l'activation de la connexion Cloud Insights, si vous supprimez les systèmes back-end ajoutés dans Astra Control Center, le système back-end cesse de créer des rapports avec Cloud Insights.

Modifier la connexion Cloud Insights

Vous pouvez modifier la connexion Cloud Insights.



Vous pouvez uniquement modifier les clés API. Pour modifier l'URL du locataire Cloud Insights, nous vous recommandons de déconnecter la connexion Cloud Insights et de vous connecter à la nouvelle URL.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les paramètres de connexion Cloud Insights.
5. Sélectionnez **Enregistrer**.

Désactiver la connexion Cloud Insights

Vous pouvez désactiver la connexion Cloud Insights pour un cluster Kubernetes géré par Astra Control Center. La désactivation de la connexion Cloud Insights ne supprime pas les données de télémétrie déjà chargées sur Cloud Insights.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération. Après avoir confirmé l'opération, sur la page **compte > connexions**, l'état Cloud Insights devient **en attente**. Le changement d'état prend quelques minutes à **déconnecté**.

Connectez-vous à Prometheus

Vous pouvez surveiller les données du centre de contrôle Astra avec Prometheus. Vous pouvez configurer Prometheus pour collecter des metrics à partir du terminal de metrics du cluster Kubernetes. Par ailleurs, vous pouvez utiliser Prometheus pour visualiser les données.

Pour plus d'informations sur l'utilisation de Prometheus, consultez leur documentation à l'adresse "[Mise en route de Prometheus](#)".

Ce dont vous aurez besoin

Assurez-vous que vous avez téléchargé et installé le package Prometheus sur le cluster Astra Control Center ou sur un autre cluster pouvant communiquer avec le cluster Astra Control Center.

Suivez les instructions de la documentation officielle à "[Installez Prometheus](#)".

Prometheus doit pouvoir communiquer avec le cluster Kubernetes Astra Control Center. Si Prometheus n'est pas installé sur le cluster Astra Control Center, vous devez vous assurer qu'ils peuvent communiquer avec le service de metrics exécuté sur le cluster Astra Control Center.

Configurez Prometheus

Astra Control Center expose un service de metrics sur le port TCP 9090 dans le cluster Kubernetes. Vous devez configurer Prometheus pour pouvoir collecter des metrics à partir de ce service.

Étapes

1. Connectez-vous au serveur Prometheus.
2. Ajoutez votre entrée de cluster dans le `prometheus.yml` fichier. Dans le `yml` ajoutez une entrée semblable à celle qui suit pour votre cluster dans le `scrape_configs` section:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
metrics_path: /accounts/<replace with your account ID>/metrics
authorization:
  credentials: <replace with your API token>
tls_config:
  insecure_skip_verify: true
static_configs:
  - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```



Si vous définissez le `tls_config insecure_skip_verify` à `true`, Le protocole de chiffrement TLS n'est pas requis.

3. Redémarrez le service Prometheus :

```
sudo systemctl restart prometheus
```

Accès à Prometheus

Accédez à l'URL Prometheus.

Étapes

1. Dans un navigateur, entrez l'URL Prometheus du port 9090.

2. Vérifiez votre connexion en sélectionnant **Statut > cibles**.

Affichez les données de Prometheus

Vous pouvez utiliser Prometheus pour afficher les données du centre de contrôle Astra.

Étapes

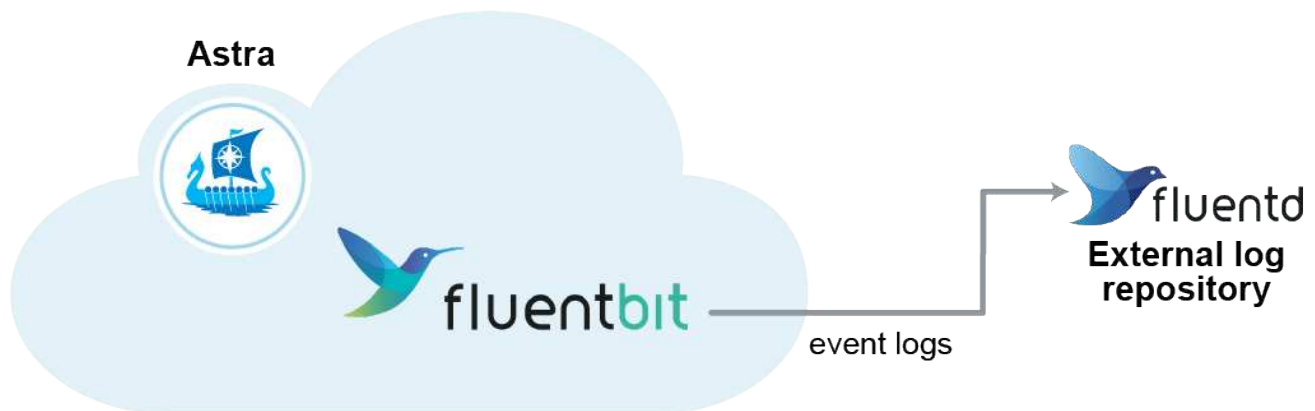
1. Dans un navigateur, entrez l'URL Prometheus.
2. Dans le menu Prometheus, sélectionnez **Graph**.
3. Pour utiliser l'Explorateur de mesures, sélectionnez l'icône en regard de **Exécuter**.
4. Sélectionnez `scrape_samples_scraped` Et sélectionnez **Exécuter**.
5. Pour voir le raclage des échantillons dans le temps, sélectionnez **Graph**.



Si plusieurs données de cluster ont été collectées, les mesures de chaque cluster apparaissent dans une couleur différente.

Connectez-vous à Fluentd

Vous pouvez envoyer des journaux (événements Kubernetes) depuis le système surveillé par Astra Control Center vers votre terminal Fluentd. La connexion Fluentd est désactivée par défaut.



Seuls les journaux d'événements des clusters gérés sont transférés à Fluentd.

Ce dont vous avez besoin

- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Astra Control Center est installé et exécuté sur un cluster Kubernetes.

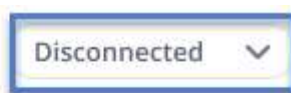


Astra Control Center ne valide pas les détails que vous entrez pour votre serveur Fluentd. Assurez-vous de saisir les valeurs correctes.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.

3. Sélectionnez **Connect** dans la liste déroulante où apparaît **déconnecté** pour ajouter la connexion.



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

4. Entrez l'adresse IP de l'hôte, le numéro de port et la clé partagée pour votre serveur Fluentd.

5. Sélectionnez **connexion**.

Résultat

Si les détails que vous avez entrés pour votre serveur Fluentd ont été enregistrés, la section **Fluentd** de la page **compte > connexions** indique qu'il est connecté. Vous pouvez maintenant visiter le serveur Fluentd que vous avez connecté et afficher les journaux d'événements.

Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.

Vous pouvez également trouver les mêmes informations sous **compte > Notifications**.



Si vous rencontrez des problèmes avec la collecte de journaux, vous devez vous connecter à votre nœud de travail et vous assurer que vos journaux sont disponibles dans `/var/log/containers/`.

Modifiez la connexion Fluentd

Vous pouvez modifier la connexion Fluentd à votre instance Astra Control Center.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les paramètres du point final Fluentd.
5. Sélectionnez **Enregistrer**.

Désactivez la connexion Fluentd

Vous pouvez désactiver la connexion Fluentd à votre instance Astra Control Center.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération.

Annuler la gestion des applications et des clusters

Supprimez toutes les applications ou clusters que vous ne souhaitez plus gérer à partir d'Astra Control Center.

Annuler la gestion d'une application

Arrêtez de gérer les applications que vous ne souhaitez plus sauvegarder, créer des instantanés ou cloner à partir d'Astra Control Center.

Lorsque vous annulez la gestion d'une application :

- Toutes les sauvegardes et tous les instantanés existants seront supprimés.
- Les applications et les données restent disponibles.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez l'application.
3. Dans le menu Options de la colonne actions, sélectionnez **Unmanage**.
4. Vérifiez les informations.
5. Tapez « Unmanage » pour confirmer.
6. Sélectionnez **Oui, annuler la gestion de l'application**.

Résultat

Astra Control Center cesse de gérer l'application.

Annuler la gestion d'un cluster

Arrêtez de gérer le cluster que vous ne souhaitez plus gérer à partir d'Astra Control Center.



Avant d'annuler la gestion du cluster, vous devez annuler la gestion des applications associées au cluster.

Lorsque vous dégérez un cluster :

- Cette action empêche votre cluster d'être géré par Astra Control Center. Elle ne modifie pas la configuration du cluster et ne supprime pas le cluster.
- Trident ne sera pas désinstallé du cluster. "[Découvrez comment désinstaller Trident](#)".

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **clusters**.
2. Cochez la case correspondant au cluster que vous ne souhaitez plus gérer.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Unmanage**.
4. Confirmez que vous souhaitez annuler la gestion du cluster, puis sélectionnez **Oui, Unmanage cluster**.

Résultat

L'état du cluster devient **Suppression**. Ensuite, le cluster sera supprimé de la page **clusters** et il n'est plus

géré par Astra Control Center.



Si le Centre de contrôle Astra et le Cloud Insights ne sont pas connectés, la dégestion du cluster supprime toutes les ressources qui ont été installées pour envoyer des données de télémétrie. **Si le Centre de contrôle Astra et le Cloud Insights sont connectés**, la dégestion du cluster supprime uniquement le `fluentbit` et `event-exporter` pods.

Mettez à niveau Astra Control Center

Pour mettre à niveau Astra Control Center, téléchargez le pack d'installation depuis le site de support NetApp et suivez ces instructions. Vous pouvez utiliser cette procédure pour mettre à niveau Astra Control Center dans des environnements connectés à Internet ou à air comprimé.

Ce dont vous avez besoin

- Avant de procéder à la mise à niveau, reportez-vous à la section "[De l'environnement opérationnel](#)" Pour garantir que votre environnement respecte les exigences minimales en matière de déploiement d'Astra Control Center. Votre environnement doit disposer des éléments suivants :
 - Une version d'Astra Trident prise en charge pour déterminer la version que vous exécutez, exécutez la commande suivante contre votre Astra Control Center existant :

```
kubectl get tridentversion -n trident
```

Reportez-vous à la section "[Documentation Astra Trident](#)" pour effectuer une mise à niveau à partir d'une ancienne version.



Vous devez effectuer une mise à niveau vers Astra Trident 22.10 * AVANT* pour la mise à niveau vers Kubernetes 1.25.

- Une distribution Kubernetes prise en charge pour déterminer la version que vous exécutez, exécutez la commande suivante par rapport à votre Astra Control Center existant : `kubectl get nodes -o wide`
- Suffisamment de ressources de cluster pour déterminer les ressources de cluster, exécutez la commande suivante dans votre cluster Astra Control Center existant : `kubectl describe node <node name>`
- Registre que vous pouvez utiliser pour diffuser et télécharger des images Astra Control Center
- Une classe de stockage par défaut pour déterminer votre classe de stockage par défaut, exécutez la commande suivante avec votre Astra Control Center existant : `kubectl get storageclass`
- (OpenShift uniquement) Assurez-vous que tous les opérateurs de cluster sont en bon état et disponibles.

```
kubectl get clusteroperators
```

- Assurez-vous que tous les services API sont dans un état sain et disponibles.

```
kubectl get apiservices
```

- Déconnectez-vous de l'interface utilisateur de l'Astra Control Center avant de commencer la mise à niveau.

Description de la tâche

Le processus de mise à niveau d'Astra Control Center vous guide à travers les étapes de haut niveau suivantes :

- [Téléchargez et extrayez Astra Control Center](#)
- [Retirez le plug-in NetApp Astra kubectl et réinstallez-le](#)
- [Ajoutez les images à votre registre local](#)
- [Poser le conducteur du centre de commande Astra mis à jour](#)
- [Mettez à niveau Astra Control Center](#)
- [Vérifiez l'état du système](#)



Ne supprimez pas l'opérateur du centre de contrôle Astra (par exemple, `kubectl delete -f astra_control_center_operator_deploy.yaml`) À tout moment pendant la mise à niveau ou l'opération Astra Control Center pour éviter de supprimer des modules.



Effectuez les mises à niveau dans une fenêtre de maintenance lorsque les planifications, les sauvegardes et les snapshots ne sont pas en cours d'exécution.

Téléchargez et extrayez Astra Control Center

1. Accédez au "[Page de téléchargement des produits Astra Control Center](#)" Sur le site de support NetApp. Vous pouvez sélectionner la dernière version ou une autre version souhaitée dans le menu déroulant.
2. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recommandé mais facultatif) Téléchargez le lot de certificats et de signatures pour Astra Control Center (`astra-control-center-certs-[version].tar.gz`) pour vérifier la signature du paquet :

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

La sortie s'affiche `Verified OK` une fois la vérification terminée.

4. Extraire les images du pack Astra Control Center :

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


Retirez le plug-in NetApp Astra kubectl et réinstallez-le

Le plug-in de ligne de commande NetApp Astra kubectl permet de gagner du temps lors de l'exécution des tâches courantes associées au déploiement et à la mise à niveau d'Astra Control Center.

1. Déterminez si le plug-in est installé :

```
kubectl astra
```

2. Faites l'une des actions suivantes :

- Si le plug-in est installé, la commande doit renvoyer l'aide du plug-in kubectl. Pour supprimer une version existante de kubectl-astra, exécutez la commande suivante : `delete /usr/local/bin/kubectl-astra`.
- Si la commande renvoie une erreur, le plug-in n'est pas installé et vous pouvez passer à l'étape suivante pour l'installer.

3. Installez le plug-in :

- a. Répertoriez les binaires NetApp Astra kubectl disponibles et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et votre architecture de processeur :



La bibliothèque de plug-ins kubectl fait partie du bundle tar et est extraite dans le dossier `kubectl-astra`.

```
ls kubectl-astra/
```

- a. Déplacez le bon binaire dans le chemin actuel et renommez-le `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Ajoutez les images à votre registre local

1. Suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Envoyez les images du package dans le répertoire d'images Astra Control Center vers votre registre local. Effectuez les remplacements suivants avant d'exécuter le `push-images` commande :

- Remplacez `<BUNDLE_FILE>` par le nom du fichier bundle Astra Control (`acc.manifest.bundle.yaml`).
- Remplacer `<MY_FULL_REGISTRY_PATH>` par l'URL du référentiel Docker, par exemple `<a href="https://<docker-registry>" class="bare">https://<docker-registry>"`.
- Remplacez `<MY_REGISTRY_USER>` par le nom d'utilisateur.
- Remplacez `<MY_REGISTRY_TOKEN>` par un jeton autorisé pour le registre.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

1. Accédez au répertoire racine du tarball. Vous devriez voir ce fichier et ce répertoire:

```
acc.manifest.bundle.yaml
acc/
```

2. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

3. Préparez et exécutez l'un des scripts suivants qui est personnalisé pour la version de Podman que vous utilisez. Remplacez `<MY_FULL_REGISTRY_PATH>` par l'URL de votre référentiel qui inclut tous les sous-répertoires.

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



Le chemin d'accès à l'image que le script crée doit ressembler aux éléments suivants, selon la configuration de votre registre : <https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

Poser le conducteur du centre de commande Astra mis à jour

1. Modifier le répertoire :

```
cd manifests
```

2. 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 ou modifiez la ligne par défaut de `imagePullSecrets: []` avec les éléments suivants :

```
imagePullSecrets:
- name: <astra-registry-cred_or_custom_name_of_secret>
```

- b. Changer `[your_registry_path]` pour le `kube-rbac-proxy` image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).
- c. Changer `[your_registry_path]` pour le `acc-operator` image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).
- d. Ajoutez les valeurs suivantes à la `env` section :

```
- name: ACCOP_HELM_UPGRADE_TIMEOUT
  value: 300m
```

```
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
  strategy:
    type: Recreate
  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: [your_registry_path]/kube-rbac-proxy:v4.8.0
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
env:
- name: ACCOP_LOG_LEVEL
  value: "2"
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
image: [your_registry_path]/acc-operator:[version x.y.z]
imagePullPolicy: IfNotPresent
livenessProbe:
  httpGet:
    path: /healthz
    port: 8081
    initialDelaySeconds: 15
    periodSeconds: 20
name: manager
readinessProbe:
  httpGet:
    path: /readyz
    port: 8081
    initialDelaySeconds: 5
    periodSeconds: 10
resources:
  limits:
    cpu: 300m
    memory: 750Mi
  requests:
    cpu: 100m
    memory: 75Mi
securityContext:
  allowPrivilegeEscalation: false
imagePullSecrets: []
securityContext:
  runAsUser: 65532
terminationGracePeriodSeconds: 10

```

3. Installez le nouveau conducteur du centre de contrôle Astra :

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

Exemple de réponse :

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

4. Vérifiez que les pods sont en cours d'exécution :

```
kubectl get pods -n netapp-acc-operator
```

Mettez à niveau Astra Control Center

1. Modifiez la ressource personnalisée Astra Control Center (CR) :

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

2. Modifier le numéro de version de l'Astra (astraVersion intérieur de Spec) vers la version que vous mettez à niveau vers :

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Vérifiez que le chemin du registre d'images correspond au chemin du registre vers lequel vous avez poussé les images dans un [étape précédente](#). Mise à jour `imageRegistry` intérieur de `Spec` si le registre a changé depuis votre dernière installation.

```
imageRegistry:
  name: "[your_registry_path]"
```

4. Ajoutez les éléments suivants à votre CRDs configuration à l'intérieur de `Spec`:

```
crds:
  shouldUpgrade: true
```

5. Ajoutez les lignes suivantes dans `additionalValues` intérieur de `Spec` Dans le CR Astra Control Center :

```
additionalValues:
  nautilus:
    startupProbe:
      periodSeconds: 30
      failureThreshold: 600
```

Une fois que vous avez enregistré et quitté l'éditeur de fichiers, les modifications seront appliquées et la mise à niveau commencera.

6. (Facultatif) Vérifiez que les modules se terminent et deviennent disponibles à nouveau :

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

7. Attendez que les conditions d'état de l'Astra Control indiquent que la mise à niveau est terminée et prête (True) :

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Réponse :

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.11.0-82	
10.111.111.111	True		



Pour surveiller le statut de la mise à niveau pendant l'opération, exécutez la commande suivante : `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`



Pour inspecter les journaux de l'opérateur de l'Astra Control Center, exécutez la commande suivante :
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Vérifiez l'état du système

1. Connectez-vous à Astra Control Center.
2. Vérifiez que la version a été mise à niveau. Consultez la page **support** de l'interface utilisateur.
3. Vérifiez que tous vos clusters et applications gérés sont toujours présents et protégés.

Désinstaller Astra Control Center

Vous devrez peut-être retirer les composants du centre de contrôle Astra si vous effectuez une mise à niveau d'un essai vers une version complète du produit. Pour déposer le centre de commande Astra et le conducteur du centre de commande Astra, exécuter les commandes décrites dans cette procédure dans l'ordre.

Si vous rencontrez des problèmes avec la désinstallation, reportez-vous à la section [Dépannage des problèmes de désinstallation](#).

Ce dont vous avez besoin

- Utilisez l'interface utilisateur d'Astra Control Center pour tout supprimer "[clusters](#)".

Étapes

1. Supprimer Astra Control Center. L'exemple de commande suivant est basé sur une installation par défaut. Modifiez la commande si vous avez créé des configurations personnalisées.

```
kubectl delete -f astra_control_center.yaml -n netapp-acc
```

Résultat :

```
astracontrolcenter.astra.netapp.io "astra" deleted
```


2. Utiliser la commande suivante pour supprimer le `netapp-acc` espace de noms :

```
kubectl delete ns netapp-acc
```

Résultat :

```
namespace "netapp-acc" deleted
```

3. Utiliser la commande suivante pour supprimer les composants du système de l'opérateur Astra Control Center :

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Résultat :

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

Dépannage des problèmes de désinstallation

Utilisez les solutions de contournement suivantes pour résoudre les problèmes que vous rencontrez lors de la désinstallation d'Astra Control Center.

La désinstallation d'Astra Control Center ne parvient pas à nettoyer le module de l'opérateur de surveillance sur le cluster géré

Si vous n'avez pas dégéré les clusters avant de désinstaller Astra Control Center, vous pouvez supprimer manuellement les pods dans l'espace de noms `netapp-Monitoring` et dans l'espace de noms à l'aide des commandes suivantes :

Étapes

1. Supprimer `acc-monitoring agent` :

```
kubectl delete agents acc-monitoring -n netapp-monitoring
```

Résultat :

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Supprimez le namespace :

```
kubectl delete ns netapp-monitoring
```

Résultat :

```
namespace "netapp-monitoring" deleted
```

3. Confirmer la suppression des ressources :

```
kubectl get pods -n netapp-monitoring
```

Résultat :

```
No resources found in netapp-monitoring namespace.
```

4. Confirmer la suppression de l'agent de surveillance :

```
kubectl get crd|grep agent
```

Résultat de l'échantillon :

```
agents.monitoring.netapp.com                2021-07-21T06:08:13Z
```

5. Supprimer les informations de définition de ressource personnalisée (CRD) :

```
kubectl delete crds agents.monitoring.netapp.com
```

Résultat :

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La désinstallation d'Astra Control Center ne parvient pas à nettoyer les CRD Traefik

Vous pouvez supprimer manuellement les CRD Traefik. Les CRDS sont des ressources globales, et leur suppression peut avoir un impact sur d'autres applications du cluster.

Étapes

1. Lister les CRD Traefik installés sur le cluster :

```
kubectl get crds |grep -E 'traefik'
```

Réponse

```
ingressroutes.traefik.containo.us          2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us       2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us       2021-06-23T23:29:12Z
middlewares.traefik.containo.us            2021-06-23T23:29:12Z
middlewareetcps.traefik.containo.us         2021-06-23T23:29:12Z
serverstransports.traefik.containo.us      2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us             2021-06-23T23:29:13Z
tlsstores.traefik.containo.us              2021-06-23T23:29:14Z
traefikservices.traefik.containo.us        2021-06-23T23:29:15Z
```

2. Supprimez les CRD :

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewareetcps.traefik.containo.us
```

Trouvez plus d'informations

- ["Problèmes connus de désinstallation"](#)

Automatisez avec l'API REST d'Astra Control

Automatisation avec l'API REST Astra Control

Astra Control est doté d'une API REST qui vous permet d'accéder directement à la fonctionnalité Astra Control à l'aide d'un langage de programmation ou d'un utilitaire tel que Curl. Vous pouvez également gérer les déploiements d'Astra Control avec Ansible et d'autres technologies d'automatisation.

Pour configurer et gérer vos applications Kubernetes, vous pouvez utiliser l'interface utilisateur Astra Control Center ou l'API Astra Control.

Pour en savoir plus, consultez le "[Documentation sur l'automatisation d'Astra](#)".

Connaissances et support

Dépannage

Apprenez à contourner certains problèmes courants que vous pourriez rencontrer.

["Base de connaissances NetApp pour Astra"](#)

Trouvez plus d'informations

- ["Comment télécharger un fichier vers NetApp \(connexion requise\)"](#)
- ["Comment télécharger manuellement un fichier vers NetApp \(connexion requise\)"](#)

Obtenez de l'aide

NetApp prend en charge Astra Control de plusieurs façons. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un canal discord. Votre compte Astra Control inclut un support technique à distance via la billetterie en ligne.



Si vous disposez d'une licence d'évaluation pour Astra Control Center, vous pouvez obtenir de l'aide technique. Toutefois, la création de dossier via le site de support NetApp (NSS) n'est pas disponible. Vous pouvez entrer en contact avec l'assistance via l'option de retour ou utiliser le canal de discord pour le libre-service.

Vous devez d'abord ["Activez le support de votre numéro de série NetApp"](#) afin d'utiliser ces options d'assistance non disponibles en libre-service. Un compte SSO du site de support NetApp (NSS) est nécessaire pour la discussion en ligne et la gestion des dossiers.

Options d'auto-assistance

Vous pouvez accéder aux options de support à partir de l'interface utilisateur du Centre de contrôle Astra en sélectionnant l'onglet **support** dans le menu principal.

Ces options sont disponibles gratuitement, 24h/24, 7j/7 :

- **"Base de connaissances (connexion requise)"**: Recherchez des articles, des FAQ, ou des renseignements sur les réparations en rapport avec Astra Control.
- **Centre de documentation**: C'est le site de documentation que vous consultez actuellement.
- **"Obtenir de l'aide par discord"**: Allez à Astra dans la catégorie Pub pour communiquer avec des pairs et des experts.
- **Créer un dossier de demande de support** : générer des packs de support pour le support NetApp à des fins de résolution de problèmes.
- **Faites-nous part de vos commentaires sur Astra Control**: Envoyez un courriel à astra.feedback@netapp.com pour nous faire part de vos pensées, idées ou préoccupations.

Activer le téléchargement quotidien de bundle de support planifié vers le support NetApp

Au cours de l'installation d'Astra Control Center, si vous spécifiez `enrolled: true` pour `autoSupport` Dans le fichier de ressources personnalisées (CR) Astra Control Center (`astra_control_center.yaml`), les offres de support quotidien sont automatiquement téléchargées sur le "[Site de support NetApp](#)".

Générez un bundle de support à fournir au support NetApp

Avec le centre de contrôle Astra, l'utilisateur administratif peut générer des bundles qui incluent des informations utiles pour le support NetApp, y compris des journaux, des événements pour tous les composants du déploiement Astra, des mesures et des informations de topologie sur les clusters et les applications sous gestion. Si vous êtes connecté à Internet, vous pouvez télécharger des packs de support sur le site de support NetApp (NSS) directement à partir de l'interface utilisateur du centre de contrôle Astra.



Le temps passé par Astra Control Center à générer le pack dépend de la taille de votre installation Astra Control Center ainsi que des paramètres du pack de support demandé. La durée spécifiée lors de la demande d'un bundle de support détermine le temps nécessaire à la génération du bundle (par exemple, une période de temps plus courte entraîne une génération plus rapide du bundle).

Avant de commencer

Déterminez si une connexion proxy sera nécessaire pour télécharger des packs sur NSS. Si une connexion proxy est nécessaire, vérifiez que le centre de contrôle Astra a été configuré pour utiliser un serveur proxy.

1. Sélectionnez **comptes > connexions**.
2. Vérifiez les paramètres du proxy dans **Paramètres de connexion**.

Étapes

1. Créez un dossier sur le portail NSS à l'aide du numéro de série de licence indiqué sur la page **support** de l'interface utilisateur du Centre de contrôle Astra.
2. Procédez comme suit pour générer le pack de support à l'aide de l'interface utilisateur du centre de contrôle Astra :
 - a. Sur la page **support**, dans la mosaïque support bundle, sélectionnez **generate**.
 - b. Dans la fenêtre **Generate a support Bundle**, sélectionnez le délai.

Vous avez le choix entre des délais rapides ou personnalisés.



Vous pouvez choisir une plage de dates personnalisée et spécifier une période d'heure personnalisée pendant la plage de dates.

- c. Après avoir effectué les sélections, sélectionnez **confirmer**.
- d. Cochez la case **Upload le bundle vers le site de support NetApp when Generated**.
- e. Sélectionnez **générer un bundle**.

Lorsque le bundle de support est prêt, une notification apparaît sur la page **comptes > notification** dans la zone alertes, sur la page **activité**, et également dans la liste des notifications (accessible en sélectionnant l'icône dans le coin supérieur droit de l'interface utilisateur).

Si la génération a échoué, une icône apparaît sur la page générer un bundle. Sélectionnez l'icône pour

afficher le message.



L'icône de notifications en haut à droite de l'interface utilisateur fournit des informations sur les événements liés au bundle de support, comme lorsque le bundle est correctement créé, lorsque la création du bundle échoue, lorsque le bundle n'a pas pu être téléchargé, lorsque le bundle n'a pas pu être téléchargé, etc.

Si vous avez une installation pneumatique

Si vous disposez d'une installation pneumatique, effectuez les opérations suivantes après la génération du pack support. Lorsque le bundle est disponible au téléchargement, l'icône Télécharger apparaît en regard de **generate** dans la section **support Bundles** de la page **support**.

Étapes

1. Sélectionnez l'icône Télécharger pour télécharger le pack localement.
2. Téléchargez manuellement le bundle sur NSS.

Pour ce faire, vous pouvez utiliser l'une des méthodes suivantes :

- Utiliser "[Téléchargement de fichiers authentifiés NetApp \(connexion requise\)](#)".
- Joignez le pack au dossier directement sur NSS.
- Faites confiance à NetApp Active IQ.

Trouvez plus d'informations

- "[Comment télécharger un fichier vers NetApp \(connexion requise\)](#)"
- "[Comment télécharger manuellement un fichier vers NetApp \(connexion requise\)](#)"

Versions antérieures de la documentation Astra Control Center

La documentation relative aux versions précédentes est disponible.

- ["Documentation Astra Control Center 22.08"](#)
- ["Documentation Astra Control Center 22.04"](#)
- ["Documentation Astra Control Center 21.12"](#)
- ["Documentation Astra Control Center 21.08"](#)

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- ["Avis concernant le centre de contrôle Astra"](#)

Licence API Astra Control

<https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf>

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 DÉLICTEUELLE (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.