Documentation d’Astra Control Center 24.02

Astra Control Center

NetApp
August 11, 2025

Sommaire

Documentation d’Astra Control Center 24.02

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"

Envoyez vos commentaires sur la documentation en devenant un "Contributeur GitHub" ou en envoyant un e-mail à doccomments@netapp.com.

Nouveautés de la nouvelle version d'Astra Control Center

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

15 mars 2024 (24.02.0)

Nouvelles fonctionnalités et prises en charge

- **Déployez Astra Control Center sans registre privé** : vous n'avez plus besoin d'envoyer les images d'Astra Control Center vers un registre privé ou d'en utiliser une dans votre environnement Astra Control.
- **Corrections mineures de bogues**

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

(Préversion technique) workflows Kubernetes déclaratifs

Cette version d'Astra Control Center contient une fonctionnalité Kubernetes déclarative qui permet d'effectuer une gestion des données à partir d'une ressource personnalisée Kubernetes native.

Après avoir installé le "Connecteur Astra" Sur le cluster que vous souhaitez gérer, vous pourrez effectuer les opérations de cluster CR suivantes dans l'interface utilisateur ou à partir d'une CR :

- "Définissez une application à l'aide d'une ressource personnalisée"
- "Définissez le compartiment"
- "Protégez l'ensemble du cluster"
- "Sauvegardez votre application"
- "Créer un snapshot"
- "Créer des plannings pour les snapshots ou les sauvegardes"
- "Restaurez une application à partir d'un snapshot ou d'une sauvegarde"

7 novembre 2023 (23.10.0)

Nouvelles fonctionnalités et prises en charge

- **Fonctionnalités de sauvegarde et de restauration pour les applications avec les systèmes back-end de stockage ontap-nas économiques à base de pilotes** : activez les opérations de sauvegarde et de restauration `ontap-nas-economy` avec certains "étapes simples".

- **Sauvegardes immuables** : Astra Control prend désormais en charge "sauvegardes inaltérables et en lecture seule" en tant que couche de sécurité supplémentaire contre les programmes malveillants et autres menaces.
- **Présentation d'Astra Control provisionner**

  Avec la version 23.10, Astra Control présente un nouveau composant logiciel appelé Astra Control Provisioner qui sera disponible pour tous les utilisateurs d'Astra Control sous licence. ASTRA Control Provisioner offre un accès à un ensemble complet de fonctionnalités de gestion et de provisionnement du stockage avancées qui vont au-delà de celles d'Astra Trident. Ces fonctionnalités sont disponibles sans frais supplémentaires pour tous les clients d'Astra Control.

  - **Commencez avec Astra Control Provisioner**
    C'est possible "Activez le mécanisme de provisionnement Astra Control" Si vous avez installé et configuré votre environnement pour utiliser Astra Trident 23.10.
  - **Fonctionnalité Astra Control Provisioner**

    Les fonctions suivantes sont disponibles avec l'Astra Control Provisioner 23.10 :

    - **Sécurité renforcée du back-end de stockage avec le cryptage Kerberos 5** : vous pouvez améliorer la sécurité du stockage par "activation du chiffrement" pour le trafic entre votre cluster géré et le back-end de stockage. ASTRA Control provisionner prend en charge le chiffrement Kerberos 5 sur connexions NFSv4.1 des clusters Red Hat OpenShift aux volumes Azure NetApp Files et ONTAP sur site
    - **Récupérer des données à l'aide d'un snapshot** : Astra Control provisionner offre une restauration rapide de volume sur place à partir d'un snapshot à l'aide du `TridentActionSnapshotRestore` (TASR) CR.
    - **Améliorations de SnapMirror** : utilisez la fonctionnalité de réplication d'applications dans les environnements où Astra Control ne dispose pas d'une connectivité directe à un cluster ONTAP ou d'un accès aux informations d'identification ONTAP. Cette fonctionnalité vous permet d'utiliser la réplication sans devoir gérer un système back-end de stockage ou ses identifiants dans Astra Control.
    - **Fonctionnalités de sauvegarde et de restauration pour les applications avec `ontap-nas-economy` Systèmes back-end avec sauvegarde par pilote** : comme décrit ci-dessus.
- **Prise en charge de la gestion des applications qui utilisent le stockage NVMe/TCP**
  ASTRA Control peut désormais gérer des applications sauvegardées par des volumes persistants et connectés via NVMe/TCP.
- **Crochets d'exécution désactivés par défaut** : à partir de cette version, la fonctionnalité crochets d'exécution peut être "activé" ou désactivé pour une sécurité supplémentaire (il est désactivé par défaut). Si vous n'avez pas encore créé de crochets d'exécution pour une utilisation avec Astra Control, vous devez le faire "activez la fonction crochets d'exécution" pour commencer à créer des crochets. Si vous avez créé des crochets d'exécution avant cette version, la fonctionnalité crochets d'exécution reste activée et vous pouvez utiliser des crochets comme vous le feriez normalement.

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

31 juillet 2023 (23.07.0)

Nouvelles fonctionnalités et prises en charge

- "Prise en charge de l'utilisation de NetApp MetroCluster dans une configuration étendue en tant que back-end de stockage"
- "Prise en charge de l'utilisation de Longhorn en tant que système back-end de stockage"
- "Il est désormais possible de répliquer des applications entre des systèmes ONTAP back-end à partir du même cluster Kubernetes"
- "ASTRA Control Center prend désormais en charge « userPrincipalName » en tant qu'attribut de connexion alternatif pour les utilisateurs distants (LDAP)"
- "Un nouveau type de crochet d'exécution « post-basculement » peut être exécuté après le basculement de réplication avec Astra Control Center"
- Les workflows de clonage ne prennent désormais en charge que les clones dynamiques (état actuel de l'application gérée). Pour cloner à partir d'un snapshot ou d'une sauvegarde, utilisez "restaurer le flux de travail".

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

18 mai 2023 (23.04.2)

Ce correctif (23.04.2) pour Astra Control Center (23.04.0) prend en charge "Plug-in externe Kubernetes CSI v6.1.0" et corrige les problèmes suivants :

- Bogue avec la restauration d'applications sur place lors de l'utilisation de hooks d'exécution
- Problèmes de connexion avec le service de godet

25 avril 2023 (23.04.0)

Nouvelles fonctionnalités et prises en charge

- "Licence d'évaluation de 90 jours activée par défaut pour les nouvelles installations d'Astra Control Center"
- "Fonctionnalité améliorée de crochets d'exécution avec options de filtrage supplémentaires"
- "Les crochets d'exécution peuvent maintenant être exécutés après le basculement de la réplication avec Astra Control Center"
- "Prise en charge de la migration des volumes de la classe de stockage « ONTAP-nas-Economy » vers la classe de stockage « ontap-nas »"
- "Prise en charge de l'inclusion ou de l'exclusion des ressources applicatives pendant les opérations de restauration"
- "Prise en charge de la gestion des applications données uniquement"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

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)

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)

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)

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)

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 :

- Les sauvegardes d'applications et les snapshots échouent si la classe volumesnapshotclass est ajoutée après la gestion d'un cluster
- La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig contient plusieurs contextes
- Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne
- La restauration à partir d'une sauvegarde lors de l'utilisation du chiffrement à la volée Kerberos peut échouer
- Les données de sauvegarde restent dans le compartiment après leur suppression pour les compartiments dont la règle de conservation a expiré

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.

La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig 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 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.

La restauration à partir d'une sauvegarde lors de l'utilisation du chiffrement à la volée Kerberos peut échouer

Lorsque vous restaurez une application à partir d'une sauvegarde vers un back-end de stockage utilisant le chiffrement à la volée Kerberos, l'opération de restauration peut échouer. Ce problème n'affecte pas la restauration à partir d'un snapshot ni la réplication des données d'application à l'aide de NetApp SnapMirror.

> Lors de l'utilisation du chiffrement à la volée Kerberos avec les volumes NFSv4, vérifiez que les volumes NFSv4 utilisent les paramètres corrects. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "Guide des améliorations et des bonnes pratiques de NetApp NFSv4".

Les données de sauvegarde restent dans le compartiment après leur suppression pour les compartiments dont la règle de conservation a expiré

Si vous supprimez la sauvegarde immuable d'une application après l'expiration de la politique de conservation du compartiment, la sauvegarde est supprimée d'Astra Control, mais pas du compartiment. Ce problème sera corrigé dans une prochaine version.

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
- Les contraintes de rôle restrictives peuvent être ignorées pour les ressources sur les clusters sans connecteur

Limites de gestion des applications

- vous ne pouvez pas restaurer collectivement plusieurs applications dans un autre espace de noms
- ASTRA Control ne prend pas en charge les applications qui utilisent plusieurs classes de stockage par 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
- Les snapshots peuvent échouer pour les clusters Kubernetes 1.25 ou versions ultérieures disposant de certaines versions de contrôleur Snapshot
- Il est possible que les sauvegardes et les snapshots ne soient pas conservés lors du retrait d'une instance Astra Control Center
- Les opérations de restauration sur place pour les classes de stockage ontap-nas échouent

Limitations générales

- Limitations de l'utilisateur et du groupe LDAP
- 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
- La page activité affiche jusqu'à 100000 événements
- SnapMirror ne prend pas en charge les applications utilisant NVMe over TCP pour les systèmes back-end

de stockage

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 kubecconfig (`.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 dégérer 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 clone ou d'une opération de restauration, l'administrateur/propriétaire du compte 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.

Les contraintes de rôle restrictives peuvent être ignorées pour les ressources sur les clusters sans connecteur

- **Si les ressources auxquelles vous accédez appartiennent à des clusters qui ont installé le dernier connecteur Astra** : lorsqu'un utilisateur reçoit plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes des rôles sont combinées. Par exemple, si un utilisateur doté d'un rôle de visualiseur local joint trois groupes liés au rôle membre, l'utilisateur dispose désormais d'un accès de rôle de visualiseur aux ressources d'origine ainsi que d'un accès de rôle membre aux ressources acquises via l'appartenance à un groupe.
- **Si les ressources auxquelles vous accédez appartiennent à des clusters qui n'ont pas installé Astra Connector** : lorsqu'un utilisateur reçoit plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus autorisé sont les seules qui prennent effet.

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 ne prend pas en charge les applications qui utilisent plusieurs classes de stockage par espace de noms

ASTRA Control prend en charge les applications qui utilisent une seule classe de stockage par espace de nom. Lorsque vous ajoutez une application à un espace de noms, assurez-vous que cette application possède la même classe de stockage que les autres applications de l'espace de noms.

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, reportez-vous à la section "Exigences du centre de contrôle Astra".

Les snapshots peuvent échouer pour les clusters Kubernetes 1.25 ou versions ultérieures disposant de certaines versions de contrôleur Snapshot

Les snapshots pour les clusters Kubernetes exécutant la version 1.25 ou ultérieure peuvent échouer si la version v1beta1 des API du contrôleur de snapshot est installée sur le cluster.

Pour contourner ce problème, procédez comme suit lorsque vous mettez à niveau des installations Kubernetes 1.25 ou ultérieures :

1. Supprimez tous les CRD de snapshot existants et tout contrôleur de snapshot existant.
2. "Désinstaller Astra Trident".
3. "Installez les CRD de snapshot et le contrôleur de snapshot".
4. "Installez la dernière version d'Astra Trident".
5. "Créez une VolumeSnapshotClass".

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.

Les opérations de restauration sur place pour les classes de stockage ontap-nas échouent

Si vous effectuez une restauration sur place d'une application (restaurez-la dans son espace de noms d'origine) et que la classe de stockage de l'application utilise le `ontap-nas-economy` pilote, l'opération de restauration peut échouer si le répertoire de snapshot n'est pas masqué. Avant de remettre le produit en place, suivez les instructions de la section "Sauvegardez et restaurez les opérations ontap-nas" pour masquer le répertoire d'instantanés.

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.

ASTRA Control ne prend pas en charge une entité LDAP (utilisateur ou groupe) qui a un DN contenant un RDN avec un espace de fin '\' ou un espace de fin.

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.

La page activité affiche jusqu'à 100000 événements

La page activité Astra Control peut afficher jusqu'à 100,000 événements. Pour afficher tous les événements consignés, récupérez-les à l'aide du "API de contrôle Astra".

SnapMirror ne prend pas en charge les applications utilisant NVMe over TCP pour les systèmes back-end de stockage

ASTRA Control Center ne prend pas en charge la réplication NetApp SnapMirror pour les systèmes back-end de stockage utilisant le protocole NVMe over TCP.

Trouvez plus d'informations

- "Problèmes connus"

Commencez

Découvrez Astra Control

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

Caractéristiques

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

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

Modèles de déploiement

Astra Control est disponible dans deux modèles de déploiement :

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

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

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

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

Fonctionnement du service Astra Control

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

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

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

    - Pour les clusters GKE, Astra Control Service utilise "NetApp Cloud Volumes Service pour Google Cloud" Ou des disques persistants Google en tant que système de stockage back-end pour vos volumes persistants.
    - Pour les clusters AKS, Astra Control Service utilise "Azure NetApp Files" Ou des disques gérés Azure en tant que backend de stockage pour les volumes persistants.
    - Pour les clusters Amazon EKS, Astra Control Service utilise "Amazon Elastic Block Store" ou "Amazon FSX pour NetApp ONTAP" en tant que système back-end de stockage pour vos volumes persistants.
- Vous ajoutez votre première solution de calcul Kubernetes à Astra Control Service. Le service de contrôle d'Astra procède ensuite aux opérations suivantes :
    - Crée un magasin d'objets sur votre compte de fournisseur cloud, où sont stockées les copies de sauvegarde.

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

Le plan gratuit d'Astra Control vous permet de gérer jusqu'à 10 espaces de noms dans votre compte. Si vous souhaitez gérer plus de 10 000 personnes, vous devrez configurer la facturation en passant du Plan gratuit au Plan Premium.

Fonctionnement du centre de contrôle Astra

Astra Control Center fonctionne localement dans votre propre cloud privé.

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

Des fonctionnalités de contrôle et de télémétrie limitées (7 jours de metrics) sont disponibles dans Astra Control Center et exportées vers des outils de surveillance natifs Kubernetes (comme Prometheus et Grafana) via des terminaux de metrics ouverts.

ASTRA Control Center est entièrement intégré à l'écosystème AutoSupport et Active IQ Digital Advisor (également appelé Digital Advisor) pour fournir aux utilisateurs et au support NetApp des informations sur le dépannage et l'utilisation.

Vous pouvez essayer Astra Control Center avec une licence d'évaluation intégrée de 90 jours. Pendant que vous évaluez Astra Control Center, vous pouvez obtenir de l'aide par e-mail et via des options

communautaires. Vous avez également accès aux articles et à la documentation de la base de connaissances à partir du tableau de bord de support des produits.

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

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

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

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

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

Pour en savoir plus

- "Documentation relative au service après-vente Astra Control"
- "Documentation Astra Control Center"
- "Documentation Astra Trident"
- "Documentation de l'API Astra Control"
- "Documentation ONTAP"

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. Assurez-vous que votre environnement répond à ces exigences pour déployer et exploiter Astra Control Center.

Environnements Kubernetes de cluster hôte pris en charge

ASTRA Control Center a été validé avec les environnements hôtes Kubernetes suivants :

> Assurez-vous que l'environnement Kubernetes que vous choisissez d'héberger Astra Control Center répond aux exigences de ressources de base indiquées dans la documentation officielle de l'environnement.

Distribution Kubernetes sur le cluster hôte	Versions prises en charge
Azure Kubernetes Service sur Azure Stack HCI	Pile Azure HCI 21H2 et 22H2 avec AKS 1.24.11 à 1.26.6

Distribution Kubernetes sur le cluster hôte	Versions prises en charge
Anthos de Google	1.15 à 1.16 (voir Exigences d'entrée de Google Anthos)
Kubernetes (en amont)	1.27 à 1.29
Rancher Kubernetes Engine (RKE)	RKE 1 : versions 1.24.17, 1.25.13, 1.26.8 avec Rancher Manager 2.7.9 RKE 2 : versions 1.23.16 et 1.24.13 avec Rancher Manager 2.6.13 RKE 2 : versions 1.24.17, 1.25.14, 1.26.9 avec Rancher Manager 2.7.9
Plateforme de conteneurs Red Hat OpenShift	4.12 à 4.14

Ressources requises pour le cluster hôte

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

> 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.

- **Extensions CPU** : les CPU de tous les noeuds de l'environnement d'hébergement doivent avoir des extensions AVX activées.
- **Nœuds de travail** : au moins 3 nœuds de travail au total, avec 4 cœurs de processeur et 12 Go de RAM chacun
- **Configuration requise pour le cluster VMware Tanzu Kubernetes Grid** : lors de l'hébergement d'Astra Control Center sur un cluster VMware Tanzu Kubernetes Grid (TKG) ou Tanzu Kubernetes Grid Integrated Edition (TKGi), tenez compte des points suivants.
  - 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"
  - 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.
  - 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.
  - Soyez conscient des exigences spécifiques pour Astra Control Provisioner lorsque vous déployez Astra Control Center dans un environnement TKG ou TKGi :
    - Le cluster doit prendre en charge les workloads privilégiés.
    - Le `--kubelet-dir` l'indicateur doit être défini sur l'emplacement du répertoire kubelet. Par défaut, il s'agit de `/var/vcap/data/kubelet`.
    - Spécifier l'emplacement du kubelet à l'aide de `--kubelet-dir` Est connu pour fonctionner avec l'opérateur Trident, Helm et `tridentctl` de nombreux déploiements.

Exigences de maillage de service

Il est fortement recommandé d'installer une version vanille prise en charge du maillage de service Istio sur le cluster hôte Astra Control Center. Reportez-vous à la section "versions prises en charge" Pour les versions prises en charge d'Istio. Les versions de marque du maillage de services Istio, telles qu'OpenShift Service mesh, ne sont pas validées avec Astra Control Center.

Pour intégrer Astra Control Center avec le maillage de service Istio installé sur le cluster hôte, vous devez effectuer l'intégration dans le cadre d'un Astra Control Center "installation" et pas indépendant de ce processus.

> L'installation et l'utilisation d'Astra Control Center sans configurer de maillage de service sur le cluster hôte peuvent avoir de graves implications en matière de sécurité.

Astra Trident

Si vous avez l'intention d'utiliser Astra Trident à la place d'Astra Control Provisioner avec cette version, Astra Trident 23.04 et versions ultérieures sont pris en charge. ASTRA Control Center requiert De provisionnement Astra Control dans les versions ultérieures.

De provisionnement Astra Control

Pour utiliser la fonctionnalité de stockage avancée Astra Control Provisioner, vous devez installer Astra Trident 23.10 ou version ultérieure et activer "Fonctionnalité Astra Control Provisioner". Pour utiliser la dernière fonctionnalité d'Astra Control Provisioner, vous avez besoin des versions les plus récentes d'Astra Trident et d'Astra Control Center.

- **Version minimale de Astra Control Provisioner à utiliser avec Astra Control Center** : Astra Control Provisioner 23.10 ou version ultérieure installée et configurée.

Configuration ONTAP avec Astra Trident

- **Classe de stockage** : configurez au moins une classe de stockage 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.
- **Pilotes de stockage et nœuds worker** : Assurez-vous de configurer les nœuds worker de votre cluster avec les pilotes de stockage appropriés afin que les pods puissent interagir avec le 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-economy` (la réplication d'application n'est pas disponible avec ce type de classe de stockage)
  - `ontap-nas-economy` (les snapshots et les règles de réplication des applications ne sont pas disponibles avec ce type de classe de stockage)

Systèmes back-end

Assurez-vous que vous disposez d'un back-end pris en charge avec une capacité suffisante.

- **Capacité de stockage requise** : au moins 500 Go disponibles

- **Systèmes back-end pris en charge** : Astra Control Center prend en charge les systèmes back-end de stockage suivants :
  - NetApp ONTAP 9.9.1 ou version ultérieure systèmes AFF, FAS et ASA
  - NetApp ONTAP Select 9.9.1 ou version ultérieure
  - NetApp Cloud Volumes ONTAP 9.9.1 ou version ultérieure
  - (Pour une présentation technique d'Astra Control Center) NetApp ONTAP 9.10.1 ou version ultérieure pour les opérations de protection des données fournies sous forme de présentation technique
  - Longhorn 1.5.0 ou version ultérieure
    - Nécessite la création manuelle d'un objet VolumeSnapshotClass. Reportez-vous à la "Documentation Longhorn" pour obtenir des instructions.
  - NetApp MetroCluster
    - Les clusters Kubernetes gérés doivent se trouver dans une configuration étendue.
  - Systèmes back-end de stockage disponibles avec les fournisseurs cloud pris en charge

Licences ONTAP

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".

NetApp MetroCluster

Lorsque vous utilisez NetApp MetroCluster comme système back-end de stockage, vous devez effectuer les opérations suivantes :

- Spécifier une LIF de gestion de SVM en tant qu'option back-end dans le pilote Astra Trident que vous utilisez
- Vérifiez que vous disposez de la licence ONTAP appropriée

Pour configurer le LIF MetroCluster, reportez-vous aux options et exemples suivants pour chaque pilote :

- "SAN"
- "NAS"

Licence Astra Control Center

ASTRA Control Center requiert une licence Astra Control Center. Lorsque vous installez Astra Control Center, une licence d'évaluation intégrée de 90 jours pour 4,800 UC est déjà activée. Si vous avez besoin de davantage de capacité ou de conditions d'évaluation différentes, ou si vous souhaitez effectuer une mise à niveau vers une licence complète, vous pouvez obtenir une autre licence d'évaluation ou une licence complète auprès de NetApp. Vous devez disposer d'une licence pour protéger vos applications et vos données.

Vous pouvez essayer Astra Control Center en vous inscrivant pour un essai gratuit. Vous pouvez vous inscrire 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".

Configuration réseau requise

Configurez votre environnement opérationnel pour vous assurer qu'Astra Control Center peut communiquer correctement. Les configurations réseau suivantes sont requises :

- **Adresse FQDN** : vous devez avoir une adresse FQDN pour Astra Control Center.
- **Accès à Internet** : vous devez déterminer si vous avez un accès extérieur à Internet. Si ce n'est pas le cas, certaines fonctionnalités peuvent être limitées, telles que l'envoi de packs de support au "Site de support NetApp".
- **Port Access** : l'environnement opérationnel qui héberge Astra Control Center communique avec les ports TCP suivants. Veillez à ce que ces ports soient autorisés par le biais de pare-feu et configurez des pare-feu pour autoriser tout trafic de sortie HTTPS provenant du réseau Astra. Certains ports nécessitent une connectivité entre 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 dans les deux sens entre Astra Control Center et le système utilisé pour accéder à Astra Control Center
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).

Source	Destination	Port	Protocole	Objectif
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
Centre de contrôle Astra	Cluster Kubernetes géré	443/6443 **REMARQUE** : le port utilisé par le cluster géré peut varier en fonction du cluster. Consultez la documentation fournie par le fournisseur du logiciel du cluster.	HTTPS	Communication avec le cluster géré : assurez-vous que ce port est ouvert des deux manières entre le cluster hébergeant Astra Control Center et chaque cluster géré

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.

Pour plus d'informations, reportez-vous à la section "Configurer l'entrée pour l'équilibrage de charge".

Exigences d'entrée de 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 d'entrée Istio, ce qui vous permet d'utiliser simplement les fonctionnalités d'entrée génériques d'Astra Control Center lors de l'installation. Reportez-vous à la section "Documentation d'installation d'Astra Control Center" pour plus d'informations.

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 des applications** : "Conditions préalables à la réplication"

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 aux exigences suivantes :

Cluster Kubernetes

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

Intégration du stockage

- "Assurez-vous que votre environnement comprend Astra Control provisionner"
- "Activez les fonctionnalités avancées de provisionnement du stockage et de gestion Astra Control"
- "Préparez les nœuds workers du cluster"
- "Configuration des systèmes back-end"
- "Configurer les classes de stockage"
- "Installez un contrôleur de snapshot de volume"
- "Créer une classe de snapshot de volume"

Informations d'identification ONTAP

- "Configurez les identifiants ONTAP"

Téléchargez et installez Astra Control Center

Effectuez les tâches d'installation suivantes :

- "Téléchargez Astra Control Center à partir de la page de téléchargements du site de support NetApp"
- Obtenez le fichier de licence NetApp :
  - Si vous évaluez Astra Control Center, une licence d'évaluation intégrée est déjà incluse
  - "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**

Effectuez quelques tâches de base pour commencer :

- "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**

Une fois la configuration d'Astra Control Center terminée, utilisez l'interface utilisateur d'Astra Control ou le "API de contrôle Astra" pour commencer à gérer et à protéger les applications :

- "Gestion des comptes": Utilisateurs, rôles, LDAP, informations d'identification, etc.
- "Gérer les notifications"
- "Gérer des applications": Définissez les ressources à gérer.
- "Protégez vos applications": Configurer des stratégies de protection et répliquer, cloner et migrer des applications.

Pour en savoir plus

- "Utilisez l'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 les images d'installation et effectuez les étapes suivantes. Vous pouvez utiliser cette procédure pour installer Astra Control Center

dans des environnements connectés à Internet ou équipés d'un filtre à air.

Pour une démonstration du processus d'installation d'Astra Control Center, reportez-vous àla section "vidéo".

Avant de commencer

- **Respecter les conditions préalables environnementales** : "Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center".

> Déployez Astra Control Center dans un troisième domaine de panne ou sur un site secondaire. Cela est recommandé pour la réplication d'applications et la reprise sur incident transparente.

- **Assurer des services sains** : vérifier que tous les services API sont en bon état et disponibles :

```
kubectl get apiservices
```

- **Assurez-vous qu'un FQDN routable** : le FQDN Astra que vous prévoyez d'utiliser peut être routé vers le 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.
- **Configurer cert Manager** : si un gestionnaire de certificats existe déjà dans le cluster, vous devez en effectuer quelques-uns "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.
- * (Pilote SAN ONTAP uniquement) Activer le multipath* : si vous utilisez un pilote SAN ONTAP, assurez-vous que le multipath est activé sur tous vos clusters Kubernetes.

Vous devez également tenir compte des points suivants :

- **Accéder au registre d'images NetApp Astra Control** :

  Vous avez la possibilité d'obtenir des images d'installation et des améliorations de fonctionnalités pour Astra Control, telles que Astra Control Provisioner, à partir du registre d'images NetApp.

  a. Notez l'ID de votre compte Astra Control dont vous aurez besoin pour vous connecter au registre.

     Votre ID de compte s'affiche dans l'interface utilisateur web d'Astra Control Service. Sélectionnez l'icône de figure en haut à droite de la page, sélectionnez **API Access** et notez votre ID de compte.

  b. A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.

  c. Connectez-vous au registre Astra Control :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Installer un maillage de services pour des communications sécurisées** : il est fortement recommandé de sécuriser les canaux de communication du cluster hôte Astra Control à l'aide d'un "maillage de service pris en charge".

L'intégration d'Astra Control Center avec un maillage de service ne peut être effectuée que dans Astra Control Center "installation" et pas indépendant de ce processus. Le retour d'un environnement maillé à un environnement non maillé n'est pas pris en charge.

Pour l'utilisation du maillage de service Istio, vous devez effectuer les opérations suivantes :

- Ajouter un `istio-injection:enabled` étiquette Dans l'espace de noms Astra avant de déployer Astra Control Center.
- Utilisez le `Generic` paramètre d'entrée et fournissent une entrée alternative pour équilibrage de la charge externe.
- Pour les clusters Red Hat OpenShift, vous devez définir `NetworkAttachmentDefinition` Sur tous les espaces de noms Astra Control Center associés (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` pour les clusters d'applications, ou tout espace de noms personnalisé ayant été substitué).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

Étapes

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

- Téléchargez et extrayez Astra Control Center
- Suivez les étapes supplémentaires si vous utilisez un 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

> 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.

Téléchargez et extrayez Astra Control Center

Téléchargez les images d'Astra Control Center à partir de l'un des emplacements suivants :

- **Registre d'images du service Astra Control** : utilisez cette option si vous n'utilisez pas de registre local avec les images d'Astra Control Center ou si vous préférez cette méthode au téléchargement du bundle à partir du site de support NetApp.
- **Site de support NetApp** : utilisez cette option si vous utilisez un registre local avec les images du Centre de contrôle Astra.

Registre d'images Astra Control

1. Connectez-vous à Astra Control Service.
2. Sur le tableau de bord, sélectionnez **Deploy a autogéré instance d'Astra Control**.
3. Suivez les instructions pour vous connecter au registre d'images Astra Control, extraire l'image d'installation d'Astra Control Center et extraire l'image.

Site de support NetApp

1. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`) du "Page de téléchargements d'Astra Control Center".
2. (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.

3. Extraire les images du pack Astra Control Center :

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

Suivez les étapes supplémentaires si vous utilisez un registre local

Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, vous devez utiliser le plug-in de ligne de commande NetApp Astra kubectl.

Installez le plug-in NetApp Astra kubectl

Procédez comme suit pour installer le dernier plug-in de ligne de commande NetApp Astra kubectl.

Avant de commencer

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.

Si vous avez déjà installé le plug-in à partir d'une installation précédente, "vérifiez que vous disposez de la dernière version" avant d'effectuer ces étapes.

Étapes

1. Répertoriez les binaires kubectl du plug-in NetApp Astra disponibles :

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 fichier dont vous avez besoin pour votre système d'exploitation et votre architecture CPU 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

1. Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

a. Accédez au répertoire racine du tarball. Vous devriez voir le `acc.manifest.bundle.yaml` et les répertoires suivants :

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. 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

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

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

c. 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=24.02.0-69
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
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
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://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Modifier le répertoire :

```
cd manifests
```

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

1. Exportez la configuration kubeconfig pour le cluster hôte Astra Control Center :

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

> Avant de terminer l'installation, assurez-vous que votre kubeconfig pointe vers le cluster où vous souhaitez installer Astra Control Center.

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
```

   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/24.02.0-69`).

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-
operator --docker-server=cr.astra.netapp.io --docker
-username=[astra_account_id] --docker-password=[astra_api_token]
```

+

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

+

> 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.

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

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

   b. Créez un secret pour le `netapp-acc` (ou espace de nom personnalisé). Ajoutez des informations relatives à Docker et exécutez l'une des commandes appropriées en fonction de vos préférences de

registre :

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom namespace] --docker-server=cr.astra.netapp.io --docker-username=[astra_account_id] --docker-password=[astra_api_token]
```

```
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]
```

Poser le conducteur du centre de commande Astra

1. (Registres locaux uniquement) si vous utilisez un registre local, procédez comme suit :

   a. Ouvrez le déploiement de l'opérateur Astra Control Center YAML :

   ```
   vim astra_control_center_operator_deploy.yaml
   ```

   Un échantillon annoté YAML suit ces étapes.

   b. 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}]
   ```

   c. Changer `ASTRA_IMAGE_REGISTRY` pour le `kube-rbac-proxy` image dans le chemin du registre où vous avez poussé les images dans un étape précédente.

   d. Changer `ASTRA_IMAGE_REGISTRY` pour le `acc-operator-controller-manager` image dans le chemin du registre où vous avez poussé les images dans un étape précédente.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
```

```
  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: ASTRA_IMAGE_REGISTRY/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: ASTRA_IMAGE_REGISTRY/acc-operator:24.02.68
        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
```

2. Poser le conducteur du centre de commande Astra :

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

Développer pour une réponse d'échantillon :

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.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
```

3. 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 :

Nom du compte

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

AstraVersion

Réglage	Guidage	Type	Exemple
`astraVersion`	La version d'Astra Control Center à déployer. Aucune action n'est nécessaire pour ce paramètre car la valeur sera pré-remplie.	chaîne	`24.02.0-69`

Adresse postale

Réglage	Guidage	Type	Exemple
`astraAddress`	Modifiez le `astraAddress` 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 `http://` ou `https://` dans l'adresse. Copier ce FQDN pour l'utiliser dans un plus tard.	chaîne	`astra.example.com`

AutoSupport

Vos sélections dans cette section déterminent si vous participerez à l'application de support proactif de NetApp, au conseiller numérique et à l'emplacement d'envoi des données. Une connexion Internet est requise (port 442) et toutes les données de support sont anonymisées.

Réglage	Utiliser	Guidage	Type	Exemple
`autoSupport.enrolled`	Soit `enrolled` ou `url` les champs doivent être sélectionnés	Changer `enrolled` Pour AutoSupport à `false` pour les sites sans connexion internet ou sans conservation `true` pour les sites connectés. Un réglage de `true` Les données anonymes peuvent être envoyées à NetApp pour bénéficier d'un support. La sélection par défaut est `false` Aucune donnée de support n'est envoyée à NetApp.	Booléen	`false` (cette valeur est la valeur par défaut)
`autoSupport.url`	Soit `enrolled` ou `url` 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`

e-mail

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`

Prénom

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`

Nom de famille

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`

Registre d'imageRegistry

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
`imageRegistry.name`	Obligatoire	Nom du registre d'images Astra Control qui héberge toutes les images requises pour déployer Astra Control Center. La valeur sera pré-remplie et aucune action n'est requise sauf si vous avez configuré un registre local. Dans le cas d'un registre local, remplacez cette valeur existante par le nom du registre d'images où vous avez poussé les images dans le étape précédente. Ne pas utiliser `http://` ou `https://` dans le nom du registre.	chaîne	`cr.astra.netapp.io` (valeur par défaut) `example.registry.com/astra` (exemple de registre local)

Réglage	Utiliser	Guidage	Type	Exemple
`imageRegistry.secret`	Facultatif	Nom du secret Kubernetes utilisé pour s'authentifier auprès du registre d'images. La valeur sera pré-remplie et aucune action n'est requise sauf si vous avez configuré un registre local et la chaîne que vous avez saisie pour ce registre dans `imageRegistry.name` requiert un secret. IMPORTANT : si vous utilisez un registre local qui ne nécessite pas d'autorisation, vous devez le supprimer `secret` ligne comprise entre `imageRegistry` sinon, l'installation échouera.	chaîne	`astra-registry-cred`

Classe de stockage

Réglage	Guidage	Type	Exemple
`storageClass`	Modifiez le `storageClass` valeur à partir de `ontap-gold` À une autre ressource de classe de stockage, comme requis par votre installation. Lancer la commande `kubectl get sc` pour déterminer vos classes de stockage configurées existantes. L'une des classes de stockage configurées par Astra Control Provisioner doit être saisie dans le fichier manifeste (`astra-control-center-<version>.manifest`) 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.	chaîne	`ontap-gold`

Volume ReclaimPolicy

Réglage	Guidage	Type	Options
`volumeReclaimPolicy`	Cette règle définit la règle de récupération pour les volumes persistants d'Astra. Définition de cette règle sur `Retain` Conserve les volumes persistants après la suppression d'Astra. Définition de cette règle sur `Delete` supprime les volumes persistants après la suppression d'astra. Si cette valeur n'est pas définie, les PV sont conservés.	chaîne	• `Retain` (Il s'agit de la valeur par défaut) • `Delete`

Type d’esseType

Réglage	Guidage	Type	Options
`ingressType`	Utilisez l'un des types d'entrées suivants : **Générique** (`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. Une fois Astra Control Center déployée, vous devez configurer le "contrôleur d'entrée" Pour exposer Astra Control Center avec une URL. IMPORTANT : si vous avez l'intention d'utiliser un maillage de service avec Astra Control Center, vous devez sélectionner `Generic` comme type d'entrée et configurez votre propre "contrôleur d'entrée". **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	chaîne	• `Generic` (il s'agit de la valeur par défaut) • `AccTraefik`

Taille de l'échelle

Réglage	Guidage	Type	Options
`scaleSize`	Par défaut, Astra utilisera la haute disponibilité (HA) `scaleSize` de `Medium`, Qui déploie la plupart des services en haute disponibilité et déploie plusieurs répliques pour assurer la redondance. Avec `scaleSize` comme `Small`, Astra réduira le nombre de répliques pour tous les services, à l'exception des services essentiels, afin de réduire la consommation. CONSEIL : `Medium` les déploiements se composent d'environ 100 pods (à l'exclusion des workloads transitoires). 100 modules sont basés sur une configuration à trois nœuds maîtres et trois nœuds workers). Tenez compte des contraintes de limite réseau par pod qui peuvent représenter un problème dans votre environnement, en particulier lors de l'examen des scénarios de reprise d'activité.	chaîne	• `Small` • `Medium` (Il s'agit de la valeur par défaut)

AstressourcesScaler

Réglage	Guidage	Type	Options
`astraResourcesScaler`	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 `astraResourcesScalar` peut être réglé sur `Off`. Cela désactive les demandes de ressources et permet un déploiement sur les clusters plus petits.	chaîne	• `Default` (Il s'agit de la valeur par défaut) • `Off`

Autres vals

Ajoutez les valeurs supplémentaires suivantes à l'Astra Control Center CR pour éviter un problème connu lors de l'installation :

```
additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

crds

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

Réglage	Guidage	Type	Exemple
`crds.externalCertManager`	Si vous utilisez un gestionnaire de certificats externe, modifiez-le `externalCertManager` à `true`. La valeur par défaut `false` Provoque l'installation d'Astra Control Center de ses propres CRD de cert Manager 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	`False` (cette valeur est la valeur par défaut)
`crds.externalTraefik`	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	`False` (cette valeur est la valeur par défaut)

Assurez-vous d'avoir sélectionné la classe de stockage et le type d'entrée appropriés pour votre configuration avant de terminer l'installation.

exemple astra_control_center.yaml

```
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: "[cr.astra.netapp.io or your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
  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]
   ```

2. Si vous utilisez un maillage de service avec Astra Control Center, ajoutez l'étiquette suivante au `netapp-acc` ou un espace de noms personnalisé :

Votre type d'entrée (`ingressType`) doit être défini sur `Generic` Dans Astra Control Center CR avant de passer à cette commande.

```
kubectl label ns [netapp-acc or custom namespace] istio-
injection:enabled
```

3. (Recommandé) "Activez les licences MTL strictes" Pour le maillage de service Istio :

```
kubectl apply -n istio-system -f - <<EOF
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
spec:
  mtls:
    mode: STRICT
EOF
```

4. 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]
```

L'opérateur d'Astra Control Center effectue une vérification automatique des exigences de l'environnement. Manquant "de formation" Peut entraîner une défaillance de votre installation ou un dysfonctionnement d'Astra Control Center. Voir la section suivante pour vérifier la présence de messages d'avertissement liés au contrôle automatique du système.

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 le processus d'installation n'a pas produit de messages d'avertissement relatifs aux vérifications de validation :

```
kubectl get acc [astra or custom Astra Control Center CR name] -n
[netapp-acc or custom namespace] -o yaml
```

Des messages d'avertissement supplémentaires sont également signalés dans les journaux de l'opérateur d'Astra Control Center.

2. Corrigez tous les problèmes de votre environnement qui ont été signalés par les vérifications automatisées des exigences.

   Vous pouvez corriger les problèmes en vous assurant que votre environnement respecte les "de formation" Pour Astra Control Center.

3. 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.

Développez pour obtenir une réponse d'échantillon

```
acc-helm-repo-5bd77c9ddd-8wxm2              1/1     Running     0
1h
activity-5bb474dc67-8l9ss                   1/1     Running     0
1h
activity-5bb474dc67-qbrtq                   1/1     Running     0
1h
api-token-authentication-6wbj2              1/1     Running     0
1h
api-token-authentication-9pgw6              1/1     Running     0
1h
api-token-authentication-tqf6d              1/1     Running     0
1h
asup-5495f44dbd-z4kft                       1/1     Running     0
1h
authentication-6fdd899858-5x45s             1/1     Running     0
1h
bucketservice-84d47487d-n9xgp               1/1     Running     0
1h
bucketservice-84d47487d-t5jhm               1/1     Running     0
1h
cert-manager-5dcb7648c4-hbldc               1/1     Running     0
1h
cert-manager-5dcb7648c4-nr9qf               1/1     Running     0
1h
cert-manager-cainjector-59b666fb75-bk2tf    1/1     Running     0
1h
cert-manager-cainjector-59b666fb75-pfnck    1/1     Running     0
1h
cert-manager-webhook-c6f9b6796-ngz2x        1/1     Running     0
1h
cert-manager-webhook-c6f9b6796-rwtbn        1/1     Running     0
1h
certificates-5f5b7b4dd-52tnj                1/1     Running     0
1h
certificates-5f5b7b4dd-gtjbx                1/1     Running     0
1h
certificates-expiry-check-28477260-dz5vw    0/1     Completed   0
1h
cloud-extension-6f58cc579c-lzfmv            1/1     Running     0
1h
cloud-extension-6f58cc579c-zw2km            1/1     Running     0
1h
cluster-orchestrator-79dd5c8d95-qjg92       1/1     Running     0
1h
```

```
composite-compute-85dc84579c-nz82f          1/1     Running     0
1h
composite-compute-85dc84579c-wx2z2          1/1     Running     0
1h
composite-volume-bff6f4f76-789nj            1/1     Running     0
1h
composite-volume-bff6f4f76-kwnd4            1/1     Running     0
1h
credentials-79fd64f788-m7m8f                1/1     Running     0
1h
credentials-79fd64f788-qnc6c                1/1     Running     0
1h
entitlement-f69cdbd77-4p2kn                 1/1     Running     0
1h
entitlement-f69cdbd77-hswm6                 1/1     Running     0
1h
features-7b9585444c-7xd7m                   1/1     Running     0
1h
features-7b9585444c-dcqwc                   1/1     Running     0
1h
fluent-bit-ds-crq8m                         1/1     Running     0
1h
fluent-bit-ds-gmgq8                         1/1     Running     0
1h
fluent-bit-ds-gzr4f                         1/1     Running     0
1h
fluent-bit-ds-j6sf6                         1/1     Running     0
1h
fluent-bit-ds-v4t9f                         1/1     Running     0
1h
fluent-bit-ds-x7j59                         1/1     Running     0
1h
graphql-server-6cc684fb46-2x8lr             1/1     Running     0
1h
graphql-server-6cc684fb46-bshbd             1/1     Running     0
1h
hybridauth-84599f79fd-fjc7k                 1/1     Running     0
1h
hybridauth-84599f79fd-s9pmn                 1/1     Running     0
1h
identity-95df98cb5-dvlmz                    1/1     Running     0
1h
identity-95df98cb5-krf59                    1/1     Running     0
1h
influxdb2-0                                 1/1     Running     0
1h
```

```
keycloak-operator-6d4d688697-cfq8b          1/1     Running     0
1h
krakend-5d5c8f4668-7bq8g                    1/1     Running     0
1h
krakend-5d5c8f4668-t8hbn                    1/1     Running     0
1h
license-689cdd4595-2gsc8                    1/1     Running     0
1h
license-689cdd4595-g6vwk                    1/1     Running     0
1h
login-ui-57bb599956-4fwgz                   1/1     Running     0
1h
login-ui-57bb599956-rhztb                   1/1     Running     0
1h
loki-0                                      1/1     Running     0
1h
metrics-facade-846999bdd4-f7jdm             1/1     Running     0
1h
metrics-facade-846999bdd4-lnsxl             1/1     Running     0
1h
monitoring-operator-6c9d6c4b8c-ggkrl        2/2     Running     0
1h
nats-0                                      1/1     Running     0
1h
nats-1                                      1/1     Running     0
1h
nats-2                                      1/1     Running     0
1h
natssync-server-6df7d6cc68-9v2gd            1/1     Running     0
1h
nautilus-64b7fbdd98-bsgwb                   1/1     Running     0
1h
nautilus-64b7fbdd98-djlhw                   1/1     Running     0
1h
openapi-864584bccc-75nlv                    1/1     Running     0
1h
openapi-864584bccc-zh6bx                    1/1     Running     0
1h
polaris-consul-consul-server-0              1/1     Running     0
1h
polaris-consul-consul-server-1              1/1     Running     0
1h
polaris-consul-consul-server-2              1/1     Running     0
1h
polaris-keycloak-0                          1/1     Running     2 (1h
ago)      1h
```

```
polaris-keycloak-1                          1/1     Running     0
1h
polaris-keycloak-db-0                       1/1     Running     0
1h
polaris-keycloak-db-1                       1/1     Running     0
1h
polaris-keycloak-db-2                       1/1     Running     0
1h
polaris-mongodb-0                           1/1     Running     0
1h
polaris-mongodb-1                           1/1     Running     0
1h
polaris-mongodb-2                           1/1     Running     0
1h
polaris-ui-66476dcf87-f6s8j                 1/1     Running     0
1h
polaris-ui-66476dcf87-ztjk7                 1/1     Running     0
1h
polaris-vault-0                             1/1     Running     0
1h
polaris-vault-1                             1/1     Running     0
1h
polaris-vault-2                             1/1     Running     0
1h
public-metrics-bfc4fc964-x4m79              1/1     Running     0
1h
storage-backend-metrics-7dbb88d4bc-g78cj    1/1     Running     0
1h
storage-provider-5969b5df5-hjvcm            1/1     Running     0
1h
storage-provider-5969b5df5-r79ld            1/1     Running     0
1h
task-service-5fc9dc8d99-4q4f4               1/1     Running     0
1h
task-service-5fc9dc8d99-815zl               1/1     Running     0
1h
task-service-task-purge-28485735-fdzkd      1/1     Running     0
12m
telegraf-ds-2rgm4                           1/1     Running     0
1h
telegraf-ds-4qp6r                           1/1     Running     0
1h
telegraf-ds-77frs                           1/1     Running     0
1h
telegraf-ds-bc725                           1/1     Running     0
1h
```

```
telegraf-ds-cvmxf                          1/1     Running     0
1h
telegraf-ds-tqzgj                          1/1     Running     0
1h
telegraf-rs-5wtd8                          1/1     Running     0
1h
telemetry-service-6747866474-5djnc         1/1     Running     0
1h
telemetry-service-6747866474-thb7r         1/1     Running     1 (1h
ago)      1h
tenancy-5669854fb6-gzdzf                   1/1     Running     0
1h
tenancy-5669854fb6-xvsm2                   1/1     Running     0
1h
traefik-8f55f7d5d-4lgfw                    1/1     Running     0
1h
traefik-8f55f7d5d-j4wt6                    1/1     Running     0
1h
traefik-8f55f7d5d-p6gcq                    1/1     Running     0
1h
trident-svc-7cb5bb4685-54cnq               1/1     Running     0
1h
trident-svc-7cb5bb4685-b28xh               1/1     Running     0
1h
vault-controller-777b9bbf88-b5bqt          1/1     Running     0
1h
vault-controller-777b9bbf88-fdfd8          1/1     Running     0
1h
```

4. (En option) regarder le `acc-operator` journaux de suivi de la progression :

```
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.

5. 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 connecterez 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  24.02.0-69
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`).

Une fois Astra Control Center déployé, vous devez configurer le contrôleur Ingress pour exposer Astra Control Center avec 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 d'étapes pour certains types de contrôleurs d'entrée courants.

Avant de commencer

- 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 allez modifier le mot de passe de l'administrateur par défaut et vous connecter au tableau de bord de l'interface utilisateur d'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. Rechercher les codes de réponse API dans la plage 400 à 500. Ceux-ci indiquent l'endroit où un échec s'est produit.

Options

- 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
```

- Pour vérifier la sortie de l'Astra Control Center CR :

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

Autres procédures d'installation

- **Installer avec Red Hat OpenShift OperatorHub** : utilisez cette option "autre procédure" Pour installer Astra Control Center sur OpenShift à l'aide d'OperatorHub.
- **Installer dans le Cloud public avec Cloud Volumes ONTAP backend**: Utiliser "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.

Et la suite

- (Facultatif) en fonction de votre environnement, effectuez l'installation complète après l'installation "étapes de configuration".
- "Une fois Astra Control Center installé, connectez-vous à l'interface utilisateur et modifiez votre mot de passe, vous pouvez configurer une licence, ajouter des clusters, activer l'authentification, gérer le stockage et ajouter des compartiments".

Configurez un gestionnaire de certificats externe

Si un gestionnaire de certificats existe déjà dans votre cluster Kubernetes, vous devez effectuer certaines étapes préalables afin qu'Astra Control Center n'installe pas son propre gestionnaire de certificats.

Étapes

1. Vérifiez qu'un gestionnaire de certificats est installé :

   ```
   kubectl get pods -A | grep 'cert-manager'
   ```

   Exemple de réponse :

   ```
   cert-manager   essential-cert-manager-84446f49d5-sf2zd              1/1
   Running    0      6d5h
   cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
   Running    0      6d5h
   cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq      1/1
   Running    0      6d5h
   ```

2. Créez une paire de certificats/clés pour le `astraAddress` FQDN :

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

   Exemple de réponse :

```
Generating a 2048 bit RSA private key
...................+++
.......................................+++
writing new private key to 'tls.key'
```

3. Créez un secret avec des fichiers générés précédemment :

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Exemple de réponse :

```
secret/selfsigned-tls created
```

4. Créer un `ClusterIssuer` fichier qui est **exactement** le suivant mais qui comprend l'emplacement de l'espace de noms où votre `cert-manager` des pods sont installés :

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Exemple de réponse :

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Vérifiez que le `ClusterIssuer` s'est correctement installé. `Ready` doit être de `True` avant de pouvoir continuer :

```
kubectl get ClusterIssuer
```

Exemple de réponse :

```
NAME                        READY   AGE
astra-ca-clusterissuer      True    9s
```

6. Complétez le "Procédure d'installation d'Astra Control Center". Il y a un "Étape de configuration requise pour le groupe de centre de contrôle Astra YAML" Dans lequel vous modifiez la valeur CRD pour indiquer que le gestionnaire de certificats est installé en externe. Vous devez effectuer cette étape pendant l'installation pour que le centre de contrôle Astra reconnaisse le responsable du certificat externe.

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. Utiliser 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.

Avant de commencer

- **Respecter les conditions préalables environnementales** : "Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center".

> Déployez Astra Control Center dans un troisième domaine de panne ou sur un site secondaire. Cela est recommandé pour la réplication d'applications et la reprise sur incident transparente.

- **Assurer la santé des opérateurs de grappes et des services API** :
  - 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
```

- **Assurez-vous qu'un FQDN routable** : le FQDN Astra que vous prévoyez d'utiliser peut être routé vers le 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.
- **Obtenir les autorisations OpenShift** : vous aurez besoin de toutes les autorisations nécessaires et de l'accès à Red Hat OpenShift Container Platform pour effectuer les étapes d'installation décrites.
- **Configurer un gestionnaire de certificats** : si un gestionnaire de certificats existe déjà dans le cluster, vous devez en effectuer un "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.
- **Configuration du contrôleur d'entrée Kubernetes** : si vous disposez d'un contrôleur d'entrée

Kubernetes qui gère l'accès externe aux services, tels que l'équilibrage de la charge dans un cluster, vous devez le configurer pour une utilisation 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.

- * (Pilote SAN ONTAP uniquement) Activer le multipath* : si vous utilisez un pilote SAN ONTAP, assurez-vous que le multipath est activé sur tous vos clusters Kubernetes.

Vous devez également tenir compte des points suivants :

- **Accéder au registre d'images NetApp Astra Control** :

  Vous avez la possibilité d'obtenir des images d'installation et des améliorations de fonctionnalités pour Astra Control, telles que Astra Control Provisioner, à partir du registre d'images NetApp.

  a. Notez l'ID de votre compte Astra Control dont vous aurez besoin pour vous connecter au registre.

     Votre ID de compte s'affiche dans l'interface utilisateur web d'Astra Control Service. Sélectionnez l'icône de figure en haut à droite de la page, sélectionnez **API Access** et notez votre ID de compte.

  b. A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.

  c. Connectez-vous au registre Astra Control :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Installer un maillage de services pour des communications sécurisées** : il est fortement recommandé de sécuriser les canaux de communication du cluster hôte Astra Control à l'aide d'un "maillage de service pris en charge".

  > ⓘ L'intégration d'Astra Control Center avec un maillage de service ne peut être effectuée que dans Astra Control Center "installation" et pas indépendant de ce processus. Le retour d'un environnement maillé à un environnement non maillé n'est pas pris en charge.

  Pour l'utilisation du maillage de service Istio, vous devez effectuer les opérations suivantes :

  - Ajouter un `istio-injection:enabled` Etiquetez vers l'espace de noms Astra avant de déployer Astra Control Center.
  - Utilisez le `Generic` paramètre d'entrée et fournissent une entrée alternative pour "équilibrage de la charge externe".
  - Pour les clusters Red Hat OpenShift, vous devez définir `NetworkAttachmentDefinition` Sur tous les espaces de noms Astra Control Center associés (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` pour les clusters d'applications, ou tout espace de noms personnalisé ayant été substitué).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

Étapes

- Téléchargez et extrayez Astra Control Center
- Suivez les étapes supplémentaires si vous utilisez un registre local
- Recherchez la page d'installation de l'opérateur
- Poser l'opérateur
- Poser le 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.

Téléchargez et extrayez Astra Control Center

Téléchargez les images d'Astra Control Center à partir de l'un des emplacements suivants :

- **Registre d'images du service Astra Control** : utilisez cette option si vous n'utilisez pas de registre local avec les images d'Astra Control Center ou si vous préférez cette méthode au téléchargement du bundle à partir du site de support NetApp.
- **Site de support NetApp** : utilisez cette option si vous utilisez un registre local avec les images du Centre de contrôle Astra.

Registre d'images Astra Control

1. Connectez-vous à Astra Control Service.
2. Sur le tableau de bord, sélectionnez **Deploy a autogéré instance d'Astra Control**.
3. Suivez les instructions pour vous connecter au registre d'images Astra Control, extraire l'image d'installation d'Astra Control Center et extraire l'image.

Site de support NetApp

1. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`) du "Page de téléchargements d'Astra Control Center".
2. (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.

3. Extraire les images du pack Astra Control Center :

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

Suivez les étapes supplémentaires si vous utilisez un registre local

Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, vous devez utiliser le plug-in de ligne de commande NetApp Astra kubectl.

Installez le plug-in NetApp Astra kubectl

Procédez comme suit pour installer le dernier plug-in de ligne de commande NetApp Astra kubectl.

Avant de commencer

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.

Si vous avez déjà installé le plug-in à partir d'une installation précédente, "vérifiez que vous disposez de la dernière version" avant d'effectuer ces étapes.

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

1. Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

a. Accédez au répertoire racine du tarball. Vous devriez voir le `acc.manifest.bundle.yaml` et les répertoires suivants :

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. 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

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

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

c. 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=24.02.0-69
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
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
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://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Modifier le répertoire :

```
cd manifests
```

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 :

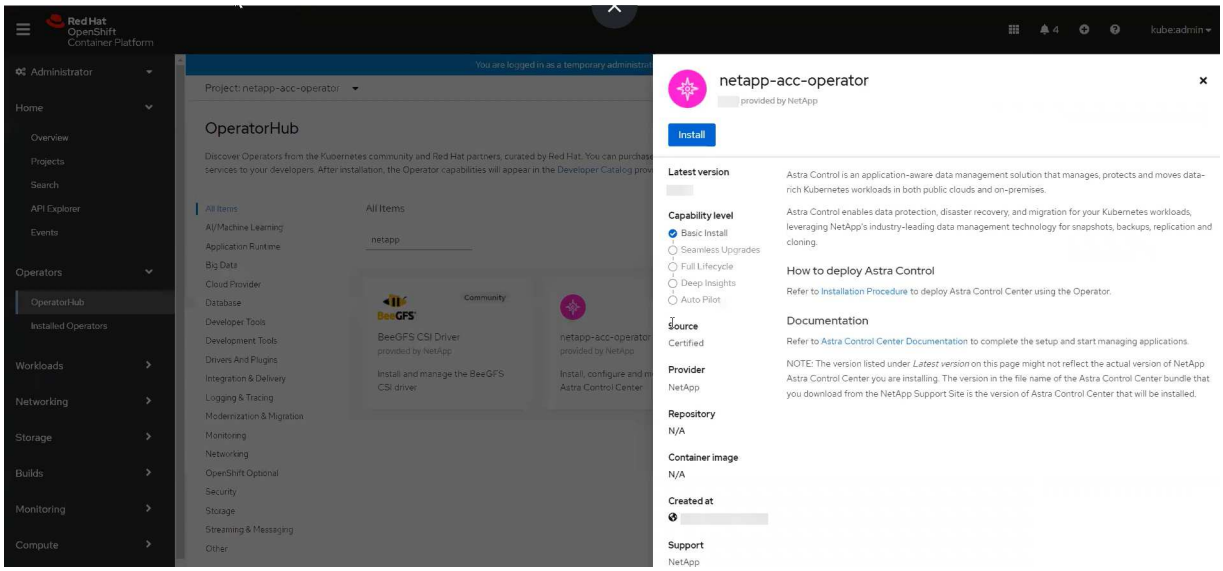
Console Web Red Hat OpenShift

a. Connectez-vous à l'interface utilisateur de OpenShift Container Platform.

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

> Vous ne pouvez effectuer la mise à niveau que vers la version actuelle d'Astra Control Center à l'aide de cet opérateur.

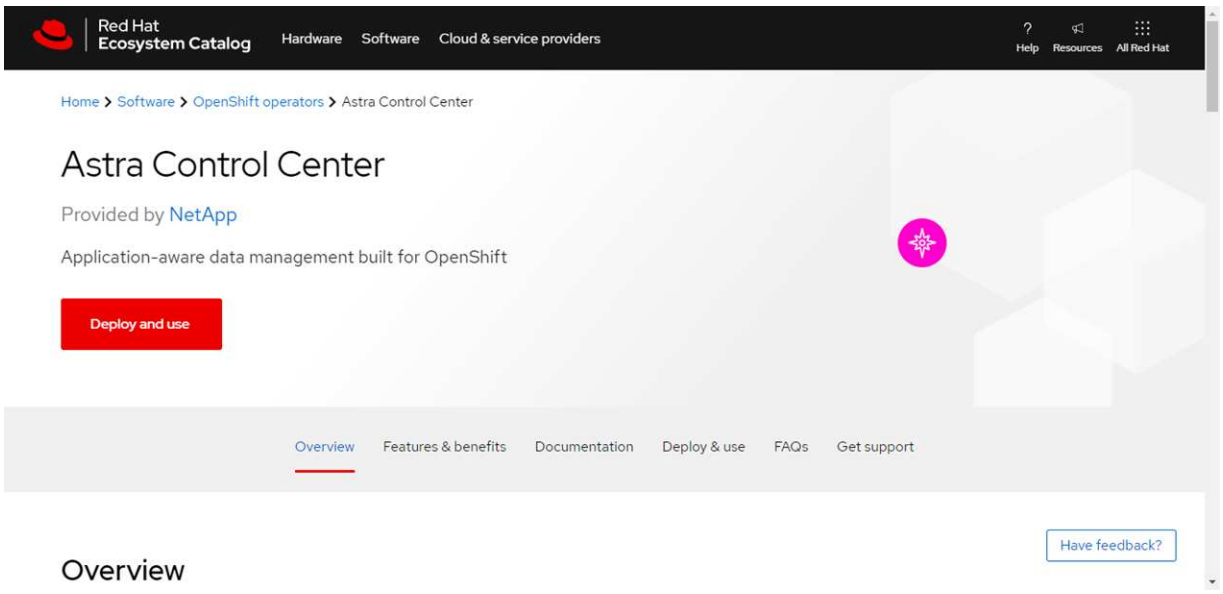
c. Recherchez `netapp-acc` Et sélectionnez l'opérateur du centre de contrôle Astra de NetApp.



Catalogue de l'écosystème Red Hat

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

b. Sélectionnez **déployer et utiliser**.



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.

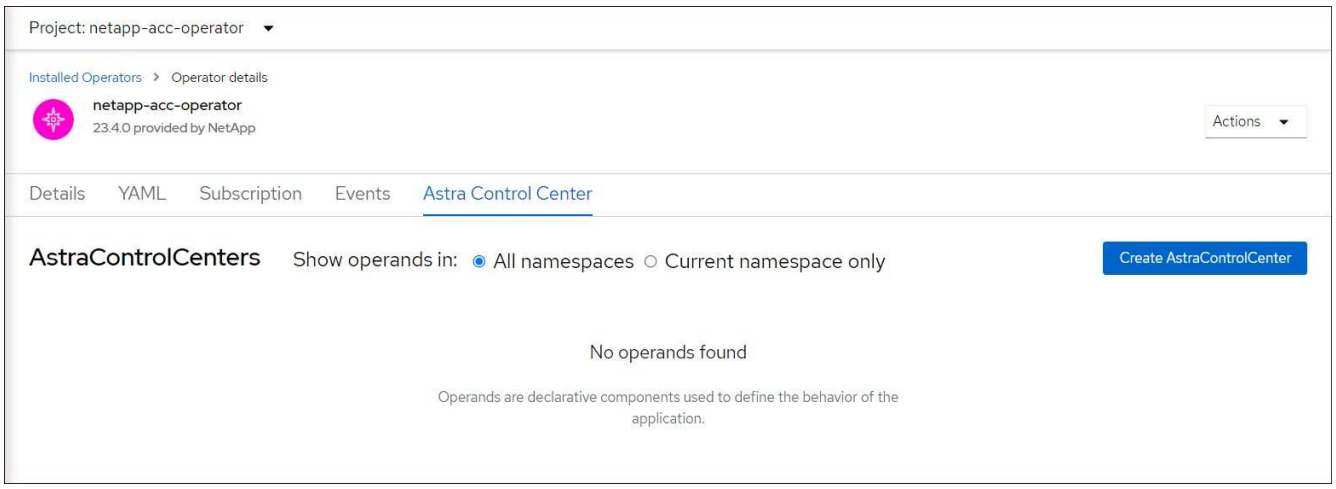
   c. Sélectionnez **installer**.

      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 :

   a. Conservez ou ajustez le nom du centre de contrôle Astra.

   b. Ajouter des étiquettes pour le centre de contrôle Astra.

   c. Activez ou désactivez Auto support. Il est recommandé de conserver la fonctionnalité Auto support.

   d. 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.

   e. Entrez la version d'Astra Control Center, par exemple 24.02.0-69.

   f. Entrez un nom de compte, une adresse e-mail et un nom d'administrateur.

   g. Choisir une règle de récupération de volume de `Retain`, `Recycle`, ou `Delete`. La valeur par défaut est `Retain`.

h. Sélectionnez la taille de l'échelle de l'installation.

> Par défaut, Astra utilisera la haute disponibilité (HA) `scaleSize` de `Medium`, Qui déploie la plupart des services en haute disponibilité et déploie plusieurs répliques pour assurer la redondance. Avec `scaleSize` comme `Small`, Astra réduira le nombre de répliques pour tous les services, à l'exception des services essentiels, afin de réduire la consommation.

i. sélectionnez le type d'entrée :

- **Générique** (`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. Une fois Astra Control Center déployée, 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 Ingress, reportez-vous à la section "De formation".

a. Dans **image Registry**, utilisez la valeur par défaut sauf si vous avez configuré un registre local. Dans le cas d'un registre local, remplacez cette valeur par le chemin du registre d'images local où vous avez poussé les images à l'étape précédente. 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. En outre, vous devez effectuer "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 autogérés 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. Reportez-vous à la section "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
- La zone hébergée AWS et l'entrée Amazon route 53 sont requises pour accéder à l'interface utilisateur d'Astra Control

Exigences de l'environnement opérationnel pour AWS

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

- Red Hat OpenShift Container Platform 4.11 à 4.13

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.

ASTRA Control Center requiert des ressources spécifiques en plus des besoins en ressources de l'environnement. Reportez-vous à la section "Exigences relatives à l'environnement opérationnel d'Astra Control Center".

Le jeton de registre AWS expire dans 12 heures. Après quoi vous devrez renouveler le secret de registre d'image 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, configurer des instances de calcul EC2 et créer un compartiment AWS S3. Si vous ne pouvez pas accéder au registre d'images NetApp Astra Control Center, vous devrez également créer un registre de conteneurs élastiques (ECR) pour héberger les images d'Astra Control Center et les transmettre à ce registre.

Suivez la documentation AWS pour suivre la procédure ci-dessous. Voir "Documentation d'installation d'AWS".

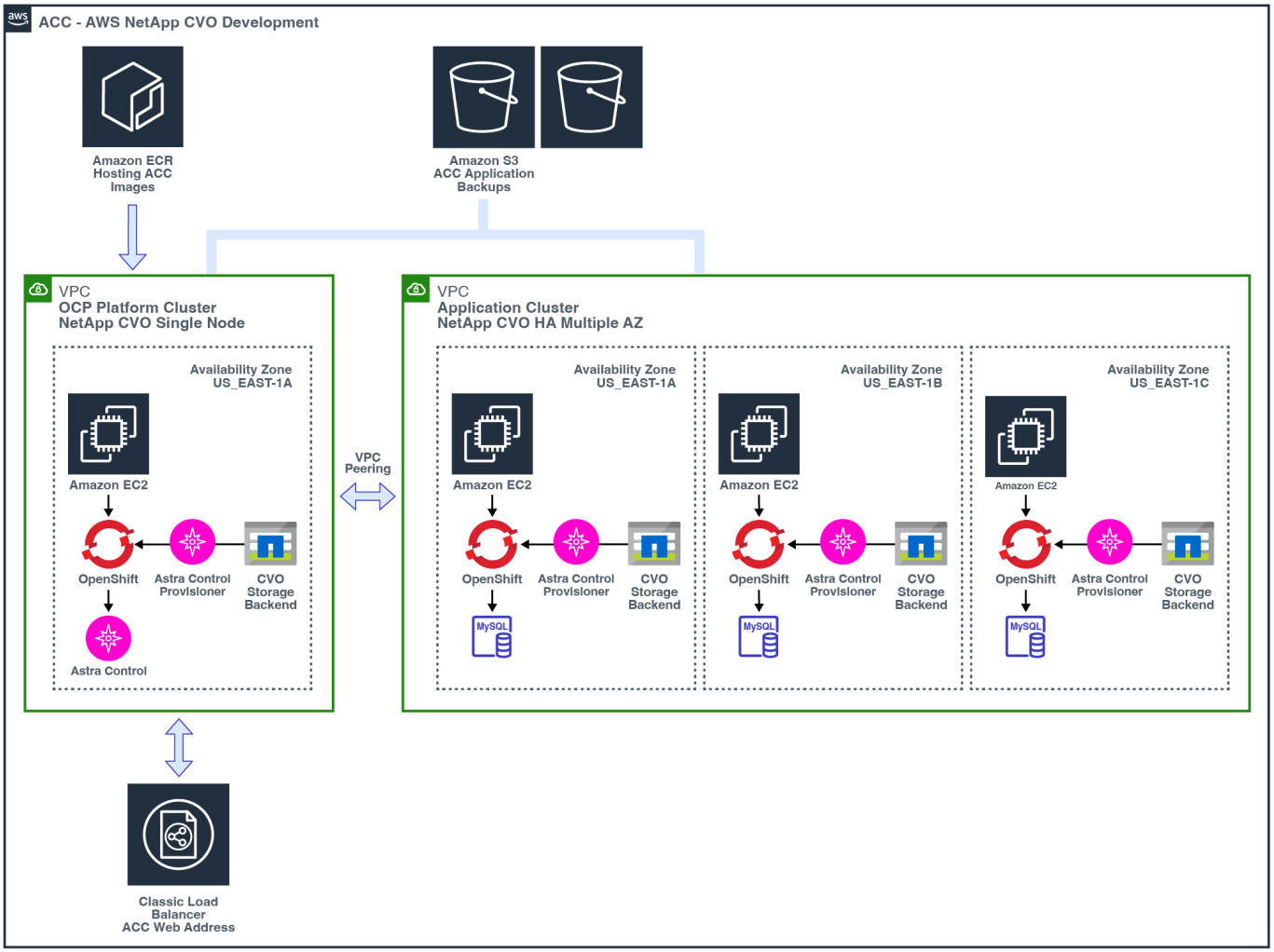
1. Créez un réseau virtuel AWS.
2. Vérifiez les instances de calcul EC2. Il peut s'agir d'un serveur bare Metal ou de machines virtuelles dans AWS.
3. Si le type d'instance ne correspond pas déjà aux exigences de ressources minimales Astra pour les nœuds maîtres et workers, modifiez le type d'instance dans AWS afin qu'il réponde aux exigences de l'Astra. Reportez-vous à la section "Exigences du centre de contrôle Astra".
4. Créez au moins un compartiment AWS S3 pour stocker vos sauvegardes.
5. (Facultatif) si vous ne pouvez pas accéder au registre d'images NetApp, procédez comme suit :
   a. Créez un registre AWS Elastic Container Registry (ECR) pour héberger toutes les images d'Astra Control Center.

      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.

   b. Envoyez les images d'Astra Control Center vers votre 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. Dans le coin supérieur droit, notez la version Astra Control Provisioner.

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.
   ASTRA Control provisionner est automatiquement installé dans le cadre du processus d'importation et de découverte.

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 devez disposer des éléments suivants :

- Licence Astra Control Center. Reportez-vous à la section "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) 4.11 à 4.13
- 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.

ASTRA Control Center requiert des ressources spécifiques en plus des besoins en ressources de l'environnement. Reportez-vous à la section "Exigences relatives à l'environnement opérationnel d'Astra Control Center".

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, configurer des instances de calcul et créer un stockage objet Google Cloud. Si vous ne pouvez pas accéder au registre d'images NetApp Astra Control Center, vous devrez également créer un registre de conteneurs Google pour héberger les images d'Astra Control Center et envoyer 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 minimales de ressources d'Astra pour les nœuds maîtres et workers, modifiez le type d'instance dans GCP pour répondre aux exigences d'Astra. Reportez-vous à la section "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. (Facultatif) si vous ne pouvez pas accéder au registre d'images NetApp, procédez comme suit :

    a. Créez un registre de conteneurs Google pour héberger les images d'Astra Control Center.
    b. 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 d'Astra Control Center peuvent être transmises à ce registre en saisissant 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=acc.manifest.bundle.yaml
GCP_CR_REGISTRY=<target GCP image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

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 < acc.manifest.bundle.yaml
```

7. 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".

Avant de commencer

- 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. Dans le coin supérieur droit, notez la version Astra Control Provisioner.
   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.
      ASTRA Control provisionner est automatiquement installé dans le cadre du processus d'importation et de découverte.
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. Reportez-vous à la section "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) 4.11 à 4.13
- 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.

ASTRA Control Center requiert des ressources spécifiques en plus des besoins en ressources de l'environnement. Reportez-vous à la section "Exigences relatives à l'environnement opérationnel d'Astra Control Center".

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, configurer des instances de calcul et créer un conteneur Azure Blob. Si vous ne pouvez pas accéder au registre d'images NetApp Astra Control Center, vous devez également créer un Registre de conteneurs Azure (ACR) pour héberger les images d'Astra Control Center et envoyer les images vers 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. Reportez-vous à la section "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. (Facultatif) si vous ne pouvez pas accéder au registre d'images NetApp, procédez comme suit :

    a. Créez un registre de conteneurs Azure (ACR) pour héberger les images d'Astra Control Center.

    b. Configurez l'accès ACR pour Docker Push/Pull pour toutes les images d'Astra Control Center.

    c. Envoyez les images d'Astra Control Center vers ce registre à l'aide du script suivant :

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

    Exemple :

```
manifestfile=acc.manifest.bundle.yaml
AZ_ACR_REGISTRY=<target Azure ACR image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

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 < acc.manifest.bundle.yaml
```

8. 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".

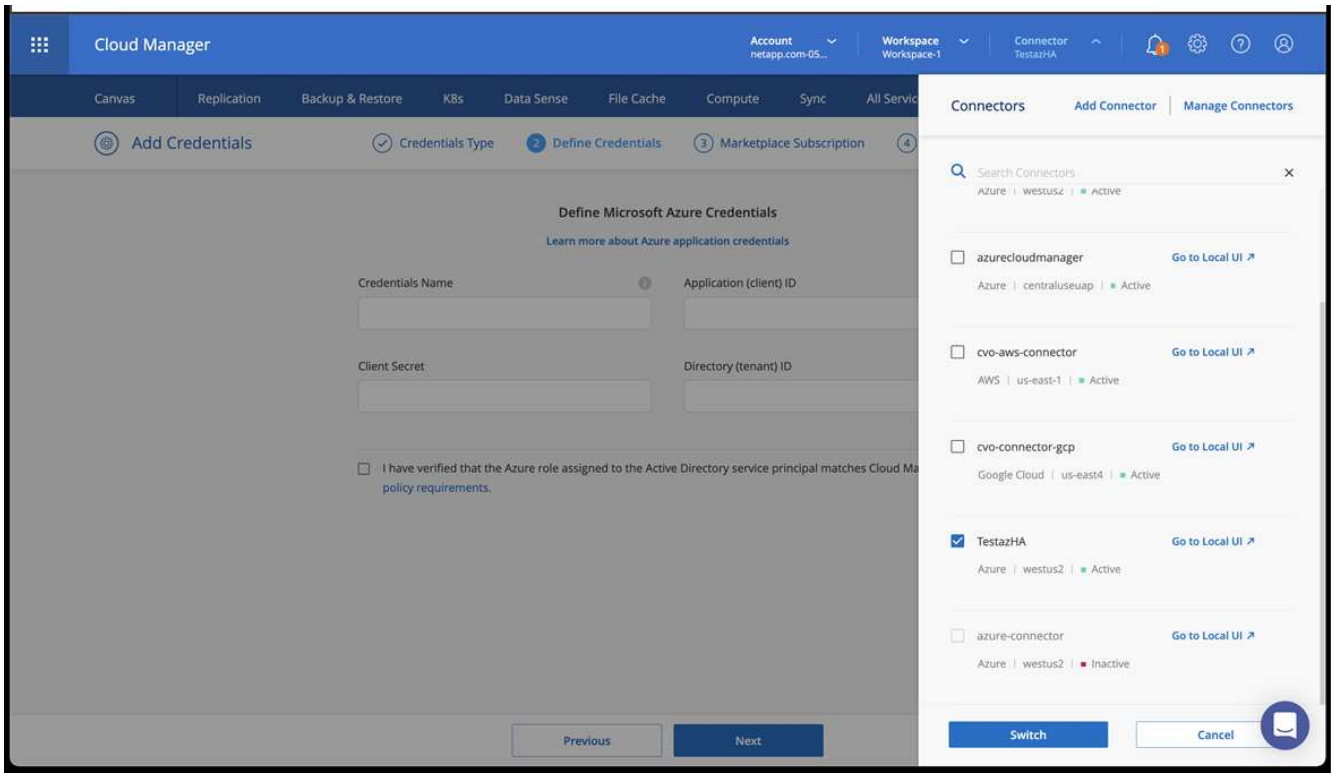
Avant de commencer

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

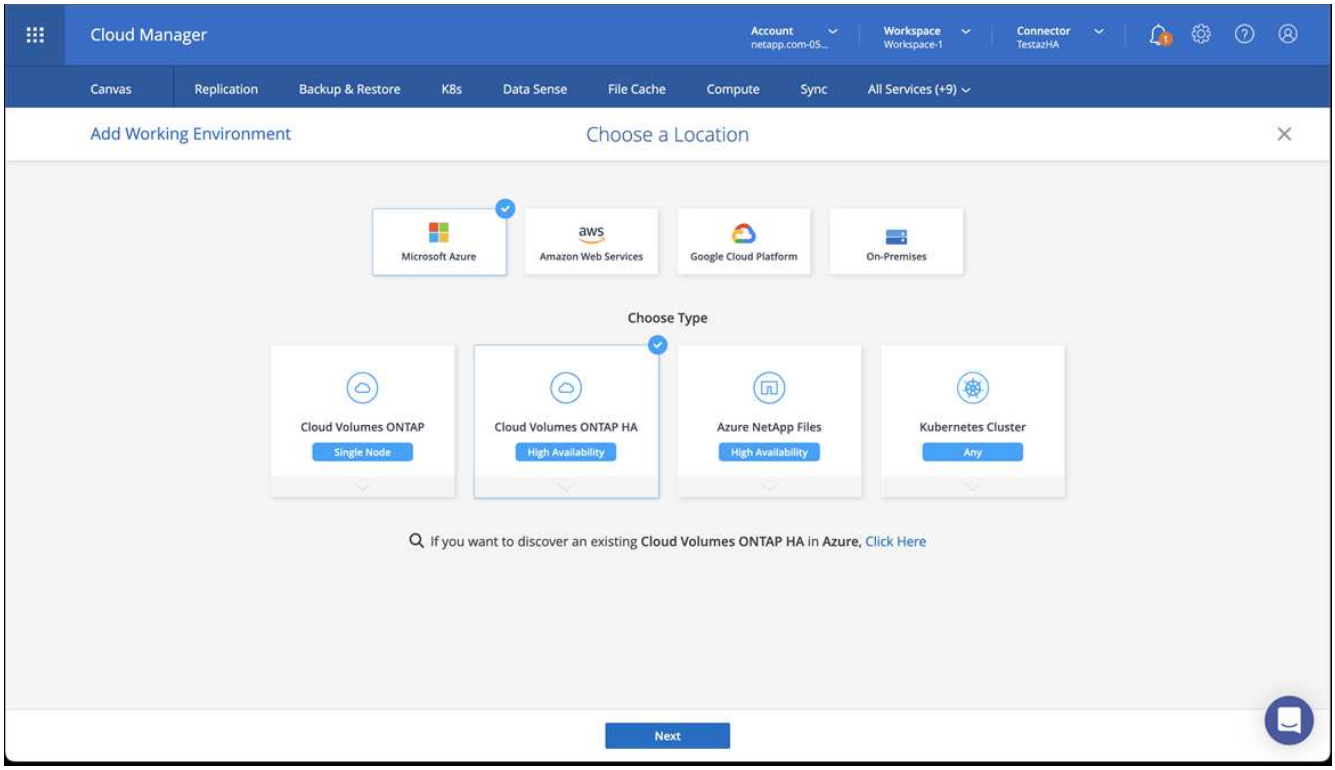
Étapes

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).

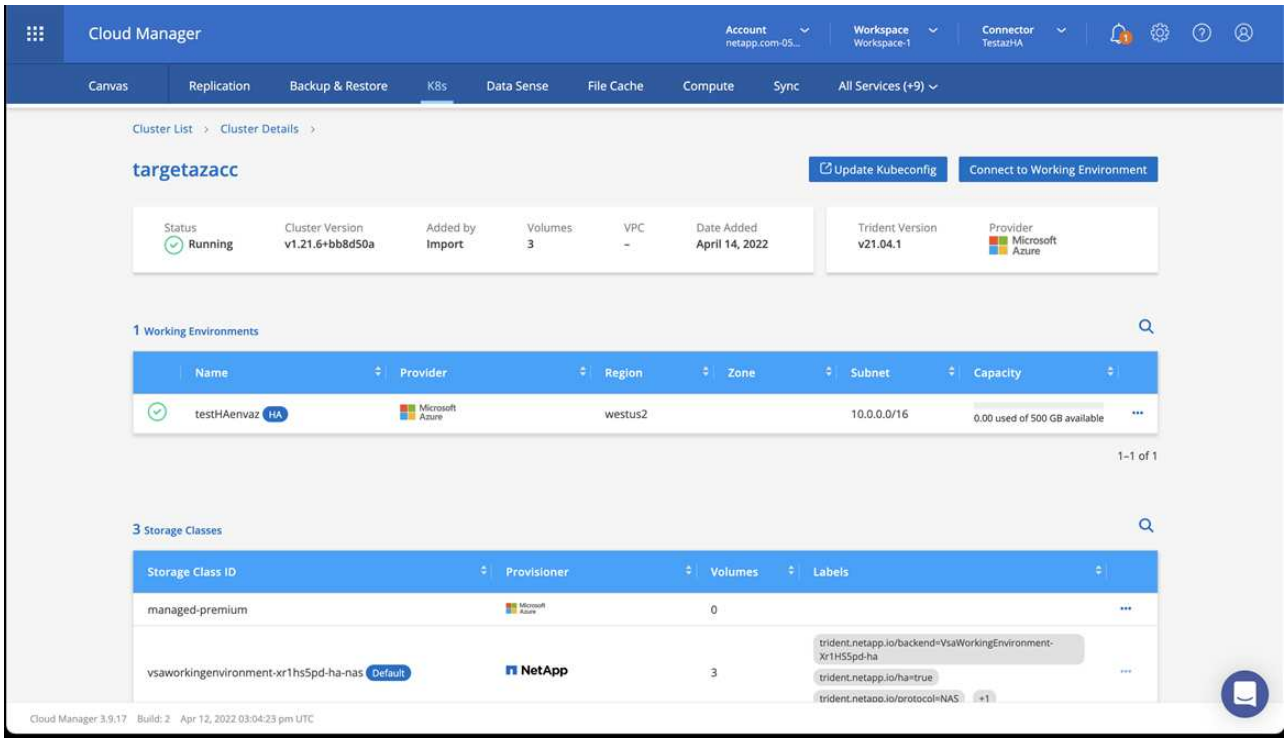
      Voir "Création d'un connecteur dans Azure à partir de BlueXPr".
3. S'assurer que le connecteur est en marche et basculer vers ce connecteur.



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. Dans le coin supérieur droit, notez la version Astra Control Provisioner.

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.
ASTRA Control provisionner est automatiquement installé dans le cadre du processus d'importation et de découverte.

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. Reportez-vous à la section "Configurer le centre de contrôle Astra et ajouter des seaux".

Configurer le centre de contrôle Astra après l'installation

En fonction de votre environnement, une configuration supplémentaire peut être nécessaire après l'installation d'Astra Control Center.

Supprimer les limitations de ressources

Certains environnements utilisent les objets ResourceQuotas et LimitRanges pour empêcher les ressources d'un namespace de consommer l'ensemble des CPU et de la mémoire disponibles sur le cluster. Le centre de contrôle Astra ne fixe pas de limites maximales, il ne sera donc pas conforme à ces ressources. Si votre environnement est configuré de cette façon, vous devez supprimer ces ressources des espaces de noms où

vous prévoyez d'installer Astra Control Center.

Vous pouvez suivre les étapes suivantes pour récupérer et supprimer ces quotas et ces limites. Dans ces exemples, la sortie de la commande est affichée immédiatement après la commande.

Étapes

1. Obtenez les quotas de ressources dans `netapp-acc` (ou nom-personnalisé) espace de noms :

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

Réponse :

```
NAME          AGE   REQUEST                                              LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. Supprimez tous les quotas de ressources par nom :

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom
namespace]
```

3. Obtenez les limites de la `netapp-acc` (ou nom-personnalisé) espace de noms :

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

Réponse :

```
NAME              CREATED AT
cpu-limit-range   2022-06-27T19:01:23Z
```

4. Supprimez les plages de limite par nom :

```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom
namespace]
```

Ajouter un certificat TLS personnalisé

Par défaut, Astra Control Center utilise un certificat TLS auto-signé pour le trafic du contrôleur d'entrée (uniquement dans certaines configurations) et l'authentification de l'interface utilisateur Web avec des navigateurs Web. Pour une utilisation en production, vous devez supprimer le certificat TLS auto-signé existant et le remplacer par un certificat TLS signé par une autorité de certification (CA).

> Le certificat auto-signé par défaut est utilisé pour deux types de connexions :
>
> - Connexions HTTPS à l'interface utilisateur Web Astra Control Center
> - Entrée du trafic du contrôleur (uniquement si le `ingressType: "AccTraefik"` la propriété a été définie dans `astra_control_center.yaml` Fichier lors de l'installation d'Astra Control Center)
>
> Le remplacement du certificat TLS par défaut remplace le certificat utilisé pour l'authentification pour ces connexions.

Avant de commencer

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

Supprimez le certificat auto-signé

Supprimez le certificat TLS auto-signé existant.

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

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

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

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

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

Ajoutez un nouveau certificat à l'aide de la ligne de commande

Ajoutez un nouveau certificat TLS signé par une autorité de certification.

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

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

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

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

CRD :

```
#spec:
#  selfSigned: {}

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

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

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

Réponse :

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

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

> Cet exemple utilise le `dnsNames` Propriété permettant de spécifier l'adresse DNS d'Astra Control Center. ASTRA Control Center ne prend pas en charge l'utilisation de la propriété Common Name (CN) pour spécifier l'adresse DNS.

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

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

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

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

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

Réponse :

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

7. Modifiez le TLS stocke CRD pour pointer vers votre nouveau nom de secret de certificat à l'aide de la commande et de l'exemple suivants, en remplaçant les valeurs d'espace réservé entre parenthèses <> par les informations appropriées

```
kubectl edit tlsstores.traefik.io -n <ACC-deployment-namespace>
```

CRD :

```
...
spec:
  defaultCertificate:
    secretName: <certificate-secret-name>
```

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

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

CRD :

```
...
 tls:
    secretName: <certificate-secret-name>
```

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

Configurer le centre de contrôle Astra

Ajoutez une licence pour Astra Control Center

Lorsque vous installez Astra Control Center, une licence d'évaluation intégrée est déjà installée. Si vous évaluez Astra Control Center, vous pouvez ignorer cette étape.

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

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".

Avant de commencer

- 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.

Activez le mécanisme de provisionnement Astra Control

Les versions 23.10 et ultérieures d'Astra Trident incluent la possibilité d'utiliser Astra Control Provisioner qui permet aux utilisateurs d'Astra Control sous licence d'accéder à des fonctionnalités avancées de provisionnement du stockage. ASTRA Control Provisioner offre cette fonctionnalité étendue en plus des fonctionnalités standard d'Astra Trident CSI.

Dans les prochaines mises à jour d'Astra Control, Astra Control Provisioner remplacera Astra Trident en tant que mécanisme de provisionnement et d'orchestration du stockage, et sera obligatoire pour l'utilisation d'Astra Control. Pour cette raison, il est fortement recommandé aux utilisateurs d'Astra Control d'activer Astra Control Provisioner. ASTRA Trident continuera à rester open source et sera publié, maintenu, pris en charge et mis à jour avec le nouveau CSI et d'autres fonctionnalités de NetApp.

Description de la tâche

Vous devez suivre cette procédure si vous êtes un utilisateur d'Astra Control Center sous licence et que vous cherchez à utiliser la fonctionnalité Astra Control Provisioner. Vous devez également suivre cette procédure si vous êtes un utilisateur d'Astra Trident et souhaitez utiliser les fonctionnalités supplémentaires d'Astra Control Provisioner sans également utiliser Astra Control.

Pour chaque cas, la fonctionnalité de provisionneur n'est pas activée par défaut dans Astra Trident 24.02 et doit être activée.

Avant de commencer

Si vous activez Astra Control Provisioner, effectuez d'abord les opérations suivantes :

ASTRA Control assure aux utilisateurs un provisionnement avec Astra Control Center

- **Obtenir une licence Astra Control Center** : vous aurez besoin d'une licence "Licence Astra Control Center" Pour activer le mécanisme de provisionnement Astra Control et accéder aux fonctionnalités qu'il fournit.
- **Installer ou mettre à niveau vers Astra Control Center 23.10 ou version ultérieure**: Vous aurez besoin de la dernière version d'Astra Control Center (24.02) si vous prévoyez d'utiliser la dernière fonctionnalité d'Astra Control Provisioner (24.02) avec Astra Control.
- **Confirmez que votre cluster a une architecture système AMD64** : l'image Astra Control Provisioner est fournie dans les architectures CPU AMD64 et ARM64, mais seul AMD64 est pris en charge par Astra Control Center.
- **Obtenez un compte Astra Control Service pour l'accès au registre**: Si vous avez l'intention d'utiliser le registre Astra Control plutôt que le site de support NetApp pour télécharger l'image Astra Control provisionner, effectuez l'enregistrement pour un "Compte Astra Control Service". Une fois que vous aurez rempli le formulaire, envoyé son formulaire et créé un compte BlueXP, vous recevrez un e-mail de bienvenue Astra Control Service.
- **Si vous avez installé Astra Trident, vérifiez que sa version se trouve dans une fenêtre à quatre versions**: Vous pouvez effectuer une mise à niveau directe vers Astra Trident 24.02 avec Astra Control Provisioner si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers la version 24.02.

Utilisateurs d'Astra Control Provisioner uniquement

- **Obtenir une licence Astra Control Center** : vous aurez besoin d'une licence "Licence Astra Control Center" Pour activer le mécanisme de provisionnement Astra Control et accéder aux fonctionnalités qu'il fournit.
- **Si vous avez installé Astra Trident, vérifiez que sa version se trouve dans une fenêtre à quatre versions**: Vous pouvez effectuer une mise à niveau directe vers Astra Trident 24.02 avec Astra Control Provisioner si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers la version 24.02.
- **Obtenez un compte Astra Control Service pour l'accès au registre**: Vous aurez besoin d'accéder au registre pour télécharger les images d'Astra Control provisionner. Pour commencer, terminez l'inscription à un "Compte Astra Control Service". Une fois que vous aurez rempli le formulaire, envoyé son formulaire et créé un compte BlueXP, vous recevrez un e-mail de bienvenue Astra Control Service.

(Étape 1) Obtenez l'image Astra Control Provisioner

Les utilisateurs d'Astra Control Center peuvent obtenir l'image d'Astra Control provisionner en utilisant le registre Astra Control ou la méthode du site de support NetApp. Les utilisateurs d'Astra Trident qui souhaitent utiliser Astra Control Provisioner sans Astra Control doivent utiliser la méthode de Registre.

Registre d'images Astra Control

> Vous pouvez utiliser Podman à la place de Docker pour les commandes de cette procédure. Si vous utilisez un environnement Windows, PowerShell est recommandé.

1. Accédez au registre d'images NetApp Astra Control :
   a. Connectez-vous à l'interface utilisateur Web d'Astra Control Service et sélectionnez l'icône de figure en haut à droite de la page.
   b. Sélectionnez **accès API**.
   c. Notez votre ID de compte.
   d. A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.
   e. Connectez-vous au registre Astra Control à l'aide de la méthode de votre choix :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Registres personnalisés uniquement) Suivez ces étapes pour déplacer l'image vers votre registre personnalisé. Si vous n'utilisez pas de registre, suivez les étapes de l'opérateur Trident dans le "section suivante".
   a. Extrayez l'image Astra Control Provisioner du Registre :

> L'image extraite ne prend pas en charge plusieurs plates-formes et ne prend en charge que la même plate-forme que l'hôte qui a extrait l'image, comme Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0 --platform <cluster platform>
```

   Exemple :

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0 --platform linux/amd64
```

   a. Marquer l'image :

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0 <my_custom_registry>/trident-acp:24.02.0
```

b. Envoyez l'image vers votre registre personnalisé :

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Vous pouvez utiliser Crane Copy comme alternative à l'exécution des commandes Docker suivantes :
`crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0 <my_custom_registry>/trident-acp:24.02.0`

Site de support NetApp

1. Téléchargez le bundle Astra Control Provisioner (`trident-acp-[version].tar`) du "Page de téléchargements d'Astra Control Center".
2. (Recommandé mais facultatif) Téléchargez le bundle de certificats et de signatures pour Astra Control Center (astra-control-Center-certs-[version].tar.gz) pour vérifier la signature du bundle trident-acp-[version] tar.

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

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Charger l'image Astra Control Provisioner :

```
docker load < trident-acp-24.02.0.tar
```

Réponse :

```
Loaded image: trident-acp:24.02.0-linux-amd64
```

4. Marquer l'image :

```
docker tag trident-acp:24.02.0-linux-amd64 <my_custom_registry>/trident-acp:24.02.0
```

5. Envoyez l'image vers votre registre personnalisé :

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

(Étape 2) Activer le provisionnement Astra Control dans Astra Trident

Déterminez si la méthode d'installation d'origine utilisait un "Opérateur (manuellement ou avec Helm) ou tridentctl" et suivez les étapes appropriées selon votre méthode d'origine.

Opérateur Astra Trident

1. "Téléchargez le programme d'installation d'Astra Trident et extrayez-le".
2. Si vous n'avez pas encore installé Astra Trident ou si vous avez supprimé l'opérateur de votre déploiement Astra Trident d'origine :
   a. Créez le CRD :

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Créer l'espace de nom trident (`kubectl create namespace trident`) ou confirmez que l'espace de nom trident existe toujours (`kubectl get all -n trident`). Si l'espace de noms a été supprimé, créez-le à nouveau.
3. Mettez à jour Astra Trident vers la version 24.02.0 :

> Pour les clusters exécutant Kubernetes 1.24 ou version antérieure, utilisez `bundle_pre_1_25.yaml`. Pour les clusters exécutant Kubernetes 1.25 ou version ultérieure, utilisez `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

4. Vérifiez que Astra Trident est en cours d'exécution :

```
kubectl get torc -n trident
```

   Réponse :

```
NAME      AGE
trident   21m
```

5. si vous avez un registre qui utilise des secrets, créez un secret à utiliser pour extraire l'image Astra Control Provisioner :

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Modifiez la CR TridentOrchestrator et apportez les modifications suivantes :

```
kubectl edit torc trident -n trident
```

a. Définissez un emplacement de Registre personnalisé pour l'image Astra Trident ou extrayez-le du Registre Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0` ou `tridentImage: netapp/trident:24.02.0`).

b. Activez le mécanisme de provisionnement Astra Control (`enableACP: true`).

c. Définissez l'emplacement de registre personnalisé pour l'image Astra Control Provisioner ou extrayez-le du registre Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0` ou `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).

d. Si vous avez établi secrets d'extraction d'image plus tôt dans cette procédure, vous pouvez les définir ici (`imagePullSecrets: - <secret_name>`). Utilisez le même nom secret que celui que vous avez établi lors des étapes précédentes.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

7. Enregistrez et quittez le fichier. Le processus de déploiement commence automatiquement.
8. Vérifiez que l'opérateur, le déploiement et les réplicateurs sont créés.

```
kubectl get all -n trident
```

> Il ne doit y avoir que **une instance** de l'opérateur dans un cluster Kubernetes. Ne créez pas plusieurs déploiements de l'opérateur Astra Trident.

9. Vérifiez le `trident-acp` le conteneur est en cours d'exécution `acpVersion` est `24.02.0` avec un état de `Installed`:

```
kubectl get torc -o yaml
```

Réponse :

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

1. "Téléchargez le programme d'installation d'Astra Trident et extrayez-le".
2. "Si vous disposez d'une Astra Trident, désinstallez-la du cluster qui l'héberge".
3. Installez Astra Trident avec Astra Control Provisioner activé (`--enable-acp=true`) :

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

4. Vérifiez que le mécanisme de provisionnement Astra Control a été activé :

```
./tridentctl -n trident version
```

Réponse :

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 24.02.0 | 24.02.0 | 24.02.0. | +----------------
+----------------+-------------+
```

Gouvernail

1. Si vous avez installé Astra Trident 23.07.1 ou une version antérieure, "désinstaller" l'opérateur et les autres composants.
2. Si votre cluster Kubernetes s'exécute sur la version 1.24 ou antérieure, supprimez la psp :

```
kubectl delete psp tridentoperatorpod
```

3. Ajout du référentiel Astra Trident Helm :

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-
chart
```

4. Mettre à jour le graphique Helm :

```
helm repo update netapp-trident
```

Réponse :

```
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. □Happy Helming!□
```

5. Répertorier les images :

```
./tridentctl images -n trident
```

Réponse :

```
| v1.28.0            | netapp/trident:24.02.0|
|                    | docker.io/netapp/trident-autosupport:24.02|
|                    | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                    | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                    | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                    | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                    | registry.k8s.io/sig-storage/csi-node-driver-
registrar:v2.10.0 |
|                    | netapp/trident-operator:24.02.0 (optional)
```

6. Vérifier que trident-Operator 24.02.0 est disponible :

```
helm search repo netapp-trident/trident-operator --versions
```

Réponse :

```
NAME                                CHART VERSION   APP VERSION
DESCRIPTION
netapp-trident/trident-operator 100.2402.0      24.02.0         A
```

7. Utiliser `helm install` et exécutez l'une des options suivantes qui incluent ces paramètres :
   - Un nom pour votre emplacement de déploiement
   - Version d'Astra Trident
   - Nom de l'image Astra Control Provisioner
   - Indicateur d'activation du provisionneur
   - (Facultatif) Un chemin de registre local. Si vous utilisez un registre local, votre "Images Trident" Peut être situé dans un registre ou dans des registres différents, mais toutes les images CSI doivent se trouver dans le même registre.
   - Espace de noms Trident

Options

- Images sans registre

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-acp:24.02.0
--set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Images dans un ou plusieurs registres

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Vous pouvez utiliser `helm list` pour vérifier les détails de l'installation tels que le nom, l'espace de noms, le graphique, l'état, la version de l'application, et numéro de révision.

Si vous rencontrez des problèmes pour déployer Trident à l'aide d'Helm, exécutez cette commande pour désinstaller complètement Astra Trident :

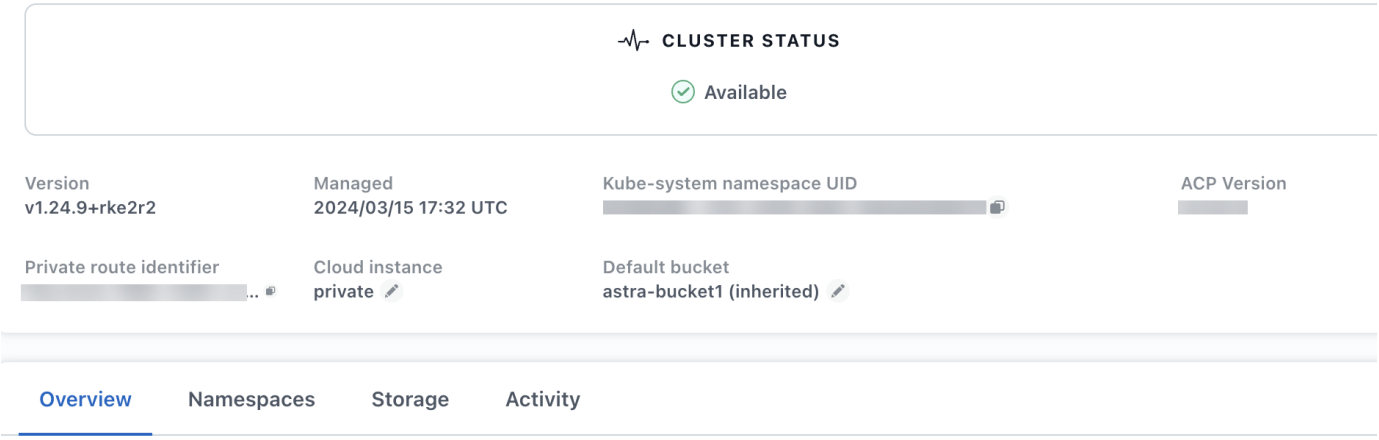
```
./tridentctl uninstall -n trident
```

Ne pas "Retirez complètement les CRD Astra Trident" Dans le cadre de votre désinstallation avant de tenter à nouveau d'activer Astra Control Provisioner.

Résultat

La fonctionnalité Astra Control Provisioner est activée et vous pouvez utiliser toutes les fonctions disponibles pour la version que vous exécutez.

(Pour les utilisateurs d'Astra Control Center uniquement) après l'installation d'Astra Control Provisioner, le cluster qui héberge le provisionneur dans l'interface utilisateur d'Astra Control Center affiche un `ACP version` plutôt que `Trident version` et le numéro de version actuellement installé.



Pour en savoir plus

- "Documentation sur les mises à niveau d'Astra Trident"

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 procéder à des vérifications d'éligibilité pour vous assurer que votre cluster est prêt à être ajouté à Astra Control Center et créer des rôles de cluster kubeconfig, si nécessaire.

ASTRA Control vous permet d'ajouter des clusters gérés par une ressource personnalisée (CR) ou un kubeconfig, en fonction de votre environnement et de vos préférences.

Avant de commencer

- **Respecter les conditions préalables environnementales** : votre environnement est conforme "de l'environnement opérationnel" Pour Astra Control Center.
- **Configurer les nœuds de travail** : assurez-vous que vous "configurez les nœuds worker" dans votre cluster avec les pilotes de stockage appropriés afin que les pods puissent interagir avec le stockage back-end.
- **Activer les restrictions PSA** : si l'application d'admission de sécurité du pod est activée sur votre cluster, ce qui est standard pour les clusters Kubernetes 1.25 et versions ultérieures, vous devez activer les restrictions PSA sur ces espaces de noms :
  - `netapp-acc-operator` espace de noms :

```
kubectl label --overwrite ns netapp-acc-operator pod-
security.kubernetes.io/enforce=privileged
```

- `netapp monitoring` espace de noms :

```
kubectl label --overwrite ns netapp-monitoring pod-
security.kubernetes.io/enforce=privileged
```

- **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
```

- **Configuration requise pour les clusters gérés par kubeconfig** : ces exigences sont spécifiques pour les clusters d'applications gérés par kubeconfig.
  - **Rendre kubeconfig. accessible**: Vous avez accès au "configuration par défaut du cluster" ça "vous avez configuré lors de l'installation".
  - **Considérations relatives à l'autorité de certification** : si vous ajoutez le cluster à l'aide d'un fichier kubeconfig qui fait référence à une autorité de certification privée (AC), ajoutez la ligne suivante au `cluster` section du fichier kubeconfig. Cela permet à Astra Control d'ajouter le cluster :

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

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

- **Configurer un back-end de stockage** : au moins un back-end de stockage doit l'être "Configuré dans Astra Trident" sur le cluster.
- **Configurer une classe de stockage** : au moins une classe de stockage doit être "Configuré dans Astra Trident" sur le cluster. Si une classe de stockage par défaut est configurée, assurez-vous qu'il s'agit de la classe de stockage **Only** qui possède l'annotation par défaut.
- **Configurer un contrôleur de snapshot de volume et installer une classe de snapshot de volume** : "Installez un contrôleur de snapshot de volume" Il est ainsi possible de créer des snapshots dans Astra Control. "Création" au moins un `VolumeSnapshotClass` Avec Astra Trident.

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

   ```
   kubectl get tridentversion -n trident
   ```

   Si Astra Trident existe, le résultat de cette commande est similaire à ce qui suit :

   ```
   NAME      VERSION
   trident   24.02.0
   ```

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

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

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

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

4. Déterminez si les classes de stockage utilisent les pilotes Astra 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 kubeconfig pour le rôle de cluster

Pour les clusters gérés à l'aide de kubeconfig, vous pouvez éventuellement créer une autorisation limitée ou un rôle d'administrateur d'autorisations étendues pour Astra Control Center. Il ne s'agit pas d'une procédure requise pour la configuration d'Astra Control Center, car vous avez déjà configuré un kubeconfig dans le cadre du "processus d'installation".

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

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

Avant de commencer

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

- 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`.

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

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

b. Appliquer le compte de service :

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

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

Rôle limité du cluster

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

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

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

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

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

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

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

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

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

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

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

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

c. Appliquer le rôle de cluster :

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

Rôle de cluster étendu

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

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

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

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

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

b. Appliquer le rôle de cluster :

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

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

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

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

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

b. Appliquer la liaison de rôle de cluster :

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

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

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

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

   b. Appliquer le secret de jeton :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token-
user

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

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

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

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

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

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

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

(Aperçu technique) installez Astra Connector pour les clusters gérés

Les clusters gérés par Astra Control Center utilisent Astra Connector pour faciliter la communication entre le cluster géré et Astra Control Center. Vous devez installer Astra Connector sur tous les clusters que vous souhaitez gérer.

Poser le connecteur Astra

Vous installez Astra Connector à l'aide des commandes Kubernetes et des fichiers de ressources personnalisées (CR).

Description de la tâche

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

Avant de commencer

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

Si le cluster est configuré avec l'application d'admission de la sécurité du pod, c'est-à-dire la configuration par défaut pour les clusters Kubernetes 1.25 et versions ultérieures, vous devez activer les restrictions PSA sur les espaces de noms appropriés. Reportez-vous à la section "Préparez votre environnement à la gestion des clusters avec Astra Control" pour obtenir des instructions.

Étapes

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

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

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

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

3. Obtenez un jeton API d'Astra Control. Reportez-vous à la "Documentation relative à l'automatisation d'Astra" pour obtenir des instructions.
4. Créez un secret à l'aide du jeton. Remplacez <API_TOKEN> par le jeton que vous avez reçu d'Astra Control :

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Créez un secret Docker à utiliser pour extraire l'image du connecteur Astra. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

<ASTRA_CONTROL_ACCOUNT_ID> est disponible dans l'interface utilisateur web d'Astra Control. Dans l'interface utilisateur Web, sélectionnez l'icône figure en haut à droite de la page et sélectionnez **accès API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Créez le fichier CR du connecteur Astra et nommez-le `astra-connector-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :

- <ASTRA_CONTROL_ACCOUNT_ID> : obtenu à partir de l'interface utilisateur web d'Astra Control au cours de l'étape précédente.
- <CLUSTER_NAME> : nom que ce cluster doit être attribué dans Astra Control.
- <ASTRA_CONTROL_URL> : l'URL de l'interface utilisateur Web d'Astra Control. Par exemple :

```
https://astra.control.url
```

```
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

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

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

8. Vérifier que le connecteur Astra est entièrement déployé :

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

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

```
kubectl get astraconnectors.astra.netapp.io -A
```

Vous devez voir les résultats similaires à ce qui suit :

```
NAMESPACE         NAME              REGISTERED   ASTRACONNECTORID
STATUS
astra-connector   astra-connector   true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Vérifiez que le cluster s'affiche dans la liste des clusters gérés sur la page **clusters** de l'interface utilisateur Web d'Astra Control.

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.

Avant de commencer

- Avant d'ajouter un cluster, vérifiez et effectuez les opérations nécessaires "tâches préalables".
- Si vous utilisez un pilote SAN ONTAP, assurez-vous que les chemins d'accès multiples sont activés sur tous vos clusters Kubernetes.

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 "ce processus", 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 configurée dans Astra Control Provisioner et prise en charge 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.

Activez l'authentification sur un système back-end de stockage ONTAP

ASTRA Control Center offre deux modes d'authentification d'un backend ONTAP :

- **Authentification basée sur les informations d'identification** : le nom d'utilisateur et le mot de passe d'un utilisateur ONTAP avec les autorisations requises. Vous devez utiliser un rôle de connexion de sécurité prédéfini, tel que admin ou vsadmin, pour assurer une compatibilité maximale avec les versions de ONTAP.
- **Authentification basée sur un certificat** : Astra Control Center peut également communiquer avec un cluster ONTAP à l'aide d'un certificat installé sur le back-end. Vous devez utiliser le certificat client, la clé et le certificat de l'autorité de certification approuvée, le cas échéant (recommandé).

Vous pouvez par la suite mettre à jour les systèmes back-end existants pour passer d'un type d'authentification à une autre. Une seule méthode d'authentification est prise en charge à la fois.

Activer l'authentification basée sur les informations d'identification

ASTRA Control Center requiert les identifiants d'un cluster-scoped `admin` Pour communiquer avec le backend ONTAP. Vous devez utiliser des rôles standard prédéfinis, tels que `admin`. La compatibilité avec les futures versions d'ONTAP qui pourraient exposer les API de fonctionnalités à utiliser dans les futures versions d'Astra Control Center est ainsi garantie.

> Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Astra Control Center, mais il n'est pas recommandé.

Un exemple de définition de back-end se présente comme suit :

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

La définition du back-end est le seul endroit où les informations d'identification sont stockées en texte brut. La création ou la mise à jour d'un back-end est la seule étape qui nécessite la connaissance des informations d'identification. Il s'agit donc d'une opération réservée à l'administrateur du stockage ou de Kubernetes.

Activer l'authentification basée sur certificat

ASTRA Control Center peut utiliser des certificats pour communiquer avec les systèmes back-end ONTAP, nouveaux et existants. Vous devez entrer les informations suivantes dans la définition du back-end.

- `clientCertificate`: Certificat client.
- `clientPrivateKey`: Clé privée associée.
- `trustedCACertificate`: Certificat de l'autorité de certification approuvée. Si vous utilisez une autorité de certification approuvée, ce paramètre doit être fourni. Ceci peut être ignoré si aucune autorité de certification approuvée n'est utilisée.

Vous pouvez utiliser l'un des types de certificats suivants :

- Certificat auto-signé
- Certificat tiers

Activez l'authentification avec un certificat auto-signé

Un flux de travail type comprend les étapes suivantes.

Étapes

1. Générez un certificat client et une clé. Lors de la génération, définissez le nom commun (CN) sur l'utilisateur ONTAP pour s'authentifier en tant que.

   ```
   openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
   -out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
   ```

2. Installez le certificat client de type `client-ca` Et sur le cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Vérifiez que le rôle de connexion de sécurité ONTAP prend en charge la méthode d'authentification par certificat.

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

4. Tester l'authentification à l'aide du certificat généré. Remplacer <LIF> et <vserver name> de ONTAP par l'IP et le nom du SVM de la LIF de gestion. Vous devez vous assurer que le LIF a sa politique de service définie sur `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-
name>"><vserver-get></vserver-get></netapp>
```

5. À l'aide des valeurs obtenues à l'étape précédente, ajoutez le back-end de stockage dans l'interface utilisateur d'Astra Control Center.

Activez l'authentification à l'aide d'un certificat tiers

Si vous disposez d'un certificat tiers, vous pouvez configurer l'authentification basée sur un certificat à l'aide de ces étapes.

Étapes

1. Générer la clé privée et la RSC :

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem
-out ontap_cert_request.csr -keyout ontap_cert_request.key -addext
"subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>”
```

2. Transmettez la RSC à l'autorité de certification Windows (autorité de certification tierce) et émettez le certificat signé.
3. Téléchargez le certificat signé et nommez-le « ontap_signed_cert.crt ».
4. Exportez le certificat racine à partir de l'autorité de certification Windows (autorité de certification tierce).
5. Nommez ce fichier `ca_root.crt`

   Vous disposez maintenant des trois fichiers suivants :

- **Clé privée** : `ontap_signed_request.key` (Il s'agit de la clé correspondante pour le certificat de serveur dans ONTAP. Elle est nécessaire lors de l'installation du certificat du serveur.)
- **Certificat signé**: `ontap_signed_cert.crt` (Il s'agit également du *certificat de serveur* dans ONTAP.)
- **Certificat CA racine** : `ca_root.crt` (Il s'agit également du certificat *Server-ca* dans ONTAP.)

6. Installez ces certificats dans ONTAP. Générer et installer `server` et `server-ca` Certificats sur ONTAP.

Développez pour Sample.yaml

```
# Copy the contents of ca_root.crt and use it here.

security certificate install -type server-ca

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:

CA:
serial:

The certificate's generated name for reference:


===

# Copy the contents of ontap_signed_cert.crt and use it here. For
key, use the contents of ontap_cert_request.key file.
security certificate install -type server
Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN PRIVATE KEY-----
<private key details>
-----END PRIVATE KEY-----

Enter certificates of certification authorities (CA) which form the
certificate chain of the server certificate. This starts with the
issuing CA certificate of the server certificate and can range up to
the root CA certificate.
Do you want to continue entering root and/or intermediate
```

```
certificates {y|n}: n

The provided certificate does not have a common name in the subject
field.
Enter a valid common name to continue installation of the
certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
The installed certificate's CA and serial number for reference:
CA:
serial:
The certificate's generated name for reference:


==
# Modify the vserver settings to enable SSL for the installed
certificate

ssl modify -vserver <vserver_name> -ca <CA>  -server-enabled true
-serial <serial number>       (security ssl modify)

==
# Verify if the certificate works fine:

openssl s_client -CAfile ca_root.crt -showcerts -servername server
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
CONNECTED(00000005)
depth=1 DC = local, DC = umca, CN = <CA>
verify return:1
depth=0
verify return:1
write W BLOCK
---
Certificate chain
0 s:
   i:/DC=local/DC=umca/<CA>

-----BEGIN CERTIFICATE-----
<Certificate details>
```

7. Créez le certificat client pour le même hôte pour la communication sans mot de passe. ASTRA Control Center utilise ce processus pour communiquer avec ONTAP.
8. Générer et installer les certificats client sur ONTAP :

Développez pour Sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"

Copy the content of ontap_test_client.pem file and use it in the
below command:
security certificate install -type client-ca -vserver <vserver_name>

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<Certificate details>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
The installed certificate's CA and serial number for reference:

CA:
serial:
The certificate's generated name for reference:


==

ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)

# Setting permissions for certificates
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>

security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>

==

#Verify passwordless communication works fine with the use of only
certificates:

curl --cacert ontap_signed_cert.crt  --key ontap_test_client.key
--cert ontap_test_client.pem
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
{
```

```
"records": [
{
"uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
"name": "<aggr_name>",
"node": {
"uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
"name": "<node_name>",
"_links": {
"self": {
"href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
}
}
},
"_links": {
"self": {
"href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-
4bf5378b41bd"
}
}
}
],
"num_records": 1,
"_links": {
"self": {
"href": "/api/storage/aggregates"
}
}
}%
```


9. Ajoutez le système back-end de stockage dans l'interface utilisateur d'Astra Control Center et fournissez les valeurs suivantes :
   - **Certificat client** : ontap_test_client.pem
   - **Clé privée** : ontap_test_client.key
   - **Certificat CA de confiance** : ontap_signed_cert.crt

Ajout d'un système back-end

Après avoir configuré les informations d'identification ou d'authentification de certificat, vous pouvez ajouter un système back-end de stockage ONTAP existant 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.

L'ajout et la gestion de systèmes back-end de stockage ONTAP dans Astra Control Center sont facultatifs si

vous utilisez la technologie NetApp SnapMirror si vous avez activé Astra Control Provisioner.

Étapes

1. Dans la zone de navigation gauche du tableau de bord, sélectionnez **Backends**.
2. Sélectionnez **Ajouter**.
3. Dans la section utiliser existant de la page Ajouter un back-end de stockage, sélectionnez **ONTAP**.
4. Sélectionnez l'une des options suivantes :
   - **Utiliser les informations d'identification de l'administrateur** : saisissez l'adresse IP de gestion du cluster ONTAP et les informations d'identification de l'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.

   - **Utiliser un certificat**: Télécharger le certificat `.pem` fichier, la clé de certificat `.key` et éventuellement le fichier de l'autorité de certification.
5. Sélectionnez **Suivant**.
6. Confirmez les détails du back-end et sélectionnez **gérer**.

Résultat

Le back-end s'affiche dans le `online` 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 de contrôle Astra". 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.

Avant de commencer

- Assurez-vous que vous disposez d'un compartiment accessible depuis vos clusters gérés par Astra Control Center.
- Vérifiez que vous disposez des informations d'identification pour le compartiment.
- S'assurer que le godet est de l'un 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".

Concepts

Architecture et composants

Astra Control est une solution de gestion du cycle de vie des données d'application Kubernetes qui simplifie les opérations pour les applications avec état et vous aide à stocker, protéger et déplacer vos charges de travail Kubernetes dans des environnements hybrides.

Capacités

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

Magasin :

- Provisionnement de stockage dynamique pour les workloads conteneurisés
- Chiffrement à la volée des données du conteneur vers les volumes persistants
- Réplication entre régions et zones

Protéger :

- Détection automatisée et protection respectueuse des applications pour l'ensemble d'une application et de ses données
- Restauration instantanée d'une application à partir de n'importe quelle version de snapshot en fonction des besoins de votre organisation
- Basculement rapide dans les zones, les régions et les fournisseurs de cloud

Déplacer :

- Mobilité complète des applications et des données dans et entre les clusters Kubernetes et les clouds
- Des clones instantanés des applications et des données entières
- Migration des applications en un clic via une interface utilisateur Web et une API cohérentes

Architecture

L'architecture d'Astra Control permet aux équipes IT de proposer des fonctionnalités avancées de gestion des données qui améliorent à la fois les fonctionnalités et la disponibilité des applications Kubernetes, simplifient la gestion, la protection et le déplacement des workloads conteneurisés dans les clouds publics et les environnements sur site. il offre également des fonctionnalités d'automatisation via son API REST et son SDK, qui permettent un accès par programmation pour une intégration transparente avec les workflows déjà en place.

ASTRA Control est natif de Kubernetes, ce qui permet des workflows de protection des données qui utilisent des ressources personnalisées tout en restant rétrocompatible avec l'API et le kit de développement logiciel existants. La protection native des données Kubernetes offre des avantages considérables. En s'intégrant de manière transparente avec les API et les ressources Kubernetes, la protection des données peut devenir inhérente au cycle de vie des applications, via les outils ci/CD et/ou GitOps d'une entreprise.

ASTRA Control est basé sur quatre composants complémentaires :

- **Astra Control** : Astra Control est le service de gestion centralisé pour tous les clusters gérés, fournissant des charges de travail orchestrées pour la protection et la mobilité des applications sur site ainsi que les fonctionnalités suivantes :
  - Vue combinée de plusieurs clusters
  - Protection des workflows orchestrés
  - Visualisation et sélection granulaires des ressources
- **Astra Connector** : Astra Connector s'associe à Astra Control pour fournir une connexion sécurisée à chaque cluster géré, offrant ainsi une exécution locale des opérations planifiées, quel que soit l'état de la connexion, ainsi que les fonctionnalités suivantes :
  - Exécution locale des opérations planifiées quel que soit l'état de la connexion
  - Opérations locales qui distribuent et optimisent l'utilisation des ressources système d'Astra sur les clusters
  - Installation locale qui active un accès avec le moins de privilèges possible au cluster pour une sécurité améliorée
- **Astra Control Provisioner** : Astra Control Provisioner fournit des fonctionnalités de provisionnement CSI de base et des capacités de gestion de stockage avancées pour une configuration de sécurité et de reprise après incident accrue, ainsi que les fonctionnalités suivantes :
  - Provisionnement de stockage dynamique pour les workloads conteneurisés
  - Gestion avancée du stockage :
    - Chiffrement à la volée des données du conteneur vers le volume persistant
    - Fonctionnalité SnapMirror Cloud avec réplication entre régions et zones
- **Astra Ressources personnalisées** : les ressources personnalisées utilisées sur chaque cluster offrent une approche Kubernetes native pour exécuter les opérations localement, simplifier l'intégration avec d'autres outils et l'automatisation compatibles Kubernetes, ainsi que les fonctionnalités suivantes :
  - Intégration directe des outils de l'écosystème et automatisation des workflows
  - Primitives de niveau inférieur permettant d'activer des flux de travail personnalisés

Modèles de déploiement

Astra Control est disponible dans un modèle de déploiement unique.

Astra Control Center : logiciel autogéré qui assure une gestion des données compatible avec les applications de clusters Kubernetes exécutés dans votre environnement sur site. Astra Control Center peut également être installé sur plusieurs environnements de fournisseur cloud avec un système back-end de stockage NetApp Cloud Volumes ONTAP.

"Documentation Astra Control Center"

	Centre de contrôle Astra
Comment est-elle proposée ?	En tant que logiciel que vous pouvez télécharger, installer et gérer
Où est-il hébergé ?	Sur votre cluster Kubernetes
Comment est-elle mise à jour ?	Vous gérez toutes les mises à jour

	Centre de contrôle Astra
Quelles sont les distributions Kubernetes prises en charge ?	• Azure Kubernetes Service sur Azure Stack HCI • Anthos de Google • Kubernetes (en amont) • Rancher Kubernetes Engine (RKE) • Plateforme de conteneurs Red Hat OpenShift
Quels sont les systèmes back-end pris en charge ?	• Systèmes NetApp ONTAP AFF et FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Pour en savoir plus

- "Documentation Astra Control Center"
- "Documentation Astra Trident"
- "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 sauvegardées pour être restaurées. Un snapshot ne vous permettrait pas de restaurer.

Sauvegardes immuables

Une sauvegarde immuable est une sauvegarde qui ne peut pas être modifiée ou supprimée au cours d'une période spécifiée. Lorsque vous créez une sauvegarde immuable, Astra Control vérifie que le compartiment que vous utilisez est un compartiment WORM (Write Once, Read Many) et, si oui, vérifie que la sauvegarde est immuable depuis Astra Control.
ASTRA Control Center prend en charge la création de sauvegardes immuables avec les plateformes et les types de compartiments suivants :

- Amazon Web Services utilisant un compartiment Amazon S3 avec le verrouillage objet S3 configuré
- NetApp StorageGRID utilisant un compartiment S3 avec verrouillage objet S3 configuré

Notez les points suivants lorsque vous travaillez avec des sauvegardes immuables :

- Si vous effectuez une sauvegarde vers un compartiment WORM sur une plateforme non prise en charge ou vers un type de compartiment non pris en charge, vous risquez d'obtenir des résultats imprévisibles, comme la suppression de la sauvegarde, même si le temps de conservation est écoulé.
- ASTRA Control ne prend pas en charge les politiques de gestion du cycle de vie des données ni la suppression manuelle d'objets dans les compartiments que vous utilisez avec des sauvegardes immuables. Assurez-vous que votre système back-end de stockage n'est pas configuré pour gérer le cycle de vie des snapshots Astra Control ou des données sauvegardées.

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 entre les systèmes back-end

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 configuré, vos applications peuvent répliquer les modifications des données et des applications d'un système back-end de stockage vers un autre, sur le même cluster ou entre différents clusters.

Vous pouvez répliquer des données entre deux SVM ONTAP sur le même cluster ONTAP ou sur différents clusters ONTAP.

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

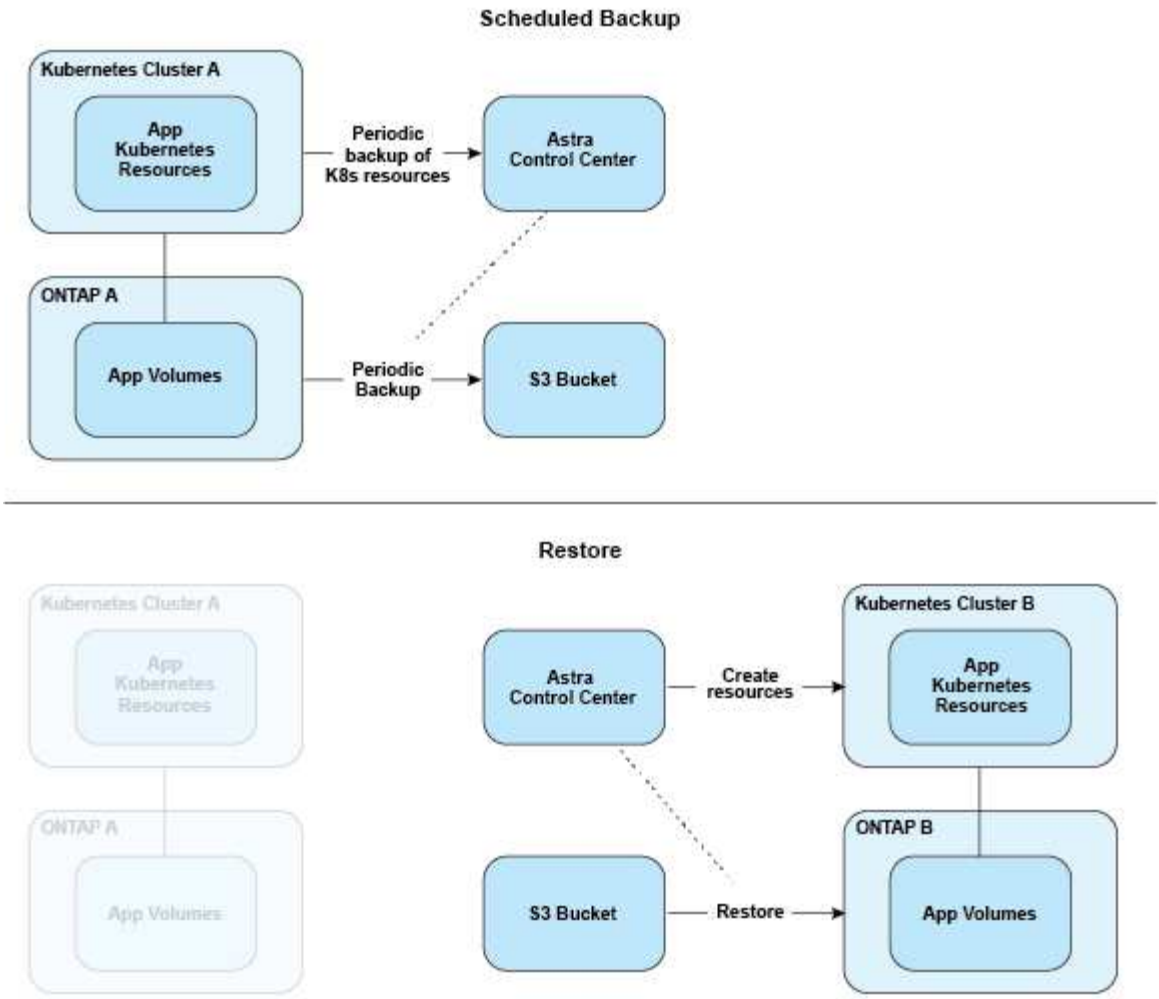
La réplication d'application est différente de la sauvegarde et de la restauration de l'application de la manière suivante :

- **Réplication d'applications** : Astra Control requiert que les clusters Kubernetes source et de destination (qui peuvent être le même cluster) soient disponibles et gérés avec leurs systèmes back-end de stockage ONTAP respectifs configurés pour activer NetApp SnapMirror. ASTRA Control utilise le Snapshot d'application piloté par des règles et le réplique vers le système de stockage back-end de destination. La technologie SnapMirror de NetApp 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. Les données du volume persistant étant déjà présentes sur le cluster ONTAP de destination, Astra Control peut offrir des délais de restauration rapides pour le basculement.
- **Sauvegarde et restauration des applications** : lors de la sauvegarde des applications, Astra Control crée un snapshot des données d'application et les 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.

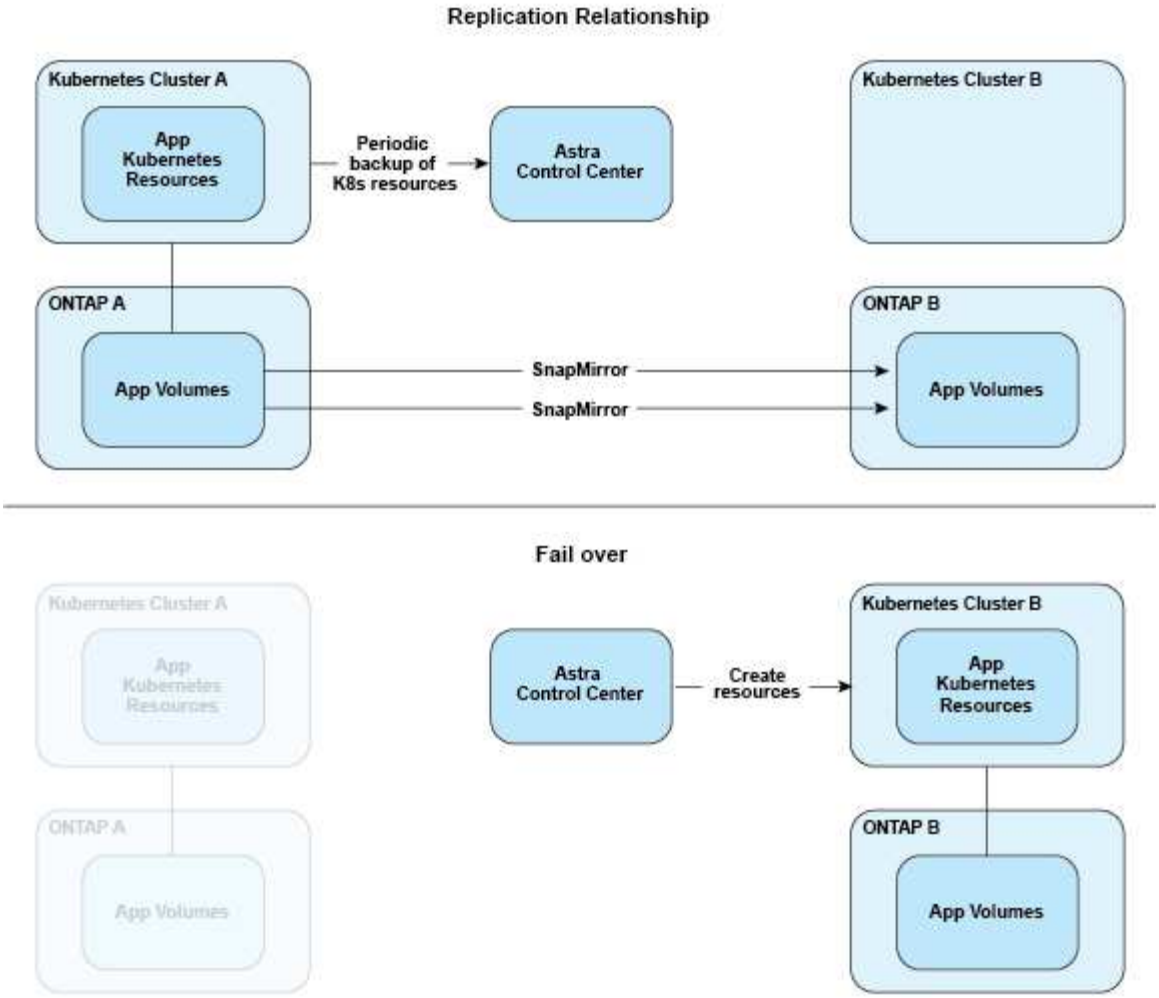
Pour savoir comment répliquer des applications, reportez-vous à la section "Répliquez vos applications sur un système distant grâce à la technologie SnapMirror".

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 :



Par contre, la réplication s'effectue via la réplication vers ONTAP, puis un basculement crée les ressources Kubernetes :



Sauvegardes, snapshots et clones avec une licence expirée

Si votre licence expire, vous pouvez ajouter une nouvelle application ou effectuer des opérations de protection des applications (telles que les copies Snapshot, les sauvegardes, les clones et les opérations de restauration) uniquement si l'application que vous ajoutez ou protégez est une autre instance d'Astra Control Center.

Licences

Lorsque vous déployez Astra Control Center, il est installé avec une licence d'évaluation intégrée de 90 jours pour 4,800 unités centrales. Si vous avez besoin de plus de capacité ou d'une période d'évaluation plus longue, ou si vous souhaitez effectuer une mise à niveau vers une licence complète, vous pouvez obtenir une autre licence d'évaluation ou une licence complète auprès de NetApp.

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

- Si vous évaluez Astra Control Center et que vous avez besoin de termes d'évaluation différents de ceux inclus dans la licence d'évaluation intégrée, contactez NetApp pour demander un fichier de licence d'évaluation différent.
- "Si vous avez déjà acheté Astra Control Center, générez votre fichier de licence NetApp (NLF)" En vous connectant au site du support NetApp et en accédant à vos licences logicielles via le menu systèmes.

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".

> Assurez-vous que votre licence active au moins autant d'UC que nécessaire. Si le nombre d'UC actuellement gérées par Astra Control Center dépasse les UC disponibles dans la nouvelle licence en cours d'application, vous ne pourrez pas appliquer la nouvelle licence.

Licences d'évaluation et licences complètes

Une licence d'évaluation intégrée est fournie avec une nouvelle installation d'Astra Control Center. Une licence d'évaluation offre les mêmes fonctionnalités qu'une licence complète pour une période limitée (90 jours). Après la période d'évaluation, une licence complète est requise pour continuer à bénéficier de toutes les fonctionnalités.

Expiration de la licence

Si la licence Astra Control Center active expire, l'interface utilisateur et les fonctionnalités d'API des fonctionnalités suivantes ne sont pas disponibles :

- Snapshots et sauvegardes locaux manuels
- Snapshots et sauvegardes locaux programmés
- Restauration à partir d'un snapshot ou d'une sauvegarde
- Clonage à partir d'un snapshot ou état actuel
- Gestion de nouvelles applications
- Configuration des règles de réplication

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 de processeur de ce cluster sont incluses dans la consommation de licence Astra Control Center, à l'exception des unités de processeur de nœud de cluster Red Hat OpenShift signalées par un à l'aide du libellé `node-role.kubernetes.io/infra: ""`.

> Les nœuds d'infrastructure Red Hat OpenShift ne consomment pas de licences dans Astra Control Center. Pour marquer un nœud en tant que nœud d'infrastructure, appliquez le libellé `node-role.kubernetes.io/infra: ""` au nœud.

Trouvez plus d'informations

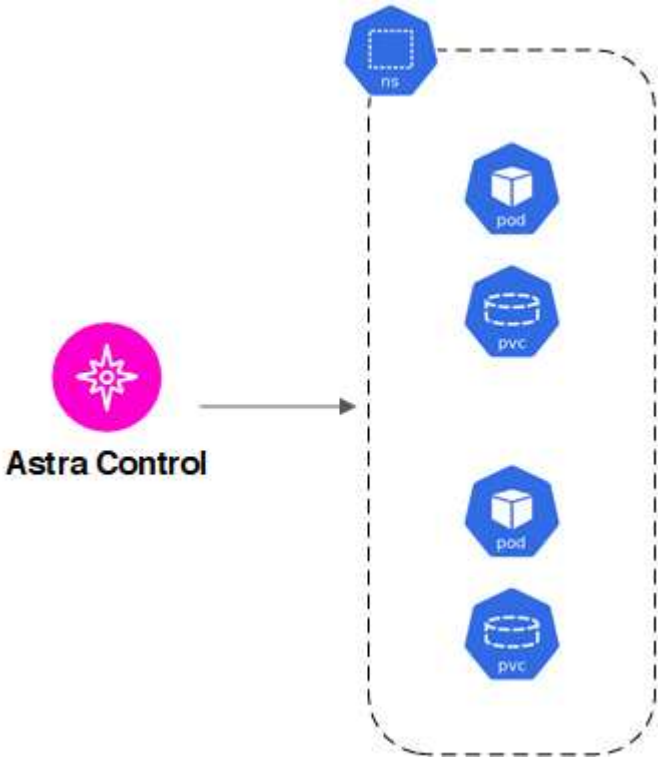
- "Ajoutez une licence lorsque vous configurez Astra Control Center pour la première fois"
- "Mettre à jour une licence existante"

Gestion des applications

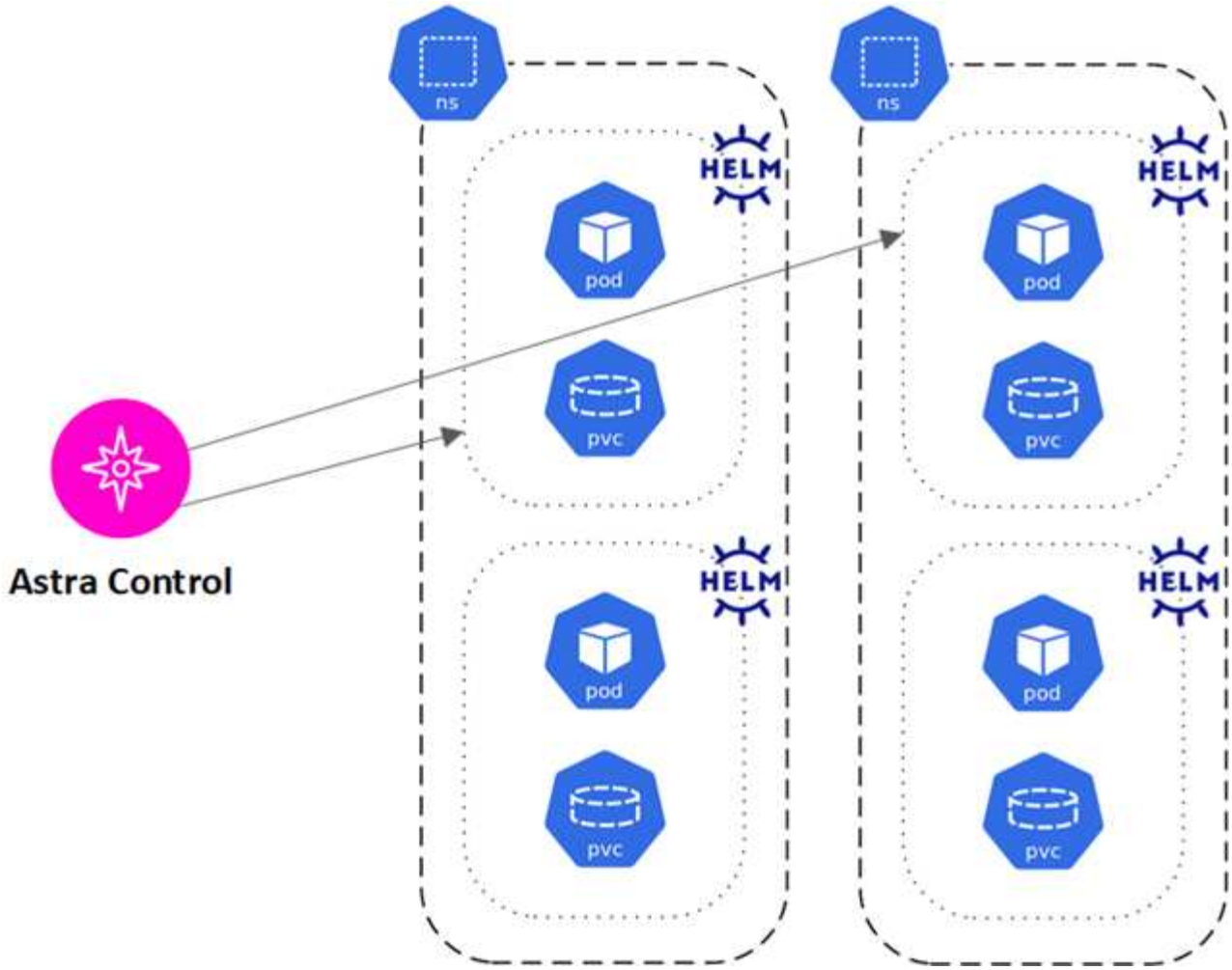
Lorsque Astra Control détecte vos clusters, les applications de ces clusters ne sont pas

gérées jusqu'à ce que vous choisissiez comment les gérer. Une application gérée d'Astra Control peut être l'une des suivantes :

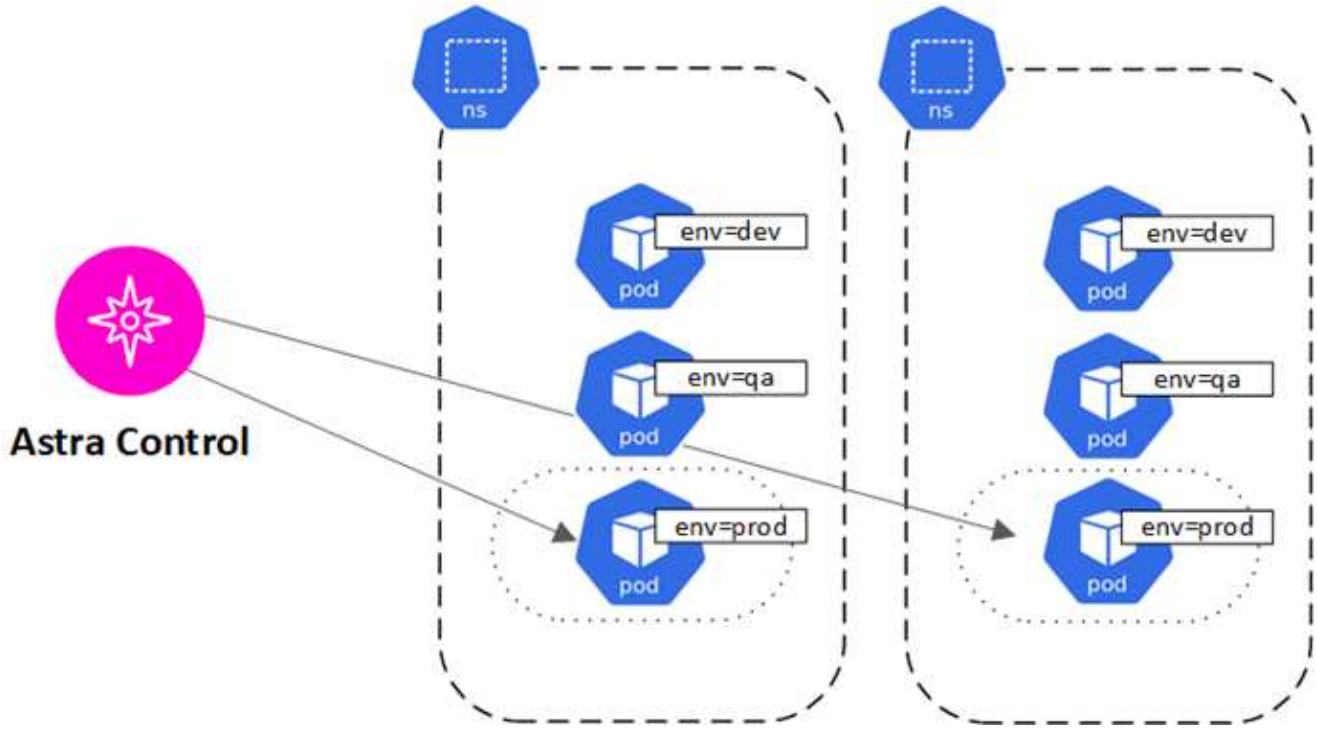
- Un espace de nom, y compris toutes les ressources de cet espace de nom



- Une application individuelle déployée au sein d'un ou plusieurs espaces de noms (helm3 est utilisé dans cet exemple)



- Groupe de ressources identifié par une étiquette Kubernetes dans un ou plusieurs espaces de noms



Classes de stockage et taille de volume persistant

ASTRA Control Center prend en charge NetApp ONTAP et Longhorn en tant que systèmes back-end de stockage.

Présentation

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

- **Classes de stockage soutenues par le stockage ONTAP** : si vous utilisez un back-end ONTAP, Astra Control Center offre la possibilité d'importer le back-end ONTAP pour générer des rapports d'informations de surveillance.
- **Classes de stockage CSI soutenues par Longhorn** : vous pouvez utiliser Longhorn avec le pilote Longhorn Container Storage interface (CSI).

Les classes de stockage doivent être "configuré" À l'aide d'Astra Control Provisioner.

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.

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"

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.

Vous pouvez définir et gérer des applications qui incluent des ressources de stockage avec des pods en cours d'exécution ou des applications qui incluent des ressources de stockage sans aucun pod en cours d'exécution. Les applications qui ne disposent pas de pods en cours d'exécution sont connues sous le nom d'applications exclusivement basées sur les données.

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 avez besoin soit de la licence d'évaluation Astra Control Center intégrée, soit d'une licence complète.
- **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 avec espace de noms qui sont, en général, conçues avec une architecture « pass-by-value » plutôt que « pass-by-Reference ». 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.

Avant de commencer

- 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.
- 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
- "(Aperçu technique) définissez une application à l'aide d'une ressource personnalisée Kubernetes"

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.

Développez pour en savoir plus sur l'ajout de ressources Cluster-scoped à vos namespaces 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.

5. (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".

6. (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.
7. (Facultatif) Entrez des critères de sélection d'étiquette ou d'étiquette pour tout espace de noms supplémentaire que vous ajoutez.
8. (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 :

a. Sélectionnez **Ajouter inclure règle**.
b. **Groupe** : dans la liste déroulante, sélectionnez le groupe de ressources API.
c. **Type** : dans la liste déroulante, sélectionnez le nom du schéma d'objet.
d. **Version** : saisissez la version de l'API.
e. **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.
f. Vérifiez la règle créée en fonction de vos entrées.
g. 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.

9. Sélectionnez **définir**.
10. 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.

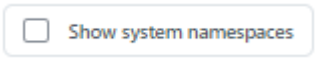
Définissez un espace de noms à gérer en tant qu'application

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. 

"En savoir plus".

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

[Aperçu technique] définissez une application à l'aide d'une ressource personnalisée Kubernetes

Vous pouvez spécifier les ressources Kubernetes que vous souhaitez gérer avec Astra Control en les définissant comme une application à l'aide d'une ressource personnalisée (CR). Vous pouvez ajouter des ressources définies dans le cluster si vous souhaitez gérer ces ressources individuellement ou toutes les ressources Kubernetes d'un namespace si, par exemple, vous avez l'intention de gérer et de protéger toutes les ressources d'un namespace spécifique de la même manière et à intervalles réguliers.

Étapes

1. Créer le fichier de ressource personnalisée (CR) et le nommer (par exemple, `astra_mysql_app.yaml`).
2. Nommez l'application dans `metadata.name`.
3. Définissez les ressources d'application à gérer :

spec.includedClusterScopedResources

Incluez les types de ressources cluster-scoped en plus de celles qu'Astra Control inclut automatiquement :

- **spec.includedClusterScopedResources**: *(Facultatif)* Une liste des types de ressource cluster-scoped à inclure.
  - **GroupVersionKind**: *(Facultatif)* identifie sans ambiguïté un type.
    - **Group**: *(requis si groupVersionKind est utilisé)* groupe API de la ressource à inclure.
    - **Version**: *(requis si groupVersionKind est utilisé)* version API de la ressource à inclure.
    - **Kind**: *(requis si groupVersionKind est utilisé)* type de la ressource à inclure.
  - **LabelSelector**: *(Facultatif)* Une requête d'étiquette pour un ensemble de ressources. Il est utilisé pour récupérer uniquement les ressources correspondant à l'étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe. Le résultat des matchLabels et des expressions matchExpressions est ANDed.
    - **MatchLabels**: *(Facultatif)* Une carte de {key,value} paires. Un {key,value} unique dans la carte matchLabels est équivalent à un élément de matchExpressions qui a un champ clé de "key", un opérateur de "in" et un tableau de valeurs contenant uniquement "Value". Les exigences sont ANDed.
    - **MatchExpressions**: *(Facultatif)* Une liste des exigences du sélecteur d'étiquettes. Les exigences sont ANDed.
      - **Key**: *(requis si matchExpressions est utilisé)* la clé de libellé associée au sélecteur de libellé.
      - **Operator**: *(requis si matchExpressions est utilisé)* représente la relation d'une clé à un ensemble de valeurs. Les opérateurs valides sont `In`, `NotIn`, `Exists` et `DoesNotExist`.
      - **Valeurs**: *(obligatoire si matchExpressions est utilisé)_un tableau de valeurs de chaîne. Si l'opérateur est `In` ou `NotIn`, le tableau de valeurs doit être _not* vide. Si l'opérateur est `Exists` ou `DoesNotExist`, le tableau de valeurs doit être vide.

spec.includedNamespaces

Inclure les espaces de noms et les ressources dans ces ressources dans l'application :

- **spec.includedNamespaces**: _(required)_définit l'espace de noms et les filtres facultatifs pour la sélection des ressources.
  - **Namespace**: *(obligatoire)* l'espace de noms qui contient les ressources d'applications que vous souhaitez gérer avec Astra Control.
  - **LabelSelector**: *(Facultatif)* Une requête d'étiquette pour un ensemble de ressources. Il est utilisé pour récupérer uniquement les ressources correspondant à l'étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe. Le résultat des matchLabels et des expressions matchExpressions est ANDed.
    - **MatchLabels**: *(Facultatif)* Une carte de {key,value} paires. Un {key,value} unique dans la carte matchLabels est équivalent à un élément de matchExpressions qui a un champ clé de "key", un opérateur de "in" et un tableau de valeurs contenant uniquement "Value". Les exigences sont ANDed.

- **MatchExpressions**: *(Facultatif)* Une liste des exigences du sélecteur d'étiquettes. `key` et `operator` sont obligatoires. Les exigences sont ANDed.
  - **Key**: *(requis si matchExpressions est utilisé)* la clé de libellé associée au sélecteur de libellé.
  - **Operator**: *(requis si matchExpressions est utilisé)* représente la relation d'une clé à un ensemble de valeurs. Les opérateurs valides sont `In`, `NotIn`, `Exists` et `DoesNotExist`.
  - **Valeurs**: *(obligatoire si matchExpressions est utilisé)* un tableau de valeurs de chaîne. Si l'opérateur est `In` ou `NotIn`, le tableau de valeurs doit être *not* vide. Si l'opérateur est `Exists` ou `DoesNotExist`, le tableau de valeurs doit être vide.

Exemple YAML :

```
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

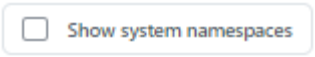
4. Après avoir renseigné le `astra_mysql_app.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

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**.



ASTRA Control Center n'est pas affiché par défaut en tant qu'application que vous pouvez gérer, mais vous pouvez sauvegarder et restaurer une instance Astra Control Center à l'aide d'une autre instance Astra Control Center.

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 stratégies* : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou 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
- Sauvegardez et restaurez les opérations ontap-nas
- Créez une sauvegarde immuable
- 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. Vous pouvez définir une règle de protection à l'aide de l'interface utilisateur Web d'Astra Control ou d'un fichier de ressource personnalisée (CR).

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".

Si vous définissez une règle de protection qui crée des sauvegardes immuables dans des compartiments WORM (Write Once, Read Many), assurez-vous que la durée de conservation des sauvegardes ne soit pas plus courte que la période de conservation configurée pour le compartiment.

Décaler les plannings de sauvegarde et de réplication pour éviter les chevauchements de planification. Par exemple, effectuez des sauvegardes en haut de l'heure toutes les heures et planifiez la réplication pour qu'elle commence avec un décalage de 5 minutes et un intervalle de 10 minutes.

Configurez une stratégie de protection à l'aide de l'interface utilisateur Web

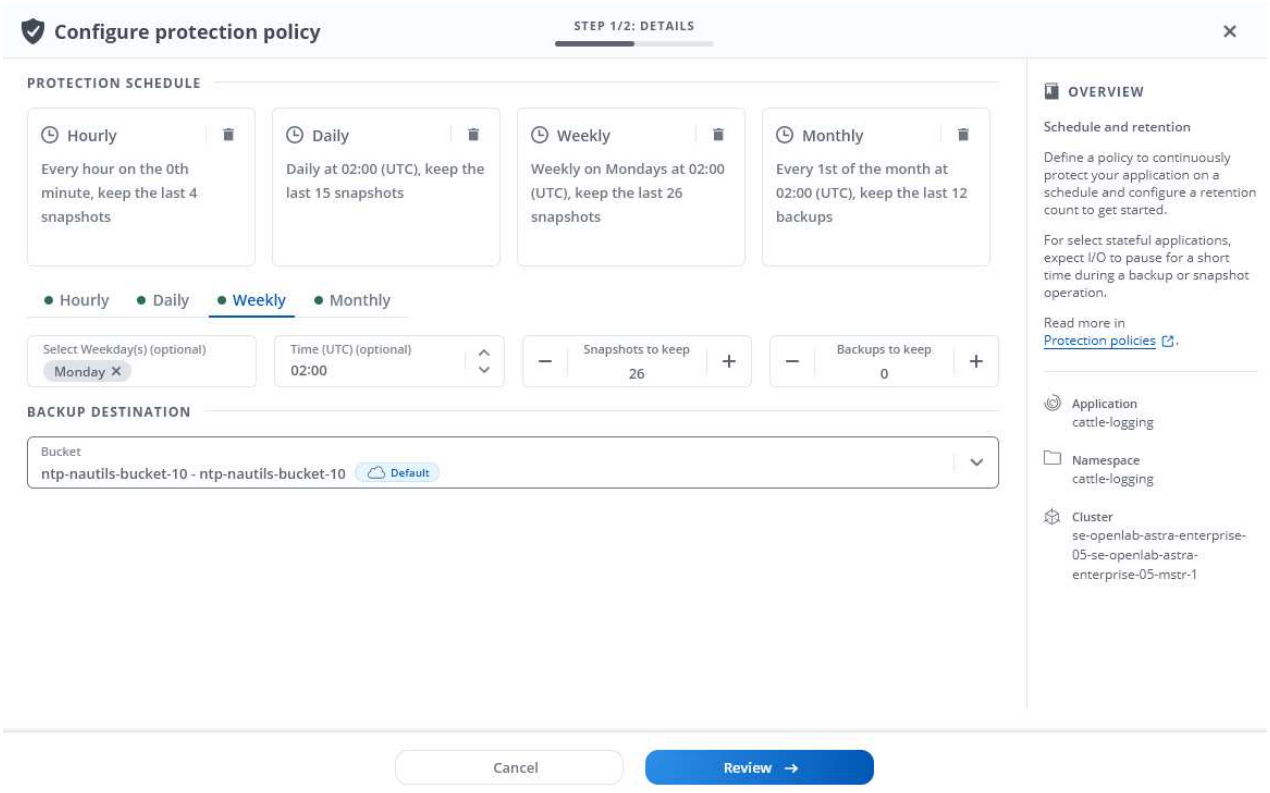
Étapes

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.



5. [**Tech Preview**] Choisissez un compartiment de destination pour les sauvegardes ou les instantanés dans la liste des compartiments de stockage.
6. Sélectionnez **Revue**.
7. Sélectionnez **définir la stratégie de protection.**

[Aperçu technique] configurez une stratégie de protection à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-schedule-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour répondre à vos besoins en matière

d'environnement Astra Control, de configuration de cluster et de protection des données :

- <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
- <APPLICATION_NAME> : nom Kubernetes de l'application à sauvegarder.
- <APPVAULT_NAME> : nom du coffre-fort dans lequel le contenu de la sauvegarde doit être stocké.
- <BACKUPS_RETAINED> : nombre de sauvegardes à conserver. Zéro indique qu'aucune sauvegarde ne doit être créée.
- <SNAPSHOTS_RETAINED> : nombre de snapshots à conserver. Zéro indique qu'aucun snapshot ne doit être créé.
- <GRANULARITY> : fréquence à laquelle le programme doit être exécuté. Valeurs possibles, ainsi que les champs associés obligatoires :
  - `hourly` (nécessite que vous spécifiiez `spec.minute`)
  - `daily` (nécessite que vous spécifiiez `spec.minute` et `spec.hour`)
  - `weekly` (nécessite que vous spécifiiez `spec.minute`, `spec.hour`, et `spec.dayOfWeek`)
  - `monthly` (nécessite que vous spécifiiez `spec.minute`, `spec.hour`, et `spec.dayOfMonth`)
- <DAY_OF_MONTH> : *(Facultatif)* le jour du mois (1 - 31) que l'horaire doit exécuter. Ce champ est obligatoire si la granularité est définie sur `monthly`.
- <DAY_OF_WEEK> : *(Facultatif)* le jour de la semaine (0 - 7) que l'horaire doit exécuter. Les valeurs 0 ou 7 indiquent dimanche. Ce champ est obligatoire si la granularité est définie sur `weekly`.
- <HOUR_OF_DAY> : *(Facultatif)* l'heure du jour (0 - 23) que le programme doit exécuter. Ce champ est obligatoire si la granularité est définie sur `daily`, `weekly`, ou `monthly`.
- <MINUTE_OF_HOUR> : *(Facultatif)* la minute de l'heure (0 - 59) que le programme doit exécuter. Ce champ est obligatoire si la granularité est définie sur `hourly`, `daily`, `weekly`, ou `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

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

```
kubectl apply -f astra-control-schedule-cr.yaml
```

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.

Description de la tâche

ASTRA Control prend en charge la création de snapshots à l'aide de classes de stockage basées sur les pilotes suivants :

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` pilote, les snapshots ne peuvent pas être créés. Utilisez une autre classe de stockage pour les snapshots.

Créez un instantané à l'aide de l'interface utilisateur Web

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. [**Tech Preview**] Choisissez un compartiment de destination pour le snapshot dans la liste des compartiments de stockage.
5. Examinez le résumé de l'instantané et sélectionnez **instantané**.

[Aperçu technique] Créez un instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
   - <APPLICATION_NAME> : nom Kubernetes de l'application à snapshot.
   - <APPVAULT_NAME> : nom du coffre-fort d'applications où le contenu de l'instantané doit être stocké.
   - <RECLAIM_POLICY> : *(Facultatif)* définit ce qui arrive à un instantané lorsque le snapshot CR est supprimé. Options valides :
     - `Retain`
     - `Delete` (valeur par défaut)

     ```
     apiVersion: astra.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: astra-connector
       name: <CR_NAME>
     spec:
       applicationRef: <APPLICATION_NAME>
       appVaultRef: <APPVAULT_NAME>
       reclaimPolicy: <RECLAIM_POLICY>
     ```

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

   ```
   kubectl apply -f astra-control-snapshot-cr.yaml
   ```

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 sauvegarder une application à tout moment.

Description de la tâche

Les compartiments d'Astra Control ne signalent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control, vérifiez les informations du compartiment dans le système de gestion du stockage approprié.

Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` pilote, vous devez activer la sauvegarde et la restauration fonctionnalité. Assurez-vous d'avoir défini un `backendType` dans votre "Objet de stockage Kubernetes" avec une valeur de `ontap-nas-economy` avant d'effectuer toute opération de protection.

ASTRA Control prend en charge la création de sauvegardes à l'aide de classes de stockage basées sur les pilotes suivants :

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

Créez une sauvegarde à l'aide de l'interface utilisateur Web

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. [**Tech Preview**] Choisissez 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**.

[Aperçu technique] Créez une sauvegarde à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
   - <APPLICATION_NAME> : nom Kubernetes de l'application à sauvegarder.
   - <APPVAULT_NAME> : nom du coffre-fort dans lequel le contenu de la sauvegarde doit être stocké.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

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

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

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.

Sauvegardez et restaurez les opérations ontap-nas

ASTRA Control Provisioner offre des fonctionnalités de sauvegarde et de restauration qui peuvent être activées pour les systèmes back-end qui utilisent le `ontap-nas-economy` classe de stockage.

Avant de commencer

- Vous avez "Mécanisme de provisionnement Astra Control activé".
- Vous avez défini une application dans Astra Control. Cette application aura une fonctionnalité de protection limitée jusqu'à ce que vous ayez terminé cette procédure.
- Vous avez `ontap-nas-economy` sélectionné comme classe de stockage par défaut pour votre système back-end de stockage.

Étapes

1. Effectuez les opérations suivantes sur le back-end de stockage ONTAP :
   a. Trouver le SVM qui héberge `ontap-nas-economy`volumes de l'application basés sur.
   b. Connectez-vous à un terminal connecté à ONTAP où les volumes sont créés.
   c. Masquer le répertoire Snapshot pour le SVM :

      Cette modification concerne l'ensemble du SVM. Le répertoire caché continuera d'être accessible.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+

      Vérifiez que le répertoire de snapshot sur le back-end de stockage ONTAP est masqué. Si ce répertoire n'est pas masqué, l'accès à votre application risque d'être perdu, en particulier s'il utilise NFSv3.

2. Effectuez les opérations suivantes dans Astra Control Provisioner :
   a. Activez le répertoire de snapshot pour chaque PV qui est `ontap-nas-economy` basé et associé à l'application :

```
tridentctl update volume <pv name> --snapshot-dir=true --pool-level
=true -n trident
```

b. Vérifiez que le répertoire de snapshot a été activé pour chaque PV associé :

```
tridentctl get volume <pv name> -n trident -o yaml | grep snapshotDir
```

Réponse :

```
snapshotDirectory: "true"
```

3. Dans Astra Control, actualisez l'application après avoir activé tous les répertoires de snapshots associés afin qu'Astra Control reconnaisse la valeur modifiée.

Résultat

L'application est prête à effectuer des sauvegardes et des restaurations à l'aide d'Astra Control. Chaque demande de volume persistant est également disponible pour être utilisée par d'autres applications à des fins de sauvegarde et de restauration.

Créez une sauvegarde immuable

Une sauvegarde immuable ne peut pas être modifiée, supprimée ou écrasée tant que la stratégie de conservation sur le compartiment qui stocke la sauvegarde l'interdit. Vous pouvez créer des sauvegardes immuables en sauvegardant les applications dans des compartiments dont une stratégie de conservation est configurée. Reportez-vous à la section "Protection des données" pour obtenir des informations importantes sur l'utilisation de sauvegardes immuables.

Avant de commencer

Vous devez configurer le compartiment de destination avec une règle de conservation. Cette procédure varie en fonction du fournisseur de stockage que vous utilisez. Pour plus d'informations, reportez-vous à la documentation du fournisseur de stockage :

- **Amazon Web Services** : "Activez le verrouillage objet S3 lors de la création du compartiment et définissez un mode de conservation par défaut de « gouvernance » avec une période de conservation par défaut".
- **NetApp StorageGRID** : "Activez le verrouillage objet S3 lors de la création du compartiment et définissez un mode de conservation par défaut de « conformité » avec une période de conservation par défaut".

Les compartiments d'Astra Control ne signalent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control, vérifiez les informations du compartiment dans le système de gestion du stockage approprié.

Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` vérifiez que vous avez défini un `backendType` dans votre "Objet de stockage Kubernetes" avec une valeur de `ontap-nas-economy` avant d'effectuer toute opération de protection.

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. Un compartiment WORM (Write Once Read Many) est indiqué par l'état « LOCKED » (verrouillé) à côté du nom du compartiment.

   Si le type de godet n'est pas pris en charge, cela est indiqué lorsque vous survolez ou sélectionnez le godet.

6. Sélectionnez **Suivant**.
7. Passez en revue le résumé des sauvegardes et sélectionnez **Sauvegarder**.

Résultat

ASTRA Control crée une sauvegarde immuable 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 essayez de créer deux sauvegardes immuables d'une même application dans le même compartiment en même temps, Astra Control empêche le démarrage de la deuxième sauvegarde. Attendez que la première sauvegarde soit terminée avant de commencer une autre sauvegarde.
- Vous ne pouvez pas annuler une sauvegarde immuable en cours d'exécution.
- 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.

Une sauvegarde immuable est indiquée avec l'état « verrouillé » à côté du compartiment qu'elle utilise.

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.

Vous ne pouvez pas annuler une sauvegarde immuable en cours d'exécution.

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. Vous ne pouvez pas supprimer une sauvegarde effectuée dans un compartiment immuable tant que la politique de conservation du compartiment ne vous y autorise pas.

Vous ne pouvez pas supprimer une sauvegarde immuable avant l'expiration de la période de conservation.

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.

[Aperçu technique] protège l'ensemble d'un cluster

Vous pouvez créer une sauvegarde automatique planifiée de tout ou partie des espaces de noms non gérés sur un cluster. NetApp fournit ces workflows en tant que compte de service Kubernetes, liaisons de rôles et tâche cron orchestrée avec un script Python.

Comment cela fonctionne

Lorsque vous configurez et installez le flux de travail de sauvegarde de cluster complet, une tâche cron s'exécute régulièrement et protège tout espace de noms qui n'est pas déjà géré, en créant automatiquement des stratégies de protection basées sur les planifications que vous choisissez pendant l'installation.

Si vous ne souhaitez pas protéger tous les espaces de noms non gérés du cluster avec le workflow complet de sauvegarde du cluster, vous pouvez utiliser le workflow de sauvegarde basé sur des libellés. Le flux de travail de sauvegarde basé sur des étiquettes utilise également une tâche cron, mais au lieu de protéger tous les espaces de noms non gérés, il identifie les espaces de noms par des étiquettes que vous fournissez pour protéger éventuellement les espaces de noms en fonction de stratégies de sauvegarde Bronze, Silver ou Gold.

Lorsqu'un nouvel espace de noms est créé et entre dans le cadre du workflow de votre choix, il est automatiquement protégé, sans aucune action d'administrateur. Ces flux de travail sont implémentés par cluster. Ainsi, différents clusters peuvent utiliser les deux flux de travail avec des niveaux de protection uniques, selon l'importance du cluster.

Exemple : protection complète du cluster

Par exemple, lorsque vous configurez et installez l'intégralité du workflow de sauvegarde du cluster, toutes les applications de n'importe quel espace de noms sont régulièrement gérées et protégées sans que l'administrateur n'ait à faire appel à lui. L'espace de noms n'a pas besoin d'exister au moment de l'installation du workflow ; si un espace de noms est ajouté ultérieurement, il sera protégé.

Exemple : protection par étiquette

Pour plus de granularité, vous pouvez utiliser le flux de production basé sur des étiquettes. Par exemple, vous pouvez installer ce flux de travail et demander à vos utilisateurs d'appliquer l'une des étiquettes à tous les espaces de noms qu'ils souhaitent protéger, en fonction du niveau de protection dont ils ont besoin. Cela permet aux utilisateurs de créer l'espace de noms avec l'une de ces étiquettes et ils n'ont pas à en avertir l'administrateur. Le nouveau namespace et toutes les applications qu'il contient sont automatiquement protégés.

Créer une sauvegarde planifiée de tous les espaces de noms

Vous pouvez créer une sauvegarde planifiée de tous les espaces de noms sur un cluster à l'aide du workflow complet de sauvegarde du cluster.

Étapes

1. Téléchargez les fichiers suivants sur un ordinateur disposant d'un accès réseau à votre cluster :
   - "Components.yaml fichier CRD"
   - "protectCluster.py script Python"
2. Pour configurer et installer la boîte à outils, "suivez les instructions fournies".

Créer une sauvegarde planifiée d'espaces de noms spécifiques

Vous pouvez créer une sauvegarde planifiée d'espaces de noms spécifiques en utilisant leurs étiquettes à l'aide du flux de travail de sauvegarde basé sur des étiquettes.

Étapes

1. Téléchargez les fichiers suivants sur un ordinateur disposant d'un accès réseau à votre cluster :
   - "Components.yaml fichier CRD"
   - "protectCluster.py script Python"
2. Pour configurer et installer la boîte à outils, "suivez les instructions fournies".

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.

Avant de commencer

- **Protéger vos applications en premier** : il est fortement recommandé de prendre un instantané ou une sauvegarde de votre application avant de la restaurer. Vous pourrez ainsi cloner à partir de l'instantané ou de la sauvegarde si la restauration échoue.
- **Vérifier les volumes de destination** : si vous restaurez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, ReadWriteMaly). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent. Par exemple, si votre volume persistant source utilise le mode d'accès RWX, en sélectionnant une classe de stockage de destination qui ne peut pas fournir RWX, comme les disques gérés Azure, AWS EBS, Google persistent Disk ou `ontap-san`, provoque l'échec de l'opération de restauration. Pour plus d'informations sur les modes d'accès aux volumes persistants, reportez-vous au "Kubernetes" documentation :
- **Planifier les besoins en espace** : lorsque vous effectuez une restauration sur place d'une application utilisant un stockage NetApp ONTAP, l'espace utilisé par l'application restaurée peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.
- * (Clusters Red Hat OpenShift uniquement) Ajouter des stratégies* : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou 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
```

- **Pilotes de classe de stockage pris en charge** : Astra Control prend en charge la restauration des sauvegardes à l'aide de classes de stockage soutenues par les pilotes suivants :
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- * (Pilote ontap-nas-Economy uniquement) sauvegardes et restaurations* : avant de sauvegarder ou de restaurer une application qui utilise une classe de stockage sauvegardée par `ontap-nas-economy` pilote, vérifiez que "Le répertoire Snapshot du système back-end de stockage ONTAP est masqué". Si ce répertoire n'est pas masqué, l'accès à votre application risque d'être perdu, en particulier s'il utilise NFSv3.
- **Les applications déployées par Helm** : les applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement prises en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.

> 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. Pour plus d'informations, voir cet exemple.

Procédez comme suit, en fonction du type d'archive à restaurer :

Restaurez les données à partir d'une sauvegarde ou d'un instantané à l'aide de l'interface utilisateur Web

Vous pouvez restaurer les données à l'aide de l'interface utilisateur web d'Astra Control.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.
3. 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.

     > Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` pilote, vous devez restaurer l'application à l'aide des classes de stockage d'origine. Vous ne pouvez pas spécifier une classe de stockage différente si vous restaurez l'application dans le même espace de noms.

     i. Sélectionnez le snapshot ou la sauvegarde à utiliser pour restaurer l'application sur place, ce qui restaure l'application à une version antérieure de elle-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.

- **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. Spécifiez le nom de l'application restaurée.
  ii. Choisissez le cluster de destination pour l'application que vous souhaitez restaurer.
  iii. 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.

  iv. Sélectionnez **Suivant**.
  v. Sélectionnez le snapshot ou la sauvegarde à utiliser pour restaurer l'application.
  vi. Sélectionnez **Suivant**.
  vii. Options au choix :
    - **Restaurer à l'aide des classes de stockage d'origine** : l'application utilise la classe de stockage associée à l'origine, sauf si elle n'existe pas sur le cluster cible. Dans ce cas, la classe de stockage par défaut du cluster sera utilisée.
    - **Restaurer à l'aide d'une classe de stockage différente** : sélectionnez une classe de stockage qui existe sur le cluster cible. Tous les volumes d'application, quelles que soient les classes de stockage qui leur sont associées à l'origine, seront migrés vers cette classe de stockage différente dans le cadre de la restauration.
  viii. Sélectionnez **Suivant**.

4. Sélectionnez les ressources à filtrer :
   - **Restaurer toutes les ressources** : restaurez toutes les ressources associées à l'application d'origine.
   - **Filtrer les ressources** : spécifiez des règles pour restaurer un sous-ensemble des ressources d'application d'origine :
     i. Choisissez d'inclure ou d'exclure des ressources de l'application restaurée.
     ii. Sélectionnez **Ajouter une règle d'inclusion** ou **Ajouter une règle d'exclusion** et configurez la règle pour filtrer les ressources appropriées lors de la restauration de l'application. Vous pouvez modifier une règle ou la supprimer et créer une nouvelle règle jusqu'à ce que la configuration soit correcte.

     Pour en savoir plus sur la configuration des règles d'inclusion et d'exclusion, reportez-vous à la section Filtrer les ressources pendant la restauration d'une application.

5. Sélectionnez **Suivant**.
6. Examinez attentivement les détails de l'action de restauration, tapez "restore" (si vous y êtes invité) et sélectionnez **Restore**.

[Aperçu technique] Restauration à partir d'une sauvegarde à l'aide d'une ressource personnalisée (CR)

Vous pouvez restaurer des données à partir d'une sauvegarde à l'aide d'un fichier de ressources personnalisées (CR) dans un espace de noms différent ou dans l'espace de noms source d'origine.

Restauration à partir d'une sauvegarde à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-restore-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE> : espace de noms source de l'opération de restauration.
   - <DESTINATION_NAMESPACE> : espace de noms de destination de l'opération de restauration.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Facultatif) si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :
   - « <INCLUDE-EXCLUDE> » : *(requis pour le filtrage)* utilisation `include` ou `exclude` Pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - <GROUP> : *(Facultatif)* Groupe de la ressource à filtrer.
     - <KIND> : *(Facultatif)* Type de la ressource à filtrer.
     - <VERSION> : *(Facultatif)* version de la ressource à filtrer.
     - <NAMES> : *(Facultatif)* noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
     - <NAMESPACES> : *(Facultatif)* namespaces dans le champ Kubernetes metadata.name de la ressource à filtrer.
     - <SELECTORS> : *(Facultatif)* chaîne de sélection d'étiquette dans le champ Kubernetes metadata.name de la ressource, comme défini dans "Documentation Kubernetes". Exemple :

"trident.netapp.io/os=linux".

Exemple :

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Après avoir renseigné le `astra-control-backup-restore-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

Restauration à partir de la sauvegarde vers l'espace de noms d'origine à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-ipr-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

2. (Facultatif) si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   ◦ « <INCLUDE-EXCLUDE> » : *(requis pour le filtrage)* utilisation `include` ou `exclude` Pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :

   - <GROUP> : *(Facultatif)* Groupe de la ressource à filtrer.
   - <KIND> : *(Facultatif)* Type de la ressource à filtrer.
   - <VERSION> : *(Facultatif)* version de la ressource à filtrer.
   - <NAMES> : *(Facultatif)* noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
   - <NAMESPACES> : *(Facultatif)* namespaces dans le champ Kubernetes metadata.name de la ressource à filtrer.
   - <SELECTORS> : *(Facultatif)* chaîne de sélection d'étiquette dans le champ Kubernetes metadata.name de la ressource, comme défini dans "Documentation Kubernetes". Exemple : `"trident.netapp.io/os=linux"`.

     Exemple :

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Après avoir renseigné le `astra-control-backup-ipr-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Aperçu technique] Restauration à partir d'un instantané à l'aide d'une ressource personnalisée (CR)

Vous pouvez restaurer les données d'un instantané à l'aide d'un fichier de ressource personnalisée (CR) dans un espace de noms différent ou dans l'espace de noms source d'origine.

Restauration à partir d'un instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-restore-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE> : espace de noms source de l'opération de restauration.
   - <DESTINATION_NAMESPACE> : espace de noms de destination de l'opération de restauration.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Facultatif) si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :
   - « <INCLUDE-EXCLUDE> » : *(requis pour le filtrage)* utilisation `include` ou `exclude` Pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - <GROUP> : *(Facultatif)* Groupe de la ressource à filtrer.
     - <KIND> : *(Facultatif)* Type de la ressource à filtrer.
     - <VERSION> : *(Facultatif)* version de la ressource à filtrer.
     - <NAMES> : *(Facultatif)* noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
     - <NAMESPACES> : *(Facultatif)* namespaces dans le champ Kubernetes metadata.name de la ressource à filtrer.
     - <SELECTORS> : *(Facultatif)* chaîne de sélection d'étiquette dans le champ Kubernetes metadata.name de la ressource, comme défini dans "Documentation Kubernetes". Exemple :

"trident.netapp.io/os=linux".

Exemple :

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Après avoir renseigné le `astra-control-snapshot-restore-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

Restauration de l'instantané vers l'espace de noms d'origine à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-ipr-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

2. (Facultatif) si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   ◦ « <INCLUDE-EXCLUDE> » : *(requis pour le filtrage)* utilisation `include` ou `exclude` Pour inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :

   - <GROUP> : *(Facultatif)* Groupe de la ressource à filtrer.
   - <KIND> : *(Facultatif)* Type de la ressource à filtrer.
   - <VERSION> : *(Facultatif)* version de la ressource à filtrer.
   - <NAMES> : *(Facultatif)* noms dans le champ Kubernetes metadata.name de la ressource à filtrer.
   - <NAMESPACES> : *(Facultatif)* namespaces dans le champ Kubernetes metadata.name de la ressource à filtrer.
   - <SELECTORS> : *(Facultatif)* chaîne de sélection d'étiquette dans le champ Kubernetes metadata.name de la ressource, comme défini dans "Documentation Kubernetes". Exemple : `"trident.netapp.io/os=linux"`.

     Exemple :

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Après avoir renseigné le `astra-control-snapshot-ipr-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

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 qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde l'accès au nouvel espace de noms.

Filtrer les ressources pendant la restauration d'une application

Vous pouvez ajouter une règle de filtre à un "restaurer" opération qui spécifie les ressources d'application existantes à inclure ou à exclure de l'application restaurée. Vous pouvez inclure ou exclure des ressources en fonction d'un espace de noms, d'un libellé ou d'un GVK (GroupVersionKind) spécifié.

Développez pour plus d'informations sur les scénarios d'inclusion et d'exclusion

- **Vous sélectionnez une règle d'inclusion avec des espaces de noms d'origine (restauration sur place)** : les ressources d'application existantes que vous définissez dans la règle seront supprimées et remplacées par celles de l'instantané ou de la sauvegarde sélectionné que vous utilisez pour la restauration. Toutes les ressources que vous ne spécifiez pas dans la règle inclure resteront inchangées.
- **Vous sélectionnez une règle d'inclusion avec de nouveaux espaces de noms** : utilisez la règle pour sélectionner les ressources spécifiques que vous voulez dans l'application restaurée. Les ressources que vous ne spécifiez pas dans la règle d'inclusion ne seront pas incluses dans l'application restaurée.
- **Vous sélectionnez une règle d'exclusion avec les espaces de noms d'origine (restauration sur place)** : les ressources que vous spécifiez pour être exclues ne seront pas restaurées et resteront inchangées. Les ressources que vous ne spécifiez pas pour exclure seront restaurées à partir de l'instantané ou de la sauvegarde. Toutes les données des volumes persistants seront supprimées et recréées si l'état correspondant fait partie des ressources filtrées.
- **Vous sélectionnez une règle d'exclusion avec de nouveaux espaces de noms** : utilisez la règle pour sélectionner les ressources spécifiques que vous souhaitez supprimer de l'application restaurée. Les ressources que vous ne spécifiez pas pour exclure seront restaurées à partir de l'instantané ou de la sauvegarde.

Les règles sont des types d'inclusion ou d'exclusion. Les règles combinant l'inclusion et l'exclusion des ressources ne sont pas disponibles.

Étapes

1. Après avoir choisi de filtrer les ressources et sélectionné une option d'inclusion ou d'exclusion dans l'assistant Restaurer l'application, sélectionnez **Ajouter une règle d'inclusion** ou **Ajouter une règle d'exclusion**.

Vous ne pouvez pas exclure des ressources dont la portée est définie par le cluster qui sont automatiquement incluses dans Astra Control.

2. Configurez la règle de filtre :

Vous devez spécifier au moins un espace de noms, un libellé ou un GVK. Assurez-vous que toutes les ressources que vous conservez après l'application des règles de filtre sont suffisantes pour que l'application restaurée reste en bon état.

   a. Sélectionnez un espace de noms spécifique pour la règle. Si vous ne faites pas de sélection, tous les espaces de noms seront utilisés dans le filtre.

Si votre application contenait initialement plusieurs espaces de noms et que vous les restaurez à de nouveaux espaces de noms, tous les espaces de noms seront créés même s'ils ne contiennent pas de ressources.

   b. (Facultatif) Entrez un nom de ressource.
   c. (Facultatif) **Sélecteur d'étiquettes** : inclure un "sélecteur d'étiquettes" pour ajouter à la règle. Le sélecteur d'étiquettes est utilisé pour filtrer uniquement les ressources correspondant à l'étiquette sélectionnée.
   d. (Facultatif) sélectionnez **utiliser GVK (GroupVersionKind) défini pour filtrer les ressources** pour des options de filtrage supplémentaires.

Si vous utilisez un filtre GVK, vous devez spécifier la version et le type.

      i. (Facultatif) **Group** : dans la liste déroulante, sélectionnez le groupe API Kubernetes.
      ii. **Type** : dans la liste déroulante, sélectionnez le schéma d'objet du type de ressource Kubernetes à utiliser dans le filtre.
      iii. **Version** : sélectionnez la version de l'API Kubernetes.

3. Vérifiez la règle créée en fonction de vos entrées.
4. Sélectionnez **Ajouter**.

Vous pouvez créer autant de règles d'inclusion et d'exclusion de ressources que vous le souhaitez. Les règles apparaissent dans le résumé de l'application de restauration avant de lancer l'opération.

Complications liées à la restauration sur place d'une application qui partage des ressources avec une autre application

Vous pouvez effectuer une opération de restauration sur place dans une application qui partage les ressources avec une autre application et produit des résultats inattendus. Toutes les ressources partagées entre les applications sont remplacées lorsqu'une restauration sur place est effectuée sur l'une des applications.

Voici un exemple de scénario qui ne convient pas lorsque vous utilisez la réplication NetApp SnapMirror pour effectuer une restauration :

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.

Réplication d'applications entre les systèmes back-end avec 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 configuré, vos applications peuvent répliquer les modifications des données et des applications d'un système back-end de stockage vers un autre, sur le même cluster ou entre différents clusters.

Pour une comparaison entre les sauvegardes/restaurations et la réplication, reportez-vous à la section "Concepts de protection des données".

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

- Du site A sur le site A sur le site A sur site
- Du site A sur site au site B sur site
- Du site au cloud avec Cloud Volumes ONTAP
- Le cloud avec Cloud Volumes ONTAP 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 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

Avant de commencer, vous devez remplir les conditions préalables suivantes :

Clusters ONTAP

- **Astra Control Provisioner ou Astra Trident** : Astra Control Provisioner ou Astra Trident doit exister sur les clusters Kubernetes source et de destination qui utilisent ONTAP en tant que back-end. ASTRA Control prend en charge la réplication avec la technologie NetApp SnapMirror à l'aide de classes de stockage basées sur les pilotes suivants :
  - `ontap-nas`
  - `ontap-san`
- **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Reportez-vous à la section "Présentation des licences SnapMirror dans ONTAP" pour en savoir plus.

Peering

- **Cluster et SVM** : les systèmes back-end de stockage ONTAP doivent être peering. Reportez-vous à la section "Présentation du cluster et de SVM peering" pour en savoir plus.

  S'assurer que les noms de SVM utilisés dans la relation de réplication entre deux clusters ONTAP sont uniques.

- **Astra Control Provisioner ou Astra Trident et SVM** : les SVM distants à peering doivent être disponibles pour Astra Control Provisioner ou Astra Trident sur le cluster destination.

  Centre de contrôle Astra

  "Déployez Astra Control Center" dans un troisième domaine de panne ou un site secondaire pour une reprise après incident transparente.

- **Systèmes back-end gérés** : vous devez ajouter et gérer des systèmes back-end de stockage ONTAP dans Astra Control Center pour créer une relation de réplication.

  L'ajout et la gestion de systèmes back-end de stockage ONTAP dans Astra Control Center sont facultatifs si vous avez activé le mécanisme de provisionnement Astra Control.

- **Clusters gérés** : ajoutez et gérez les clusters suivants avec Astra Control, idéalement sur différents sites ou domaines de défaillance :
  - Cluster Kubernetes source
  - Cluster Kubernetes de destination
  - Clusters ONTAP associés
- **Comptes d'utilisateur** : lorsque vous ajoutez un back-end de stockage ONTAP à Astra Control Center, appliquez les informations d'identification de l'utilisateur avec le rôle « admin ». Ce rôle a des méthodes d'accès `http` et `ontapi` Activation sur les clusters ONTAP source et de destination Reportez-vous à la section "Gérer les comptes utilisateur dans la documentation ONTAP" pour en savoir plus.

  Grâce à la fonctionnalité Astra Control Provisioner, vous n'avez pas besoin de définir spécifiquement un rôle d'administrateur pour gérer les clusters dans Astra Control Center, car ces identifiants ne sont pas requis par Astra Control Center.

ASTRA Control Center ne prend pas en charge la réplication NetApp SnapMirror pour les systèmes back-end de stockage utilisant le protocole NVMe over TCP.

Configuration d'Astra Trident et ONTAP

ASTRA Control Center exige que vous configuriez au moins un système back-end de stockage qui prend en charge la réplication pour les clusters source et de destination. Si les clusters source et cible sont identiques, l'application de destination doit utiliser un back-end de stockage différent de l'application source pour une résilience optimale.

> La réplication Astra Control prend en charge les applications qui utilisent une seule classe de stockage. Lorsque vous ajoutez une application à un espace de noms, assurez-vous que cette application possède la même classe de stockage que les autres applications de l'espace de noms. Lorsque vous ajoutez une demande de volume persistant à une application répliquée, assurez-vous que la nouvelle demande de volume persistant possède la même classe de stockage que les autres demandes de volume persistant dans l'espace de noms.

Configuration d'une relation de réplication

La configuration d'une relation de réplication implique les éléments suivants :

- Choix de la fréquence à laquelle vous souhaitez qu'Astra Control prenne une copie Snapshot d'application (qui inclut les ressources Kubernetes de l'application et les copies Snapshot de volume pour chacun des volumes de l'application)
- Choix de la planification de réplication (ressources Kubernetes incluses ainsi que données de volume persistant)
- Définition de la durée de prise de l'instantané

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Sélectionnez l'onglet **protection des données** > **réplication**.
3. 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 :
    - **Cluster de destination** : entrez un cluster de destination (il peut être identique au cluster source).
    - **Classe de stockage de destination** : sélectionnez ou entrez la classe de stockage qui utilise le SVM peering sur le cluster ONTAP de destination. Dans le cadre de la meilleure pratique, la classe de stockage de destination doit pointer vers un système back-end de stockage différent de la classe de stockage source.
    - **Type de réplication** : `Asynchronous` 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 snapshot et le réplique vers la destination.
    - **Offset** : définit le nombre de minutes à partir du haut de l'heure où vous souhaitez qu'Astra Control prenne un instantané. Vous pouvez utiliser un décalage afin qu'il ne coïncide pas avec d'autres opérations planifiées.

Décaler les plannings de sauvegarde et de réplication pour éviter les chevauchements de planification. Par exemple, effectuez des sauvegardes en haut de l'heure toutes les heures et planifiez la réplication pour qu'elle commence avec un décalage de 5 minutes et un intervalle de 10 minutes.

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** > **instantanés**.

   Le nom du snapshot utilise le format de `replication-schedule-<string>`. ASTRA Control conserve le dernier snapshot utilisé pour la réplication. Les anciens snapshots de réplication sont supprimés après la fin 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.
- Effectue un snapshot initial cohérent avec les applications.
- Établit la relation SnapMirror pour les volumes persistants utilisant le snapshot initial.

La page **Data protection** affiche l'état et l'état de la relation de réplication :
<Health status> | <Relationship life 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. Sélectionnez l'onglet **protection des données** > **réplication**.
3. Dans le menu actions, sélectionnez **basculement**.
4. Dans la page basculement, consultez les informations et sélectionnez **basculer**.

Résultat

La procédure de basculement entraîne les actions suivantes :

- L'application de destination démarre sur la base 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 règle de protection de l'application source est copiée vers l'application de destination en fonction des plannings présents sur l'application source au moment du basculement.
- Si un ou plusieurs crochets d'exécution post-restauration sont activés dans l'application source, ces crochets d'exécution sont exécutés pour l'application de destination.
- 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. Sélectionnez l'onglet **protection des données** > **réplication**.
3. 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 back-end de stockage de destination tout en continuant à répliquer vers le back-end de stockage source d'origine. ASTRA Control arrête l'application source et réplique les données vers la destination avant de basculer vers l'application de destination.

Dans ce cas, vous permutez la source et la destination.

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Sélectionnez l'onglet **protection des données** > **réplication**.
3. Dans le menu actions, sélectionnez **réplication inversée**.
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 des ressources Kubernetes de l'application source d'origine est effectuée.
- 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 copies Snapshot des volumes de l'application sont prises et répliquées.
- 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 du snapshot de pré-arrêt, à l'aide des données du volume répliquées après la fermeture 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 le « retour arrière » après une opération de basculement à l'aide de la séquence d'opérations suivante. Dans ce flux de travail pour restaurer le sens de réplication d'origine, Astra Control réplique (resyncs) toute modification d'application vers l'application source d'origine avant d'inverser le sens de réplication.

Ce processus commence à partir d'une relation qui a effectué 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. Sélectionnez l'onglet **protection des données** > **réplication**.
3. Dans le menu actions, sélectionnez **Resync**.
4. Pour une opération de retour arrière, choisissez l'application de basculement comme source de l'opération de resynchronisation (conservation des données écrites après 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. Sélectionnez l'onglet **protection des données** > **réplication**.
3. Dans la zone protection des applications ou dans le diagramme des 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 soit établie, soit 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 a donc été répliqué avec succès et un basculement est possible), mais le snapshot le plus récent a échoué ou n'a pas pu être répliqué.

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

resynchronyée ou inversée.

- **Créé** : il existe une relation de réplication. ASTRA Control vérifie régulièrement que les ESV sont disponibles, vérifie la relation de réplication, crée régulièrement des instantanés de l'application et identifie les nouvelles 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 snapshot d'application répliqué avec succès.
- **Basculement** : Astra Control arrête la réplication à partir du cluster source, utilise le snapshot d'application répliqué le plus récent (avec succès) sur la destination et restaure les ressources Kubernetes.
- **Resynchronisation** : le contrôle Astra resynchronque 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' est 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.

Avant de commencer

- **Vérifier les volumes de destination** : si vous clonez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, ReadWriteMaly). L'opération de clonage échoue si le mode d'accès au volume persistant de destination est différent. Par exemple, si votre volume persistant source utilise le mode d'accès RWX, en sélectionnant une classe de stockage de destination qui ne peut pas fournir RWX, comme les disques gérés Azure, AWS EBS, Google persistent Disk ou `ontap-san`, provoque l'échec de l'opération de clonage. Pour plus d'informations sur les modes d'accès aux volumes persistants, reportez-vous au "Kubernetes" documentation :
- 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.
- **Applications économiques ontap-nas** : vous ne pouvez pas utiliser d'opérations de clonage si la classe de stockage de votre application est prise en charge par `ontap-nas-economy` conducteur. Vous pouvez cependant "sauvegardez et restaurez les opérations ontap-nas".
- **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 qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde 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.
- **Avec une version spécifique de PostgreSQL** : les clones d'applications dans le 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.

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.
   - Entrer 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**.
   - Choisissez de conserver la classe de stockage d'origine associée à l'application ou de sélectionner une autre classe de stockage.

     Vous pouvez migrer la classe de stockage d'une application vers une classe de stockage de fournisseur cloud native ou vers une autre classe de stockage prise en charge, puis migrer une application à partir d'une classe de stockage prise en charge par `ontap-nas-economy` à une classe de stockage soutenue par `ontap-nas` sur le même cluster, ou copiez l'application vers un autre cluster dont la classe de stockage est prise en charge par `ontap-nas-economy` conducteur.

   Si vous sélectionnez une classe de stockage différente et que cette classe de stockage n'existe pas au moment de la restauration, une erreur est renvoyée.

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 qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde 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 un crochet d'exécution pour suspendre 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 Center 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
- Après le basculement

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un crochet d'exécution à une application, vous pouvez ajouter des filtres à un crochet d'exécution pour gérer les conteneurs auxquels le crochet correspond. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais ils peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels des crochets d'exécution s'exécutent sur certains conteneurs, mais pas nécessairement tous identiques. Si vous créez plusieurs filtres pour un seul crochet d'exécution, ils sont combinés avec un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.

Chaque filtre que vous ajoutez à un crochet d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un crochet correspond à un conteneur, le crochet exécute son script associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe de l'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre qui exclut les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe prise en charge par Astra Control pour les expressions régulières dans les filtres de crochet d'exécution, voir "Prise en charge de la syntaxe de l'expression régulière 2 (RE2)".

Si vous ajoutez un filtre d'espace de noms à un crochet d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage sont dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Remarques importantes sur les crochets d'exécution personnalisés

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

Puisque les crochets d'exécution réduisent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils s'exécutent, vous devez toujours essayer de réduire le temps d'exécution de vos crochets 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. Cela signifie que la logique utilisée dans un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde a été effectuée.

- La fonction crochets d'exécution est désactivée par défaut pour les nouveaux déploiements d'Astra Control.
  - Vous devez activer la fonction crochets d'exécution avant de pouvoir utiliser les crochets d'exécution.
  - Les utilisateurs propriétaires ou administrateurs peuvent activer ou désactiver la fonction crochets d'exécution pour tous les utilisateurs définis dans le compte Astra Control actuel. Reportez-vous à la section Activez la fonction crochets d'exécution et Désactivez la fonction crochets d'exécution pour obtenir des instructions.
  - Le statut d'activation de la fonctionnalité est conservé pendant les mises à niveau d'Astra Control.
- 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 des données à la demande, 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 Astra Control Center bascule une application source répliquée vers l'application de destination, tous les crochets d'exécution post-basculement activés pour l'application source sont exécutés pour l'application de destination une fois le basculement terminé.

> Si vous avez exécuté des crochets de post-restauration avec Astra Control Center 23.04 et mis à niveau votre Astra Control Center vers la version 23.07 ou ultérieure, les crochets d'exécution post-restauration ne seront plus exécutés après une réplication de basculement. Vous devez créer de nouveaux crochets d'exécution post-basculement pour vos applications. Vous pouvez également remplacer le type d'opération des crochets post-restauration existants destinés aux basculements par « post-restauration » ou « post-basculement ».

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 ayant tous les types 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	Sauvegarde existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets	Les crochets de basculement s'exécutent
1	Clonage	N	N	Nouveau	Identique	Y	N	Y	N
2	Clonage	N	N	Nouveau	Différente	Y	Y	Y	N
3	Cloner ou restaurer	Y	N	Nouveau	Identique	N	N	Y	N
4	Cloner ou restaurer	N	Y	Nouveau	Identique	N	N	Y	N
5	Cloner ou restaurer	Y	N	Nouveau	Différente	N	N	Y	N
6	Cloner ou restaurer	N	Y	Nouveau	Différente	N	N	Y	N
7	Restaurer	Y	N	Existant	Identique	N	N	Y	N
8	Restaurer	N	Y	Existant	Identique	N	N	Y	N
9	Snapshot	S/O	S/O	S/O	S/O	Y	S/O	S/O	N
10	Sauvegarde	N	S/O	S/O	S/O	Y	Y	S/O	N
11	Sauvegarde	Y	S/O	S/O	S/O	N	N	S/O	N

Scénario	Fonctionnement	Snapshot existant	Sauvegarde existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets	Les crochets de basculement s'exécutent
12	Basculement	Y	S/O	Créé par réplication	Différente	N	N	N	Y
13	Basculement	Y	S/O	Créé par réplication	Identique	N	N	N	Y

Exemples de crochet d'exécution

Consultez le "Projet GitHub NetApp Verda" Pour télécharger des crochets d'exécution réels pour des applications courantes telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres crochets d'exécution personnalisés.

Activez la fonction crochets d'exécution

Si vous êtes propriétaire ou administrateur, vous pouvez activer la fonction crochets d'exécution. Lorsque vous activez la fonctionnalité, tous les utilisateurs définis dans ce compte Astra Control peuvent utiliser des crochets d'exécution et afficher des crochets d'exécution et des scripts hook existants.

Étapes

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

   L'onglet **compte** > **paramètres de fonction** s'affiche.

4. Dans le volet **crochets d'exécution**, sélectionnez le menu Paramètres.
5. Sélectionnez **Activer**.
6. Notez l'avertissement de sécurité qui s'affiche.
7. Sélectionnez **Oui, activer les crochets d'exécution**.

Désactivez la fonction crochets d'exécution

Si vous êtes propriétaire ou administrateur, vous pouvez désactiver la fonction crochets d'exécution pour tous les utilisateurs définis dans ce compte Astra Control. Vous devez supprimer tous les crochets d'exécution existants avant de pouvoir désactiver la fonction crochets d'exécution. Reportez-vous à la section Supprimer un crochet d'exécution pour obtenir des instructions sur la suppression d'un crochet d'exécution existant.

Étapes

1. Accédez à **compte**, puis sélectionnez l'onglet **Paramètres de fonction**.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Dans le volet **crochets d'exécution**, sélectionnez le menu Paramètres.

4. Sélectionnez **Désactiver**.
5. Notez l'avertissement qui s'affiche.
6. Type `disable` pour confirmer que vous souhaitez désactiver la fonction pour tous les utilisateurs.
7. Sélectionnez **Oui, désactiver**.

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, le nombre de conteneurs correspondant, le temps de création et le moment où il s'exécute (pré ou post-opération). Vous pouvez sélectionner le + icône en regard du nom du crochet pour développer la liste des conteneurs sur lequel il sera exécuté. Pour afficher les journaux d'événements entourant les crochets d'exécution de cette application, accédez à l'onglet **activité**.

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

Chaque crochet d'exécution doit utiliser un script pour effectuer des actions. Vous pouvez ajouter un ou plusieurs scripts que les crochets d'exécution peuvent référencer. De nombreux crochets d'exécution peuvent référencer le même script ; ceci vous permet de mettre à jour de nombreux crochets d'exécution en modifiant un seul script.

Étapes

1. Assurez-vous que la fonction crochets d'exécution est activé.
2. Accédez à **compte**.
3. Sélectionnez l'onglet **scripts**.
4. Sélectionnez **Ajouter**.
5. 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.

6. 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 et l'ajouter à Astra Control. Reportez-vous à la section 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. Assurez-vous que la fonction crochets d'exécution est activé.
2. Sélectionnez **applications**, puis le nom d'une application gérée.
3. Sélectionnez l'onglet **crochets d'exécution**.
4. Sélectionnez **Ajouter**.

5. Dans la zone **Détails du crochet** :
   a. Déterminez quand le crochet doit fonctionner en sélectionnant un type d'opération dans le menu déroulant **opération**.
   b. Saisissez un nom unique pour le crochet.
   c. (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.
6. (Facultatif) dans la zone **Détails du filtre de crochet**, vous pouvez ajouter des filtres pour contrôler les conteneurs sur lesquels le crochet d'exécution s'exécute :
   a. Sélectionnez **Ajouter filtre**.
   b. Dans la colonne Type de filtre **Hook**, choisissez un attribut sur lequel filtrer dans le menu déroulant.
   c. Dans la colonne **Regex**, entrez une expression régulière à utiliser comme filtre. Astra Control utilise le "Expression régulière 2 (RE2) syntaxe regex".

      Si vous filtrez le nom exact d'un attribut (comme un nom de pod) sans autre texte dans le champ expression régulière, une correspondance de sous-chaîne est effectuée. Pour faire correspondre un nom exact et ce nom uniquement, utilisez la syntaxe de correspondance de chaîne exacte (par exemple, `^exact_podname$`).

   d. Pour ajouter d'autres filtres, sélectionnez **Ajouter filtre**.

      Plusieurs filtres pour un crochet d'exécution sont combinés à un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.

7. Lorsque vous avez terminé, sélectionnez **Suivant**.
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 **Suivant**.
10. Vérifiez la configuration du crochet d'exécution.
11. Sélectionnez **Ajouter**.

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.

Modifier un crochet d'exécution

Vous pouvez modifier un crochet d'exécution si vous souhaitez modifier ses attributs, filtres ou le script qu'il utilise. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour modifier 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 modifier.
4. Sélectionnez **Modifier**.
5. Apportez les modifications nécessaires en sélectionnant **Suivant** après avoir terminé chaque section.
6. Sélectionnez **Enregistrer**.

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**.
5. Dans la boîte de dialogue qui s'affiche, tapez « Supprimer » pour confirmer.
6. Sélectionnez **Oui, supprimez le crochet d'exécution**.

Pour en savoir plus

- "Projet GitHub NetApp Verda"

Protégez Astra Control Center à l'aide d'Astra Control Center

Pour mieux assurer la résilience contre les erreurs fatales sur le cluster Kubernetes sur lequel Astra Control Center s'exécute, protégez l'application Astra Control Center elle-même. Vous pouvez sauvegarder et restaurer Astra Control Center à l'aide d'une instance Astra Control Center secondaire ou utiliser la réplication Astra si le stockage sous-jacent utilise ONTAP.

Dans ces scénarios, une deuxième instance d'Astra Control Center est déployée et configurée dans un domaine de pannes différent et s'exécute sur un second cluster Kubernetes différent de l'instance Astra Control Center principale. La deuxième instance d'Astra Control est utilisée pour sauvegarder et restaurer potentiellement l'instance principale d'Astra Control Center. Une instance Astra Control Center restaurée ou

répliquée continuera d'assurer la gestion des données d'application pour les applications du cluster d'applications et de restaurer l'accessibilité aux sauvegardes et aux snapshots de ces applications.

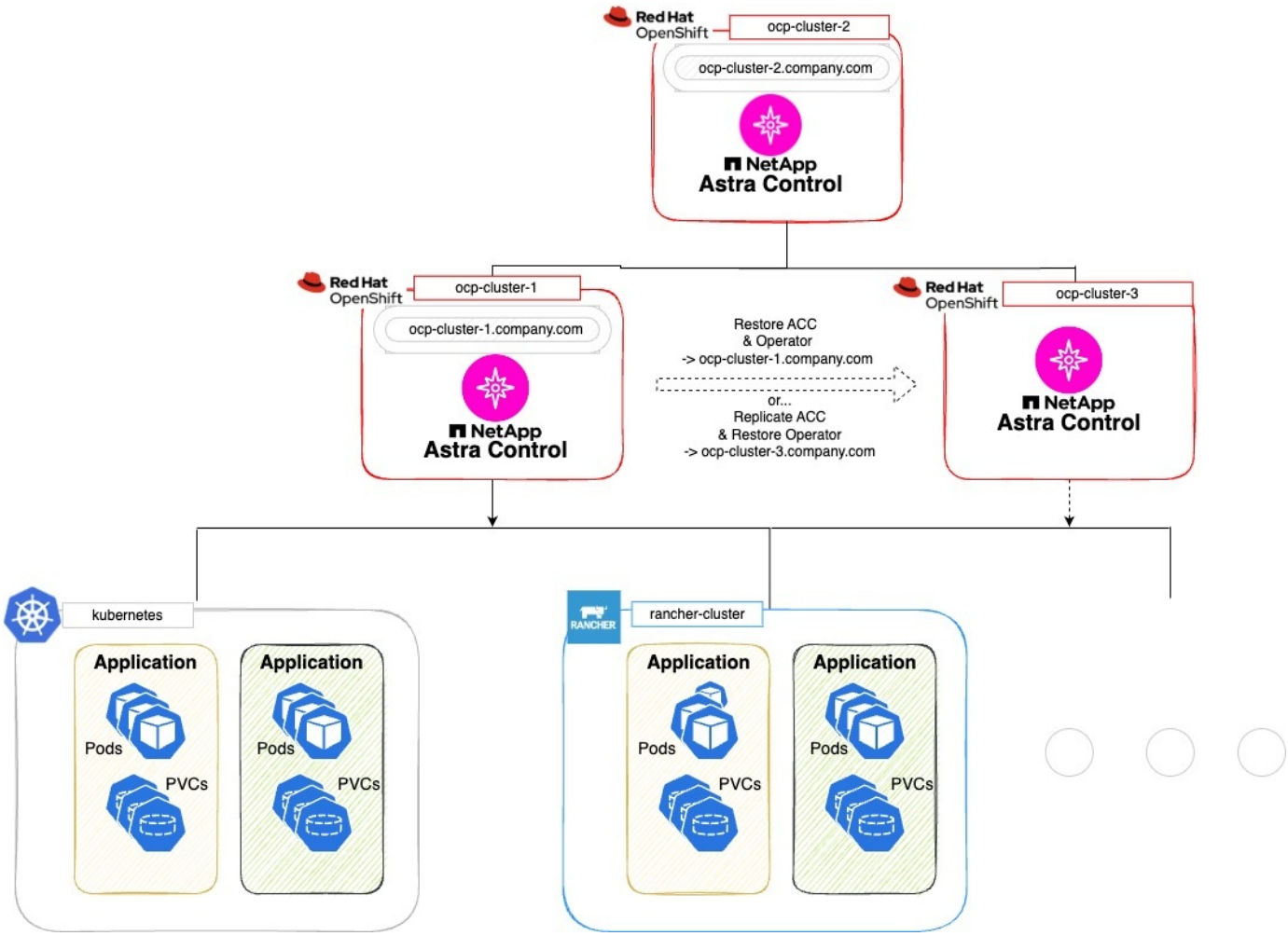
Avant de commencer

Assurez-vous d'avoir les éléments suivants avant de configurer des scénarios de protection pour Astra Control Center :

- **Un cluster Kubernetes exécutant l'instance principale d'Astra Control Center** : ce cluster héberge l'instance principale d'Astra Control Center qui gère les clusters d'applications.
- **Un deuxième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal qui exécute l'instance Astra Control Center secondaire** : ce cluster héberge l'instance Astra Control Center qui gère l'instance Astra Control Center principale.
- **Un troisième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal** : ce cluster hébergera l'instance restaurée ou répliquée d'Astra Control Center. Il doit disposer du même espace de noms Astra Control Center disponible qui est actuellement déployé sur le système principal. Par exemple, si Astra Control Center est déployé dans le namespace `netapp-acc` sur le cluster source, le namespace `netapp-acc` Doit être disponible et non utilisé par des applications sur le cluster Kubernetes de destination.
- **Compartiments compatibles S3** : chaque instance d'Astra Control Center dispose d'un compartiment de stockage objet accessible compatible avec S3.
- **Un équilibreur de charge configuré** : l'équilibreur de charge fournit une adresse IP pour Astra et doit disposer d'une connectivité réseau aux clusters d'applications et aux deux compartiments S3.
- **Les clusters répondent aux exigences d'Astra Control Center** : chaque cluster utilisé dans Astra Control Center est conforme "Exigences générales d'Astra Control Center".

Description de la tâche

Ces procédures décrivent les étapes nécessaires à la restauration d'Astra Control Center sur un nouveau cluster à l'aide des deux sauvegarder et restaurer ou la réplication. Les étapes sont basées sur l'exemple de configuration présenté ici :



Dans cet exemple de configuration, les éléments suivants sont présentés :

- **Un cluster Kubernetes exécutant l'instance principale d'Astra Control Center** :
  - Cluster OpenShift : `ocp-cluster-1`
  - Instance principale d'Astra Control Center : `ocp-cluster-1.company.com`
  - Ce cluster gère les clusters d'applications.
- **Le deuxième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal qui exécute l'instance Astra Control Center secondaire** :
  - Cluster OpenShift : `ocp-cluster-2`
  - Instance secondaire Astra Control Center : `ocp-cluster-2.company.com`
  - Ce cluster sera utilisé pour sauvegarder l'instance principale d'Astra Control Center ou pour configurer la réplication sur un autre cluster (dans cet exemple, le `ocp-cluster-3` cluster).
- **Un troisième cluster Kubernetes du même type de distribution Kubernetes que le principal qui sera utilisé pour les opérations de restauration** :
  - Cluster OpenShift : `ocp-cluster-3`
  - Troisième instance d'Astra Control Center : `ocp-cluster-3.company.com`
  - Ce cluster sera utilisé pour le basculement de réplication ou de restauration d'Astra Control Center.

Dans l'idéal, le cluster d'applications doit être situé en dehors des trois clusters Astra Control Center, comme illustré dans les clusters kubernetes et Rancher dans l'image ci-dessus.

Non représenté dans le schéma :

- Tous les clusters disposent de systèmes back-end ONTAP avec Astra Trident ou Astra Control Provisioner installé.
- Dans cette configuration, les clusters OpenShift utilisent MetalLB comme équilibreur de charge.
- Le contrôleur de snapshot et VolumeSnapshotClass sont également installés sur tous les clusters, comme indiqué dans le "prérequis".

Option de l'étape 1 : sauvegarde et restauration d'Astra Control Center

Cette procédure décrit les étapes nécessaires à la restauration d'Astra Control Center sur un nouveau cluster à l'aide de la sauvegarde et de la restauration.

Dans cet exemple, Astra Control Center est toujours installé sous `netapp-acc` l'espace de noms et l'opérateur sont installés sous le `netapp-acc-operator` espace de noms.

Bien que cela ne soit pas décrit, l'opérateur d'Astra Control Center peut également être déployé dans le même espace de nom que Astra CR.

Avant de commencer

- Vous avez installé le centre Astra Control Center principal sur un cluster.
- Vous avez installé le centre Astra Control Center secondaire sur un autre cluster.

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire (s'exécutant sur le système `ocp-cluster-2` cluster) :
   a. Connectez-vous à l'instance Astra Control Center secondaire.
   b. "Ajoutez le cluster Astra Control Center principal" (`ocp-cluster-1`).
   c. "Ajouter le troisième cluster de destination" (`ocp-cluster-3`) qui sera utilisé pour la restauration.
2. Gérez Astra Control Center et l'opérateur Astra Control Center sur l'Astra Control Center secondaire :
   a. Dans la page applications, sélectionnez **définir**.
   b. Dans la fenêtre **Define application**, entrez le nom de la nouvelle application (`netapp-acc`).
   c. Choisissez le cluster qui exécute le principal Astra Control Center (`ocp-cluster-1`) Dans la liste déroulante **Cluster**.
   d. Choisissez le `netapp-acc` Espace de noms pour Astra Control Center dans la liste déroulante **namespace**.
   e. Sur la page Ressources du cluster, cochez **inclure des ressources supplémentaires de cluster-scoped**.
   f. Sélectionnez **Ajouter inclure règle**.
   g. Sélectionnez ces entrées et sélectionnez **Ajouter** :
      - Sélecteur d'étiquette : <label name>

- Groupe : apiextensions.k8s.io
- Version : v1
- Type : CustomResourceDefinition

h. Confirmez les informations de l'application.

i. Sélectionnez **définir**.

Après avoir sélectionné **définir**, répétez le processus définir l'application pour l'opérateur `netapp-acc-operator`) et sélectionnez le `netapp-acc-operator` Espace de noms dans l'assistant définir l'application.

3. Sauvegardez Astra Control Center et l'opérateur :

a. Sur le centre de contrôle Astra secondaire, accédez à la page applications en sélectionnant l'onglet applications.

b. "Sauvegarde" L'application Astra Control Center (`netapp-acc`).

c. "Sauvegarde" l'opérateur (`netapp-acc-operator`).

4. Une fois que vous avez sauvegardé Astra Control Center et l'opérateur, simulez un scénario de reprise d'activité de "Désinstallation d'Astra Control Center" à partir du cluster principal.

> Vous allez restaurer Astra Control Center sur un nouveau cluster (le troisième cluster Kubernetes décrit dans cette procédure) et utiliser le même DNS que le cluster principal pour Astra Control Center récemment installé.

5. À l'aide du centre Astra Control Center secondaire, "restaurer" L'instance principale de l'application Astra Control Center à partir de sa sauvegarde :

a. Sélectionnez **applications**, puis sélectionnez le nom de l'application Astra Control Center.

b. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.

c. Choisissez le type de restauration **Restaurer vers les nouveaux espaces de noms**.

d. Entrez le nom de la restauration (`netapp-acc`).

e. Choisissez le troisième cluster de destination (`ocp-cluster-3`).

f. Mettez à jour l'espace de noms de destination de sorte qu'il s'agisse du même espace de noms que l'espace de noms d'origine.

g. Sur la page Source de restauration, sélectionnez la sauvegarde d'application qui sera utilisée comme source de restauration.

h. Sélectionnez **Restaurer à l'aide des classes de stockage d'origine**.

i. Sélectionnez **Restaurer toutes les ressources**.

j. Examinez les informations de restauration, puis sélectionnez **Restore** pour démarrer le processus de restauration qui restaure Astra Control Center sur le cluster de destination (`ocp-cluster-3`). La restauration est terminée lorsque l'application entre `available` état.

6. Configurer Astra Control Center sur le cluster de destination :

a. Ouvrez un terminal et connectez-le au cluster de destination à l'aide du kubeconfig (`ocp-cluster-3`) Qui contient l'Astra Control Center restaurée.

b. Confirmez que le `ADDRESS` Dans la configuration Astra Control Center, la colonne fait référence au nom DNS du système principal :

```
kubectl get acc -n netapp-acc
```

Réponse :

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
1.company.com           True
```

a. Si le `ADDRESS` Dans la réponse ci-dessus, le champ ne contient pas le nom de domaine complet de l'instance principale d'Astra Control Center. Mettez à jour la configuration pour référencer le DNS d'Astra Control Center :

```
kubectl edit acc -n netapp-acc
```

i. Modifiez le `astraAddress` sous `spec:` Au FQDN (`ocp-cluster-1.company.com` Dans cet exemple) de l'instance principale d'Astra Control Center.

ii. Enregistrez la configuration.

iii. Vérifiez que l'adresse a été mise à jour :

```
kubectl get acc -n netapp-acc
```

b. Accédez au Restaurez l'opérateur Astra Control Center de ce document pour terminer le processus de restauration.

Option de l'étape 1 : protégez Astra Control Center à l'aide de la réplication

Cette procédure décrit les étapes nécessaires à la configuration "Réplication Astra Control Center" Pour protéger l'instance principale d'Astra Control Center.

Dans cet exemple, Astra Control Center est toujours installé sous `netapp-acc` l'espace de noms et l'opérateur sont installés sous le `netapp-acc-operator` espace de noms.

Avant de commencer

- Vous avez installé le centre Astra Control Center principal sur un cluster.
- Vous avez installé le centre Astra Control Center secondaire sur un autre cluster.

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire :
   a. Connectez-vous à l'instance Astra Control Center secondaire.
   b. "Ajoutez le cluster Astra Control Center principal" (`ocp-cluster-1`).
   c. "Ajouter le troisième cluster de destination" (`ocp-cluster-3`) qui sera utilisé pour la réplication.

2. Gérez Astra Control Center et l'opérateur Astra Control Center sur l'Astra Control Center secondaire :
   a. Sélectionnez **clusters** et sélectionnez le cluster qui contient l'Astra Control Center principal (`ocp-cluster-1`).
   b. Sélectionnez l'onglet **espaces de noms**.
   c. Sélectionnez `netapp-acc` et `netapp-acc-operator` espaces de noms.
   d. Sélectionnez le menu actions et sélectionnez **définir comme applications**.
   e. Sélectionnez **Afficher dans les applications** pour voir les applications définies.
3. Configurer les systèmes back-end pour la réplication :

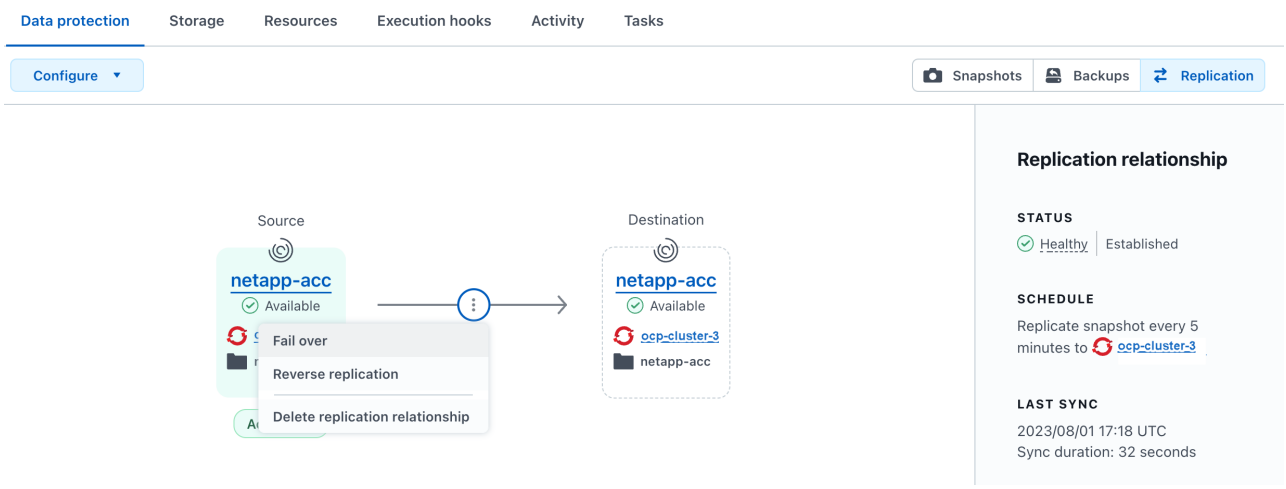
   La réplication nécessite le cluster principal Astra Control Center et le cluster de destination (`ocp-cluster-3`) Utiliser des systèmes back-end de stockage ONTAP peering différents. Une fois chaque back-end ajouté à Astra Control, le back-end apparaît dans l'onglet **découvert** de la page Backends.

   a. "Ajoutez un arrière-plan de peering" Vers Astra Control Center sur le cluster principal.
   b. "Ajoutez un arrière-plan de peering" Vers Astra Control Center sur le cluster de destination.
4. Configurer la réplication :
   a. Sur l'écran applications, sélectionnez `netapp-acc` client supplémentaire.
   b. Sélectionnez **configurer la stratégie de réplication**.
   c. Sélectionnez `ocp-cluster-3` en tant que cluster de destination.
   d. Sélectionnez la classe de stockage.
   e. Entrez `netapp-acc` comme espace de noms de destination.
   f. Modifiez la fréquence de réplication si vous le souhaitez.
   g. Sélectionnez **Suivant**.
   h. Vérifiez que la configuration est correcte et sélectionnez **Enregistrer**.

      La relation de réplication passe de `Establishing` à `Established`. Lorsqu'elle est active, cette réplication se produit toutes les cinq minutes jusqu'à ce que la configuration de réplication soit supprimée.
5. Basculez la réplication vers l'autre cluster si le système principal est corrompu ou n'est plus accessible :

   Assurez-vous que Astra Control Center n'est pas installé sur le cluster de destination pour assurer un basculement réussi.

   a. Sélectionnez l'icône des ellipses verticales et sélectionnez **basculement**.



b. Confirmez les détails et sélectionnez **basculement** pour lancer le processus de basculement.

   L'état de la relation de réplication passe à `Failing over` puis `Failed over` une fois l'opération terminée.

6. Compléter la configuration de basculement :

   a. Ouvrez un terminal et connectez-le à l'aide du kubeconfig du troisième cluster (`ocp-cluster-3`). Ce cluster est désormais équipé d'Astra Control Center.

   b. Déterminez le nom de domaine complet d'Astra Control Center sur le troisième cluster (`ocp-cluster-3`).

   c. Mettez à jour la configuration pour référencer le DNS Astra Control Center :

```
kubectl edit acc -n netapp-acc
```

      i. Modifiez le `astraAddress` sous `spec:` Avec le FQDN (`ocp-cluster-3.company.com`) du troisième cluster de destination.

      ii. Enregistrez la configuration.

      iii. Vérifiez que l'adresse a été mise à jour :

```
kubectl get acc -n netapp-acc
```

   d. Vérifiez que tous les CRD de traefik requis sont présents :

```
kubectl get crds | grep traefik
```

   CRDS de traefik requis :

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Si certains des CRD ci-dessus sont manquants :
   i. Accédez à "documentation de traefik".
   ii. Copiez la zone « Définitions » dans un fichier.
   iii. Appliquer les modifications :

```
kubectl apply -f <file name>
```

   iv. Redémarrer le traefik :

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Accédez au Restaurez l'opérateur Astra Control Center de ce document pour terminer le processus de restauration.

Étape 2 : restaurez l'opérateur Astra Control Center

À l'aide d'Astra Control Center secondaire, restaurez l'opérateur principal d'Astra Control Center à partir d'une sauvegarde. L'espace de noms de destination doit être identique à l'espace de noms source. Si vous avez supprimé Astra Control Center du cluster source principal, des sauvegardes existent toujours pour effectuer les mêmes étapes de restauration.

Étapes

1. Sélectionnez **applications**, puis sélectionnez le nom de l'application opérateur (`netapp-acc-operator`).

2. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**
3. Choisissez le type de restauration **Restaurer vers les nouveaux espaces de noms**.
4. Choisissez le troisième cluster de destination (`ocp-cluster-3`).
5. Modifiez le namespace pour qu'il soit identique au namespace associé au cluster source principal (`netapp-acc-operator`).
6. Sélectionnez la sauvegarde précédemment effectuée en tant que source de restauration.
7. Sélectionnez **Restaurer à l'aide des classes de stockage d'origine**.
8. Sélectionnez **Restaurer toutes les ressources**.
9. Vérifiez les détails, puis cliquez sur **Restaurer** pour lancer le processus de restauration.

   La page applications affiche l'opérateur Astra Control Center en cours de restauration sur le troisième cluster de destination (`ocp-cluster-3`). Lorsque le processus est terminé, l'état indique `Available`. Dans les dix minutes qui suivent, l'adresse DNS doit être résolue sur la page.

Résultat

ASTRA Control Center, ses clusters enregistrés et les applications gérées avec leurs copies Snapshot et leurs sauvegardes sont désormais disponibles sur le troisième cluster de destination (`ocp-cluster-3`). Toutes les stratégies de protection que vous aviez sur l'original sont également présentes sur la nouvelle instance. Vous pouvez continuer à effectuer des sauvegardes et des snapshots programmés ou à la demande.

Dépannage

Déterminez l'état du système et si les processus de protection ont réussi.

- **Les pods ne sont pas en cours d'exécution**: Confirmez que tous les pods sont en cours d'exécution:

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

  Si certains modules se trouvent dans le `CrashLookBackOff` indiquez, redémarrez-les et passez à `Running` état.

- **Confirmer l'état du système** : confirmer que le système Astra Control Center est en `ready` état :

  ```
  kubectl get acc -n netapp-acc
  ```

  Réponse :

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
  1.company.com           True
  ```

- **Confirmez l'état du déploiement** : affichez les informations de déploiement d'Astra Control Center pour le confirmer `Deployment State` est `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **L'interface utilisateur d'Astra Control Center restaurée renvoie une erreur 404** : si cela se produit lorsque vous avez sélectionné `AccTraefik` en tant qu'option d'entrée, cochez la case CRD de traefik pour vous assurer qu'ils sont tous installés.

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 de communication (si Astra Control peut communiquer avec l'application), son état de protection (qu'il soit entièrement protégé en cas de défaillance), les pods, le stockage persistant, etc.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **applications**, puis le nom d'une application.
2. Vérifiez les informations.

   Statut de l'application
   Fournit un état qui indique si Astra Control peut communiquer avec l'application.

   - **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'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.

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.

Avant de commencer

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 **correspondance utilisateur**, procédez comme suit :
   a. Entrez le DN de base et un filtre de recherche d'utilisateur approprié à utiliser lors de la récupération des informations utilisateur à partir du serveur LDAP.
   b. (Facultatif) si votre répertoire utilise l'attribut de connexion utilisateur `userPrincipalName` au lieu de `mail`, entrez `userPrincipalName` Dans l'attribut correct dans le champ **User login attribute**.
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.

> Si vous êtes un utilisateur LDAP et que vous vous déconnectez, votre session prend fin immédiatement 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. ASTRA Control Center prend en charge jusqu'à 10,000 utilisateurs distants LDAP.

ASTRA Control Center utilise l'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.

Vous ne pouvez pas ajouter un utilisateur distant si un utilisateur local avec la même adresse e-mail (basée sur l'attribut « mail » ou « nom principal de l'utilisateur ») existe déjà sur le système. Pour ajouter l'utilisateur en tant qu'utilisateur distant, supprimez d'abord l'utilisateur local du système.

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 peuvent se connecter à Astra Control et héritent du même rôle que le groupe.

ASTRA Control Center prend en charge jusqu'à 5,000 groupes distants LDAP.

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 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**.

- **Si les ressources auxquelles vous accédez appartiennent à des clusters qui ont installé le dernier connecteur Astra** : lorsqu'un utilisateur reçoit plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes des rôles sont combinées. Par exemple, si un utilisateur doté d'un rôle de visualiseur local joint trois groupes liés au rôle membre, l'utilisateur dispose désormais d'un accès de rôle de visualiseur aux ressources d'origine ainsi que d'un accès de rôle membre aux ressources acquises via l'appartenance à un groupe.
- **Si les ressources auxquelles vous accédez appartiennent à des clusters qui n'ont pas installé Astra Connector** : lorsqu'un utilisateur reçoit plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus autorisé sont les seules qui prennent effet.

9. Sélectionnez **Ajouter**.

Résultat

Le nouveau groupe apparaît dans la liste des groupes distants. Les utilisateurs distants de ce groupe n'apparaissent pas dans la liste des utilisateurs distants tant que chaque utilisateur distant ne se connecte pas. 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 votre propre fichier kubeconfig, vous ne devez définir que l'élément de contexte **one**. Reportez-vous à la section "Documentation Kubernetes" pour plus d'informations sur la création de fichiers kubeconfig.

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.

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
- "[Aperçu technique Gérez un compartiment à l'aide d'une ressource personnalisée"]

> 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.
- Vous ne pouvez pas supprimer un compartiment WORM (Write Once, Read Many) avant l'expiration de la période de conservation du fournisseur cloud du compartiment. Les godets À VIS SANS FIN sont signalés par « verrouillé » à côté du nom du compartiment.

- 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.

Avant de commencer

- 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**.

[Aperçu technique] Gérez un compartiment à l'aide d'une ressource personnalisée

Vous pouvez ajouter un compartiment à l'aide d'une ressource personnalisée Astra Control (CR) sur le cluster d'applications. 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 utilisez la méthode de ressources personnalisées, la fonctionnalité de snapshots

d'applications requiert un compartiment.

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 ressource personnalisée du compartiment pour Astra Control est appelée AppVault. Ce CR contient les configurations nécessaires à l'utilisation d'un godet dans les opérations de protection.

Avant de commencer

- Assurez-vous que vous disposez d'un compartiment accessible depuis vos clusters gérés par Astra Control Center.
- Vérifiez que vous disposez des informations d'identification pour le compartiment.
- S'assurer que le godet est de l'un des types suivants :
  - NetApp ONTAP S3
  - NetApp StorageGRID S3
  - Microsoft Azure
  - S3 générique

Amazon Web Services (AWS) utilise 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. Créer le fichier de ressource personnalisée (CR) et le nommer (par exemple, `astra-appvault.yaml`).
2. Configurez les attributs suivants :
   - **metadata.name**: *(obligatoire)* le nom de la ressource personnalisée AppVault.
   - **Spec.prefix**: *(Facultatif)* chemin précédé des noms de toutes les entités stockées dans le AppVault.
   - **spec.providerConfig**: *(obligatoire)* stocke la configuration nécessaire pour accéder à AppVault à l'aide du fournisseur spécifié.
   - **spec.providerCredentials**: *(obligatoire)* stocke les références à toute information d'identification requise pour accéder à AppVault à l'aide du fournisseur spécifié.
     - **spec.providerCredentials.valueFromSecret**: *(Facultatif)* indique que la valeur d'identification doit provenir d'un secret.
       - **Key**: *(requis si valueFromSecret est utilisé)* la clé valide du secret à sélectionner.
       - **Nom**: *(requis si valueFromSecret est utilisé)* Nom du secret contenant la valeur de ce champ. Doit être dans le même espace de noms.
   - **spec.providerType**: *(obligatoire)* détermine ce qui fournit la sauvegarde, par exemple, NetApp ONTAP S3 ou Microsoft Azure.

     Exemple YAML :

```
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Après avoir renseigné le `astra-appvault.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```

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".

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.

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
- Modifier les détails de l'authentification du système back-end du stockage
- Gérez un système back-end de stockage découvert
- 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.

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.

Modifier les détails de l'authentification du système back-end du stockage

ASTRA Control Center offre deux modes d'authentification d'un backend ONTAP.

- **Authentification basée sur les informations d'identification** : le nom d'utilisateur et le mot de passe d'un utilisateur ONTAP avec les autorisations requises. Vous devez utiliser un rôle de connexion de sécurité prédéfini, tel que admin, pour garantir une compatibilité maximale avec les versions de ONTAP.
- **Authentification basée sur un certificat** : Astra Control Center peut également communiquer avec un cluster ONTAP à l'aide d'un certificat installé sur le back-end. Vous devez utiliser le certificat client, la clé et le certificat de l'autorité de certification approuvée, le cas échéant (recommandé).

Vous pouvez mettre à jour les systèmes back-end existants pour passer d'un type d'authentification à une autre méthode. Une seule méthode d'authentification est prise en charge à la fois.

Pour plus d'informations sur l'activation de l'authentification basée sur un certificat, reportez-vous à la section

"Activez l'authentification sur le back-end de stockage ONTAP".

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le champ informations d'identification, sélectionnez l'icône **Modifier**.
4. Dans la page Modifier, sélectionnez l'une des options suivantes.
   - **Utiliser les informations d'identification de l'administrateur** : saisissez l'adresse IP de gestion du cluster ONTAP et les informations d'identification de l'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.

   - **Utiliser un certificat**: Télécharger le certificat `.pem` fichier, la clé de certificat `.key` et éventuellement le fichier de l'autorité de certification.
5. Sélectionnez **Enregistrer**.

Gérez un système back-end de stockage découvert

Vous pouvez choisir de gérer un système back-end de stockage non géré, mais découvert. Lorsque vous gérez un système back-end de stockage, Astra Control indique si un certificat pour l'authentification a expiré.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez l'option **découvert**.
3. Sélectionnez le système back-end.
4. Dans le menu Options de la colonne **actions**, sélectionnez **gérer**.
5. Effectuez les modifications.
6. Sélectionnez **Enregistrer**.

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.

Avant de commencer

- 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".

[Aperçu technique] Gérez les applications Astra Control à l'aide de CRS

Gérez vos applications Astra Control à l'aide de ressources personnalisées Kubernetes (CR). Les options suivantes sont disponibles :

- "Définissez une application à l'aide d'une ressource personnalisée Kubernetes"
- "Gérez un compartiment à l'aide d'une ressource personnalisée"

Surveillez l'infrastructure avec des connexions Prometheus ou Fluentd

Vous pouvez configurer plusieurs paramètres en option pour améliorer votre expérience avec Astra Control Center. Pour surveiller l'ensemble de votre infrastructure et obtenir des informations exploitables, configurez Prometheus ou ajoutez une connexion Fluentd.

Si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour vous connecter à Internet (pour télécharger des packs de support sur le site de support NetApp), vous devez configurer un serveur proxy dans Astra Control Center.

- Connectez-vous à Prometheus
- Connectez-vous à Fluentd

Ajoutez un serveur proxy pour les connexions au site de support NetApp

Si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour vous connecter à Internet (pour télécharger des packs de support sur le site de support NetApp), vous devez configurer un serveur proxy dans Astra Control Center.

> 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.

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.

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 des 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 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 avez 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

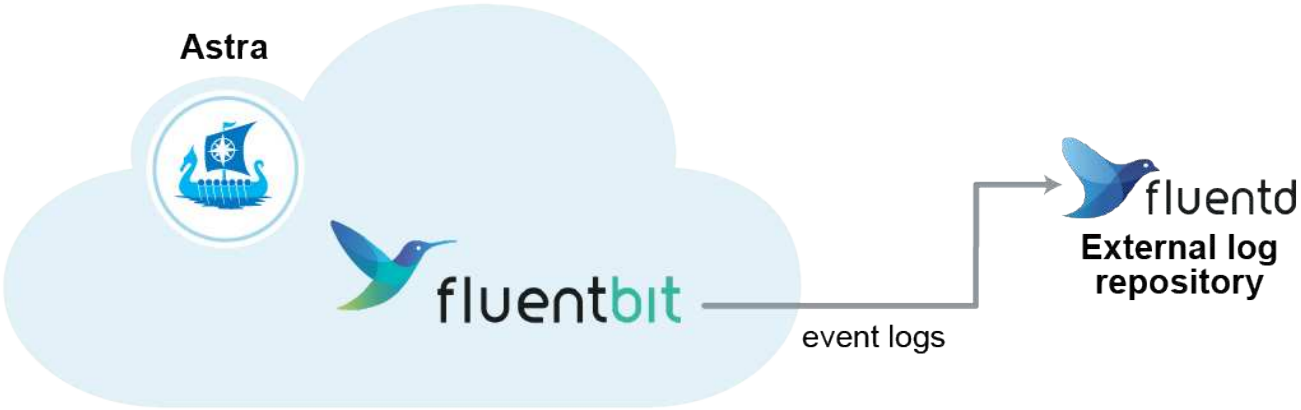
1. Dans un navigateur, entrez l'URL Prometheus.
2. Dans le menu Prometheus, sélectionnez **Graph**.
3. Pour utiliser l'Explorateur de mesures, sélectionnez l'icône en regard de **Exécuter**.
4. Sélectionnez `scrape_samples_scraped` Et sélectionnez **Exécuter**.
5. Pour voir le raclage des échantillons 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) à partir d'un système surveillé par Astra Control Center vers votre terminal Fluentd. La connexion Fluentd est désactivée par défaut.

Les connexions Fluentd ne sont pas prises en charge pour les clusters gérés avec des workflows Kubernetes déclaratifs. Vous pouvez connecter Fluentd uniquement aux clusters gérés avec des workflows non natifs Kubernetes.



Seuls les journaux d'événements des clusters gérés sont transférés à Fluentd.

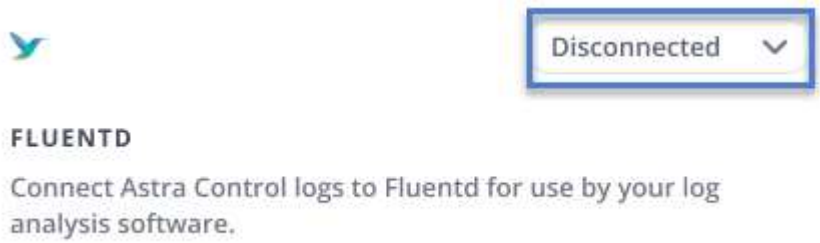
Avant de commencer

- 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.



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.

- ASTRA Control Provisioner ou Astra Trident ne seront pas désinstallés du cluster. "Découvrez comment désinstaller Astra 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.

L'annulation de la gestion du cluster supprime toutes les ressources qui ont été installées pour l'envoi de données de télémétrie.

Mettez à niveau Astra Control Center

Pour mettre à niveau Astra Control Center, téléchargez les images d'installation 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.

Ces instructions décrivent le processus de mise à niveau d'Astra Control Center, qui passe de la deuxième version la plus récente à cette version actuelle. Vous ne pouvez pas effectuer une mise à niveau directement à partir d'une version qui est à au moins deux versions derrière la version actuelle. Si la version d'Astra Control Center installée est plusieurs versions derrière la dernière version, vous devrez peut-être effectuer des mises à niveau de chaîne vers des versions plus récentes jusqu'à ce que votre Astra Control Center installée ne soit qu'une seule version derrière la dernière version. Pour obtenir la liste complète des versions publiées, reportez-vous au "notes de version".

Avant de commencer

Avant de procéder à la mise à niveau, assurez-vous que votre environnement respecte toujours le "Configuration minimale requise pour le déploiement d'Astra Control Center". Votre environnement doit disposer des éléments suivants :

- **Un activé "De provisionnement Astra Control" Avec Astra Trident en cours d'exécution**
  a. Déterminez la version d'Astra Trident que vous exécutez :

```
kubectl get tridentversion -n trident
```

Si vous exécutez Astra Trident 23.01 ou une version antérieure, utilisez-les "instructions" Pour effectuer une mise à niveau vers une version plus récente d'Astra Trident avant de passer à Astra Control Provisioner. Vous pouvez effectuer une mise à niveau directe vers Astra Control Provisioner 24.02 si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers Astra Control Provisioner 24.02.

  b. Vérifiez que le mécanisme de provisionnement Astra Control a été utilisé "activé". ASTRA Control

Provisioner ne fonctionnera pas avec les versions d'Astra Control Center antérieures à 23.10. Mettez à niveau votre mécanisme de provisionnement Astra Control afin qu'il dispose de la même version que l'Astra Control Center que vous mettez à niveau pour accéder aux toutes dernières fonctionnalités.

- **Une distribution Kubernetes prise en charge**

  Déterminez la version Kubernetes que vous exécutez :

  ```
  kubectl get nodes -o wide
  ```

- **Ressources du cluster suffisantes**

  Déterminer les ressources disponibles du cluster :

  ```
  kubectl describe node <node name>
  ```

- **Une classe de stockage par défaut**

  Déterminez votre classe de stockage par défaut :

  ```
  kubectl get storageclass
  ```

- **Services API sains et disponibles**

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

  ```
  kubectl get apiservices
  ```

- * (Registres locaux uniquement) Un registre local que vous pouvez utiliser pour envoyer et télécharger des images Astra Control Center*
- * (OpenShift uniquement) opérateurs de grappes sains et disponibles*

  S'assurer que tous les opérateurs du groupe d'instruments sont en état de fonctionnement et disponibles.

  ```
  kubectl get clusteroperators
  ```

Vous devez également tenir compte des points suivants :

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.

- **Accès au registre d'images NetApp Astra Control** :
  Vous avez la possibilité d'obtenir des images d'installation et des améliorations de fonctionnalités pour Astra Control, telles que Astra Control Provisioner, à partir du registre d'images NetApp.

a. Notez l'ID de votre compte Astra Control dont vous aurez besoin pour vous connecter au registre.

   Votre ID de compte s'affiche dans l'interface utilisateur web d'Astra Control Service. Sélectionnez l'icône de figure en haut à droite de la page, sélectionnez **API Access** et notez votre ID de compte.

b. A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.

c. Connectez-vous au registre Astra Control :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Déploiements de maillage de service Istio**
  Si vous avez installé un maillage de service Istio pendant l'installation d'Astra Control Center, cette mise à niveau d'Astra Control Center inclura le maillage de service Istio. Si vous n'avez pas encore de maillage de service, vous ne pouvez en installer qu'un pendant un "déploiement initial" D'Astra Control Center.

Description de la tâche

Le processus de mise à niveau d'Astra Control Center vous guide à travers les étapes de haut niveau suivantes :

> Déconnectez-vous de l'interface utilisateur de l'Astra Control Center avant de commencer la mise à niveau.

- Téléchargez et extrayez Astra Control Center
- Suivez les étapes supplémentaires si vous utilisez un 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.

Téléchargez et extrayez Astra Control Center

Téléchargez les images d'Astra Control Center à partir de l'un des emplacements suivants :

- **Registre d'images du service Astra Control** : utilisez cette option si vous n'utilisez pas de registre local avec les images d'Astra Control Center ou si vous préférez cette méthode au téléchargement du bundle à partir du site de support NetApp.
- **Site de support NetApp** : utilisez cette option si vous utilisez un registre local avec les images du Centre de contrôle Astra.

Registre d'images Astra Control

1. Connectez-vous à Astra Control Service.
2. Sur le tableau de bord, sélectionnez **Deploy a autogéré instance d'Astra Control**.
3. Suivez les instructions pour vous connecter au registre d'images Astra Control, extraire l'image d'installation d'Astra Control Center et extraire l'image.

Site de support NetApp

1. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`) du "Page de téléchargements d'Astra Control Center".
2. (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.

3. Extraire les images du pack Astra Control Center :

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

Suivez les étapes supplémentaires si vous utilisez un registre local

Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, vous devez utiliser le plug-in de ligne de commande NetApp Astra kubectl.

Retirez le plug-in NetApp Astra kubectl et réinstallez-le

Vous devez utiliser la dernière version du plug-in de ligne de commande NetApp Astra kubectl pour envoyer les images vers un référentiel Docker local.

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 et vous pouvez supprimer la version existante de kubectl-astra : `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

1. Si vous prévoyez d'envoyer le bundle Astra Control Center vers votre registre local, suivez la séquence d'étapes appropriée pour votre moteur de mise en conteneurs :

Docker

a. Accédez au répertoire racine du tarball. Vous devriez voir le `acc.manifest.bundle.yaml` et les répertoires suivants :

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. 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

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

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

c. 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=24.02.0-69
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
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
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://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Modifier le répertoire :

```
cd manifests
```

Poser le conducteur du centre de commande Astra mis à jour

1. (Registres locaux uniquement) si vous utilisez un registre local, procédez comme suit :

   a. Ouvrez le déploiement de l'opérateur Astra Control Center YAML :

   ```
   vim astra_control_center_operator_deploy.yaml
   ```

   Un échantillon annoté YAML suit ces étapes.

   b. 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}]
   ```

   c. Changer `ASTRA_IMAGE_REGISTRY` pour le `kube-rbac-proxy` image dans le chemin du registre où vous avez poussé les images dans un étape précédente.

   d. Changer `ASTRA_IMAGE_REGISTRY` pour le `acc-operator` image dans le chemin du registre où vous avez poussé les images dans un étape précédente.

   e. Ajoutez les valeurs suivantes à la `env` section :

   ```
   - name: ACCOP_HELM_UPGRADETIMEOUT
     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: ASTRA_IMAGE_REGISTRY/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: ASTRA_IMAGE_REGISTRY/acc-operator:24.02.68
        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
```

2. 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.as
tra.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
```

3. 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]
```

Un échantillon annoté YAML suit ces étapes.

2. Modifier le numéro de version de l'Astra (`astraVersion` intérieur de `spec`) de `23.10.0` à `24.02.0`:

Vous ne pouvez pas effectuer une mise à niveau directement à partir d'une version qui est à au moins deux versions derrière la version actuelle. Pour obtenir la liste complète des versions publiées, reportez-vous au "notes de version".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Modifiez le registre d'images :
   - (Registres locaux uniquement) si vous utilisez un registre local, vérifiez que le chemin du registre d'images correspond au chemin du registre auquel vous avez transmis les images dans un étape précédente. Mise à jour `imageRegistry` intérieur de `spec` si le registre local a changé depuis votre dernière installation.
   - (Registre d'images Astra Control) utilisez le registre d'images Astra Control (`cr.astra.netapp.io`) Vous avez utilisé pour télécharger le bundle Astra Control mis à jour.

```
  imageRegistry:
    name: "[cr.astra.netapp.io or 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
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Enregistrez et quittez l'éditeur de fichiers. Les modifications seront appliquées et la mise à niveau commencera.
7. (Facultatif) Vérifiez que les modules se terminent et deviennent disponibles à nouveau :

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

8. 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   24.02.0-69
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.

Mettez à niveau Astra Control Center à l'aide d'OpenShift OperatorHub

Si vous avez installé Astra Control Center à l'aide de son opérateur certifié Red Hat, vous pouvez mettre à niveau Astra Control Center à l'aide d'un opérateur mis à jour à partir d'OperatorHub. Utilisez cette procédure pour mettre à niveau Astra Control Center à partir du "Catalogue de l'écosystème Red Hat" Ou utilisez Red Hat OpenShift Container Platform.

Avant de commencer

- **Respecter les conditions préalables environnementales** : avant de procéder à la mise à niveau, assurez-vous que votre environnement respecte toujours le "Configuration minimale requise pour le déploiement d'Astra Control Center".
- **Assurez-vous que vous avez activé "De provisionnement Astra Control" Avec Astra Trident en cours d'exécution**
  a. Déterminez la version d'Astra Trident que vous exécutez :

```
kubectl get tridentversion -n trident
```

> Si vous exécutez Astra Trident 23.01 ou une version antérieure, utilisez-les "instructions" Pour effectuer une mise à niveau vers une version plus récente d'Astra Trident avant de passer à Astra Control Provisioner. Vous pouvez effectuer une mise à niveau directe vers Astra Control Provisioner 24.02 si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers Astra Control Provisioner 24.02.

  b. Vérifiez que le mécanisme de provisionnement Astra Control a été utilisé "activé". ASTRA Control Provisioner ne fonctionnera pas avec les versions d'Astra Control Center antérieures à 23.10. Mettez à niveau votre mécanisme de provisionnement Astra Control afin qu'il dispose de la même version que l'Astra Control Center que vous mettez à niveau pour accéder aux toutes dernières fonctionnalités.
- **Assurer la santé des opérateurs de grappes et des services API** :
  - 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
```

- **Autorisations OpenShift** : vous disposez de toutes les autorisations nécessaires et de l'accès à Red Hat OpenShift Container Platform pour effectuer les étapes de mise à niveau décrites.
- * (Pilote SAN ONTAP uniquement) Activer le multipath* : si vous utilisez un pilote SAN ONTAP, assurez-vous que le multipath est activé sur tous vos clusters Kubernetes.

Vous devez également tenir compte des points suivants :

- **Accéder au registre d'images NetApp Astra Control** :

  Vous avez la possibilité d'obtenir des images d'installation et des améliorations de fonctionnalités pour Astra Control, telles que Astra Control Provisioner, à partir du registre d'images NetApp.

  a. Notez l'ID de votre compte Astra Control dont vous aurez besoin pour vous connecter au registre.

     Votre ID de compte s'affiche dans l'interface utilisateur web d'Astra Control Service. Sélectionnez l'icône de figure en haut à droite de la page, sélectionnez **API Access** et notez votre ID de compte.

b. A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.

c. Connectez-vous au registre Astra Control :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

Étapes

- Accéder à la page d'installation de l'opérateur
- Désinstallez l'opérateur existant
- Installez le dernier opérateur
- Mettez à niveau Astra Control Center

Accéder à la page d'installation de l'opérateur

1. Complétez la procédure correspondante pour OpenShift Container Platform ou Ecosystem Catalog :

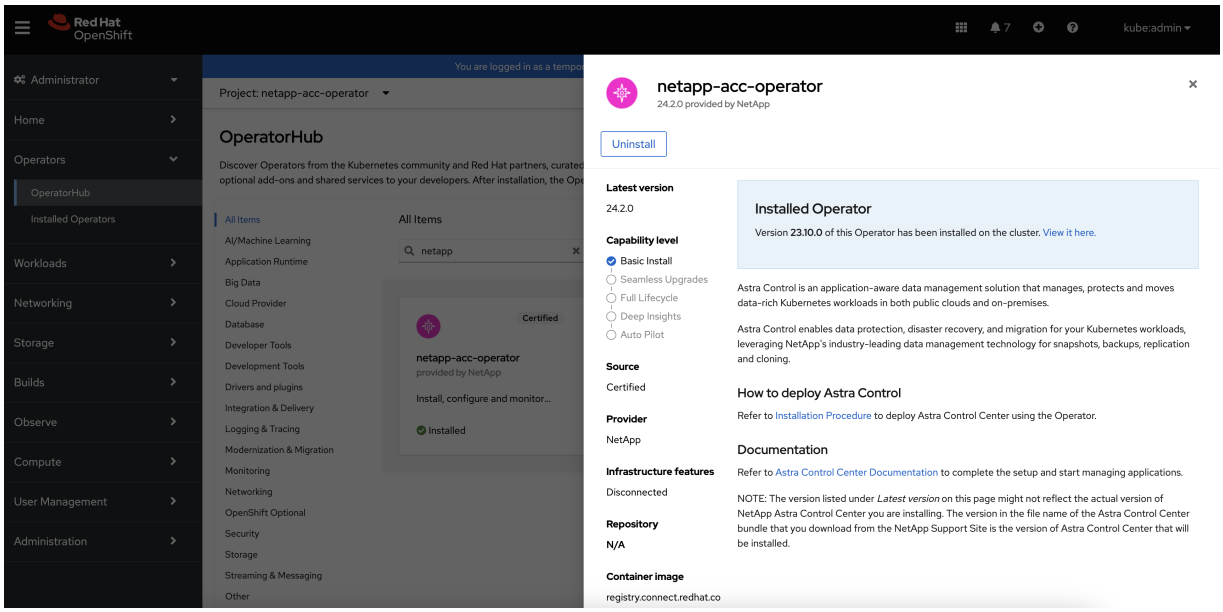
Console Web Red Hat OpenShift

a. Connectez-vous à l'interface utilisateur de OpenShift Container Platform.

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

> Vous ne pouvez effectuer la mise à niveau que vers la version actuelle d'Astra Control Center à l'aide de cet opérateur.

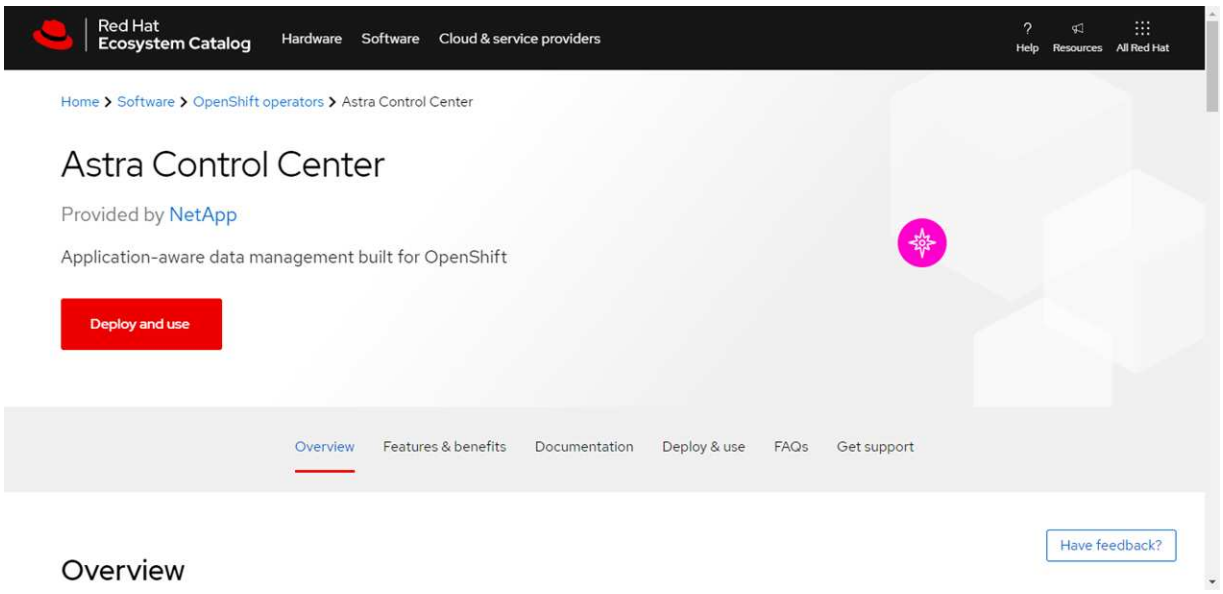
c. Recherchez `netapp-acc` Et sélectionnez l'opérateur du centre de contrôle Astra de NetApp.



Catalogue de l'écosystème Red Hat

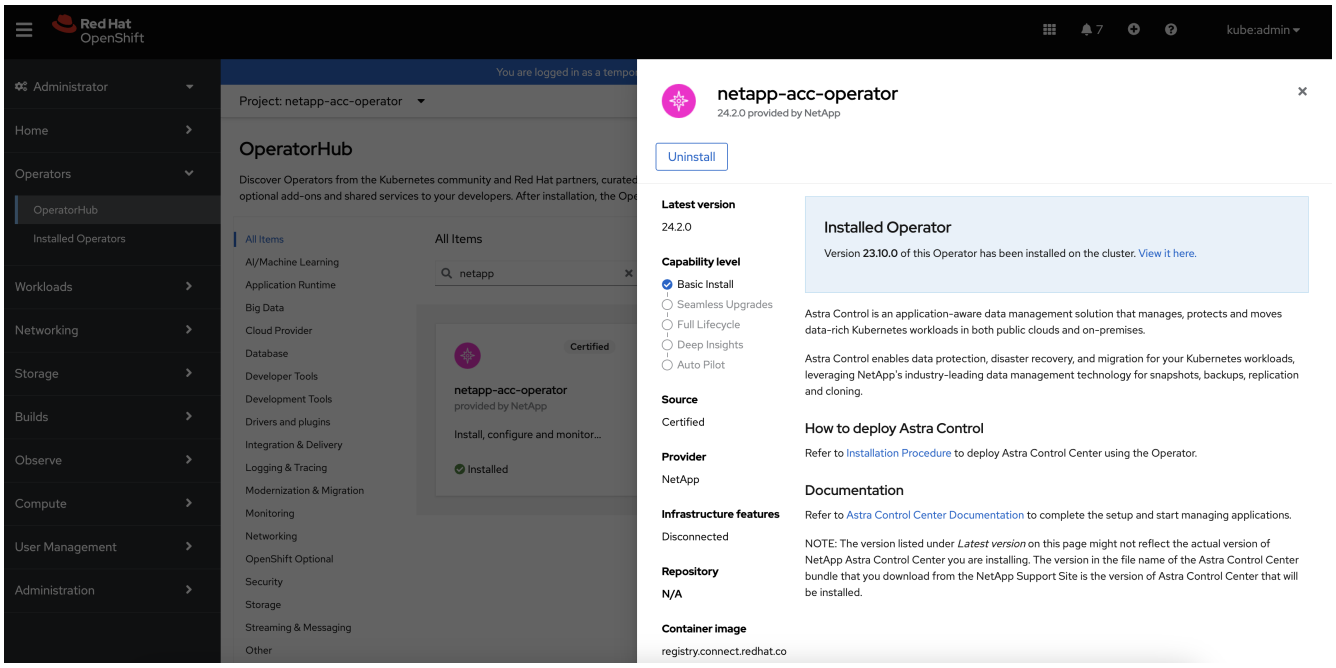
a. Sélectionnez le centre de contrôle NetApp Astra "opérateur".

b. Sélectionnez **déployer et utiliser**.



Désinstallez l’opérateur existant

1. Sur la page **netapp-acc-operator**, sélectionnez **Uninstall** pour supprimer votre opérateur existant.

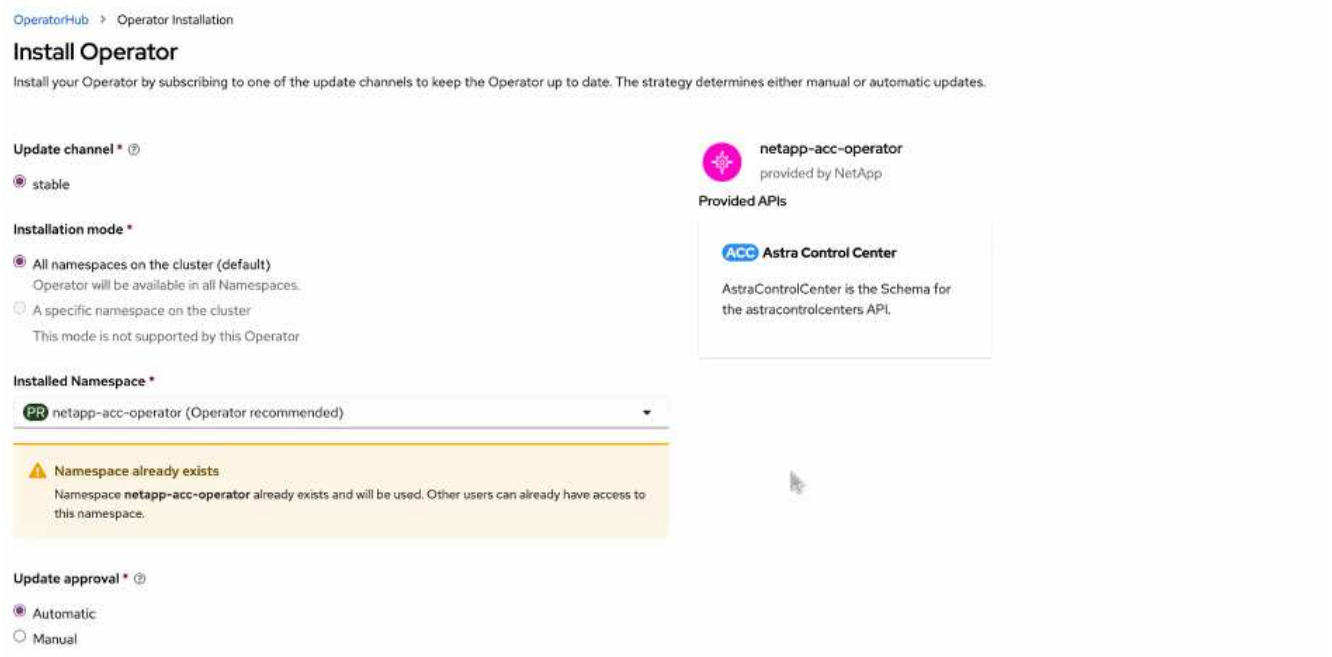


2. Confirmer l’opération

> Cette opération supprime l’opérateur netapp suivant, mais préserve l’espace de noms et les ressources associés d’origine, tels que les secrets.

Installez le dernier opérateur

1. Accédez au `netapp-acc` page opérateur à nouveau.
2. Complétez la page **installer l’opérateur** et installez l’opérateur le plus récent :



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

a. Sélectionnez l'opérateur `netapp-acc-operator` espace de noms (ou espace de noms personnalisé) restant de l'installation précédente de l'opérateur supprimé.

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

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

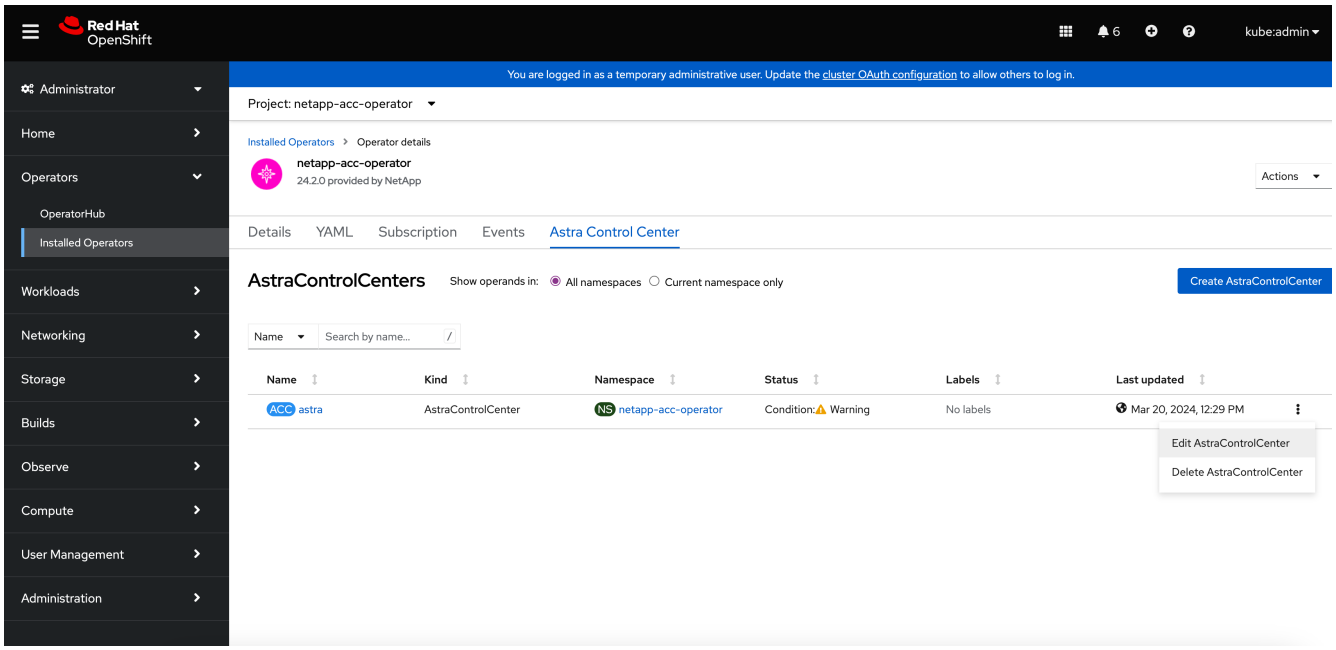
c. Sélectionnez **installer**.

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

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

Mettez à niveau Astra Control Center

1. Dans l'onglet opérateur Astra Control Center, sélectionnez Astra Control Center qui reste de l'installation précédente et sélectionnez **Edit AstraControlCenter**.



2. Mettez à jour le `AstraControlCenter` YAML :
   a. Entrez la dernière version d'Astra Control Center, par exemple 24.02.0-69.
   b. Dans `imageRegistry.name`, mettez à jour le chemin du registre d'images selon les besoins :
      - Si vous utilisez l'option de registre Astra Control, remplacez le chemin par `cr.astra.netapp.io`.
      - Si vous avez configuré un registre local, modifiez ou conservez le chemin du registre d'images local où vous avez poussé les images à l'étape précédente.

      > N'entrez pas `http://` ou `https://` dans le champ d'adresse.

   c. Mettez à jour le `imageRegistry.secret` au besoin.

      > Le processus de désinstallation par l'opérateur ne supprime pas les secrets existants. Vous n'avez besoin de mettre à jour ce champ que si vous créez un nouveau secret avec un nom différent du secret existant.

   d. Ajoutez les éléments suivants à votre `crds` configuration :

```
crds:
  shouldUpgrade: true
```

3. Enregistrez les modifications.
4. L'interface utilisateur vérifie que la mise à niveau a réussi.

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.

Avant de commencer

1. "Annulez la gestion de toutes les applications" sur les clusters.
2. "Dégérer tous les 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` (ou nom-personnalisé) espace de noms :

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

   Exemple de 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
middlewaretcps.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
middlewaretcps.traefik.containo.us
```

Trouvez plus d’informations

- "Problèmes connus de désinstallation"

Utilisez Astra Control Provisioner

Configurer le chiffrement du système back-end de stockage

Avec Astra Control Provisioner, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement pour le trafic entre votre cluster géré et le back-end de stockage.

ASTRA Control Provisioner prend en charge le chiffrement Kerberos pour deux types de systèmes back-end de stockage :

- **ONTAP** sur site - Astra Control provisionner prend en charge le chiffrement Kerberos sur les connexions NFSv3 et NFSv4 depuis les clusters Red Hat OpenShift et Kubernetes en amont vers les volumes ONTAP sur site.
- **Azure NetApp Files** - Astra Control Provisioner prend en charge le chiffrement Kerberos sur les connexions NFSv4.1 à partir de clusters Kubernetes en amont vers des volumes Azure NetApp Files.

Vous pouvez créer, supprimer, redimensionner, snapshot, cloner clone en lecture seule et importation des volumes qui utilisent le chiffrement NFS.

Configurez le chiffrement Kerberos à la volée avec les volumes ONTAP sur site

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un système back-end de stockage ONTAP sur site.

> Le chiffrement Kerberos pour le trafic NFS avec les systèmes back-end de stockage ONTAP sur site n'est pris en charge que par le `ontap-nas` pilote de stockage

Avant de commencer

- Vérifiez que vous avez "Mécanisme de provisionnement Astra Control activé" sur le cluster géré.
- Assurez-vous d'avoir accès au `tridentctl` informatique.
- Assurez-vous de disposer d'un accès administrateur au système back-end de stockage ONTAP.
- Assurez-vous de connaître le nom du ou des volumes que vous partagerez à partir du back-end de stockage ONTAP.
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP à prendre en charge le chiffrement Kerberos pour les volumes NFS. Reportez-vous à la section "Activez Kerberos sur une LIF donnée" pour obtenir des instructions.
- Vérifiez que tous les volumes NFSv4 utilisés avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "Guide des améliorations et des bonnes pratiques de NetApp NFSv4".

Ajoutez ou modifiez les règles d'export ONTAP

Vous devez ajouter des règles aux règles d'export ONTAP existantes ou créer de nouvelles règles d'export qui prennent en charge le chiffrement Kerberos pour le volume racine de la VM de stockage ONTAP ainsi que tous les volumes ONTAP partagés avec le cluster Kubernetes en amont. Les règles d'export-policy que vous ajoutez ou les nouvelles règles d'export que vous créez doivent prendre en charge les protocoles d'accès et autorisations d'accès suivants :

Protocoles d'accès

Configurez la export policy avec les protocoles d'accès NFS, NFSv3 et NFSv4.

Accédez aux informations

Vous pouvez configurer l'une des trois versions différentes du cryptage Kerberos, en fonction de vos besoins pour le volume :

- **Kerberos 5** - (authentification et cryptage)
- **Kerberos 5i** - (authentification et chiffrement avec protection d'identité)
- **Kerberos 5p** - (authentification et chiffrement avec protection de l'identité et de la vie privée)

Configurez la règle d'export ONTAP avec les autorisations d'accès appropriées. Par exemple, si les clusters montant les volumes NFS avec un mélange de cryptage Kerberos 5i et Kerberos 5p, utilisez les paramètres d'accès suivants :

Type	Accès en lecture seule	Accès en lecture/écriture	Accès superutilisateur
UNIX	Activé	Activé	Activé
Kerberos 5i	Activé	Activé	Activé
Kerberos 5p	Activé	Activé	Activé

Pour plus d'informations sur la création de règles d'export ONTAP et de règles d'export-policy, reportez-vous à la documentation suivante :

- "Créer une export-policy"
- "Ajouter une règle à une export-policy"

Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Astra Control Provisioner qui inclut une fonctionnalité de chiffrement Kerberos.

Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `spec.nfsMountOptions` paramètre :

- `spec.nfsMountOptions: sec=krb5` (authentification et chiffrement)
- `spec.nfsMountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `spec.nfsMountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de cryptage Kerberos dans la liste des paramètres, seule la première option est utilisée.

Étapes

1. Sur le cluster géré, créez un fichier de configuration du back-end de stockage à l'aide de l'exemple suivant. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

```
tridentctl create backend -f <backend-configuration-file>
```

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez exécuter de nouveau la commande create.

Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec le chiffrement Kerberos.

Description de la tâche

Lorsque vous créez un objet de classe de stockage, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `mountOptions` paramètre :

- `mountOptions: sec=krb5` (authentification et chiffrement)
- `mountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `mountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de cryptage Kerberos dans la liste des paramètres, seule la première option est utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du back-end de stockage est différent du niveau que vous spécifiez dans l'objet classe de stockage, l'objet classe de stockage a priorité.

Étapes

1. Créez un objet StorageClass Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Créer la classe de stockage :

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc ontap-nas-sc
```

   Vous devez voir les résultats similaires à ce qui suit :

```
NAME            PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Reportez-vous à ces instructions pour "le provisionnement d'un volume".

Configurez le chiffrement Kerberos à la volée avec les volumes Azure NetApp Files

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un seul système back-end de stockage Azure NetApp Files ou un pool virtuel de systèmes back-end de stockage Azure NetApp Files.

Avant de commencer

- Vérifiez que vous avez activé Astra Control Provisioner sur le cluster Red Hat OpenShift géré. Reportez-vous à la section "Activez le mécanisme de provisionnement Astra Control" pour obtenir des instructions.
- Assurez-vous d'avoir accès au `tridentctl` informatique.
- Assurez-vous d'avoir préparé le système back-end de stockage Azure NetApp Files pour le chiffrement Kerberos en notant les exigences et en suivant les instructions de la section "Documentation Azure NetApp Files".
- Vérifiez que tous les volumes NFSv4 utilisés avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "Guide des améliorations et des bonnes pratiques de NetApp NFSv4".

Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Azure NetApp Files qui inclut une fonctionnalité de chiffrement Kerberos.

Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le cryptage Kerberos, vous pouvez le définir de manière à ce qu'il soit appliqué à l'un des deux niveaux possibles :

- Le **niveau du backend de stockage** utilisant le `spec.kerberos` légale
- **Niveau de pool virtuel** utilisant le `spec.storage.kerberos` légale

Lorsque vous définissez la configuration au niveau du pool virtuel, le pool est sélectionné à l'aide du libellé de la classe de stockage.

À chaque niveau, vous pouvez spécifier l'une des trois versions différentes du cryptage Kerberos :

- `kerberos: sec=krb5` (authentification et chiffrement)
- `kerberos: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `kerberos: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Étapes

1. Sur le cluster géré, créez un fichier de configuration back-end de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le back-end de stockage (niveau du back-end de stockage ou niveau du pool virtuel). Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

Exemple au niveau du back-end de stockage

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Exemple de pool virtuel

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

```
tridentctl create backend -f <backend-configuration-file>
```

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez exécuter de nouveau la commande create.

Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec le chiffrement Kerberos.

Étapes

1. Créez un objet StorageClass Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Créer la classe de stockage :

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc anf-sc-nfs
```

Vous devez voir les résultats similaires à ce qui suit :

```
NAME          PROVISIONER             AGE
anf-sc-nfs    csi.trident.netapp.io   15h
```

Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Reportez-vous à ces instructions pour "le provisionnement d'un volume".

Restaurer les données de volume à l'aide d'un snapshot

ASTRA Control Provisioner assure une restauration rapide de volume sur place à partir d'une copie Snapshot à l'aide du `TridentActionSnapshotRestore` (TASR) CR. Cette CR fonctionne comme une action Kubernetes impérative et ne persiste pas une

fois l'opération terminée.

ASTRA Control Provisioner prend en charge la restauration Snapshot sur le `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, et `solidfire-san` pilotes.

Avant de commencer

Vous devez disposer d'une demande de volume liée et d'un instantané de volume disponible.

- Vérifiez que l'état de la demande de volume persistant est lié.

```
kubectl get pvc
```

- Vérifiez que le snapshot du volume est prêt à être utilisé.

```
kubectl get vs
```

Étapes

1. Créer la CR TASR. Cet exemple crée une demande de modification pour la demande de volume persistant `pvc1` et le snapshot de volume `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: trident.netapp.io/v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Appliquez la CR pour effectuer une restauration à partir de l'instantané. Cet exemple permet de restaurer des données à partir d'un snapshot `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Résultats

ASTRA Control Provisioner restaure les données à partir du snapshot. Vous pouvez vérifier l'état de la restauration des snapshots.

```
kubectl get tasr -o yaml

apiVersion: trident.netapp.io/v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- Dans la plupart des cas, Astra Control Provisioner ne réessaiera pas automatiquement l'opération en cas de panne. Vous devrez exécuter à nouveau l'opération.
- Les utilisateurs Kubernetes sans accès administrateur peuvent avoir à obtenir l'autorisation de l'administrateur pour créer une CR ASR dans l'espace de noms de leur application.

Réplication de volumes à l'aide de SnapMirror

À l'aide d'Astra Control Provisioner, vous pouvez créer des relations de miroir entre un volume source sur un cluster et le volume de destination sur le cluster peering pour la réplication des données pour la reprise après incident. Vous pouvez utiliser une définition de ressource personnalisée (CRD) avec un espace de nom pour effectuer les opérations suivantes :

- Création de relations de symétrie entre les volumes (ESV)
- Supprimez les relations de symétrie entre les volumes
- Rompez les relations de symétrie
- Promotion du volume secondaire en cas d'incident (basculements)
- Transition sans perte des applications d'un cluster à un autre (en cas de basculements ou de migrations planifiés)

Conditions préalables à la réplication

Assurez-vous que les conditions préalables suivantes sont remplies avant de commencer :

Clusters ONTAP

- **Astra Control Provisioner** : Astra Control Provisioner version 23.10 ou ultérieure ou a "Prise en charge d'Astra Trident" Doit exister sur les clusters Kubernetes source et destination qui utilisent ONTAP en tant que back-end.
- **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Reportez-vous à la section "Présentation des licences SnapMirror dans ONTAP" pour en savoir plus.

Peering

- **Cluster et SVM** : les systèmes back-end de stockage ONTAP doivent être peering. Reportez-vous à la section "Présentation du cluster et de SVM peering" pour en savoir plus.

> S'assurer que les noms de SVM utilisés dans la relation de réplication entre deux clusters ONTAP sont uniques.

- **Astra Control Provisioner et SVM** : les SVM distants à peering doivent être disponibles pour Astra Control Provisioner sur le cluster de destination.

Pilotes pris en charge

- La réplication de volume est prise en charge pour les pilotes ontap-nas et ontap-san.

Créer une demande de volume persistant en miroir

Suivez ces étapes et utilisez les exemples CRD pour créer une relation miroir entre les volumes principal et secondaire.

Étapes

1. Effectuez les étapes suivantes sur le cluster Kubernetes principal :
   a. Créez un objet StorageClass avec le `trident.netapp.io/replication: true` paramètre.

      Exemple

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        backendType: "ontap-nas"
        fsType: "nfs"
        trident.netapp.io/replication: "true"
      ```

   b. Créez une demande de volume persistant avec une classe de stockage précédemment créée.

Exemple

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Créez une demande de modification MirrorRelationship avec des informations locales.

Exemple

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

ASTRA Control Provisioner récupère les informations internes du volume et l'état actuel de la protection des données (DP) du volume, puis remplit le champ d'état de MirrorRelationship.

d. Obtenir le CR TridentMirrorRelationship pour obtenir le nom interne et la SVM du PVC.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Effectuez les étapes suivantes sur le cluster Kubernetes secondaire :
   a. Créez une classe de stockage avec le paramètre trident.netapp.io/replication: true.

      Exemple

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Créez une demande de modification MirrorRelationship avec les informations de destination et de source.

      Exemple

      ```
      kind: TridentMirrorRelationship
      apiVersion: trident.netapp.io/v1
      metadata:
        name: csi-nas
      spec:
        state: established
        volumeMappings:
        - localPVCName: csi-nas
          remoteVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      ```

ASTRA Control Provisioner crée une relation SnapMirror avec le nom de la stratégie de relation configurée (ou par défaut pour ONTAP) et l'initialise.

c. Créez une demande de volume persistant avec une classe de stockage précédemment créée pour agir en tant que classe secondaire (destination SnapMirror).

Exemple

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

ASTRA Control Provisioner vérifiera le CRD TridentMirrorRelationship et ne créera pas le volume si la relation n'existe pas. Si la relation existe, Astra Control Provisioner s'assurera que le nouveau volume FlexVol est placé sur un SVM peering avec le SVM distant défini dans le MirrorRelationship.

États de réplication des volumes

Une relation de miroir Trident (TMR) est une relation CRD qui représente une extrémité d'une relation de réplication entre les ESV. La TMR de destination a un état qui indique à Astra Control provisionner l'état souhaité. La TMR de destination a les États suivants :

- **Établi** : le PVC local est le volume de destination d'une relation miroir, et il s'agit d'une nouvelle relation.
- **Promu**: Le PVC local est ReadWrite et montable, sans relation de miroir actuellement en vigueur.
- **Rétabli**: Le PVC local est le volume de destination d'une relation miroir et était également auparavant dans cette relation miroir.
  - L'état rétabli doit être utilisé si le volume de destination était déjà en relation avec le volume source car il écrase le contenu du volume de destination.
  - L'état rétabli échouera si le volume n'était pas auparavant dans une relation avec la source.

Promotion de la demande de volume persistant secondaire en cas de basculement non planifié

Effectuez l'étape suivante sur le cluster Kubernetes secondaire :

- Mettez à jour le champ *spec.state* de TridentMirrorRelationship vers `promoted`.

Promotion de la demande de volume persistant secondaire lors d'un basculement planifié

Lors d'un basculement planifié (migration), effectuez les étapes suivantes pour promouvoir la demande de volume persistant secondaire :

Étapes

1. Sur le cluster Kubernetes principal, créez un snapshot de la demande de volume persistant et attendez que le snapshot soit créé.
2. Sur le cluster Kubernetes principal, créez la CR SnapshotInfo pour obtenir des informations internes.

   Exemple

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. Sur le cluster Kubernetes secondaire, mettez à jour le champ *spec.state* du *TridentMirrorRelationship* CR en *promu* et *spec.promotedSnapshotHandle* en tant que nom interne du snapshot.
4. Sur le cluster Kubernetes secondaire, confirmez l'état (champ status.state) de TridentMirrorRelationship à promu.

Restaurer une relation de miroir après un basculement

Avant de restaurer une relation de symétrie, choisissez le côté que vous voulez faire comme nouveau principal.

Étapes

1. Sur le cluster Kubernetes secondaire, assurez-vous que les valeurs du champ *spec.remoteVolumeHandle* du champ TridentMirrorRelationship sont mises à jour.
2. Sur le cluster Kubernetes secondaire, mettez à jour le champ *spec.mirror* de TridentMirrorRelationship vers `reestablished`.

Opérations supplémentaires

ASTRA Control Provisioner prend en charge les opérations suivantes sur les volumes principal et secondaire :

Répliquer la demande de volume persistant primaire sur une nouvelle demande de volume secondaire

Assurez-vous que vous avez déjà un PVC primaire et un PVC secondaire.

Étapes

1. Supprimez les CRD PersistentVolumeClaim et TridentMirrorRelationship du cluster secondaire (destination) établi.
2. Supprimez le CRD TridentMirrorRelationship du cluster principal (source).
3. Créez un nouveau CRD TridentMirrorRelationship sur le cluster principal (source) pour le nouveau PVC

secondaire (destination) que vous souhaitez établir.

Redimensionner une PVC en miroir, principale ou secondaire

La demande de volume persistant peut être redimensionnée normalement, ONTAP étendra automatiquement les flevxols de destination si la quantité de données dépasse la taille actuelle.

Supprimer la réplication d'une demande de volume persistant

Pour supprimer la réplication, effectuez l'une des opérations suivantes sur le volume secondaire actuel :

- Supprimez MirrorRelationship sur le PVC secondaire. Cela interrompt la relation de réplication.
- Ou, mettez à jour le champ spec.state à *promu*.

Suppression d'une demande de volume persistant (qui était auparavant mise en miroir)

Le mécanisme de provisionnement Astra Control vérifie si des demandes de volume persistant sont répliquées et libère la relation de réplication avant toute tentative de suppression du volume.

Supprimer une TMR

La suppression d'une TMR d'un côté d'une relation symétrique entraîne la transition de la TMR restante vers l'état *promu* avant que Astra Control Provisioner ne termine la suppression. Si la TMR sélectionnée pour la suppression est déjà à l'état *promoted*, il n'y a pas de relation miroir existante et la TMR sera supprimée et Astra Control Provisioner promouvra le PVC local à *ReadWrite*. Cette suppression libère les métadonnées SnapMirror pour le volume local dans ONTAP. Si ce volume est utilisé dans une relation miroir à l'avenir, il doit utiliser une nouvelle TMR avec un état de réplication *établi* volume lors de la création de la nouvelle relation miroir.

Mettre à jour les relations miroir lorsque ONTAP est en ligne

Les relations miroir peuvent être mises à jour à tout moment après leur établissement. Vous pouvez utiliser le `state: promoted` ou `state: reestablished` champs permettant de mettre à jour les relations. Lors de la promotion d'un volume de destination en volume ReadWrite standard, vous pouvez utiliser *promotedSnapshotHandle* pour spécifier un snapshot spécifique dans lequel restaurer le volume actuel.

Mettre à jour les relations en miroir lorsque ONTAP est hors ligne

Vous pouvez utiliser un CRD pour effectuer une mise à jour SnapMirror sans qu'Astra Control ne dispose d'une connectivité directe au cluster ONTAP. Reportez-vous à l'exemple de format de TridentActionMirrorUpdate suivant :

Exemple

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Reflète l'état du CRD TridentActionMirrorUpdate. Il peut prendre une valeur de *succeed*, *In Progress* ou *FAILED*.

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 Control"

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 discorde. 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 discorde 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 :

- **"Utiliser la base de connaissances** (connexion requise)": Recherchez des articles, des FAQ, ou des renseignements sur les réparations en rapport avec Astra Control.
- **Reportez-vous à la documentation du produit** : il s'agit du site doc que vous consultez actuellement.
- **"Obtenir de l'aide par discorde"**: 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.
   - Utilisez Digital Advisor.

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 d'Astra Control Center 23.10"
- "Documentation d'Astra Control Center 23.07"
- "Documentation d'Astra Control Center 23.04"
- "Documentation Astra Control Center 22.11"
- "Documentation Astra Control Center 22.08"
- "Documentation Astra Control Center 22.04"
- "Documentation Astra Control Center 21.12"
- "Documentation Astra Control Center 21.08"

Foire aux questions

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 Astra Control ?

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 une licence d'évaluation. Comment passer à la licence complète ?

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **compte** > **Licence**.
2. Dans la vue d'ensemble de la licence, à droite des informations de licence, sélectionnez le menu Options.
3. Sélectionnez **remplacer**.
4. Naviguez jusqu'au fichier de licence que vous avez téléchargé et sélectionnez **Ajouter**.

J'utilise une licence d'évaluation. Est-il toujours possible de gérer des applications ?

Oui, vous pouvez tester la fonctionnalité de gestion des applications avec une licence d'évaluation (y compris la licence d'évaluation intégrée installée par défaut). Il n'y a pas de différence entre les capacités ou les fonctionnalités d'une licence d'évaluation et d'une licence complète; la licence d'évaluation a simplement une durée de vie plus courte. Reportez-vous à la section "Licences" pour en savoir plus.

Enregistrement des clusters Kubernetes

Je dois ajouter des nœuds workers à mon cluster Kubernetes après l'ajout d'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 gérer 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 mes données après la suppression du 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.

Est-ce que le mécanisme de provisionnement Astra Control (ou Astra Trident) est automatiquement désinstallé d'un cluster lorsque je ne le gère pas ?

Lorsque vous dégérez un cluster depuis Astra Control Center, Astra Control Provisioner ou Astra Trident n'est pas automatiquement désinstallé du cluster. Pour désinstaller Astra Control Provisioner et ses composants ou Astra Trident, vous devez le faire "Procédez comme suit pour désinstaller l'instance Astra Trident qui contient le service Astra Control Provisioner".

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.

Qu'arrive-t-il aux applications après l'arrêt de leur gestion depuis 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 non NetApp ?

Non Même si Astra Control peut détecter les applications qui utilisent un stockage non-NetApp, il ne peut pas gérer une application utilisant un stockage non-NetApp.

Dois-je gérer Astra Control elle-même ?

ASTRA Control Center n'est pas affiché par défaut en tant qu'application que vous pouvez gérer, mais vous le pouvez "sauvegarde et restauration" Instance Astra Control Center utilisant une autre instance Astra Control Center.

Les pods défectueux affectent-ils la gestion des applications ?

Non, l'état des pods n'a pas d'impact sur la gestion des applications.

Les opérations de gestion des données

Mon application utilise plusieurs volumes persistants. ASTRA Control prendra-t-il des copies Snapshot 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 snapshots 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.

De provisionnement Astra Control

En quoi les fonctionnalités de provisionnement du stockage d'Astra Control Provisioner sont-elles différentes de celles d'Astra Trident ?

ASTRA Control Provisioner, dans le cadre d'Astra Control, prend en charge un ensemble complet de fonctionnalités de provisionnement du stockage qui ne sont pas disponibles dans Astra Trident open source. Ces fonctionnalités viennent s'ajouter à toutes les fonctionnalités disponibles pour Trident open source.

Le mécanisme de provisionnement Astra Control remplace-t-il Astra Trident ?

ASTRA Control Provisioner a remplacé Astra Trident en tant que mécanisme de provisionnement et d'orchestration du stockage dans l'architecture Astra Control. Les utilisateurs d'Astra Control devraient "Activez le mécanisme de provisionnement Astra Control" Utilisation d'Astra Control ASTRA Trident sera toujours pris en charge dans cette version, mais ne le sera pas dans les prochaines versions. ASTRA Trident demeurera une solution open source et sera publié, maintenu, pris en charge et mis à jour avec le nouveau CSI et d'autres fonctionnalités de NetApp. Seul le mécanisme de provisionnement Astra Control, qui contient la fonctionnalité Astra Trident CSI et des fonctionnalités de gestion du stockage étendues, peut être utilisé avec les prochaines versions d'Astra Control.

Dois-je payer pour Astra Trident ?

Non ASTRA Trident continuera d'être open source et téléchargeable gratuitement. L'utilisation de la fonctionnalité Astra Control Provisioner nécessite maintenant une licence Astra Control.

Puis-je utiliser les fonctionnalités de gestion et de provisionnement du stockage dans Astra Control sans installer et utiliser toutes les fonctionnalités d'Astra Control ?

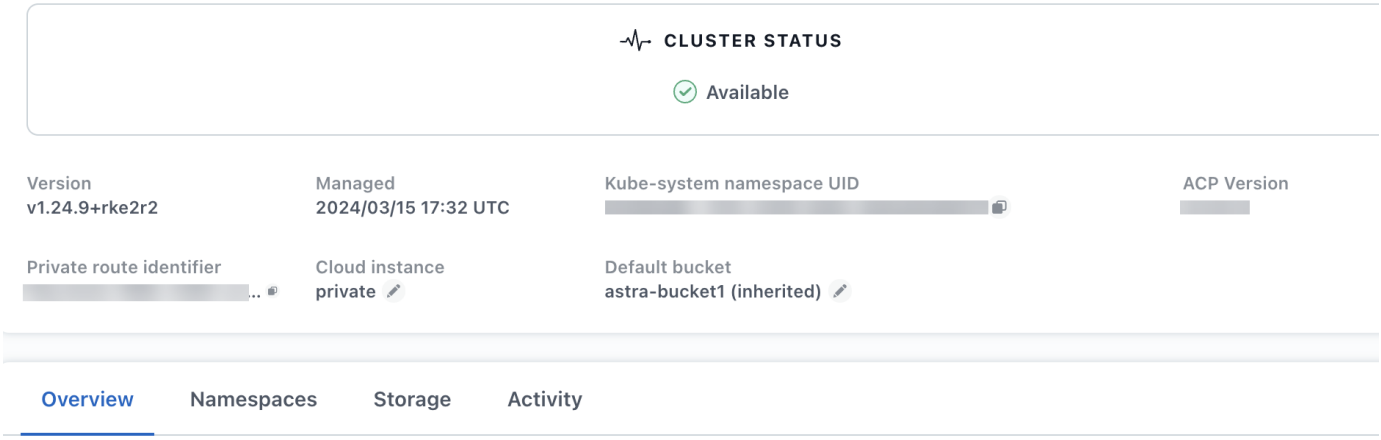
Oui, vous pouvez effectuer une mise à niveau vers Astra Control provisionner et utiliser sa fonctionnalité même si vous ne souhaitez pas utiliser l'ensemble complet de fonctionnalités de gestion de données Astra Control.

Comment passer d'un système Astra Trident existant à Astra Control en vue d'utiliser la fonctionnalité avancée de gestion et de provisionnement du stockage ?

Si vous utilisez Astra Trident (y compris les utilisateurs d'Astra Trident dans le cloud public), vous devez d'abord acquérir une licence Astra Control. À cette fin, vous pouvez télécharger le bundle Astra Control Provisioner, mettre à niveau Astra Trident et "Activez la fonctionnalité Astra Control Provisioner".

Comment savoir si Astra Control Provisioner a remplacé Astra Trident sur mon cluster ?

Une fois Astra Control Provisioner installé, le cluster hôte dans l'interface utilisateur Astra Control affiche un `ACP version` plutôt que `Trident version` et le numéro de version actuellement installé.



Si vous n’avez pas accès à l’interface utilisateur, vous pouvez confirmer que l’installation a réussi en utilisant les méthodes suivantes :

Opérateur Astra Trident

Vérifiez le `trident-acp` le conteneur est en cours d'exécution `acpVersion` est `23.10.0` ou ultérieure (23.10 est la version minimale) avec un état de `Installed`:

```
kubectl get torc -o yaml
```

Réponse :

```
status:
  acpVersion: 24.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:24.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

Vérifiez que le mécanisme de provisionnement Astra Control a été activé :

```
./tridentctl -n trident version
```

Réponse :

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 24.10.0 | 24.10.0 | 24.10.0. | +----------------
+----------------+-------------+
```

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/"

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/"

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/"

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