Documentation Astra Control Center 22.08

Astra Control Center

NetApp
November 21, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-center-2208/index.html on November 21, 2023. Always check docs.netapp.com for the latest.

Sommaire

Documentation Astra Control Center 22.08

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"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"
- "Limites connues"

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

Nouveautés de cette version d'Astra Control Center

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

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"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"
- "Restrictions connues pour cette version"

26 avril 2022 (22.04.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Déploiement d'un magasin de données Astra Control Center"
- "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"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"
- "Restrictions connues pour cette version"

14 décembre 2021 (21.12)

Détails

Nouvelles fonctionnalités et prises en charge

- "Restauration des applications"
- "Crochets d'exécution"
- "Prise en charge des applications déployées avec des opérateurs du système namespace"
- "Prise en charge supplémentaire de Kubernetes et Rancher en amont"
- "Découvrez la gestion et la surveillance du système back-end avec Astra Data Store"
- "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"
- "Problèmes connus avec la présentation d'Astra Data Store et ce centre de contrôle Astra"
- "Restrictions connues pour cette version"

5 août 2021 (21.08)

Détails

Lancement initial du centre de contrôle Astra.

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

Trouvez plus d'informations

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"
- "Documentation Astra Data Store"
- "Versions antérieures de la documentation Astra Control Center"

Problèmes connus

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

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

En applications

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

Clusters

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

Autres questions

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

- Les snapshots peuvent échouer avec la version 4.2.0 du contrôleur de snapshot

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

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

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

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

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

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

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

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

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

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

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

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

Les 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.

Les snapshots peuvent échouer avec la version 4.2.0 du contrôleur de snapshot

Lorsque vous utilisez le snapshot-contrôleur Kubernetes (également appelé External-snapshotter) version 4.2.0 avec Kubernetes 1.20 ou 1.21, les snapshots peuvent échouer. Pour éviter cela, utilisez un autre "version prise en charge" D'un snapshoter externe, comme la version 4.2.1, avec Kubernetes version 1.20 ou 1.21.

1. Exécutez un appel POST pour ajouter un fichier kubeconfig mis à jour au `/credentials` et récupérer le noeud final affecté `id` du corps de réponse.
2. Effectuer un APPEL PUT à partir du `/clusters` À l'aide de l'ID de cluster approprié et définissez le `credentialID` à la `id` valeur de l'étape précédente.

Une fois ces étapes terminées, les informations d'identification associées au cluster sont mises à jour et le cluster doit se reconnecter et mettre à jour son état sur `available`.

Trouvez plus d'informations

- "Problèmes connus avec la présentation d'Astra Data Store et ce centre de contrôle Astra"
- "Limites connues"

Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra

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

"Découvrez d'autres problèmes connus avec le data Store d'Astra" Il pourrait donc avoir un impact sur la gestion du magasin de données Astra avec la version actuelle du centre de contrôle Astra.

Les détails du volume du magasin de données Astra n'apparaissent pas dans la page Storage Backend de l'interface utilisateur du centre de contrôle Astra

Des détails tels que la capacité et le débit n'apparaissent pas dans l'interface utilisateur. Lorsque ce problème se produit, annulez la gestion du stockage back-end et ajoutez-end à nouveau.

La dégestion d'un cluster avec Astra Data Store requiert d'abord la suppression d'une application système gérée

Si vous avez ajouté un cluster contenant Astra Data Store à un cluster Astra Control Center, l'application système astrads est gérée par défaut comme une application masquée. Pour annuler la gestion du cluster, vous devez d'abord annuler la gestion de l'application système astrads. Vous ne pouvez pas annuler la gestion de ce type d'application à l'aide de l'interface utilisateur du centre de contrôle Astra. Utilisez plutôt une demande d'API de contrôle Astra pour supprimer manuellement l'application :

Détails

Étapes

1. Obtenez l'ID du cluster géré à l'aide de cette API :

```
/accounts/{account_id}/topology/v1/managedClusters
```

Réponse :

```
{
"items": [
{
"type": "application/astra-managedCluster",
"version": "1.1",
"id": "123ab987-0bc0-00d0-a00a-1234567abd8d",
"name": "astrads-cluster-1234567",
...
```

2. Obtenir l'ID d'application du système astrads géré :

```
/accounts/{account_id}/topology/v2/managedClusters/{managedCluster_id}/apps
```

Réponse :

```
{
  "items": [
    [
      "1b011d11-bb88-40c7-a1a1-ab1234c123d3",
      "astrads-system",
      "ready"
    ]
  ],
  "metadata": {}
}
```

3. Supprimez l'application système astrads à l'aide de l'ID d'application que vous avez acquis à l'étape précédente (`1b011d11-bb88-40c7-a1a1-ab1234c123d3`).

```
/accounts/{account_id}/k8s/v2/apps/{astrads-system_app_id}
```

Trouvez plus d'informations

- "Problèmes connus"
- "Limites connues"

Limites connues

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

Limites de gestion du cluster

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

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

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

Limites de gestion des applications

- Les clones des applications installées à l'aide d'opérateurs pass-by-Reference peuvent échouer
- Les opérations de restauration sur place des applications qui utilisent un gestionnaire de certificats ne sont pas prises en charge
- Applications activées par OLM et déployées par l'opérateur à étendue de cluster non prises en charge
- Les applications déployées avec Helm 2 ne sont pas prises en charge

Limitations générales

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

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 carte de configuration kubeadm-config :

```
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 espace de noms par une opération de clonage ou de restauration, le compte admin/propriétaire peut modifier le `member` contraintes de compte d'utilisateur et de rôle de mise à jour pour l'utilisateur affecté pour accorder l'accès au nouvel espace de noms.

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.

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

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

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

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

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

Si vous utilisez Helm pour déployer des applications, Astra Control Center requiert Helm version 3. La gestion

et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Pour plus d'informations, voir "Exigences du centre de contrôle Astra".

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

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

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

Assurez-vous que vous "entrez les valeurs correctes" lors de l'établissement d'une connexion.

Les connexions existantes à un pod Postgres provoquent des défaillances

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

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

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

Trouvez plus d'informations

- "Problèmes connus"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"

Concepts

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
- Réplication d'applications sur un système distant grâce à la technologie NetApp SnapMirror
- Migrez des applications et des données d'un cluster Kubernetes vers un autre
- Cloner facilement une application de la production au stockage intermédiaire
- Visualiser l'état de santé et de protection des applications
- Utilisez une interface utilisateur ou une API pour implémenter vos workflows de sauvegarde et de migration

Modèles de déploiement

Astra Control est disponible dans deux modèles de déploiement :

- **Astra Control Service** : service géré par NetApp qui permet la gestion des données intégrant la cohérence applicative de clusters Kubernetes dans Google Kubernetes Engine (GKE) et Azure Kubernetes Service (AKS).
- **Astra Control Center** : logiciel autogéré qui assure une gestion des données compatible avec les applications de clusters Kubernetes exécutés dans votre environnement sur site.

	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 téléchargez, installez et gérez
Où est-il hébergé ?	Dans le cloud public de votre choix	Sur le cluster Kubernetes fourni
Comment est-elle mise à jour ?	Géré par NetApp	Vous gérez toutes les mises à jour
Quelles sont les fonctionnalités de gestion des données applicatives ?	Mêmes fonctionnalités sur les deux plateformes, avec des exceptions au système de stockage back-end ou aux services externes	Mêmes fonctionnalités sur les deux plateformes, avec des exceptions au système de stockage back-end ou aux services externes

	Service Astra Control	Centre de contrôle Astra
Qu'est-ce que le système back-end prend en charge ?	Offres de services clouds NetApp	• Systèmes NetApp ONTAP AFF et FAS • Astra Data Store comme système de stockage back-end • Système back-end Cloud Volumes ONTAP

Fonctionnement du service Astra Control

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

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

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

    Dans Azure, Astra Control Service crée également un groupe de ressources, un compte de stockage et des clés pour le conteneur Blob.
  - Crée un nouveau rôle d'administrateur et un compte de service Kubernetes sur le cluster.
  - Utilise ce nouveau rôle d'administrateur pour l'installation "Astra Trident" sur le cluster et pour créer une ou plusieurs classes de stockage.
  - Si vous utilisez Azure NetApp Files ou NetApp Cloud Volumes Service pour Google Cloud comme backend de stockage, Astra Control Service utilise Astra Trident pour provisionner des volumes persistants pour vos applications.
- 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 programme gratuit d'Astra Control vous permet de gérer jusqu'à 10 applications dans votre compte. Si vous voulez gérer plus de 10 applications, vous devrez configurer la facturation en passant du Plan gratuit au Plan Premium.

Fonctionnement du centre de contrôle Astra

Astra Control Center fonctionne localement dans votre propre cloud privé.

Astra Control Center prend en charge les clusters Kubernetes avec :

- Système back-end de stockage Trident avec ONTAP 9.5 et versions ultérieures
- Systèmes back-end de stockage de magasin de données Astra

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

Astra Control Center est entièrement intégré à l'écosystème AutoSupport et Active IQ. Il fournit aux utilisateurs et au support NetApp des informations relatives à la résolution de problèmes et à l'utilisation.

Vous pouvez essayer Astra Control Center avec une licence d'évaluation de 90 jours. La version d'évaluation est prise en charge par e-mail et par la communauté (Channel Slack). 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".

Le centre de contrôle Astra :

- Détecte les détails sur le cluster, y compris les espaces de noms, et vous permet de définir et protéger les applications.
- Détecte la configuration du data store Astra Trident ou Astra sur les clusters que vous avez à gérer et vous permet de surveiller le système back-end.

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.

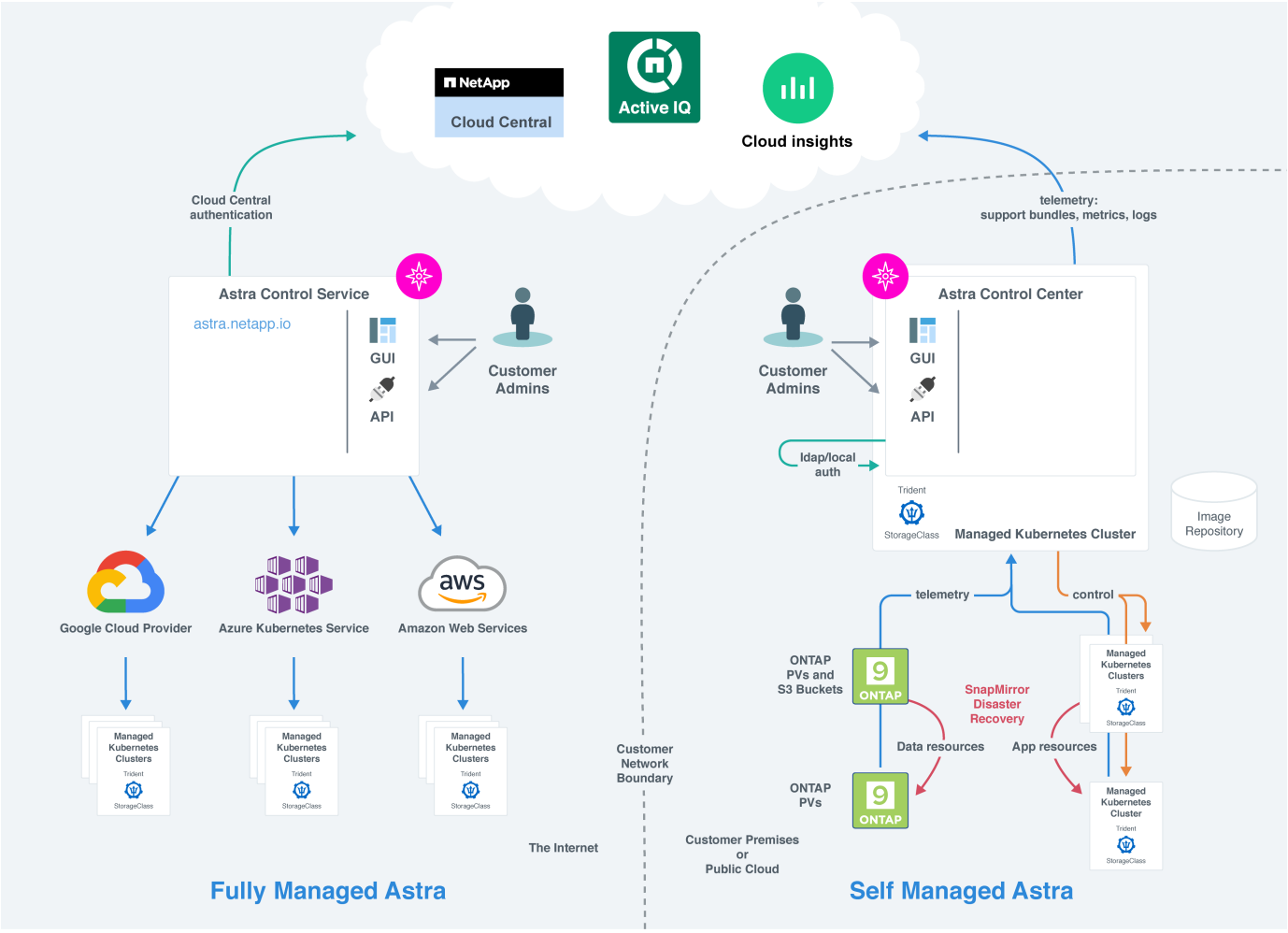
Pour en savoir plus

- "Documentation relative au service après-vente Astra Control"
- "Documentation Astra Control Center"

- "Documentation Astra Data Store"
- "Documentation Astra Trident"
- "Utilisez l'API de contrôle Astra"
- "Documentation Cloud Insights"
- "Documentation ONTAP"

Architecture et composants

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



Composants d'Astra Control

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

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

Interfaces de contrôle Astra

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

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

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

Pour en savoir plus

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

Protection des données

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

Snapshots, sauvegardes et règles de protection

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.

Une *backup* est stockée dans le magasin d'objets externe et peut être plus lente à effectuer 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 d'instantanés et de sauvegardes à conserver dans le planning. L'automatisation de vos sauvegardes et instantanés avec une règle de protection constitue le meilleur moyen de garantir la protection de chaque application en fonction des besoins de votre entreprise.

> *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.

Clones

Un *clone* est une copie exacte d'une application, de sa configuration et de son stockage persistant. Vous pouvez créer manuellement un clone sur le même cluster Kubernetes ou sur un autre cluster. Le clonage d'une application peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre.

Réplication sur un cluster distant

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

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

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

- **Réplication d'application** : Astra Control requiert la disponibilité et la gestion des clusters Kubernetes source et de destination avec leur système back-end de stockage ONTAP respectif configuré pour activer NetApp SnapMirror. Astra Control transfère la copie Snapshot de l'application pilotée par des règles vers le cluster distant. La technologie NetApp SnapMirror est utilisée pour répliquer les données de volume persistant. Pour basculer, Astra Control peut rendre l'application répliquée en ligne en recréant les objets d'application sur le cluster Kubernetes de destination avec les volumes répliqués sur le cluster ONTAP de

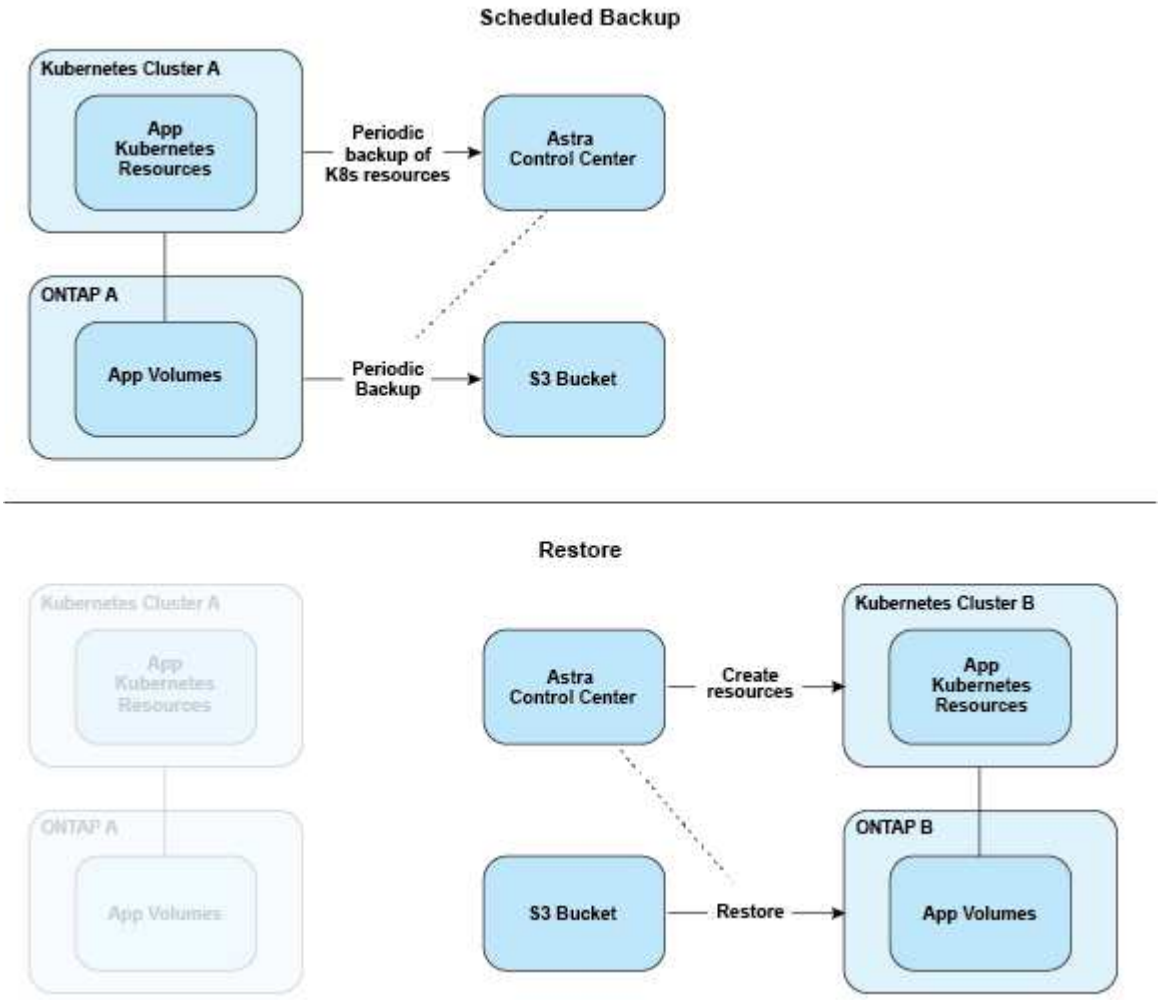
destination. Comme les données de volume persistant sont déjà présentes sur le cluster ONTAP de destination, Astra Control peut bénéficier d'un temps de récupération rapide pour le basculement.

- **Sauvegarde et restauration d'applications** : lors de la sauvegarde d'applications, Astra Control crée un instantané des données d'application et le stocke dans un compartiment de stockage objet. Lorsqu'une restauration est nécessaire, les données du compartiment doivent être copiées sur un volume persistant du cluster ONTAP. Pour réaliser l'opération de sauvegarde et de restauration, le cluster Kubernetes/ONTAP secondaire ne doit pas être disponible et géré, mais la copie de données supplémentaire peut générer des délais de restauration plus longs.

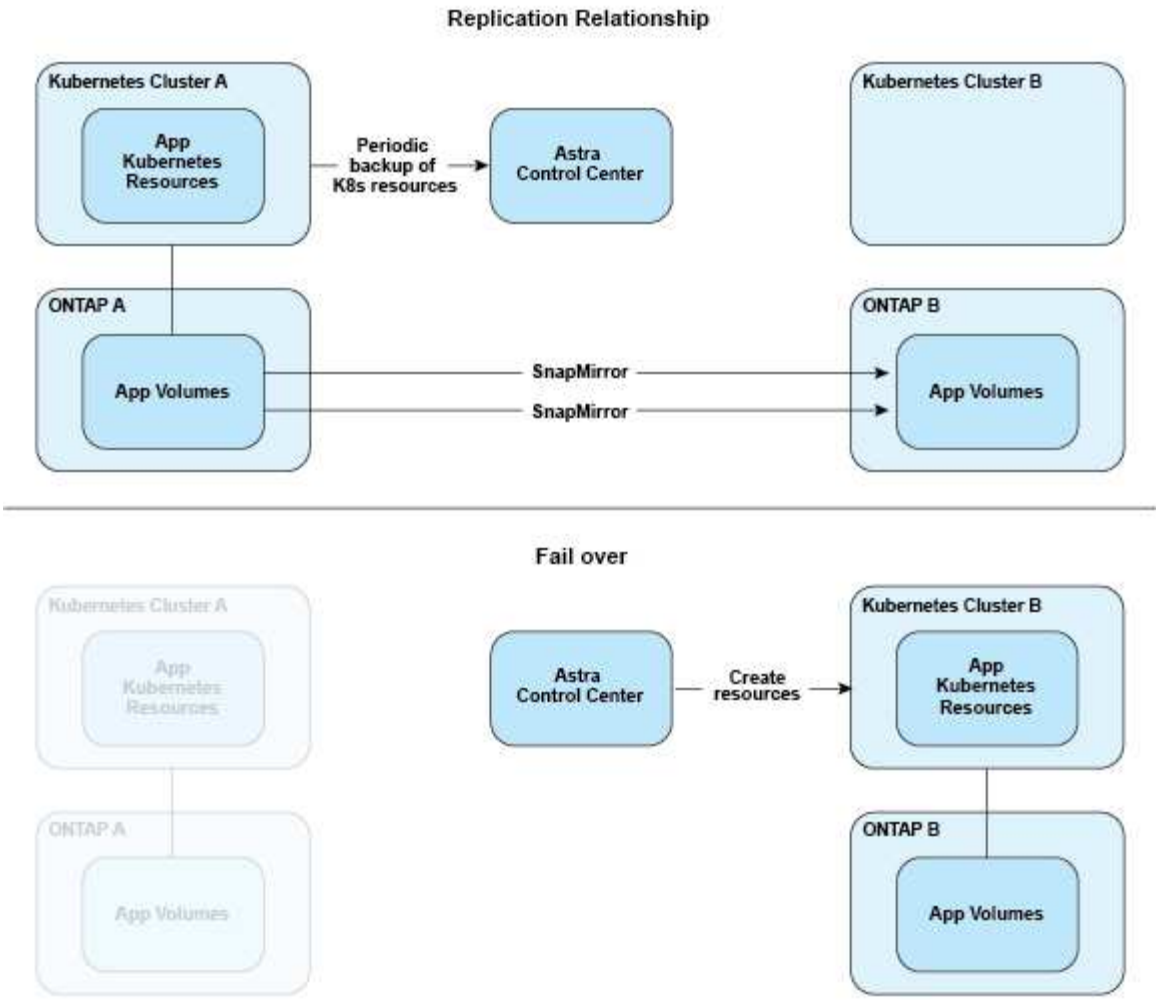
Pour savoir comment répliquer des applications, voir "Répliquez vos applications sur un système distant grâce à la technologie SnapMirror".

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

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



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



Licences

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

Vous devez disposer d'une licence pour protéger vos applications et vos données. Se reporter à Astra Control Center "caractéristiques" pour plus d'informations.

Après l'achat du produit, vous recevez un numéro de série et une licence. Vous pouvez générer le fichier de licence NetApp (NLF) à partir du "Site de support NetApp".

Vous pouvez également essayer Astra Control Center avec une licence d'évaluation qui vous permet d'utiliser Astra Control Center pendant 90 jours à compter de la date de téléchargement de la licence. Pour plus de détails, reportez-vous à "De formation".

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

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

Mode de calcul de la consommation des licences

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

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

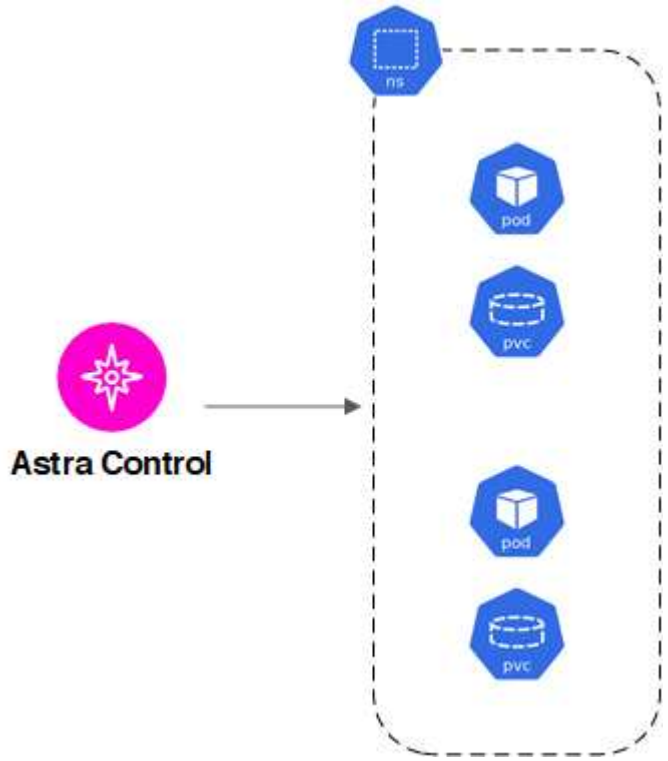
Trouvez plus d'informations

- "Mettre à jour une licence existante"

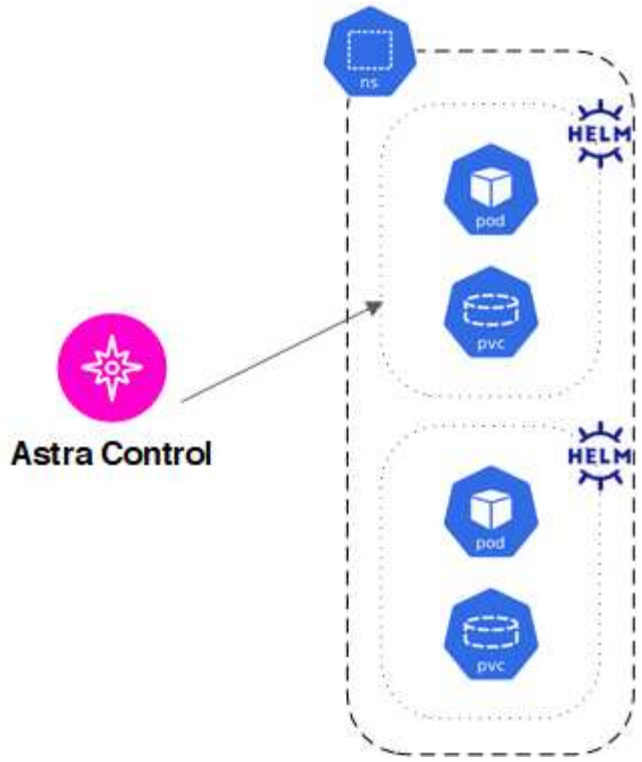
Comprendre la gestion des applications

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 :

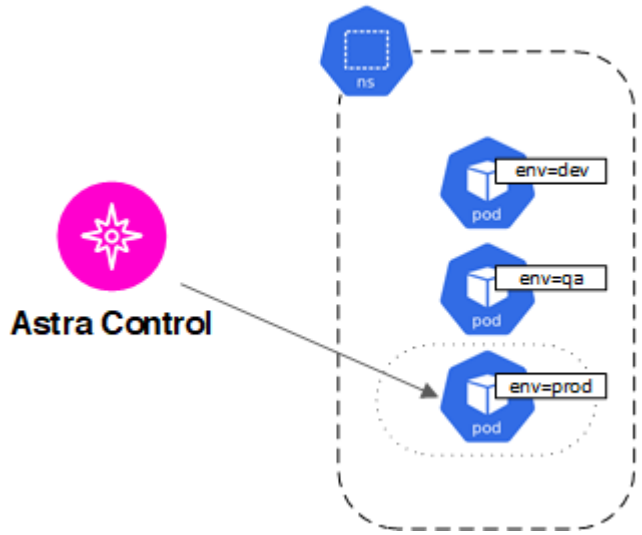
- Un espace de nom, y compris toutes les ressources de cet espace de nom



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



- Groupe de ressources identifié par une étiquette Kubernetes dans un namespace



Classes de stockage et taille de volume persistant

Le centre de contrôle Astra prend en charge ONTAP ou le magasin de données Astra comme système de stockage back-end.

Présentation

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

- **Classes de stockage Trident soutenues par le stockage de magasin de données Astra** : si vous avez installé manuellement un ou plusieurs clusters Astra Data Store, Astra Control Center permet de les

importer et de récupérer leur topologie (nœuds, disques) ainsi que divers États.

Astra Control Center affiche le cluster Kubernetes sous-jacent de la configuration du magasin de données Astra, le cloud dont le cluster Kubernetes appartient, tout volume persistant provisionné par Astra Data Store, le nom du volume interne correspondant, l'application qui utilise le volume persistant et le cluster contenant l'application.

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

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

Classes de stockage

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

Lorsque vous utilisez Astra Control Center intégré à un système back-end de stockage de magasin de données, aucune classe de stockage n'est définie après l'installation. Vous devez créer la classe de stockage par défaut Trident et l'appliquer au système back-end. Voir "Lancement d'Astra Data Store" Pour créer une classe de stockage de magasin de données Astra par défaut.

Pour en savoir plus

- "Documentation Astra Trident"

Rôles et espaces de noms d'utilisateur

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

Rôles utilisateur

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

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

Vous pouvez ajouter des contraintes à un membre ou à un visualiseur pour limiter l'utilisateur à un ou plusieurs

Espaces de noms.

Espaces de noms

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

Trouvez plus d'informations

"Gérez les rôles"

Commencez

Exigences du centre de contrôle Astra

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

- De l'environnement opérationnel
- Systèmes back-end de stockage pris en charge
- Configuration requise en cluster des applications
- De gestion des applications
- Conditions préalables à la réplication
- Accès à Internet
- Licence
- Entrée pour les clusters Kubernetes sur site
- Configuration réseau requise
- Navigateurs Web pris en charge

De l'environnement opérationnel

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

- Google Anthos 1.10 ou 1.11
- Kubernetes 1.22 à 1.24
- Rancher Kubernetes Engine (RKE) :
  - RKE 1.2.16 avec Rancher 2.5.12 et RKE 1.3.3 avec 2.6.3
  - RKE 2 (v1.23,6+rke2r2) avec Rancher 2.6.3
- Red Hat OpenShift Container Platform 4.8, 4.9 ou 4.10
- VMware Tanzu Kubernetes Grid 1.4 ou 1.5
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2 ou 1.13

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

Composant	Conditions requises
Capacité du système back-end	Au moins 500 Go disponibles
Nœuds worker	Au moins 3 nœuds workers au total, avec 4 cœurs de processeurs et 12 Go de RAM chacun
Adresse FQDN	Une adresse FQDN pour Astra Control Center

Composant	Conditions requises
Astra Trident	Astra Trident 21.10.1 ou version ultérieure installé et configuré avec Astra Trident 22.07 ou version ultérieure pour la réplication d'applications basée sur SnapMirror

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

- **Registre d'images**: Vous devez avoir un registre d'images privé Docker existant à laquelle vous pouvez pousser les images de construction d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images.
- **Configuration de l'Astra Trident / ONTAP** : le Centre de contrôle Astra requiert la création et la définition d'une classe de stockage comme classe de stockage par défaut. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Astra Trident :
  - ontap-nas
  - ontap-san
  - ontap-san-économie

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`

Si vous prévoyez d'ajouter un deuxième environnement opérationnel OpenShift comme ressource de calcul gérée, vous devez vous assurer que la fonctionnalité Snapshot de volume Astra Trident est activée. Pour activer et tester des copies Snapshot de volumes avec Astra Trident, "Consultez les instructions officielles de l'Astra Trident".

Configuration requise pour le cluster VMware Tanzu Kubernetes Grid

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

- Désactivez la mise en œuvre par défaut des classes de stockage TKG ou TKGi sur les clusters d'applications devant être gérés par Astra Control. Vous pouvez le faire en modifiant le `TanzuKubernetesCluster` ressource sur le cluster d'espace de noms.
- Dans le cadre de l'installation d'Astra Control Center, les ressources suivantes sont créées dans un environnement restreint de politique de sécurité de pod (PSP) :
  - politique de sécurité des pods

    - Le rôle RBAC
    - RBAC RoleBinding les ressources RBAC et RoleBinding sont créées dans le `netapp-acc` espace de noms.
- Tenez compte des exigences spécifiques de l'Astra Trident lorsque vous déployez le centre de contrôle Astra dans un environnement TKG ou TKGi. Pour plus d'informations, reportez-vous à la section "Documentation Astra Trident".

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

Exigences des clusters Google Anthos

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

Systèmes back-end de stockage pris en charge

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

- NetApp ONTAP 9.5 ou versions ultérieures, AFF et FAS
- NetApp ONTAP 9.8 ou versions ultérieures AFF et FAS pour la réplication d'applications basée sur SnapMirror
- NetApp Cloud Volumes 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

Vous pouvez vérifier si votre système ONTAP dispose des licences requises. Reportez-vous à la section "Gérer les licences ONTAP".

Configuration requise en cluster des applications

Astra Control Center a les exigences suivantes pour les clusters que vous prévoyez de gérer à partir d'Astra Control Center. Ces exigences s'appliquent également si le cluster que vous prévoyez de gérer est le cluster d'environnement opérationnel qui héberge Astra Control Center.

- La version la plus récente de Kubernetes "composant de snapshot-controller" est installé
- Découvrez Astra Trident "objet volumesnapshotclass" a été défini par un administrateur
- Une classe de stockage Kubernetes par défaut existe sur le cluster

- Au moins une classe de stockage est configurée pour utiliser Astra Trident

> Votre cluster d'applications doit disposer d'un `kubeconfig.yaml` fichier qui définit un seul *context* element. Consultez la documentation Kubernetes sur "informations sur la création de fichiers kubeconfig".

> Lors de la gestion des clusters d'applications dans un environnement Rancher, modifiez le contexte par défaut du cluster d'applications dans `kubeconfig` Fichier fourni par Rancher pour utiliser un contexte de plan de contrôle au lieu du contexte de serveur API Rancher. La charge est réduite sur le serveur API Rancher et les performances sont améliorées.

De gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer des applications à l'aide d'Astra Control Center, vous devez disposer d'une licence Astra Control Center.
- **Espaces de noms** : Astra Control exige qu'une application ne couvre pas plus d'un seul espace de noms, mais qu'un espace de noms peut contenir plus d'une application.
- **StorageClass** : si vous installez explicitement une application avec une classe de stockage 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 explicitement définie sur 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	Ressource CustomResource
Ensemble de démonstrations	Déploiement.Config	HorizontalPodAutoscaler
Entrée	MutatingWebhook	Stratégie réseau
Demande de volume persistant	Pod	PodPetitionBudget
PodTemplate	Et de réplication	Rôle
RoleBinding	Itinéraire	Secret
Service	Compte de service	StatefulSet
ValidétingWebhook		

Conditions préalables à la réplication

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

- Pour assurer une reprise après incident transparente, nous vous recommandons de déployer Astra Control Center dans un troisième domaine de pannes ou un troisième site secondaire.
- Le cluster Kubernetes hôte de l'application et un cluster Kubernetes de destination doivent être disponibles

et connectés à deux clusters ONTAP, idéalement dans des domaines ou sites de défaillance différents.

- Les clusters ONTAP et le SVM hôte doivent être associés. Voir "Présentation du cluster et de SVM peering".
- Le SVM distant associé doit être disponible auprès de Trident sur le cluster de destination.
- Trident version 22.07 ou supérieure doit exister sur les clusters ONTAP source et de destination.
- Les licences asynchrones ONTAP SnapMirror via le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Voir "Présentation des licences SnapMirror dans ONTAP".
- Lorsque vous ajoutez un système de stockage back-end ONTAP à Astra Control Center, appliquez les identifiants de l'utilisateur avec le rôle « admin » qui possède des méthodes d'accès `http` et `ontapi` Activé sur les deux clusters ONTAP. Voir "Gérer les comptes d'utilisateurs" pour en savoir plus.
- Les clusters Kubernetes source et destination et les clusters ONTAP doivent être gérés par Astra Control.

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

Découvrez comment "Répliquez vos applications sur un système distant grâce à la technologie SnapMirror".

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 de l'espace de noms. Les applications suivantes ont été validées pour ce modèle d'installation :
  - "Apache K8ssandra"
  - "IC Jenkins"
  - "Cluster Percona XtraDB"

> 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.

Accès à Internet

Vous devez déterminer si vous avez un accès externe à Internet. Si ce n'est pas le cas, certaines fonctionnalités peuvent être limitées, comme la réception de données de surveillance et de metrics depuis NetApp Cloud Insights ou l'envoi de packs de support au "Site de support NetApp".

Licence

Astra Control Center requiert une licence Astra Control Center pour bénéficier de toutes les fonctionnalités. Obtenez une licence d'évaluation ou une licence complète auprès de NetApp. Vous devez disposer d'une licence pour protéger vos applications et vos données. Reportez-vous à la section "Caractéristiques du centre de contrôle Astra" pour plus d'informations.

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

Pour 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".

Pour plus d'informations sur le fonctionnement des licences, reportez-vous à la section "Licences".

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'en 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.

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

Pour plus d'informations, voir "Configurer l'entrée pour l'équilibrage de charge".

Configuration réseau requise

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

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

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

Navigateurs Web pris en charge

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

Et la suite

Afficher le "démarrage rapide" présentation.

Démarrage rapide pour Astra Control Center

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

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

1 **Vérifiez la configuration des clusters Kubernetes**

- Astra fonctionne avec les clusters Kubernetes avec un système de stockage ONTAP configuré par Trident

ou avec un système back-end de stockage du magasin de données Astra.

- Les clusters doivent fonctionner correctement, avec au moins trois nœuds de travail en ligne.
- Le cluster doit exécuter Kubernetes.

En savoir plus sur le "Exigences du centre de contrôle Astra".

2 Téléchargez et installez Astra Control Center

- Téléchargez Astra Control Center à partir du "Page de téléchargements de l'Astra Control Center du site de support NetApp".
- Installez Astra Control Center dans votre environnement local.

  Vous pouvez également installer Astra Control Center à l'aide de Red Hat OperatorHub.

  Vous pouvez également installer Astra Control Center avec un système de stockage back-end Cloud Volumes ONTAP.

En savoir plus sur "Installation du centre de contrôle Astra".

3 Effectuez certaines tâches de configuration initiales

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

En savoir plus sur le "processus de configuration initiale".

4 Utilisez Astra Control Center

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

- Gérer une application. En savoir plus "gérer des applications".
- Protégez les applications en configurant des stratégies de protection pour les applications, en répliquant les applications sur des systèmes distants et en migrant les applications. En savoir plus "protégez vos applications".
- Gérez les comptes (utilisateurs, rôles, LDAP pour l'authentification des utilisateurs, informations d'identification, connexions au référentiel, etc.). En savoir plus "gérer les utilisateurs".
- Vous pouvez également vous connecter à NetApp Cloud Insights pour afficher des mesures sur l'état de santé de votre système, la capacité et le débit dans l'interface utilisateur de l'Astra Control Center. En savoir plus sur "Connexion à Cloud Insights".

5 Continuez à partir de ce démarrage rapide

"Poser le centre de contrôle Astra".

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"

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"

Installer le centre de contrôle Astra en suivant la procédure standard

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

Pour les environnements Red Hat OpenShift, vous pouvez utiliser un "autre procédure" Pour installer Astra Control Center à l'aide d'OpenShift OperatorHub.

Ce dont vous avez besoin

- "Avant de commencer l'installation, préparez votre environnement pour le déploiement d'Astra Control Center".
- Si vous avez configuré ou que vous souhaitez configurer des stratégies de sécurité de pod dans votre environnement, familiarisez-vous avec les stratégies de sécurité de pod et leur incidence sur l'installation d'Astra Control Center. Voir "Comprendre les restrictions de la stratégie de sécurité du pod".
- S'assurer que tous les opérateurs du groupe d'instruments sont en état de fonctionnement et disponibles.

```
kubectl get clusteroperators
```

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

```
kubectl get apiservices
```

- Assurez-vous que le FQDN Astra que vous prévoyez d'utiliser est routable vers ce cluster. Cela signifie que vous avez une entrée DNS dans votre serveur DNS interne ou que vous utilisez une route URL de base déjà enregistrée.
- Si un cert-Manager existe déjà dans le cluster, vous devez en effectuer certaines "étapes préalables" Pour qu'Astra Control Center n'installe pas son propre cert-Manager.

Description de la tâche

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

- Installe les composants Astra dans le `netapp-acc` (ou espace de nom personnalisé).
- Crée un compte par défaut.

- Définit une adresse e-mail d'utilisateur administratif par défaut et un mot de passe unique par défaut. Ce rôle propriétaire est attribué à cet utilisateur dans le système qui est nécessaire pour la première connexion à l'interface utilisateur.
- Vous aide à déterminer que toutes les POD Astra Control Center sont en cours d'exécution.
- Installe l'interface utilisateur Astra.

> (Applicable uniquement à la version EAP (Data Store Early Access Program) d'Astra) si vous prévoyez de gérer le magasin de données Astra à l'aide d'Astra Control Center et d'activer les flux de travail VMware, déployez Astra Control Center uniquement sur le `pcloud` et pas sur le `netapp-acc` espace de noms ou espace de noms personnalisé décrits dans les étapes de cette procédure.

> N'exécutez pas la commande suivante pendant l'intégralité du processus d'installation pour éviter de supprimer toutes les pods Astra Control Center : `kubectl delete -f astra_control_center_operator_deploy.yaml`

> Si vous utilisez le Podman de Red Hat au lieu de Docker Engine, vous pouvez utiliser les commandes Podman à la place des commandes Docker.

Étapes

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

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

Téléchargez et déballez le pack Astra Control Center

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

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

4. Extraire les images :

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

Installez le plug-in NetApp Astra kubectl

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

Ce dont vous avez besoin

NetApp fournit des binaires pour différents systèmes d'exploitation et architectures CPU. Avant d'effectuer cette tâche, vous devez savoir quelle unité centrale et quel système d'exploitation vous possédez. Sur les systèmes d'exploitation Linux et Mac, vous pouvez utiliser `uname -a` commande permettant de collecter ces informations.

Étapes

1. Répertoriez l'Astra de NetApp disponible `kubectl` Les binaires du plug-in, et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et l'architecture de l'UC :

```
ls kubectl-astra/
```

2. Copiez le fichier au même emplacement que la norme `kubectl` informatique. Dans cet exemple, le `kubectl` l'utilitaire se trouve dans le `/usr/local/bin` répertoire. Remplacement `<binary-name>` avec le nom du fichier dont vous avez besoin :

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

Ajoutez les images à votre registre local

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

Docker

1. Passez au répertoire Astra :

```
cd acc
```

2. placez les images du paquet dans le répertoire d'images Astra Control Center dans votre registre local. Exécutez les substitutions suivantes avant d'exécuter la commande :
   - Remplacez BUNDLE_FILE par le nom du fichier bundle Astra Control (par exemple, `acc.manifest.yaml`).
   - Remplacez MON_REGISTRE par l'URL du référentiel Docker.
   - Remplacez MON_REGISTRE_UTILISATEUR par le nom d'utilisateur.
   - Remplacez MON_REGISTRY_TOKEN par un jeton autorisé pour le Registre.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Connectez-vous à votre registre :

```
podman login [your_registry_path]
```

2. Exécutez le script suivant, en procédant à la substitution <YOUR_REGISTRY> comme indiqué dans les commentaires :

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

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

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

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

2. Si vous utilisez un registre qui nécessite une authentification, vous devez procéder comme suit :

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

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

   Réponse :

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

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

> Le paramètre fictif `your_registry_path` doit correspondre à l'emplacement des images que vous avez téléchargées précédemment (par exemple, `[Registry_URL]/netapp/astra/astracc/22.08.1-26`).

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

Exemple de réponse :

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

> Si vous supprimez l'espace de noms après la génération du secret, vous devez régénérer le secret pour l'espace de noms après la recréation de l'espace de noms.

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

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

Exemple de réponse :

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

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

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

Réponse

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

a. (Facultatif) si vous souhaitez que le cluster soit automatiquement géré par Astra Control Center après

l'installation, assurez-vous de fournir le kubeconfig comme secret dans l'espace de noms de l'Astra Control Center que vous souhaitez déployer à l'aide de cette commande :

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom namespace]
```

Poser le conducteur du centre de commande Astra

1. Modifier le répertoire :

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

> Un échantillon annoté YAML suit ces étapes.

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

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

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

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

d. (Pour les installations utilisant l'aperçu d'Astra Data Store) Découvrez ce problème connu concernant "Les spécialistes en provisionnement de classe de stockage et les changements supplémentaires que vous devrez apporter au YAML".

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Poser le conducteur du centre de commande Astra :

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

Exemple de réponse :

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

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

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

Configurer le centre de contrôle Astra

1. Modifiez le fichier de ressources personnalisées (CR) Astra Control Center (`astra_control_center_min.yaml`) Pour créer des comptes, AutoSupport, registre et autres configurations nécessaires :

> `astra_control_center_min.yaml` Est le CR par défaut et convient à la plupart des installations. Familiarisez-vous avec tous "Les options CR et leurs valeurs potentielles" Pour vous assurer de déployer le centre de contrôle Astra correctement pour votre environnement. Si d'autres personnalisations sont nécessaires pour votre environnement, vous pouvez l'utiliser `astra_control_center.yaml` En tant que CR alternatif.

```
vim astra_control_center_min.yaml
```

> Si vous utilisez un registre qui ne requiert pas d'autorisation, vous devez supprimer le `secret` ligne comprise entre `imageRegistry` sinon, l'installation échouera.

a. Changer `[your_registry_path]` vers le chemin du registre où vous avez poussé les images à l'étape précédente.

b. Modifiez le `accountName` chaîne du nom que vous souhaitez associer au compte.

c. Modifiez le `astraAddress` Chaîne du FQDN que vous souhaitez utiliser dans votre navigateur pour accéder à Astra. Ne pas utiliser `http://` ou `https://` dans l'adresse. Copier ce FQDN pour l'utiliser dans un plus tard.

d. Modifiez le `email` chaîne à l'adresse d'administrateur initiale par défaut. Copiez cette adresse e-mail pour l'utiliser dans un plus tard.

e. Changer `enrolled` Pour AutoSupport à `false` pour les sites sans connexion internet ou sans conservation `true` pour les sites connectés.

f. Si vous utilisez un cert-Manager externe, ajoutez les lignes suivantes à `spec`:

```
spec:
  crds:
    externalCertManager: true
```

g. (Facultatif) Ajouter un prénom `firstName` et nom `lastName` de l'utilisateur associé au compte. Vous pouvez effectuer cette étape maintenant ou plus tard dans l'interface utilisateur.

h. (Facultatif) modifiez le `storageClass` Valeur ajoutée pour une autre ressource de stockage Trident si votre installation l'exige.

i. (Facultatif) si vous souhaitez que le cluster soit géré automatiquement par Astra Control Center après l'installation et que vous l'ayez déjà fait créé le secret contenant le kubecconfig pour ce cluster, Indiquez le nom du secret en ajoutant un nouveau champ à ce fichier YAML appelé `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

j. Effectuez l'une des opérations suivantes :

- **Autre contrôleur d'entrée (ingressType:Generic)**: Il s'agit de l'action par défaut avec Astra Control Center. Après le déploiement du centre de contrôle Astra, vous devrez configurer le contrôleur d'entrée pour exposer le centre de contrôle Astra à une URL.

  L'installation par défaut d'Astra Control Center configure sa passerelle (`service/traefik`) pour être du type `ClusterIP`. Avec cette installation par défaut, vous devez également configurer une entrée/un contrôleur Kubernetes IngressController pour y acheminer le trafic. Si vous souhaitez utiliser une entrée, reportez-vous à la section "Configurer l'entrée pour l'équilibrage de charge".

- **Équilibreur de charge de service (ingressType:AccTraefik)**: Si vous ne souhaitez pas installer un IngressController ou créer une ressource d'entrée, définissez `ingressType` à `AccTraefik`.

  Ceci déploie le centre de contrôle Astra `traefik` Passerelle en tant que service de type Kubernetes LoadBalancer.

  Le centre de contrôle Astra utilise un service de type « équilibreur de charge » (`svc/traefik` Dans l'espace de noms du centre de contrôle Astra), et exige qu'il se voit attribuer une adresse IP externe accessible. Si des équilibreurs de charge sont autorisés dans votre environnement et que vous n'en avez pas encore configuré, vous pouvez utiliser MetalLB ou un autre équilibreur de charge de service externe pour attribuer une adresse IP externe au service. Dans la configuration du serveur DNS interne, pointez le nom DNS choisi pour Astra Control Center vers l'adresse IP à équilibrage de charge.

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

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

Installation complète du centre de contrôle Astra et du conducteur

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

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

   Exemple de réponse :

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

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

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

   Exemple de réponse :

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

Vérifiez l'état du système

> Si vous préférez utiliser OpenShift, vous pouvez utiliser des commandes oc comparables pour les étapes de vérification.

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

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

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

Exemple de réponse

```
NAME                                        READY   STATUS    RESTARTS
AGE
acc-helm-repo-6b44d68d94-d8m55              1/1     Running   0
13m
activity-78f99ddf8-hltct                    1/1     Running   0
10m
api-token-authentication-457nl              1/1     Running   0
9m28s
api-token-authentication-dgwsz              1/1     Running   0
9m28s
api-token-authentication-hmqqc              1/1     Running   0
9m28s
asup-75fd554dc6-m6qzh                       1/1     Running   0
9m38s
authentication-6779b4c85d-92gds             1/1     Running   0
8m11s
bucketservice-7cc767f8f8-lqwr8              1/1     Running   0
9m31s
certificates-549fd5d6cb-5kmd6               1/1     Running   0
9m56s
certificates-549fd5d6cb-bkjh9               1/1     Running   0
9m56s
cloud-extension-7bcb7948b-hn8h2             1/1     Running   0
10m
cloud-insights-service-56ccf86647-fgg69     1/1     Running   0
9m46s
composite-compute-677685b9bb-7vgsf          1/1     Running   0
10m
composite-volume-657d6c5585-dnq79           1/1     Running   0
9m49s
credentials-755fd867c8-vrlmt                1/1     Running   0
11m
entitlement-86495cdf5b-nwhh2                1/1     Running   2
10m
features-5684fb8b56-8d6s8                   1/1     Running   0
10m
fluent-bit-ds-rhx7v                         1/1     Running   0
7m48s
fluent-bit-ds-rjms4                         1/1     Running   0
7m48s
fluent-bit-ds-zf5ph                         1/1     Running   0
7m48s
graphql-server-66d895f544-w6hjd             1/1     Running   0
3m29s
```

```
identity-744df448d5-rlcmm                1/1     Running   0
10m
influxdb2-0                              1/1     Running   0
13m
keycloak-operator-75c965cc54-z7csw       1/1     Running   0
8m16s
krakend-798d6df96f-9z2sk                 1/1     Running   0
3m26s
license-5fb7d75765-f8mjg                 1/1     Running   0
9m50s
login-ui-7d5b7df85d-l2s7s                1/1     Running   0
3m20s
loki-0                                   1/1     Running   0
13m
metrics-facade-599b9d7fcc-gtmgl          1/1     Running   0
9m40s
monitoring-operator-67cc74f844-cdplp     2/2     Running   0
8m11s
nats-0                                   1/1     Running   0
13m
nats-1                                   1/1     Running   0
13m
nats-2                                   1/1     Running   0
12m
nautilus-769f5b74cd-k5jxm                1/1     Running   0
9m42s
nautilus-769f5b74cd-kd9gd                1/1     Running   0
8m59s
openapi-84f6ccd8ff-76kvp                 1/1     Running   0
9m34s
packages-6f59fc67dc-4g2f5                1/1     Running   0
9m52s
polaris-consul-consul-server-0           1/1     Running   0
13m
polaris-consul-consul-server-1           1/1     Running   0
13m
polaris-consul-consul-server-2           1/1     Running   0
13m
polaris-keycloak-0                       1/1     Running   0
8m7s
polaris-keycloak-1                       1/1     Running   0
5m49s
polaris-keycloak-2                       1/1     Running   0
5m15s
polaris-keycloak-db-0                    1/1     Running   0
8m6s
```

```
polaris-keycloak-db-1                     1/1     Running   0
5m49s
polaris-keycloak-db-2                     1/1     Running   0
4m57s
polaris-mongodb-0                         2/2     Running   0
13m
polaris-mongodb-1                         2/2     Running   0
12m
polaris-mongodb-2                         2/2     Running   0
12m
polaris-ui-565f56bf7b-zwr8b               1/1     Running   0
3m19s
polaris-vault-0                           1/1     Running   0
13m
polaris-vault-1                           1/1     Running   0
13m
polaris-vault-2                           1/1     Running   0
13m
public-metrics-6d86d66444-2wbzl           1/1     Running   0
9m30s
storage-backend-metrics-77c5d98dcd-dbhg5 1/1     Running   0
9m44s
storage-provider-78c885f57c-6zcv4         1/1     Running   0
9m36s
telegraf-ds-2l2m9                         1/1     Running   0
7m48s
telegraf-ds-qfzgh                         1/1     Running   0
7m48s
telegraf-ds-shrms                         1/1     Running   0
7m48s
telegraf-rs-bjpkt                         1/1     Running   0
7m48s
telemetry-service-6684696c64-qzfdf        1/1     Running   0
10m
tenancy-6596b6c54d-vmpsm                  1/1     Running   0
10m
traefik-7489dc59f9-6mnst                  1/1     Running   0
3m19s
traefik-7489dc59f9-xrkgg                  1/1     Running   0
3m4s
trident-svc-6c8dc458f5-jswcl              1/1     Running   0
10m
vault-controller-6b954f9b76-gz9nm         1/1     Running   0
11m
```

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

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

> `accHost` l'enregistrement du cluster est l'une des dernières opérations. en cas de défaillance, le déploiement ne pourra pas échouer. Dans l'éventualité où un échec d'enregistrement de cluster était indiqué dans les journaux, vous pouvez réessayer d'enregistrer via le flux de production Add cluster "Dans l'interface utilisateur" Ou API.

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

```
kubectl get AstraControlCenter -n netapp-acc
```

Réponse :

```
NAME    UUID                                      VERSION     ADDRESS
READY
astra   ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  22.08.1-26
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, comme l'équilibrage de la charge dans un cluster.

Cette procédure explique comment configurer un contrôleur d'entrée (`ingressType:Generic`). Il s'agit de l'action par défaut avec Astra Control Center. Après le déploiement du centre de contrôle Astra, vous devrez configurer le contrôleur d'entrée pour exposer le centre de contrôle Astra à une URL.

> Si vous ne souhaitez pas configurer un contrôleur d'entrée, vous pouvez le configurer `ingressType:AccTraefik)`. Le centre de contrôle Astra utilise un service de type « équilibreur de charge » (`svc/traefik` Dans l'espace de noms du centre de contrôle Astra), et exige qu'il se voit attribuer une adresse IP externe accessible. Si des équilibreurs de charge sont autorisés dans votre environnement et que vous n'en avez pas encore configuré, vous pouvez utiliser MetalLB ou un autre équilibreur de charge de service externe pour attribuer une adresse IP externe au service. Dans la configuration du serveur DNS interne, pointez le nom DNS choisi pour Astra Control Center vers l'adresse IP à équilibrage de charge. Pour plus de détails sur le type de service « LoadBalancer » et l'entrée, voir "De formation".

Les étapes diffèrent en fonction du type de contrôleur d'entrée utilisé :

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

Ce dont vous avez besoin

- Le requis "contrôleur d'entrée" doit déjà être déployé.
- Le "classe d'entrée" correspondant au contrôleur d'entrée doit déjà être créé.
- Vous utilisez les versions de Kubernetes entre et, y compris v1.19 et v1.22.

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. Déployez une ressource entrée dans `netapp-acc` (Ou espace de noms personnalisé) utilisant soit l'espace de noms v1beta1 (obsolète dans la version Kubernetes inférieure à ou 1.22) soit le type de ressource v1 pour un schéma obsolète ou un nouveau schéma :

   Résultat :

```
apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          serviceName: traefik
          servicePort: 80
```

Pour le nouveau schéma v1, suivez cet exemple :

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

Résultat :

```
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: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Déployez Astra Control Center comme d'habitude.
6. Vérifier l'état de l'entrée :

```
kubectl get ingress -n netapp-acc
```

Réponse :

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

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 espace de nom personnalisé) utilisant l'un ou l'autre `v1beta1` (Obsolète dans la version Kubernetes inférieure à ou 1.22) ou `v1` type de ressource pour un schéma obsolète ou nouveau :

   a. Pour un `v1beta1` schéma obsolète, suivre cet exemple :

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

   b. Pour le `v1` nouveau schéma, suivez cet exemple :

```yaml
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 addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

Étapes du contrôleur d'entrée OpenShift

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

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

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

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

Étapes

1. Dans un navigateur, entrez le FQDN que vous avez utilisé dans le `astraAddress` dans le `astra_control_center_min.yaml` CR quand Vous avez installé Astra Control Center.
2. Acceptez les certificats auto-signés lorsque vous y êtes invité.

> Vous pouvez créer un certificat personnalisé après la connexion.

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

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

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

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

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

Dépanner l'installation

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

Étapes

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

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

Et la suite

Terminez le déploiement en effectuant le processus "tâches de configuration".

=
:allow-uri-read:

Comprendre les restrictions de la stratégie de sécurité du pod

Astra Control Center prend en charge la limitation des privilèges via les politiques de sécurité du pod (PSP). Les stratégies de sécurité des pods vous permettent de limiter les utilisateurs ou les groupes capables d'exécuter des conteneurs et les privilèges dont ils disposent.

Certaines distributions Kubernetes, telles que RKE2, ont une stratégie de sécurité de pod par défaut trop restrictive et provoquent des problèmes lors de l'installation d'Astra Control Center.

Vous pouvez utiliser les informations et exemples inclus ici pour comprendre les politiques de sécurité du pod que le Control Center d'Astra et configurer les règles de sécurité du pod qui fournissent la protection dont vous avez besoin sans interférer avec les fonctions du Control Center d'Astra.

PSP installé par Astra Control Center

Astra Control Center crée plusieurs politiques de sécurité de pod pendant l'installation. Certaines sont permanentes, certaines d'entre elles sont créées pendant certaines opérations et sont supprimées une fois l'opération terminée.

PSP créé lors de l'installation

Lors de l'installation d'Astra Control Center, l'opérateur d'Astra Control Center installe une stratégie de sécurité de pod personnalisée, un objet de rôle et un objet RoleBinding pour prendre en charge le déploiement des services Astra Control Center dans l'espace de noms Astra Control Center.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                            PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
avp-psp                         false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *
netapp-astra-deployment-psp     false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                     CREATED AT
netapp-astra-deployment-role             2022-06-27T19:34:58Z

kubectl get rolebinding

NAME                                     ROLE
AGE
netapp-astra-deployment-rb               Role/netapp-astra-deployment-role
32m
```

PSP créé pendant les opérations de sauvegarde

Pendant les opérations de sauvegarde, Astra Control Center crée une règle de sécurité dynamique de pod, un objet ClusterRole et un objet RoleBinding. Ils prennent en charge le processus de sauvegarde, qui se produit dans un espace de noms distinct.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                   CREATED AT
netapp-astra-backup    2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                   ROLE                        AGE
netapp-astra-backup    Role/netapp-astra-backup    62s
```

PSP créé lors de la gestion du cluster

Lorsque vous gérez un cluster, Astra Control Center installe l'opérateur de surveillance netapp dans le cluster géré. Cet opérateur crée une politique de sécurité pod, un objet ClusterRole et un objet RoleBinding pour déployer des services de télémétrie dans l'espace de noms Astra Control Center.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo      true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                            CREATED AT
netapp-monitoring-role-privileged               2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                                                    ROLE
AGE
netapp-monitoring-role-binding-privileged               Role/netapp-
monitoring-role-privileged              2m5s
```

Activer la communication réseau entre les espaces de noms

Certains environnements utilisent les constructions NetworkPolicy pour limiter le trafic entre les espaces de noms. L'opérateur d'Astra Control Center, Astra Control Center et le plug-in Astra pour VMware vSphere sont tous dans des espaces de noms différents. Les services de ces différents espaces de noms doivent être capables de communiquer les uns avec les autres. Pour activer cette communication, procédez comme suit.

Étapes

1. Supprimez toutes les ressources NetworkPolicy qui existent dans l'espace de noms Astra Control Center :

```
kubectl get networkpolicy -n netapp-acc
```

2. Pour chaque objet NetworkPolicy renvoyé par la commande précédente, utilisez la commande suivante pour le supprimer. Remplacez <NOM_OBJET> par le nom de l'objet renvoyé :

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Appliquez le fichier de ressources suivant pour configurer l'objet de stratégie réseau-acc-avp pour permettre à Astra Plugin pour les services VMware vSphere de faire des demandes aux services Astra Control Center. Remplacez entre parenthèses <> par les informations relatives à votre environnement :

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. Appliquez le fichier de ressources suivant pour configurer l'objet de stratégie réseau ACC-opérateur pour permettre à l'opérateur Astra Control Center de communiquer avec les services Astra Control Center. Remplacez entre parenthèses <> par les informations relatives à votre environnement :

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME
```

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. Vous devez les supprimer 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 l'espace de noms netapp-acc :

```
kubectl get quota -n netapp-acc
```

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
```

```
kubectl delete resourcequota  pods-low -n netapp-acc
```

```
kubectl delete resourcequota  pods-medium -n netapp-acc
```

3. Consultez les plages de limite dans l'espace de noms netapp-acc :

```
kubectl get limits -n netapp-acc
```

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
```

=
:allow-uri-read:

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

Si vous utilisez Red Hat OpenShift, vous pouvez installer Astra Control Center à l'aide de l'opérateur certifié Red Hat. 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.

Ce dont vous avez besoin

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

```
oc get clusteroperators
```

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

est `true`) :

```
oc get apiservices
```

- Créez une adresse FQDN pour Astra Control Center dans votre centre de données.
- Obtenez les autorisations nécessaires et l'accès à Red Hat OpenShift Container Platform pour effectuer les étapes d'installation décrites.
- Si un cert-Manager existe déjà dans le cluster, vous devez en effectuer certaines "étapes préalables" Pour qu'Astra Control Center n'installe pas son propre cert-Manager.

Étapes

- Téléchargez et déballez le pack Astra Control Center
- Installez le plug-in NetApp Astra kubectl
- Ajoutez les images à votre registre local
- Recherchez la page d'installation de l'opérateur
- Poser l'opérateur
- Poser le centre de contrôle Astra

Téléchargez et déballez le pack Astra Control Center

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

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

4. Extraire les images :

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

Installez le plug-in NetApp Astra kubectl

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

Ce dont vous avez besoin

NetApp fournit des binaires pour différents systèmes d'exploitation et architectures CPU. Avant d'effectuer cette tâche, vous devez savoir quelle unité centrale et quel système d'exploitation vous possédez. Sur les systèmes d'exploitation Linux et Mac, vous pouvez utiliser `uname -a` commande permettant de collecter ces informations.

Étapes

1. Répertoriez l'Astra de NetApp disponible `kubectl` Les binaires du plug-in, et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et l'architecture de l'UC :

```
ls kubectl-astra/
```

2. Copiez le fichier au même emplacement que la norme `kubectl` informatique. Dans cet exemple, le `kubectl` l'utilitaire se trouve dans le `/usr/local/bin` répertoire. Remplacement `<binary-name>` avec le nom du fichier dont vous avez besoin :

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

Ajoutez les images à votre registre local

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

Docker

1. Passez au répertoire Astra :

```
cd acc
```

2. placez les images du paquet dans le répertoire d'images Astra Control Center dans votre registre local. Exécutez les substitutions suivantes avant d'exécuter la commande :
   - Remplacez BUNDLE_FILE par le nom du fichier bundle Astra Control (par exemple, `acc.manifest.yaml`).
   - Remplacez MON_REGISTRE par l'URL du référentiel Docker.
   - Remplacez MON_REGISTRE_UTILISATEUR par le nom d'utilisateur.
   - Remplacez MON_REGISTRY_TOKEN par un jeton autorisé pour le Registre.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Connectez-vous à votre registre :

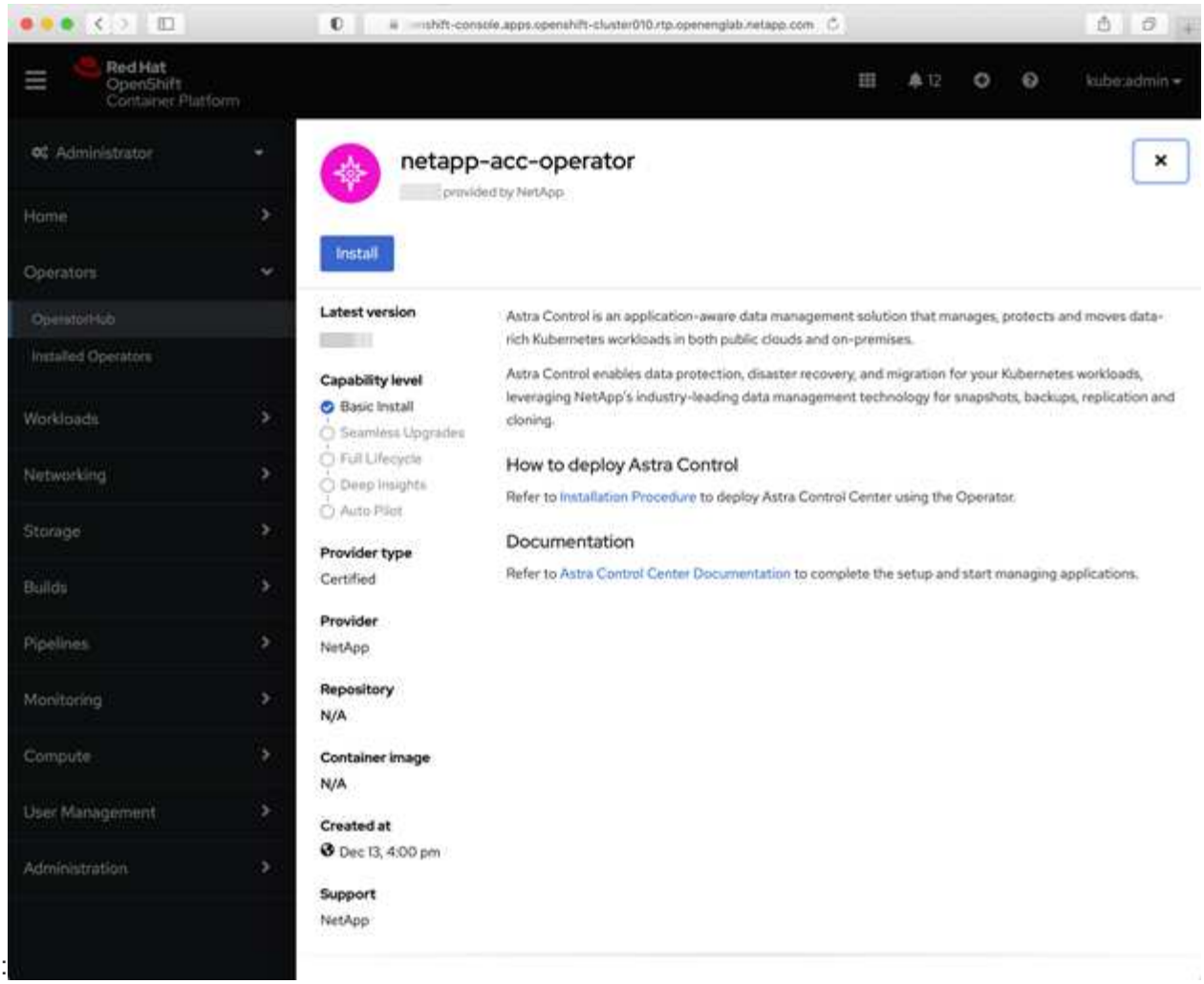
```
podman login [your_registry_path]
```

2. Exécutez le script suivant, en procédant à la substitution <YOUR_REGISTRY> comme indiqué dans les commentaires :

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Recherchez la page d'installation de l'opérateur

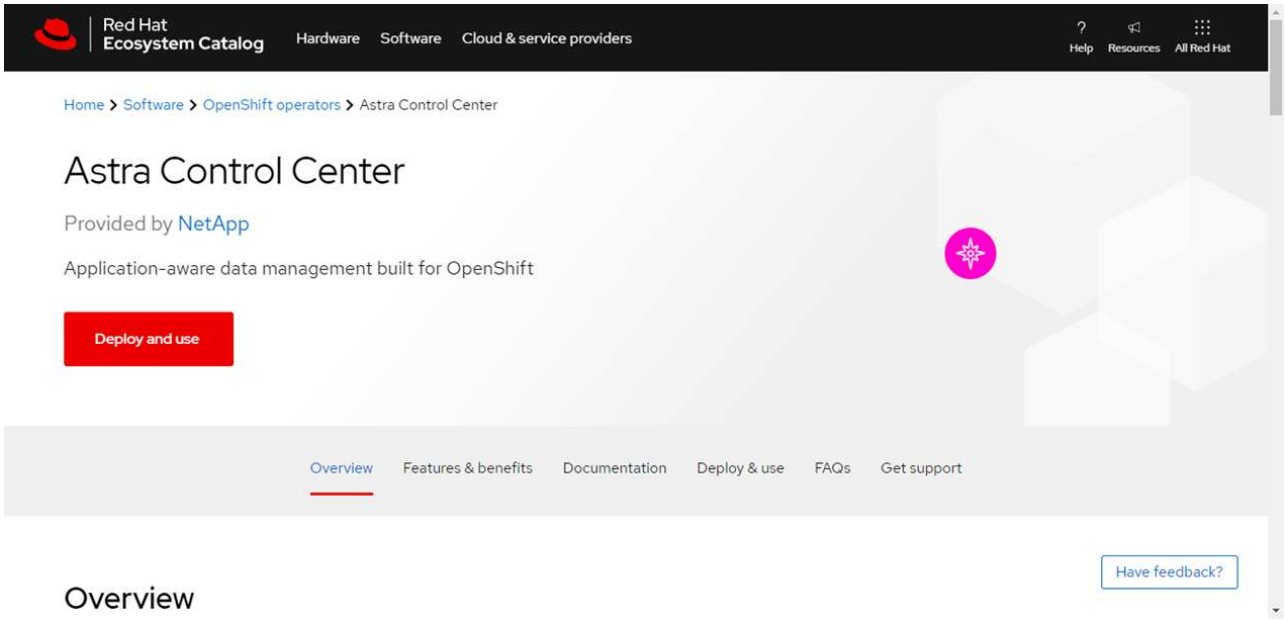
1. Effectuez l'une des procédures suivantes pour accéder à la page d'installation de l'opérateur :
   - Depuis la console Web Red Hat OpenShift



:

i. Connectez-vous à l'interface utilisateur de OpenShift Container Platform.
ii. Dans le menu latéral, sélectionnez **Operators > OperatorHub**.
iii. Sélectionnez l'opérateur du centre de contrôle Astra NetApp.
iv. Sélectionnez **installer**.

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



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

ii. 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. Depuis la console dans la vue détaillée du conducteur du centre de contrôle Astra, sélectionnez `Create instance` Dans la section API fournies.

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

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

   b. (Facultatif) Activer ou désactiver Auto support. Il est recommandé de conserver la fonctionnalité Auto support.

c. Entrez l'adresse du centre de contrôle Astra. N'entrez pas `http://` ou `https://` dans l'adresse.
d. Entrez la version Astra Control Center, par exemple 21.12.60.
e. Entrez un nom de compte, une adresse e-mail et un nom d'administrateur.
f. Conservez la règle de récupération du volume par défaut.
g. Dans **image Registry**, entrez le chemin d'accès au registre d'images du conteneur local. N'entrez pas `http://` ou `https://` dans l'adresse.
h. Si vous utilisez un registre qui nécessite une authentification, saisissez le secret.
i. Entrez le prénom de l'administrateur.
j. Configurer l'évolutivité des ressources.
k. Conservez la classe de stockage par défaut.
l. Définissez les préférences de gestion de CRD.

3. Sélectionnez `Create`.

Et la suite

Vérifier que le centre de contrôle Astra a été correctement installé et terminer le "les étapes restantes" pour vous connecter. De plus, vous terminez le déploiement en effectuant également des opérations "tâches de configuration".

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

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

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

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

- Déploiement d'Astra Control Center dans Amazon Web Services
- Déployez Astra Control Center dans Google Cloud Platform
- Déploiement d'Astra Control Center dans Microsoft Azure

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

Déploiement d'Astra Control Center dans Amazon Web Services

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

Ce dont vous avez besoin pour AWS

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

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

Exigences de l'environnement opérationnel pour AWS

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

- Red Hat OpenShift Container Platform 4.8

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

Le Centre de contrôle Astra requiert les ressources suivantes en plus des exigences de l'environnement en matière de ressources :

Composant	Conditions requises
Backend la capacité de stockage Cloud Volumes ONTAP	300 Go au moins disponibles
Nœuds workers (exigence AWS EC2)	Au moins 3 nœuds workers au total, avec 4 cœurs de vCPU et 12 Go de RAM chacun
Équilibrage de la charge	Type de service « LoadBalancer » disponible pour que le trafic d'entrée soit envoyé aux services du cluster d'environnement opérationnel
FQDN	Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée
Astra Trident (installé dans le cadre de la découverte du cluster Kubernetes dans NetApp Cloud Manager)	Astra Trident 21.04 ou version ultérieure installé et configuré et NetApp ONTAP 9.5 ou version ultérieure en tant que système de stockage back-end

Composant	Conditions requises
Registre d'images	Vous devez disposer d'un registre privé existant, comme AWS Elastic Container Registry, auquel vous pouvez pousser les images de création Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images. Le cluster hébergé par Astra Control Center et le cluster géré doivent avoir accès au même registre d'images pour pouvoir sauvegarder et restaurer des applications à l'aide de l'image Restic.
Configuration d'Astra Trident et ONTAP	Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. L'Astra Control Center prend en charge les classes de stockage Kubernetes suivantes de ONTAP qui sont créées lorsque vous importez le cluster Kubernetes dans NetApp Cloud Manager. Découvrez Astra Trident : • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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

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

Présentation du déploiement pour AWS

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

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

1. Assurez-vous que vous disposez de suffisamment d'autorisations IAM.
2. Installez un cluster Red Hat OpenShift sur AWS.
3. Configurez AWS.
4. Configurez NetApp Cloud Manager.
5. Poser le centre de contrôle Astra.

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 Cloud Manager.

Voir "Identifiants AWS initiaux".

Installez un cluster Red Hat OpenShift sur AWS

Installez un cluster Red Hat OpenShift Container Platform sur AWS.

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

Configurez AWS

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

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

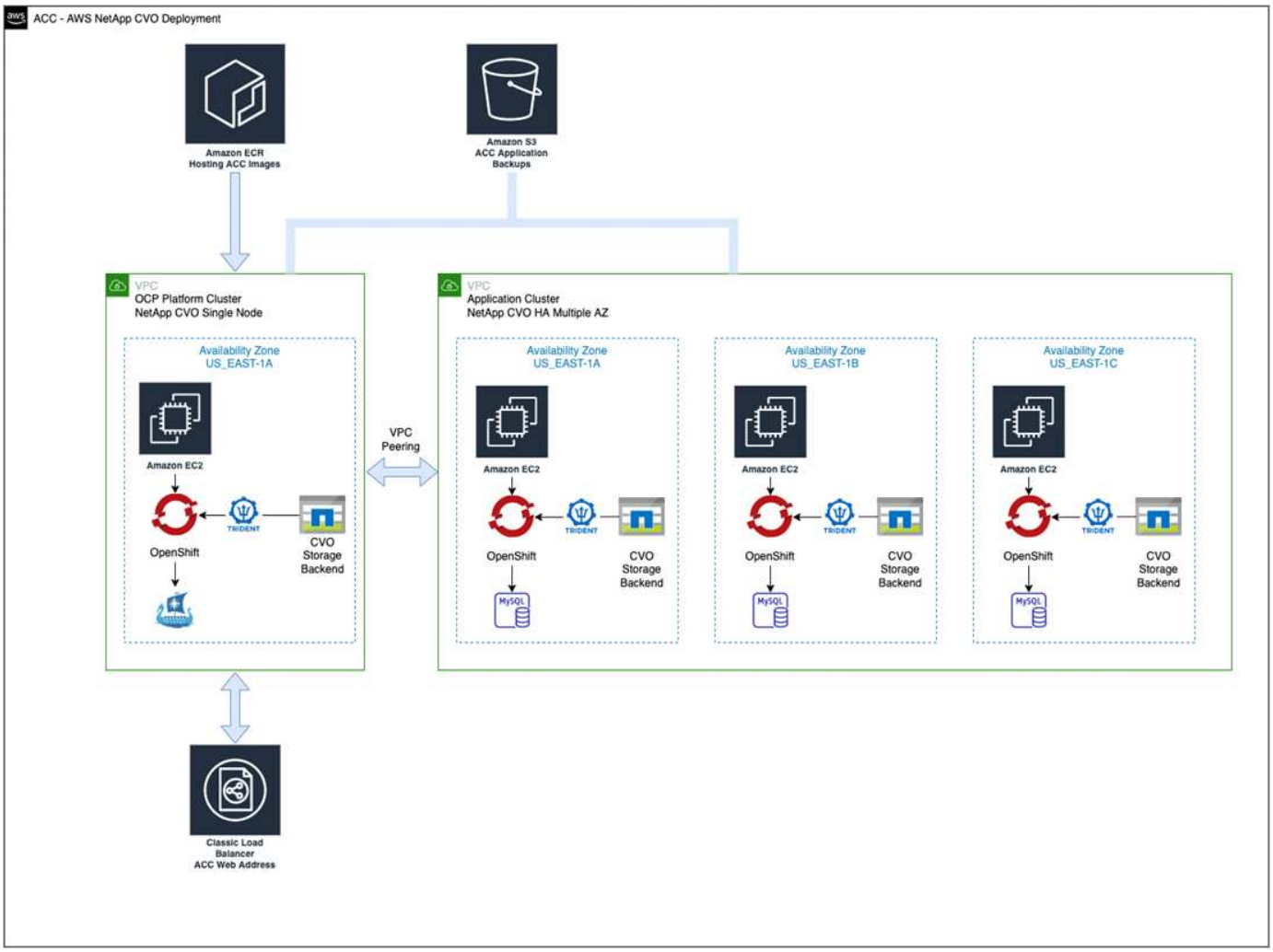
1. Créez un réseau virtuel AWS.
2. Vérifiez les instances de calcul EC2. Il peut s'agir d'un serveur bare Metal ou de machines virtuelles dans AWS.
3. Si le type d'instance ne correspond pas déjà aux exigences de ressources minimales Astra pour les nœuds maîtres et workers, modifiez le type d'instance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

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

6. Poussez les images ACC dans le registre défini.

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

Voici un exemple de déploiement AWS :



Configurez NetApp Cloud Manager

Avec Cloud Manager, créez un espace de travail, ajoutez un connecteur à AWS, créez un environnement de travail et importez le cluster.

Suivez la documentation de Cloud Manager 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 Cloud Manager"

Étapes

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

b. Notez la version Trident dans le coin supérieur droit.

c. Notez les classes de stockage du cluster Cloud Volumes ONTAP indiquant NetApp comme provisionneur.

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

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

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

Poser le centre de contrôle Astra

Respectez la norme "Instructions d'installation du centre de contrôle Astra".

> AWS utilise le type de compartiment S3 générique.

Déployez Astra Control Center dans Google Cloud Platform

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

Éléments requis pour GCP

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

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

Exigences de l'environnement opérationnel pour GCP

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

Le Centre de contrôle Astra requiert les ressources suivantes en plus des exigences de l'environnement en matière de ressources :

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

Composant	Conditions requises
Nœuds workers (exigences de calcul GCP)	Au moins 3 nœuds workers au total, avec 4 cœurs de vCPU et 12 Go de RAM chacun
Équilibrage de la charge	Type de service « LoadBalancer » disponible pour que le trafic d'entrée soit envoyé aux services du cluster d'environnement opérationnel
FQDN (ZONE DNS GCP)	Méthode permettant de pointer le FQDN de Astra Control Center vers l'adresse IP à charge équilibrée
Astra Trident (installé dans le cadre de la découverte du cluster Kubernetes dans NetApp Cloud Manager)	Astra Trident 21.04 ou version ultérieure installé et configuré et NetApp ONTAP 9.5 ou version ultérieure en tant que système de stockage back-end
Registre d'images	Vous devez disposer d'un registre privé existant, tel que le registre de conteneurs Google, auquel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous allez télécharger les images. Vous devez activer l'accès anonyme pour extraire les images Restic pour les sauvegardes.
Configuration d'Astra Trident et ONTAP	Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. L'Astra Control Center prend en charge les classes de stockage Kubernetes suivantes de ONTAP qui sont créées lorsque vous importez le cluster Kubernetes dans NetApp Cloud Manager. Découvrez Astra Trident : • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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

Présentation du déploiement pour GCP

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

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

1. Installez un cluster Red Hat OpenShift sur GCP.
2. Création d'un projet GCP et d'un cloud privé virtuel.
3. Assurez-vous que vous disposez de suffisamment d'autorisations IAM.
4. Configurez GCP.
5. Configurez NetApp Cloud Manager.
6. Installer et configurer le centre de contrôle Astra.

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 Cloud Manager.

Voir "Identifiants et autorisations GCP initiaux".

Configurez GCP

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

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

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

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

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

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

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

   Exemple :

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

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

8. Configurer les zones DNS.

Configurez NetApp Cloud Manager

Avec Cloud Manager, créez un espace de travail, ajoutez un connecteur à GCP, créez un environnement de travail et importez le cluster.

Suivez la documentation de Cloud Manager pour effectuer les étapes suivantes. Voir "Mise en route de Cloud Volumes ONTAP dans GCP".

Ce dont vous avez besoin

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

Étapes

1. Ajoutez vos identifiants à Cloud Manager. 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 Cloud Manager".
   c. S'assurer que le connecteur est en marche et basculer vers ce connecteur.

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

      Cela importe votre cluster Red Hat OpenShift et lui attribue une classe de stockage par défaut. Vous sélectionnez la classe de stockage. Trident est automatiquement installé dans le cadre du processus d'importation et de détection.
5. Noter tous les volumes et volumes persistants sur ce déploiement Cloud Volumes ONTAP

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

Poser le centre de contrôle Astra

Respectez la norme "Instructions d'installation du centre de contrôle Astra".

> GCP utilise le type de compartiment S3 générique.

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

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

Déploiement d'Astra Control Center dans Microsoft Azure

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

Ce dont vous avez besoin pour Azure

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

- Licence Astra Control Center. Voir "Exigences de licence d'Astra Control Center".
- "Découvrez les exigences d'Astra Control Center".
- Compte NetApp Cloud Central
- Si vous utilisez OCP, Red Hat OpenShift Container Platform (OCP) 4.8

- En cas d'utilisation des autorisations OCP, Red Hat OpenShift Container Platform (OCP) (au niveau de l'espace de noms pour créer des pods)
- Les identifiants Azure avec autorisations qui vous permettent de créer des compartiments et des connecteurs

Exigences de l'environnement opérationnel pour Azure

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

Le Centre de contrôle Astra requiert les ressources suivantes en plus des exigences de l'environnement en matière de ressources :

Voir "Exigences relatives à l'environnement opérationnel d'Astra Control Center".

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

Composant	Conditions requises
Configuration d'Astra Trident et ONTAP	Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. L'Astra Control Center prend en charge les classes de stockage Kubernetes suivantes de ONTAP qui sont créées lorsque vous importez le cluster Kubernetes dans NetApp Cloud Manager. Découvrez Astra Trident : • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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

Présentation du déploiement pour Azure

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

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

1. Installez un cluster Red Hat OpenShift sur Azure.
2. Créez des groupes de ressources Azure.
3. Assurez-vous que vous disposez de suffisamment d'autorisations IAM.
4. Configurez Azure.
5. Configurez NetApp Cloud Manager.
6. Installer et configurer le centre de contrôle Astra.

Installez un cluster Red Hat OpenShift sur Azure

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

Pour obtenir des instructions d'installation, reportez-vous à la documentation RedHat sur "Installation du cluster OpenShift sur Azure" et "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 Cloud Manager.

Voir "Identifiants et autorisations Azure".

Configurez Azure

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

Suivez la documentation Azure pour suivre les étapes ci-dessous. Voir "Installation du cluster OpenShift sur Azure".

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

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

   Exemple :

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

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

10. Configurer les zones DNS.

Configurez NetApp Cloud Manager

Avec Cloud Manager, créez un espace de travail, ajoutez un connecteur à Azure, créez un environnement de travail et importez le cluster.

Suivez la documentation de Cloud Manager pour effectuer les étapes suivantes. Voir "Mise en route de Cloud Manager dans Azure".

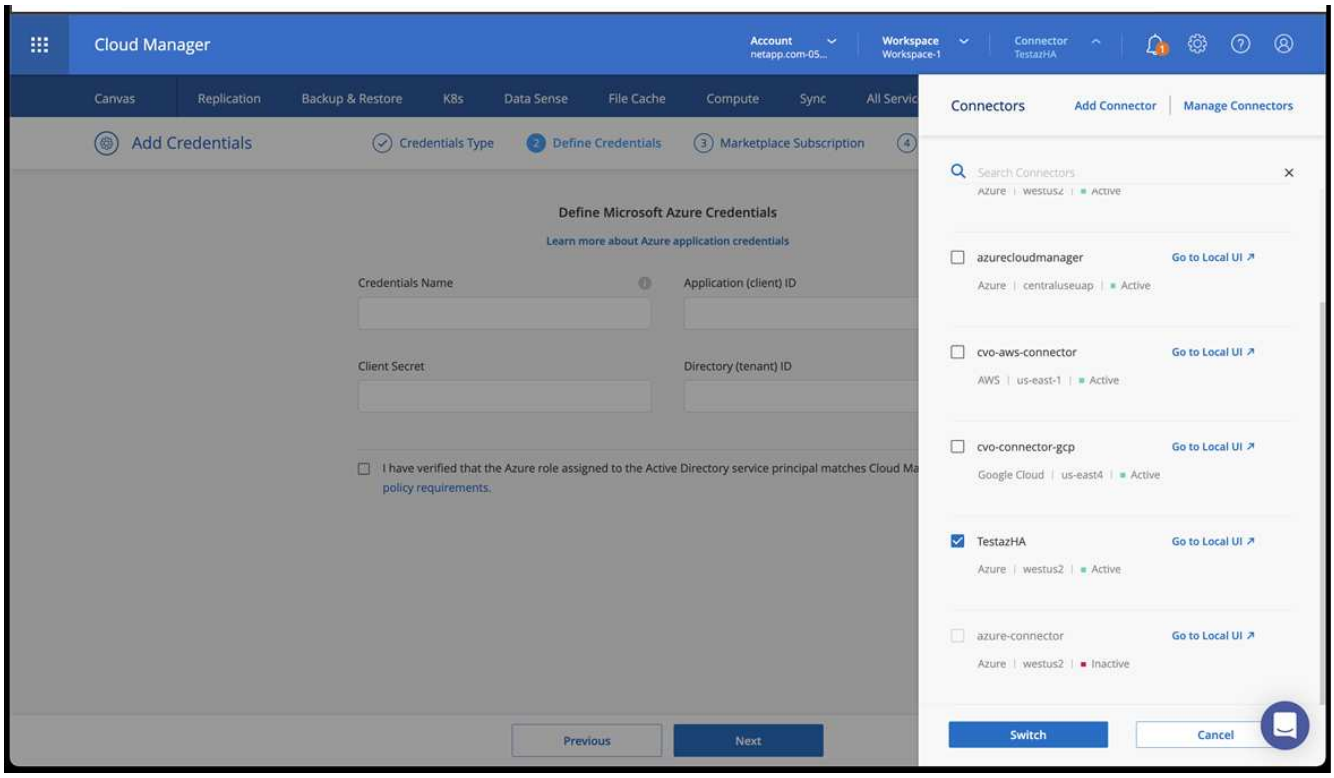
Ce dont vous avez besoin

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

Étapes

1. Ajoutez vos identifiants à Cloud Manager.
2. Ajoutez un connecteur pour Azure. Voir "Règles de Cloud Manager".
   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).

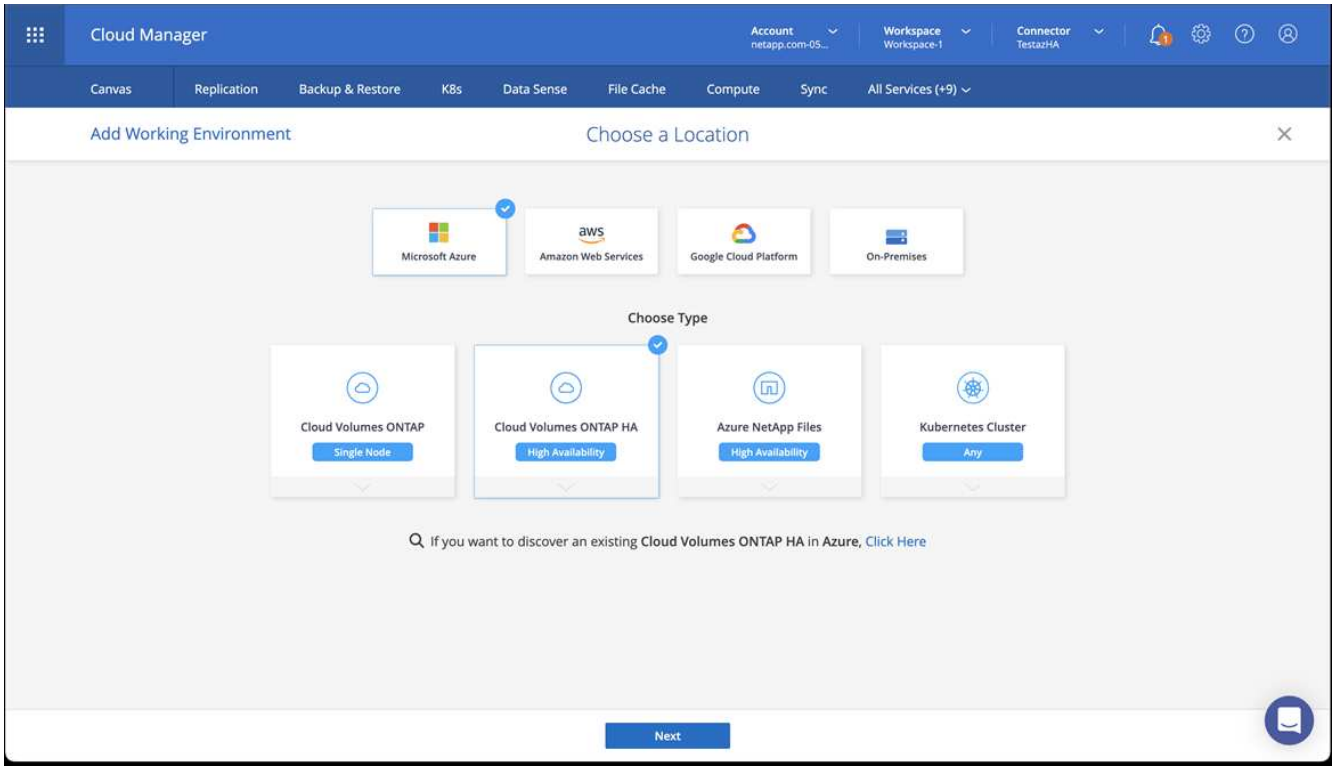
      Voir "Création d'un connecteur dans Azure à partir de Cloud Manager".
3. S'assurer que le connecteur est en marche et basculer vers ce connecteur.



4. Créez un environnement de travail pour votre environnement cloud.

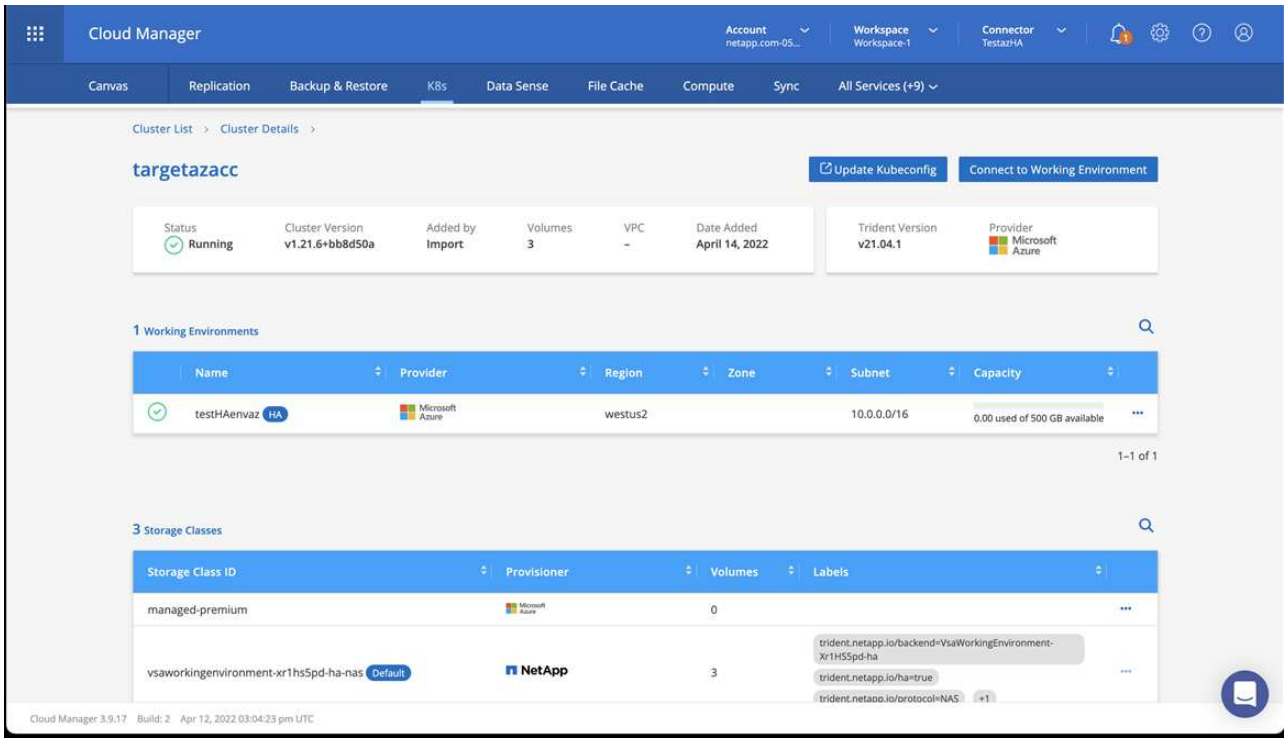
   a. Emplacement : « Microsoft Azure ».

   b. Type : « Cloud Volumes ONTAP HA ».



5. Importer le cluster OpenShift Le cluster se connecte à l'environnement de travail que vous venez de créer.

   a. Pour en savoir plus sur le cluster NetApp, sélectionnez **K8s** > **liste des clusters** > **Détails du cluster**.



b. Notez la version Trident dans le coin supérieur droit.

c. Notez les classes de stockage du cluster Cloud Volumes ONTAP indiquant NetApp comme provisionneur.

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

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

Installer et configurer le centre de contrôle Astra

Installer le centre de contrôle Astra de série "instructions d'installation".

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

Configurer le centre de contrôle Astra

Astra Control Center prend en charge et surveille ONTAP et Astra Data Store en tant que système back-end de stockage. Après avoir installé Astra Control Center, connectez-vous à l'interface utilisateur et modifiez votre mot de passe, vous devez configurer une licence, ajouter des clusters, gérer le stockage et ajouter des compartiments.

Tâches

- Ajoutez une licence pour Astra Control Center
- Ajouter un cluster
- Ajout d'un système back-end

- Ajouter un godet

Ajoutez une licence pour Astra Control Center

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

Pour plus d'informations sur le calcul des licences, reportez-vous à la section "Licences".

> Pour mettre à jour une évaluation existante ou une licence complète, voir "Mettre à jour une licence existante".

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

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

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

Ce dont vous avez besoin

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

Étapes

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

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

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

Ajouter un cluster

Pour commencer à gérer vos applications, ajoutez un cluster Kubernetes et gérez-le comme une ressource de calcul. Il faut ajouter un cluster pour découvrir vos applications Kubernetes pour Astra Control Center. Avec Astra Data Store, vous pouvez ajouter le cluster d'applications Kubernetes qui contient des applications qui utilisent des volumes provisionnés par Astra Data Store.

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

Lorsque Astra Control gère un cluster, il conserve le suivi de la classe de stockage par défaut du cluster. Si vous modifiez la classe de stockage à l'aide de `kubectl` Contrôle Astra rétablit le changement. Pour modifier la classe de stockage par défaut d'un cluster géré par Astra Control, utilisez l'une des méthodes suivantes :

- Utilisez l'API de contrôle Astra `PUT /managedClusters` et attribuez une classe de stockage par défaut différente à l' `DefaultStorageClass` paramètre.
- Utilisez l'interface utilisateur Web Astra Control pour attribuer une classe de stockage par défaut différente. Voir Modifiez la classe de stockage par défaut.

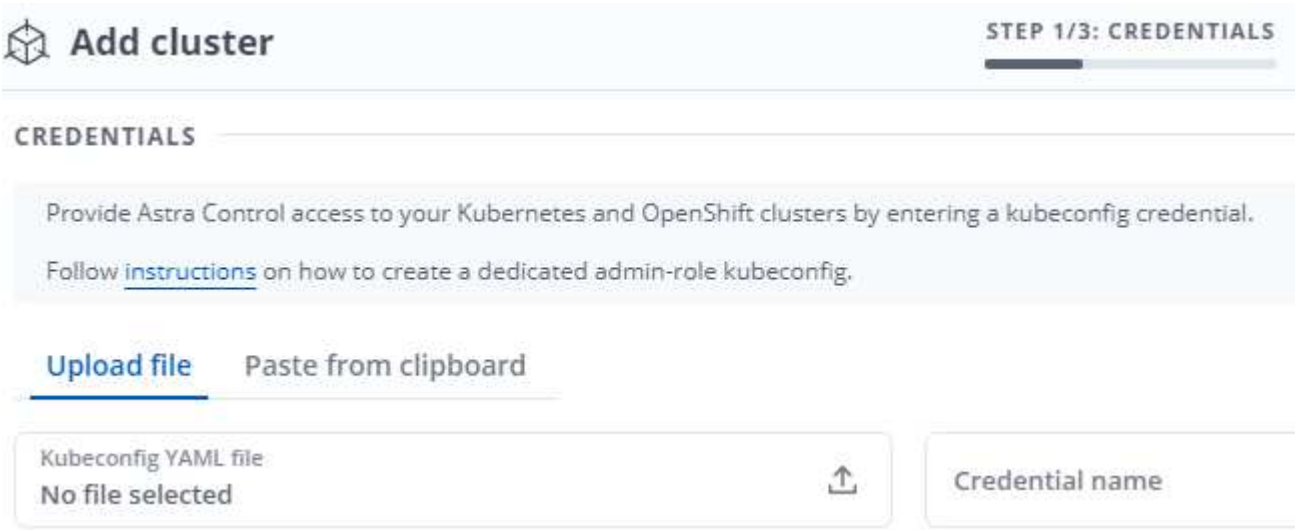
Ce dont vous avez besoin

- Avant d'ajouter un cluster, vérifiez et effectuez les opérations nécessaires "tâches préalables".

Étapes

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

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

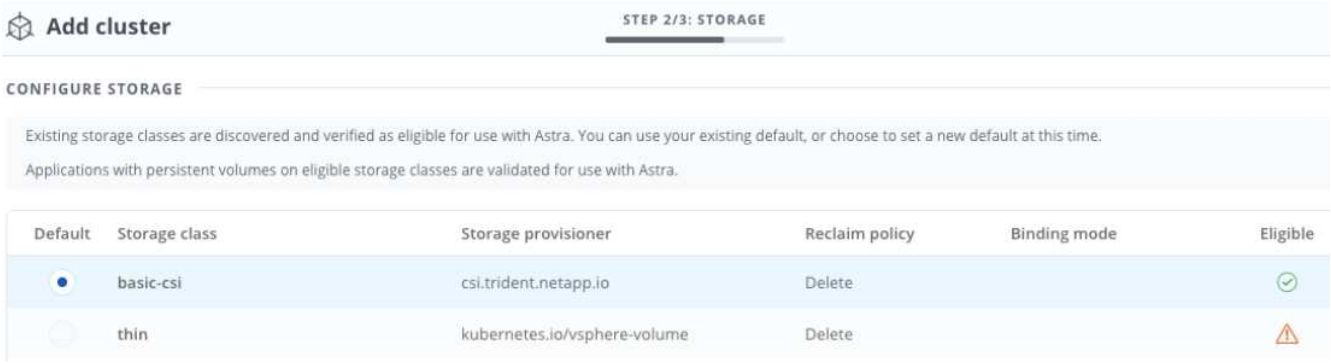


   Si vous créez la vôtre `kubeconfig` fichier, vous ne devez définir que **un** élément de contexte dans celui-ci. Voir "Documentation Kubernetes" pour plus d'informations sur la création `kubeconfig` fichiers.

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

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

> Nous vous recommandons de sélectionner une classe de stockage Trident avec le stockage ONTAP ou le magasin de données Astra.



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

Résultat

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

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

Ajout d'un système back-end

Vous pouvez ajouter un système de stockage back-end pour qu'Astra Control puisse gérer ses ressources. Vous pouvez déployer un système back-end de stockage sur un cluster géré ou utiliser un système back-end existant.

La gestion des clusters de stockage d'Astra Control en tant que backend de stockage vous permet d'obtenir des liens entre les volumes persistants (PVS) et le back-end de stockage, ainsi que des metrics de stockage supplémentaires.

Il vous faudra pour déployer un data Store Astra

- Vous avez ajouté votre cluster d'applications Kubernetes et le cluster de calcul sous-jacent.

> Lorsque vous ajoutez votre cluster d'applications Kubernetes pour Astra Data Store et qu'il est géré par Astra Control, le cluster apparaît comme `unmanaged` dans la liste des systèmes back-end découverts. Vous devez ensuite ajouter le cluster de calcul qui contient Astra Data Store et qui intègre le cluster d'applications Kubernetes. Vous pouvez le faire à partir de **Backends** dans l'interface utilisateur. Sélectionnez le menu actions du cluster, puis `Manage`, et "ajouter le cluster". Après l'état du cluster de `unmanaged` Modifications au nom du cluster Kubernetes, vous pouvez procéder à l'ajout d'un back-end.

Il vous faudra de nouveaux déploiements de data Store Astra

- Vous avez "a chargé la version du pack d'installation que vous envisagez de déployer" À un endroit accessible à Astra Control.
- Vous avez ajouté le cluster Kubernetes que vous souhaitez utiliser pour le déploiement.
- Vous avez téléchargé le Licence Astra Data Store Pour votre déploiement vers un emplacement accessible à Astra Control.

Options

- Déploiement des ressources de stockage
- Utiliser un système back-end existant

Déploiement des ressources de stockage

Vous pouvez déployer un nouveau magasin de données Astra et gérer le stockage back-end associé.

Étapes

1. Naviguer dans le tableau de bord ou le menu Backends :
   - Dans **Dashboard** : dans le Résumé des ressources, sélectionnez un lien dans le volet stockage arrière-plans et sélectionnez **Ajouter** dans la section Backends.
   - À partir de **Backends** :
     i. Dans la zone de navigation de gauche, sélectionnez **Backends**.
     ii. Sélectionnez **Ajouter**.
2. Sélectionnez l'option de déploiement **Astra Data Store** dans l'onglet **Deploy**.
3. Sélectionnez le package de magasin de données Astra à déployer :
   a. Entrez un nom pour l'application de magasin de données Astra.
   b. Choisissez la version d'Astra que vous voulez déployer.

   > Si vous n'avez pas encore téléchargé la version que vous avez l'intention de déployer, vous pouvez utiliser l'option **Ajouter un paquet** ou quitter l'assistant et utiliser "gestion des packages" pour télécharger le pack d'installation.

4. Sélectionnez une licence Astra Data Store que vous avez déjà téléchargée ou utilisez l'option **Ajouter une licence** pour télécharger une licence à utiliser avec l'application.

> Les licences Astra Data Store avec autorisation complète sont associées à votre cluster Kubernetes, et ces clusters associés doivent apparaître automatiquement. S'il n'y a pas de cluster géré, vous pouvez sélectionner l'option **Ajouter un cluster** pour en ajouter un à Astra Control Management. Pour les licences Astra Data Store, si aucune association n'a été établie entre la licence et le cluster, vous pouvez définir cette association à la page suivante de l'assistant.

5. Si vous n'avez pas ajouté de cluster Kubernetes à la gestion Astra Control, vous devez le faire depuis la page **cluster Kubernetes**. Sélectionnez un cluster existant dans la liste ou sélectionnez **Ajouter le cluster sous-jacent** pour ajouter un cluster à la gestion Astra Control.
6. Sélectionnez une taille de modèle pour le cluster Kubernetes qui fournira les ressources pour le magasin de données Astra. Vous pouvez choisir l'une des options suivantes :
   - Si vous le souhaitez `Recommended Kubernetes worker node requirements`, sélectionnez un modèle de grande à petite en fonction de ce que votre licence autorise.
   - Si vous le souhaitez `Custom Kubernetes worker node requirements`, sélectionnez le nombre de cœurs et la mémoire totale que vous souhaitez pour chaque nœud de cluster. Vous pouvez également afficher le nombre de nœuds éligibles qui répondent à vos critères de sélection pour les cœurs et la mémoire.

> Lorsque vous choisissez un modèle, sélectionnez des nœuds de grande taille avec plus de mémoire et de cœurs pour des charges de travail plus importantes ou un nombre plus important de nœuds pour des charges de travail plus petites. Vous devez sélectionner un modèle en fonction de ce que votre licence autorise. Chaque option de modèle recommandée indique le nombre de nœuds éligibles qui répondent au modèle de modèle pour la mémoire, les cœurs et la capacité de chaque nœud.

7. Configurez les nœuds :
   a. Ajoutez une étiquette de nœud pour identifier le pool de nœuds de travail qui prend en charge ce cluster de magasin de données Astra.

> L'étiquette doit être ajoutée à chaque nœud du cluster qui sera utilisé pour le déploiement du magasin de données Astra avant le début du déploiement, sinon le déploiement échouera.

   b. Configurez la capacité (Gio) par nœud manuellement ou sélectionnez la capacité maximale de nœud autorisée.
   c. Configurez un nombre maximum de nœuds autorisés dans le cluster ou autorisez le nombre maximum de nœuds sur le cluster.
8. (Licences complètes de l'Astra Data Store uniquement) Entrez la clé de l'étiquette que vous souhaitez utiliser pour les domaines de protection.

> Créez au moins trois étiquettes uniques pour la clé pour chaque nœud. Par exemple, si votre clé est `astra.datastore.protection.domain`, vous pouvez créer les étiquettes suivantes : `astra.datastore.protection.domain=domain1` ,`astra.datastore.protection.domain=domain2`, et `astra.datastore.protection.domain=domain3`.

9. Configurez le réseau de gestion :

a. Saisissez une adresse IP de gestion pour la gestion interne du magasin de données Astra qui se trouve sur le même sous-réseau que les adresses IP du nœud de travail.
b. Choisissez d'utiliser la même carte réseau à la fois pour les réseaux de gestion et de données ou de les configurer séparément.
c. Entrez le pool d'adresses IP du réseau de données, le masque de sous-réseau et la passerelle pour l'accès au stockage.

10. Vérifiez la configuration et sélectionnez **Deploy** pour commencer l'installation.

Résultat

Après une installation réussie, le système back-end apparaît dans `available` état dans la liste des systèmes back-end avec des informations de performance actives.

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

Utiliser un système back-end existant

Vous pouvez intégrer un système back-end de stockage ONTAP ou Astra dans la gestion du centre de contrôle d'Astra.

Étapes

1. Naviguer dans le tableau de bord ou le menu Backends :
   - Dans **Dashboard** : dans le Résumé des ressources, sélectionnez un lien dans le volet stockage arrière-plans et sélectionnez **Ajouter** dans la section Backends.
   - À partir de **Backends** :
     i. Dans la zone de navigation de gauche, sélectionnez **Backends**.
     ii. Sélectionnez **Manage** sur un back-end découvert à partir du cluster géré ou sélectionnez **Add** pour gérer un back-end existant supplémentaire.
2. Sélectionnez l'onglet **utiliser existant**.
3. Effectuez l'une des opérations suivantes en fonction de votre type de système back-end :
   - **Magasin de données Astra**:
     i. Sélectionnez **Astra Data Store**.
     ii. Sélectionnez le cluster de calcul géré et sélectionnez **Suivant**.
     iii. Confirmez les détails du back-end et sélectionnez **Ajouter le back-end de stockage**.
   - **ONTAP** :
     i. Sélectionnez **ONTAP** et sélectionnez **Suivant**.
     ii. Saisissez l'adresse IP de gestion du cluster ONTAP et les identifiants d'administrateur.

     > 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, activez les méthodes d'accès `ontapi` et `http` Pour l'utilisateur sur les deux clusters ONTAP. Voir "Gérer les comptes d'utilisateurs" pour en savoir plus.

     iii. Sélectionnez **Revue**.
     iv. Confirmez les détails du back-end et sélectionnez **Ajouter le back-end de stockage**.

Résultat

Le back-end apparaît dans `available` état dans la liste avec des informations récapitulatives.

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

Ajouter un godet

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

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

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

Utiliser l'un des types de godet suivants :

- NetApp ONTAP S3
- NetApp StorageGRID S3
- S3 générique

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

- Microsoft Azure

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

- Microsoft Azure

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

Étapes

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

   > Lorsque vous ajoutez un compartiment, sélectionnez le 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.

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

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

d. Entrez le nom ou l'adresse IP du terminal S3.

e. Si vous souhaitez que ce compartiment soit utilisé comme compartiment par défaut pour toutes les sauvegardes, vérifiez le `Make this bucket the default bucket for this private cloud` option.

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

f. Continuez en ajoutant informations d'identification.

Ajoutez des identifiants d'accès S3

Ajoutez les identifiants d'accès S3 à tout moment.

Étapes

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

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster.

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**.

Et la suite ?

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

- "Gérer les utilisateurs"
- "Commencez à gérer les applications"
- "Protégez vos applications"
- "Clonage des applications"
- "Gérer les notifications"
- "Connectez-vous à Cloud Insights"

- "Ajouter un certificat TLS personnalisé"

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"
- "Problèmes connus"

Conditions préalables à l'ajout d'un cluster

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

Ce dont vous avez besoin avant d'ajouter un cluster

Assurez-vous que votre cluster répond aux exigences décrites dans "Configuration requise en cluster des applications".

> Si vous prévoyez d'ajouter un deuxième cluster OpenShift 4.6, 4.7 ou 4.8 en tant que ressource de calcul gérée, assurez-vous que la fonctionnalité Snapshot de volume Astra Trident est activée. Découvrez l'Astra Trident officielle "instructions" Pour activer et tester des copies Snapshot de volume avec Astra Trident.

- Les classes de stockage Astra Trident sont configurées avec un "système back-end pris en charge" (requis pour tout type de cluster)
- Le superutilisateur et l'ID utilisateur définis sur le système ONTAP de sauvegarde pour sauvegarder et restaurer des applications avec le Centre de contrôle Astra. Exécutez la commande suivante dans la ligne de commande ONTAP :
  `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Découvrez Astra Trident `volumesnapshotclass` objet défini par un administrateur. Découvrez Astra Trident "instructions" Pour activer et tester des copies Snapshot de volume avec Astra Trident.
- Assurez-vous de n'avoir qu'une seule classe de stockage par défaut définie pour votre cluster Kubernetes.

Effectuer des vérifications d'éligibilité

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

Étapes

1. Vérifiez la version de Trident.

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

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

```
NAME      VERSION
trident   21.04.0
```

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

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

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

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

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

Créez un kubeconfig. Rôle admin

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

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

Étapes

1. Créer un compte de service comme suit :

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

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

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

+

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

a. Appliquer le compte de service :

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

2. (Facultatif) si votre cluster utilise une politique de sécurité de pod restrictive qui ne permet pas la création de pod privilégié ou l'exécution des processus dans les conteneurs de pod en tant qu'utilisateur racine, créez une politique de sécurité de pod personnalisée pour le cluster qui permet à Astra Control de créer et de gérer des pods. Pour obtenir des instructions, reportez-vous à la section "Créez une stratégie de sécurité de pod personnalisée".
3. Accordez des autorisations d'administration du cluster comme suit :

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

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

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

+

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

a. Appliquer la liaison de rôle de cluster :

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

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

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

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

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

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

5. Générez le kubeconfig comme suit :

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

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

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

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

CONTEXT=$(kubectl config current-context)

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

```
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

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

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

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

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

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

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

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

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

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

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

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

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

6. (**Facultatif**) Renommer le kubeconfig en un nom significatif pour votre grappe. Protéger les informations d'identification du cluster.

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

Et la suite ?

Maintenant que vous avez vérifié que les conditions préalables sont remplies, vous êtes prêt à "ajouter un cluster".

Trouvez plus d'informations

- "Documentation Trident"
- "Utilisez l'API de contrôle Astra"

Ajouter un certificat TLS personnalisé

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

Ce dont vous avez besoin

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

Supprimez le certificat auto-signé

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

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>
....

#spec:
#  selfSigned: {}

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Créez une stratégie de sécurité de pod personnalisée

Astra Control doit créer et gérer des pods Kubernetes sur les clusters qu'il gère. Si votre cluster utilise une politique de sécurité de pod restrictive qui ne permet pas la création de pod privilégié ou l'exécution des processus dans les conteneurs de pod en tant qu'utilisateur racine, vous devez créer une stratégie de sécurité de pod moins restrictive pour permettre à Astra Control de créer et de gérer ces pods.

Étapes

1. Créez une politique de sécurité du pod pour le cluster qui est moins restrictive par défaut et enregistrez-la dans un fichier. Par exemple :

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. Créez un nouveau rôle pour la stratégie de sécurité du pod.

```
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. Lier le nouveau rôle au compte de service.

```
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

Foire aux questions pour Astra Control Center

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

Présentation

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

Accès au centre de contrôle Astra

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

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

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

Licences

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

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

Étapes

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

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

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

Enregistrement des clusters Kubernetes

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

De nouveaux nœuds workers peuvent être ajoutés aux pools existants. Elles seront automatiquement découvertes par Astra Control. Si les nouveaux nœuds ne sont pas visibles dans Astra Control, vérifiez si les nouveaux nœuds de travail exécutent le type d'image pris en charge. Vous pouvez également vérifier l'état de santé des nouveaux nœuds workers à l'aide de la `kubectl get nodes` commande.

Comment puis-je dégérer correctement un cluster?

1. "Gérez les applications avec Astra Control".
2. "Dégérer le cluster à partir d'Astra Control".

Que se passe-t-il pour mes applications et données après avoir retiré le cluster Kubernetes d'Astra Control?

La suppression d'un cluster d'Astra Control ne modifie pas la configuration du cluster (applications et stockage persistant). Toute restauration de snapshots ou de sauvegardes Astra Control effectuée sur ce cluster sera indisponible. Les sauvegardes de stockage persistant créées par Astra Control restent dans le contrôle d'Astra, mais elles sont indisponibles pour les restaurations.

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

NetApp Trident est-il automatiquement désinstallé d'un cluster lorsque je le dégère ? lorsque vous dégérez un cluster depuis Astra Control Center, Trident n'est pas automatiquement désinstallé du cluster. Pour désinstaller Trident, vous devez procéder comme ça "Suivez ces étapes dans la documentation Trident".

La gestion des applications

Astra Control peut-il déployer une application?

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

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

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

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

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

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

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

Les opérations de gestion des données

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

Dans certains cas, Astra Control crée automatiquement un snapshot dans le cadre d'un processus de sauvegarde, de clonage ou de restauration.

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

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

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

différent?

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

Utilisez Astra

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 commencer à gérer les applications et leurs ressources.

Pour plus d'informations, voir "Besoins en termes de gestion des applications".

Méthodes d'installation d'applications prises en charge

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

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

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

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

  Voici quelques applications opérateur qui suivent ces modèles :

  - "Apache K8ssandra"

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

  - "IC Jenkins"
  - "Cluster Percona XtraDB"

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

Installez les applications sur votre cluster

Après vous l'avez "a ajouté votre cluster" Avec Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application dont l'étendue correspond à un espace de noms unique peut être gérée.

Gérer des 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 "gérez tout un espace de noms comme une seule application ou gérez une ou plusieurs applications dans l'espace de noms individuellement". 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), il est recommandé de choisir l'un ou l'autre. Les actions que vous prenez dans Astra Control peuvent échouer si les actions ont lieu en même temps au niveau de l'espace de noms et de l'application.

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

Ce dont vous avez besoin

- Un cluster Kubernetes ajouté à Astra Control.
- Une ou plusieurs applications installées sur le cluster. En savoir plus sur les méthodes d'installation d'applications prises en charge.
- Un ou plusieurs pods actifs.
- Les espaces de noms spécifiés 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".

Avant de commencer, vous devez également comprendre "gestion des espaces de noms standard et système".

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

Options supplémentaires de gestion des applications

- Annuler la gestion des applications

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 des ressources Kubernetes peut provoquer des conflits de données. Pour en savoir plus sur les meilleures pratiques,

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 l'espace de nom de votre application dans la liste déroulante **namespace**.

   > Les applications ne peuvent être définies que au sein d'un espace de nom spécifié sur un même cluster. Astra Control ne prend pas en charge la capacité des applications à s'étendre sur plusieurs espaces de noms ou clusters.

5. Saisissez un libellé pour l'application et l'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. 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 apparaît 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.

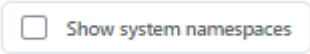
Définissez un espace de noms à gérer en tant qu'application

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 gérer plusieurs espaces de noms, sélectionnez-les, puis sélectionnez le bouton **actions** dans le coin supérieur gauche et sélectionnez **gérer**.

> 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.

Annuler la gestion des applications

Lorsque vous ne souhaitez plus sauvegarder, créer des copies Snapshot ou cloner une application, vous pouvez arrêter de la gérer.

> Si vous annulez la gestion d'une application, toutes les sauvegardes ou instantanés créés précédemment seront perdus.

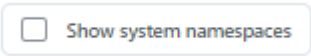
Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez l'application.
3. Dans le menu de la colonne **actions**, sélectionnez **Unmanage**.
4. Vérifiez les informations.
5. Tapez « Unmanage » pour confirmer.
6. Sélectionnez **Oui, Annuler la gestion de l'application**.

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

Exemple : politique de protection distincte pour différentes versions

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

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

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

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

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"

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 Astra ou "API de contrôle Astra" pour protéger les applications.

Si vous utilisez Helm pour déployer des applications, Astra Control Center requiert Helm version 3. La gestion et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.

Lorsque vous créez un projet d'hébergement d'une application sur un cluster OpenShift, un UID SecurityContext est attribué au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

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

- Configurer une règle de protection
- Créer un snapshot
- Créer une sauvegarde
- Afficher les snapshots et les sauvegardes
- Supprimer les instantanés
- Annuler les sauvegardes
- Supprimer les sauvegardes

Configurer une règle de protection

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

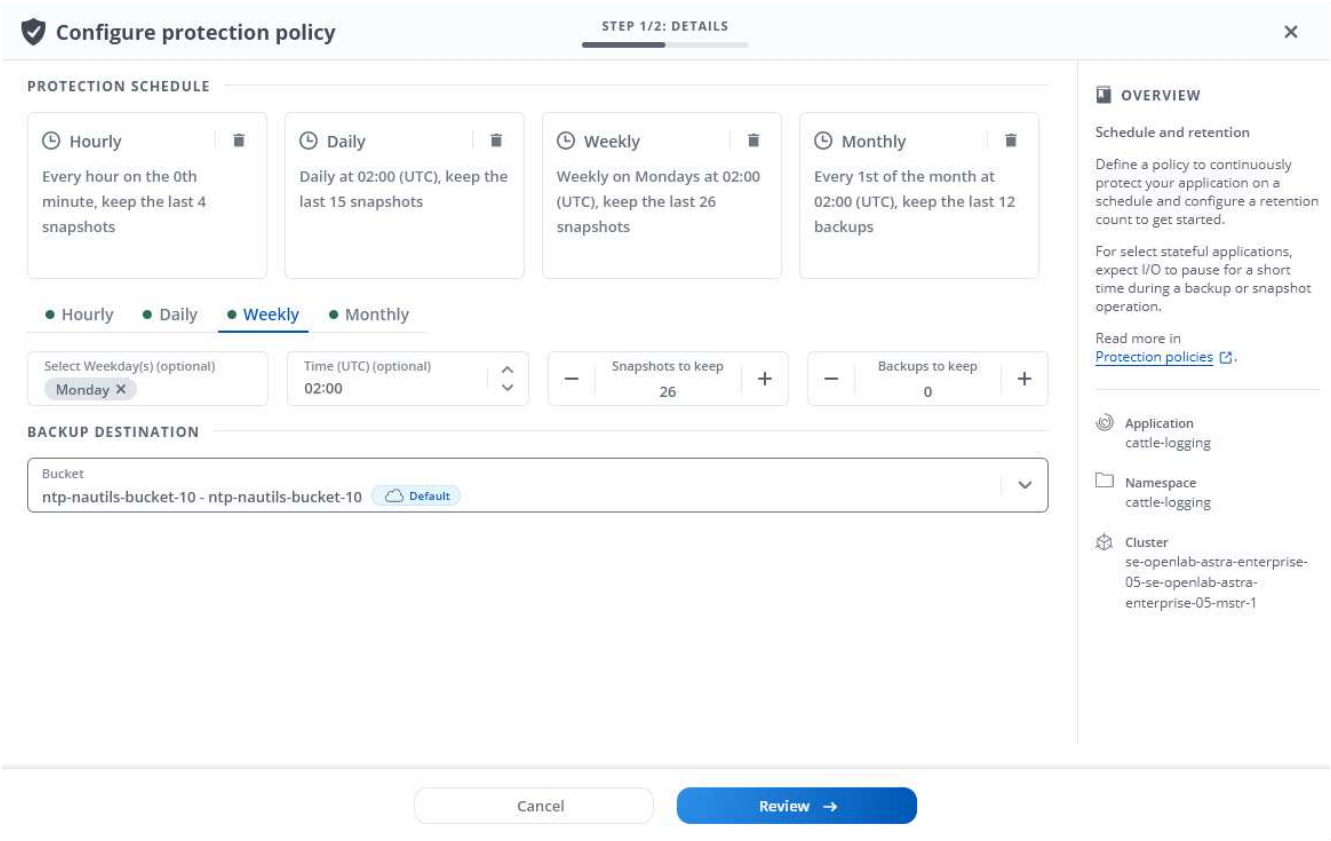
exemple, une règle de protection peut créer des sauvegardes hebdomadaires et des snapshots quotidiens, et conserver les sauvegardes et les snapshots pendant un mois. La fréquence de création des snapshots et des sauvegardes et la durée de conservation dépendent des besoins de votre entreprise.

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.

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

Résultat

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

Créer un snapshot

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

Étapes

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

Résultat

Le processus d'instantané commence. Un instantané a réussi lorsque l'état est **disponible** dans la colonne **actions** de la page **protection des données** > **snapshots**.

Créer une sauvegarde

Vous pouvez également sauvegarder une application à tout moment.

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

Étapes

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

Résultat

Astra Control Center 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.

> Il est impossible d'arrêter une sauvegarde en cours d'exécution. Si vous devez supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez les instructions de la section Supprimer les sauvegardes. Pour supprimer une sauvegarde défaillante, "Utilisez l'API de contrôle Astra".

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

Afficher les snapshots et les sauvegardes

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

Étapes

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

   Les snapshots s'affichent par défaut.

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

Supprimer les instantanés

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

> Vous ne pouvez pas supprimer une copie Snapshot en cours de réplication.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
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 Center supprime le snapshot.

Annuler les sauvegardes

Vous pouvez annuler une sauvegarde en cours.

> Pour annuler une sauvegarde, la sauvegarde doit être en cours d'exécution. Vous ne pouvez pas annuler une sauvegarde à l'état en attente.

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 la suppression, puis sélectionnez **Oui, annuler la sauvegarde**.

Supprimer les sauvegardes

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

> Il est impossible d'arrêter une sauvegarde en cours d'exécution. Si vous devez supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez ces instructions. Pour supprimer une sauvegarde défaillante, "Utilisez l'API de contrôle Astra".

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 Center supprime la sauvegarde.

Restaurez les applications

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

Description de la tâche

- Il est fortement recommandé de prendre un instantané de ou de sauvegarder votre application avant de la restaurer. Cela vous permettra de cloner à partir du snapshot ou de la sauvegarde en cas d'échec de la restauration.
- Si vous utilisez Helm pour déployer des applications, Astra Control Center requiert Helm version 3. La gestion et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.
- Si vous effectuez une restauration sur un autre cluster, assurez-vous que le cluster utilise le même mode d'accès aux volumes persistants (par exemple, ReadWriteMany). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent.
- Tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par libellés 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 entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.
- Lorsque vous créez un projet d'hébergement d'une application sur un cluster OpenShift, un UID SecurityContext est attribué au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Si vous souhaitez effectuer une restauration à partir d'un instantané, conservez l'icône **snapshots** sélectionnée. Sinon, sélectionnez l'icône **backups** pour restaurer à partir d'une sauvegarde.
4. Dans le menu Options de la colonne **actions** pour l'instantané ou la sauvegarde à partir duquel vous souhaitez restaurer, sélectionnez **Restaurer l'application**.
5. **Détails de restauration** : spécifiez les détails de l'application restaurée. Par défaut, le cluster et l'espace de noms actuels apparaissent. Laissez ces valeurs intactes pour restaurer une application sur place, ce qui rétablit sa version antérieure. Modifiez ces valeurs si vous souhaitez restaurer vers un autre cluster ou espace de noms.
   - Entrez un nom et un espace de noms pour l'application.
   - Choisissez le cluster de destination de l'application.
   - Sélectionnez **Revue**.

   > 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.

6. **Résumé de restauration** : consultez les détails de l'action de restauration, tapez "Restaurer", puis sélectionnez **Restaurer**.

Résultat

Astra Control Center 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.

> À l'issue d'une opération de protection des données (clonage, sauvegarde, restauration) et du redimensionnement ultérieur du volume persistant, la nouvelle taille du volume est retardée de vingt minutes avant que celle-ci ne s'affiche dans l'interface utilisateur Web. 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.

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

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

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

Vous pouvez répliquer des applications dans différents scénarios, comme : uniquement sur site,

environnements hybrides et multicloud :

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

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

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

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

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

Conditions préalables à la réplication

Voir la "conditions préalables à la réplication" avant de commencer.

Configuration d'une relation de réplication

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

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

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection** > **Replication**.
3. Dans l'onglet protection des données > réplication, sélectionnez **configurer la stratégie de réplication**. Ou, dans la zone protection des applications, sélectionnez l'option actions et sélectionnez **configurer la stratégie de réplication**.
4. Entrez ou sélectionnez les informations suivantes :

- Cluster de destination
- **Classe de stockage de destination** : sélectionnez ou entrez la classe de stockage qui utilise le SVM apparié sur le cluster ONTAP de destination.
- **Type de réplication**: "Asynchrone" est actuellement le seul type de réplication disponible.
- **Espace de noms de destination** : saisissez un espace de noms de destination nouveau ou existant pour le cluster de destination.

  > Toute ressource en conflit dans l'espace de noms sélectionné sera remplacée.

- **Fréquence de réplication**: Définissez la fréquence à laquelle vous souhaitez qu'Astra Control prenne un instantané et le réplique à sa destination.
- **Décalage**: Définissez le nombre de minutes à partir du haut de l'heure que vous voulez que le contrôle Astra prenne un instantané. Vous pouvez utiliser un décalage afin qu'il ne coïncide pas avec d'autres opérations planifiées. Par exemple, si vous voulez prendre l'instantané toutes les 5 minutes à partir de 10:02, entrez "02" comme minutes de décalage. Le résultat serait 10:02, 10:07, 10:12, etc

5. Sélectionnez **Suivant**, examinez le résumé et sélectionnez **Enregistrer**.

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

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

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

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

Résultat

Cela crée la relation de réplication.

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

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

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

Par exemple : normal | établi

En savoir plus sur les États et l'état de réplication ci-dessous.

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

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

Étapes

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

Résultat

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

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

Resynchroniser un basculement de réplication impossible

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

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

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

Étapes

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

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

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

Résultat

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

- La page réplication affiche la relation mise à jour.

Réplication inverse des applications

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

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

Étapes

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

Résultat

Les actions suivantes se produisent suite à la réplication inverse :

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

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

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

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

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

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection** > **Replication**.

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

Résultat

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

Supprime une relation de réplication d'application

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

Étapes

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

Résultat

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

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

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

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

États d'intégrité des relations de réplication

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

- **Normal** : la relation est établie ou a été établie, et le snapshot le plus récent a été transféré avec succès.
- **Avertissement** : la relation est soit basculée, soit a échoué (et donc ne protège plus l'app source).
- **Critique**
  - La relation est établie ou a échoué et la dernière tentative de réconciliation a échoué.

- La relation est établie, et la dernière tentative de concilier l'ajout d'un nouveau PVC est un échec.
- La relation est établie (un snapshot réussi a été répliqué, et le basculement est possible), mais le Snapshot le plus récent a échoué ou a échoué à répliquer.

États du cycle de vie de la réplication

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

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

Clonez une application existante pour créer une application dupliquée sur le même cluster Kubernetes ou sur un autre cluster. Lorsque Astra Control Center clone une application, 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 Astra ou "API de contrôle Astra" clonage et migration des applications.

Ce dont vous avez besoin

Pour cloner les applications vers un autre cluster, il vous faut un compartiment par défaut. Lorsque vous

ajoutez votre premier compartiment, il devient le compartiment par défaut.

Description de la tâche

- Si vous déployez une application avec une classe de stockage définie de manière explicite 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 explicitement définie sur un cluster ne disposant pas de la même classe de stockage échouera.
- 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.
- 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.
- Lors d'une sauvegarde 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.
- Tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par libellés 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 entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

Considérations d'OpenShift

- Si vous clonez une application entre les clusters, les clusters source et destination 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.
- Lorsque vous créez un projet d'hébergement d'une application sur un cluster OpenShift, un UID SecurityContext est attribué au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

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. **Détails du clone** : spécifiez les détails du clone :
   - Entrez un nom.

    - Entrez un namespace pour le clone.
    - Choisissez un cluster de destination pour le clone.
    - Indiquez si vous souhaitez créer le clone à partir d'un snapshot ou d'une sauvegarde existant. Si vous ne sélectionnez pas cette option, Astra Control Center crée le clone à partir de l'état actuel de l'application.
5. **Source** : si vous choisissez de cloner à partir d'un snapshot ou d'une sauvegarde existant, choisissez le snapshot ou la sauvegarde que vous souhaitez utiliser.
6. Sélectionnez **Revue**.
7. **Résumé du clone** : consultez les détails sur le clone et sélectionnez **Clone**.

Résultat

Astra Control Center clone cette application en fonction des informations que vous avez fournies. L'opération de clonage est réussie lorsque le nouveau clone d'application est dans `Available` Indiquez la page **applications**.

> 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.

Gérer les crochets d'exécution de l'application

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

Types de crochets d'exécution

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

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

Remarques importantes sur les crochets d'exécution personnalisés

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

- Un crochet d'exécution doit utiliser un script pour effectuer des actions. De nombreux crochets d'exécution peuvent référencer le même script.

- Astra Control exige que les scripts utilisés par les crochets d'exécution soient écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.
- Astra Control utilise les paramètres de crochet d'exécution et tout critère de correspondance pour déterminer quels crochets s'appliquent à une opération de snapshot, de sauvegarde ou de restauration.
- Toutes les défaillances de crochet d'exécution sont des pannes logicielles ; d'autres crochets et l'opération de protection des données sont toujours tentées même en cas de défaillance d'un crochet. Cependant, lorsqu'un crochet échoue, un événement d'avertissement est enregistré dans le journal des événements de la page **activité**.
- Pour créer, modifier ou supprimer des crochets d'exécution, vous devez être un utilisateur disposant des autorisations propriétaire, administrateur ou membre.
- Si l'exécution d'un crochet d'exécution prend plus de 25 minutes, le crochet échoue, créant une entrée de journal d'événements avec un code retour « N/A ». Tout instantané affecté expire et sera marqué comme ayant échoué, avec une entrée du journal des événements qui en résulte indiquant le délai d'attente.
- Pour les opérations de protection de données ad hoc, tous les événements hook sont générés et enregistrés dans le journal des événements de la page **Activity**. Cependant, pour les opérations planifiées de protection des données, seuls les événements de défaillance de type « hook » sont enregistrés dans le journal des événements (les événements générés par les opérations de protection des données planifiées sont toujours enregistrés).

> Puisque les crochets d'exécution réduisent souvent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils sont en cours d'exécution, vous devez toujours essayer de réduire le temps d'exécution de vos crochets d'exécution personnalisés. Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée.

Ordre d'exécution

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

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

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

1. Crochets de pré-secours exécutés
2. Crochets pré-instantanés exécutés

3. Crochets post-snapshot exécutés
4. Crochets post-secours exécutés
5. Crochets post-restauration exécutés

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

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

Déterminez si un crochet va courir

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

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

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

> Si vous démarrez mais annulez ensuite une sauvegarde qui inclut un instantané et qu'il y a des crochets d'exécution associés, certains crochets peuvent s'exécuter, et d'autres peuvent ne pas. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée. Gardez à l'esprit les points suivants pour les sauvegardes annulées avec les crochets d'exécution associés :
>
> - Les crochets de pré-secours et post-secours sont toujours exécutés.
> - Si la sauvegarde inclut un nouvel instantané et que l'instantané a démarré, les crochets pré-instantané et post-instantané sont exécutés.
> - Si la sauvegarde est annulée avant le démarrage de l'instantané, les crochets pré-instantané et post-instantané ne sont pas exécutés.

Scénario	Fonctionnement	Snapshot existant	Sauvegarde existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets
1	Clonage	N	N	Nouveau	Identique	Y	N	Y
2	Clonage	N	N	Nouveau	Différente	Y	Y	Y
3	Cloner ou restaurer	Y	N	Nouveau	Identique	N	N	Y

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
4	Cloner ou restaurer	N	Y	Nouveau	Identique	N	N	Y
5	Cloner ou restaurer	Y	N	Nouveau	Différente	N	Y	Y
6	Cloner ou restaurer	N	Y	Nouveau	Différente	N	N	Y
7	Restaurer	Y	N	Existant	Identique	N	N	Y
8	Restaurer	N	Y	Existant	Identique	N	N	Y
9	Snapshot	S/O	S/O	S/O	S/O	Y	S/O	S/O
10	Sauvegarde	N	S/O	S/O	S/O	Y	Y	S/O
11	Sauvegarde	Y	S/O	S/O	S/O	N	Y	S/O

Afficher les crochets d’exécution existants

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

Étapes

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

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

Afficher les scripts existants

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

Étapes

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

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

Ajouter un script

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

Étapes

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

Résultat

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

Supprimer un script

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

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **scripts**.
3. Choisissez un script à supprimer et sélectionnez le menu dans la colonne **actions**.
4. Sélectionnez **Supprimer**.

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

Créer un crochet d'exécution personnalisé

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

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

Étapes

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

     Cela indique au crochet d'exécution d'utiliser ce script.

9. Sélectionnez **Ajouter crochet**.

Vérifier l'état d'un crochet d'exécution

Une fois qu'une opération de snapshot, de sauvegarde ou de restauration a terminé, vous pouvez vérifier l'état des crochets d'exécution qui ont été exécutés dans le cadre de l'opération. Vous pouvez utiliser ces informations d'état pour déterminer si vous souhaitez maintenir le crochet d'exécution, le modifier ou le supprimer.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **protection des données**.
3. Sélectionnez **snapshots** pour voir exécution de snapshots ou **sauvegardes** pour voir exécution de sauvegardes.

   L'état **Hook** indique l'état de la séquence de crochet d'exécution une fois l'opération terminée. Vous pouvez passer le curseur de la souris sur l'état pour plus de détails. Par exemple, si des échecs de crochet d'exécution se produisent au cours d'un snapshot, le fait de passer le curseur sur l'état de crochet pour ce snapshot donne une liste des crochets d'exécution ayant échoué. Pour voir les raisons de chaque échec, vous pouvez consulter la page **activité** dans la zone de navigation de gauche.

Afficher l'utilisation du script

Vous pouvez voir quels crochets d'exécution utilisent un script particulier dans l'interface utilisateur Web Astra Control.

Étapes

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

   La colonne **utilisé par** de la liste des scripts contient des détails sur les crochets qui utilisent chaque script de la liste.

3. Sélectionnez les informations de la colonne **utilisé par** pour un script qui vous intéresse.

   Une liste plus détaillée s'affiche, avec les noms des crochets qui utilisent le script et le type d'opération avec lesquels ils sont configurés pour s'exécuter.

Désactivez un crochet d'exécution

Vous pouvez désactiver un crochet d'exécution si vous souhaitez l'empêcher temporairement de s'exécuter avant ou après un instantané d'une application. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour désactiver les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez désactiver.
4. Sélectionnez **Désactiver**.

Supprimer un crochet d’exécution

Vous pouvez supprimer entièrement un crochet d’exécution si vous n’en avez plus besoin. Vous devez disposer d’autorisations propriétaire, administrateur ou membre pour supprimer les crochets d’exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d’une application gérée.
2. Sélectionnez l’onglet **crochets d’exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.

Exemples de crochet d’exécution

Utilisez les exemples suivants pour avoir une idée de la structure de vos crochets d’exécution. Vous pouvez utiliser ces crochets comme modèles ou comme scripts de test.

Exemple de réussite simple

Voici un exemple de crochet simple qui réussit et écrit un message sur une sortie standard et une erreur standard.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
```

```
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemple de réussite simple (version bash)

Voici un exemple de crochet simple qui réussit et écrit un message sur une sortie standard et une erreur standard, écrit pour bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
```

```
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemple de réussite simple (version zsh)

Voici un exemple de crochet simple qui réussit et écrit un message sur une sortie standard et une erreur standard, écrite pour le shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#
```

```
#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemple de réussite avec les arguments

L’exemple suivant montre comment utiliser des args dans un crochet.

```
#!/bin/sh
```

```
# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
```

```
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemple de crochet pré-instantané/post-instantané

L'exemple suivant montre comment le même script peut être utilisé à la fois pour un pré-snapshot et un crochet post-snapshot.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
```

```
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
```

```
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

Exemple de panne

L'exemple suivant montre comment vous pouvez gérer les défaillances d'un crochet.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
```

```
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Exemple détaillé d'échec

L'exemple suivant montre comment gérer les défaillances d'un crochet, avec une consignation plus détaillée.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
```

```
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
```

```
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

Échec avec un exemple de code de sortie

L'exemple suivant illustre l'échec d'un crochet avec un code de sortie.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
```

```
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Exemple de succès après échec

L'exemple suivant illustre l'échec d'un crochet lors de sa première exécution, mais la réussite après la seconde course.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

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 et les détails des clusters

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.

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.

Afficher l'état de santé et les détails d'une application

Après avoir commencé à gérer une application, Astra fournit des informations détaillées sur l'application qui vous permet d'identifier son état (qu'il s'agisse d'une application en bon état), son état de protection (qu'il soit entièrement protégé en cas de défaillance), les pods, le stockage persistant, et bien plus encore.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **applications**, puis le nom d'une application.
2. Trouvez les informations que vous recherchez :

   Statut de l'application

   Fournit un état qui reflète l'état de l'application dans Kubernetes. Par exemple, les pods et les volumes persistants sont-ils en ligne ? Si une application est défectueuse, vous devez chercher à résoudre le problème sur le cluster en consultant les journaux Kubernetes. Astra ne fournit pas d'informations pour vous aider à réparer une application défaillante.

   État de la protection des applications

   Fournit un 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

Vous permet de configurer une règle de protection des données et d'afficher les snapshots et les sauvegardes existants.

Stockage

Vous indique 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

Gérer les utilisateurs

Vous pouvez inviter, 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. À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra correspondant aux définitions LDAP. Voir "Authentification LDAP" pour en savoir plus.

Inviter des utilisateurs

Les propriétaires et administrateurs de comptes peuvent inviter de nouveaux utilisateurs à Astra Control Center.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.

3. Sélectionnez **inviter utilisateur**.
4. Entrez le nom et l'adresse e-mail de l'utilisateur.
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 rôles".

7. Sélectionnez **inviter des utilisateurs**.

   L'utilisateur reçoit un e-mail l'informant qu'il a été invité à Astra Control Center. L'e-mail inclut un mot de passe temporaire qu'il devra modifier lors de la première connexion.

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 rôles".

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**.

Modifier le rôle d'un utilisateur

Les utilisateurs ayant le rôle propriétaire peuvent modifier le rôle de tous les utilisateurs, tandis que les utilisateurs disposant du rôle Administrateur peuvent modifier le rôle des utilisateurs qui ont le rôle Administrateur, membre ou Visionneuse.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez la liste déroulante **actions**.

3. Sélectionnez **Modifier le rôle**.
4. Sélectionnez un nouveau rôle.
5. Pour appliquer des contraintes au rôle, activez la case à cocher **restreindre le rôle aux contraintes** et sélectionnez une contrainte dans la liste.

   S'il n'y a pas de contraintes, vous pouvez ajouter une contrainte. Pour plus d'informations, voir "Gérez les rôles".

6. Sélectionnez **confirmer**.

Résultat

Astra Control Center met à jour les autorisations de l'utilisateur en fonction du nouveau rôle que vous avez sélectionné.

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.

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"

Afficher et gérer les notifications

Astra vous avertit lorsque les actions sont terminées ou en échec. Par exemple, vous verrez une notification si une sauvegarde d'une application a réussi.

Vous pouvez gérer ces notifications en haut à droite de l'interface :

Étapes

1. Sélectionnez le nombre de notifications non lues en haut à droite.
2. Examinez les notifications, puis sélectionnez **Marquer comme lu** ou **Afficher toutes les notifications**.

   Si vous avez sélectionné **Afficher toutes les notifications**, la page Notifications se charge.

3. Sur la page **Notifications**, affichez les notifications, sélectionnez celles que vous souhaitez marquer comme lu, sélectionnez **action** et **Marquer comme lu**.

Ajouter et supprimer des informations d'identification

Ajoutez et supprimez des identifiants pour les fournisseurs de cloud privé local, comme ONTAP S3, les clusters Kubernetes gérés avec OpenShift ou les clusters Kubernetes non gérés depuis votre compte à tout moment. Astra Control Center utilise ces identifiants pour détecter les clusters Kubernetes et les applications sur les clusters et provisionner les ressources en votre nom.

Notez que tous les utilisateurs d'Astra Control Center partagent les mêmes informations d'identification.

Ajouter des informations d'identification

Vous pouvez ajouter des informations d'identification à Astra Control Center lorsque vous gérez des clusters. Pour ajouter des informations d'identification en ajoutant un nouveau cluster, reportez-vous à la section "Ajouter un cluster Kubernetes".

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

Supprimer les informations d'identification

Supprimez les informations d'identification d'un compte à tout moment. Vous ne devez supprimer les informations d'identification qu'après "annuler la gestion de tous les clusters associés".

> Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control Center est toujours utilisé car Astra Control Center utilise les informations d'identification pour s'authentifier auprès du compartiment de secours. Il est préférable de ne pas supprimer ces informations d'identification.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **informations d'identification**.
3. Sélectionnez le menu Options dans la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer les informations d'identification**.

Résultat

Astra Control Center supprime les informations d'identification du compte.

Surveillez l'activité des comptes

Vous pouvez consulter les détails des activités de votre compte Astra Control. Par exemple, lorsque de nouveaux utilisateurs ont été invités, lorsqu'un cluster a été ajouté ou lorsqu'un snapshot a été créé. Vous pouvez également exporter votre activité de compte vers un fichier CSV.

> Si vous gérez des clusters Kubernetes à partir d'Astra Control et qu'Astra Control est connecté à Cloud Insights, Astra Control envoie des journaux d'événements à Cloud Insights. Les informations du journal, y compris les informations sur le déploiement du pod et les pièces jointes en PVC, apparaissent dans le journal des activités de contrôle Astra. Utilisez ces informations pour identifier les problèmes éventuels sur les clusters Kubernetes que vous gérez.

Afficher toutes les activités du compte dans Astra Control

1. Sélectionnez **activité**.
2. Utilisez les filtres pour réduire la liste des activités ou utilisez la zone de recherche pour trouver exactement ce que vous recherchez.
3. Sélectionnez **Exporter au format CSV** pour télécharger l'activité de votre compte dans un fichier CSV.

Afficher l'activité d'un compte pour une application spécifique

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **activité**.

Afficher l'activité des comptes pour les clusters

1. Sélectionnez **clusters**, puis le nom du cluster.
2. Sélectionnez **activité**.

Prenez des mesures pour résoudre les événements qui nécessitent votre attention

1. Sélectionnez **activité**.
2. Sélectionnez un événement qui nécessite une attention particulière.
3. Sélectionnez l'option de liste déroulante **prendre une action**.

   Dans cette liste, vous pouvez consulter les actions correctives possibles, consulter la documentation associée au problème et obtenir de l'aide pour résoudre ce dernier.

Mettre à jour une licence existante

Vous pouvez convertir une licence d'évaluation en licence complète, ou mettre à jour une évaluation existante ou une licence complète avec une nouvelle licence. Si vous ne disposez pas d'une licence complète, contactez votre contact commercial NetApp pour obtenir une licence complète et un numéro de série. Vous pouvez utiliser l'interface utilisateur 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"

Gérer les connexions au référentiel

Vous pouvez connecter des référentiels à Astra Control afin de les utiliser comme référence pour les images d'installation de progiciels et les artefacts. Lorsque vous importez des logiciels, Astra Control fait référence aux images d'installation dans le référentiel d'images, les binaires et autres artefacts dans le référentiel d'artefacts.

Ce dont vous avez besoin

- Cluster Kubernetes avec Astra Control Center installé
- Un référentiel Docker en cours d'exécution auquel vous pouvez accéder
- Un référentiel d'artéfacts en cours d'exécution (comme Artifactory) auquel vous pouvez accéder

Connectez un référentiel d'images Docker

Vous pouvez connecter un référentiel d'images Docker pour contenir des images d'installation de package, telles que celles d'Astra Data Store. Lorsque vous installez des packages, Astra Control importe les fichiers d'image du package à partir du référentiel d'images.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **connexions**.
3. Dans la section **Docker image Repository**, sélectionnez le menu en haut à droite.
4. Sélectionnez **connexion**.
5. Ajoutez l'URL et le port du référentiel.
6. Saisissez les informations d'identification du référentiel.
7. Sélectionnez **connexion**.

Résultat

Le référentiel est connecté. Dans la section **Docker image Repository**, le référentiel doit afficher l'état connecté.

Déconnectez un référentiel d'images Docker

Vous pouvez supprimer la connexion à un référentiel d'images Docker s'il n'est plus nécessaire.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **connexions**.
3. Dans la section **Docker image Repository**, sélectionnez le menu en haut à droite.
4. Sélectionnez **déconnecter**.
5. Sélectionnez **Oui, déconnectez le référentiel d'images Docker**.

Résultat

Le référentiel est déconnecté. Dans la section **Docker image Repository**, le référentiel doit afficher un état déconnecté.

Connectez un référentiel d'artefacts

Vous pouvez connecter un référentiel d'artéfacts à des artefacts hôtes tels que les binaires du progiciel. Lorsque vous installez des packages, Astra Control importe les artefacts des packages logiciels à partir du référentiel d'images.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **connexions**.
3. Dans la section **dépôt d'artéfacts**, sélectionnez le menu en haut à droite.
4. Sélectionnez **connexion**.
5. Ajoutez l'URL et le port du référentiel.
6. Si une authentification est requise, activez la case à cocher **use Authentication** et entrez les informations d'identification du référentiel.
7. Sélectionnez **connexion**.

Résultat

Le référentiel est connecté. Dans la section **artefact Repository**, le référentiel doit afficher un état connecté.

Déconnectez un référentiel d'artefacts

Vous pouvez supprimer la connexion à un référentiel d'artefacts s'il n'est plus nécessaire.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **connexions**.
3. Dans la section **dépôt d'artéfacts**, sélectionnez le menu en haut à droite.
4. Sélectionnez **déconnecter**.
5. Sélectionnez **Oui, déconnectez le référentiel d'artefacts**.

Résultat

Le référentiel est déconnecté. Dans la section **artefact Repository**, le référentiel doit afficher un état connecté.

Trouvez plus d'informations

- "Gérer les packs logiciels"

Gérer les packs logiciels

NetApp propose des fonctionnalités supplémentaires pour Astra Control Center avec des packages logiciels que vous pouvez télécharger sur le site de support NetApp. Après avoir connecté Docker et les référentiels d'artéfacts, vous pouvez télécharger et importer des packages pour ajouter cette fonctionnalité à Astra Control Center. Vous pouvez utiliser l'interface CLI ou l'interface utilisateur Web Astra Control Center pour gérer les progiciels.

Ce dont vous avez besoin

- Cluster Kubernetes avec Astra Control Center installé
- Un référentiel d'images Docker connecté pour conserver les images du progiciel. Pour plus d'informations, voir "Gérer les connexions au référentiel".
- Un référentiel d'artéfacts connecté pour contenir les fichiers binaires et les artefacts du logiciel. Pour plus d'informations, voir "Gérer les connexions au référentiel".
- Un pack logiciel sur le site de support NetApp

Téléchargez des images de progiciels dans les référentiels

Astra Control Center référence les images de package et les artefacts dans les référentiels connectés. Vous pouvez télécharger des images et des artéfacts vers les référentiels à l'aide de l'interface de ligne de commande.

Étapes

1. Téléchargez le pack logiciel depuis le site de support NetApp et enregistrez-le sur une machine équipée du `kubectl` utilitaire installé.
2. Extrayez le fichier de package compressé et remplacez le répertoire par l'emplacement du fichier de bundle Astra Control (par exemple, `acc.manifest.yaml`).
3. Envoyez les images du package vers le référentiel Docker. Effectuer les substitutions suivantes :
   - Remplacez BUNDLE_FILE par le nom du fichier bundle Astra Control (par exemple, `acc.manifest.yaml`).
   - Remplacez MON_REGISTRE par l'URL du référentiel Docker.
   - Remplacez MON_REGISTRE_UTILISATEUR par le nom d'utilisateur.
   - Remplacez MON_REGISTRY_TOKEN par un jeton autorisé pour le Registre.

   ```
   kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
   MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
   ```

4. Si le package contient des artefacts, copiez les artefacts dans le référentiel d'artefacts. Remplacez BUNDLE_FILE par le nom du fichier de bundle Astra Control et NETWORK_LOCATION par l'emplacement du réseau pour copier les fichiers d'artefact vers :

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

Ajouter un pack logiciel

Vous pouvez importer des packages logiciels à l'aide d'un fichier bundle Astra Control Center. Cela permet d'installer le paquet et de mettre à disposition le logiciel pour Astra Control Center.

Ajoutez un logiciel à l'aide de l'interface utilisateur Web Astra Control

Vous pouvez utiliser l'interface utilisateur Web Astra Control Center pour ajouter un progiciel qui a été chargé dans les référentiels connectés.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **Forfaits**.
3. Sélectionnez le bouton **Ajouter**.
4. Dans la boîte de dialogue de sélection de fichier, sélectionnez l'icône de téléchargement.
5. Choisissez un fichier de pack Astra Control, dans `.yaml` format, pour charger.
6. Sélectionnez **Ajouter**.

Résultat

Si le fichier de bundle est valide et que les images de package et les artefacts se trouvent dans vos référentiels connectés, le package est ajouté à Astra Control Center. Lorsque l'état de la colonne **Status** devient **Available**, vous pouvez utiliser le package. Vous pouvez positionner le curseur de la souris sur l'état d'un pack pour obtenir plus d'informations.

> Si une ou plusieurs images ou artefacts d'un package sont introuvables dans votre référentiel, un message d'erreur s'affiche pour ce package.

Ajout d'un pack logiciel à l'aide de l'interface de ligne de commandes

Vous pouvez utiliser l'interface de ligne de commande pour importer un progiciel que vous avez téléchargé vers les référentiels connectés. Pour ce faire, vous devez d'abord enregistrer votre ID de compte Astra Control Center et un jeton API.

Étapes

1. À l'aide d'un navigateur Web, connectez-vous à l'interface utilisateur Web Astra Control Center.
2. Dans le Tableau de bord, sélectionnez l'icône utilisateur en haut à droite.
3. Sélectionnez **accès API**.
4. Notez l'ID du compte en haut de l'écran.
5. Sélectionnez **Generate API token**.
6. Dans la boîte de dialogue qui s'affiche, sélectionnez **Generate API token**.
7. Notez le jeton obtenu et sélectionnez **Fermer**. Dans l'interface de ligne de commande, passez aux répertoires à l'emplacement du `.yaml` fichier de bundle dans le contenu du pack extrait.
8. Importez le package à l'aide du fichier de regroupement, en procédant comme suit :
   - Remplacez BUNDLE_FILE par le nom du fichier bundle Astra Control.
   - Remplacez LE SERVEUR par le nom DNS de l'instance Astra Control.
   - Remplacez ACCOUNT_ID et TOKEN par l'ID de compte et le jeton API que vous avez enregistrés précédemment.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

Résultat

Si le fichier de bundle est valide et que les images de package et les artefacts se trouvent dans vos référentiels connectés, le package est ajouté à Astra Control Center.

> Si une ou plusieurs images ou artefacts d'un package sont introuvables dans votre référentiel, un message d'erreur s'affiche pour ce package.

Supprimer un pack logiciel

Vous pouvez utiliser l'interface utilisateur Web Astra Control Center pour supprimer un logiciel que vous avez précédemment importé dans Astra Control Center.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **Forfaits**.

   Vous pouvez voir la liste des packages installés et leur état sur cette page.

3. Dans la colonne **actions** du paquet, ouvrez le menu actions.
4. Sélectionnez **Supprimer**.

Résultat

Le package est supprimé d'Astra Control Center, mais les images et les artefacts du package restent dans vos référentiels.

Trouvez plus d'informations

- "Gérer les connexions au référentiel"

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 S3 génériques, Astra Control Center peut ne pas prendre en charge tous les fournisseurs de magasins d'objets qui affirment la prise en charge d'Amazon S3.

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
- Faire pivoter ou supprimer les identifiants de compartiment
- Déposer un godet

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

Modifier un godet

Vous pouvez modifier les informations d'identification d'accès pour un compartiment et modifier si un compartiment sélectionné est le compartiment par défaut.

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu Options 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**.

Faire pivoter ou supprimer les identifiants de compartiment

Astra Control utilise des identifiants de compartiment pour accéder à ce compartiment et fournit des clés secrètes pour le compartiment S3 afin qu'Astra Control Center puisse communiquer avec le compartiment.

Faire pivoter les identifiants du godet

Si vous faites pivoter les informations d'identification, faites-les pivoter pendant une fenêtre de maintenance lorsqu'aucune sauvegarde n'est en cours (planifiée ou à la demande).

Procédure de modification et de rotation des informations d'identification

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu Options de la colonne **actions**, sélectionnez **Modifier**.
3. Créer les nouvelles informations d'identification.
4. Sélectionnez **mettre à jour**.

Supprimer les identifiants du compartiment

Le retrait des identifiants de compartiment est uniquement possible si de nouvelles informations d'identification ont été appliquées à un compartiment ou si ce dernier n'est plus utilisé activement.

> Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control est toujours utilisé car Astra Control utilise les informations d'identification pour authentifier le compartiment de secours. Ne pas supprimer ces identifiants si le compartiment est en cours d'utilisation, car cela entraînera des défaillances de sauvegarde et des problèmes d'indisponibilité des sauvegardes.

> Si vous supprimez les identifiants de compartiment actifs, reportez-vous à la section "dépannage de la dépose des informations d'identification du godet".

Pour obtenir des instructions sur la suppression des informations d'identification S3 à l'aide de l'API de contrôle Astra, reportez-vous au "Informations sur l'automatisation et les API d'Astra".

Déposer un godet

Il est possible de retirer un godet qui n'est plus utilisé ou qui n'est pas en bon état. Pour simplifier et à jour la configuration du magasin d'objets,

> Vous ne pouvez pas supprimer un compartiment par défaut. Si vous souhaitez retirer ce compartiment, sélectionnez tout d'abord un autre compartiment comme valeur par défaut.

Ce dont vous avez besoin

- Avant de commencer, assurez-vous qu'aucune sauvegarde n'est en cours d'exécution ou terminée pour ce compartiment.
- Vérifiez que le godet n'est pas utilisé dans le cadre d'une politique de protection active.

Si c'est le cas, vous ne pourrez pas continuer.

Étapes

1. Dans la navigation à gauche, sélectionnez **seaux**.

2. Dans le menu **actions**, sélectionnez **Supprimer**.

> Astra Control veille à l'absence de règles de planification qui utilise le compartiment pour les sauvegardes et à l'absence de sauvegardes actives dans le compartiment.

3. Tapez « Supprimer » pour confirmer l'action.
4. Sélectionnez **Oui, retirez le godet**.

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"

Gérer le stockage back-end

La gestion des clusters de stockage d'Astra Control en tant que backend de stockage vous permet d'obtenir des liens entre les volumes persistants (PVS) et le back-end de stockage, ainsi que des metrics de stockage supplémentaires. Il est possible de surveiller la capacité du stockage et les informations concernant son état, y compris les performances si le centre de contrôle Astra est connecté à Cloud Insights.

Pour obtenir des instructions sur la gestion des systèmes back-end avec l'API Astra Control, consultez le "Informations sur l'automatisation et les API d'Astra".

Vous pouvez effectuer les tâches suivantes liées à la gestion d'un système back-end :

- "Ajout d'un système back-end"
- Afficher les détails du système back-end
- Annuler la gestion d'un système back-end
- Mettre à jour une licence backend de stockage de magasin de données Astra
- Mettez à niveau le système back-end de stockage de magasin de données Astra
- Retirer un système back-end
- Ajout de nœuds à un cluster back-end de stockage
- Retirer des nœuds d'un cluster back-end de stockage

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.

Sur la page Détails du système back-end de stockage, pour le magasin de données Astra, vous trouverez les informations suivantes :

- Cluster de magasin de données Astra
  - Débit, IOPS et latence
  - Capacité utilisée par rapport à la capacité totale
- Pour chaque volume de cluster de magasin de données Astra
  - Capacité utilisée par rapport à la capacité totale
  - Débit

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 la section Storage backend qui affiche l'état :
    - **Malsain**: Le stockage n'est pas dans un état optimal. Cela peut être dû à un problème de latence ou à une application dégradée en raison d'un problème de conteneur, par exemple.
    - **Tout en bonne santé**: Le stockage a été géré et est dans un état optimal.
    - **Découvert**: Le stockage a été découvert, mais pas géré par Astra Control.

Afficher les détails du système de stockage back-end à partir de l'option Backends

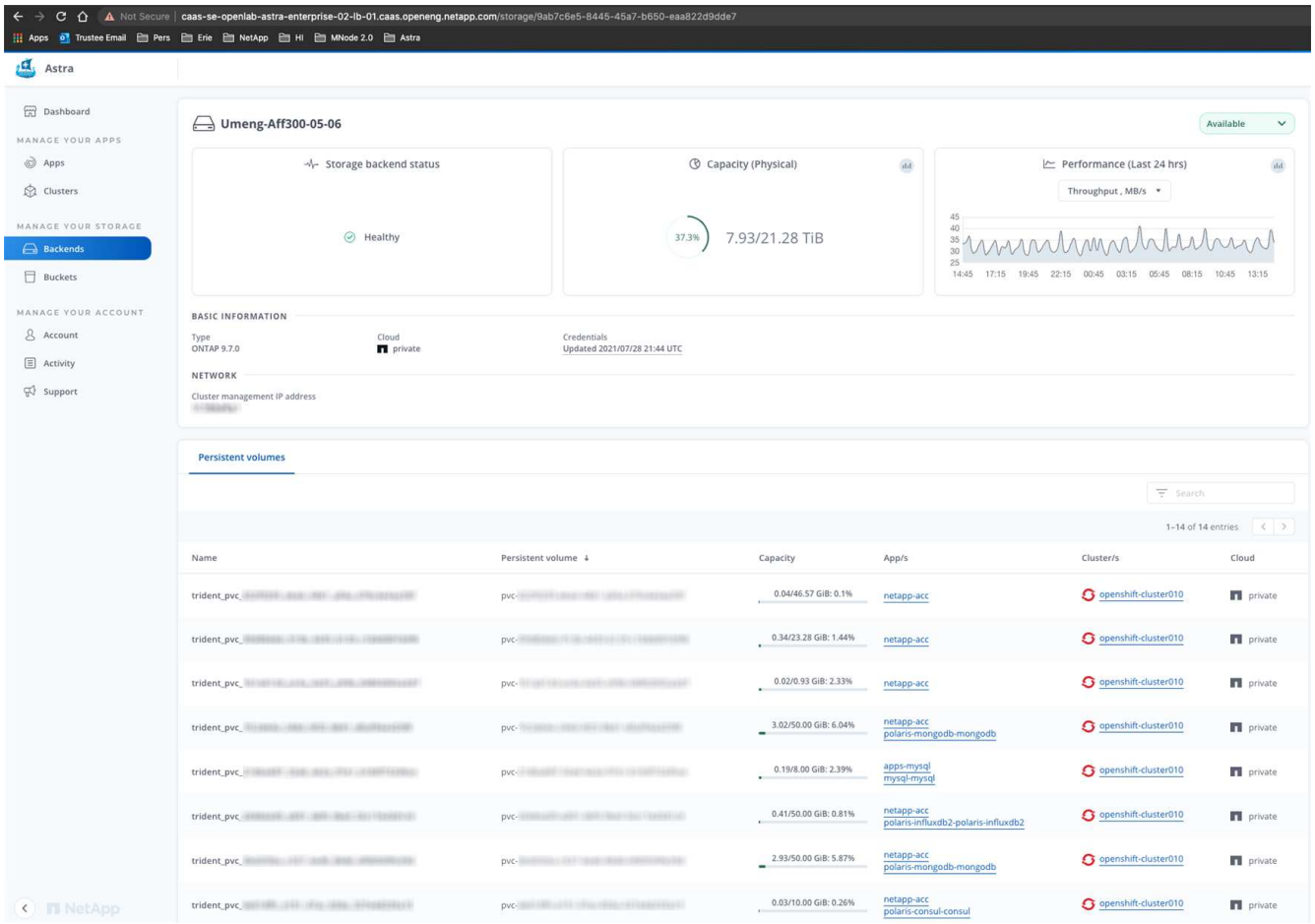
Affichez des informations sur l'état du système back-end, la capacité et les performances (débit et/ou latence des IOPS).

Vous pouvez voir les volumes utilisés par les applications Kubernetes, qui sont stockés sur un back-end de stockage sélectionné. Avec Cloud Insights, des informations supplémentaires s'affichent. Voir "Documentation Cloud Insights".

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.

> Si vous êtes connecté à NetApp Cloud Insights, des extraits de données de Cloud Insights s'affichent sur la page Backends.



3. Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Annuler la gestion d'un système back-end

Vous pouvez annuler la gestion du système back-end.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Unmanage**.
4. Saisissez « Unmanage » pour confirmer l'action.
5. Sélectionnez **Oui, annulez la gestion du stockage back-end**.

Retirer un système back-end

Vous pouvez supprimer un système back-end de stockage qui n'est plus utilisé. Pour que votre configuration reste simple et à jour, nous vous le souhaitons.

> Si vous supprimez un système back-end de magasin de données Astra, il ne doit pas avoir été créé par vCenter.

Ce dont vous avez besoin

- Assurez-vous que le système de stockage back-end n'est pas géré.
- Assurez-vous que le système back-end ne contient aucun volume associé au cluster de magasin de données Astra.

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**.

Mettre à jour une licence backend de stockage de magasin de données Astra

Vous pouvez mettre à jour la licence d'un système back-end de stockage en magasin de données Astra afin de prendre en charge un déploiement plus important ou des fonctionnalités améliorées.

Ce dont vous avez besoin

- Un système back-end de stockage de magasin de données Astra déployé et géré
- Fichier de licence Astra Data Store (contactez votre ingénieur commercial NetApp pour acheter une licence Astra Data Store)

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionner le nom d'un système back-end de stockage.
3. Sous **informations de base**, vous pouvez voir le type de licence installé.

   Si vous passez le curseur sur les informations de licence, une fenêtre contextuelle contenant plus d'informations, telles que l'expiration et les droits d'utilisation s'affiche.

4. Sous **Licence**, sélectionnez l'icône de modification en regard du nom de la licence.
5. Dans la page **mettre à jour la licence**, effectuez l'une des opérations suivantes :

État de la licence	Action
Au moins une licence a été ajoutée à Astra Data Store.	Sélectionnez une licence dans la liste.

État de la licence	Action
Aucune licence n'a été ajoutée à Astra Data Store.	a. Sélectionnez le bouton **Ajouter**. b. Sélectionnez un fichier de licence à télécharger. c. Sélectionnez **Ajouter** pour télécharger le fichier de licence.

6. Sélectionnez **mettre à jour**.

Mettez à niveau le système back-end de stockage de magasin de données Astra

Vous pouvez mettre à niveau votre magasin de données Astra depuis le centre de contrôle Astra. Pour ce faire, vous devez d'abord télécharger un forfait de mise à niveau. Astra Control Center utilisera ce kit de mise à niveau pour mettre à niveau Astra Data Store.

Ce dont vous avez besoin

- Système back-end géré de stockage de magasin de données Astra
- Un kit de mise à niveau Astra Data Store chargé (voir "Gérer les packs logiciels")

Étapes

1. Sélectionnez **Backends**.
2. Choisissez un back-end de stockage de données Astra dans la liste et sélectionnez le menu correspondant dans la colonne **actions**.
3. Sélectionnez **Upgrade**.
4. Sélectionnez une version de mise à niveau dans la liste.

   Si vous disposez de plusieurs packages de mise à niveau dans votre référentiel qui sont des versions différentes, vous pouvez ouvrir la liste déroulante pour sélectionner la version dont vous avez besoin.

5. Sélectionnez **Suivant**.
6. Sélectionnez **Démarrer la mise à niveau**.

Résultat

La page **Backends** affiche l'état **Upgrade** dans la colonne **Status** jusqu'à la fin de la mise à niveau.

Ajout de nœuds à un cluster back-end de stockage

Vous pouvez ajouter des nœuds à un cluster Astra Data Store, jusqu'au nombre de nœuds pris en charge par le type de licence installé pour Astra Data Store.

Ce dont vous avez besoin

- Système back-end de stockage de magasin de données Astra déployé et sous licence
- Vous avez ajouté le logiciel Astra Data Store dans Astra Control Center
- Un ou plusieurs nœuds à ajouter au cluster

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.

2. Sélectionner le nom d'un système back-end de stockage.
3. Sous informations de base, vous pouvez voir le nombre de nœuds dans ce cluster back-end de stockage.
4. Sous **noeuds**, sélectionnez l'icône de modification en regard du nombre de noeuds.
5. Dans la page **Ajouter des nœuds**, entrez les informations sur le ou les nouveaux nœuds :
   a. Attribuez un libellé de nœud à chaque nœud.
   b. Effectuez l'une des opérations suivantes :
      - Si vous souhaitez qu'Astra Data Store utilise toujours le nombre maximal de nœuds disponibles en fonction de votre licence, activez la case à cocher **toujours utiliser jusqu'au nombre maximum de nœuds autorisés**.
      - Si vous ne souhaitez pas qu'Astra Data Store utilise toujours le nombre maximal de nœuds disponibles, sélectionnez le nombre total de nœuds à utiliser.
   c. Si vous avez déployé Astra Data Store avec les domaines de protection activés, affectez le ou les nouveaux nœuds aux domaines de protection.
6. Sélectionnez **Suivant**.
7. Entrez l'adresse IP et les informations réseau pour chaque nouveau nœud. Entrez une adresse IP unique pour un nouveau nœud ou un pool d'adresses IP pour plusieurs nouveaux nœuds.

   Si le magasin de données Astra peut utiliser les adresses IP configurées pendant le déploiement, il n'est pas nécessaire de saisir des informations d'adresse IP.

8. Sélectionnez **Suivant**.
9. Vérifiez la configuration du ou des nouveaux nœuds.
10. Sélectionnez **Ajouter nœuds**.

Retirer des nœuds d'un cluster back-end de stockage

Vous pouvez supprimer des nœuds d'un cluster de magasin de données Astra. Ces nœuds peuvent être défectueux ou en état de fonctionnement.

Le retrait d'un nœud d'un cluster de magasin de données Astra déplace ses données vers d'autres nœuds du cluster et supprime le nœud du magasin de données Astra.

Le processus nécessite les conditions suivantes :

- L'espace disponible sur les autres nœuds doit être suffisant pour recevoir les données.
- Le cluster doit comporter au moins 4 nœuds.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionner le nom d'un système back-end de stockage.
3. Sélectionnez l'onglet **noeuds**.
4. Dans le menu actions, sélectionnez **Supprimer**.
5. Confirmez la suppression en entrant « supprimer ».
6. Sélectionnez **Oui, supprimer le noeud**.

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"

Surveillez l'infrastructure à l'aide de Cloud Insights et de connexions Fluentd

Vous pouvez configurer plusieurs paramètres en option pour améliorer votre expérience avec Astra Control Center. Pour contrôler et obtenir des informations sur l'ensemble de votre infrastructure, créez une connexion à NetApp Cloud Insights. Pour collecter des événements Kubernetes à partir de systèmes surveillés par Astra Control Center, ajoutez une connexion Fluentd.

Si le réseau sur lequel vous exécutez Astra Control Center requiert un proxy pour vous connecter à Internet (pour télécharger des bundles de support vers le site de support NetApp ou établir une connexion avec Cloud Insights), vous devez configurer un serveur proxy dans Astra Control Center.

Il est également possible de surveiller le débit interne du stockage de données Astra, les IOPS et la capacité du système de stockage back-end d'Astra Control Center. Voir "Gestion des systèmes back-end".

Ajoutez un serveur proxy pour les connexions à Cloud Insight ou au site de support NetApp

Si le réseau sur lequel vous exécutez Astra Control Center requiert un proxy pour vous connecter à Internet (pour télécharger des bundles de support vers le site de support NetApp ou établir une connexion avec Cloud Insights), vous devez configurer un serveur proxy dans 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 à d'autres connexions.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin**/**propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération.

Connectez-vous à Cloud Insights

Pour surveiller et obtenir des informations exploitables sur l'ensemble de votre infrastructure, connectez NetApp Cloud Insights à votre instance Astra Control Center. Cloud Insights est inclus dans votre licence Astra Control Center.

Cloud Insights doit être accessible à partir du réseau utilisé par Astra Control Center, ou indirectement via un serveur proxy.

Lorsque le centre de contrôle Astra est connecté à Cloud Insights, un pod d'unité d'acquisition est créé. Ce pod collecte les données des systèmes back-end gérés par Astra Control Center et les pousse dans Cloud Insights. Ce pod requiert 8 Go de RAM et 2 cœurs de CPU.

En outre, si vous gérez des clusters de magasin de données Astra avec un contrôleur Astra (qui est connecté à Cloud Insights), un pod d'unité d'acquisition est créé sur le magasin de données Astra pour chaque cluster de magasin de données Astra, et les mesures sont envoyées du magasin de données Astra vers le système Cloud Insights couplé. Chaque pod requiert 8 Go de RAM et 2 cœurs de CPU.

Après avoir activé la connexion Cloud Insights, vous pouvez afficher les informations de débit sur la page **Backends** et vous connecter à Cloud Insights à partir de là après avoir sélectionné un back-end de stockage. Vous trouverez également des informations sur le **Tableau de bord** dans la section Cluster et vous y connectez également à Cloud Insights.

Ce dont vous avez besoin

- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Licence Astra Control Center valide.
- Un serveur proxy si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour se connecter à Internet.

Si vous découvrez Cloud Insights, familiarisez-vous avec les fonctions et les fonctionnalités. Voir "Documentation Cloud Insights".

Étapes

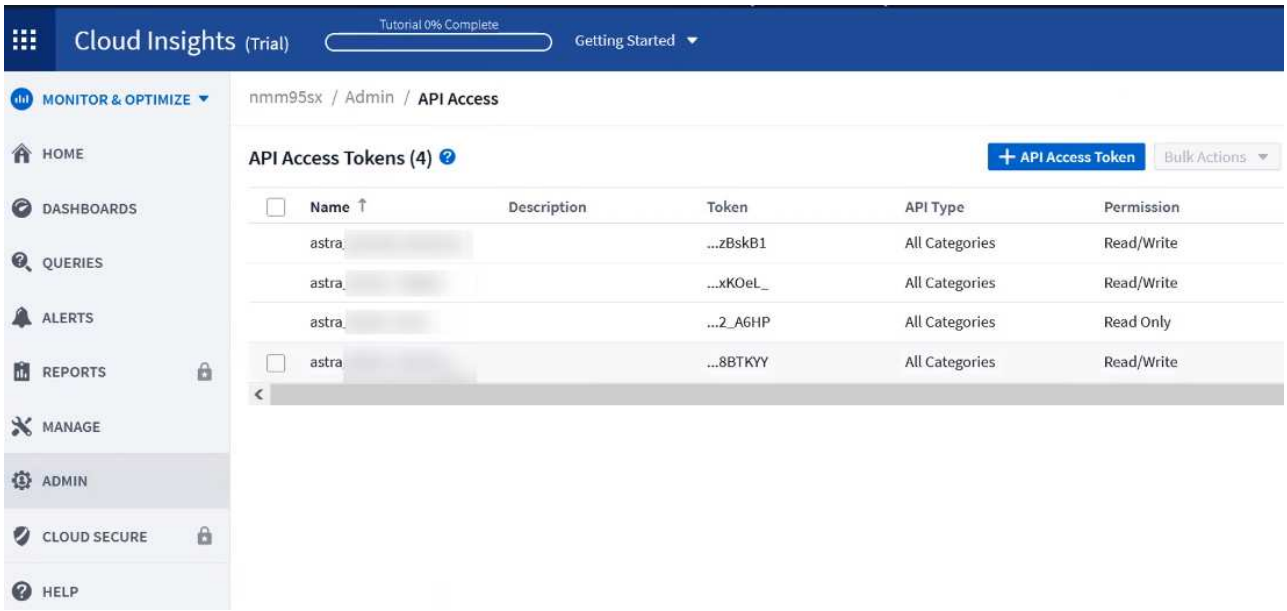
1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **Connect** où apparaît **déconnecté** dans la liste déroulante pour ajouter la connexion.

4. Entrez les jetons de l'API Cloud Insights et l'URL du locataire. L'URL du locataire a le format suivant, par exemple :

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Vous obtenez l'URL du locataire lorsque vous obtenez la licence Cloud Insights. Si vous ne disposez pas de l'URL du locataire, reportez-vous à la section "Documentation Cloud Insights".

a. Pour obtenir le "Jeton API", Connectez-vous à l'URL de votre locataire Cloud Insights.
b. Dans Cloud Insights, générez un jeton d'accès à l'API **lecture/écriture** et un jeton d'accès à l'API **lecture seule** en cliquant sur **Admin** > **API Access**.



c. Copiez la clé **lecture seule**. Vous devrez la coller dans la fenêtre du centre de contrôle Astra pour activer la connexion Cloud Insights. Pour les autorisations de clé de token d'accès à l'API de lecture, sélectionnez : actifs, alertes, unité d'acquisition et collecte de données.

d. Copiez la clé **lecture/écriture**. Vous devrez le coller dans la fenêtre Centre de contrôle Astra **connexion Cloud Insights**. Pour les autorisations de clés de token d'accès à l'API Read/Write, sélectionnez : Assets, Data ingestion, gestion des journaux, unité d'acquisition, Et collecte de données.

> Nous vous recommandons de générer une clé **lecture seule** et une clé **lecture/écriture**, et de ne pas utiliser la même clé à ces deux fins. Par défaut, la période d'expiration du token est définie sur un an. Nous vous recommandons de conserver la sélection par défaut pour donner au token la durée maximale avant son expiration. Si votre jeton expire, la télémétrie s'arrête.

e. Collez les clés que vous avez copiées de Cloud Insights dans le centre de contrôle Astra.

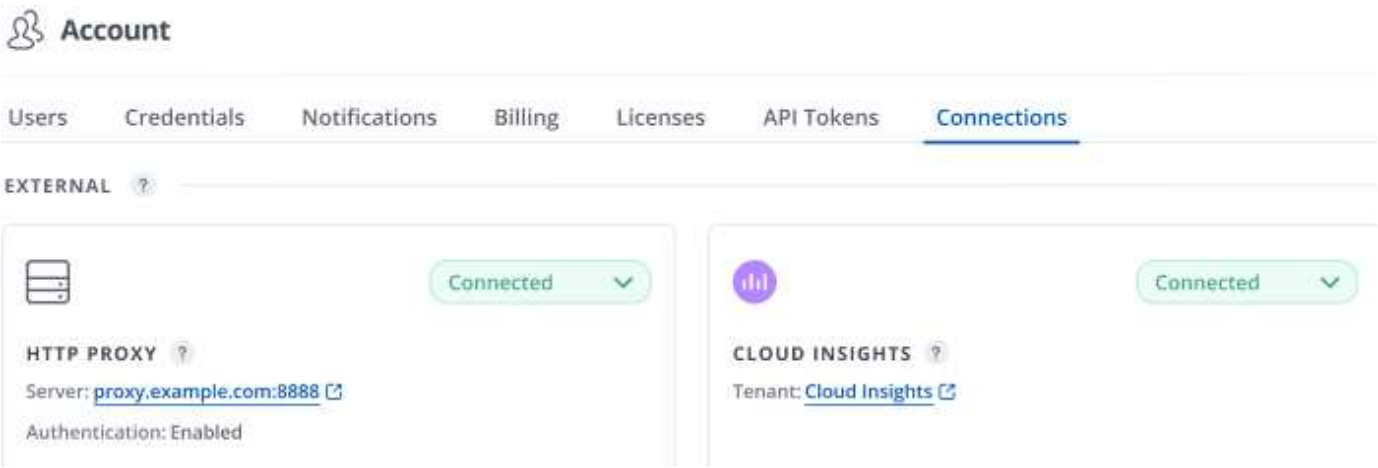
5. Sélectionnez **connexion**.

> Après avoir sélectionné **connexion,** l'état de la connexion devient **en attente** dans la section **Cloud Insights** de la page **compte** > **connexions**. Il peut y avoir quelques minutes pour que la connexion soit activée et que l'état passe à **Connected**.

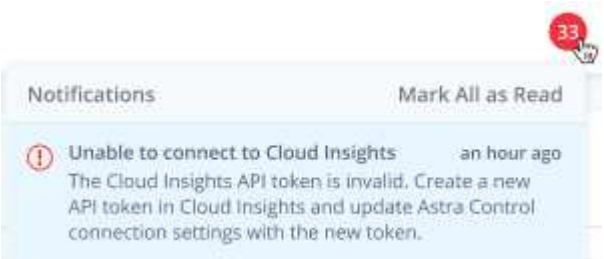
> Pour passer facilement entre le centre de contrôle Astra et les interfaces utilisateur Cloud Insights, assurez-vous d'être connecté aux deux.

Afficher les données dans Cloud Insights

Si la connexion a réussi, la section **Cloud Insights** de la page **compte** > **connexions** indique qu'elle est connectée et affiche l'URL du locataire. Vous pouvez accéder à Cloud Insights pour consulter les données reçues et affichées avec succès.

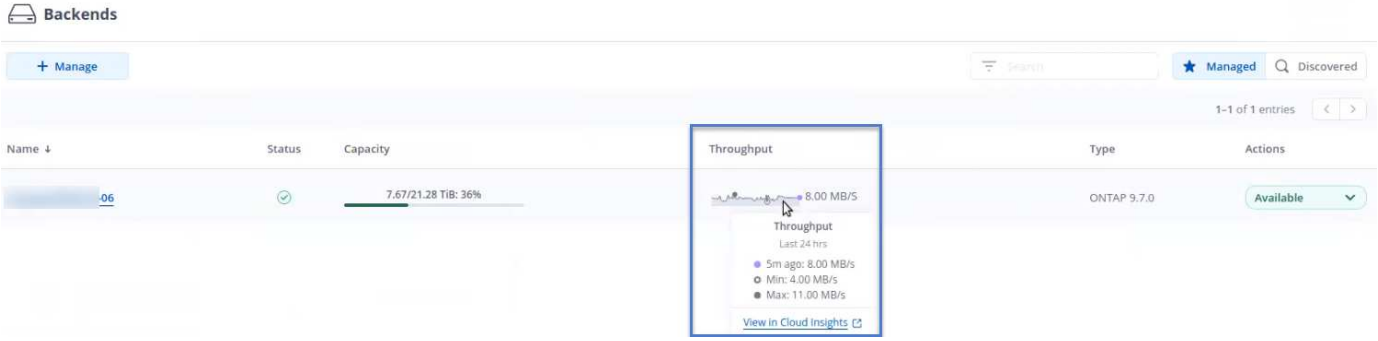


Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.



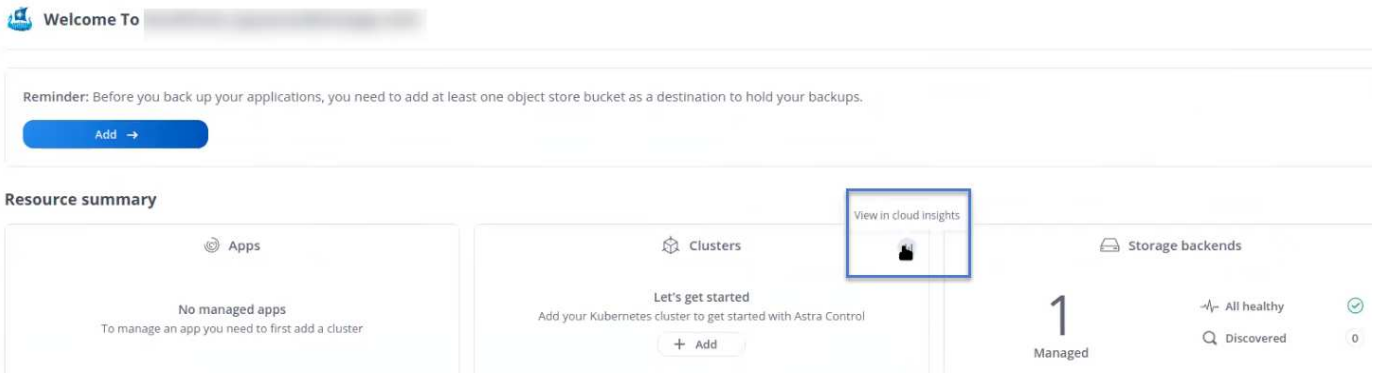
Vous pouvez également trouver les mêmes informations sous **compte** > **Notifications**.

À partir du Centre de contrôle Astra, vous pouvez afficher les informations sur le débit sur la page **Backends** et vous connecter à Cloud Insights à partir d'ici après avoir sélectionné un back-end de stockage.



Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Vous pouvez également trouver les informations sur le **Dashboard**.



Après l'activation de la connexion Cloud Insights, si vous supprimez les systèmes back-end ajoutés dans Astra Control Center, le système back-end cesse de créer des rapports avec Cloud Insights.

Modifier la connexion Cloud Insights

Vous pouvez modifier la connexion Cloud Insights.

Vous pouvez uniquement modifier les clés API. Pour modifier l'URL du locataire Cloud Insights, nous vous recommandons de déconnecter la connexion Cloud Insights et de vous connecter à la nouvelle URL.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les paramètres de connexion Cloud Insights.
5. Sélectionnez **Enregistrer**.

Désactiver la connexion Cloud Insights

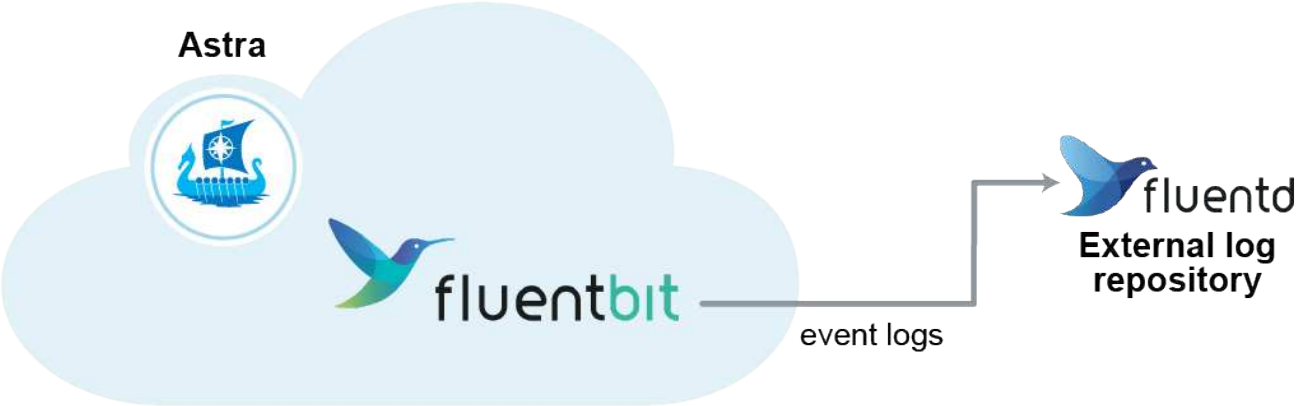
Vous pouvez désactiver la connexion Cloud Insights pour un cluster Kubernetes géré par Astra Control Center. La désactivation de la connexion Cloud Insights ne supprime pas les données de télémétrie déjà chargées sur Cloud Insights.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération. Après avoir confirmé l'opération, sur la page **compte** > **connexions**, l'état Cloud Insights devient **en attente**. Le changement d'état prend quelques minutes à **déconnecté**.

Connectez-vous à Fluentd

Vous pouvez envoyer des journaux (événements Kubernetes) depuis Astra Control Center vers votre terminal Fluentd. La connexion Fluentd est désactivée par défaut.



Seuls les journaux d'événements des clusters gérés sont transférés à Fluentd.

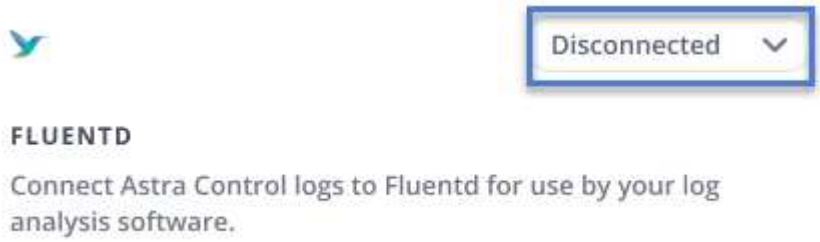
Ce dont vous avez besoin

- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Astra Control Center est installé et exécuté sur un cluster Kubernetes.

Astra Control Center ne valide pas les détails que vous entrez pour votre serveur Fluentd. Assurez-vous de saisir les valeurs correctes.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **Connect** dans la liste déroulante où apparaît **déconnecté** pour ajouter la connexion.



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.

- 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. Cochez la case correspondant aux applications que vous ne souhaitez plus gérer.
3. Dans le menu **action**, sélectionnez **Unmanage**.
4. Tapez « Unmanage » pour confirmer.
5. Confirmez que vous souhaitez annuler la gestion des applications, puis sélectionnez **Oui, annuler la gestion de l'application**.

Résultat

Astra Control Center cesse de gérer l'application.

Annuler la gestion d'un cluster

Dégérer le cluster que vous ne souhaitez plus gérer à partir d'Astra Control Center.

- Cette action empêche votre cluster d'être géré par Astra Control Center. Elle ne modifie pas la configuration du cluster et ne supprime pas le cluster.
- Trident ne sera pas désinstallé du cluster. "Découvrez comment désinstaller Trident".

> Avant d'annuler la gestion du cluster, vous devez annuler la gestion des applications associées au cluster.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **clusters**.
2. Cochez la case correspondant au groupe d'instruments que vous ne souhaitez plus gérer dans Astra Control Center.
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 passe à **Suppression** et le cluster sera supprimé de la page **clusters** et n'est plus géré par Astra Control Center.

> **Si le Centre de contrôle Astra et le Cloud Insights ne sont pas connectés**, la dégestion du cluster supprime toutes les ressources qui ont été installées pour envoyer des données de télémétrie. **Si le Centre de contrôle Astra et le Cloud Insights sont connectés**, la dégestion du cluster supprime uniquement le `fluentbit` et `event-exporter` pods.

Mettez à niveau Astra Control Center

Pour mettre à niveau Astra Control Center, téléchargez le pack d'installation depuis le site de support NetApp et suivez ces instructions pour mettre à niveau les composants d'Astra Control Center dans votre environnement. Vous pouvez utiliser cette procédure pour mettre à niveau Astra Control Center dans des environnements connectés à Internet ou à air comprimé.

Ce dont vous avez besoin

- "Avant de commencer la mise à niveau, assurez-vous que votre environnement satisfait aux exigences minimales relatives au déploiement d'Astra Control Center".
- S'assurer que tous les opérateurs du groupe d'instruments sont en état de fonctionnement et disponibles.

```
kubectl get clusteroperators
```

- Assurez-vous que tous les services API sont dans un état sain et disponibles.

```
kubectl get apiservices
```

- Déconnectez-vous de votre centre de contrôle Astra.

Description de la tâche

Le processus de mise à niveau d'Astra Control Center vous guide à travers les étapes de haut niveau suivantes :

- Téléchargez le pack Astra Control Center
- Déballez le bundle et modifiez le répertoire
- Ajoutez les images à votre registre local
- Poser le conducteur du centre de commande Astra mis à jour
- Mettez à niveau Astra Control Center
- Mise à niveau de services tiers (facultatif)
- Vérifiez l'état du système
- Configurer l'entrée pour l'équilibrage de charge

N'exécutez pas la commande suivante pendant l'intégralité du processus de mise à niveau pour éviter de supprimer toutes les pods Astra Control Center : `kubectl delete -f astra_control_center_operator_deploy.yaml`

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.

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

Téléchargez le pack Astra Control Center

1. Téléchargez le pack de mise à niveau Astra Control Center (`astra-control-center-[version].tar.gz`) Du site de support https:mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp^].
2. (Facultatif) utilisez la commande suivante pour vérifier la signature du pack :

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

Déballez le bundle et modifiez le répertoire

1. Extraire les images :

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

Ajoutez les images à votre registre local

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

Docker

1. Passez au répertoire Astra :

```
cd acc
```

2. placez les images du paquet dans le répertoire d'images Astra Control Center dans votre registre local. Exécutez les substitutions suivantes avant d'exécuter la commande :
   - Remplacez BUNDLE_FILE par le nom du fichier bundle Astra Control (par exemple, `acc.manifest.yaml`).
   - Remplacez MON_REGISTRE par l'URL du référentiel Docker.
   - Remplacez MON_REGISTRE_UTILISATEUR par le nom d'utilisateur.
   - Remplacez MON_REGISTRY_TOKEN par un jeton autorisé pour le Registre.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Connectez-vous à votre registre :

```
podman login [your_registry_path]
```

2. Exécutez le script suivant, en procédant à la substitution <YOUR_REGISTRY> comme indiqué dans les commentaires :

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Poser le conducteur du centre de commande Astra mis à jour

1. Modifier le répertoire :

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

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

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

d. Ajoutez les valeurs suivantes à la `env` section :

```
- name: ACCOP_HELM_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
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Installez le nouveau conducteur du centre de contrôle Astra :

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

Exemple de réponse :

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

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

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

Mettez à niveau Astra Control Center

1. Modifier la ressource personnalisée Astra Control Center (CR) (`astra_control_center_min.yaml`) Et modifiez la version Astra (`astraVersion` intérieur de `Spec`) numéro au plus tard :

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> Votre chemin de registre doit correspondre au chemin du registre où vous avez poussé les images dans un étape précédente.

2. Ajoutez les lignes suivantes dans `additionalValues` intérieur de `Spec` Dans le CR Astra Control Center :

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Effectuez l'une des opérations suivantes :
   a. Si vous n'avez pas votre propre IngresController ou entrée et que vous avez utilisé le Centre de contrôle Astra avec sa passerelle Trafik comme service de type LoadBalancer et que vous souhaitez poursuivre cette configuration, spécifiez un autre champ `ingressType` (s'il n'est pas déjà présent) et réglez-le sur `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Si vous voulez passer au déploiement d'entrée générique par défaut du centre de contrôle Astra, fournissez votre propre configuration d'entrée/contrôleur IngressController (avec terminaison TLS, etc.), ouvrez un itinéraire vers le centre de contrôle Astra, et définissez `ingressType` à `Generic`.

      ```
      ingressType: Generic
      ```

      Si vous omettez le champ, le processus devient le déploiement générique. Si vous ne voulez pas le déploiement générique, assurez-vous d'ajouter le champ.

4. (Facultatif) Vérifiez que les modules se terminent et deviennent disponibles à nouveau :

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

5. Attendez que les conditions d'état de l'Astra indiquent que la mise à niveau est terminée et prête :

   ```
   kubectl get -o yaml -n [netapp-acc or custom namespace]
   astracontrolcenters.astra.netapp.io astra
   ```

   Réponse :

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

6. Connectez-vous et vérifiez que tous les clusters et applications gérés sont toujours présents et protégés.
7. Si l'opérateur n'a pas mis à jour le Cert-Manager, mettez à niveau les services tiers, puis.

Mise à niveau de services tiers (facultatif)

Les services tiers Traefik et Cert-Manager ne sont pas mis à niveau au cours des étapes de mise à niveau précédentes. Vous pouvez éventuellement les mettre à niveau à l'aide de la procédure décrite ici ou conserver les versions de service existantes si votre système l'exige.

- **Traefik**: Par défaut, Astra Control Center gère le cycle de vie du déploiement Traefik. Réglage `externalTraefik` à `false` (Valeur par défaut) indique qu'aucun Traefik externe n'existe dans le système et que Traefik est installé et géré par Astra Control Center. Dans ce cas, `externalTraefik` est défini sur `false`.

  D'autre part, si vous avez votre propre déploiement Trafik, définissez `externalTraefik` à `true`. Dans ce cas, vous entretenez le déploiement et Astra Control Center ne mettra pas à niveau les CRD, sauf si `shouldUpgrade` est défini sur `true`.

- **Cert-Manager**: Par défaut, Astra Control Center installe le cert-Manager (et les CRD) sauf si vous avez défini `externalCertManager` à `true`. Réglez `shouldUpgrade` à `true` Pour mettre à niveau les CRD d'Astra Control Center.

Traefik est mis à niveau si l'une des conditions suivantes est remplie :

- ExternalTraefik : faux
- ExternalTraefik: Vrai ET shouldUpgrade: Vrai.

Étapes

1. Modifiez le `acc` CR :

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

2. Modifiez le `externalTraefik` et le `shouldUpgrade` pour l'un ou l'autre `true` ou `false` au besoin.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

Vérifiez l'état du système

1. Connectez-vous à Astra Control Center.
2. Vérifiez que tous vos clusters et applications gérés sont toujours présents et protégés.

Configurer l'entrée pour l'équilibrage de charge

Vous pouvez configurer un objet d'entrée Kubernetes qui gère l'accès externe aux services, comme l'équilibrage de charge dans un cluster.

- La mise à niveau par défaut utilise le déploiement d'entrée générique. Dans ce cas, vous devrez également configurer un contrôleur d'entrée ou une ressource d'entrée.
- Si vous ne voulez pas un contrôleur d'entrée et voulez conserver ce que vous avez déjà, définissez `ingressType` à `AccTraefik`.

> Pour plus de détails sur le type de service « LoadBalancer » et l'entrée, voir "De formation".

Les étapes diffèrent en fonction du type de contrôleur d'entrée utilisé :

- Contrôleur d'entrée Nginx
- Contrôleur d'entrée OpenShift

Ce dont vous avez besoin

- Dans la spécification CR,
  - Si `crd.externalTraefik` est présent, il doit être réglé sur `false` OU
  - Si `crd.externalTraefik` est `true`, `crd.shouldUpgrade` devrait également être `true`.
- Le requis "contrôleur d'entrée" doit déjà être déployé.
- Le "classe d'entrée" correspondant au contrôleur d'entrée doit déjà être créé.
- Vous utilisez des versions Kubernetes entre et comprenant v1.19 et v1.21.

Étapes du contrôleur d'entrée Nginx

1. Utilisez le secret existant `secure-testing-cert` ou créez 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 espace de noms personnalisés) pour un schéma obsolète ou un nouveau schéma :
   a. Pour un schéma obsolète, suivez cet exemple :

```
apiVersion: extensions/v1beta1
kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Pour un nouveau schéma, suivez 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
```

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
```

Vérifiez la configuration de l'entrée

Vous pouvez vérifier la configuration de l'entrée avant de continuer.

1. Assurez-vous que Traefik a changé en `clusterIP` De l'équilibreur de charge :

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

2. Vérifier les itinéraires dans Traefik :

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

Le résultat doit être vide.

Désinstaller Astra Control Center

Vous devrez peut-être retirer les composants du centre de contrôle Astra si vous effectuez une mise à niveau d'un essai vers une version complète du produit. Pour déposer le centre de commande Astra et le conducteur du centre de commande Astra, exécuter les commandes décrites dans cette procédure dans l'ordre.

Si vous rencontrez des problèmes avec la désinstallation, reportez-vous à la section Dépannage des problèmes de désinstallation.

Ce dont vous avez besoin

- Utilisez l'interface utilisateur d'Astra Control Center pour tout supprimer "clusters".

Étapes

1. Supprimer Astra Control Center. L'exemple de commande suivant est basé sur une installation par défaut. Modifiez la commande si vous avez créé des configurations personnalisées.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Résultat :

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utiliser la commande suivante pour supprimer le `netapp-acc` espace de noms :

   ```
   kubectl delete ns netapp-acc
   ```

   Résultat :

   ```
   namespace "netapp-acc" deleted
   ```

3. Utiliser la commande suivante pour supprimer les composants du système de l'opérateur Astra Control Center :

   ```
   kubectl delete -f astra_control_center_operator_deploy.yaml
   ```

Résultat :

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

Dépannage des problèmes de désinstallation

Utilisez les solutions de contournement suivantes pour résoudre les problèmes que vous rencontrez lors de la désinstallation d'Astra Control Center.

La désinstallation d'Astra Control Center ne parvient pas à nettoyer le module de l'opérateur de surveillance sur le cluster géré

Si vous n'avez pas dégéré les clusters avant de désinstaller Astra Control Center, vous pouvez supprimer manuellement les pods dans l'espace de noms netapp-Monitoring et dans l'espace de noms à l'aide des commandes suivantes :

Étapes

1. Supprimer `acc-monitoring` agent :

   ```
   kubectl delete agents acc-monitoring -n netapp-monitoring
   ```

   Résultat :

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Supprimez le namespace :

   ```
   kubectl delete ns netapp-monitoring
   ```

Résultat :

```
namespace "netapp-monitoring" deleted
```

3. Confirmer la suppression des ressources :

```
kubectl get pods -n netapp-monitoring
```

Résultat :

```
No resources found in netapp-monitoring namespace.
```

4. Confirmer la suppression de l'agent de surveillance :

```
kubectl get crd|grep agent
```

Résultat de l'échantillon :

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Supprimer les informations de définition de ressource personnalisée (CRD) :

```
kubectl delete crds agents.monitoring.netapp.com
```

Résultat :

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La désinstallation d'Astra Control Center ne parvient pas à nettoyer les CRD Traefik

Vous pouvez supprimer manuellement les CRD Traefik. Les CRDS sont des ressources globales, et leur suppression peut avoir un impact sur d'autres applications du cluster.

Étapes

1. Lister les CRD Traefik installés sur le cluster :

```
kubectl get crds |grep -E 'traefik'
```

Réponse

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
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"

Automatisez avec les API REST

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 ou l’API Astra Control.

Pour en savoir plus, consultez le "Documentation sur l’automatisation d’Astra".

Connaissances et support

Dépannage

Apprenez à contourner certains problèmes courants que vous pourriez rencontrer.

"Base de connaissances NetApp pour Astra"

Trouvez plus d'informations

- "Comment télécharger un fichier vers NetApp (connexion requise)"
- "Comment télécharger manuellement un fichier vers NetApp (connexion requise)"

Obtenez de l'aide

NetApp prend en charge Astra Control de plusieurs façons. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un canal 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 :

- "**Base de connaissances** (connexion requise)": Recherchez des articles, des FAQ, ou des renseignements sur les réparations en rapport avec Astra Control.
- **Centre de documentation**: C'est le site de documentation que vous consultez actuellement.
- "**Obtenir de l'aide par 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 CRD (Custom Resource Definition) Astra Control Center (`astra_control_center_min.yaml`), les offres de support quotidien sont automatiquement téléchargées sur le "Site de support NetApp".

Générez un bundle de support à fournir au support NetApp

Avec le centre de contrôle Astra, l'utilisateur administratif peut générer des bundles qui incluent des informations utiles pour le support NetApp, y compris des journaux, des événements pour tous les composants du déploiement Astra, des mesures et des informations de topologie sur les clusters et les applications sous gestion. Si vous êtes connecté à Internet, vous pouvez télécharger des packs de support sur le site de support NetApp (NSS) directement à partir de l'interface utilisateur du centre de contrôle Astra.

> Le temps passé par Astra Control Center à générer le pack dépend de la taille de votre installation Astra Control Center ainsi que des paramètres du pack de support demandé. La durée spécifiée lors de la demande d'un bundle de support détermine le temps nécessaire à la génération du bundle (par exemple, une période de temps plus courte entraîne une génération plus rapide du bundle).

Avant de commencer

Déterminez si une connexion proxy sera nécessaire pour télécharger des packs sur NSS. Si une connexion proxy est nécessaire, vérifiez que le centre de contrôle Astra a été configuré pour utiliser un serveur proxy.

1. Sélectionnez **comptes** > **connexions**.
2. Vérifiez les paramètres du proxy dans **Paramètres de connexion**.

Étapes

1. Créez un dossier sur le portail NSS à l'aide du numéro de série de licence indiqué sur la page **support** de l'interface utilisateur du Centre de contrôle Astra.
2. Procédez comme suit pour générer le pack de support à l'aide de l'interface utilisateur du centre de contrôle Astra :
   a. Sur la page **support**, dans la mosaïque support bundle, sélectionnez **generate**.
   b. Dans la fenêtre **Generate a support Bundle**, sélectionnez le délai.

      Vous avez le choix entre des délais rapides ou personnalisés.

      > Vous pouvez choisir une plage de dates personnalisée et spécifier une période d'heure personnalisée pendant la plage de dates.

   c. Après avoir effectué les sélections, sélectionnez **confirmer**.
   d. Cochez la case **Upload le bundle vers le site de support NetApp when Generated**.
   e. Sélectionnez **générer un bundle**.

      Lorsque le bundle de support est prêt, une notification apparaît sur la page **comptes** > **notification** dans la zone alertes, sur la page **activité**, et également dans la liste des notifications (accessible en sélectionnant l'icône dans le coin supérieur droit de l'interface utilisateur).

Si la génération a échoué, une icône apparaît sur la page générer un bundle. Sélectionnez l'icône pour afficher le message.

> L'icône de notifications en haut à droite de l'interface utilisateur fournit des informations sur les événements liés au bundle de support, comme lorsque le bundle est correctement créé, lorsque la création du bundle échoue, lorsque le bundle n'a pas pu être téléchargé, lorsque le bundle n'a pas pu être téléchargé, etc.

Si vous avez une installation pneumatique

Si vous disposez d'une installation pneumatique, effectuez les opérations suivantes après la génération du pack support. Lorsque le bundle est disponible au téléchargement, l'icône Télécharger apparaît en regard de **generate** dans la section **support Bundles** de la page **support**.

Étapes

1. Sélectionnez l'icône Télécharger pour télécharger le pack localement.
2. Téléchargez manuellement le bundle sur NSS.

   Pour ce faire, vous pouvez utiliser l'une des méthodes suivantes :

   - Utiliser "Téléchargement de fichiers authentifiés NetApp (connexion requise)".
   - Joignez le pack au dossier directement sur NSS.
   - Faites confiance à NetApp Active IQ.

Trouvez plus d'informations

- "Comment télécharger un fichier vers NetApp (connexion requise)"
- "Comment télécharger manuellement un fichier vers NetApp (connexion requise)"

Versions antérieures de la documentation Astra Control Center

La documentation relative aux versions précédentes est disponible.

- "Documentation Astra Control Center 22.04"
- "Documentation Astra Control Center 21.12"
- "Documentation Astra Control Center 21.08"

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

"https://www.netapp.com/company/legal/copyright/"

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"
- "Avis concernant le magasin de données Astra"

Licence API Astra Control

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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