



Utilisez Astra

Astra Control Center

NetApp
November 21, 2023

Sommaire

- Utilisez Astra 1
 - Gérer des applications 1
 - Protégez vos applications 7
 - Afficher l'état des applications et des clusters 30
 - Gérez votre compte 33
 - Gestion des compartiments 44
 - Gérer le stockage back-end 46
 - Contrôle et protection de l'infrastructure 51
 - Annuler la gestion des applications et des clusters 58
 - Mettez à niveau Astra Control Center 59
 - Désinstaller Astra Control Center 70

Utilisez Astra

Gérer des applications

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

Notez qu'Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture de "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.



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.

Installez les applications sur votre cluster

Maintenant que vous avez ajouté votre cluster à Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application étendue à un espace de noms peut être gérée. Une fois les pods en ligne, vous pouvez gérer l'application avec Astra Control.

Pour obtenir de l'aide sur le déploiement des applications validées à partir des graphiques Helm, consultez les éléments suivants :

- ["Déployer des bases de données MariaDB à partir d'un graphique Helm"](#)
- ["Déployer MySQL à partir d'un graphique Helm"](#)
- ["Déploiement de Postgres à partir d'un graphique Helm"](#)
- ["Déployez Jenkins à partir d'un graphique Helm"](#)

Gérer des applications

Astra Control vous permet de gérer vos applications au niveau de l'espace de noms ou du label Kubernetes.



Les applications installées avec Helm 2 ne sont pas prises en charge.

Vous pouvez effectuer les opérations suivantes pour gérer les applications :

- Gérer des applications
 - [Gérer les applications par espace de noms](#)
 - [Gérer les applications par étiquette Kubernetes](#)
- [Ignorer les applications](#)
- [Annuler la gestion des applications](#)



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. Pour afficher les applications système, utilisez le filtre "Afficher les applications 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"](#).



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 applications par espace de noms

La section **découverts** de la page Apps affiche les espaces de noms et toutes les applications installées par Helm ou les applications étiquetées sur mesure dans ces espaces de noms. Vous pouvez choisir de gérer chaque application individuellement ou au niveau de l'espace de noms. La granularité est en effet au niveau de granularité requis pour les opérations de protection des données.

Par exemple, vous pouvez définir une stratégie de sauvegarde pour « maria » qui a une cadence 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 un espace de noms unique.

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.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez le filtre **découvert**.



3. Afficher la liste des espaces de noms découverts. Développez l'espace de noms pour afficher les applications et les ressources associées.

Astra Control présente les applications Helm et les applications étiquetées sur mesure dans l'espace de noms. Si des étiquettes Helm sont disponibles, elles sont désignées par une icône de balise.

4. Consultez la colonne **Groupe** pour voir dans quel espace de noms l'application s'exécute (elle est désignée par l'icône du dossier).
5. Décidez si vous souhaitez gérer chaque application individuellement ou au niveau de l'espace de noms.
6. Recherchez l'application souhaitée dans la hiérarchie et sélectionnez **gérer** dans le menu Options de la colonne **actions**.
7. Si vous ne souhaitez pas gérer une application, sélectionnez **Ignorer** dans le menu Options de la colonne **actions**.

Par exemple, si vous souhaitez gérer ensemble toutes les applications sous l'espace de noms « maria » afin qu'elles aient les mêmes stratégies de snapshot et de sauvegarde, vous devez gérer l'espace de noms et ignorer les applications dans l'espace de noms.

8. Pour afficher la liste des applications gérées, sélectionnez **Managed** comme filtre d'affichage.



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.

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

Résultat

Les applications que vous avez choisi de gérer sont désormais disponibles dans l'onglet **Managed**. Toutes les applications ignorées seront transférées vers l'onglet **ignoré**. Idéalement, l'onglet découvert affiche zéro application, de sorte qu'à mesure que de nouvelles applications sont installées, elles sont plus faciles à trouver et à gérer.

Gérer les applications par étiquette Kubernetes

Astra Control inclut une action en haut de la page applications nommée **define Custom app**. Vous pouvez utiliser cette action pour gérer les applications identifiées avec une étiquette Kubernetes. ["En savoir plus sur la définition d'applications personnalisées par Kubernetes label"](#).

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **définir**.

3. Dans la boîte de dialogue **Define Custom application**, indiquez les informations requises pour gérer l'application :

- a. **Nouvelle application** : saisissez le nom d'affichage de l'application.
- b. **Cluster** : sélectionnez le cluster où réside l'application.
- c. **Espace de noms** : sélectionnez l'espace de noms de l'application.
- d. **Label**: Entrez un libellé ou sélectionnez un libellé parmi les ressources ci-dessous.
- e. **Ressources sélectionnées** : affichez et gérez les ressources Kubernetes sélectionnées que vous souhaitez protéger (pods, secrets, volumes persistants, etc.).
 - Affichez les étiquettes disponibles en développant une ressource et en sélectionnant le nombre d'étiquettes.
 - Sélectionnez l'un des libellés.

Une fois que vous avez choisi un libellé, celui-ci s'affiche dans le champ **Label**. Astra Control met également à jour la section **Ressources non sélectionnées** pour afficher les ressources qui ne correspondent pas à l'étiquette sélectionnée.

- f. **Ressources non sélectionnées** : vérifiez les ressources de l'application que vous ne voulez pas protéger.

4. Sélectionnez **définir l'application personnalisée**.

Résultat

Astra Control permet de gérer l'application. Vous pouvez maintenant le trouver dans l'onglet **Managed**.

Ignorer les applications

Si une application a été découverte, elle apparaît dans la liste découverte. Dans ce cas, vous pouvez nettoyer la liste découverte afin que les nouvelles applications qui viennent d'être installées soient plus faciles à trouver. Vous pouvez aussi avoir des applications que vous gérez et décider par la suite que vous ne souhaitez plus les gérer. Si vous ne souhaitez pas gérer ces applications, vous pouvez indiquer qu'elles doivent être ignorées.

Par ailleurs, vous pouvez avoir besoin de gérer les applications sous un seul espace de noms (géré par un espace de noms). Vous pouvez ignorer les applications que vous souhaitez exclure de l'espace de noms.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **découvert** comme filtre.
3. Sélectionnez l'application.
4. Dans le menu Options de la colonne **actions**, sélectionnez **Ignorer**.
5. Pour annuler l'ignorer, sélectionnez **Unignore**.

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.

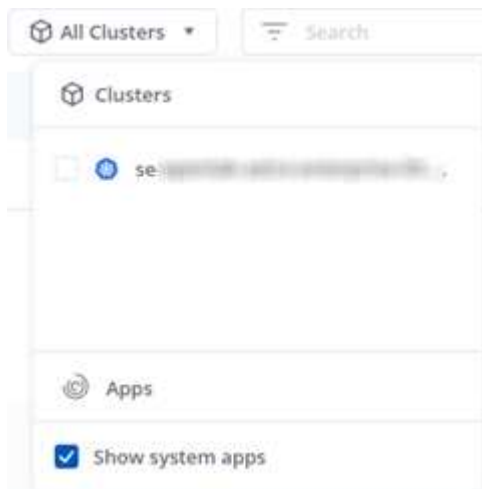
Étapes

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

Qu'en est-il des applications système ?

Astra Control détecte également les applications système qui s'exécutent sur un cluster Kubernetes. Nous ne vous montrons pas par défaut ces applications système car il est rare que vous ayez besoin de les sauvegarder.

Vous pouvez afficher les applications système à partir de la page applications en cochant la case **Afficher les applications système** sous le filtre clusters dans la barre d'outils.



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.

Trouvez plus d'informations

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

Définir un exemple d'application personnalisée

La création d'une application personnalisée vous permet de regrouper des éléments de votre cluster Kubernetes dans une seule application. Cette collection de ressources Kubernetes est basée sur un namespace et une étiquette.

Une application personnalisée vous offre un contrôle plus granulaire sur les éléments à inclure dans une opération Astra Control, notamment :

- Clonage
- Snapshot
- Sauvegarde
- Règle de protection

Dans la plupart des cas, vous voudrez utiliser les fonctions d'Astra Control sur l'ensemble de votre application. Toutefois, vous pouvez également créer une application personnalisée pour utiliser ces fonctionnalités par les étiquettes que vous attribuez aux objets Kubernetes dans un espace de noms.



Les applications personnalisées ne peuvent être créées qu'au sein d'un espace de nom spécifié sur un même cluster. Astra Control ne prend pas en charge la capacité d'une application personnalisée à s'étendre sur plusieurs espaces de noms ou clusters.

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](#)".



Le chevauchement de stratégies pour la même ressource sous des noms différents peut entraîner des conflits de données. Si vous créez une application personnalisée pour une ressource, assurez-vous qu'elle n'est pas en cours de clonage ou de sauvegarde dans le cadre d'autres stratégies.

Ce dont vous avez besoin

- Un groupe d'instruments est ajouté à Astra Control

Étapes

1. Sur la page applications, sélectionnez **+ définir**.

La fenêtre Custom App indique quelles ressources seront incluses ou exclues de votre application personnalisée. Cela vous permet de vous assurer que vous choisissez les critères appropriés pour définir votre application personnalisée.

2. Dans la fenêtre contextuelle, entrez le nom de l'application, choisissez le cluster dans la liste déroulante **Cluster** et choisissez l'espace de noms de l'application dans la liste déroulante **namespace**.
3. Dans la liste déroulante **Label**, sélectionnez un libellé pour les applications et l'espace de noms.
4. Après avoir défini l'application personnalisée pour un déploiement, répétez le processus pour les autres déploiements, selon les besoins.

Lorsque vous avez terminé de créer les deux applications personnalisées, vous pouvez traiter ces ressources comme n'importe quelle autre application Astra Control. Ils peuvent les cloner, créer des sauvegardes et des snapshots et créer une règle de protection personnalisée pour chaque groupe de ressources en fonction des étiquettes Kubernetes.

Exemple : politique de protection distincte pour différentes versions

Dans cet exemple, l'équipe devops gère un déploiement canary Release. Leur cluster 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 personnalisées: Une pour la libération "canary", et une pour la version "stable". Les sauvegardes, snapshots et opérations de clonage sont donc séparés pour les deux groupes d'objets Kubernetes.

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"](#).

Workflow de protection des applications

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

[Une seule] Sauvegardez toutes les 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] Facultatif : ajustez 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] En cas d'incident, restaurez vos applications

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).

Protéger les applications avec les snapshots et les sauvegardes

Protégez vos 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
```

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.

Configure protection policy
STEP 1/2: DETAILS
✕

PROTECTION SCHEDULE

Hourly ✕

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

Daily ✕

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

Weekly ✕

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

Monthly ✕

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

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

Select Weekday(s) (optional)

Monday X

Time (UTC) (optional)

02:00

− Snapshots to keep +

26

− Backups to keep +

0

BACKUP DESTINATION

Bucket

ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10 Default

OVERVIEW

Schedule and retention

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

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

Read more in [Protection policies](#)

- Application
cattle-logging
- Namespace
cattle-logging
- Cluster
se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel

Review
→

5. Sélectionnez **Revue**.

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

Résultat

Astra Control 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.

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.

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](#)".

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.

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 un script personnalisé que vous pouvez exécuter avant ou après un instantané 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.

Crochets d'exécution par défaut et expressions régulières

Pour certaines applications, Astra Control est doté de crochets d'exécution par défaut fournis par NetApp qui gèrent les opérations de gel et de dégel avant et après les snapshots. Astra Control utilise des expressions régulières pour faire correspondre l'image de conteneur d'une application à ces applications :

- MariaDB

- Expression régulière correspondante : `\bmariadb\b`
- MySQL
 - Expression régulière correspondante : `\bmysql\b`
- PostgreSQL
 - Expression régulière correspondante : `\bpostgres\b`

S'il y a une correspondance, les crochets d'exécution par défaut fournis par NetApp pour cette application apparaissent dans la liste des crochets d'exécution actifs de l'application, et ces crochets s'exécutent automatiquement lorsque des instantanés de cette application sont effectués. Si l'une de vos applications personnalisées possède un nom d'image similaire qui correspond à l'une des expressions régulières (et que vous ne souhaitez pas utiliser les crochets d'exécution par défaut), vous pouvez modifier le nom de l'image, ou désactiver le crochet d'exécution par défaut pour cette application et utiliser plutôt un crochet personnalisé.

Vous ne pouvez pas supprimer ou modifier les crochets d'exécution par défaut.

Remarques importantes sur les crochets d'exécution personnalisés

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

- Astra Control nécessite que les crochets d'exécution soient écrits au format de scripts shell exécutables.
- La taille du script est limitée à 128 Ko.
- Astra Control utilise les paramètres de crochet d'exécution et tout critère de correspondance pour déterminer quels crochets s'appliquent à un instantané.
- Toutes les défaillances de crochet d'exécution sont des défaillances logicielles ; d'autres crochets et l'instantané sont toujours tentés 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.



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.

Lors de l'exécution d'un instantané, les événements de hook d'exécution ont lieu dans l'ordre suivant :

1. Tous les crochets d'exécution par défaut fournis par NetApp s'exécutent sur les conteneurs appropriés.
2. Tous les crochets d'exécution pré-snapshot personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets pré-snapshot personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets avant que le snapshot ne soit ni garanti ni configurable.
3. Le snapshot est effectué.
4. Tous les crochets d'exécution post-snapshot personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets post-snapshot personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets après le snapshot n'est ni garanti ni configurable.
5. Tous les crochets d'exécution post-snapshot par défaut fournis par NetApp s'exécutent sur les conteneurs appropriés.



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 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, puis tester l'application.

Afficher les crochets d'exécution existants

Vous pouvez afficher les crochets d'exécution d'une application personnalisés ou par défaut fournis par NetApp.

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-instantané). Pour afficher les journaux d'événements entourant les crochets d'exécution, accédez à la page **activité** dans la zone de navigation de gauche.

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 linux 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 un nouveau crochet**.
4. Dans la zone **Détails du crochet**, selon le moment où le crochet doit être exécuté, choisissez **Préinstantané** ou **Post-instantané**.
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 :
 - 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.
- Coller dans un script personnalisé à partir du presse-papiers.
 - i. Sélectionnez l'option **Coller dans le presse-papiers**.
 - 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.
9. Sélectionnez **Ajouter crochet**.

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
```

Afficher 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.

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.

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 logiciels 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'artefacts 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'artefacts 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'artefacts**, 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'artefacts**, 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'artefacts, 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'artefacts 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 artefacts 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 `kubect1` 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.bundle.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.
 - Remplacez `MON_REGISTRE` par l'URL du référentiel Docker.
 - Remplacez `MON_REGISTRE_USER` et `MON_MOT_DE_PASSE_REGISTRE` par les informations d'identification du référentiel.

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

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
- 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.

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](#)
- [Ajout de nœuds à un cluster back-end de stockage](#)
- [Retirer un système back-end](#)

Afficher les détails du système back-end

Vous pouvez afficher les informations de stockage back-end à partir du tableau de bord ou de l'option Backends.

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).

Avec une connexion à Cloud Insights, vous pouvez voir les volumes utilisés par les applications Kubernetes, qui sont stockés sur un back-end de stockage sélectionné.

Étapes

1. Dans la zone de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.



Si vous êtes connecté à NetApp Cloud Insights, des extraits de données de Cloud Insights s'affichent sur la page Backends.

| Name | Persistent volume | Capacity | App/s | Cluster/s | Cloud |
|-----------------|-------------------|-----------------------|---|----------------------|---------|
| trident_pvc_... | pvc-... | 0.04/46.57 GiB: 0.1% | netapp-acc | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 0.34/23.28 GiB: 1.44% | netapp-acc | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 0.02/0.93 GiB: 2.33% | netapp-acc | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 3.02/50.00 GiB: 6.04% | netapp-acc polaris-mongodb-mongodb | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 0.19/8.00 GiB: 2.39% | apps-mysql mysql-mysql | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 0.41/50.00 GiB: 0.81% | netapp-acc polaris-influxdb2-polaris-influxdb2 | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 2.93/50.00 GiB: 5.87% | netapp-acc polaris-mongodb-mongodb | openshift-cluster010 | private |
| trident_pvc_... | pvc-... | 0.03/10.00 GiB: 0.26% | netapp-acc polaris-consul-consul | openshift-cluster010 | private |

3. Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Annuler la gestion d'un système back-end

Vous pouvez annuler la gestion du système back-end.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Unmanage**.
4. Saisissez « Unmanage » pour confirmer l'action.
5. Sélectionnez **Oui, annulez la gestion du stockage back-end**.

Retirer un système back-end

Vous pouvez supprimer un système back-end de stockage qui n'est plus utilisé. Pour que votre configuration reste simple et à jour, nous vous le souhaitons.



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

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. | <ol style="list-style-type: none"> Sélectionnez le bouton Ajouter. Sélectionnez un fichier de licence à télécharger. Sélectionnez Ajouter pour télécharger le fichier de licence. |

6. Sélectionnez **mettre à jour**.

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**.

Trouvez plus d'informations

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

Contrôle et protection de l'infrastructure

Vous pouvez configurer plusieurs paramètres en option pour améliorer votre expérience avec Astra Control Center. 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. 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.

Ajouter un serveur proxy

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.



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected

Connect

4. Entrez le nom du serveur proxy ou l'adresse IP et le numéro du port proxy.
5. Si votre serveur proxy nécessite une authentification, cochez la case et saisissez le nom d'utilisateur et le mot de passe.
6. Sélectionnez **connexion**.

Résultat

Si les informations de proxy que vous avez saisies ont été enregistrées, la section **HTTP Proxy** de la page **Account > Connections** indique qu'elle est connectée et affiche le nom du serveur.



Connected



HTTP PROXY

Server: proxy.example.com:8888

Authentication: Enabled

Modifier les paramètres du serveur proxy

Vous pouvez modifier les paramètres du serveur proxy.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les détails du serveur et les informations d'authentification.
5. Sélectionnez **Enregistrer**.

Désactiver la connexion au serveur proxy

Vous pouvez désactiver la connexion au serveur proxy. Vous serez averti avant de désactiver cette interruption potentielle à d'autres connexions.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération.

Connectez-vous à Cloud Insights

Pour surveiller et obtenir des informations exploitables sur l'ensemble de votre infrastructure, connectez NetApp Cloud Insights à votre instance Astra Control Center. Cloud Insights est inclus dans votre licence Astra Control Center.

Cloud Insights doit être accessible à partir du réseau utilisé par Astra Control Center, ou indirectement via un serveur proxy.

Lorsque le centre de contrôle Astra est connecté à Cloud Insights, un pod d'unité d'acquisition est créé. Ce pod collecte les données des systèmes back-end gérés par Astra Control Center et les pousse dans Cloud Insights. Ce pod requiert 8 Go de RAM et 2 cœurs de CPU.



Après avoir activé la connexion Cloud Insights, vous pouvez afficher les informations de débit sur la page **Backends** et vous connecter à Cloud Insights à partir de là après avoir sélectionné un back-end de stockage. Vous trouverez également des informations sur le **Tableau de bord** dans la section Cluster et vous y connectez également à Cloud Insights.

Ce dont vous avez besoin

- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Licence Astra Control Center valide.
- Un serveur proxy si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour se connecter à Internet.



Si vous découvrez Cloud Insights, familiarisez-vous avec les fonctions et les fonctionnalités. Voir "[Documentation Cloud Insights](#)".

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Connect** où apparaît **déconnecté** dans la liste déroulante pour ajouter la connexion.



4. Entrez les jetons de l'API Cloud Insights et l'URL du locataire. L'URL du locataire a le format suivant, par exemple :

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Vous obtenez l'URL du locataire lorsque vous obtenez la licence Cloud Insights. Si vous ne disposez pas de l'URL du locataire, reportez-vous à la section "[Documentation Cloud Insights](#)".

- a. Pour obtenir le "[Jeton API](#)", Connectez-vous à l'URL de votre locataire Cloud Insights.
- b. Dans Cloud Insights, générez un jeton d'accès à l'API **lecture/écriture** et un jeton d'accès à l'API **lecture seule** en cliquant sur **Admin > API Access**.

| <input type="checkbox"/> | Name ↑ | Description | Token | API Type | Permission |
|--------------------------|-----------|-------------|-----------|----------------|------------|
| <input type="checkbox"/> | astra_... | | ...zBskB1 | All Categories | Read/Write |
| <input type="checkbox"/> | astra_... | | ...xKOeL_ | All Categories | Read/Write |
| <input type="checkbox"/> | astra_... | | ...2_A6HP | All Categories | Read Only |
| <input type="checkbox"/> | astra_... | | ...8BTKYY | All Categories | Read/Write |

- 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.

EXTERNAL ?

The screenshot shows two connection cards. The first is for 'HTTP PROXY' with a server address 'proxy.example.com:8888' and 'Authentication: Enabled'. The second is for 'CLOUD INSIGHTS' with a tenant 'Cloud Insights'. Both cards have a green 'Connected' button with a dropdown arrow.

Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.

The notification panel shows a red warning icon and a message: 'Unable to connect to Cloud Insights' received 'an hour ago'. The message states: 'The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.'

Vous pouvez également trouver les mêmes informations sous **compte > Notifications**.

À partir du Centre de contrôle Astra, vous pouvez afficher les informations sur le débit sur la page **Backends** et vous connecter à Cloud Insights à partir d'ici après avoir sélectionné un back-end de stockage.

The screenshot shows the 'Backends' page with a table of storage backends. The table has columns for Name, Status, Capacity, Throughput, Type, and Actions. A tooltip for the 'Throughput' metric of the '06' backend is shown, displaying a line graph and the following data: '5m ago: 8.00 MB/s', 'Min: 4.00 MB/s', and 'Max: 11.00 MB/s'. There is also a 'View in Cloud Insights' link in the tooltip.

Pour accéder directement à Cloud Insights, sélectionnez l'icône **Cloud Insights** située en regard de l'image de metrics.

Vous pouvez également trouver les informations sur le **Dashboard**.

Reminder: Before you back up your applications, you need to add at least one object store bucket as a destination to hold your backups.

Add →

Resource summary

The screenshot shows the 'Resource summary' page in Astra Control Center. It features three main panels: 'Apps' (no managed apps), 'Clusters' (with a 'View in cloud insights' button highlighted by a blue box), and 'Storage backends' (showing 1 managed and 0 discovered items).



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

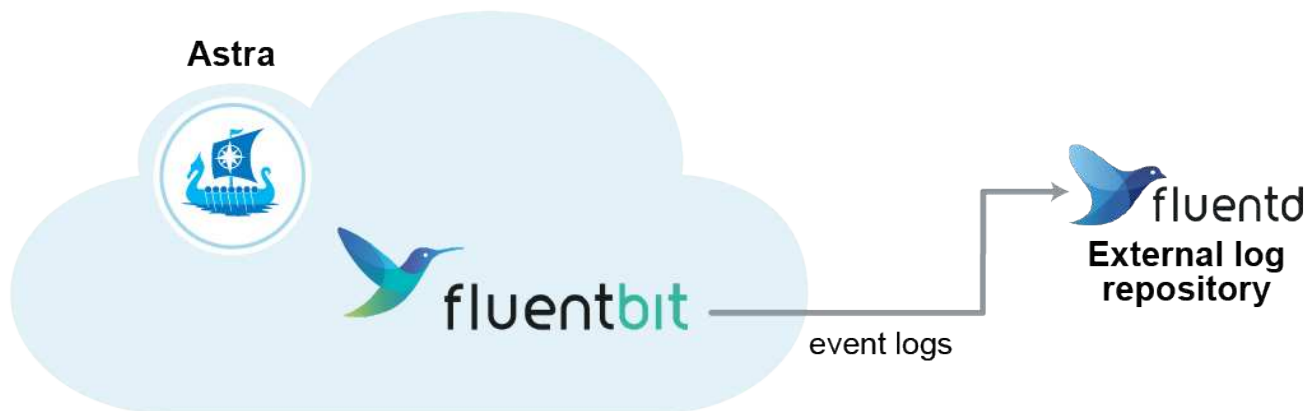
Vous pouvez désactiver la connexion Cloud Insights pour un cluster Kubernetes géré par Astra Control Center. La désactivation de la connexion Cloud Insights ne supprime pas les données de télémétrie déjà chargées sur Cloud Insights.

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

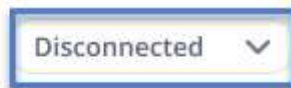
- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Astra Control Center est installé et exécuté sur un cluster Kubernetes.



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.



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

4. Entrez l'adresse IP de l'hôte, le numéro de port et la clé partagée pour votre serveur Fluentd.
5. Sélectionnez **connexion**.

Résultat

Si les détails que vous avez entrés pour votre serveur Fluentd ont été enregistrés, la section **Fluentd** de la page **compte > connexions** indique qu'il est connecté. Vous pouvez maintenant visiter le serveur Fluentd que vous avez connecté et afficher les journaux d'événements.

Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.

Vous pouvez également trouver les mêmes informations sous **compte > Notifications**.



Si vous rencontrez des problèmes avec la collecte de journaux, vous devez vous connecter à votre nœud de travail et vous assurer que vos journaux sont disponibles dans `/var/log/containers/`.

Modifiez la connexion Fluentd

Vous pouvez modifier la connexion Fluentd à votre instance Astra Control Center.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Modifier** dans la liste déroulante pour modifier la connexion.
4. Modifiez les paramètres du point final Fluentd.
5. Sélectionnez **Enregistrer**.

Désactivez la connexion Fluentd

Vous pouvez désactiver la connexion Fluentd à votre instance Astra Control Center.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte > connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération.

Annuler la gestion des applications et des clusters

Supprimez toutes les applications ou clusters que vous ne souhaitez plus gérer à partir d'Astra Control Center.

Annuler la gestion d'une application

Arrêtez de gérer les applications que vous ne souhaitez plus sauvegarder, créer des instantanés ou cloner à partir d'Astra Control Center.

- 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.

Exemple OpenShift :

```
oc get clusteroperators
```

- Assurez-vous que tous les services API sont dans un état sain et disponibles.

Exemple OpenShift :

```
oc 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 NetApp](#)".
2. (Facultatif) utilisez la commande suivante pour vérifier la signature du pack :

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

Déballez le bundle et modifiez le répertoire

1. Extraire les images :

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

2. Passez au répertoire Astra.

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

Ajoutez les images à votre registre local

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



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

a. Connectez-vous à votre registre Docker :

```
docker login [your_registry_path]
```

b. Chargez les images dans Docker.

c. Marquez les images.

d. envoyez les images dans votre registre local.

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

Poser le conducteur du centre de commande Astra mis à jour

1. 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_UPGRADE_TIMEOUT  
  value: 300m
```



```

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
    name: acc-operator-controller-manager
    namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  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_UPGRADE_TIMEOUT
              value: 300m
          image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
          imagePullSecrets: []

```

2. Installez le nouveau conducteur du centre de contrôle Astra :

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

Exemple de réponse :

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.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
```

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` : FALSE OR
- `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: Ingress
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 :

```
astracenter.astra.netapp.io "astra" deleted
```

2. Utiliser la commande suivante pour supprimer le `netapp-acc` espace de noms :

```
kubectl delete ns netapp-acc
```

Résultat :

```
namespace "netapp-acc" deleted
```

3. Utiliser la commande suivante pour supprimer les composants du système de l'opérateur Astra Control Center :

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```


Résultat :

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

Dépannage des problèmes de désinstallation

Utilisez les solutions de contournement suivantes pour résoudre les problèmes que vous rencontrez lors de la désinstallation d'Astra Control Center.

La désinstallation d'Astra Control Center ne parvient pas à nettoyer le module de l'opérateur de surveillance sur le cluster géré

Si vous n'avez pas dégéré les clusters avant de désinstaller Astra Control Center, vous pouvez supprimer manuellement les pods dans l'espace de noms netapp-Monitoring et dans l'espace de noms à l'aide des commandes suivantes :

Étapes

1. Supprimer acc-monitoring agent :

```
kubectl delete agents acc-monitoring -n netapp-monitoring
```

Résultat :

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Supprimez le namespace :

```
kubectl delete ns netapp-monitoring
```

Résultat :

```
namespace "netapp-monitoring" deleted
```

3. Confirmer la suppression des ressources :

```
kubectl get pods -n netapp-monitoring
```

Résultat :

```
No resources found in netapp-monitoring namespace.
```

4. Confirmer la suppression de l'agent de surveillance :

```
kubectl get crd|grep agent
```

Résultat de l'échantillon :

```
agents.monitoring.netapp.com                2021-07-21T06:08:13Z
```

5. Supprimer les informations de définition de ressource personnalisée (CRD) :

```
kubectl delete crds agents.monitoring.netapp.com
```

Résultat :

```
customresourcedefinition.apiextensions.k8s.io  
"agents.monitoring.netapp.com" deleted
```

La désinstallation d'Astra Control Center ne parvient pas à nettoyer les CRD Traefik

Vous pouvez supprimer manuellement les CRD Traefik. Les CRDS sont des ressources globales, et leur suppression peut avoir un impact sur d'autres applications du cluster.

Étapes

1. Lister les CRD Traefik installés sur le cluster :

```
kubectl get crds |grep -E 'traefik'
```

Réponse

```
ingressroutes.traefik.containo.us          2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us       2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us       2021-06-23T23:29:12Z
middlewares.traefik.containo.us            2021-06-23T23:29:12Z
middlewareetcps.traefik.containo.us         2021-06-23T23:29:12Z
serverstransports.traefik.containo.us       2021-06-23T23:29:13Z
tloptions.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 tloptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewareetcps.traefik.containo.us
```

Trouvez plus d'informations

- ["Problèmes connus de désinstallation"](#)

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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