Utilisez Astra

Astra Control Center

NetApp
November 21, 2023

Sommaire

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.

Besoins en termes de gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licensing**: Pour gérer des applications à l'aide d'Astra Control Center, vous devez disposer d'une licence Astra Control Center.
- **Espaces de noms** : Astra Control exige qu'une application ne couvre pas plus d'un seul espace de noms, mais qu'un espace de noms peut contenir plus d'une application.
- **StorageClass** : si vous installez explicitement une application avec une classe de stockage et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage explicitement définie sur un cluster ne disposant pas de la même classe de stockage échouera.
- **Ressources Kubernetes** : les applications qui utilisent les ressources Kubernetes non collectées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control collecte les ressources Kubernetes suivantes :
  - ClusterRole
  - ClusterRoleBinding
  - ConfigMap
  - CustomResourceDefinition
  - Ressource CustomResource
  - Ensemble de démonstrations
  - Déploiement
  - Déploiement.Config
  - Entrée
  - MutatingWebhook
  - Demande de volume persistant
  - Pod
  - Et de réplication
  - RoleBinding
  - Rôle
  - Itinéraire
  - Secret
  - Service

- Compte de service
- StatefulSet
- ValidétingWebhook

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

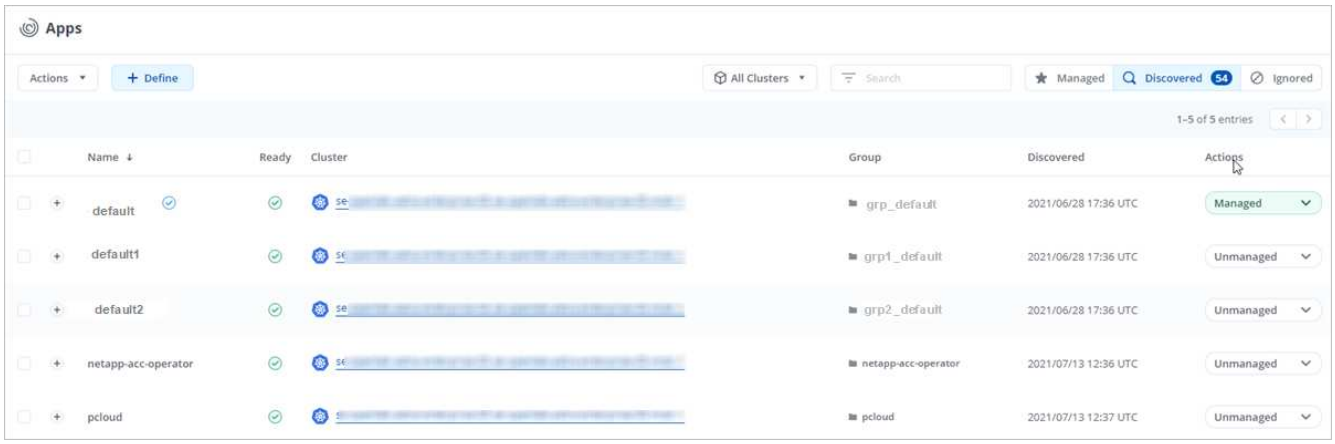
La section **découverts** de la page Apps affiche les espaces de noms et toutes les applications installées par Helm ou les applications étiquetées sur mesure dans ces espaces de noms. Vous pouvez choisir de gérer chaque application individuellement ou au niveau de l'espace de noms. La granularité est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



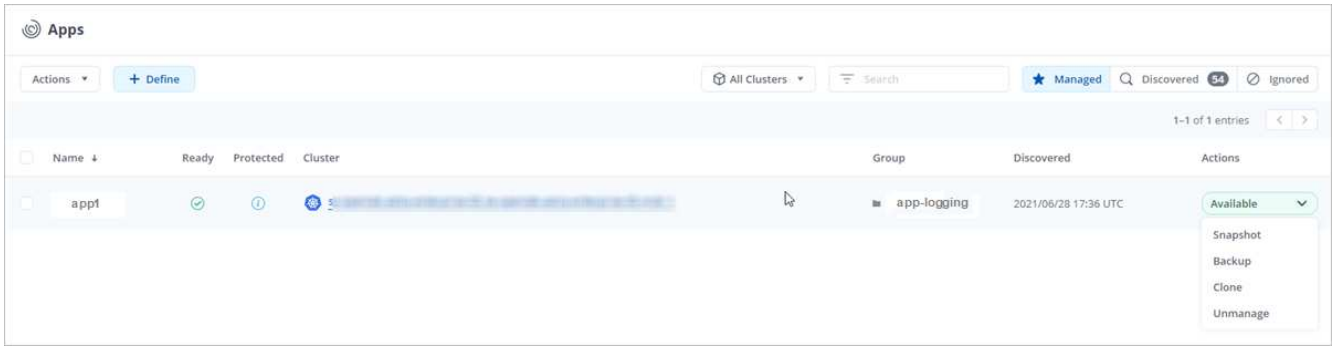
3. Afficher la liste des espaces de noms découverts. Développez l'espace de noms pour afficher les applications et les ressources associées.

   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 au niveau souhaité dans la hiérarchie, et dans le menu actions, sélectionnez **gérer**.
7. Si vous ne souhaitez pas gérer une application, sélectionnez **Ignorer** dans le menu actions situé à côté de l'application.

   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.



   Notez que l'application que vous venez d'ajouter comporte une icône d'avertissement sous la colonne protégée, 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

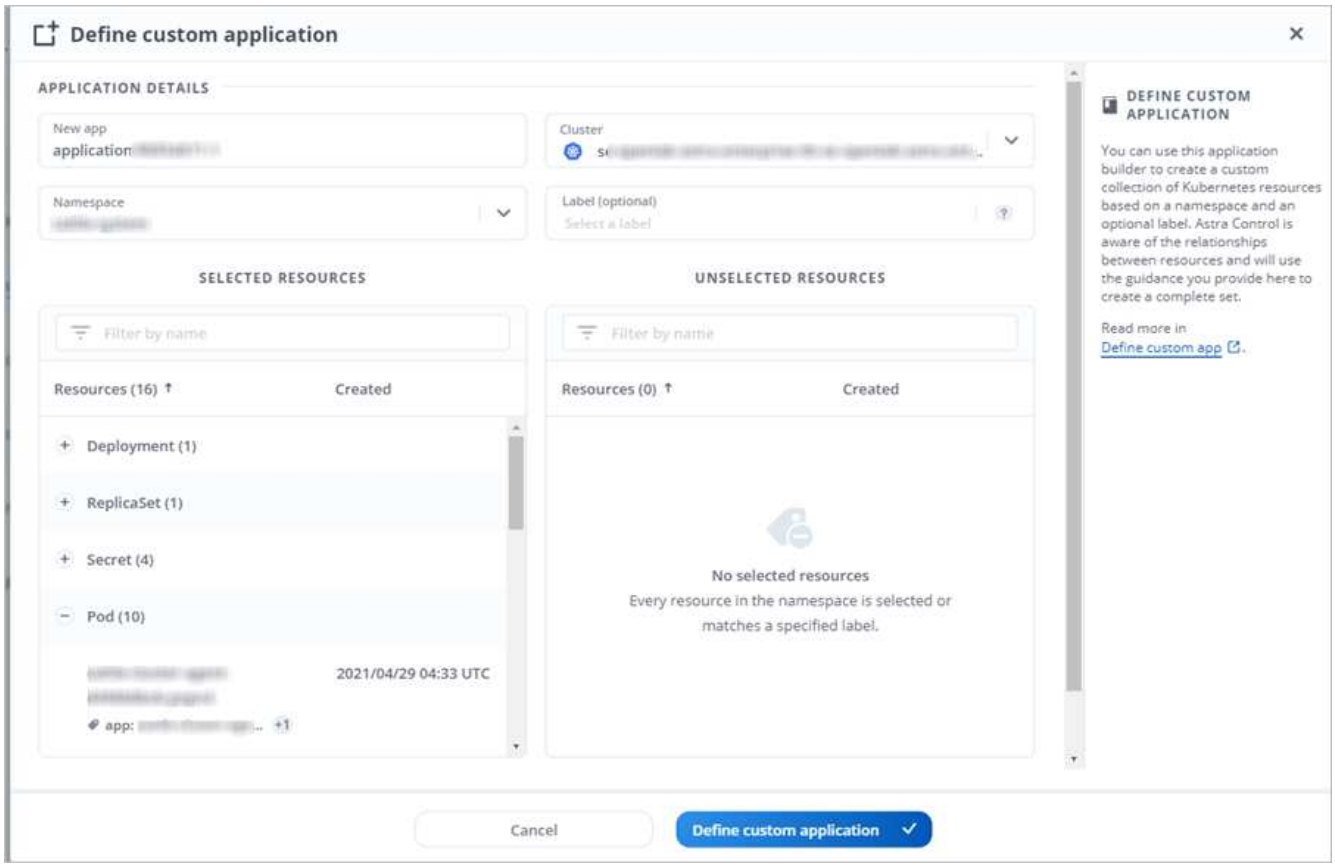
application, de sorte qu'à mesure que de nouvelles applications sont installées, elles sont plus faciles à trouver et à gérer.

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 actions, sélectionnez **Ignorer**.
5. Pour annuler l'ignorer, dans le menu actions, 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.

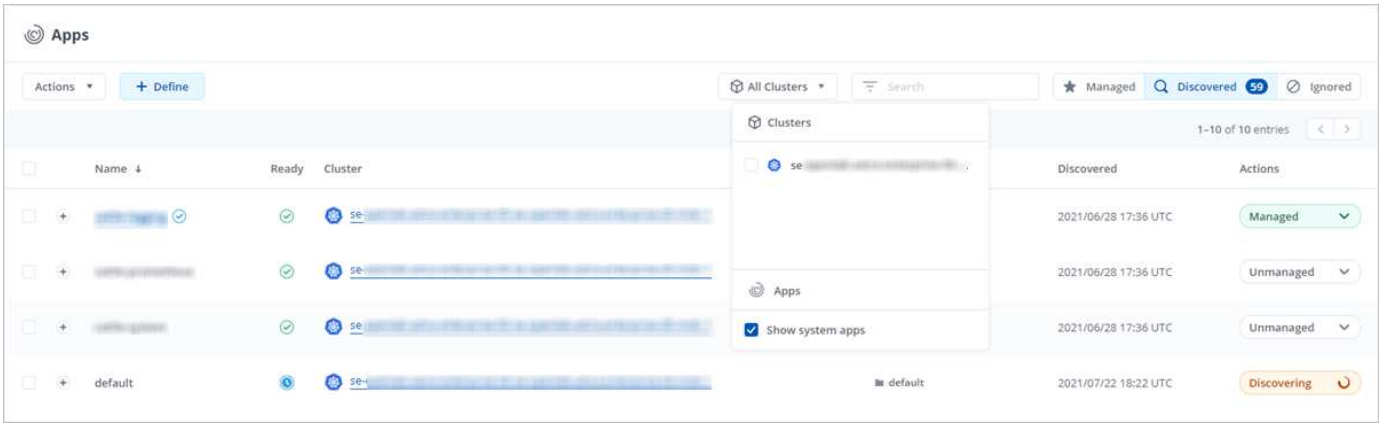
Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **géré** comme filtre.
3. Sélectionnez l'application.
4. Dans le menu 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. Vous

pouvez afficher les applications système en cochant la case **Afficher les applications système** sous le filtre Cluster dans la barre d'outils.



Nous ne vous montrons pas par défaut ces applications système car il est rare que vous ayez besoin de les sauvegarder.

> 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".

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.

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.

Pour créer une application personnalisée, accédez à la page applications et sélectionnez **+ définir**.

Lorsque vous effectuez vos sélections, la fenêtre de l'application personnalisée vous 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.

> 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.

Exemple : politique de protection séparée pour la libération de canaris

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 version canary, et une pour la version stable. Les sauvegardes, snapshots et opérations de clonage sont donc séparés pour les deux groupes d'objets Kubernetes.

Étapes

1. Une fois que l'équipe a ajouté le cluster à Astra Control, l'étape suivante consiste à définir une application personnalisée. Pour ce faire, l'équipe sélectionne le bouton **+ Define** sur la page Apps.
2. Dans la fenêtre contextuelle qui s'affiche, l'association est définie `devops-canary-deployment` comme nom de l'application. L'équipe choisit le cluster dans la liste déroulante **Cluster**, puis l'espace de noms de l'application dans la liste déroulante **namespace**.
3. L'association peut saisir l'une ou l'autre `deployment=canary` Dans le champ **étiquettes**, ou sélectionnez cette étiquette parmi les ressources répertoriées ci-dessous.
4. Après avoir défini l'application personnalisée pour le déploiement canary, l'équipe répète le processus pour un déploiement stable.

Lorsque l'équipe a fini de créer les deux applications personnalisées, elle peut 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.

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

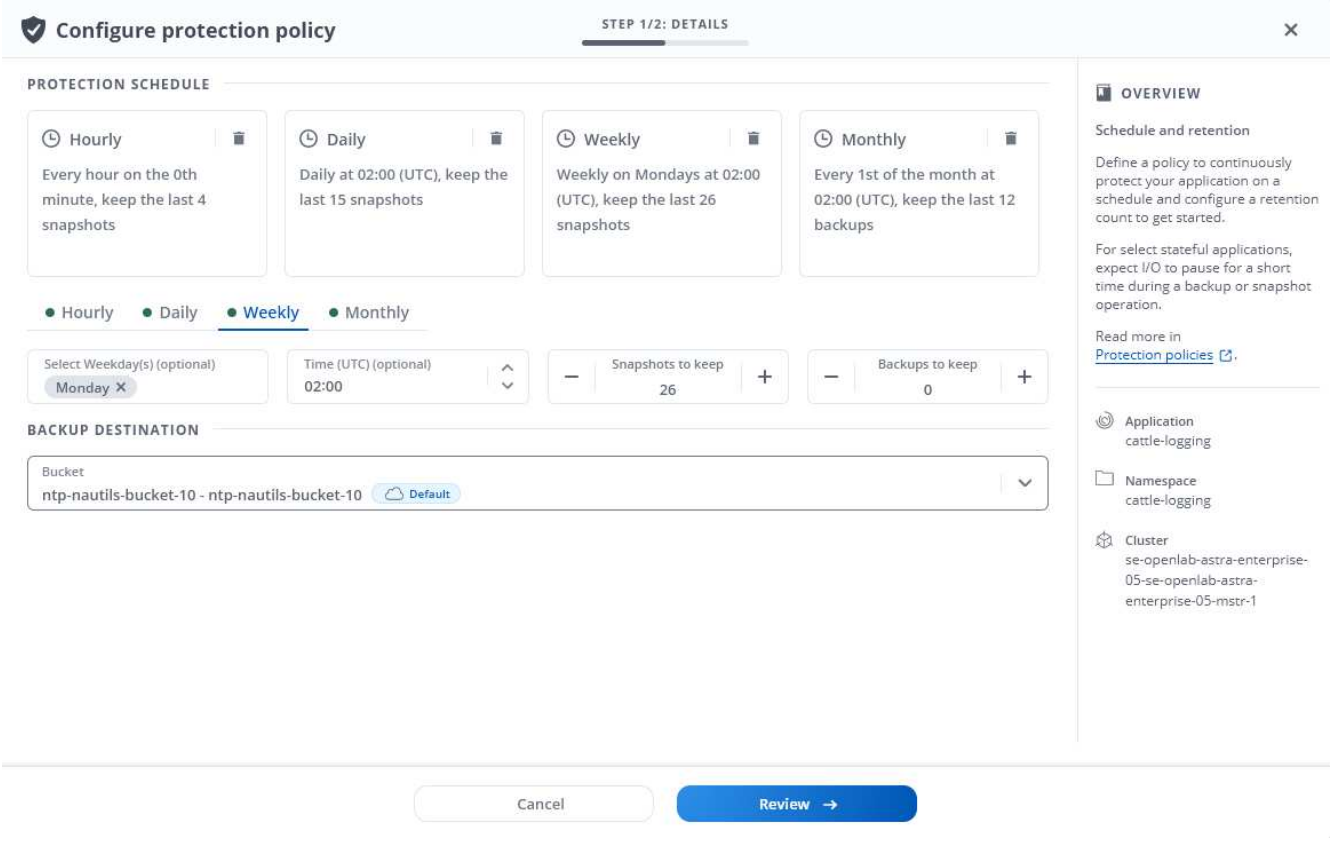
Une règle de protection protège une application en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Vous pouvez choisir de créer des snapshots et des sauvegardes toutes les heures, tous les jours, toutes les semaines et tous les mois, et vous pouvez spécifier le nombre de copies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



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. Sélectionnez la liste déroulante dans la colonne **actions** pour l'application souhaitée.
3. Sélectionnez **instantané**.
4. Personnalisez le nom de l'instantané, puis sélectionnez **Review**.
5. 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. Sélectionnez la liste déroulante dans la colonne **actions** pour l'application souhaitée.
3. Sélectionnez **Backup**.
4. Personnaliser le nom de la sauvegarde.
5. 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.
6. Choisissez une destination pour la sauvegarde en sélectionnant dans la liste des compartiments de stockage.
7. Sélectionnez **Revue**.
8. 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. Sélectionnez la liste déroulante dans la colonne **actions** pour l'instantané souhaité.
4. Sélectionnez **Supprimer instantané**.
5. 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. Sélectionnez la liste déroulante dans la colonne **actions** pour la sauvegarde souhaitée.
5. Sélectionnez **Supprimer sauvegarde**.
6. 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.

> 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.

> 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. Sélectionnez la liste déroulante dans la colonne **actions** pour l'instantané ou la sauvegarde à partir duquel vous souhaitez restaurer.
5. Sélectionnez **Restaurer l'application**.
6. **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**.
7. **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.

> 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.

Cloner et migrer les applications

Clonez une application existante pour créer une application dupliquée sur le même cluster Kubernetes ou sur un autre cluster. 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.

> 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.

> 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 Astra Control Center clone une application, il crée un clone de la configuration des applications et du stockage persistant.

> 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.

> 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
> ```

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.

Étapes

1. Sélectionnez **applications**.
2. Effectuez l'une des opérations suivantes :
   - Sélectionnez la liste déroulante 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 : \bpostgresql\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 désactivez le crochet d'exécution par défaut pour cette application et utilisez 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 tentées même en cas de défaillance d'un crochet. Cependant, lorsqu'un crochet échoue, un événement d'avertissement est enregistré dans le journal des événements de la page **activité**.
- Pour créer, modifier ou supprimer des crochets d'exécution, vous devez être un utilisateur disposant des autorisations propriétaire, administrateur ou membre.
- Si l'exécution d'un crochet d'exécution prend plus de 25 minutes, le crochet échoue, créant une entrée de journal d'événements avec un code retour « N/A ». Tout instantané affecté expire et sera marqué comme ayant échoué, avec une entrée du journal des événements qui en résulte indiquant le délai d'attente.

> 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 la liste déroulante **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 la liste déroulante **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.
#
```

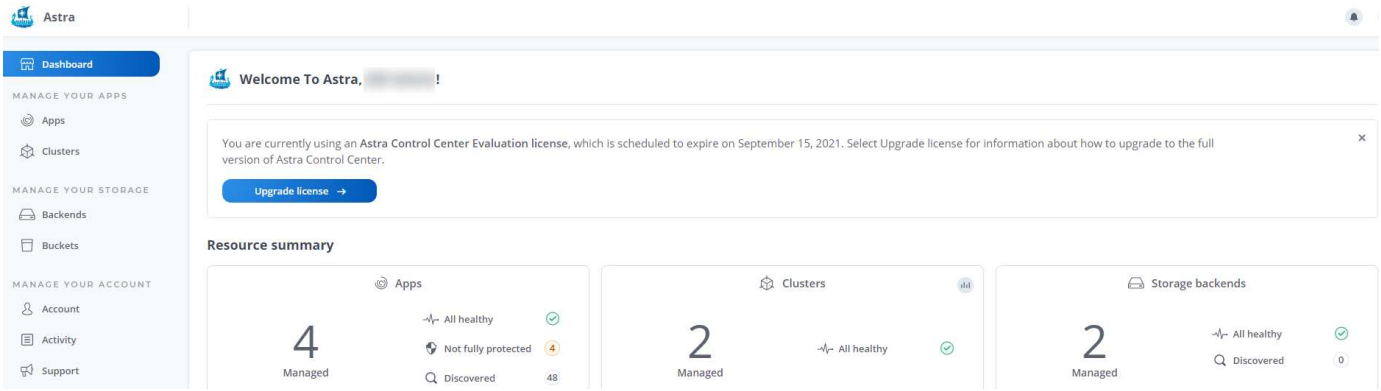
```
# args: None
#

#
# 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 chacun de ces numéros. 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.
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 ajouter, supprimer et modifier les utilisateurs de votre installation Astra Control Center à l'aide de l'interface utilisateur du Centre de contrôle Astra. Vous pouvez utiliser l'interface utilisateur Astra ou "API de contrôle Astra" pour gérer les utilisateurs.

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, mais ne peut pas annuler la gestion des applications ou des clusters, ni supprimer des instantanés ou 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. 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. Sélectionnez la liste déroulante **actions** et sélectionnez **Modifier le 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. Dans l'onglet **utilisateurs**, sélectionnez la liste déroulante dans la colonne **état** de l'utilisateur.
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. Dans l'onglet **utilisateurs**, sélectionnez la liste déroulante dans la colonne **rôle** de l'utilisateur.
3. Sélectionnez un nouveau rôle, puis sélectionnez **changer le rôle** lorsque vous y êtes invité.

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. Sélectionnez **actions** et sélectionnez **Supprimer utilisateur/s**.
4. Lorsque vous y êtes invité, confirmez la suppression en saisissant le mot "supprimer", puis sélectionnez **Oui, Supprimer l'utilisateur**.

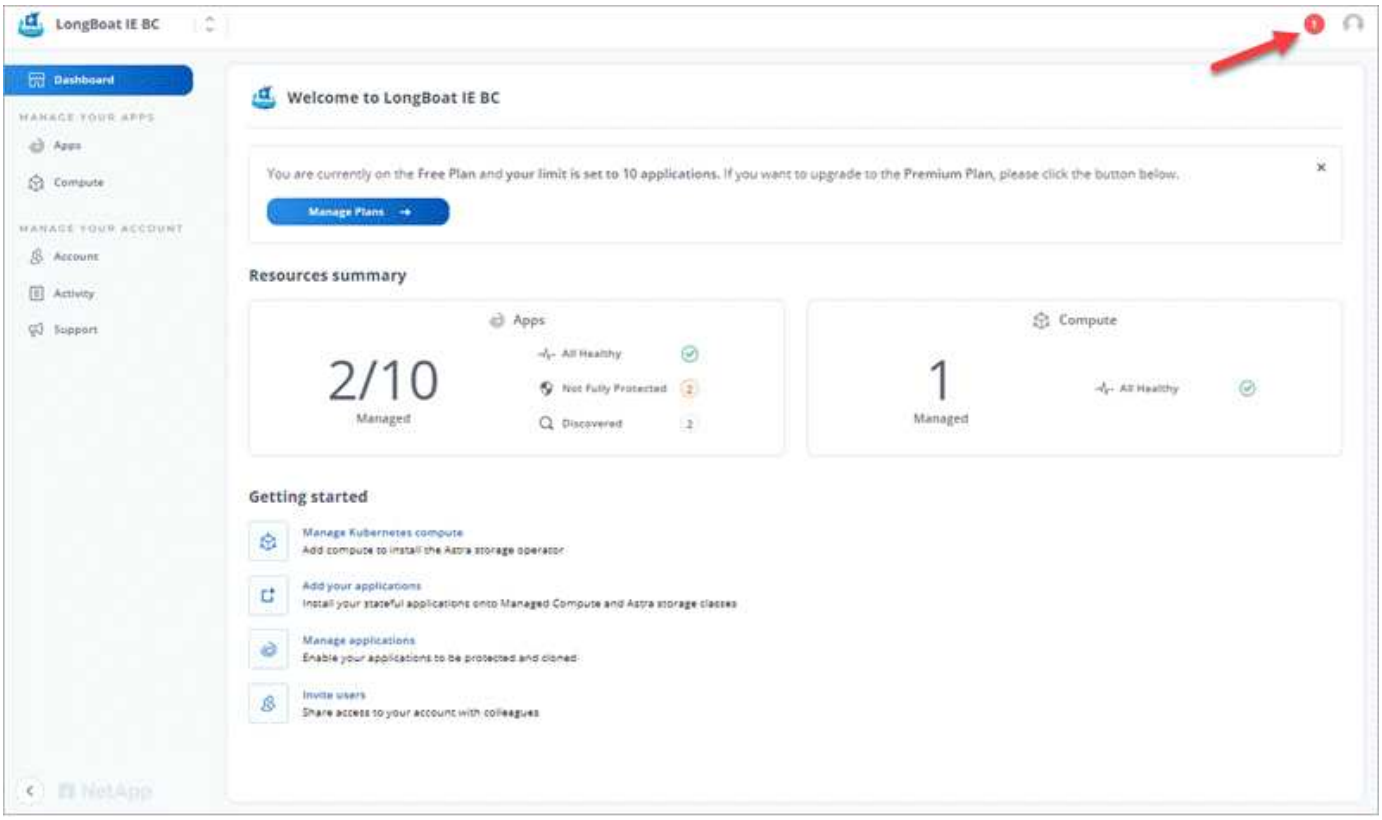
Résultat

Astra Control Center supprime l'utilisateur du compte.

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.

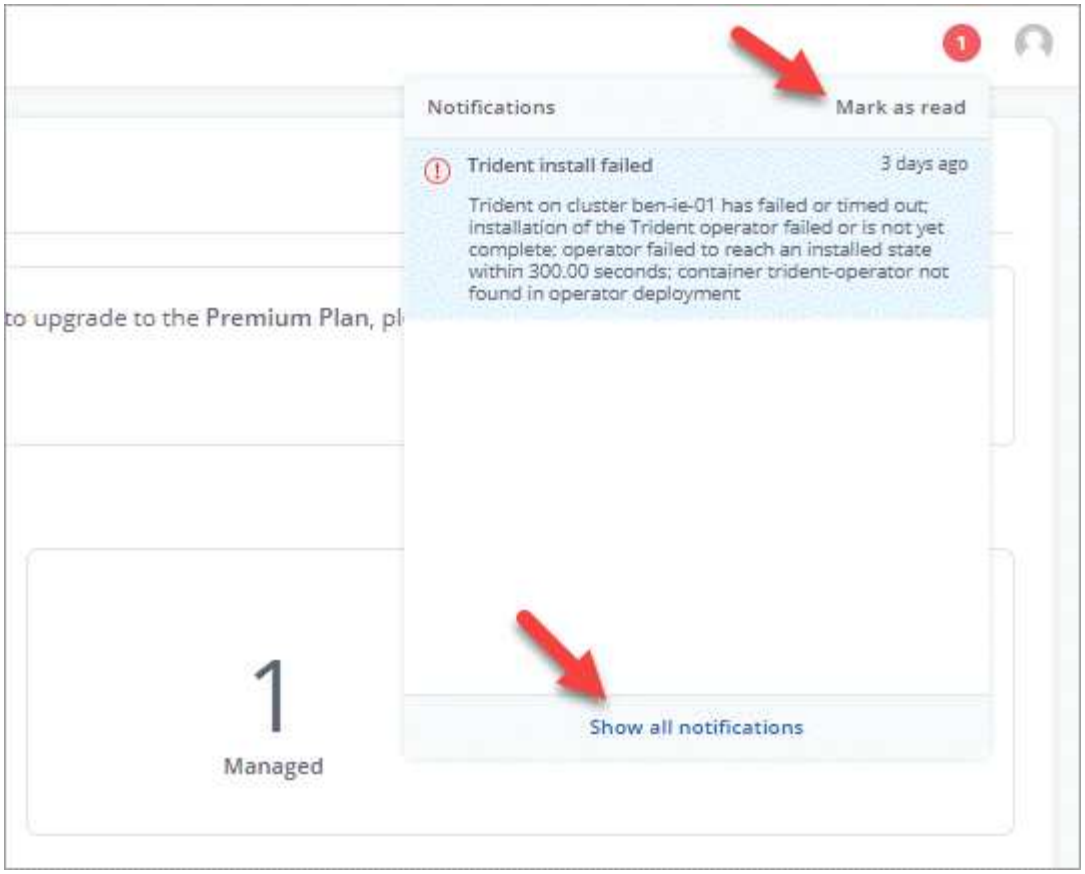
Le nombre de notifications non lues est disponible dans le coin supérieur droit de l'interface :



Vous pouvez afficher ces notifications et les marquer comme lues (cela peut s'avérer pratique si vous souhaitez effacer les notifications non lues comme nous le faisons).

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.

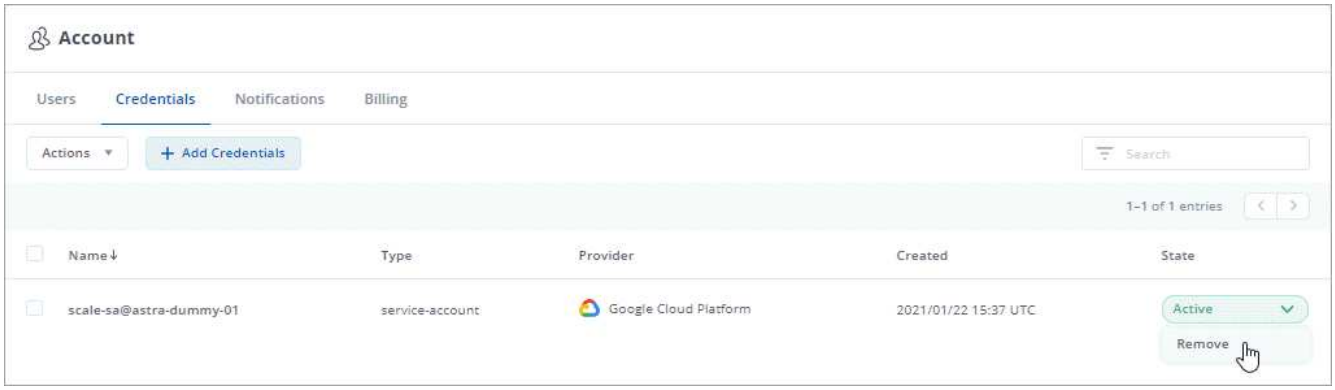
Supprimer les informations d'identification

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 > informations d'identification**.
2. Sélectionnez la liste déroulante dans la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
3. Sélectionnez **Supprimer**.



4. 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.

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.

Utiliser l'un des fournisseurs de compartiments suivants :

- NetApp ONTAP S3
- NetApp StorageGRID S3

- S3 générique

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

Vous ne pouvez pas supprimer un compartiment, mais vous pouvez le modifier.

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

> 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.

Supprimer les informations d'identification

Supprimez les identifiants S3 d'un compte à tout moment à l'aide de l'API Astra Control.

Pour plus de détails, voir "Utilisez l'API de contrôle Astra".

> 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. Il est préférable de ne pas supprimer ces informations d'identification.

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 la navigation à gauche, sélectionnez **seaux**.
2. Dans le menu 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**.

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

Afficher les détails du système back-end

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

Affichez les détails du système de stockage back-end à partir du tableau de bord

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Tableau de bord**.
2. Vérifiez 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

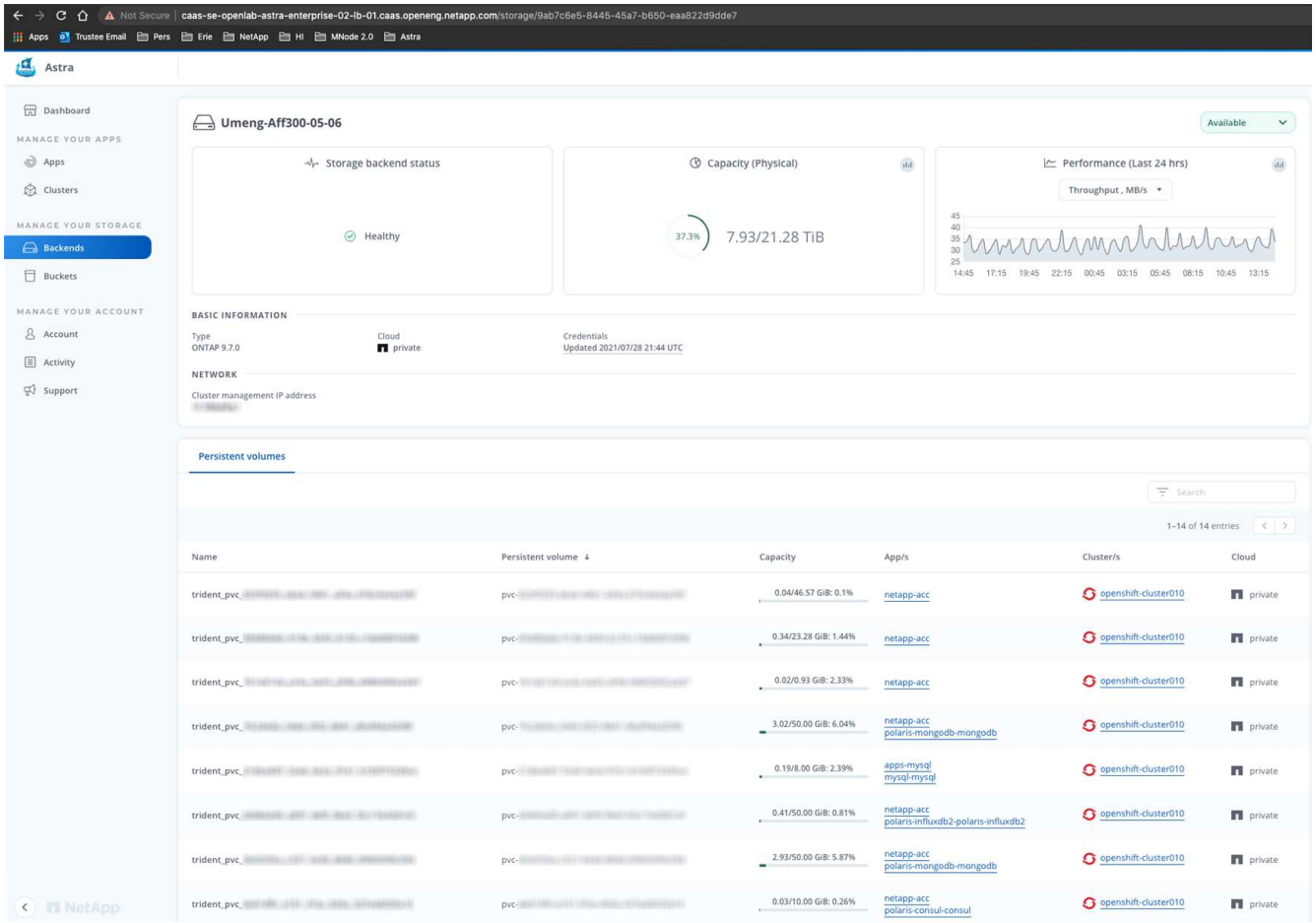
Affichez des informations sur l'état du système back-end, la capacité et les performances (débit et/ou latence des IOPS).

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.



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 gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le menu actions, sélectionnez **Unmanage**.
4. Tapez « Unmanage » pour confirmer la suppression.
5. Sélectionnez **Oui, retirez le back-end de stockage**.

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.

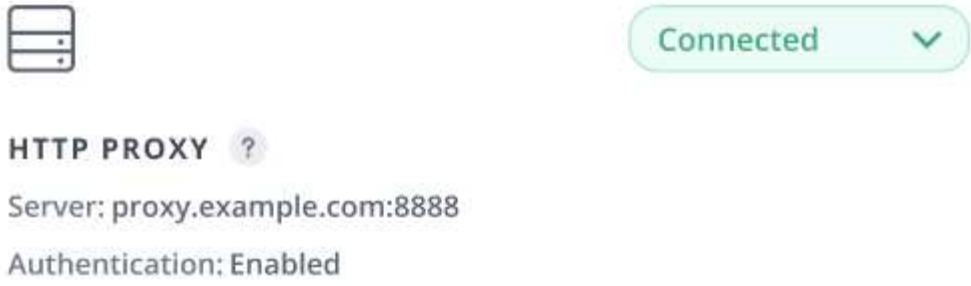
Étapes

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.

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 entrez le nom d'utilisateur et le mot de passe.
6. Sélectionnez **connexion**.

Résultat

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



Modifier les paramètres du serveur proxy

Vous pouvez modifier les paramètres du serveur proxy.

Étapes

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

Désactiver la connexion au serveur proxy

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

Étapes

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

Connectez-vous à Cloud Insights

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

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

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

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

Ce dont vous avez besoin

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

> Si vous découvrez Cloud Insights, familiarisez-vous avec les fonctions et les fonctionnalités. Voir "Documentation Cloud Insights".

Étapes

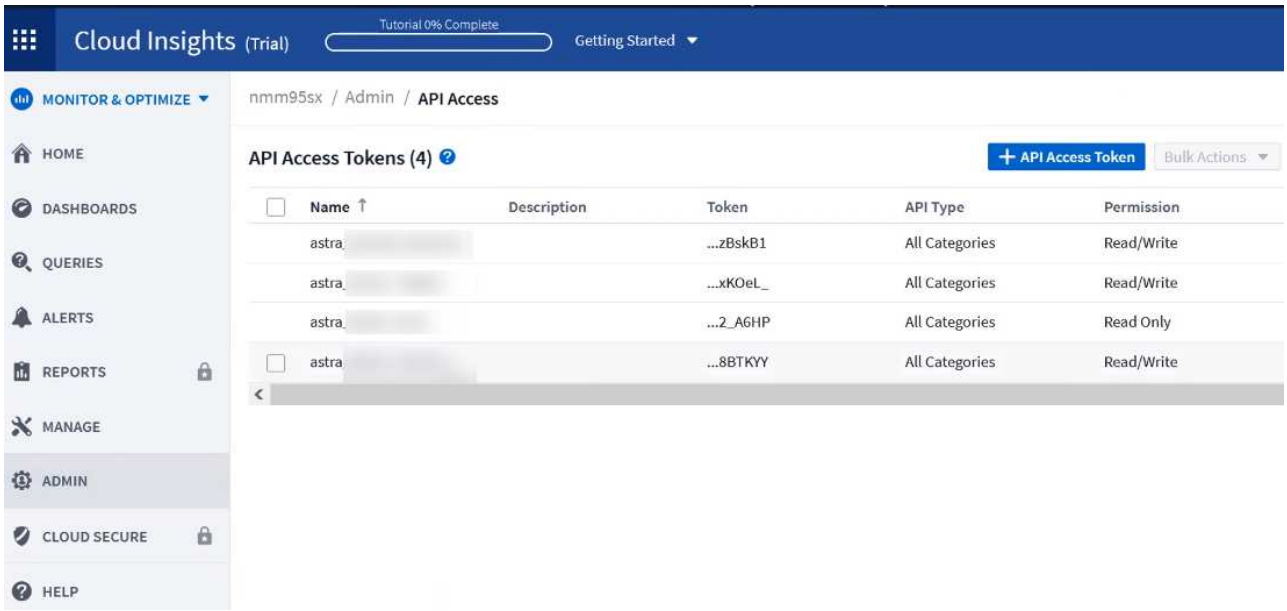
1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **Connect** où apparaît **déconnecté** dans la liste déroulante pour ajouter la connexion.

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

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

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

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



c. Copiez la clé **lecture seule**. Vous devrez la coller dans la fenêtre du centre de contrôle Astra pour activer la connexion Cloud Insights. Pour les autorisations de clé de token d'accès à l'API de lecture, sélectionnez : actifs, alertes, unité d'acquisition et collecte de données.

d. Copiez la clé **lecture/écriture**. Vous devrez le coller dans la fenêtre Centre de contrôle Astra **connexion Cloud Insights**. Pour les autorisations de clés de token d'accès à l'API Read/Write, sélectionnez : Assets, Data ingestion, gestion des journaux, unité d'acquisition, Et collecte de données.

> Nous vous recommandons de générer une clé **lecture seule** et une clé **lecture/écriture**, et de ne pas utiliser la même clé à ces deux fins. Par défaut, la période d'expiration du token est définie sur un an. Nous vous recommandons de conserver la sélection par défaut pour donner au token la durée maximale avant son expiration. Si votre jeton expire, la télémétrie s'arrête.

e. Collez les clés que vous avez copiées de Cloud Insights dans le centre de contrôle Astra.

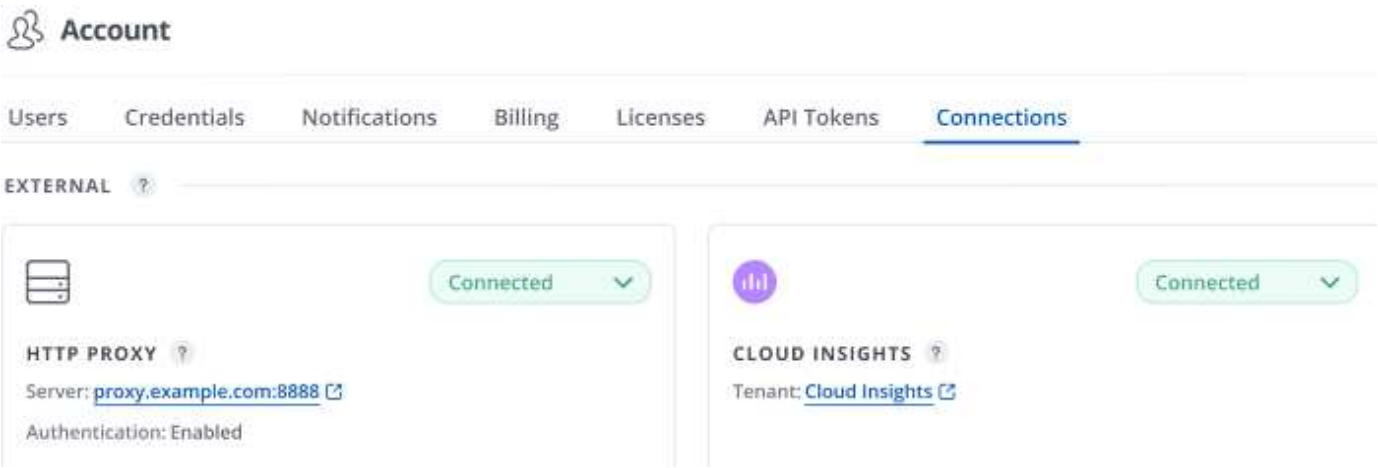
5. Sélectionnez **connexion**.

> Après avoir sélectionné **connexion,** l'état de la connexion devient **en attente** dans la section **Cloud Insights** de la page **compte** > **connexions**. Il peut y avoir quelques minutes pour que la connexion soit activée et que l'état passe à **Connected**.

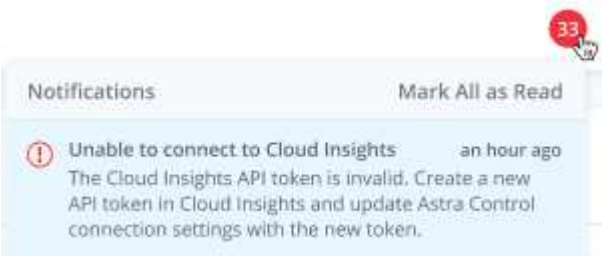
> Pour passer facilement entre le centre de contrôle Astra et les interfaces utilisateur Cloud Insights, assurez-vous d'être connecté aux deux.

Afficher les données dans Cloud Insights

Si la connexion a réussi, la section **Cloud Insights** de la page **compte** > **connexions** indique qu'elle est connectée et affiche l'URL du locataire. Vous pouvez accéder à Cloud Insights pour consulter les données reçues et affichées avec succès.

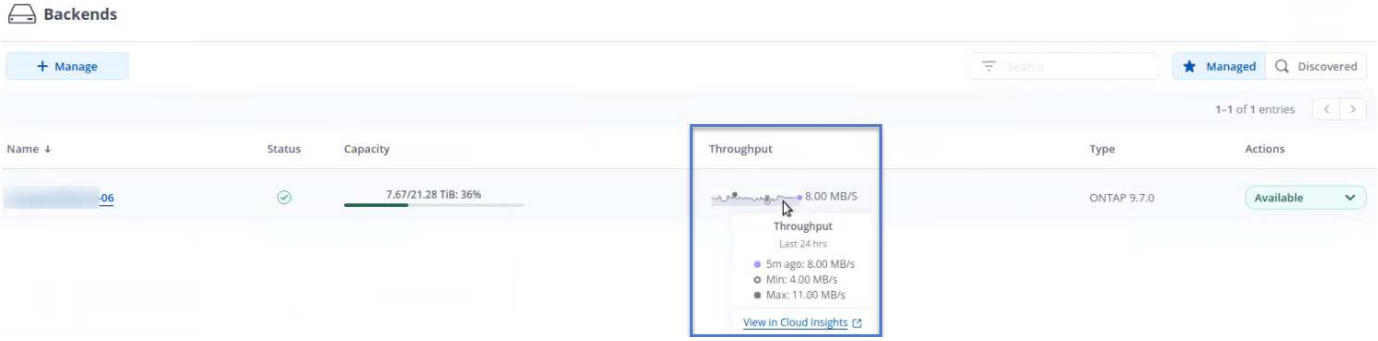


Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.



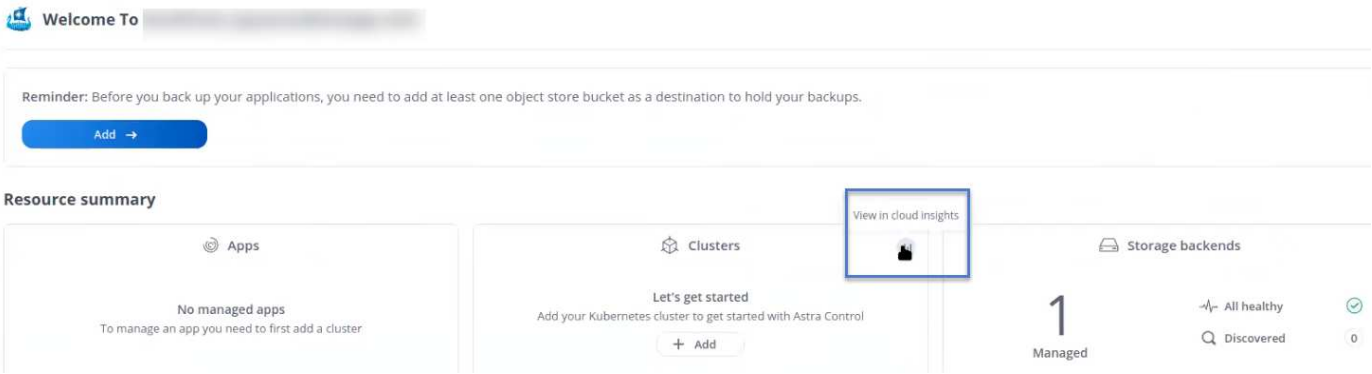
Vous pouvez également trouver les mêmes informations sous **compte** > **Notifications**.

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



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

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



> Après l'activation de la connexion Cloud Insights, si vous supprimez les systèmes back-end ajoutés dans Astra Control Center, le système back-end cesse de créer des rapports avec Cloud Insights.

Modifier la connexion Cloud Insights

Vous pouvez modifier la connexion Cloud Insights.

> Vous pouvez uniquement modifier les clés API. Pour modifier l'URL du locataire Cloud Insights, nous vous recommandons de déconnecter la connexion Cloud Insights et de vous connecter à la nouvelle URL.

Étapes

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

Désactiver la connexion Cloud Insights

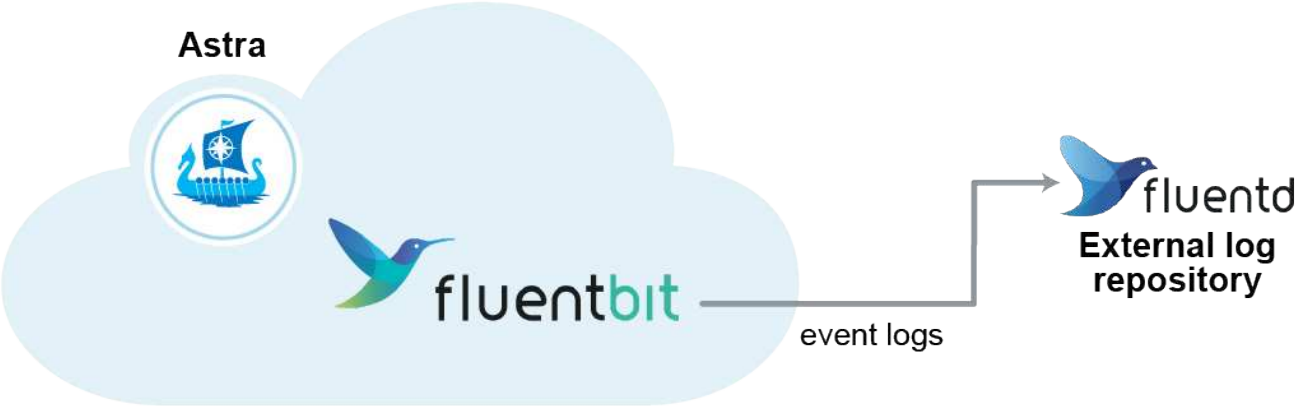
Vous pouvez désactiver la connexion Cloud Insights pour un cluster Kubernetes géré par Astra Control Center. La désactivation de la connexion Cloud Insights ne supprime pas les données de télémétrie déjà chargées sur Cloud Insights.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
2. Sélectionnez **compte** > **connexions**.
3. Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
4. Dans la boîte de dialogue qui s'ouvre, confirmez l'opération. Après avoir confirmé l'opération, sur la page **compte** > **connexions**, l'état Cloud Insights devient **en attente**. Le changement d'état prend quelques minutes à **déconnecté**.

Connectez-vous à Fluentd

Vous pouvez envoyer des journaux (événements Kubernetes) depuis Astra Control Center vers votre terminal Fluentd. La connexion Fluentd est désactivée par défaut.



Seuls les journaux d'événements des clusters gérés sont transférés à Fluentd.

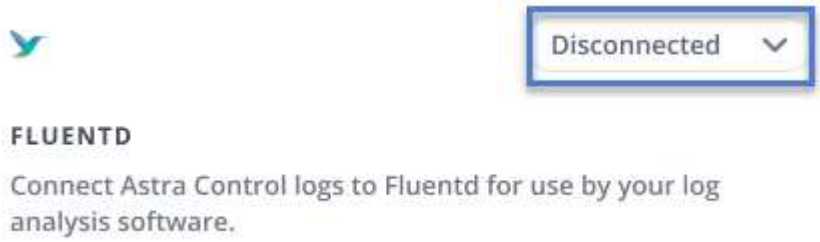
Ce dont vous avez besoin

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

Astra Control Center ne valide pas les détails que vous entrez pour votre serveur Fluentd. Assurez-vous de saisir les valeurs correctes.

Étapes

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



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

Résultat

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

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

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

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

Modifiez la connexion Fluentd

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

Étapes

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

Désactivez la connexion Fluentd

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

Étapes

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

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.

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 cluster que vous ne souhaitez plus gérer dans Astra Control Center.
3. Dans le menu **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
- Mettre à niveau des services tiers
- Vérifiez l'état du système

> 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.

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

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. Modifiez la ressource personnalisée Astra Control Center (CR) et modifiez la version Astra (`astraVersion` intérieur de `Spec`) numéro au plus tard :

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> La modification de la version d'Astra est la seule exigence pour une mise à niveau du centre de contrôle Astra. Votre chemin de registre doit correspondre au chemin du registre où vous avez poussé les images dans un étape précédente.

2. Vérifiez que les pods s'arrêtent et deviennent disponibles à nouveau :

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

3. Vérifiez que tous les composants du système ont été mis à niveau.

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

Chaque pod doit avoir un statut de `Running` et `Age` c'est récent. Le déploiement des modules du système peut prendre plusieurs minutes.

Exemple de réponse :

```
NAME                                          READY   STATUS    RESTARTS
AGE
acc-helm-repo-5f75c5f564-bzqmt             1/1     Running   0
11m
activity-6b8f7cccb9-mlrn4                  1/1     Running   0
9m2s
api-token-authentication-6hznt             1/1     Running   0
8m50s
api-token-authentication-qpfgb             1/1     Running   0
8m50s
api-token-authentication-sqnb7             1/1     Running   0
8m50s
asup-5578bbdd57-dxkbp                      1/1     Running   0
9m3s
authentication-56bff4f95d-mspmq            1/1     Running   0
7m31s
bucketservice-6f7968b95d-9rrrl             1/1     Running   0
8m36s
cert-manager-5f6cf4bc4b-82khn              1/1     Running   0
6m19s
cert-manager-cainjector-76cf976458-sdrbc   1/1     Running   0
6m19s
cert-manager-webhook-5b7896bfd8-2n45j      1/1     Running   0
6m19s
cloud-extension-749d9f684c-8bdhq           1/1     Running   0
9m6s
cloud-insights-service-7d58687d9-h5tzw     1/1     Running   2
8m56s
composite-compute-968c79cb5-nv7l4          1/1     Running   0
9m11s
composite-volume-7687569985-jg9gg          1/1     Running   0
8m33s
credentials-5c9b75f4d6-nx9cz               1/1     Running   0
8m42s
entitlement-6c96fd8b78-zt7f8               1/1     Running   0
8m28s
features-5f7bfc9f68-gsjnl                  1/1     Running   0
8m57s
fluent-bit-ds-h88p7                        1/1     Running   0
7m22s
fluent-bit-ds-krhnj                        1/1     Running   0
7m23s
fluent-bit-ds-l5bjj                        1/1     Running   0
7m22s
```

```
fluent-bit-ds-lrclb                        1/1     Running   0
7m23s
fluent-bit-ds-s5t4n                        1/1     Running   0
7m23s
fluent-bit-ds-zpr6v                        1/1     Running   0
7m22s
graphql-server-5f5976f4bd-vbb4z            1/1     Running   0
7m13s
identity-56f78b8f9f-8h9p9                  1/1     Running   0
8m29s
influxdb2-0                                1/1     Running   0
11m
krakend-6f8d995b4d-5khkl                   1/1     Running   0
7m7s
license-5b5db87c97-jmxzc                   1/1     Running   0
9m
login-ui-57b57c74b8-6xtv7                  1/1     Running   0
7m10s
loki-0                                     1/1     Running   0
11m
monitoring-operator-9dbc9c76d-8znck        2/2     Running   0
7m33s
nats-0                                     1/1     Running   0
11m
nats-1                                     1/1     Running   0
10m
nats-2                                     1/1     Running   0
10m
nautilus-6b9d88bc86-h8kfb                  1/1     Running   0
8m6s
nautilus-6b9d88bc86-vn68r                  1/1     Running   0
8m35s
openapi-b87d77dd8-5dz9h                    1/1     Running   0
9m7s
polaris-consul-consul-5ljfb                1/1     Running   0
11m
polaris-consul-consul-s5d5z                1/1     Running   0
11m
polaris-consul-consul-server-0             1/1     Running   0
11m
polaris-consul-consul-server-1             1/1     Running   0
11m
polaris-consul-consul-server-2             1/1     Running   0
11m
polaris-consul-consul-twmpq                1/1     Running   0
11m
```

```
polaris-mongodb-0                          2/2     Running   0
11m
polaris-mongodb-1                          2/2     Running   0
10m
polaris-mongodb-2                          2/2     Running   0
10m
polaris-ui-84dc87847f-zrg8w                1/1     Running   0
7m12s
polaris-vault-0                            1/1     Running   0
11m
polaris-vault-1                            1/1     Running   0
11m
polaris-vault-2                            1/1     Running   0
11m
public-metrics-657698b66f-67pgt            1/1     Running   0
8m47s
storage-backend-metrics-6848b9fd87-w7x8r   1/1     Running   0
8m39s
storage-provider-5ff5868cd5-r9hj7          1/1     Running   0
8m45s
telegraf-ds-dw4hg                          1/1     Running   0
7m23s
telegraf-ds-k92gn                          1/1     Running   0
7m23s
telegraf-ds-mmxjl                          1/1     Running   0
7m23s
telegraf-ds-nhs8s                          1/1     Running   0
7m23s
telegraf-ds-rj7lw                          1/1     Running   0
7m23s
telegraf-ds-tqrkb                          1/1     Running   0
7m23s
telegraf-rs-9mwgj                          1/1     Running   0
7m23s
telemetry-service-56c49d689b-ffrzx         1/1     Running   0
8m42s
tenancy-767c77fb9d-g9ctv                   1/1     Running   0
8m52s
traefik-5857d87f85-7pmx8                   1/1     Running   0
6m49s
traefik-5857d87f85-cpxgv                   1/1     Running   0
5m34s
traefik-5857d87f85-lvmlb                   1/1     Running   0
4m33s
traefik-5857d87f85-t2xlk                   1/1     Running   0
4m33s
```

```
traefik-5857d87f85-v9wpf                    1/1     Running   0
7m3s
trident-svc-595f84dd78-zb8l6                1/1     Running   0
8m54s
vault-controller-86c94fbf4f-krttq           1/1     Running   0
9m24s
```

4. Vérifiez 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
```

Mettre à niveau des services tiers

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. Voici la séquence de mise à niveau recommandée pour Trafik et Certs-Manager :

1. Configurez ACC-Helm-repo pour mettre à niveau Trafik et Cert-Manager
2. Mettre à jour le service Traefik à l'aide de acc-Helm-repo
3. Mettez à jour le service Cert-Manager

Configurez ACC-Helm-repo pour mettre à niveau Trafik et Cert-Manager

1. Trouvez le `enterprise-helm-repo` Chargé dans votre cache Docker local :

```
docker images enterprise-helm-repo
```

Réponse :

```
REPOSITORY             TAG         IMAGE ID       CREATED        SIZE
enterprise-helm-repo   21.10.218   7a182d6b30f3   20 hours ago   464MB
```

2. Démarrer un conteneur à l'aide de la balise de l'étape précédente :

```
docker run -dp 8082:8080 enterprise-helm-repo:21.10.218
```

Réponse :

```
940436e67fa86d2c4559ac4987b96bb35588313c2c9ddc9cec195651963f08d8
```

3. Ajoutez le Helm Repo à vos référentiels hôtes locaux :

```
helm repo add acc-helm-repo http://localhost:8082/
```

Réponse :

```
"acc-helm-repo" has been added to your repositories
```

4. Enregistrer le script Python suivant en tant que fichier, par exemple, `set_previous_values.py`:

> Ce script Python crée deux fichiers utilisés lors des étapes ultérieures de mise à niveau pour conserver les valeurs Helm.

```
#!/usr/bin/env python3
import json
import os

NAMESPACE = "netapp-acc"

os.system(f"helm get values traefik -n {NAMESPACE} -o json >
traefik_values.json")
os.system(f"helm get values cert-manager -n {NAMESPACE} -o json >
cert_manager_values.json")

# reformat traefik values
f = open("traefik_values.json", "r")
traefik_values = {'traefik': json.load(f)}
f.close()

with open('traefik_values.json', 'w') as output_file:
    json.dump(traefik_values, output_file)

# reformat cert-manager values
f = open("cert_manager_values.json", "r")
cm_values = {'cert-manager': json.load(f)}
f.close()

cm_values['global'] = cm_values['cert-manager']['global']
del cm_values['cert-manager']['global']

with open('cert_manager_values.json', 'w') as output_file:
    json.dump(cm_values, output_file)

print('Done')
```

5. Exécutez le script :

```
python3.7 ./set_previous_values.py
```

Mettre à jour le service Traefik à l'aide de acc-Helm-repo

Vous devez déjà avoir configurer acc-helm-repo avant de terminer la procédure suivante.

1. Téléchargez le pack Traefik à l'aide d'un outil sécurisé de transfert de fichiers, tel que GNU wget :

```
wget http://localhost:8082/traefik-0.2.0.tgz
```

2. Extraire les images :

```
tar -vxzf traefik-0.2.0.tgz
```

3. Appliquer les CRD Traefik :

```
kubectl apply -f ./traefik/charts/traefik/crds/
```

4. Recherchez la version du graphique Helm à utiliser avec votre Traefik mis à niveau :

```
helm search repo acc-helm-repo/traefik
```

Réponse :

```
NAME                                    CHART VERSION   APP VERSION
DESCRIPTION
acc-helm-repo/traefik                 0.2.0           2.5.3       Helm
chart for Traefik Ingress controller
acc-helm-repo/traefik-ingressroutes   0.2.0           2.5.3       A Helm
chart for Kubernetes
```

5. Validez le fichier trafik_values.json pour la mise à niveau :
   a. Ouvrez le fichier trafik_values.json.
   b. Vérifiez si la valeur du est présente `imagePullSecret` légale. S'il est vide, supprimez le texte suivant du fichier :

   ```
   "imagePullSecrets": [{"name": ""}],
   ```

   c. Assurez-vous que l'image de trafik est dirigée vers le bon emplacement et qu'elle porte le nom correct :

   ```
   image: [your_registry_path]/traefik
   ```

6. Mettez à niveau votre configuration Traefik :

```
helm upgrade --version 0.2.0 --namespace netapp-acc -f
traefik_values.json traefik acc-helm-repo/traefik
```

Réponse :

```
Release "traefik" has been upgraded. Happy Helming!
NAME: traefik
LAST DEPLOYED: Mon Oct 25 22:53:19 2021
NAMESPACE: netapp-acc
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

Mettez à jour le service Cert-Manager

> Vous devez déjà avoir terminé le Mise à jour de Trafik et Ajout de acc-Helm-Repo dans Helm avant de terminer la procédure suivante.

1. Recherchez la version du graphique Helm à utiliser avec votre cert-Manager mis à niveau :

   ```
   helm search repo acc-helm-repo/cert-manager
   ```

   Réponse :

   ```
   NAME CHART VERSION APP VERSION DESCRIPTION
   acc-helm-repo/cert-manager 0.3.0 v1.5.4 A Helm chart for cert-manager
   acc-helm-repo/cert-manager-certificates 0.1.0 1.16.0 A Helm chart for
   Kubernetes
   ```

2. Validez le fichier cert_Manager_values.json pour la mise à niveau :
   a. Ouvrez le fichier cert_Manager_values.json.
   b. Vérifiez si la valeur du est présente `imagePullSecret` légale. S'il est vide, supprimez le texte suivant du fichier :

      ```
      "imagePullSecrets": [{"name": ""}],
      ```

   c. Assurez-vous que les trois images du Gestionnaire de certificats sont dirigées vers le bon emplacement et portent les noms corrects.
3. Mettez à niveau votre configuration cert-Manager :

   ```
   helm upgrade --version 0.3.0 --namespace netapp-acc -f
   cert_manager_values.json cert-manager acc-helm-repo/cert-manager
   ```

   Réponse :

```
Release "cert-manager" has been upgraded. Happy Helming!
NAME: cert-manager
LAST DEPLOYED: Tue Nov 23 11:20:05 2021
NAMESPACE: netapp-acc
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

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.

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.

Ce dont vous avez besoin

- Utilisez l'interface utilisateur d'Astra Control Center pour tout supprimer "clusters".

Étapes

1. Supprimer Astra Control Center. L'exemple de commande suivant est basé sur une installation par défaut. Modifiez la commande si vous avez créé des configurations personnalisées.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Résultat :

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

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

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

   Résultat :

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

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

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

Résultat :

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

Trouvez plus d’informations

- "Problèmes connus de désinstallation"