



Utilisez Astra

Astra Control Center

NetApp
February 20, 2023

Table des matières

- Utilisez Astra 1
 - Gérer des applications 1
 - Protégez vos applications 7
 - Afficher l'état des applications et des clusters 14
 - Gérez votre compte 16
 - Gestion des compartiments 22
 - Gérer le stockage back-end 23
 - Contrôle et protection de l'infrastructure 25
 - Mettre à jour une licence existante 33
 - Annuler la gestion des applications et des clusters 33
 - Désinstaller Astra Control Center 34

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.

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 déployées 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, consultez le "[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 **Apps**.
2. Sélectionnez **découvert**.

Name	Ready	Cluster	Group	Discovered	Actions
default			grp_default	2021/06/28 17:36 UTC	Managed
default1			grp1_default	2021/06/28 17:36 UTC	Unmanaged
default2			grp2_default	2021/06/28 17:36 UTC	Unmanaged
netapp-acc-operator			netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
pcloud			pcloud	2021/07/13 12:37 UTC	Unmanaged

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

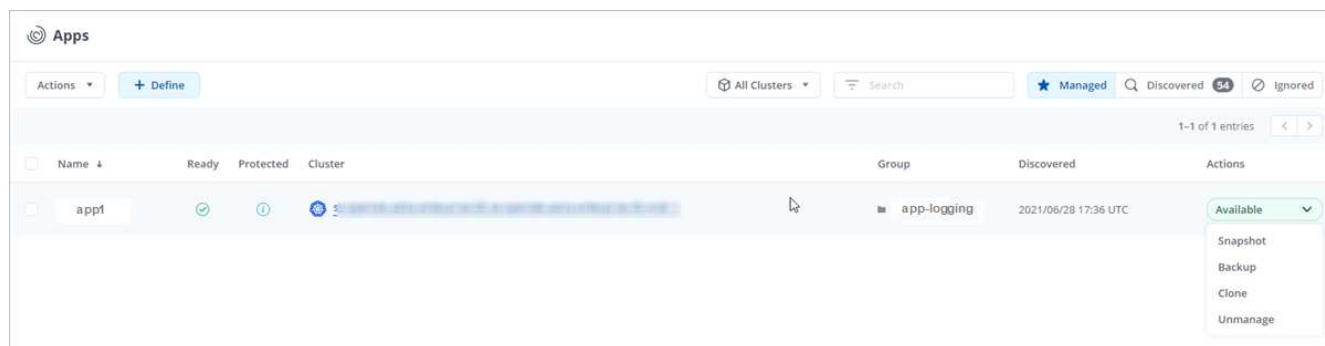
Astra Control présente les applications Helm et les applications étiquetées sur mesure dans l'espace de noms. Si des étiquettes Helm sont disponibles, elles sont désignées par une icône de balise.

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

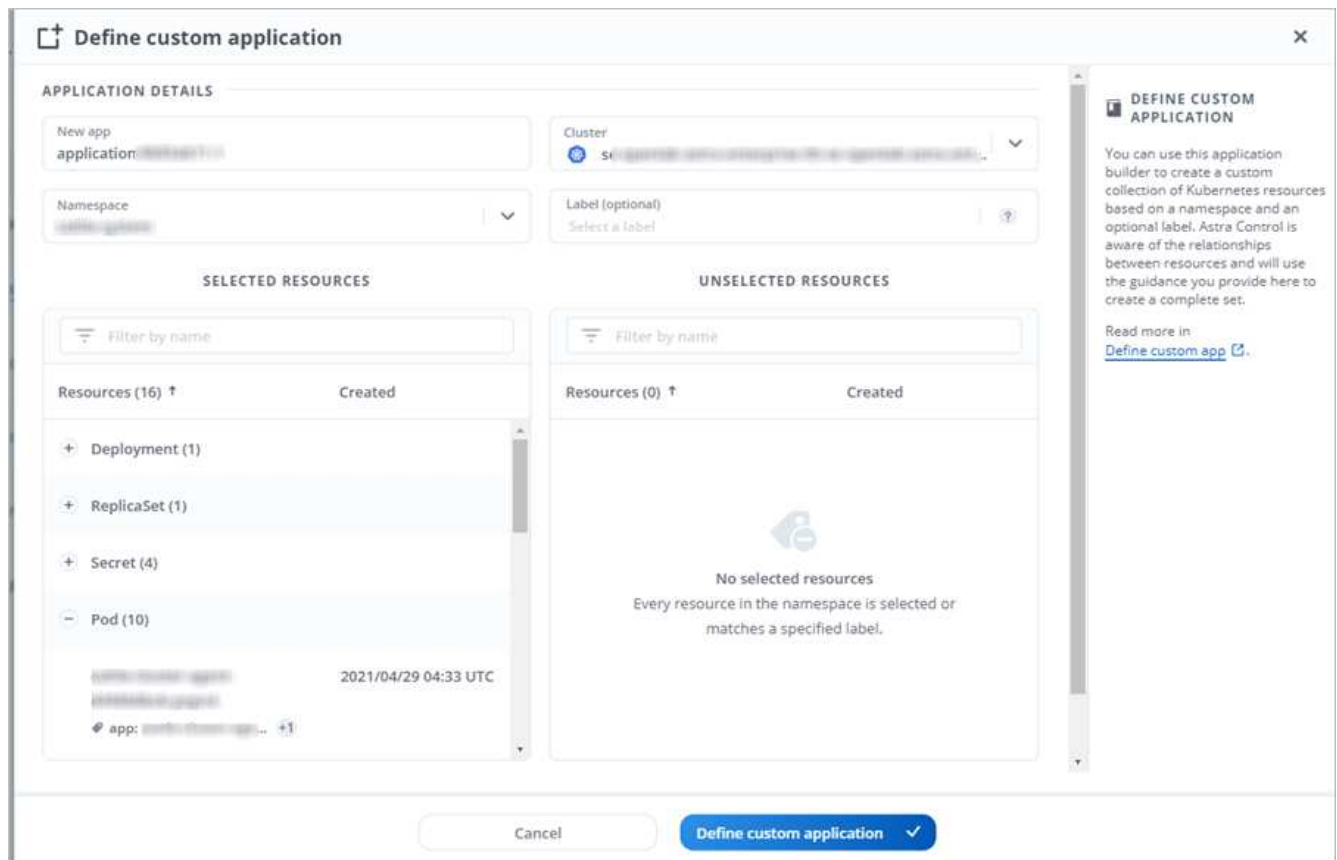
Les applications que vous avez choisi de gérer sont désormais disponibles dans l'onglet **Managed**. Toutes les applications ignorées seront transférées vers l'onglet **ignoré**. Idéalement, l'onglet découvert affiche zéro application, de sorte qu'à mesure que de nouvelles applications sont installées,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

Name	Ready	Cluster	Discovery Date	Status
se-...	✓	se-...	2021/06/28 17:36 UTC	Managed
se-...	✓	se-...	2021/06/28 17:36 UTC	Unmanaged
se-...	✓	se-...	2021/06/28 17:36 UTC	Unmanaged
default	ⓘ	se-...	2021/07/22 18:22 UTC	Discovering

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 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 cliquez sur **+ 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 clique sur le bouton **+ Define** de 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

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 "[L'API 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
```

Snapshots et sauvegardes

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

Une *backup* est stockée dans le magasin d'objets externe. Les sauvegardes peuvent être plus lentes que les snapshots locaux. Vous pouvez migrer une application en restaurant sa sauvegarde sur un autre cluster. Vous pouvez également choisir une période de conservation plus longue pour les sauvegardes.



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.

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.

Étapes

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

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

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

Configure protection policy
STEP 1/2: DETAILS
✕

PROTECTION SCHEDULE

🕒 Hourly

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

🕒 Daily

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

🕒 Weekly

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

🕒 Monthly

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

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

Select Weekday(s) (optional)

Monday X

Time (UTC) (optional)

02:00

– Snapshots to keep +

26

– Backups to keep +

0

BACKUP DESTINATION

Bucket

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

OVERVIEW

Schedule and retention

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

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

Read more in [Protection policies](#)

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

Cancel

Review →

5. Cliquez sur **Revue**.

6. Cliquez sur **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. Cliquez sur **Apps**.
2. Cliquez sur la liste déroulante de la colonne **actions** pour l'application souhaitée.
3. Cliquez sur **instantané**.
4. Personnalisez le nom du snapshot, puis cliquez sur **Review**.
5. Examinez le résumé de l'instantané et cliquez sur **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. Cliquez sur **Apps**.
2. Cliquez sur la liste déroulante de la colonne **actions** pour l'application souhaitée.
3. Cliquez sur **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. Cliquez sur **Revue**.
8. Vérifiez le résumé de la sauvegarde et cliquez sur **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 défectueuse, "[Utilisez l'API 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. Cliquez sur **Apps**, puis sur le nom d'une application.
2. Cliquez sur **Data protection**.

Les snapshots s'affichent par défaut.

3. Cliquez sur **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. Cliquez sur **Apps**, puis sur le nom d'une application.
2. Cliquez sur **Data protection**.
3. Cliquez sur la liste déroulante de la colonne **actions** pour l'instantané souhaité.
4. Cliquez sur **Supprimer le snapshot**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis cliquez sur **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 Astra"](#).

1. Cliquez sur **Apps**, puis sur le nom d'une application.
2. Cliquez sur **Data protection**.
3. Cliquez sur **backups**.
4. Cliquez sur la liste déroulante de la colonne **actions** pour la sauvegarde souhaitée.
5. Cliquez sur **Supprimer la sauvegarde**.
6. Tapez le mot "supprimer" pour confirmer la suppression, puis cliquez sur **Oui, Supprimer la sauvegarde**.

Résultat

Astra Control Center supprime la sauvegarde.

Restaurez les applications

Astra Control Center peut restaurer votre application à partir d'un snapshot ou d'une sauvegarde. Les sauvegardes de stockage persistant et les snapshots sont transférés depuis votre magasin d'objets. La restauration à partir d'un Snapshot existant vers le même cluster est donc plus rapide que d'autres méthodes. Vous pouvez utiliser l'interface utilisateur Astra ou ["L'API 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. Cliquez sur **Apps**, puis sur le nom d'une application.
2. Cliquez sur **protection des données**.
3. Si vous souhaitez effectuer une restauration à partir d'un instantané, conservez l'icône **snapshots** sélectionnée. Sinon, cliquez sur l'icône **backups** pour effectuer une restauration à partir d'une sauvegarde.
4. Cliquez sur la liste déroulante de la colonne **actions** pour l'instantané ou la sauvegarde à partir duquel vous souhaitez restaurer.
5. Cliquez sur **Restaurer l'application**.
6. **Détails de restauration** : spécifiez les détails de la restauration :
 - Entrez un nom et un espace de noms pour l'application.



Si vous restaurez une application qui a été supprimée, choisissez un nom et un espace de noms différents pour l'application que le nom d'origine. Si le nom de l'application restaurée est identique à celui de l'application supprimée, l'opération de restauration échoue.

- Choisissez le cluster de destination de l'application.
 - Cliquez sur **Revue**.
7. **Résumé de restauration** : consultez les détails de l'action de restauration et cliquez sur **Restaurer**.

Résultat

Astra Control Center restaure l'application en fonction des informations que vous avez fournies.



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 "[L'API Astra](#)" pour le clonage et migration des applications.



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. Cliquez sur **Apps**.
2. Effectuez l'une des opérations suivantes :
 - Cliquez sur la liste déroulante de la colonne **actions** pour l'application souhaitée.
 - Cliquez sur le nom de l'application souhaitée et sélectionnez la liste déroulante d'état en haut à droite de la page.
3. Cliquez sur **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. Cliquez sur **Revue**.
7. **Résumé du clone** : consultez les détails du clone et cliquez sur **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 dans la page **Apps**.



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 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.

The screenshot shows the Astra Control Center Dashboard. The left sidebar contains navigation options: Dashboard, Apps, Clusters, Backends, Buckets, Account, Activity, and Support. The main content area displays a 'Welcome To Astra' message and a license expiration notice. Below this is a 'Resource summary' section with three cards:

Resource Type	Managed Count	Health Status	Discovery Status
Apps	4	All healthy (green checkmark)	Not fully protected (4 icons), Discovered (48)
Clusters	2	All healthy (green checkmark)	None
Storage backends	2	All healthy (green checkmark)	Discovered (0)

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

La mosaïque **Apps** 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 **Apps**, puis le nom d'une application.
2. Cliquez autour de pour trouver 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 **Apps** sous **Resource Summary**, vous pouvez sélectionner les applications gérées, qui vous permettent d'accéder à la page **Apps**. Après avoir accédé à la page **Apps**, 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 "[L'API 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**, cliquez sur **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. Cliquez sur **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. Cliquez sur l'icône utilisateur en haut à droite de l'écran.
2. Sélectionnez **Profile**.
3. Cliquez sur 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. Cliquez sur **Modifier le 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**, cliquez sur **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. Cliquez sur **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**, cliquez sur **compte**.
2. Dans l'onglet **utilisateurs**, sélectionnez la liste déroulante dans la colonne **rôle** de l'utilisateur.
3. Sélectionnez un nouveau rôle, puis cliquez sur **Modifier 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**, cliquez sur **compte**.
2. Dans l'onglet **Users**, cochez la case de la ligne de chaque utilisateur que vous souhaitez supprimer.
3. Cliquez sur **actions** et sélectionnez **Supprimer utilisateur/s**.
4. Lorsque vous y êtes invité, confirmez la suppression en saisissant le mot "supprimer", puis cliquez sur **Oui, Supprimer l'utilisateur**.

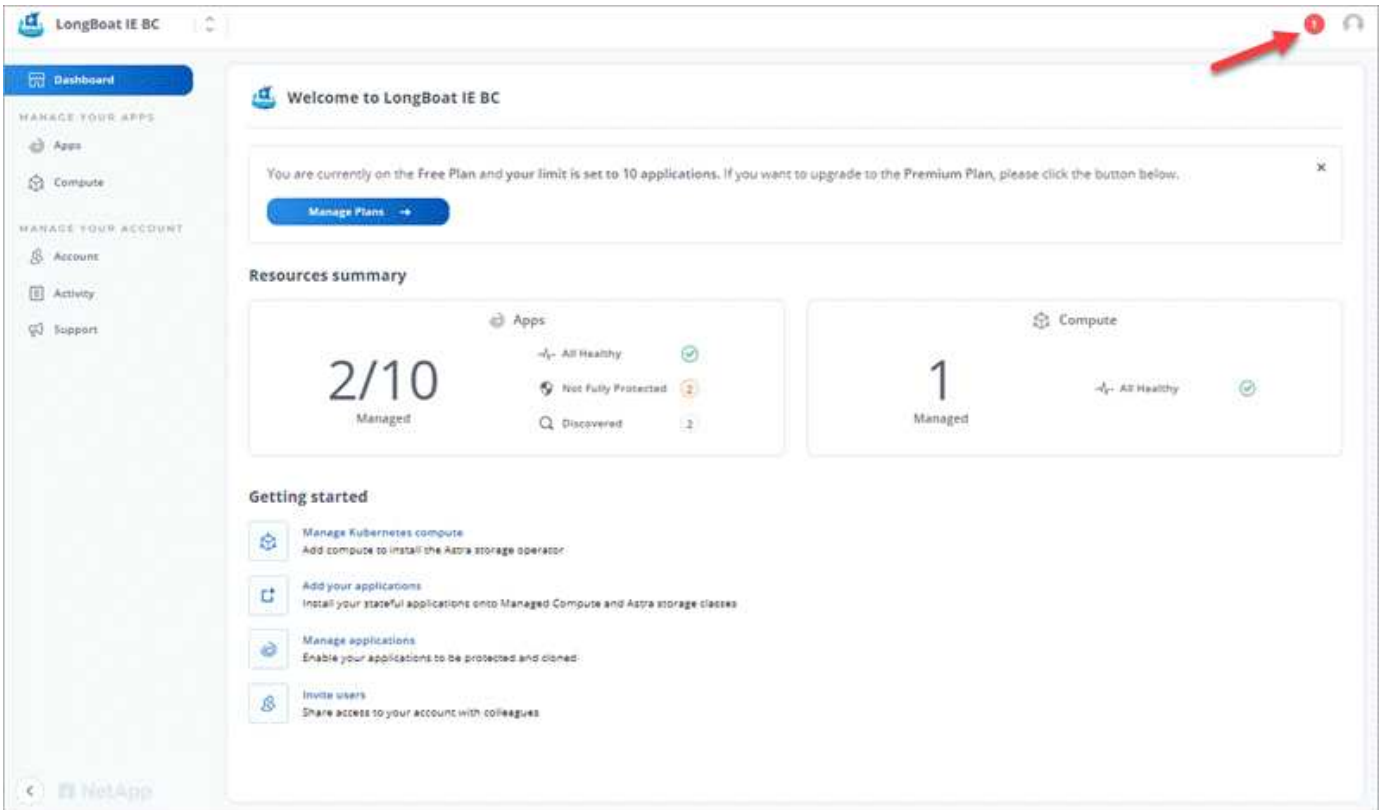
Résultat

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.

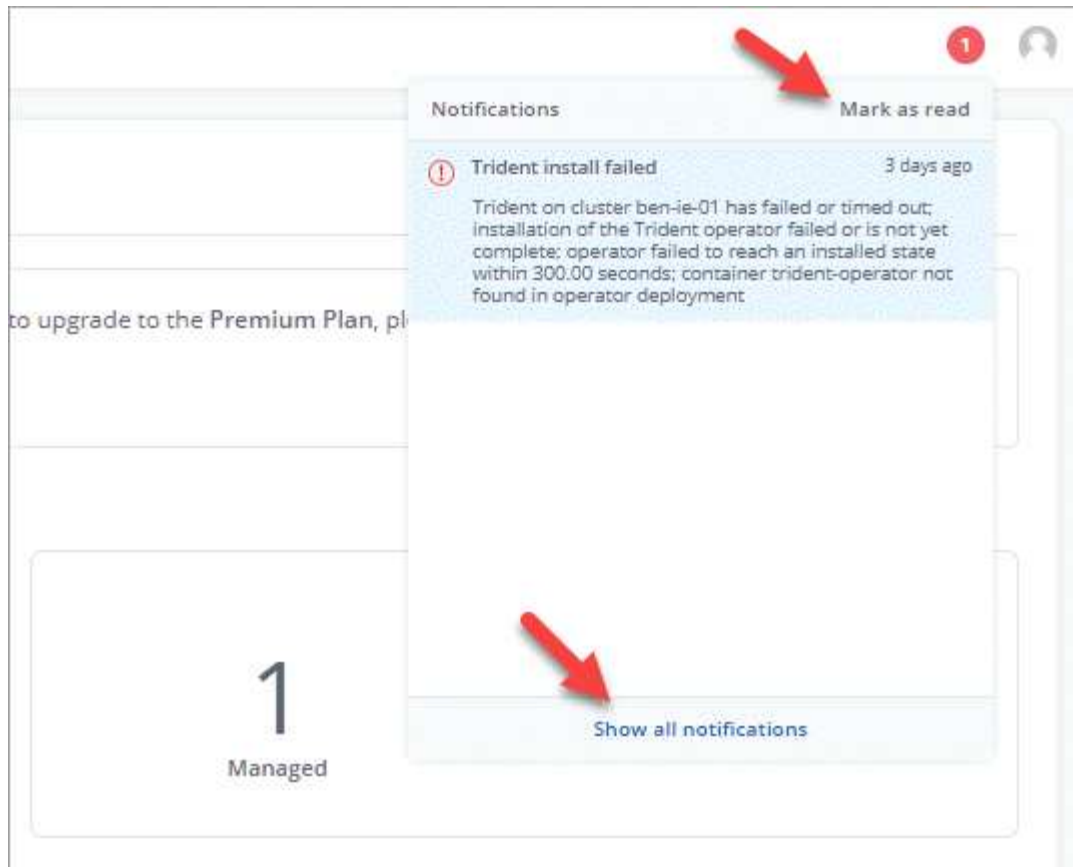
Le nombre de notifications non lues est disponible dans le coin supérieur droit de l'interface :



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. Cliquez sur le nombre de notifications non lues dans le coin supérieur droit.



2. Examinez les notifications, puis cliquez sur **Marquer comme lu** ou **Afficher toutes les notifications**.

Si vous avez cliqué sur **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, cliquez sur **action** et sélectionnez **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

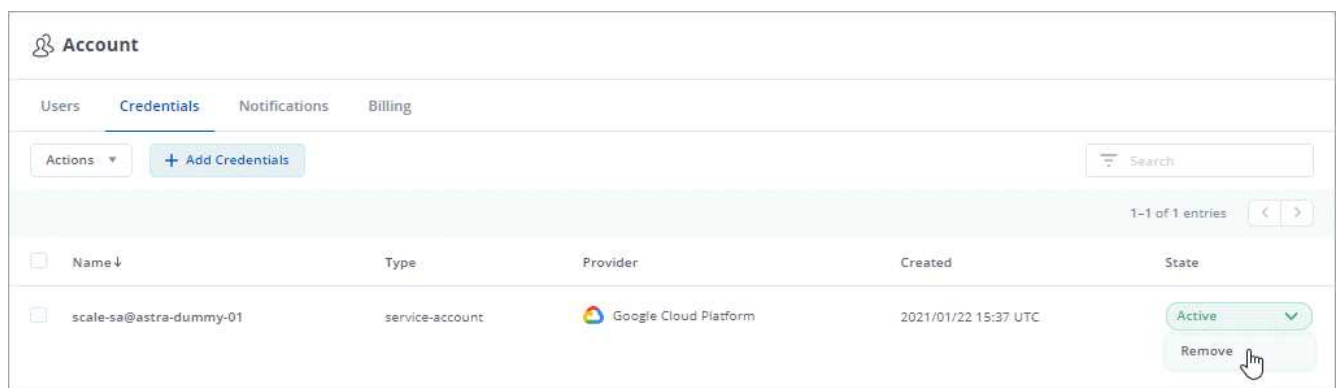
Supprimez les informations d'identification d'un compte à tout moment. Vous ne devez supprimer les informations d'identification qu'après "[annuler la gestion de tous les clusters associés](#)".



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. Cliquez sur **compte > informations d'identification**.
2. Cliquez sur la liste déroulante de la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.



4. Tapez le mot "supprimer" pour confirmer la suppression, puis cliquez sur **Oui, Supprimer les informations d'identification**.

Résultat

Astra Control Center supprime les informations d'identification du compte.

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 "[L'API 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**, cliquez sur 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 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 type de fournisseur de compartiment approprié avec les identifiants appropriés pour ce fournisseur. Par exemple, l'interface utilisateur accepte NetApp ONTAP S3 comme type avec 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 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, 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](#)"
- <https://docs.netapp.com/fr-fr/astra-control-center-2108/Annuler la gestion d&.html#8217;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.

The screenshot displays the Astra web interface for a storage system named "Umeng-Aff300-05-06". The interface is divided into several sections:

- Navigation Sidebar:** Includes "Dashboard", "MANAGE YOUR APPS" (Apps, Clusters), "MANAGE YOUR STORAGE" (Backends, Buckets), and "MANAGE YOUR ACCOUNT" (Account, Activity, Support).
- Storage Backend Status:** Shows a "Healthy" status with a green checkmark.
- Capacity (Physical):** A gauge showing 37.3% usage, with 7.93/21.28 TiB remaining.
- Performance (Last 24 hrs):** A line graph showing throughput in MB/s over time.
- BASIC INFORMATION:** Type: ONTAP 9.7.0, Cloud: private, Credentials: Updated 2021/07/28 21:44 UTC.
- NETWORK:** Cluster management IP address: 10.10.10.10.
- Persistent volumes:** A table listing 14 entries with columns for Name, Persistent volume, Capacity, App/s, Cluster/s, and Cloud.

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

3. Pour accéder directement à Cloud Insights, cliquez sur 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. Sélectionner le système de stockage 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 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.



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 pouvez vous connecter à Cloud Insights à partir d'ici.

Ajouter un serveur proxy

Si le réseau sur lequel vous exécutez Astra Control Center requiert un proxy pour vous connecter à Internet (pour télécharger des bundles de support vers le site de support NetApp ou établir une connexion avec Cloud Insights), vous devez configurer un serveur proxy dans Astra Control Center.



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

Étapes

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



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected ▼

Connect

4. Entrez le nom du serveur proxy ou l'adresse IP et le numéro du port proxy.
5. Si votre serveur proxy nécessite une authentification, cochez la case et 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 > Connexions** indique qu'elle est connectée et affiche le nom du serveur.



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Connected ▼

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.

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 "[ici](#)".

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.



CLOUD INSIGHTS

Monitor and analyze your applications and the infrastructure they run on.

Disconnected

Connect

- 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](#)".

- Pour obtenir le "[Jeton API](#)", connectez-vous à l'URL de votre locataire Cloud Insights.
- Dans Cloud Insights, générez un jeton API de type **lecture seule**.

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission
<input type="checkbox"/>	astra_...		...zBskB1	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...xK0eL_	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...2_A6HP	All Categories	Read Only
<input type="checkbox"/>	astra		...8BTKYY	All Categories	Read/Write

- Copiez la clé **lecture seule**. Vous devrez la coller dans la fenêtre du centre de contrôle Astra pour activer la connexion Cloud Insights.
- Dans Cloud Insights, générez un jeton API de type **lecture/écriture**.
- Copiez la clé **lecture/écriture**. Vous devrez le coller dans la fenêtre Centre de contrôle Astra **connexion Cloud Insights**.



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.

- 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.

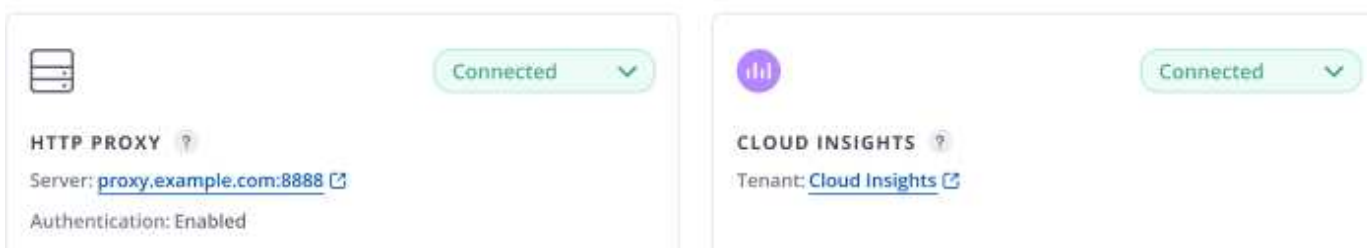
Afficher les données dans Cloud Insights

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.

Account

Users Credentials Notifications Billing Licenses API Tokens **Connections**

EXTERNAL ?



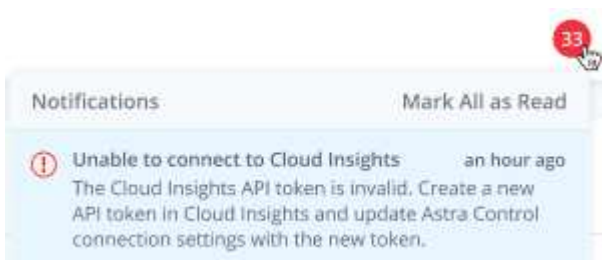
HTTP PROXY ?
Server: [proxy.example.com:8888](#)
Authentication: Enabled

Connected


CLOUD INSIGHTS ?
Tenant: [Cloud Insights](#)

Connected

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.

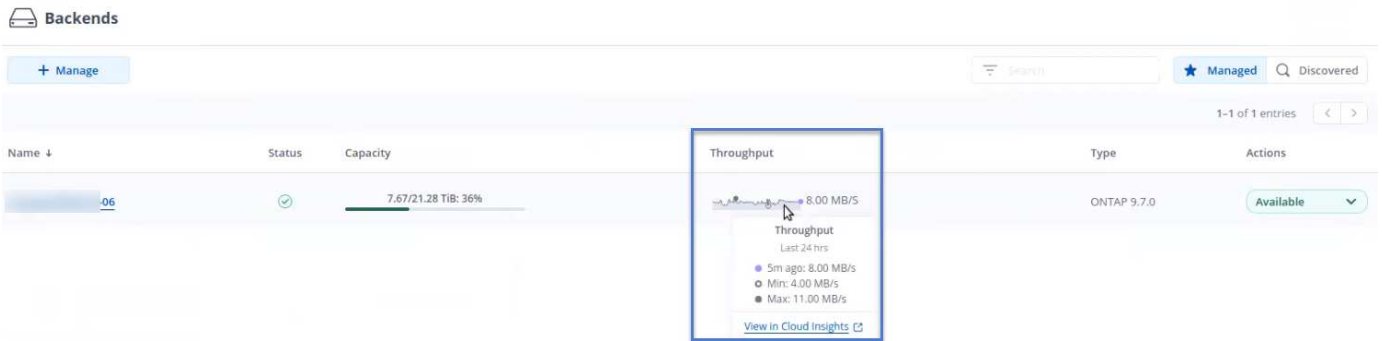


Notifications Mark All as Read

 Unable to connect to Cloud Insights an hour ago
The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.

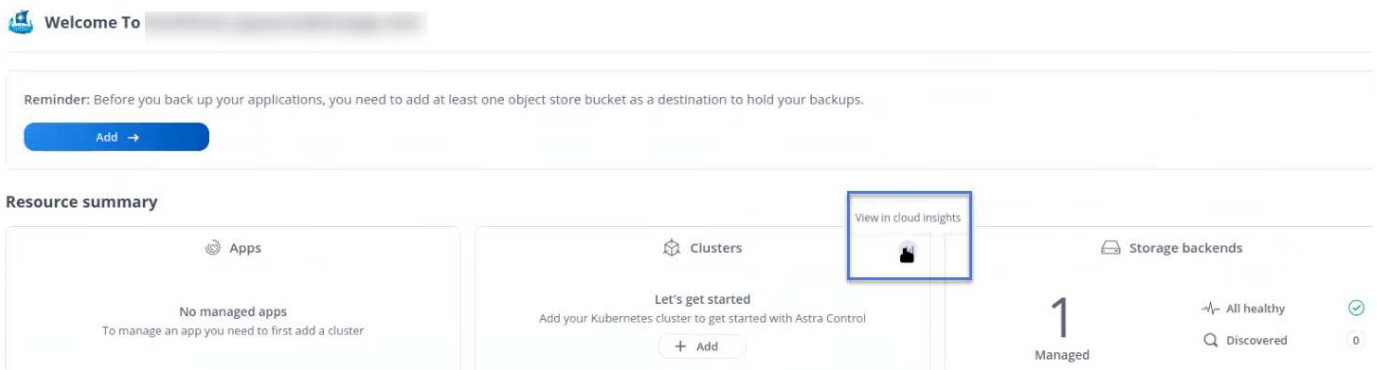
Vous pouvez également trouver les mêmes informations sous **compte > Notifications**.

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



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

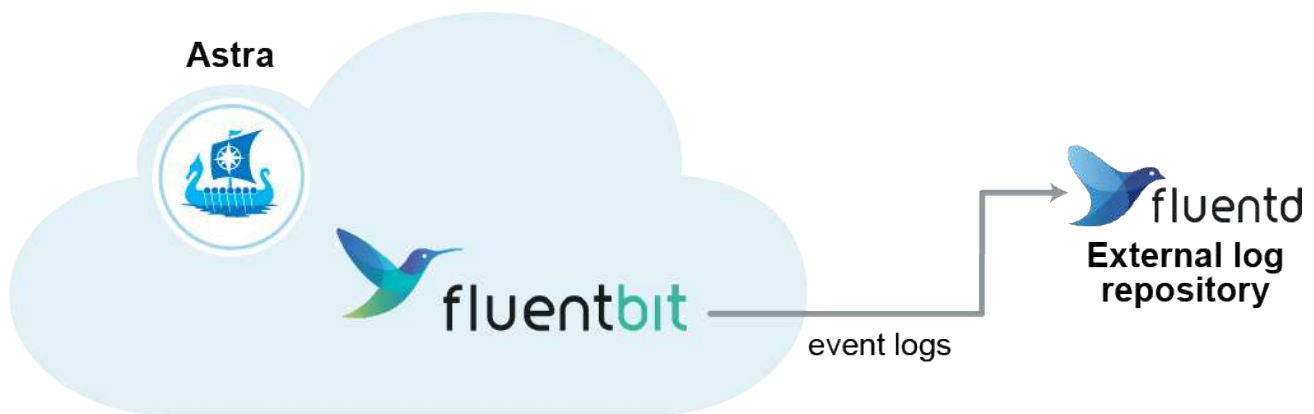
Cloud Insights.

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.



FLUENTD

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

- Entrez l'adresse IP de l'hôte, le numéro de port et la clé partagée pour votre serveur Fluentd.
- 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

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

Désactivez la connexion Fluentd

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

Étapes

- Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.
- Sélectionnez **compte > connexions**.
- Sélectionnez **déconnecter** dans la liste déroulante pour désactiver la connexion.
- 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 "[L'API 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**, cliquez sur 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 **Apps**.
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`.

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"](#)

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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