



Utilisez Astra Control Center

Astra Control Center

NetApp
August 11, 2025

Sommaire

Utilisez Astra Control Center	1
Commencez à gérer les applications	1
De gestion des applications	1
Méthodes d'installation d'applications prises en charge	1
Installez les applications sur votre cluster	2
Définir les applications	2
Qu'en est-il des espaces de noms système	6
Exemple : politique de protection distincte pour différentes versions	6
Trouvez plus d'informations	6
Protégez vos applications	7
Présentation de la protection	7
Protéger les applications avec les snapshots et les sauvegardes	8
Restaurez les applications	15
Réplication d'applications entre les systèmes back-end avec la technologie SnapMirror	20
Cloner et migrer les applications	28
Gérer les crochets d'exécution de l'application	30
Protégez Astra Control Center à l'aide d'Astra Control Center	40
Surveillez l'état des applications et des clusters	49
Affichez un récapitulatif de l'état des applications et du cluster	49
Afficher l'état de santé des clusters et gérer les classes de stockage	50
Afficher l'état de santé et les détails d'une application	51
Gérez votre compte	52
Gérez les utilisateurs et les rôles locaux	52
Gérer l'authentification à distance	55
Gérez des utilisateurs et des groupes distants	58
Afficher et gérer les notifications	60
Ajouter et supprimer des informations d'identification	60
Surveillez l'activité des comptes	61
Mettre à jour une licence existante	62
Gestion des compartiments	62
Modifier un godet	63
Définir le compartiment par défaut	64
Faire pivoter ou supprimer les identifiants de compartiment	64
Déposer un godet	65
Trouvez plus d'informations	65
Gérer le stockage back-end	65
Afficher les détails du système back-end	66
Modifier les détails de l'authentification du système back-end du stockage	67
Gérez un système back-end de stockage découvert	68
Annuler la gestion d'un système back-end	68
Retirer un système back-end	68
Trouvez plus d'informations	69
Surveillez les tâches en cours d'exécution	69

Surveillez l'infrastructure avec des connexions Cloud Insights, Prometheus ou Fluentd	70
Ajoutez un serveur proxy pour les connexions à Cloud Insights ou au site de support NetApp	70
Connectez-vous à Cloud Insights	71
Connectez-vous à Prometheus	75
Connectez-vous à Fluentd	77
Annuler la gestion des applications et des clusters	79
Annuler la gestion d'une application	79
Annuler la gestion d'un cluster	79
Mettez à niveau Astra Control Center	80
Téléchargez et extrayez Astra Control Center	82
Retirez le plug-in NetApp Astra kubectl et réinstallez-le	83
Ajoutez les images à votre registre local	84
Poser le conducteur du centre de commande Astra mis à jour	86
Mettez à niveau Astra Control Center	90
Vérifiez l'état du système	92
Activez le mécanisme de provisionnement Astra Control	92
(Étape 1) Téléchargez et extrayez Astra Control Provisioner	93
(Étape 2) Activer le provisionnement Astra Control dans Astra Trident	96
Résultat	99
Désinstaller Astra Control Center	100
Dépannage des problèmes de désinstallation	101
Trouvez plus d'informations	103

Utilisez Astra Control Center

Commencez à gérer les applications

Après vous "[Ajoutez un cluster à la gestion Astra Control](#)", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour définir les applications et leurs ressources.

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

De gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer des applications à l'aide d'Astra Control Center, vous avez besoin soit de la licence d'évaluation Astra Control Center intégrée, soit d'une licence complète.
- **Espaces de noms** : les applications peuvent être définies au sein d'un ou plusieurs espaces de noms spécifiés sur un même cluster à l'aide d'Astra Control. Une application peut contenir des ressources couvrant plusieurs espaces de noms au sein d'un même cluster. Astra Control ne prend pas en charge la possibilité de définir des applications entre plusieurs clusters.
- **Classe de stockage** : si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Ressources Kubernetes** : les applications qui utilisent des ressources Kubernetes non collectées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control collecte les ressources Kubernetes suivantes :

ClusterRole	ClusterRoleBinding	ConfigMap
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

Méthodes d'installation d'applications prises en charge

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

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

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

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

Voici quelques applications opérateur qui suivent ces modèles :

- ["Apache K8ssandra"](#)



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

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

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

Installez les applications sur votre cluster

Après vous l'avez ["a ajouté votre cluster"](#) Avec Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application dont la portée est étendue à un ou plusieurs espaces de noms peut être gérée.

Définir les applications

Une fois qu'Astra Control détecte les espaces de noms sur vos clusters, vous pouvez définir les applications que vous souhaitez gérer. Vous pouvez choisir [gérer une application couvrant un ou plusieurs espaces de noms](#) ou [gérer la totalité d'un namespace comme une seule application](#). La granularité est en effet au niveau de granularité requis pour les opérations de protection des données.

Bien qu'Astra Control vous permet de gérer séparément les deux niveaux de la hiérarchie (l'espace de noms et les applications dans cet espace de noms ou les espaces de noms d'extension), il est recommandé de choisir l'un ou l'autre. Les actions que vous prenez dans Astra Control peuvent échouer si les actions ont lieu en même temps au niveau de l'espace de noms et de l'application.



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

Avant de commencer

- Un cluster Kubernetes ajouté à Astra Control.
- Une ou plusieurs applications installées sur le cluster. [En savoir plus sur les méthodes d'installation d'applications prises en charge](#).
- Espaces de noms existants sur le cluster Kubernetes que vous avez ajouté à Astra Control.
- (Facultatif) Étiquette Kubernetes de toute ["Ressources Kubernetes prises en charge"](#).



Une étiquette est une paire clé/valeur que vous pouvez attribuer aux objets Kubernetes pour identification. Elles facilitent le tri, l'organisation et la recherche des objets Kubernetes. Pour en savoir plus sur les étiquettes Kubernetes, ["Consultez la documentation officielle Kubernetes"](#).

Description de la tâche

- Avant de commencer, vous devez également comprendre ["gestion des espaces de noms standard et système"](#).
- Si vous prévoyez d'utiliser plusieurs espaces de noms avec vos applications dans Astra Control, ["modifier les rôles utilisateur avec des contraintes d'espace de noms"](#) Après la mise à niveau vers une version Astra Control Center avec prise en charge de plusieurs espaces de noms.
- Pour obtenir des instructions sur la gestion des applications à l'aide de l'API Astra Control, reportez-vous au ["Informations sur l'automatisation et les API d'Astra"](#).

Options de gestion des applications

- [Définissez les ressources à gérer en tant qu'application](#)
- [Définissez un espace de noms à gérer en tant qu'application](#)

Définissez les ressources à gérer en tant qu'application

Vous pouvez spécifier le ["Ressources Kubernetes qui constituent une application"](#) Que vous voulez gérer avec Astra Control. La définition d'une application vous permet de regrouper des éléments de votre cluster Kubernetes dans une seule application. Cette collection de ressources Kubernetes est organisée par critères d'espace de noms et de sélecteur d'étiquettes.

La définition d'une application vous offre un contrôle plus granulaire sur les éléments à inclure dans une opération Astra Control, notamment le clonage, les snapshots et les sauvegardes.



Lors de la définition d'applications, assurez-vous de ne pas inclure de ressource Kubernetes dans plusieurs applications avec des règles de protection. Le chevauchement des règles de protection sur les ressources Kubernetes peut entraîner des conflits de données. [En savoir plus dans un exemple](#).

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

Vous pouvez importer des ressources de cluster associées aux ressources d'espace de noms en plus de celles incluses automatiquement dans Astra Control. Vous pouvez ajouter une règle qui inclura des ressources d'un groupe, un type, une version et, éventuellement, une étiquette. Vous voudrez peut-être le faire si certaines ressources qu'Astra Control n'incluent pas automatiquement.

Vous ne pouvez exclure aucune des ressources à périmètre de cluster qui sont automatiquement incluses par Astra Control.

Vous pouvez ajouter les éléments suivants `apiVersions` (Qui sont les groupes combinés avec la version API) :

Type de ressource	ApiVersions (groupe + version)
ClusterRole	rbac.authorization.k8s.io/v1
ClusterRoleBinding	rbac.authorization.k8s.io/v1
CustomResource	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
CustomResourceDefinition	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
MutatingWebhookConfiguration	admissionregistration.k8s.io/v1
ValidatingWebhookConfiguration	admissionregistration.k8s.io/v1

Étapes

1. Dans la page applications, sélectionnez **définir**.
2. Dans la fenêtre **define application**, entrez le nom de l'application.
3. Choisissez le cluster sur lequel votre application s'exécute dans la liste déroulante **Cluster**.
4. Choisissez un espace de nom pour votre application dans la liste déroulante **namespace**.



Les applications peuvent être définies au sein d'un ou plusieurs espaces de noms spécifiés sur un même cluster à l'aide d'Astra Control. Une application peut contenir des ressources couvrant plusieurs espaces de noms au sein d'un même cluster. Astra Control ne prend pas en charge la possibilité de définir des applications entre plusieurs clusters.

5. (Facultatif) Indiquez une étiquette pour les ressources Kubernetes dans chaque espace de noms. Vous pouvez spécifier un seul libellé ou un seul critère de sélection d'étiquette (requête).



Pour en savoir plus sur les étiquettes Kubernetes, "[Consultez la documentation officielle Kubernetes](#)".

6. (Facultatif) Ajouter des espaces de noms supplémentaires pour l'application en sélectionnant **Ajouter un espace de noms** et en choisissant l'espace de noms dans la liste déroulante.
7. (Facultatif) Entrez des critères de sélection d'étiquette ou d'étiquette pour tout espace de noms supplémentaire que vous ajoutez.
8. (Facultatif) pour inclure des ressources à périmètre de cluster en plus de celles qu'Astra Control inclut automatiquement, cochez **inclure des ressources supplémentaires à périmètre de cluster** et

complétez les éléments suivants :

- a. Sélectionnez **Ajouter inclure règle**.
- b. **Groupe** : dans la liste déroulante, sélectionnez le groupe de ressources API.
- c. **Type** : dans la liste déroulante, sélectionnez le nom du schéma d'objet.
- d. **Version** : saisissez la version de l'API.
- e. **Sélecteur d'étiquettes** : si vous le souhaitez, incluez un libellé à ajouter à la règle. Cette étiquette est utilisée pour récupérer uniquement les ressources correspondant à cette étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe.
- f. Vérifiez la règle créée en fonction de vos entrées.
- g. Sélectionnez **Ajouter**.



Vous pouvez créer autant de règles de ressources à périmètre cluster que vous le souhaitez. Les règles apparaissent dans le Résumé de l'application définir.

9. Sélectionnez **définir**.

10. Après avoir sélectionné **définir**, répétez le processus pour les autres applications, selon les besoins.

Une fois que vous avez terminé de définir une application, celle-ci s'affiche dans `Healthy` Dans la liste des applications de la page applications. Vous pouvez désormais le cloner et créer des sauvegardes et des snapshots.



Il se peut que l'application que vous venez d'ajouter comporte une icône d'avertissement sous la colonne protégé, indiquant qu'elle n'est pas encore sauvegardée et qu'elle n'est pas planifiée pour les sauvegardes.



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

Pour afficher les ressources ajoutées à cette application, sélectionnez l'onglet **Ressources**. Sélectionnez le numéro après le nom de la ressource dans la colonne ressource ou entrez le nom de la ressource dans la recherche pour voir les ressources supplémentaires comprises dans la portée du cluster.

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

Vous pouvez ajouter toutes les ressources Kubernetes dans un namespace à la gestion d'Astra Control en définissant les ressources de ce namespace comme une application. Cette méthode est préférable à définir des applications individuellement si vous avez l'intention de gérer et de protéger toutes les ressources d'un espace de noms particulier de la même manière et à intervalles communs.

Étapes

1. Sur la page clusters, sélectionnez un cluster.
2. Sélectionnez l'onglet **espaces de noms**.
3. Sélectionnez le menu actions de l'espace de noms contenant les ressources d'application que vous souhaitez gérer et sélectionnez **définir comme application**.



Si vous souhaitez définir plusieurs applications, sélectionnez dans la liste Namespaces et sélectionnez le bouton **actions** dans le coin supérieur gauche et sélectionnez **définir comme application**. Cela définira plusieurs applications individuelles dans leurs espaces de noms individuels. Pour les applications à espace de noms multiples, voir [Définissez les ressources à gérer en tant qu'application](#).



Cochez la case **Afficher les espaces de noms système** pour afficher les espaces de noms système qui ne sont généralement pas utilisés dans la gestion des applications par défaut. Show system namespaces ["En savoir plus"](#).

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

Qu'en est-il des espaces de noms système

Astra Control détecte également les espaces de noms système sur un cluster Kubernetes. Nous ne vous montrons pas ces espaces de noms système par défaut, car il est rare qu'il soit nécessaire de sauvegarder les ressources d'applications système.

Vous pouvez afficher les espaces de noms système à partir de l'onglet espaces de noms d'un cluster sélectionné en cochant la case **Afficher les espaces de noms système**.

 Show system namespaces

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

Exemple : politique de protection distincte pour différentes versions

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

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

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

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

Trouvez plus d'informations

- ["Utilisez l'API de contrôle Astra"](#)
- ["Annuler la gestion d'une application"](#)

Protégez vos applications

Présentation de la protection

Vous pouvez créer des sauvegardes, des clones, des copies Snapshot et des règles de protection pour vos applications à l'aide d'Astra Control Center. La sauvegarde de vos applications aide vos services et vos données associées à être aussi disponibles que possible. En cas d'incident, la restauration à partir d'une sauvegarde permet une restauration complète d'une application et de ses données, avec une interruption minimale. Les sauvegardes, les clones et les snapshots contribuent à vous protéger contre les menaces classiques, comme les ransomwares, la perte accidentelle de données et les incidents environnementaux. ["Découvrez les types de protection des données disponibles dans Astra Control Center et le moment de les utiliser"](#).

En outre, vous pouvez répliquer des applications sur un cluster distant en préparation de la reprise après incident.

Workflow de protection des applications

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

[Une seule] Protégez toutes vos applications

Pour être sûr que vos applications sont immédiatement protégées, ["créez une sauvegarde manuelle de toutes les applications"](#).

[Deux] Configurez une stratégie de protection pour chaque application

Pour automatiser les sauvegardes et snapshots futurs, ["configurez une stratégie de protection pour chaque application"](#). Par exemple, vous pouvez commencer avec des sauvegardes hebdomadaires et des snapshots quotidiens, et en conserver un mois pour les deux. Il est fortement recommandé d'automatiser les sauvegardes et les snapshots avec une règle de protection par rapport aux sauvegardes et snapshots manuels.

[Trois] Ajuster les règles de protection

À mesure que les applications et leurs modèles d'utilisation évoluent, ajustez les règles de protection selon les besoins pour bénéficier d'une protection optimale.

[Quatre] Répliquer les applications sur un cluster distant

["Réplication d'applications"](#) À un cluster distant à l'aide de la technologie NetApp SnapMirror. Astra Control réplique les copies Snapshot sur un cluster distant, offrant une fonctionnalité de reprise après incident asynchrone.

[Cinq] En cas d'incident, restaurez vos applications avec la dernière sauvegarde ou réplification sur un système distant

En cas de perte de données, vous pouvez effectuer une restauration par ["restauration de la dernière sauvegarde"](#) d'abord pour chaque application. Vous pouvez alors restaurer le dernier snapshot (si disponible). Vous pouvez également utiliser la réplification sur un système distant.

Protéger les applications avec les snapshots et les sauvegardes

Protégez toutes les applications en effectuant des copies Snapshot et des sauvegardes à l'aide d'une stratégie de protection automatisée ou ad hoc. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou "[API de contrôle Astra](#)" pour protéger les applications.

Description de la tâche

- **Helm Deployed apps** : si vous utilisez Helm pour déployer des applications, Astra Control Center nécessite Helm version 3. La gestion et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.
- * (Clusters OpenShift uniquement) Ajouter des stratégies* : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

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

- [Configurer une règle de protection](#)
- [Créer un snapshot](#)
- [Créer une sauvegarde](#)
- [Sauvegardez et restaurez les opérations ontap-nas](#)
- [Créer une sauvegarde immuable](#)
- [Afficher les snapshots et les sauvegardes](#)
- [Supprimer les instantanés](#)
- [Annuler les sauvegardes](#)
- [Supprimer les sauvegardes](#)

Configurer une règle de protection

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

Si vous avez besoin de sauvegardes ou de snapshots pour qu'ils s'exécutent plus fréquemment qu'une fois par heure, vous pouvez "[Utilisez l'API REST Astra Control pour créer des snapshots et des sauvegardes](#)".



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



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

Étapes

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

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

Lorsque vous définissez un niveau de conservation pour les sauvegardes, vous pouvez choisir le compartiment dans lequel vous souhaitez stocker les sauvegardes.

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

The screenshot shows the 'Configure protection policy' interface. The title bar includes a shield icon, the text 'Configure protection policy', and 'STEP 1/2: DETAILS' with a close button. The main content is divided into two sections: 'PROTECTION SCHEDULE' and 'BACKUP DESTINATION'.
PROTECTION SCHEDULE: Four cards represent different schedules: '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), and 'Monthly' (Every 1st of the month at 02:00 (UTC), keep the last 12 backups). Below these cards are radio buttons for 'Hourly', 'Daily', 'Weekly' (selected), and 'Monthly'. Further down are input fields for 'Select Weekday(s) (optional)' (Monday X), 'Time (UTC) (optional)' (02:00), 'Snapshots to keep' (26), and 'Backups to keep' (0).
BACKUP DESTINATION: A 'Bucket' dropdown menu is set to 'ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10' with a 'Default' icon and a dropdown arrow.
OVERVIEW: A sidebar on the right titled 'OVERVIEW' contains the text '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.', and 'Read more in Protection policies' with a link icon. Below this are three expandable sections: 'Application cattle-logging', 'Namespace cattle-logging', and 'Cluster se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1'.
At the bottom of the interface are two buttons: 'Cancel' and 'Review →'.

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

Résultat

Astra Control implémente la règle de protection des données en créant et en conservant des snapshots et des

sauvegardes à l'aide du calendrier et de la règle de conservation que vous avez définis.

Créer un snapshot

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

Description de la tâche

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

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



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

Étapes

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

Résultat

Le processus d'instantané commence. Un instantané a réussi lorsque l'état est **Healthy** dans la colonne **State** de la page **Data protection > snapshots**.

Créer une sauvegarde

Vous pouvez sauvegarder une application à tout moment.

Description de la tâche

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

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

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



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

Étapes

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

Résultat

Astra Control crée une sauvegarde de l'application.



- Si votre réseau est en panne ou anormalement lent, une opération de sauvegarde risque d'être terminée. Ceci entraîne l'échec de la sauvegarde.
- Si vous devez annuler une sauvegarde en cours d'exécution, suivez les instructions de la section [Annuler les sauvegardes](#). Pour supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez les instructions de la section [Supprimer les sauvegardes](#).
- Après une opération de protection des données (clonage, sauvegarde, restauration) et après le redimensionnement du volume persistant, il y a vingt minutes de retard avant que la nouvelle taille du volume ne s'affiche dans l'interface utilisateur. La protection des données fonctionne avec succès en quelques minutes et vous pouvez utiliser le logiciel de gestion pour le système back-end pour confirmer la modification de la taille du volume.

Sauvegardez et restaurez les opérations `ontap-nas`

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

Avant de commencer

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

Développez pour les étapes de configuration

1. Effectuez les opérations suivantes sur le back-end de stockage ONTAP :

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



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

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

+



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

2. Effectuez les opérations suivantes dans Astra Trident :

- a. Activez le répertoire de snapshot pour chaque PV qui est `ontap-nas-economy` basé et associé à l'application :

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

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

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

Réponse :

```
snapshotDirectory: "true"
```

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

Résultat

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

Créez une sauvegarde immuable

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

Avant de commencer

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

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



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



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

Étapes

1. Sélectionnez **applications**.
2. Dans le menu Options de la colonne **actions** de l'application souhaitée, sélectionnez **Sauvegarder**.
3. Personnaliser le nom de la sauvegarde.
4. Choisissez de sauvegarder l'application à partir d'un snapshot existant. Si vous sélectionnez cette option, vous pouvez choisir parmi une liste de snapshots existants.
5. Choisir un compartiment de destination pour la sauvegarde dans la liste des compartiments de stockage. Un compartiment WORM (Write Once Read Many) est indiqué par l'état « LOCKED » (verrouillé) à côté du nom du compartiment.



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

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

Résultat

ASTRA Control crée une sauvegarde immuable de l'application.



- Si votre réseau est en panne ou anormalement lent, une opération de sauvegarde risque d'être terminée. Ceci entraîne l'échec de la sauvegarde.
- Si vous essayez de créer deux sauvegardes immuables d'une même application dans le même compartiment en même temps, Astra Control empêche le démarrage de la deuxième sauvegarde. Attendez que la première sauvegarde soit terminée avant de commencer une autre sauvegarde.
- Vous ne pouvez pas annuler une sauvegarde immuable en cours d'exécution.
- Après une opération de protection des données (clonage, sauvegarde, restauration) et après le redimensionnement du volume persistant, il y a vingt minutes de retard avant que la nouvelle taille du volume ne s'affiche dans l'interface utilisateur. La protection des données fonctionne avec succès en quelques minutes et vous pouvez utiliser le logiciel de gestion pour le système back-end pour confirmer la modification de la taille du volume.

Afficher les snapshots et les sauvegardes

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



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

Étapes

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

Les snapshots s'affichent par défaut.

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

Supprimer les instantanés

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



Vous ne pouvez pas supprimer un snapshot en cours de réplication.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez **protection des données**.
3. Dans le menu Options de la colonne **actions** pour l'instantané souhaité, sélectionnez **Supprimer instantané**.
4. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer l'instantané**.

Résultat

Astra Control supprime le snapshot.

Annuler les sauvegardes

Vous pouvez annuler une sauvegarde en cours.



Pour annuler une sauvegarde, la sauvegarde doit être dans `Running` état. Vous ne pouvez pas annuler une sauvegarde dans `Pending` état.



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

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Sélectionnez **backups**.
4. Dans le menu Options de la colonne **actions** pour la sauvegarde souhaitée, sélectionnez **Annuler**.
5. Tapez le mot "annuler" pour confirmer l'opération, puis sélectionnez **Oui, annuler la sauvegarde**.

Supprimer les sauvegardes

Supprimez les sauvegardes planifiées ou à la demande qui ne vous sont plus nécessaires. Vous ne pouvez pas supprimer une sauvegarde effectuée dans un compartiment immuable tant que la politique de conservation du compartiment ne vous y autorise pas.



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



Si vous devez annuler une sauvegarde en cours d'exécution, suivez les instructions de la section [Annuler les sauvegardes](#). Pour supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez ces instructions.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Sélectionnez **backups**.
4. Dans le menu Options de la colonne **actions** pour la sauvegarde souhaitée, sélectionnez **Supprimer sauvegarde**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer sauvegarde**.

Résultat

Astra Control supprime la sauvegarde.

Restaurez les applications

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

Avant de commencer

- **Protéger vos applications en premier** : il est fortement recommandé de prendre un instantané ou une sauvegarde de votre application avant de la restaurer. Vous pourrez ainsi cloner à partir de l'instantané ou

de la sauvegarde si la restauration échoue.

- **Vérifier les volumes de destination** : si vous restaurez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, ReadWriteMany). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent. Par exemple, si votre volume persistant source utilise le mode d'accès RWX, en sélectionnant une classe de stockage de destination qui ne peut pas fournir RWX, comme les disques gérés Azure, AWS EBS, Google persistent Disk ou `ontap-san`, provoque l'échec de l'opération de restauration. Pour plus d'informations sur les modes d'accès aux volumes persistants, reportez-vous au "[Kubernetes](#)" documentation :
- **Planifier les besoins en espace** : lorsque vous effectuez une restauration sur place d'une application utilisant un stockage NetApp ONTAP, l'espace utilisé par l'application restaurée peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.
- * (Clusters Red Hat OpenShift uniquement) Ajouter des stratégies* : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

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



L'exécution d'une opération de restauration sur place sur une application qui partage des ressources avec une autre application peut avoir des résultats inattendus. Toutes les ressources partagées entre les applications sont remplacées lorsqu'une restauration sur place est effectuée sur l'une des applications. Pour plus d'informations, voir [cet exemple](#).

Étapes

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

- **Restaurer les espaces de noms d'origine** : utilisez cette procédure pour restaurer l'app sur place dans le cluster d'origine.



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

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



Si vous restaurez vers un espace de nom qui a déjà été supprimé, un nouvel espace de nom avec le même nom est créé dans le cadre du processus de restauration. Tous les utilisateurs disposant des droits de gestion des applications dans l'espace de noms précédemment supprimé doivent restaurer manuellement les droits sur l'espace de noms nouvellement créé.

- **Restaurer vers de nouveaux espaces de noms** : utilisez cette procédure pour restaurer l'application vers un autre cluster ou avec des espaces de noms différents de la source.
 - i. Spécifiez le nom de l'application restaurée.
 - ii. Choisissez le cluster de destination pour l'application que vous souhaitez restaurer.
 - iii. Entrez un espace de noms de destination pour chaque espace de noms source associé à l'application.



Astra Control crée de nouveaux espaces de noms de destination dans le cadre de cette option de restauration. Les espaces de noms de destination que vous spécifiez ne doivent pas être déjà présents sur le cluster de destination.

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

- viii. Sélectionnez **Suivant**.

4. Sélectionnez les ressources à filtrer :

- **Restaurer toutes les ressources** : restaurez toutes les ressources associées à l'application d'origine.
- **Filtrer les ressources** : spécifiez des règles pour restaurer un sous-ensemble des ressources d'application d'origine :
 - i. Choisissez d'inclure ou d'exclure des ressources de l'application restaurée.

- ii. Sélectionnez **Ajouter une règle d'inclusion** ou **Ajouter une règle d'exclusion** et configurez la règle pour filtrer les ressources appropriées lors de la restauration de l'application. Vous pouvez modifier une règle ou la supprimer et créer une nouvelle règle jusqu'à ce que la configuration soit correcte.



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

5. Sélectionnez **Suivant**.

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

Résultat

Astra Control restaure l'application en fonction des informations que vous avez fournies. Si vous avez restauré l'application sur place, le contenu des volumes persistants existants est remplacé par le contenu des volumes persistants de l'application restaurée.



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



Tout utilisateur membre aux contraintes de namespace par nom/ID d'espace de noms ou par libellés de namespace peut cloner ou restaurer une application vers un nouvel espace de noms sur le même cluster ou vers tout autre cluster du compte de son entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde l'accès au nouvel espace de noms.

Filtrer les ressources pendant la restauration d'une application

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

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

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

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

Étapes

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



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

2. Configurez la règle de filtre :



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

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



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

- b. (Facultatif) Entrez un nom de ressource.
- c. (Facultatif) **Sélecteur d'étiquettes** : inclure un "sélecteur d'étiquettes" pour ajouter à la règle. Le sélecteur d'étiquettes est utilisé pour filtrer uniquement les ressources correspondant à l'étiquette sélectionnée.

- d. (Facultatif) sélectionnez **utiliser GVK (GroupVersionKind) défini pour filtrer les ressources** pour des options de filtrage supplémentaires.



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

- i. (Facultatif) **Group** : dans la liste déroulante, sélectionnez le groupe API Kubernetes.
 - ii. **Type** : dans la liste déroulante, sélectionnez le schéma d'objet du type de ressource Kubernetes à utiliser dans le filtre.
 - iii. **Version** : sélectionnez la version de l'API Kubernetes.
3. Vérifiez la règle créée en fonction de vos entrées.
4. Sélectionnez **Ajouter**.



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

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

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

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

1. Vous définissez l'application `app1` utilisation de l'espace de noms `ns1`.
2. Vous configurez une relation de réplication pour `app1`.
3. Vous définissez l'application `app2` (sur le même cluster) utilisant les namespaces `ns1` et `ns2`.
4. Vous configurez une relation de réplication pour `app2`.
5. La réplication est inversée pour `app2`. Ceci provoque le `app1` l'application sur le cluster source à désactiver.

Réplication d'applications entre les systèmes back-end avec la technologie SnapMirror

Avec Astra Control, vous pouvez assurer la continuité de l'activité de vos applications avec un objectif de point de récupération (RPO) et un objectif de délai de restauration (RTO) faible grâce aux fonctionnalités de réplication asynchrone de la technologie NetApp SnapMirror. Une fois configuré, vos applications peuvent répliquer les modifications des données et des applications d'un système back-end de stockage vers un autre, sur le même cluster ou entre différents clusters.

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

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

environnements hybrides et multicloud :

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

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



Vous pouvez répliquer simultanément une autre application dans la direction opposée. Par exemple, les applications A, B, C peuvent être répliquées depuis Datacenter 1 vers Datacenter 2. Et les applications X, y, Z peuvent être répliquées depuis Datacenter 2 vers Datacenter 1.

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

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

Conditions préalables à la réplication

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

Clusters ONTAP

- **Astra Trident** : Astra Trident version 22.10 ou ultérieure doit exister sur les clusters Kubernetes source et de destination qui utilisent ONTAP en tant que back-end. ASTRA Control prend en charge la réplication avec la technologie NetApp SnapMirror à l'aide de classes de stockage basées sur les pilotes suivants :
 - `ontap-nas`
 - `ontap-san`
- **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Reportez-vous à la section "[Présentation des licences SnapMirror dans ONTAP](#)" pour en savoir plus.

Peering

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



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

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

Centre de contrôle Astra

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

Astra Control Provisioner uniquement : l'ajout et la gestion de systèmes back-end de stockage ONTAP dans Astra Control Center sont facultatifs si vous avez activé Astra Control Provisioner pour Astra Control Center 23.10 ou version ultérieure.

- **Clusters gérés** : ajoutez et gérez les clusters suivants avec Astra Control, idéalement sur différents sites ou domaines de défaillance :
 - Cluster Kubernetes source
 - Cluster Kubernetes de destination
 - Clusters ONTAP associés
- **Comptes d'utilisateur** : lorsque vous ajoutez un back-end de stockage ONTAP à Astra Control Center, appliquez les informations d'identification de l'utilisateur avec le rôle « admin ». Ce rôle a des méthodes d'accès `http` et `ontapi` Activation sur les clusters ONTAP source et de destination Reportez-vous à la section "[Gérer les comptes utilisateur dans la documentation ONTAP](#)" pour en savoir plus.

Astra Control Provisioner Only: Si vous avez activé la fonctionnalité Astra Control Provisioner, vous n'avez plus besoin de définir spécifiquement un rôle « admin » pour gérer les clusters dans Astra Control Center, car ces identifiants ne sont plus requis dans Astra Control Center.



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



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

Configuration d'Astra Trident et ONTAP

ASTRA Control Center exige que vous configuriez au moins un système back-end de stockage qui prend en charge la réplication pour les clusters source et de destination. Si les clusters source et cible sont identiques, l'application de destination doit utiliser un back-end de stockage différent de l'application source pour une résilience optimale.



La réplication Astra Control prend en charge les applications qui utilisent une seule classe de stockage. Lorsque vous ajoutez une application à un espace de noms, assurez-vous que cette application possède la même classe de stockage que les autres applications de l'espace de noms. Lorsque vous ajoutez une demande de volume persistant à une application répliquée, assurez-vous que la nouvelle demande de volume persistant possède la même classe de stockage que les autres demandes de volume persistant dans l'espace de noms.

Configuration d'une relation de réplication

La configuration d'une relation de réplication implique les éléments suivants :

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

- Définition de la durée de prise de l'instantané

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Sélectionnez l'onglet **protection des données > réplication**.
3. Sélectionnez **configurer la stratégie de réplication**. Ou, dans la zone protection des applications, sélectionnez l'option actions et sélectionnez **configurer la stratégie de réplication**.
4. Entrez ou sélectionnez les informations suivantes :
 - **Cluster de destination** : entrez un cluster de destination (il peut être identique au cluster source).
 - **Classe de stockage de destination** : sélectionnez ou entrez la classe de stockage qui utilise le SVM peering sur le cluster ONTAP de destination. Dans le cadre de la meilleure pratique, la classe de stockage de destination doit pointer vers un système back-end de stockage différent de la classe de stockage source.
 - **Type de réplication** : `Asynchronous` est actuellement le seul type de réplication disponible.
 - **Espace de noms de destination** : saisissez des espaces de noms de destination nouveaux ou existants pour le cluster de destination.
 - (Facultatif) Ajouter des espaces de noms supplémentaires en sélectionnant **Ajouter espace de noms** et en choisissant l'espace de noms dans la liste déroulante.
 - **Fréquence de réplication** : définissez la fréquence à laquelle vous souhaitez qu'Astra Control prenne un snapshot et le réplique vers la destination.
 - **Offset** : définit le nombre de minutes à partir du haut de l'heure où vous souhaitez qu'Astra Control prenne un instantané. Vous pouvez utiliser un décalage afin qu'il ne coïncide pas avec d'autres opérations planifiées.



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

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



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

ASTRA Control crée un snapshot d'application utilisé pour la réplication.

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

Le nom du snapshot utilise le format de `replication-schedule-<string>`. ASTRA Control conserve le dernier snapshot utilisé pour la réplication. Les anciens snapshots de réplication sont supprimés après la fin de la réplication.

Résultat

Cela crée la relation de réplication.

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

- Crée un espace de noms sur la destination (s'il n'existe pas)

- Crée une demande de volume persistant sur l'espace de noms de destination correspondant aux demandes de volume virtuel de l'application source.
- Effectue un snapshot initial cohérent avec les applications.
- Établit la relation SnapMirror pour les volumes persistants utilisant le snapshot initial.

La page **Data protection** affiche l'état et l'état de la relation de réplication :
<Health status> | <Relationship life cycle state>

Par exemple :
Normal | établi

Pour en savoir plus sur l'état et l'état de la réplication, consultez cette rubrique.

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

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

Étapes

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

Résultat

La procédure de basculement entraîne les actions suivantes :

- L'application de destination démarre sur la base du dernier snapshot répliqué.
- Le cluster source et l'app (si opérationnel) ne sont pas arrêtés et continuent à fonctionner.
- L'état de réplication passe à « basculement » puis à « basculement » une fois terminé.
- La règle de protection de l'application source est copiée vers l'application de destination en fonction des plannings présents sur l'application source au moment du basculement.
- Si un ou plusieurs crochets d'exécution post-restauration sont activés dans l'application source, ces crochets d'exécution sont exécutés pour l'application de destination.
- Astra Control affiche l'application sur les clusters source et de destination et son état de santé respectif.

Resynchroniser un basculement de réplication impossible

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

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



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

Étapes

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



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

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

Résultat

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

Réplication inverse des applications

Il s'agit de l'opération planifiée pour déplacer l'application vers le back-end de stockage de destination tout en continuant à répliquer vers le back-end de stockage source d'origine. ASTRA Control arrête l'application source et réplique les données vers la destination avant de basculer vers l'application de destination.

Dans ce cas, vous permutez la source et la destination.

Étapes

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

Résultat

Les actions suivantes se produisent suite à la réplication inverse :

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

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

Avec Astra Control, vous pouvez obtenir le « retour arrière » après une opération de basculement à l'aide de la séquence d'opérations suivante. Dans ce flux de travail pour restaurer le sens de réplication d'origine, Astra Control réplique (resyncs) toute modification d'application vers l'application source d'origine avant d'inverser le sens de réplication.

Ce processus commence à partir d'une relation qui a effectué un basculement vers une destination et implique les étapes suivantes :

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

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Sélectionnez l'onglet **protection des données > réplication**.
3. Dans le menu actions, sélectionnez **Resync**.
4. Pour une opération de retour arrière, choisissez l'application de basculement comme source de l'opération de resynchronisation (conservation des données écrites après basculement).
5. Tapez « resynchroniser » pour confirmer.
6. Sélectionnez **Oui, resynchronisation** pour terminer.
7. Une fois la resynchronisation terminée, dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **réplication inverse**.
8. Dans la page réplication inverse, vérifiez les informations et sélectionnez **réplication inverse**.

Résultat

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

Supprime une relation de réplication d'application

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

Étapes

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

Résultat

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

- Si la relation est établie mais que l'application n'a pas encore été mise en ligne sur le cluster de destination (échec), Astra Control conserve les demandes de volume persistant créées lors de l'initialisation, laisse une application gérée « vide » sur le cluster de destination et conserve l'application de destination pour conserver les sauvegardes qui pourraient avoir été créées.

- Si l'application a été mise en ligne sur le cluster de destination (avec échec), Astra Control conserve les demandes de volume persistant et les applications de destination. Les applications source et de destination sont désormais traitées comme des applications indépendantes. Les planifications de sauvegarde restent sur les deux applications mais ne sont pas associées les unes aux autres.

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

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

États d'intégrité des relations de réplication

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

- **Normal** : la relation est soit établie, soit établie, et le snapshot le plus récent a été transféré avec succès.
- **Avertissement** : la relation est soit basculée, soit a échoué (et donc ne protège plus l'app source).
- **Critique**
 - La relation est établie ou a échoué et la dernière tentative de réconciliation a échoué.
 - La relation est établie, et la dernière tentative de concilier l'ajout d'un nouveau PVC est un échec.
 - La relation est établie (un snapshot a donc été répliqué avec succès et un basculement est possible), mais le snapshot le plus récent a échoué ou n'a pas pu être répliqué.

États du cycle de vie de la réplication

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

- **Établissement**: Une nouvelle relation de réplication est en cours de création. Astra Control crée un espace de noms si nécessaire, crée des demandes de volume persistant sur les nouveaux volumes du cluster de destination et crée des relations SnapMirror. Cet état peut également indiquer que la réplication est resynchronisée ou inversée.
- **Créé** : il existe une relation de réplication. ASTRA Control vérifie régulièrement que les ESV sont disponibles, vérifie la relation de réplication, crée régulièrement des instantanés de l'application et identifie les nouvelles ESV source dans l'application. Si c'est le cas, Astra Control crée les ressources qui les incluent dans la réplication.
- **Basculement** : Astra Control rompt les relations SnapMirror et restaure les ressources Kubernetes de l'application à partir du dernier snapshot d'application répliqué avec succès.
- **Basculement** : Astra Control arrête la réplication à partir du cluster source, utilise le snapshot d'application répliqué le plus récent (avec succès) sur la destination et restaure les ressources Kubernetes.
- **Resynchronisation** : le contrôle Astra resynchronise les nouvelles données de la source de resynchronisation vers la destination de resynchronisation à l'aide de la resynchronisation SnapMirror. Cette opération peut écraser certaines données de la destination en fonction de la direction de la synchronisation. Astra Control arrête l'application exécutée sur l'espace de noms de destination et supprime l'application Kubernetes. Pendant le processus de resynchronisation, l'état indique « établissement ».
- **Reversing** : l'opération planifiée pour déplacer l'application vers le cluster de destination tout en continuant à effectuer la réplication vers le cluster source d'origine. Astra Control arrête l'application du cluster source. Il réplique les données vers la destination avant de basculer l'application vers le cluster de destination. Pendant la réplication inverse, l'état indique « établissement ».
- **Suppression** :
 - Si la relation de réplication a été établie mais n'a pas encore été rétablie, Astra Control supprime les

demandes de volume persistant qui ont été créées pendant la réplication et supprime l'application gérée de destination.

- Si la réplication a déjà échoué, Astra Control conserve les ESV et l'application de destination.

Cloner et migrer les applications

Vous pouvez cloner une application existante pour créer une application dupliquée sur le même cluster Kubernetes ou sur un autre cluster. Lorsque vous clonez une application Astra Control, il crée un clone de la configuration des applications et du stockage persistant.

Le clonage peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre. Par exemple, il peut être intéressant de déplacer les workloads dans un pipeline ci/CD et entre les espaces de noms Kubernetes. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou ["API de contrôle Astra"](#) clonage et migration des applications.

Avant de commencer

- **Vérifier les volumes de destination** : si vous clonez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, ReadWriteMany). L'opération de clonage échoue si le mode d'accès au volume persistant de destination est différent. Par exemple, si votre volume persistant source utilise le mode d'accès RWX, en sélectionnant une classe de stockage de destination qui ne peut pas fournir RWX, comme les disques gérés Azure, AWS EBS, Google persistent Disk ou `ontap-san`, provoque l'échec de l'opération de clonage. Pour plus d'informations sur les modes d'accès aux volumes persistants, reportez-vous au ["Kubernetes"](#) documentation :
- Pour cloner les applications sur un autre cluster, vous devez vérifier que les instances cloud contenant les clusters source et de destination (le cas échéant) disposent d'un compartiment par défaut. Vous devez attribuer un compartiment par défaut à chaque instance de cloud.
- Lors des opérations de clonage, les applications nécessitant une ressource IngressClass ou des crochets Web ne doivent pas avoir ces ressources déjà définies sur le cluster de destination.

Lors du clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour cela, il faut configurer une policy d'exportation de volume ONTAP afin de permettre ces opérations. Pour ce faire, utilisez les commandes suivantes :



1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limites des clones

- **Classes de stockage explicites** : si vous déployez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Applications économiques ontap-nas** : vous ne pouvez pas utiliser d'opérations de clonage si la classe de stockage de votre application est prise en charge par `ontap-nas-economy` conducteur. Vous pouvez cependant ["sauvegardez et restaurez les opérations ontap-nas"](#).

- **Clones et contraintes utilisateur** : tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par étiquette d'espace de noms peut cloner ou restaurer une application dans un nouvel espace de noms sur le même cluster ou sur tout autre cluster du compte de son organisation. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde l'accès au nouvel espace de noms.
- **Les clones utilisent des compartiments par défaut** : lors d'une sauvegarde d'application ou d'une restauration d'application, vous pouvez éventuellement spécifier un ID de compartiment. Cependant, une opération de clonage d'application utilise toujours le compartiment par défaut défini. Il n'existe aucune option pour modifier les compartiments d'un clone. Si vous souhaitez contrôler le godet utilisé, vous pouvez l'un des deux "[modifiez les paramètres par défaut du compartiment](#)" ou faites un "[sauvegarde](#)" suivi d'un "[restaurer](#)" séparément.
- **Avec Jenkins ci** : si vous clonez une instance déployée par l'opérateur de Jenkins ci, vous devez restaurer manuellement les données persistantes. Il s'agit d'une limitation du modèle de déploiement de l'application.
- **Avec les compartiments S3**: Les compartiments S3 dans Astra Control Center n'indiquent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.
- **Avec une version spécifique de PostgreSQL** : les clones d'applications dans le même cluster échouent systématiquement avec le graphique Bitnami PostgreSQL 11.5.0. Pour effectuer un clonage réussi, utilisez une version antérieure ou ultérieure du graphique.

Considérations d'OpenShift

- **Clusters et versions OpenShift** : si vous clonez une application entre les clusters, les clusters source et cible doivent être de la même distribution qu'OpenShift. Par exemple, si vous clonez une application depuis un cluster OpenShift 4.7, utilisez un cluster de destination qui est également OpenShift 4.7.
- **Projets et UID** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, le projet (ou l'espace de noms Kubernetes) est affecté à un UID SecurityContext. Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

Étapes

1. Sélectionnez **applications**.
2. Effectuez l'une des opérations suivantes :
 - Sélectionnez le menu Options dans la colonne **actions** pour l'application souhaitée.
 - Sélectionnez le nom de l'application souhaitée et sélectionnez la liste déroulante d'état en haut à droite de la page.
3. Sélectionnez **Clone**.
4. Spécifiez les détails du clone :
 - Entrez un nom.

- Choisissez un cluster de destination pour le clone.
- Entrez les espaces de noms de destination du clone. Chaque espace de noms source associé à l'application est mappé à l'espace de noms de destination que vous définissez.



Astra Control crée de nouveaux espaces de noms de destination dans le cadre de l'opération de clonage. Les espaces de noms de destination que vous spécifiez ne doivent pas être déjà présents sur le cluster de destination.

- Sélectionnez **Suivant**.
- Choisissez de conserver la classe de stockage d'origine associée à l'application ou de sélectionner une autre classe de stockage.



Vous pouvez migrer la classe de stockage d'une application vers une classe de stockage de fournisseur cloud native ou vers une autre classe de stockage prise en charge, puis migrer une application à partir d'une classe de stockage prise en charge par `ontap-nas-economy` à une classe de stockage soutenue par `ontap-nas` sur le même cluster, ou copiez l'application vers un autre cluster dont la classe de stockage est prise en charge par `ontap-nas-economy` conducteur.



Si vous sélectionnez une classe de stockage différente et que cette classe de stockage n'existe pas au moment de la restauration, une erreur est renvoyée.

5. Sélectionnez **Suivant**.

6. Vérifiez les informations sur le clone et sélectionnez **Clone**.

Résultat

Astra Control clone l'application en fonction des informations que vous avez fournies. L'opération de clonage a réussi lorsque le nouveau clone d'application est dans `Healthy` Indiquez la page **applications**.

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



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

Gérer les crochets d'exécution de l'application

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

Types de crochets d'exécution

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

- Pré-instantané
- Post-snapshot
- Avant sauvegarde
- Post-sauvegarde
- Post-restauration
- Après le basculement

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un crochet d'exécution à une application, vous pouvez ajouter des filtres à un crochet d'exécution pour gérer les conteneurs auxquels le crochet correspond. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais ils peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels des crochets d'exécution s'exécutent sur certains conteneurs, mais pas nécessairement tous identiques. Si vous créez plusieurs filtres pour un seul crochet d'exécution, ils sont combinés avec un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.

Chaque filtre que vous ajoutez à un crochet d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un crochet correspond à un conteneur, le crochet exécute son script associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe de l'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre qui exclut les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe prise en charge par Astra Control pour les expressions régulières dans les filtres de crochet d'exécution, voir "[Prise en charge de la syntaxe de l'expression régulière 2 \(RE2\)](#)".



Si vous ajoutez un filtre d'espace de noms à un crochet d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage sont dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Remarques importantes sur les crochets d'exécution personnalisés

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



Puisque les crochets d'exécution réduisent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils s'exécutent, vous devez toujours essayer de réduire le temps d'exécution de vos crochets personnalisés.

Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Cela signifie que la logique utilisée dans un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde a été effectuée.

- La fonction crochets d'exécution est désactivée par défaut pour les nouveaux déploiements d'Astra Control.
 - Vous devez activer la fonction crochets d'exécution avant de pouvoir utiliser les crochets d'exécution.

- Les utilisateurs propriétaires ou administrateurs peuvent activer ou désactiver la fonction crochets d'exécution pour tous les utilisateurs définis dans le compte Astra Control actuel. Reportez-vous à la section [Activez la fonction crochets d'exécution](#) et [Désactivez la fonction crochets d'exécution](#) pour obtenir des instructions.
- Le statut d'activation de la fonctionnalité est conservé pendant les mises à niveau d'Astra Control.
- Un crochet d'exécution doit utiliser un script pour effectuer des actions. De nombreux crochets d'exécution peuvent référencer le même script.
- Astra Control exige que les scripts utilisés par les crochets d'exécution soient écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.
- Astra Control utilise les paramètres de crochet d'exécution et tout critère de correspondance pour déterminer quels crochets s'appliquent à une opération de snapshot, de sauvegarde ou de restauration.
- Toutes les défaillances de crochet d'exécution sont des pannes logicielles ; d'autres crochets et l'opération de protection des données sont toujours tentées même en cas de défaillance d'un crochet. Cependant, lorsqu'un crochet échoue, un événement d'avertissement est enregistré dans le journal des événements de la page **activité**.
- Pour créer, modifier ou supprimer des crochets d'exécution, vous devez être un utilisateur disposant des autorisations propriétaire, administrateur ou membre.
- Si l'exécution d'un crochet d'exécution prend plus de 25 minutes, le crochet échoue, créant une entrée de journal d'événements avec un code retour « N/A ». Tout instantané affecté expire et sera marqué comme ayant échoué, avec une entrée du journal des événements qui en résulte indiquant le délai d'attente.
- Pour les opérations de protection des données ad hoc, tous les événements hook sont générés et enregistrés dans le journal des événements de la page **Activity**. Cependant, pour les opérations planifiées de protection des données, seuls les événements de défaillance de type « hook » sont enregistrés dans le journal des événements (les événements générés par les opérations de protection des données planifiées sont toujours enregistrés).
- Si Astra Control Center bascule une application source répliquée vers l'application de destination, tous les crochets d'exécution post-basculement activés pour l'application source sont exécutés pour l'application de destination une fois le basculement terminé.



Si vous avez exécuté des crochets de post-restauration avec Astra Control Center 23.04 et mis à niveau votre Astra Control Center vers la version 23.07 ou ultérieure, les crochets d'exécution post-restauration ne seront plus exécutés après une réplication de basculement. Vous devez créer de nouveaux crochets d'exécution post-basculement pour vos applications. Vous pouvez également remplacer le type d'opération des crochets post-restauration existants destinés aux basculements par « post-restauration » ou « post-basculement ».

Ordre d'exécution

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

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

3. Tous les crochets d'exécution de post-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets post-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets après l'opération n'est ni garanti ni configurable.

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

1. Crochets de pré-secours exécutés
2. Crochets pré-instantanés exécutés
3. Crochets post-snapshot exécutés
4. Crochets post-secours exécutés
5. Crochets post-restauration exécutés

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



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

Déterminez si un crochet va courir

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

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

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



Si vous démarrez mais annulez ensuite une sauvegarde qui inclut un instantané et qu'il y a des crochets d'exécution associés, certains crochets peuvent s'exécuter, et d'autres peuvent ne pas. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée. Gardez à l'esprit les points suivants pour les sauvegardes annulées avec les crochets d'exécution associés :

- Les crochets de pré-secours et post-secours sont toujours exécutés.
- Si la sauvegarde inclut un nouvel instantané et que l'instantané a démarré, les crochets pré-instantané et post-instantané sont exécutés.
- Si la sauvegarde est annulée avant le démarrage de l'instantané, les crochets pré-instantané et post-instantané ne sont pas exécutés.

Scénario	Fonctionnement	Snapshot existant	Sauvegarde existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets	Les crochets de basculement s'exécutent
1	Clonage	N	N	Nouveau	Identique	Y	N	Y	N
2	Clonage	N	N	Nouveau	Différente	Y	Y	Y	N
3	Cloner ou restaurer	Y	N	Nouveau	Identique	N	N	Y	N
4	Cloner ou restaurer	N	Y	Nouveau	Identique	N	N	Y	N
5	Cloner ou restaurer	Y	N	Nouveau	Différente	N	N	Y	N
6	Cloner ou restaurer	N	Y	Nouveau	Différente	N	N	Y	N
7	Restaurer	Y	N	Existant	Identique	N	N	Y	N
8	Restaurer	N	Y	Existant	Identique	N	N	Y	N
9	Snapshot	S/O	S/O	S/O	S/O	Y	S/O	S/O	N
10	Sauvegarde	N	S/O	S/O	S/O	Y	Y	S/O	N
11	Sauvegarde	Y	S/O	S/O	S/O	N	N	S/O	N
12	Basculement	Y	S/O	Créé par réplication	Différente	N	N	N	Y
13	Basculement	Y	S/O	Créé par réplication	Identique	N	N	N	Y

Exemples de crochet d'exécution

Consultez le "[Projet GitHub NetApp Verda](#)" Pour télécharger des crochets d'exécution réels pour des applications courantes telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres crochets d'exécution personnalisés.

Activez la fonction crochets d'exécution

Si vous êtes propriétaire ou administrateur, vous pouvez activer la fonction crochets d'exécution. Lorsque vous activez la fonctionnalité, tous les utilisateurs définis dans ce compte Astra Control peuvent utiliser des crochets d'exécution et afficher des crochets d'exécution et des scripts hook existants.

Étapes

1. Accédez à **applications**, puis sélectionnez le nom d'une application gérée.

2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez **Activer les crochets d'exécution**.

L'onglet **compte** > **paramètres de fonction** s'affiche.

4. Dans le volet **crochets d'exécution**, sélectionnez le menu Paramètres.
5. Sélectionnez **Activer**.
6. Notez l'avertissement de sécurité qui s'affiche.
7. Sélectionnez **Oui, activer les crochets d'exécution**.

Désactivez la fonction crochets d'exécution

Si vous êtes propriétaire ou administrateur, vous pouvez désactiver la fonction crochets d'exécution pour tous les utilisateurs définis dans ce compte Astra Control. Vous devez supprimer tous les crochets d'exécution existants avant de pouvoir désactiver la fonction crochets d'exécution. Reportez-vous à la section [Supprimer un crochet d'exécution](#) pour obtenir des instructions sur la suppression d'un crochet d'exécution existant.

Étapes

1. Accédez à **compte**, puis sélectionnez l'onglet **Paramètres de fonction**.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Dans le volet **crochets d'exécution**, sélectionnez le menu Paramètres.
4. Sélectionnez **Désactiver**.
5. Notez l'avertissement qui s'affiche.
6. Type `disable` pour confirmer que vous souhaitez désactiver la fonction pour tous les utilisateurs.
7. Sélectionnez **Oui, désactiver**.

Afficher les crochets d'exécution existants

Vous pouvez afficher les crochets d'exécution personnalisés existants pour une application.

Étapes

1. Accédez à **applications**, puis sélectionnez le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.

Vous pouvez afficher tous les crochets d'exécution activés ou désactivés dans la liste résultante. Vous pouvez voir l'état d'un crochet, le nombre de conteneurs correspondant, le temps de création et le moment où il s'exécute (pré ou post-opération). Vous pouvez sélectionner le + icône en regard du nom du crochet pour développer la liste des conteneurs sur lequel il sera exécuté. Pour afficher les journaux d'événements entourant les crochets d'exécution de cette application, accédez à l'onglet **activité**.

Afficher les scripts existants

Vous pouvez afficher les scripts chargés existants. Vous pouvez également voir quels scripts sont en cours d'utilisation, et quels crochets les utilisent, sur cette page.

Étapes

1. Accédez à **compte**.

2. Sélectionnez l'onglet **scripts**.

Cette page affiche la liste des scripts chargés existants. La colonne **utilisé par** indique les crochets d'exécution qui utilisent chaque script.

Ajouter un script

Chaque crochet d'exécution doit utiliser un script pour effectuer des actions. Vous pouvez ajouter un ou plusieurs scripts que les crochets d'exécution peuvent référencer. De nombreux crochets d'exécution peuvent référencer le même script ; ceci vous permet de mettre à jour de nombreux crochets d'exécution en modifiant un seul script.

Étapes

1. Assurez-vous que la fonction crochets d'exécution est **activé**.
2. Accédez à **compte**.
3. Sélectionnez l'onglet **scripts**.
4. Sélectionnez **Ajouter**.
5. Effectuez l'une des opérations suivantes :
 - Charger un script personnalisé.
 - i. Sélectionnez l'option **Télécharger le fichier**.
 - ii. Accédez à un fichier et téléchargez-le.
 - iii. Donnez un nom unique au script.
 - iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
 - v. Sélectionnez **Enregistrer le script**.
 - Coller dans un script personnalisé à partir du presse-papiers.
 - i. Sélectionnez l'option **Coller ou type**.
 - ii. Sélectionnez le champ de texte et collez le texte du script dans le champ.
 - iii. Donnez un nom unique au script.
 - iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
6. Sélectionnez **Enregistrer le script**.

Résultat

Le nouveau script apparaît dans la liste de l'onglet **scripts**.

Supprimer un script

Vous pouvez supprimer un script du système s'il n'est plus nécessaire et s'il n'est pas utilisé par les crochets d'exécution.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **scripts**.
3. Choisissez un script à supprimer et sélectionnez le menu dans la colonne **actions**.

4. Sélectionnez **Supprimer**.



Si le script est associé à un ou plusieurs crochets d'exécution, l'action **Delete** n'est pas disponible. Pour supprimer le script, modifiez d'abord les crochets d'exécution associés et associez-les à un autre script.

Créer un crochet d'exécution personnalisé

Vous pouvez créer un crochet d'exécution personnalisé pour une application et l'ajouter à Astra Control. Reportez-vous à la section [Exemples de crochet d'exécution](#) pour des exemples de crochet. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour créer des crochets d'exécution.



Lorsque vous créez un script de shell personnalisé à utiliser comme crochet d'exécution, n'oubliez pas de spécifier le shell approprié au début du fichier, sauf si vous exécutez des commandes spécifiques ou fournissez le chemin complet à un exécutable.

Étapes

1. Assurez-vous que la fonction crochets d'exécution est [activé](#).
2. Sélectionnez **applications**, puis le nom d'une application gérée.
3. Sélectionnez l'onglet **crochets d'exécution**.
4. Sélectionnez **Ajouter**.
5. Dans la zone **Détails du crochet** :
 - a. Déterminez quand le crochet doit fonctionner en sélectionnant un type d'opération dans le menu déroulant **opération**.
 - b. Saisissez un nom unique pour le crochet.
 - c. (Facultatif) saisissez les arguments à transmettre au crochet pendant l'exécution, en appuyant sur la touche entrée après chaque argument que vous entrez pour enregistrer chacun.
6. (Facultatif) dans la zone **Détails du filtre de crochet**, vous pouvez ajouter des filtres pour contrôler les conteneurs sur lesquels le crochet d'exécution s'exécute :
 - a. Sélectionnez **Ajouter filtre**.
 - b. Dans la colonne Type de filtre **Hook**, choisissez un attribut sur lequel filtrer dans le menu déroulant.
 - c. Dans la colonne **Regex**, entrez une expression régulière à utiliser comme filtre. Astra Control utilise le ["Expression régulière 2 \(RE2\) syntaxe regex"](#).

Si vous filtrez sur le nom exact d'un attribut (tel qu'un nom de pod) sans autre texte dans le champ expression régulière, une correspondance de sous-chaîne est effectuée. Pour faire correspondre un nom exact et ce nom uniquement, utilisez la syntaxe de correspondance de chaîne exacte (par exemple, `^exact_podname$`).
 - d. Pour ajouter d'autres filtres, sélectionnez **Ajouter filtre**.

Plusieurs filtres pour un crochet d'exécution sont combinés à un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.
7. Lorsque vous avez terminé, sélectionnez **Suivant**.
8. Dans la zone **script**, effectuez l'une des opérations suivantes :

- Ajouter un nouveau script.
 - i. Sélectionnez **Ajouter**.
 - ii. Effectuez l'une des opérations suivantes :
 - Charger un script personnalisé.
 - I. Sélectionnez l'option **Télécharger le fichier**.
 - II. Accédez à un fichier et téléchargez-le.
 - III. Donnez un nom unique au script.
 - IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
 - V. Sélectionnez **Enregistrer le script**.
 - Coller dans un script personnalisé à partir du presse-papiers.
 - I. Sélectionnez l'option **Coller ou type**.
 - II. Sélectionnez le champ de texte et collez le texte du script dans le champ.
 - III. Donnez un nom unique au script.
 - IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
- Sélectionnez un script existant dans la liste.

Cela indique au crochet d'exécution d'utiliser ce script.

9. Sélectionnez **Suivant**.

10. Vérifiez la configuration du crochet d'exécution.

11. Sélectionnez **Ajouter**.

Vérifier l'état d'un crochet d'exécution

Une fois qu'une opération de snapshot, de sauvegarde ou de restauration a terminé, vous pouvez vérifier l'état des crochets d'exécution qui ont été exécutés dans le cadre de l'opération. Vous pouvez utiliser ces informations d'état pour déterminer si vous souhaitez maintenir le crochet d'exécution, le modifier ou le supprimer.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **protection des données**.
3. Sélectionnez **snapshots** pour voir exécution de snapshots ou **sauvegardes** pour voir exécution de sauvegardes.

L'état **Hook** indique l'état de la séquence de crochet d'exécution une fois l'opération terminée. Vous pouvez passer le curseur de la souris sur l'état pour plus de détails. Par exemple, si des échecs de crochet d'exécution se produisent au cours d'un snapshot, le fait de passer le curseur sur l'état de crochet pour ce snapshot donne une liste des crochets d'exécution ayant échoué. Pour voir les raisons de chaque échec, vous pouvez consulter la page **activité** dans la zone de navigation de gauche.

Afficher l'utilisation du script

Vous pouvez voir quels crochets d'exécution utilisent un script particulier dans l'interface utilisateur Web Astra Control.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **scripts**.

La colonne **utilisé par** de la liste des scripts contient des détails sur les crochets qui utilisent chaque script de la liste.

3. Sélectionnez les informations de la colonne **utilisé par** pour un script qui vous intéresse.

Une liste plus détaillée s'affiche, avec les noms des crochets qui utilisent le script et le type d'opération avec lesquels ils sont configurés pour s'exécuter.

Modifier un crochet d'exécution

Vous pouvez modifier un crochet d'exécution si vous souhaitez modifier ses attributs, filtres ou le script qu'il utilise. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour modifier les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez modifier.
4. Sélectionnez **Modifier**.
5. Apportez les modifications nécessaires en sélectionnant **Suivant** après avoir terminé chaque section.
6. Sélectionnez **Enregistrer**.

Désactivez un crochet d'exécution

Vous pouvez désactiver un crochet d'exécution si vous souhaitez l'empêcher temporairement de s'exécuter avant ou après un instantané d'une application. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour désactiver les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez désactiver.
4. Sélectionnez **Désactiver**.

Supprimer un crochet d'exécution

Vous pouvez supprimer entièrement un crochet d'exécution si vous n'en avez plus besoin. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour supprimer les crochets d'exécution.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez le menu Options dans la colonne **actions** pour un crochet que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.
5. Dans la boîte de dialogue qui s'affiche, tapez « Supprimer » pour confirmer.
6. Sélectionnez **Oui, supprimez le crochet d'exécution**.

Pour en savoir plus

- ["Projet GitHub NetApp Verda"](#)

Protégez Astra Control Center à l'aide d'Astra Control Center

Pour mieux assurer la résilience contre les erreurs fatales sur le cluster Kubernetes sur lequel Astra Control Center s'exécute, protégez l'application Astra Control Center elle-même. Vous pouvez sauvegarder et restaurer Astra Control Center à l'aide d'une instance Astra Control Center secondaire ou utiliser la réplication Astra si le stockage sous-jacent utilise ONTAP.

Dans ces scénarios, une deuxième instance d'Astra Control Center est déployée et configurée dans un domaine de pannes différent et s'exécute sur un second cluster Kubernetes différent de l'instance Astra Control Center principale. La deuxième instance d'Astra Control est utilisée pour sauvegarder et restaurer potentiellement l'instance principale d'Astra Control Center. Une instance Astra Control Center restaurée ou répliquée continuera d'assurer la gestion des données d'application pour les applications du cluster d'applications et de restaurer l'accessibilité aux sauvegardes et aux snapshots de ces applications.

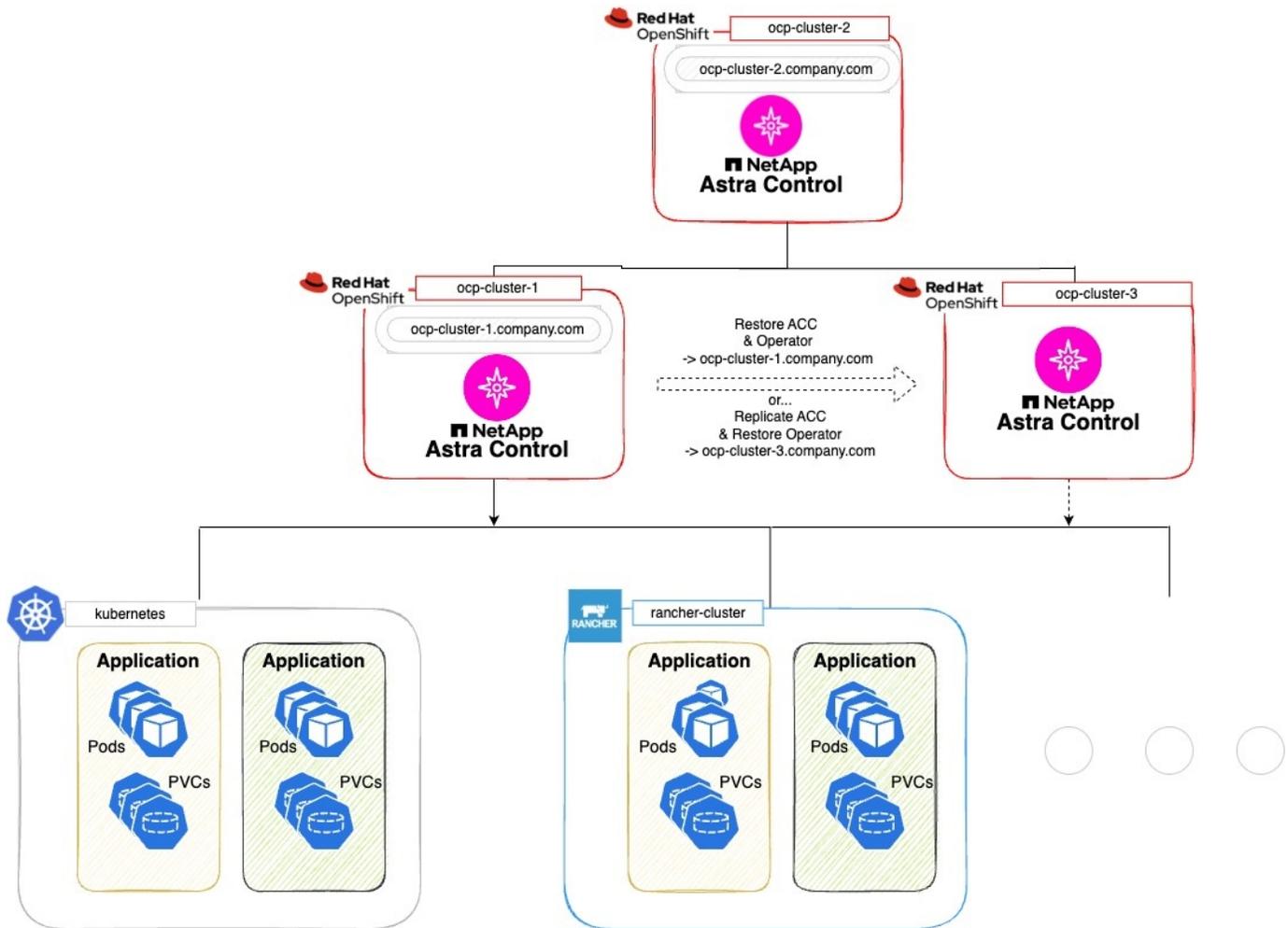
Avant de commencer

Assurez-vous d'avoir les éléments suivants avant de configurer des scénarios de protection pour Astra Control Center :

- **Un cluster Kubernetes exécutant l'instance principale d'Astra Control Center** : ce cluster héberge l'instance principale d'Astra Control Center qui gère les clusters d'applications.
- **Un deuxième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal qui exécute l'instance Astra Control Center secondaire** : ce cluster héberge l'instance Astra Control Center qui gère l'instance Astra Control Center principale.
- **Un troisième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal** : ce cluster hébergera l'instance restaurée ou répliquée d'Astra Control Center. Il doit disposer du même espace de noms Astra Control Center disponible qui est actuellement déployé sur le système principal. Par exemple, si Astra Control Center est déployé dans le namespace `netapp-acc` sur le cluster source, le namespace `netapp-acc` doit être disponible et non utilisé par des applications sur le cluster Kubernetes de destination.
- **Compartiments compatibles S3** : chaque instance d'Astra Control Center dispose d'un compartiment de stockage objet accessible compatible avec S3.
- **Un équilibreur de charge configuré** : l'équilibreur de charge fournit une adresse IP pour Astra et doit disposer d'une connectivité réseau aux clusters d'applications et aux deux compartiments S3.
- **Les clusters répondent aux exigences d'Astra Control Center** : chaque cluster utilisé dans Astra Control Center est conforme "[Exigences générales d'Astra Control Center](#)".

Description de la tâche

Ces procédures décrivent les étapes nécessaires à la restauration d'Astra Control Center sur un nouveau cluster à l'aide des deux [sauvegarder et restaurer](#) ou [la réplication](#). Les étapes sont basées sur l'exemple de configuration présenté ici :



Dans cet exemple de configuration, les éléments suivants sont présentés :

- **Un cluster Kubernetes exécutant l'instance principale d'Astra Control Center :**
 - Cluster OpenShift : `ocp-cluster-1`
 - Instance principale d'Astra Control Center : `ocp-cluster-1.company.com`
 - Ce cluster gère les clusters d'applications.
- **Le deuxième cluster Kubernetes du même type de distribution Kubernetes que le cluster principal qui exécute l'instance Astra Control Center secondaire :**
 - Cluster OpenShift : `ocp-cluster-2`
 - Instance secondaire Astra Control Center : `ocp-cluster-2.company.com`
 - Ce cluster sera utilisé pour sauvegarder l'instance principale d'Astra Control Center ou pour configurer la réplication sur un autre cluster (dans cet exemple, le `ocp-cluster-3` cluster).
- **Un troisième cluster Kubernetes du même type de distribution Kubernetes que le principal qui sera utilisé pour les opérations de restauration :**

- Cluster OpenShift : `ocp-cluster-3`
- Troisième instance d'Astra Control Center : `ocp-cluster-3.company.com`
- Ce cluster sera utilisé pour le basculement de réplication ou de restauration d'Astra Control Center.



Dans l'idéal, le cluster d'applications doit être situé en dehors des trois clusters Astra Control Center, comme illustré dans les clusters kubernetes et Rancher dans l'image ci-dessus.

Non représenté dans le schéma :

- Tous les clusters disposent de systèmes ONTAP back-end avec Trident installé.
- Dans cette configuration, les clusters OpenShift utilisent MetalLB comme équilibreur de charge.
- Le contrôleur de snapshot et VolumeSnapshotClass sont également installés sur tous les clusters, comme indiqué dans le "[prérequis](#)".

Option de l'étape 1 : sauvegarde et restauration d'Astra Control Center

Cette procédure décrit les étapes nécessaires à la restauration d'Astra Control Center sur un nouveau cluster à l'aide de la sauvegarde et de la restauration.

Dans cet exemple, Astra Control Center est toujours installé sous `netapp-acc` l'espace de noms et l'opérateur sont installés sous le `netapp-acc-operator` espace de noms.



Bien que cela ne soit pas décrit, l'opérateur d'Astra Control Center peut également être déployé dans le même espace de nom que Astra CR.

Avant de commencer

- Vous avez installé le centre Astra Control Center principal sur un cluster.
- Vous avez installé le centre Astra Control Center secondaire sur un autre cluster.

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire (s'exécutant sur le système `ocp-cluster-2` cluster) :
 - a. Connectez-vous à l'instance Astra Control Center secondaire.
 - b. "[Ajoutez le cluster Astra Control Center principal](#)" (`ocp-cluster-1`).
 - c. "[Ajouter le troisième cluster de destination](#)" (`ocp-cluster-3`) qui sera utilisé pour la restauration.
2. Gérez Astra Control Center et l'opérateur Astra Control Center sur l'Astra Control Center secondaire :
 - a. Dans la page applications, sélectionnez **définir**.
 - b. Dans la fenêtre **Define application**, entrez le nom de la nouvelle application (`netapp-acc`).
 - c. Choisissez le cluster qui exécute le principal Astra Control Center (`ocp-cluster-1`) Dans la liste déroulante **Cluster**.
 - d. Choisissez le `netapp-acc` Espace de noms pour Astra Control Center dans la liste déroulante **namespace**.
 - e. Sur la page Ressources du cluster, cochez **inclure des ressources supplémentaires de cluster-scoped**.
 - f. Sélectionnez **Ajouter inclure règle**.

g. Sélectionnez ces entrées et sélectionnez **Ajouter** :

- Sélecteur d'étiquette : <label name>
- Groupe : apiextensions.k8s.io
- Version : v1
- Type : CustomResourceDefinition

h. Confirmez les informations de l'application.

i. Sélectionnez **définir**.

Après avoir sélectionné **définir**, répétez le processus définir l'application pour l'opérateur `netapp-acc-operator` et sélectionnez le `netapp-acc-operator` Espace de noms dans l'assistant définir l'application.

3. Sauvegardez Astra Control Center et l'opérateur :

- Sur le centre de contrôle Astra secondaire, accédez à la page applications en sélectionnant l'onglet applications.
- "Sauvegarde" L'application Astra Control Center (`netapp-acc`).
- "Sauvegarde" l'opérateur (`netapp-acc-operator`).

4. Une fois que vous avez sauvegardé Astra Control Center et l'opérateur, simulez un scénario de reprise d'activité de "Désinstallation d'Astra Control Center" à partir du cluster principal.



Vous allez restaurer Astra Control Center sur un nouveau cluster (le troisième cluster Kubernetes décrit dans cette procédure) et utiliser le même DNS que le cluster principal pour Astra Control Center récemment installé.

5. À l'aide du centre Astra Control Center secondaire, "restaurer" L'instance principale de l'application Astra Control Center à partir de sa sauvegarde :

- Sélectionnez **applications**, puis sélectionnez le nom de l'application Astra Control Center.
- Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.
- Choisissez le type de restauration **Restaurer vers les nouveaux espaces de noms**.
- Entrez le nom de la restauration (`netapp-acc`).
- Choisissez le troisième cluster de destination (`ocp-cluster-3`).
- Mettez à jour l'espace de noms de destination de sorte qu'il s'agisse du même espace de noms que l'espace de noms d'origine.
- Sur la page Source de restauration, sélectionnez la sauvegarde d'application qui sera utilisée comme source de restauration.
- Sélectionnez **Restaurer à l'aide des classes de stockage d'origine**.
- Sélectionnez **Restaurer toutes les ressources**.
- Examinez les informations de restauration, puis sélectionnez **Restore** pour démarrer le processus de restauration qui restaure Astra Control Center sur le cluster de destination (`ocp-cluster-3`). La restauration est terminée lorsque l'application entre `available` état.

6. Configurer Astra Control Center sur le cluster de destination :

- Ouvrez un terminal et connectez-le au cluster de destination à l'aide du `kubeconfig` (`ocp-cluster-3`)

Qui contient l'Astra Control Center restaurée.

- b. Confirmez que le ADDRESS Dans la configuration Astra Control Center, la colonne fait référence au nom DNS du système principal :

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

Réponse :

```
NAME      UUID                               VERSION  ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com                True
```

- a. Si le ADDRESS Dans la réponse ci-dessus, le champ ne contient pas le nom de domaine complet de l'instance principale d'Astra Control Center. Mettez à jour la configuration pour référencer le DNS d'Astra Control Center :

```
kubectl edit acc -n netapp-acc
```

- i. Modifiez le astraAddress sous spec: Au FQDN (ocp-cluster-1.company.com Dans cet exemple) de l'instance principale d'Astra Control Center.
- ii. Enregistrez la configuration.
- iii. Vérifiez que l'adresse a été mise à jour :

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

- b. Accédez au [Restaurez l'opérateur Astra Control Center](#) de ce document pour terminer le processus de restauration.

Option de l'étape 1 : protégez Astra Control Center à l'aide de la réplication

Cette procédure décrit les étapes nécessaires à la configuration "[Réplication Astra Control Center](#)" Pour protéger l'instance principale d'Astra Control Center.

Dans cet exemple, Astra Control Center est toujours installé sous netapp-acc l'espace de noms et l'opérateur sont installés sous le netapp-acc-operator espace de noms.

Avant de commencer

- Vous avez installé le centre Astra Control Center principal sur un cluster.
- Vous avez installé le centre Astra Control Center secondaire sur un autre cluster.

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire :

- a. Connectez-vous à l'instance Astra Control Center secondaire.
 - b. "Ajoutez le cluster Astra Control Center principal" (`ocp-cluster-1`).
 - c. "Ajouter le troisième cluster de destination" (`ocp-cluster-3`) qui sera utilisé pour la réplication.
2. Gérez Astra Control Center et l'opérateur Astra Control Center sur l'Astra Control Center secondaire :
- a. Sélectionnez **clusters** et sélectionnez le cluster qui contient l'Astra Control Center principal (`ocp-cluster-1`).
 - b. Sélectionnez l'onglet **espaces de noms**.
 - c. Sélectionnez `netapp-acc` et `netapp-acc-operator` espaces de noms.
 - d. Sélectionnez le menu actions et sélectionnez **définir comme applications**.
 - e. Sélectionnez **Afficher dans les applications** pour voir les applications définies.
3. Configurer les systèmes back-end pour la réplication :



La réplication nécessite le cluster principal Astra Control Center et le cluster de destination (`ocp-cluster-3`) Utiliser des systèmes back-end de stockage ONTAP peering différents. Une fois chaque back-end ajouté à Astra Control, le back-end apparaît dans l'onglet **découvert** de la page Backends.

- a. "Ajoutez un arrière-plan de peering" Vers Astra Control Center sur le cluster principal.
 - b. "Ajoutez un arrière-plan de peering" Vers Astra Control Center sur le cluster de destination.
4. Configurer la réplication :
- a. Sur l'écran applications, sélectionnez `netapp-acc` client supplémentaire.
 - b. Sélectionnez **configurer la stratégie de réplication**.
 - c. Sélectionnez `ocp-cluster-3` en tant que cluster de destination.
 - d. Sélectionnez la classe de stockage.
 - e. Entrez `netapp-acc` comme espace de noms de destination.
 - f. Modifiez la fréquence de réplication si vous le souhaitez.
 - g. Sélectionnez **Suivant**.
 - h. Vérifiez que la configuration est correcte et sélectionnez **Enregistrer**.

La relation de réplication passe de `Establishing` à `Established`. Lorsqu'elle est active, cette réplication se produit toutes les cinq minutes jusqu'à ce que la configuration de réplication soit supprimée.

5. Basculez la réplication vers l'autre cluster si le système principal est corrompu ou n'est plus accessible :



Assurez-vous que Astra Control Center n'est pas installé sur le cluster de destination pour assurer un basculement réussi.

- a. Sélectionnez l'icône des ellipses verticales et sélectionnez **basculement**.

Data protection Storage Resources Execution hooks Activity Tasks

Configure ▾ Snapshots Backups Replication

b. Confirmez les détails et sélectionnez **basculement** pour lancer le processus de basculement.

L'état de la relation de réplication passe à `Failing over` puis `Failed over` une fois l'opération terminée.

6. Compléter la configuration de basculement :

- Ouvrez un terminal et connectez-le à l'aide du kubeconfig du troisième cluster (`ocp-cluster-3`). Ce cluster est désormais équipé d'Astra Control Center.
- Déterminez le nom de domaine complet d'Astra Control Center sur le troisième cluster (`ocp-cluster-3`).
- Mettez à jour la configuration pour référencer le DNS Astra Control Center :

```
kubectl edit acc -n netapp-acc
```

- Modifiez le `astraAddress` sous `spec` : Avec le FQDN (`ocp-cluster-3.company.com`) du troisième cluster de destination.
- Enregistrez la configuration.
- Vérifiez que l'adresse a été mise à jour :

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

d. Vérifiez que tous les CRD de traefik requis sont présents :

```
kubectl get crds | grep traefik
```

CRDS de traefik requis :

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewareetcps.traefik.containo.us
middlewareetcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tloptions.traefik.containo.us
tloptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Si certains des CRD ci-dessus sont manquants :

- i. Accédez à "[documentation de traefik](#)".
- ii. Copiez la zone « Définitions » dans un fichier.
- iii. Appliquer les modifications :

```
kubectl apply -f <file name>
```

iv. Redémarrer le traefik :

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print $1}' | xargs kubectl delete pod -n netapp-acc
```

b. Accédez au [Restaurez l'opérateur Astra Control Center](#) de ce document pour terminer le processus de restauration.

Étape 2 : restaurez l'opérateur Astra Control Center

À l'aide d'Astra Control Center secondaire, restaurez l'opérateur principal d'Astra Control Center à partir d'une sauvegarde. L'espace de noms de destination doit être identique à l'espace de noms source. Si vous avez supprimé Astra Control Center du cluster source principal, des sauvegardes existent toujours pour effectuer les mêmes étapes de restauration.

Étapes

1. Sélectionnez **applications**, puis sélectionnez le nom de l'application opérateur (`netapp-acc-operator`).

2. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**
3. Choisissez le type de restauration **Restaurer vers les nouveaux espaces de noms**.
4. Choisissez le troisième cluster de destination (`ocp-cluster-3`).
5. Modifiez le namespace pour qu'il soit identique au namespace associé au cluster source principal (`netapp-acc-operator`).
6. Sélectionnez la sauvegarde précédemment effectuée en tant que source de restauration.
7. Sélectionnez **Restaurer à l'aide des classes de stockage d'origine**.
8. Sélectionnez **Restaurer toutes les ressources**.
9. Vérifiez les détails, puis cliquez sur **Restaurer** pour lancer le processus de restauration.

La page applications affiche l'opérateur Astra Control Center en cours de restauration sur le troisième cluster de destination (`ocp-cluster-3`). Lorsque le processus est terminé, l'état indique `Available`. Dans les dix minutes qui suivent, l'adresse DNS doit être résolue sur la page.

Résultat

ASTRA Control Center, ses clusters enregistrés et les applications gérées avec leurs copies Snapshot et leurs sauvegardes sont désormais disponibles sur le troisième cluster de destination (`ocp-cluster-3`). Toutes les stratégies de protection que vous aviez sur l'original sont également présentes sur la nouvelle instance. Vous pouvez continuer à effectuer des sauvegardes et des snapshots programmés ou à la demande.

Dépannage

Déterminez l'état du système et si les processus de protection ont réussi.

- **Les pods ne sont pas en cours d'exécution:** Confirmez que tous les pods sont en cours d'exécution:

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

Si certains modules se trouvent dans le `CrashLookBackOff` indiquez, redémarrez-les et passez à `Running` état.

- **Confirmer l'état du système :** confirmer que le système Astra Control Center est en `ready` état :

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

Réponse :

```
NAME      UUID                                VERSION  ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com                True
```

- **Confirmez l'état du déploiement :** affichez les informations de déploiement d'Astra Control Center pour le confirmer `Deployment State est Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **L'interface utilisateur d'Astra Control Center restaurée renvoie une erreur 404** : si cela se produit lorsque vous avez sélectionné `AccTraefik` en tant qu'option d'entrée, cochez la case [CRD de traefik](#) pour vous assurer qu'ils sont tous installés.

Surveillez l'état des applications et des clusters

Affichez un récapitulatif de l'état des applications et du cluster

Sélectionnez **Dashboard** pour afficher une vue de haut niveau de vos applications, clusters, systèmes back-end de stockage et leur état de santé.

Il ne s'agit pas seulement de numéros statiques ou d'États, mais vous pouvez explorer les données à partir de chacun d'entre eux. Par exemple, si les applications ne sont pas totalement protégées, vous pouvez passer le curseur de la souris sur l'icône pour identifier les applications qui ne sont pas totalement protégées, ce qui explique pourquoi.

Mosaïque applications

La mosaïque **applications** vous aide à identifier les éléments suivants :

- Combien d'applications gérez-vous actuellement avec Astra ?
- Si ces applications gérées sont en bon état.
- Que les applications soient entièrement protégées (elles sont protégées si des sauvegardes récentes sont disponibles).
- Le nombre d'applications découvertes, mais non gérées.

Dans l'idéal, ce nombre est égal à zéro, car vous pouvez gérer ou ignorer les applications après leur découverte. Vous devez ensuite surveiller le nombre d'applications découvertes dans le tableau de bord pour déterminer quand les développeurs ajoutent de nouvelles applications à un cluster.

Mosaïque de groupes

La mosaïque **clusters** fournit des détails similaires sur l'état de santé des clusters que vous gérez en utilisant Astra Control Center, et vous pouvez explorer vers le bas pour obtenir plus de détails comme vous pouvez avec une application.

Mosaïque des systèmes back-end de stockage

La mosaïque **Storage backend** fournit des informations pour vous aider à identifier la santé des systèmes back-end :

- Nombre de systèmes back-end gérés
- Que ces systèmes back-end gérés soient en bon état
- Que les systèmes back-end soient entièrement protégés
- Le nombre de systèmes back-end découverts et ne sont pas encore gérés.

Afficher l'état de santé des clusters et gérer les classes de stockage

Une fois que vous avez ajouté des clusters à gérer par Astra Control Center, vous pouvez afficher des informations détaillées sur le cluster, notamment son emplacement, les nœuds de travail, les volumes persistants et les classes de stockage. Vous pouvez également modifier la classe de stockage par défaut des clusters gérés.

Afficher les détails et l'état de santé des clusters

Vous pouvez afficher des informations détaillées sur le cluster, telles que son emplacement, les nœuds de travail, les volumes persistants et les classes de stockage.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster dont vous souhaitez afficher les détails.



Si un cluster se trouve dans le `removed` État et pourtant, la connectivité cluster et réseau semble saine (les tentatives externes d'accès au cluster via les API Kubernetes sont réussies). Le kubeconfig que vous avez fourni au contrôle Astra pourrait ne plus être valide. Cela peut être dû à une rotation ou à une expiration du certificat sur le cluster. Pour corriger ce problème, mettez à jour les informations d'identification associées au cluster dans Astra Control à l'aide du "[API de contrôle Astra](#)".

3. Consultez les informations sur les onglets **Présentation**, **stockage** et **activité** pour trouver les informations que vous recherchez.
 - **Présentation** : détails sur les nœuds de travail, y compris leur état.
 - **Stockage** : volumes persistants associés au calcul, y compris la classe et l'état du stockage.
 - **Activité** : affiche les activités liées au cluster.



Vous pouvez également afficher les informations du groupe d'instruments à partir du Centre de contrôle Astra **Tableau de bord**. Dans l'onglet **clusters** sous **Résumé des ressources**, vous pouvez sélectionner les clusters gérés, qui vous permettent d'accéder à la page **clusters**. Après avoir accédé à la page **clusters**, suivez les étapes décrites ci-dessus.

Modifiez la classe de stockage par défaut

Vous pouvez modifier la classe de stockage par défaut d'un cluster. Lorsque Astra Control gère un cluster, il conserve le suivi de la classe de stockage par défaut du cluster.



Ne modifiez pas la classe de stockage à l'aide des commandes kubectl. Utilisez plutôt cette procédure. Astra Control va rétablir les modifications si elles ont été effectuées à l'aide de kubectl.

Étapes

1. Dans l'interface utilisateur Web Astra Control Center, sélectionnez **clusters**.
2. Sur la page **clusters**, sélectionnez le cluster que vous souhaitez modifier.
3. Sélectionnez l'onglet **stockage**.
4. Sélectionnez la catégorie **classes de stockage**.

5. Sélectionnez le menu **actions** pour la classe de stockage que vous souhaitez définir par défaut.
6. Sélectionnez **définir comme valeur par défaut**.

Afficher l'état de santé et les détails d'une application

Une fois que vous avez commencé à gérer une application, Astra Control fournit des informations détaillées sur l'application qui vous permet d'identifier son état de communication (si Astra Control peut communiquer avec l'application), son état de protection (qu'il soit entièrement protégé en cas de défaillance), les pods, le stockage persistant, etc.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **applications**, puis le nom d'une application.
2. Vérifiez les informations.

Statut de l'application

Fournit un état qui indique si Astra Control peut communiquer avec l'application.

- **App protection Status** : indique l'état de protection de l'application :
 - **Entièrement protégé** : l'application dispose d'un programme de sauvegarde actif et d'une sauvegarde réussie qui a moins d'une semaine
 - **Partiellement protégé** : l'application dispose d'un programme de sauvegarde actif, d'un programme de snapshots actif ou d'une sauvegarde ou d'un snapshot réussi
 - **Non protégé** : Les applications qui ne sont ni totalement protégées ni partiellement protégées.

Vous ne pouvez pas être entièrement protégé tant que vous n'avez pas une sauvegarde récente. Ceci est important, car les sauvegardes sont stockées dans un magasin d'objets à distance des volumes persistants. En cas de défaillance ou d'accident, le cluster doit être doté d'un stockage persistant, alors vous devez effectuer une sauvegarde pour effectuer une restauration. Un snapshot ne vous permettrait pas de restaurer votre système.

- **Présentation** : informations sur l'état des modules associés à l'application.
- **Protection des données** : permet de configurer une stratégie de protection des données et d'afficher les snapshots et sauvegardes existants.
- **Storage** : affiche les volumes persistants au niveau de l'application. L'état d'un volume persistant est du point de vue du cluster Kubernetes.
- **Ressources** : vous permet de vérifier quelles ressources sont sauvegardées et gérées.
- **Activité** : affiche les activités associées à l'application.



Vous pouvez également afficher les informations de l'application à partir du Centre de contrôle Astra **Tableau de bord**. Dans l'onglet **applications** sous **Résumé des ressources**, vous pouvez sélectionner les applications gérées, qui vous permettent d'accéder à la page **applications**. Après avoir accédé à la page **applications**, suivez les étapes décrites ci-dessus.

Gérez votre compte

Gérez les utilisateurs et les rôles locaux

Vous pouvez ajouter, supprimer et modifier les utilisateurs de votre installation Astra Control Center à l'aide de l'interface utilisateur Astra Control. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou ["API de contrôle Astra"](#) pour gérer les utilisateurs.

Vous pouvez également utiliser LDAP pour effectuer l'authentification pour certains utilisateurs.

Utiliser LDAP

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control. À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP. Pour plus d'informations, reportez-vous à la documentation suivante :

- ["Utilisez l'API de contrôle Astra pour gérer l'authentification à distance et les utilisateurs"](#)
- ["Utilisez l'interface utilisateur Astra Control pour gérer les utilisateurs et les groupes distants"](#)
- ["Utilisez l'interface utilisateur Astra Control pour gérer l'authentification à distance"](#)

Ajouter des utilisateurs

Les propriétaires et administrateurs de comptes peuvent ajouter d'autres utilisateurs à l'installation d'Astra Control Center.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Sélectionnez **Ajouter utilisateur**.
4. Entrez le nom de l'utilisateur, son adresse e-mail et son mot de passe temporaire.

L'utilisateur doit modifier le mot de passe lors de sa première connexion.

5. Sélectionnez un rôle d'utilisateur avec les autorisations système appropriées.

Chaque rôle offre les autorisations suivantes :

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

6. Pour ajouter des contraintes à un utilisateur avec un rôle membre ou visualiseur, activez la case à cocher **restreindre le rôle aux contraintes**.

Pour plus d'informations sur l'ajout de contraintes, voir "[Gérez les utilisateurs et les rôles locaux](#)".

7. Sélectionnez **Ajouter**.

Gérer les mots de passe

Vous pouvez gérer les mots de passe des comptes utilisateur dans Astra Control Center.

Changer votre mot de passe

Vous pouvez modifier le mot de passe de votre compte utilisateur à tout moment.

Étapes

1. Sélectionnez l'icône utilisateur en haut à droite de l'écran.
2. Sélectionnez **Profile**.
3. Dans le menu Options de la colonne **actions**, sélectionnez **changer mot de passe**.
4. Saisissez un mot de passe conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.
6. Sélectionnez **changer mot de passe**.

Réinitialiser le mot de passe d'un autre utilisateur

Si votre compte dispose des autorisations de rôle Administrateur ou propriétaire, vous pouvez réinitialiser les mots de passe des autres comptes utilisateur ainsi que les vôtres. Lorsque vous réinitialisez un mot de passe, vous attribuez un mot de passe temporaire que l'utilisateur devra modifier lors de la connexion.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez la liste déroulante **actions**.
3. Sélectionnez **Réinitialiser le mot de passe**.
4. Saisissez un mot de passe temporaire conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.



Lors de la prochaine connexion de l'utilisateur, l'utilisateur est invité à modifier le mot de passe.

6. Sélectionnez **Réinitialiser le mot de passe**.

Supprimer des utilisateurs

Les utilisateurs disposant du rôle propriétaire ou administrateur peuvent à tout moment supprimer d'autres utilisateurs du compte.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Dans l'onglet **Users**, cochez la case de la ligne de chaque utilisateur que vous souhaitez supprimer.

3. Dans le menu Options de la colonne **actions**, sélectionnez **Supprimer utilisateur/s**.
4. Lorsque vous y êtes invité, confirmez la suppression en saisissant le mot "supprimer", puis sélectionnez **Oui, Supprimer l'utilisateur**.

Résultat

Astra Control Center supprime l'utilisateur du compte.

Gérez les rôles

Vous pouvez gérer les rôles en ajoutant des contraintes d'espace de noms et en restreignant les rôles des utilisateurs à ces contraintes. Cela vous permet de contrôler l'accès aux ressources de votre organisation. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "[API de contrôle Astra](#)" pour gérer les rôles.

Ajoutez une contrainte d'espace de noms à un rôle

Un administrateur ou un propriétaire peut ajouter des contraintes d'espace de noms aux rôles de membre ou de visualiseur.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur.
4. Sélectionnez **Modifier le rôle**.
5. Activez la case à cocher **restreindre le rôle aux contraintes**.

La case à cocher n'est disponible que pour les rôles de membre ou de visualiseur. Vous pouvez sélectionner un autre rôle dans la liste déroulante **role**.

6. Sélectionnez **Ajouter une contrainte**.

Vous pouvez afficher la liste des contraintes disponibles par espace de noms ou par étiquette d'espace de noms.

7. Dans la liste déroulante **Type de contrainte**, sélectionnez **espace de noms Kubernetes** ou **étiquette d'espace de noms Kubernetes** selon la configuration de vos espaces de noms.
8. Sélectionnez un ou plusieurs espaces de noms ou étiquettes dans la liste pour composer une contrainte qui restreint les rôles à ces espaces de noms.
9. Sélectionnez **confirmer**.

La page **Modifier rôle** affiche la liste des contraintes que vous avez choisies pour ce rôle.

10. Sélectionnez **confirmer**.

Sur la page **compte**, vous pouvez afficher les contraintes pour n'importe quel rôle de membre ou de visualiseur dans la colonne **rôle**.



Si vous activez des contraintes pour un rôle et que vous sélectionnez **confirmer** sans ajouter de contraintes, le rôle est considéré comme étant soumis à des restrictions complètes (le rôle est refusé l'accès aux ressources affectées aux espaces de noms).

Supprime une contrainte d'espace de noms d'un rôle

Un utilisateur Admin ou propriétaire peut supprimer une contrainte d'espace de noms d'un rôle.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur ayant des contraintes actives.
4. Sélectionnez **Modifier le rôle**.

La boîte de dialogue **Modifier le rôle** affiche les contraintes actives du rôle.

5. Sélectionnez **X** à droite de la contrainte à supprimer.
6. Sélectionnez **confirmer**.

Pour en savoir plus

- ["Rôles et espaces de noms d'utilisateur"](#)

Gérer l'authentification à distance

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control.

À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP.



ASTRA Control Center utilise l'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.

Ajoutez un certificat pour l'authentification LDAPS

Ajoutez le certificat TLS privé pour le serveur LDAP afin que Astra Control Center puisse s'authentifier auprès du serveur LDAP lorsque vous utilisez une connexion LDAPS. Vous ne devez le faire qu'une seule fois, ou lorsque le certificat que vous avez installé expire.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **certificats**.
3. Sélectionnez **Ajouter**.

4. Téléchargez le `.pem` importez ou collez le contenu du fichier à partir du presse-papiers.
5. Cochez la case **approuvé**.
6. Sélectionnez **Ajouter un certificat**.

Activez l'authentification à distance

Vous pouvez activer l'authentification LDAP et configurer la connexion entre Astra Control et le serveur LDAP distant.

Avant de commencer

Si vous prévoyez d'utiliser LDAPS, assurez-vous que le certificat TLS privé pour le serveur LDAP est installé dans Astra Control Center afin que le centre de contrôle Astra puisse s'authentifier auprès du serveur LDAP. Voir [Ajoutez un certificat pour l'authentification LDAPS](#) pour obtenir des instructions.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **connexion**.
4. Entrez l'adresse IP du serveur, le port et le protocole de connexion préféré (LDAP ou LDAPS).



Il est recommandé d'utiliser LDAPS lors de la connexion au serveur LDAP. Vous devez installer le certificat TLS privé du serveur LDAP dans Astra Control Center avant de vous connecter avec LDAPS.

5. Saisissez les informations d'identification du compte de service au format e-mail (administrator@example.com). Astra Control utilisera ces informations d'identification lors de la connexion au serveur LDAP.
6. Dans la section **correspondance utilisateur**, procédez comme suit :
 - a. Entrez le DN de base et un filtre de recherche d'utilisateur approprié à utiliser lors de la récupération des informations utilisateur à partir du serveur LDAP.
 - b. (Facultatif) si votre répertoire utilise l'attribut de connexion utilisateur `userPrincipalName` au lieu de `mail`, entrez `userPrincipalName` dans l'attribut correct dans le champ **User login attribute**.
7. Dans la section **correspondance de groupe**, entrez le nom unique de base de recherche de groupe et un filtre de recherche de groupe personnalisé approprié.



Veillez à utiliser le nom unique de base (DN) correct et un filtre de recherche approprié pour **User Match** et **Group Match**. Le DN de base indique à Astra Control à quel niveau de l'arborescence de répertoire démarrer la recherche, et le filtre de recherche limite les parties de l'arborescence de répertoires Astra Control à partir de.

8. Sélectionnez **soumettre**.

Résultat

L'état du volet **authentification à distance** passe à **en attente**, puis à **connecté** lorsque la connexion au serveur LDAP est établie.

Désactiver l'authentification à distance

Vous pouvez désactiver temporairement une connexion active au serveur LDAP.



Lorsque vous désactivez une connexion à un serveur LDAP, tous les paramètres sont enregistrés et tous les utilisateurs et groupes distants ajoutés à Astra Control à partir de ce serveur LDAP sont conservés. Vous pouvez vous reconnecter à ce serveur LDAP à tout moment.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Désactiver**.

Résultat

L'état du volet **authentification à distance** passe à **Désactivé**. Tous les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont conservés et vous pouvez réactiver la connexion à tout moment.

Modifier les paramètres d'authentification à distance

Si vous avez désactivé la connexion au serveur LDAP ou si le volet **authentification à distance** est à l'état "erreur de connexion", vous pouvez modifier les paramètres de configuration.



Vous ne pouvez pas modifier l'adresse IP ou l'URL du serveur LDAP lorsque le volet **authentification distante** est à l'état "Désactivé". Vous devez le faire [Déconnectez l'authentification à distance](#) tout d'abord.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Modifier**.
4. Apportez les modifications nécessaires et sélectionnez **Modifier**.

Déconnectez l'authentification à distance

Vous pouvez vous déconnecter d'un serveur LDAP et supprimer les paramètres de configuration d'Astra Control.



Si vous êtes un utilisateur LDAP et que vous vous déconnectez, votre session prend fin immédiatement. Lorsque vous vous déconnectez du serveur LDAP, tous les paramètres de configuration de ce serveur LDAP sont supprimés d'Astra Control, ainsi que tous les utilisateurs et groupes distants ajoutés à partir de ce serveur LDAP.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **déconnecter**.

Résultat

L'état du volet **authentification à distance** passe à **déconnecté**. Les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont supprimés d'Astra Control.

Gérez des utilisateurs et des groupes distants

Si vous avez activé l'authentification LDAP sur votre système Astra Control, vous pouvez rechercher des utilisateurs et des groupes LDAP et les inclure dans les utilisateurs approuvés du système.

Ajouter un utilisateur distant

Les propriétaires et administrateurs de comptes peuvent ajouter des utilisateurs distants à Astra Control. ASTRA Control Center prend en charge jusqu'à 10,000 utilisateurs distants LDAP.



ASTRA Control Center utilise l'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.



Vous ne pouvez pas ajouter un utilisateur distant si un utilisateur local avec la même adresse e-mail (basée sur l'attribut « mail » ou « nom principal de l'utilisateur ») existe déjà sur le système. Pour ajouter l'utilisateur en tant qu'utilisateur distant, supprimez d'abord l'utilisateur local du système.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **utilisateurs distants**.
4. Sélectionnez **Ajouter**.
5. Vous pouvez également rechercher un utilisateur LDAP en saisissant l'adresse e-mail de l'utilisateur dans le champ **Filter by email**.
6. Sélectionnez un ou plusieurs utilisateurs dans la liste.
7. Attribuez un rôle à l'utilisateur.



Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à cet utilisateur et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.



Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouvel utilisateur apparaît dans la liste des utilisateurs distants. Dans cette liste, vous pouvez voir les contraintes actives sur l'utilisateur et gérer l'utilisateur à partir du menu **actions**.

Ajouter un groupe distant

Pour ajouter plusieurs utilisateurs distants à la fois, les propriétaires et administrateurs de comptes peuvent ajouter des groupes distants à Astra Control. Lorsque vous ajoutez un groupe distant, tous les utilisateurs distants de ce groupe peuvent se connecter à Astra Control et héritent du même rôle que le groupe.

ASTRA Control Center prend en charge jusqu'à 5,000 groupes distants LDAP.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **Remote Groups**.
4. Sélectionnez **Ajouter**.

Dans cette fenêtre, vous pouvez voir une liste des noms communs et des noms distinctifs des groupes LDAP récupérés par Astra Control à partir du répertoire.

5. Vous pouvez également rechercher un groupe LDAP en saisissant le nom commun du groupe dans le champ **Filter by common name**.
6. Sélectionnez un ou plusieurs groupes dans la liste.
7. Attribuez un rôle aux groupes.



Le rôle que vous sélectionnez est attribué à tous les utilisateurs de ce groupe. Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle le plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à ce groupe et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.



Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouveau groupe apparaît dans la liste des groupes distants. Les utilisateurs distants de ce groupe n'apparaissent pas dans la liste des utilisateurs distants tant que chaque utilisateur distant ne se connecte pas. Dans cette liste, vous pouvez afficher les détails du groupe et gérer le groupe à partir du menu **actions**.

Afficher et gérer les notifications

Astra vous avertit lorsque les actions sont terminées ou en échec. Par exemple, vous verrez une notification si une sauvegarde d'une application a réussi.

Vous pouvez gérer ces notifications en haut à droite de l'interface :



Étapes

1. Sélectionnez le nombre de notifications non lues en haut à droite.
2. Examinez les notifications, puis sélectionnez **Marquer comme lu** ou **Afficher toutes les notifications**.

Si vous avez sélectionné **Afficher toutes les notifications**, la page Notifications se charge.

3. Sur la page **Notifications**, affichez les notifications, sélectionnez celles que vous souhaitez marquer comme lu, sélectionnez **action** et **Marquer comme lu**.

Ajouter et supprimer des informations d'identification

Ajoutez et supprimez des identifiants pour les fournisseurs de cloud privé local, comme ONTAP S3, les clusters Kubernetes gérés avec OpenShift ou les clusters Kubernetes non gérés depuis votre compte à tout moment. Astra Control Center utilise ces identifiants pour détecter les clusters Kubernetes et les applications sur les clusters et provisionner les ressources en votre nom.

Notez que tous les utilisateurs d'Astra Control Center partagent les mêmes informations d'identification.

Ajouter des informations d'identification

Vous pouvez ajouter des informations d'identification à Astra Control Center lorsque vous gérez des clusters. Pour ajouter des informations d'identification en ajoutant un nouveau cluster, reportez-vous à la section "[Ajouter un cluster Kubernetes](#)".



Si vous créez votre propre fichier kubeconfig, vous ne devez définir que l'élément de contexte **one**. Reportez-vous à la section "[Documentation Kubernetes](#)" pour plus d'informations sur la création de fichiers kubeconfig.

Supprimer les informations d'identification

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



Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control Center est toujours utilisé car Astra Control Center utilise les informations d'identification pour s'authentifier auprès du compartiment de secours. Il est préférable de ne pas supprimer ces informations d'identification.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **informations d'identification**.
3. Sélectionnez le menu Options dans la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer les informations d'identification**.

Résultat

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

Surveillez l'activité des comptes

Vous pouvez consulter les détails des activités de votre compte Astra Control. Par exemple, lorsque de nouveaux utilisateurs ont été invités, lorsqu'un cluster a été ajouté ou lorsqu'un snapshot a été créé. Vous pouvez également exporter votre activité de compte vers un fichier CSV.



Si vous gérez des clusters Kubernetes à partir d'Astra Control et qu'Astra Control est connecté à Cloud Insights, Astra Control envoie des journaux d'événements à Cloud Insights. Les informations du journal, y compris les informations sur le déploiement du pod et les pièces jointes en PVC, apparaissent dans le journal des activités de contrôle Astra. Utilisez ces informations pour identifier les problèmes éventuels sur les clusters Kubernetes que vous gérez.

Afficher toutes les activités du compte dans Astra Control

1. Sélectionnez **activité**.
2. Utilisez les filtres pour réduire la liste des activités ou utilisez la zone de recherche pour trouver exactement ce que vous recherchez.
3. Sélectionnez **Exporter au format CSV** pour télécharger l'activité de votre compte dans un fichier CSV.

Afficher l'activité d'un compte pour une application spécifique

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **activité**.

Afficher l'activité des comptes pour les clusters

1. Sélectionnez **clusters**, puis le nom du cluster.
2. Sélectionnez **activité**.

Prenez des mesures pour résoudre les événements qui nécessitent votre attention

1. Sélectionnez **activité**.

2. Sélectionnez un événement qui nécessite une attention particulière.
3. Sélectionnez l'option de liste déroulante **prendre une action**.

Dans cette liste, vous pouvez consulter les actions correctives possibles, consulter la documentation associée au problème et obtenir de l'aide pour résoudre ce dernier.

Mettre à jour une licence existante

Vous pouvez convertir une licence d'évaluation en licence complète, ou mettre à jour une évaluation existante ou une licence complète avec une nouvelle licence. Si vous ne disposez pas d'une licence complète, contactez votre contact commercial NetApp pour obtenir une licence complète et un numéro de série. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou "[API de contrôle Astra](#)" pour mettre à jour une licence existante.

Étapes

1. Connectez-vous au "[Site de support NetApp](#)".
2. Accédez à la page de téléchargement d'Astra Control Center, entrez le numéro de série et téléchargez le fichier de licence NetApp complet (NLF).
3. Connectez-vous à l'interface utilisateur du centre de contrôle Astra.
4. Dans le menu de navigation de gauche, sélectionnez **compte > Licence**.
5. Dans la page **compte > Licence**, sélectionnez le menu déroulant d'état de la licence existante et sélectionnez **remplacer**.
6. Accédez au fichier de licence que vous avez téléchargé.
7. Sélectionnez **Ajouter**.

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

Pour en savoir plus

- "[Licence Astra Control Center](#)"

Gestion des compartiments

Un fournisseur de compartiments de stockage est essentiel pour la sauvegarde de vos applications et du stockage persistant, ou pour le clonage d'applications entre les clusters. Avec Astra Control Center, ajoutez un fournisseur de magasin d'objets comme destination de sauvegarde externe pour vos applications.

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

Utilisez l'un des fournisseurs de compartiments Amazon simple Storage Service (S3) suivants :

- NetApp ONTAP S3
- NetApp StorageGRID S3

- Microsoft Azure
- S3 générique



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



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

Un godet peut être dans l'un des États suivants :

- En attente : le compartiment est planifié pour la découverte.
- Disponible : le godet est disponible.
- Retiré : le godet n'est pas accessible actuellement.

Pour plus d'informations sur la gestion des compartiments à l'aide de l'API de contrôle Astra, reportez-vous au ["Informations sur l'automatisation et les API d'Astra"](#).

Vous pouvez effectuer les tâches suivantes liées à la gestion des compartiments :

- ["Ajouter un godet"](#)
- [Modifier un godet](#)
- [Définir le compartiment par défaut](#)
- [Faire pivoter ou supprimer les identifiants de compartiment](#)
- [Déposer un godet](#)



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

Modifier un godet

Vous pouvez modifier les informations d'identification d'accès pour un compartiment et modifier si un compartiment sélectionné est le compartiment par défaut.



Lorsque vous ajoutez un compartiment, sélectionnez le fournisseur approprié et fournissez les identifiants appropriés pour ce fournisseur. Par exemple, l'interface utilisateur accepte NetApp ONTAP S3 comme type et accepte les identifiants StorageGRID. Toutefois, toutes les futures sauvegardes et restaurations des applications à l'aide de ce compartiment échoueront. Voir la ["Notes de version"](#).

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu de la colonne **actions**, sélectionnez **Modifier**.
3. Modifier toute information autre que le type de godet.



Vous ne pouvez pas modifier le type de compartiment.

4. Sélectionnez **mettre à jour**.

Définir le compartiment par défaut

Lorsque vous effectuez un clone entre les clusters, Astra Control requiert un compartiment par défaut. La procédure suivante permet de définir un compartiment par défaut pour l'ensemble des clusters.

Étapes

1. Accédez à **Cloud instances**.
2. Sélectionnez le menu dans la colonne **actions** pour l'instance de Cloud dans la liste.
3. Sélectionnez **Modifier**.
4. Dans la liste **godet**, sélectionnez le compartiment par défaut.
5. Sélectionnez **Enregistrer**.

Faire pivoter ou supprimer les identifiants de compartiment

Astra Control utilise des identifiants de compartiment pour accéder à ce compartiment et fournit des clés secrètes pour le compartiment S3 afin qu'Astra Control Center puisse communiquer avec le compartiment.

Faire pivoter les identifiants du godet

Si vous faites pivoter les informations d'identification, faites-les pivoter pendant une fenêtre de maintenance lorsqu'aucune sauvegarde n'est en cours (planifiée ou à la demande).

Procédure de modification et de rotation des informations d'identification

1. Dans le menu de navigation de gauche, sélectionnez **seaux**.
2. Dans le menu Options de la colonne **actions**, sélectionnez **Modifier**.
3. Créer les nouvelles informations d'identification.
4. Sélectionnez **mettre à jour**.

Supprimer les identifiants du compartiment

Le retrait des identifiants de compartiment est uniquement possible si de nouvelles informations d'identification ont été appliquées à un compartiment ou si ce dernier n'est plus utilisé activement.



Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control est toujours utilisé car Astra Control utilise les informations d'identification pour authentifier le compartiment de secours. Ne pas supprimer ces identifiants si le compartiment est en cours d'utilisation, car cela entraînera des défaillances de sauvegarde et des problèmes d'indisponibilité des sauvegardes.



Si vous supprimez les identifiants de compartiment actifs, reportez-vous à la section "[dépannage de la dépose des informations d'identification du godet](#)".

Pour obtenir des instructions sur la suppression des informations d'identification S3 à l'aide de l'API de contrôle Astra, reportez-vous au "[Informations sur l'automatisation et les API d'Astra](#)".

Déposer un godet

Il est possible de retirer un godet qui n'est plus utilisé ou qui n'est pas en bon état. Pour simplifier et à jour la configuration du magasin d'objets,



- Vous ne pouvez pas supprimer un compartiment par défaut. Si vous souhaitez retirer ce compartiment, sélectionnez tout d'abord un autre compartiment comme valeur par défaut.
- Vous ne pouvez pas supprimer un compartiment WORM (Write Once, Read Many) avant l'expiration de la période de conservation du fournisseur cloud du compartiment. Les godets À VIS SANS FIN sont signalés par « verrouillé » à côté du nom du compartiment.

- Vous ne pouvez pas supprimer un compartiment par défaut. Si vous souhaitez retirer ce compartiment, sélectionnez tout d'abord un autre compartiment comme valeur par défaut.

Avant de commencer

- Avant de commencer, assurez-vous qu'aucune sauvegarde n'est en cours d'exécution ou terminée pour ce compartiment.
- Vérifiez que le godet n'est pas utilisé dans le cadre d'une politique de protection active.

Si c'est le cas, vous ne pourrez pas continuer.

Étapes

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



Astra Control veille à l'absence de règles de planification qui utilise le compartiment pour les sauvegardes et à l'absence de sauvegardes actives dans le compartiment.

3. Tapez « Supprimer » pour confirmer l'action.
4. Sélectionnez **Oui, retirez le godet**.

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](#)
- [Modifier les détails de l'authentification du système back-end du stockage](#)
- [Gérez un système back-end de stockage découvert](#)
- [Annuler la gestion d'un système back-end](#)
- [Retirer un système back-end](#)

Afficher les détails du système back-end

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

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

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Tableau de bord**.
2. Vérifiez le panneau Storage backend du tableau de bord indiquant l'état :
 - **Malsain**: Le stockage n'est pas dans un état optimal. Cela peut être dû à un problème de latence ou à une application dégradée en raison d'un problème de conteneur, par exemple.
 - **Tout en bonne santé**: Le stockage a été géré et est dans un état optimal.
 - **Découvert**: Le stockage a été découvert, mais pas géré par Astra Control.

Afficher les détails du système de stockage back-end à partir de l'option Backends

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

Vous pouvez voir les volumes utilisés par les applications Kubernetes, qui sont stockés sur un back-end de stockage sélectionné. Avec Cloud Insights, des informations supplémentaires s'affichent. Voir "[Documentation Cloud Insights](#)".

Étapes

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



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

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

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

Modifier les détails de l'authentification du système back-end du stockage

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

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

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

Pour plus d'informations sur l'activation de l'authentification basée sur un certificat, reportez-vous à la section "[Activez l'authentification sur le back-end de stockage ONTAP](#)".

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez le système back-end.
3. Dans le champ informations d'identification, sélectionnez l'icône **Modifier**.

4. Dans la page Modifier, sélectionnez l'une des options suivantes.
 - **Utiliser les informations d'identification de l'administrateur** : saisissez l'adresse IP de gestion du cluster ONTAP et les informations d'identification de l'administrateur. Les identifiants doivent être identifiants au niveau du cluster.



L'utilisateur dont vous saisissez ici les informations d'identification doit disposer du `ontapi` Méthode d'accès de connexion utilisateur activée dans ONTAP System Manager sur le cluster ONTAP. Si vous prévoyez d'utiliser la réplication SnapMirror, appliquez les identifiants de l'utilisateur au rôle « admin », qui dispose des méthodes d'accès `ontapi` et `http`, Sur les clusters ONTAP source et destination. Reportez-vous à la section "[Gérer les comptes utilisateur dans la documentation ONTAP](#)" pour en savoir plus.

- **Utiliser un certificat**: Télécharger le certificat `.pem` fichier, la clé de certificat `.key` et éventuellement le fichier de l'autorité de certification.

5. Sélectionnez **Enregistrer**.

Gérez un système back-end de stockage découvert

Vous pouvez choisir de gérer un système back-end de stockage non géré, mais découvert. Lorsque vous gérez un système back-end de stockage, Astra Control indique si un certificat pour l'authentification a expiré.

Étapes

1. Dans le menu de navigation de gauche, sélectionnez **Backends**.
2. Sélectionnez l'option **découvert**.
3. Sélectionnez le système back-end.
4. Dans le menu Options de la colonne **actions**, sélectionnez **gérer**.
5. Effectuez les modifications.
6. Sélectionnez **Enregistrer**.

Annuler la gestion d'un système back-end

Vous pouvez annuler la gestion du système back-end.

Étapes

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

Retirer un système back-end

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

Avant de commencer

- Assurez-vous que le système de stockage back-end n'est pas géré.
- Assurez-vous que le système back-end ne dispose d'aucun volume associé au cluster.

Étapes

1. Dans le menu de navigation gauche, sélectionnez **Backends**.
2. Si le système back-end est géré, le annuler sa gestion.
 - a. Sélectionnez **géré**.
 - b. Sélectionnez le système back-end.
 - c. Dans l'option **actions**, sélectionnez **Unmanage**.
 - d. Saisissez « Unmanage » pour confirmer l'action.
 - e. Sélectionnez **Oui, annulez la gestion du stockage back-end**.
3. Sélectionnez **découvert**.
 - a. Sélectionnez le système back-end.
 - b. Dans l'option **actions**, sélectionnez **Supprimer**.
 - c. Tapez « Supprimer » pour confirmer l'action.
 - d. Sélectionnez **Oui, retirez le back-end de stockage**.

Trouvez plus d'informations

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

Surveillez les tâches en cours d'exécution

Vous pouvez afficher des détails sur l'exécution des tâches et des tâches qui ont terminé, échoué ou ont été annulées au cours des 24 dernières heures dans Astra Control. Par exemple, vous pouvez afficher l'état d'une opération de sauvegarde, de restauration ou de clonage. Pour plus d'informations, reportez-vous aux pourcentages terminés et au temps restant estimé. Vous pouvez afficher l'état d'une opération planifiée exécutée ou d'une opération que vous avez démarrée manuellement.

Lors de l'affichage d'une tâche en cours d'exécution ou terminée, vous pouvez développer les détails de la tâche pour afficher l'état de chacune des sous-tâches. La barre de progression de la tâche est verte pour les tâches en cours ou terminées, bleue pour les tâches annulées et rouge pour les tâches ayant échoué en raison d'une erreur.



Pour les opérations de clonage, les sous-tâches se composent d'un snapshot et d'une opération de restauration de snapshot.

Pour plus d'informations sur les tâches ayant échoué, reportez-vous à la section ["Surveillez l'activité des comptes"](#).

Étapes

1. Pendant qu'une tâche est en cours d'exécution, accédez à **applications**.
2. Sélectionnez le nom d'une application dans la liste.

3. Dans les détails de l'application, sélectionnez l'onglet **tâches**.

Vous pouvez afficher les détails des tâches actuelles ou passées et filtrer par état de tâche.



Les tâches sont conservées dans la liste **tâches** pour un maximum de 24 heures. Vous pouvez configurer cette limite et d'autres paramètres du moniteur de tâches à l'aide de l' "[API de contrôle Astra](#)".

Surveillez l'infrastructure avec des connexions Cloud Insights, Prometheus ou Fluentd

Vous pouvez configurer plusieurs paramètres en option pour améliorer votre expérience avec Astra Control Center. Pour contrôler l'ensemble de votre infrastructure et obtenir des informations exploitables, créez une connexion à NetApp Cloud Insights, configurez Prometheus ou ajoutez une connexion Fluentd.

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

- [Connectez-vous à Cloud Insights](#)
- [Connectez-vous à Prometheus](#)
- [Connectez-vous à Fluentd](#)

Ajoutez un serveur proxy pour les connexions à Cloud Insights ou au site de support NetApp

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



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

Étapes

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



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected

Connect

4. Entrez le nom du serveur proxy ou l'adresse IP et le numéro du port proxy.

5. Si votre serveur proxy nécessite une authentification, cochez la case et saisissez le nom d'utilisateur et le mot de passe.
6. Sélectionnez **connexion**.

Résultat

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



Connected



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Modifier les paramètres du serveur proxy

Vous pouvez modifier les paramètres du serveur proxy.

Étapes

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

Désactiver la connexion au serveur proxy

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

Étapes

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

Connectez-vous à Cloud Insights

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

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

Lorsque le centre de contrôle Astra est connecté à Cloud Insights, un pod d'unité d'acquisition est créé. Ce

pod collecte les données des systèmes back-end gérés par Astra Control Center et les pousse dans Cloud Insights. Ce pod requiert 8 Go de RAM et 2 cœurs de CPU.



Lorsque Astra Control Center est couplée à Cloud Insights, vous ne devez pas utiliser l'option **Modifier le déploiement** dans Cloud Insights.



Après avoir activé la connexion Cloud Insights, vous pouvez afficher les informations de débit sur la page **systèmes back-end** et vous connecter à Cloud Insights après avoir sélectionné un système back-end de stockage. Vous pouvez également trouver les informations sur le **Tableau de bord** dans la section cluster et vous y connecter à Cloud Insights.

Avant de commencer

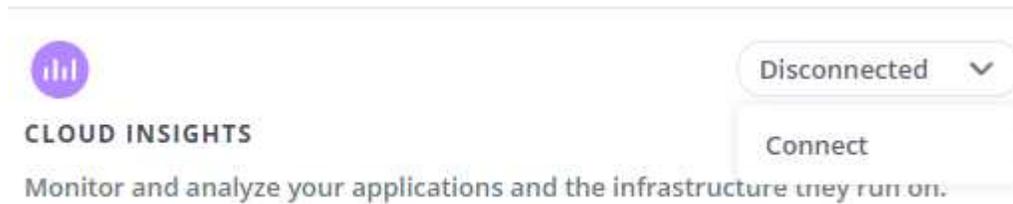
- Un compte Astra Control Center avec **admin/propriétaire** privilèges.
- Licence Astra Control Center valide.
- Un serveur proxy si le réseau sur lequel vous exécutez Astra Control Center nécessite un proxy pour se connecter à Internet.



Si vous découvrez Cloud Insights, familiarisez-vous avec les fonctions et les fonctionnalités. Reportez-vous à la section "[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**.

Cloud Insights (Trial) Tutorial 0% Complete Getting Started

MONITOR & OPTIMIZE

nmm95sx / Admin / API Access

API Access Tokens (4)

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

+ API Access Token Bulk Actions

- 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 clé de token d'accès à l'API Read/Write, sélectionnez : data ingestion, gestion des journaux, unité d'acquisition et collecte de données.



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

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

5. Sélectionnez **connexion**.



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



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

Afficher les données dans Cloud Insights

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

EXTERNAL ?

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

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

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

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

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

The screenshot shows the 'Backends' page with a table. The table has columns: Name, Status, Capacity, Throughput, Type, and Actions. A tooltip for the 'Throughput' column is open, displaying a line graph and the following metrics: 'Throughput Last 24 hrs', '5m ago: 8.00 MB/s', 'Min: 4.00 MB/s', and 'Max: 11.00 MB/s'. There is a link 'View in Cloud Insights' at the bottom of the tooltip.

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

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

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

Add →

Resource summary

The screenshot shows the Astra Control Center dashboard. It has three main sections: 'Apps', 'Clusters', and 'Storage backends'. The 'Apps' section shows 'No managed apps'. The 'Clusters' section has a 'Let's get started' message and an 'Add' button. A blue box highlights a 'View in cloud insights' link with a person icon. The 'Storage backends' section shows '1 Managed' and '0 Discovered' items.



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

Modifier la connexion Cloud Insights

Vous pouvez modifier la connexion Cloud Insights.



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

Étapes

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

Désactiver la connexion Cloud Insights

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

Étapes

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

Connectez-vous à Prometheus

Vous pouvez surveiller les données du centre de contrôle Astra avec Prometheus. Vous pouvez configurer Prometheus pour collecter des metrics à partir du terminal de metrics du cluster Kubernetes. Par ailleurs, vous

pouvez utiliser Prometheus pour visualiser les données.

Pour plus d'informations sur l'utilisation de Prometheus, consultez leur documentation à l'adresse "[Mise en route de Prometheus](#)".

Ce dont vous avez besoin

Assurez-vous que vous avez téléchargé et installé le package Prometheus sur le cluster Astra Control Center ou sur un autre cluster pouvant communiquer avec le cluster Astra Control Center.

Suivez les instructions de la documentation officielle à "[Installez Prometheus](#)".

Prometheus doit pouvoir communiquer avec le cluster Kubernetes Astra Control Center. Si Prometheus n'est pas installé sur le cluster Astra Control Center, vous devez vous assurer qu'ils peuvent communiquer avec le service de metrics exécuté sur le cluster Astra Control Center.

Configurez Prometheus

Astra Control Center expose un service de metrics sur le port TCP 9090 dans le cluster Kubernetes. Vous devez configurer Prometheus pour pouvoir collecter des metrics à partir de ce service.

Étapes

1. Connectez-vous au serveur Prometheus.
2. Ajoutez votre entrée de cluster dans le `prometheus.yml` fichier. Dans le `yml` ajoutez une entrée semblable à celle qui suit pour votre cluster dans le `scrape_configs` section:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
metrics_path: /accounts/<replace with your account ID>/metrics
authorization:
  credentials: <replace with your API token>
tls_config:
  insecure_skip_verify: true
static_configs:
  - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```



Si vous définissez le `tls_config insecure_skip_verify` à `true`, Le protocole de chiffrement TLS n'est pas requis.

3. Redémarrez le service Prometheus :

```
sudo systemctl restart prometheus
```

Accès à Prometheus

Accédez à l'URL Prometheus.

Étapes

1. Dans un navigateur, entrez l'URL Prometheus du port 9090.
2. Vérifiez votre connexion en sélectionnant **Statut > cibles**.

Affichez les données de Prometheus

Vous pouvez utiliser Prometheus pour afficher les données du centre de contrôle Astra.

Étapes

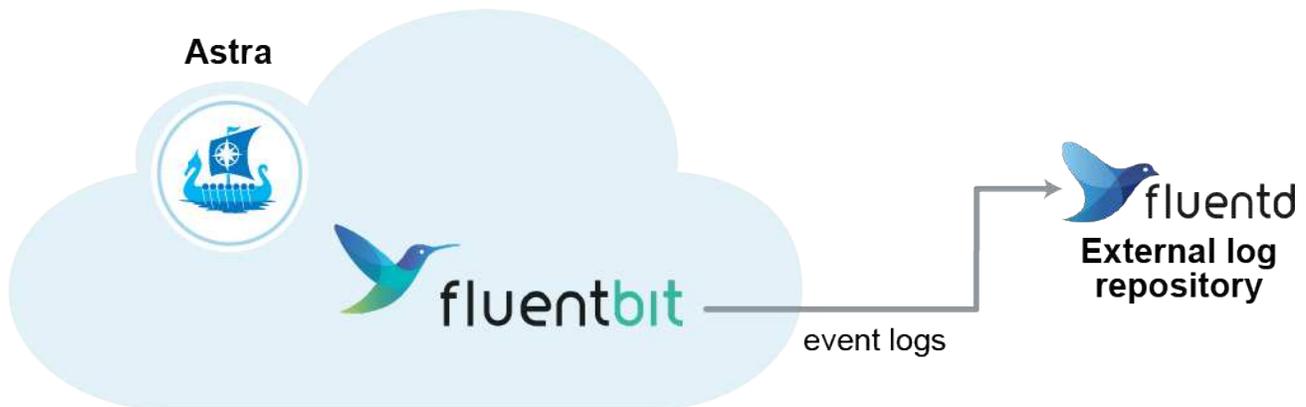
1. Dans un navigateur, entrez l'URL Prometheus.
2. Dans le menu Prometheus, sélectionnez **Graph**.
3. Pour utiliser l'Explorateur de mesures, sélectionnez l'icône en regard de **Exécuter**.
4. Sélectionnez `scrape_samples_scraped` Et sélectionnez **Exécuter**.
5. Pour voir le raclage des échantillons dans le temps, sélectionnez **Graph**.



Si plusieurs données de cluster ont été collectées, les mesures de chaque cluster apparaissent dans une couleur différente.

Connectez-vous à Fluentd

Vous pouvez envoyer des journaux (événements Kubernetes) à partir d'un système surveillé par Astra Control Center vers votre terminal Fluentd. La connexion Fluentd est désactivée par défaut.



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

Avant de commencer

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

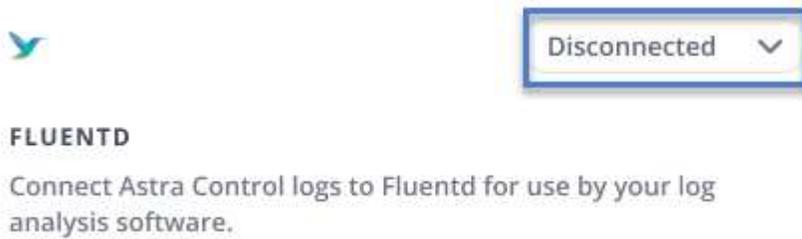


Astra Control Center ne valide pas les détails que vous entrez pour votre serveur Fluentd. Assurez-vous de saisir les valeurs correctes.

Étapes

1. Connectez-vous à Astra Control Center à l'aide d'un compte disposant du privilège **admin/propriétaire**.

2. Sélectionnez **compte > connexions**.
3. Sélectionnez **Connect** dans la liste déroulante où apparaît **déconnecté** pour ajouter la connexion.



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

Résultat

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

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

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



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

Modifiez la connexion Fluentd

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

Étapes

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

Désactivez la connexion Fluentd

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

Étapes

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

Annuler la gestion des applications et des clusters

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

Annuler la gestion d'une application

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

Lorsque vous annulez la gestion d'une application :

- Toutes les sauvegardes et tous les instantanés existants seront supprimés.
- Les applications et les données restent disponibles.

Étapes

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

Résultat

Astra Control Center cesse de gérer l'application.

Annuler la gestion d'un cluster

Arrêtez de gérer le cluster que vous ne souhaitez plus gérer à partir d'Astra Control Center.



Avant d'annuler la gestion du cluster, vous devez annuler la gestion des applications associées au cluster.

Lorsque vous dégérez un cluster :

- Cette action empêche votre cluster d'être géré par Astra Control Center. Elle ne modifie pas la configuration du cluster et ne supprime pas le cluster.
- Astra Trident ne sera pas désinstallé du cluster. "[Découvrez comment désinstaller Astra Trident](#)".

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **clusters**.
2. Cochez la case correspondant au cluster que vous ne souhaitez plus gérer.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Unmanage**.
4. Confirmez que vous souhaitez annuler la gestion du cluster, puis sélectionnez **Oui, Unmanage cluster**.

Résultat

L'état du cluster devient **Suppression**. Ensuite, le cluster sera supprimé de la page **clusters** et il n'est plus

géré par Astra Control Center.



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. Vous pouvez utiliser cette procédure pour mettre à niveau Astra Control Center dans des environnements connectés à Internet ou à air comprimé.

Ces instructions décrivent le processus de mise à niveau d'Astra Control Center, qui passe de la deuxième version la plus récente à cette version actuelle. Vous ne pouvez pas effectuer une mise à niveau directement à partir d'une version qui est à au moins deux versions derrière la version actuelle. Si la version d'Astra Control Center installée est plusieurs versions derrière la dernière version, vous devrez peut-être effectuer des mises à niveau de chaîne vers des versions plus récentes jusqu'à ce que votre Astra Control Center installée ne soit qu'une seule version derrière la dernière version. Pour obtenir la liste complète des versions publiées, reportez-vous au "[notes de version](#)".

Avant de commencer

Avant de procéder à la mise à niveau, assurez-vous que votre environnement respecte toujours le "[Configuration minimale requise pour le déploiement d'Astra Control Center](#)". Votre environnement doit disposer des éléments suivants :

- A "**pris en charge**" Version d'Astra Trident

Développez pour les étapes

Déterminez la version de Trident que vous exécutez :

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



Le cas échéant, mettez à niveau Astra Trident en utilisant ces outils "[instructions](#)".



La version 23.10 est la dernière version d'Astra Control Center à prendre en charge Astra Trident. Il est fortement recommandé que vous "[Activez le mécanisme de provisionnement Astra Control](#)". D'accéder à des fonctionnalités avancées de gestion et de provisionnement du stockage qui vont au-delà de celles d'Astra Trident. Vous devez tous les deux effectuer une mise à niveau vers Astra Control Center 23.10 et activer Astra Control Provisioner pour utiliser cette fonctionnalité étendue. ASTRA Control Provisioner ne fonctionnera pas avec les versions antérieures d'Astra Control Center.

- Une distribution Kubernetes prise en charge

Développez pour les étapes

Déterminez la version Kubernetes que vous exécutez :

```
kubectl get nodes -o wide
```

- **Ressources du cluster suffisantes**

Développez pour les étapes

Déterminer les ressources disponibles du cluster :

```
kubectl describe node <node name>
```

- **Un registre que vous pouvez utiliser pour envoyer et télécharger des images Astra Control Center**
- **Une classe de stockage par défaut**

Développez pour les étapes

Déterminez votre classe de stockage par défaut :

```
kubectl get storageclass
```

- **Services API sains et disponibles**

Développez pour les étapes

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

```
kubectl get apiservices
```

- *** (OpenShift uniquement) opérateurs de grappes sains et disponibles***

Développez pour les étapes

S'assurer que tous les opérateurs du groupe d'instruments sont en état de fonctionnement et disponibles.

```
kubectl get clusteroperators
```

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

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

Développez pour les étapes

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

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

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

c. Connectez-vous au registre Astra Control :

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

Description de la tâche

Le processus de mise à niveau d'Astra Control Center vous guide à travers les étapes de haut niveau suivantes :



Déconnectez-vous de l'interface utilisateur de l'Astra Control Center avant de commencer la mise à niveau.

- [Téléchargez et extrayez Astra Control Center](#)
- [Retirez le plug-in NetApp Astra kubectl et réinstallez-le](#)
- [Ajoutez les images à votre registre local](#)
- [Poser le conducteur du centre de commande Astra mis à jour](#)
- [Mettez à niveau Astra Control Center](#)
- [Vérifiez l'état du système](#)



Ne supprimez pas l'opérateur du centre de contrôle Astra (par exemple, `kubectl delete -f astra_control_center_operator_deploy.yaml`) À tout moment pendant la mise à niveau ou l'opération Astra Control Center pour éviter de supprimer des modules.



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.

Téléchargez et extrayez Astra Control Center

Vous pouvez choisir de télécharger le bundle Astra Control Center depuis le site du support NetApp ou d'utiliser Docker pour extraire le bundle du registre d'images Astra Control Service.

Site de support NetApp

1. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`) du "[Page de téléchargements d'Astra Control Center](#)".
2. (Recommandé mais facultatif) Téléchargez le lot de certificats et de signatures pour Astra Control Center (`astra-control-center-certs-[version].tar.gz`) pour vérifier la signature du paquet.

Développez pour plus d'informations

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

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

La sortie s'affiche `Verified OK` une fois la vérification terminée.

3. Extraire les images du pack Astra Control Center :

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

Registre d'images Astra Control

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

Retirez le plug-in NetApp Astra kubectl et réinstallez-le

Vous pouvez utiliser le plug-in de ligne de commande NetApp Astra kubectl pour envoyer les images vers un référentiel Docker local.

1. Déterminez si le plug-in est installé :

```
kubectl astra
```

2. Faites l'une des actions suivantes :
 - Si le plug-in est installé, la commande doit renvoyer l'aide du plug-in kubectl et vous pouvez supprimer la version existante de kubectl-astra : `delete /usr/local/bin/kubectl-astra`.
 - Si la commande renvoie une erreur, le plug-in n'est pas installé et vous pouvez passer à l'étape

suivante pour l'installer.

3. Installez le plug-in :

- a. Répertoriez les binaires NetApp Astra kubectl disponibles et notez le nom du fichier dont vous avez besoin pour votre système d'exploitation et votre architecture de processeur :



La bibliothèque de plug-ins kubectl fait partie du bundle tar et est extraite dans le dossier `kubectl-astra`.

```
ls kubectl-astra/
```

- a. Déplacez le bon binaire dans le chemin actuel et renommez-le `kubectl-astra`:

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

Ajoutez les images à votre registre local

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

Docker

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

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

2. Envoyez les images du package dans le répertoire d'images Astra Control Center vers votre registre local. Effectuez les remplacements suivants avant d'exécuter le `push-images` commande :
 - Remplacez `<BUNDLE_FILE>` par le nom du fichier bundle Astra Control (`acc.manifest.bundle.yaml`).
 - Remplacer `<MY_FULL_REGISTRY_PATH>` par l'URL du référentiel Docker, par exemple "`<a href="https://<docker-registry>" class="bare">https://<docker-registry>"`".
 - Remplacez `<MY_REGISTRY_USER>` par le nom d'utilisateur.
 - Remplacez `<MY_REGISTRY_TOKEN>` par un jeton autorisé pour le registre.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r  
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p  
<MY_REGISTRY_TOKEN>
```

Podman

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

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

2. Connectez-vous à votre registre :

```
podman login <YOUR_REGISTRY>
```

3. Préparez et exécutez l'un des scripts suivants qui est personnalisé pour la version de Podman que vous utilisez. Remplacez `<MY_FULL_REGISTRY_PATH>` par l'URL de votre référentiel qui inclut tous les sous-répertoires.

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



Le chemin d'accès à l'image que le script crée doit ressembler aux éléments suivants, selon la configuration de votre registre :

```

https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version

```

Poser le conducteur du centre de commande Astra mis à jour

1. Modifier le répertoire :

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets: [{name: astra-registry-cred}]
```

- b. Changer `ASTRA_IMAGE_REGISTRY` pour le `kube-rbac-proxy` image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).
- c. Changer `ASTRA_IMAGE_REGISTRY` pour le `acc-operator` image dans le chemin du registre où vous avez poussé les images dans un [étape précédente](#).
- d. Ajoutez les valeurs suivantes à la `env` section :

```
- name: ACCOP_HELM_UPGRADE_TIMEOUT  
  value: 300m
```

Exemple astra_control_Center_Operator_Deploy.yaml :

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_UPGRADE_TIMEOUT
              value: 300m
          image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
```

```
    port: 8081
    initialDelaySeconds: 15
    periodSeconds: 20
name: manager
readinessProbe:
  httpGet:
    path: /readyz
    port: 8081
    initialDelaySeconds: 5
    periodSeconds: 10
resources:
  limits:
    cpu: 300m
    memory: 750Mi
  requests:
    cpu: 100m
    memory: 75Mi
securityContext:
  allowPrivilegeEscalation: false
imagePullSecrets: []
securityContext:
  runAsUser: 65532
terminationGracePeriodSeconds: 10
```

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

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

Exemple de réponse :

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

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

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

Mettez à niveau Astra Control Center

1. Modifiez la ressource personnalisée Astra Control Center (CR) :

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

2. Modifier le numéro de version de l'Astra (astraVersion intérieur de spec) de 23.07.0 à 23.10.0:



Vous ne pouvez pas effectuer une mise à niveau directement à partir d'une version qui est à au moins deux versions derrière la version actuelle. Pour obtenir la liste complète des versions publiées, reportez-vous au ["notes de version"](#).

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Vérifiez que le chemin du registre d'images correspond au chemin du registre vers lequel vous avez poussé les images dans un [étape précédente](#). Mise à jour `imageRegistry` intérieur de `spec` si le registre a changé depuis votre dernière installation.

```
imageRegistry:
  name: "[your_registry_path]"
```

4. Ajoutez les éléments suivants à votre `crds` configuration à l'intérieur de `spec`:

```
crds:
  shouldUpgrade: true
```

5. Ajoutez les lignes suivantes dans `additionalValues` intérieur de `spec` Dans le CR Astra Control Center :

```
additionalValues:
  nautilus:
    startupProbe:
      periodSeconds: 30
      failureThreshold: 600
  keycloak-operator:
    livenessProbe:
      initialDelaySeconds: 180
    readinessProbe:
      initialDelaySeconds: 180
```

6. Enregistrez et quittez l'éditeur de fichiers. Les modifications seront appliquées et la mise à niveau commencera.
7. (Facultatif) Vérifiez que les modules se terminent et deviennent disponibles à nouveau :

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

8. Attendez que les conditions d'état de l'Astra Control indiquent que la mise à niveau est terminée et prête (True) :

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

Réponse :

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.10.0-68	
10.111.111.111	True		



Pour surveiller le statut de la mise à niveau pendant l'opération, exécutez la commande suivante : `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`



Pour inspecter les journaux de l'opérateur de l'Astra Control Center, exécutez la commande suivante :
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Vérifiez l'état du système

1. Connectez-vous à Astra Control Center.
2. Vérifiez que la version a été mise à niveau. Consultez la page **support** de l'interface utilisateur.
3. Vérifiez que tous vos clusters et applications gérés sont toujours présents et protégés.

Activez le mécanisme de provisionnement Astra Control

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

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

Description de la tâche

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

Pour chaque cas, la fonctionnalité de provisionneur n'est pas activée par défaut dans Astra Trident 23.10, mais peut être activée via ce processus.

Avant de commencer

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

ASTRA Control assure aux utilisateurs un provisionnement avec Astra Control Center

- **Obtenir une licence Astra Control Center** : vous aurez besoin d'une licence "[Licence Astra Control Center](#)" Pour activer le mécanisme de provisionnement Astra Control et accéder aux fonctionnalités qu'il fournit.
- **Installer ou mettre à niveau vers Astra Control Center 23.10**: Vous aurez besoin de cette version si vous prévoyez d'utiliser Astra Control Provisioner avec Astra Control.
- **Confirmez que votre cluster a une architecture système AMD64** : l'image Astra Control Provisioner est fournie dans les architectures CPU AMD64 et ARM64, mais seul AMD64 est pris en charge par Astra Control Center.
- **Obtenez un compte Astra Control Service pour l'accès au registre**: Si vous avez l'intention d'utiliser le registre Astra Control plutôt que le site de support NetApp pour télécharger l'image Astra Control provisionner, effectuez l'enregistrement pour un "[Compte Astra Control Service](#)". Une fois que vous aurez rempli le formulaire, envoyé son formulaire et créé un compte BlueXP, vous recevrez un e-mail de bienvenue Astra Control Service.
- **Si vous avez installé Astra Trident, vérifiez que sa version se trouve dans une fenêtre à quatre versions**: Vous pouvez effectuer une mise à niveau directe vers Astra Trident 23.10 avec Astra Control Provisioner si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 23.10. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 22.10 vers la version 23.10.

Utilisateurs d'Astra Control Provisioner uniquement

- **Obtenir une licence Astra Control Center** : vous aurez besoin d'une licence "[Licence Astra Control Center](#)" Pour activer le mécanisme de provisionnement Astra Control et accéder aux fonctionnalités qu'il fournit.
- **Si vous avez installé Astra Trident, vérifiez que sa version se trouve dans une fenêtre à quatre versions**: Vous pouvez effectuer une mise à niveau directe vers Astra Trident 23.10 avec Astra Control Provisioner si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 23.10. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 22.10 vers la version 23.10.
- **Obtenez un compte Astra Control Service pour l'accès au registre**: Vous aurez besoin d'accéder au registre pour télécharger les images d'Astra Control provisionner. Pour commencer, terminez l'inscription à un "[Compte Astra Control Service](#)". Une fois que vous aurez rempli le formulaire, envoyé son formulaire et créé un compte BlueXP, vous recevrez un e-mail de bienvenue Astra Control Service.

(Étape 1) Téléchargez et extrayez Astra Control Provisioner

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

(En option) site de support NetApp

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

Développez pour plus d'informations

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

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

3. Charger l'image Astra Control Provisioner :

```
docker load < trident-acp-23.10.0.tar
```

Réponse :

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Marquer l'image :

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-  
acp:23.10.0
```

5. Envoyez l'image vers votre registre personnalisé :

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Option) Registre d'images Astra Control



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

1. Accédez au registre d'images NetApp Astra Control :

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

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

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

2. Si vous disposez d'un registre personnalisé, procédez comme suit pour déplacer l'image vers votre registre personnalisé. Si vous n'utilisez pas de registre, suivez les étapes de l'opérateur Trident dans le "[section suivante](#)".



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

Docker

- a. Extrayez l'image Astra Control Provisioner du Registre :



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

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Exemple :

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

- b. Marquer l'image :

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

- c. Envoyez l'image vers votre registre personnalisé :

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Grue

- a. Copiez le manifeste Astra Control Provisioner dans votre registre personnalisé :

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

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

Déterminez si la méthode d'installation d'origine utilisait un et suivez les étapes appropriées selon votre méthode d'origine.



N'utilisez pas HHelm pour activer le mécanisme de provisionnement Astra Control. Si vous avez utilisé Helm pour l'installation d'origine et que vous effectuez une mise à niveau vers la version 23.10, vous devez utiliser l'opérateur Trident ou tridentctl pour activer Astra Control Provisioner.

Opérateur Astra Trident

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

a. Créez le CRD :

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

b. Créer l'espace de nom trident (`kubectl create namespace trident`) ou confirmez que l'espace de nom trident existe toujours (`kubectl get all -n trident`). Si l'espace de noms a été supprimé, créez-le à nouveau.

3. Mettez à jour Astra Trident vers la version 23.10.0 :



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

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

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

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

Réponse :

```
NAME      AGE
trident   21m
```

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

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

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

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

- a. Définissez un emplacement de Registre personnalisé pour l'image Astra Trident ou extrayez-le du Registre Astra Control (`tridentImage: <my_custom_registry>/trident:23.10.0` ou `tridentImage: netapp/trident:23.10.0`).
- b. Activez le mécanisme de provisionnement Astra Control (`enableACP: true`).
- c. Définissez l'emplacement de registre personnalisé pour l'image Astra Control Provisioner ou extrayez-le du registre Astra Control (`acpImage: <my_custom_registry>/trident-acp:23.10.0` ou `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).
- d. Si vous avez établi [secrets d'extraction d'image](#) plus tôt dans cette procédure, vous pouvez les définir ici (`imagePullSecrets: - <secret_name>`). Utilisez le même nom secret que celui que vous avez établi lors des étapes précédentes.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

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

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



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

9. Vérifiez le `trident-acp` le conteneur est en cours d'exécution `acpVersion` est `23.10.0` avec un état de `Installed`:

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

Réponse :

```

status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
status: Installed

```

tridentctl

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

```

./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10

```

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

```

./tridentctl -n trident version

```

Réponse :

```

+-----+-----+-----+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +-----+-----+
+-----+ | 23.10.0 | 23.10.0 | 23.10.0. | +-----+
+-----+-----+

```

Résultat

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

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

The screenshot shows the Astra Control Center interface. At the top right, there is a 'CLUSTER STATUS' section with a green checkmark and the word 'Available'. Below this, a table displays cluster details: Version (v1.23.8), Managed (2023/10/11 02:22 UTC), Location (centraluseap), and ACP Version (23.10.0). At the bottom, there are navigation tabs: Overview (selected), Namespaces, Storage, and Activity.

Version	Managed	Location	ACP Version
v1.23.8	2023/10/11 02:22 UTC	centraluseap	23.10.0

Navigation tabs: Overview, Namespaces, Storage, Activity

Pour en savoir plus

- ["Documentation sur les mises à niveau d'Astra Trident"](#)

Désinstaller Astra Control Center

Vous devrez peut-être retirer les composants du centre de contrôle Astra si vous effectuez une mise à niveau d'un essai vers une version complète du produit. Pour déposer le centre de commande Astra et le conducteur du centre de commande Astra, exécuter les commandes décrites dans cette procédure dans l'ordre.

Si vous rencontrez des problèmes avec la désinstallation, reportez-vous à la section [Dépannage des problèmes de désinstallation](#).

Avant de commencer

1. ["Annulez la gestion de toutes les applications"](#) sur les clusters.
2. ["Dégérer tous les clusters"](#).

Étapes

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

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

Résultat :

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

2. Utiliser la commande suivante pour supprimer le netapp-acc (ou nom-personnalisé) espace de noms :

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

Exemple de résultat :

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

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

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

Résultat :

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

Dépannage des problèmes de désinstallation

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

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

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

Étapes

1. Supprimer acc-monitoring agent :

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

Résultat :

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

2. Supprimez le namespace :

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

Résultat :

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

3. Confirmer la suppression des ressources :

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

Résultat :

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

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

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

Résultat de l'échantillon :

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

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

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

Résultat :

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

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

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

Étapes

1. Lister les CRD Traefik installés sur le cluster :

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

Réponse

```
ingressroutes.traefik.containo.us          2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us       2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us       2021-06-23T23:29:12Z
middlewares.traefik.containo.us           2021-06-23T23:29:12Z
middlewareetcps.traefik.containo.us        2021-06-23T23:29:12Z
serverstransports.traefik.containo.us      2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us             2021-06-23T23:29:13Z
tlsstores.traefik.containo.us             2021-06-23T23:29:14Z
traefikservices.traefik.containo.us       2021-06-23T23:29:15Z
```

2. Supprimez les CRD :

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewareetcps.traefik.containo.us
```

Trouvez plus d'informations

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

Informations sur le copyright

Copyright © 2025 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 DÉLICTEUELLE (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.