Utilisez Astra Control Center

Astra Control Center

NetApp
June 07, 2024

Sommaire

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.

De gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer des applications à l'aide d'Astra Control Center, vous devez disposer d'une licence Astra Control Center.
- **Espaces de noms** : 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 situés à l'étendue de l'espace de noms qui sont, en général, conçus avec une architecture « valeur par passe » plutôt que « par référence ». Un opérateur et l'application qu'il installe doivent utiliser le même espace de noms ; vous devrez peut-être modifier le fichier .yaml de déploiement pour que l'opérateur s'assure que c'est le cas.

  Voici quelques applications opérateur qui suivent ces modèles :

  - "Apache K8ssandra"

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

  - "IC Jenkins"
  - "Cluster Percona XtraDB"

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

Installez les applications sur votre cluster

Après vous l'avez "a ajouté votre cluster" Avec Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application dont 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.

Ce dont vous avez besoin

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

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

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.

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. Par exemple, le scénario suivant génère une situation indésirable lors de l'utilisation de la réplication NetApp SnapMirror :

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.

** a propos de l'ajout de ressources cluster-scoped à vos espaces de noms 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.

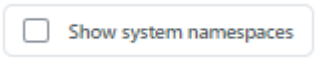
Définissez un espace de noms à gérer en tant qu'application

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. 

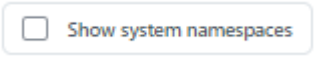
"En savoir plus".

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**.



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

Exemple : politique de protection distincte pour différentes versions

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

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

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

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

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"
- "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" Sur un cluster distant avec la technologie NetApp SnapMirror. Astra Control réplique les copies Snapshot sur un cluster distant, offrant une fonctionnalité de reprise après incident asynchrone.

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

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

Protéger les applications avec les snapshots et les sauvegardes

Protégez toutes les applications en effectuant des copies Snapshot et des sauvegardes à l'aide d'une stratégie de protection automatisée ou ad hoc. Vous pouvez utiliser l'interface utilisateur 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 règles** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

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

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

Configurer une règle de protection

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

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".

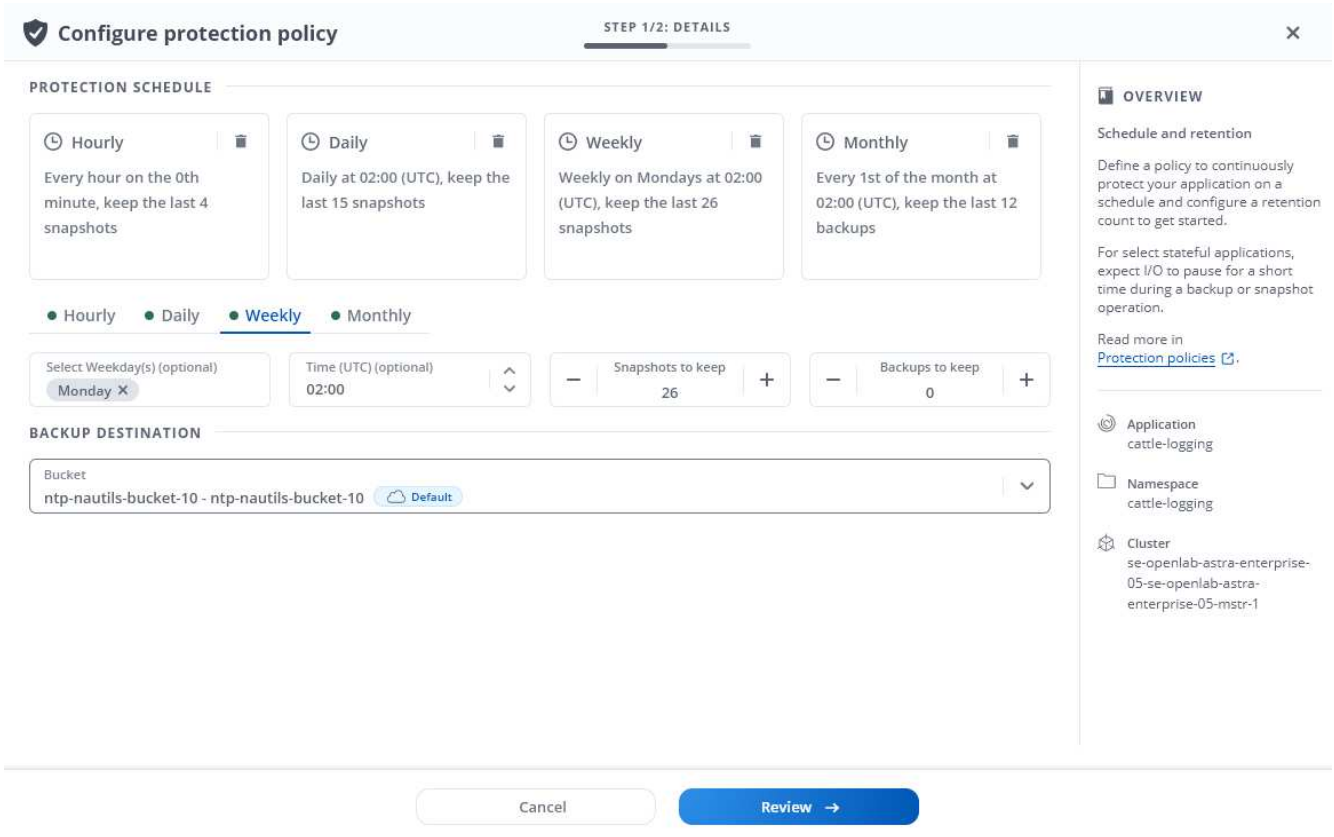
Étapes

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.



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.

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 également sauvegarder une application à tout moment.

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

Étapes

1. Sélectionnez **applications**.
2. Dans le menu Options de la colonne **actions** de l'application souhaitée, sélectionnez **Sauvegarder**.
3. Personnaliser le nom de la sauvegarde.
4. Choisissez de sauvegarder l'application à partir d'un snapshot existant. Si vous sélectionnez cette option, vous pouvez choisir parmi une liste de snapshots existants.
5. 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.

Afficher les snapshots et les sauvegardes

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

Étapes

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

   Les snapshots s'affichent par défaut.

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

Supprimer les instantanés

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

Vous ne pouvez pas supprimer 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.

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.

> 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.

> Lorsque vous effectuez une restauration sur place d'une application qui utilise un stockage NetApp ONTAP, l'espace utilisé par cette application peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.

Description de la tâche

- **Protéger vos applications d'abord**: Il est fortement recommandé de prendre un instantané de ou de sauvegarder votre application avant de la restaurer. Cela vous permettra de cloner à partir du snapshot ou de la sauvegarde en cas d'échec de la restauration.
- **Vérifiez les volumes de destination** : si vous restaurez sur un autre cluster, assurez-vous que le cluster utilise le même mode d'accès aux volumes persistants (par exemple, ReadWriteMany). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent.
- **(clusters OpenShift uniquement) Ajouter des règles** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

- **Helm Deployed apps** : le clonage des applications déployées avec Helm 3 (ou mis à niveau de Helm 2 vers Helm 3) est entièrement pris en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **protection des données**.
3. Si vous souhaitez effectuer une restauration à partir d'un instantané, conservez l'icône **snapshots** sélectionnée. Sinon, sélectionnez l'icône **backups** pour restaurer à partir d'une sauvegarde.
4. Dans le menu Options de la colonne **actions** pour l'instantané ou la sauvegarde à partir duquel vous souhaitez restaurer, sélectionnez **Restaurer l'application**.
5. 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.

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. Par exemple, le scénario suivant génère une situation indésirable lors de l'utilisation de la réplication NetApp SnapMirror :

i. Vous définissez l'application `app1` utilisation de l'espace de noms `ns1`.
ii. Vous configurez une relation de réplication pour `app1`.
iii. Vous définissez l'application `app2` (sur le même cluster) utilisant les namespaces `ns1` et `ns2`.
iv. Vous configurez une relation de réplication pour `app2`.
v. La réplication est inversée pour `app2`. Ceci provoque le `app1` l'application sur le cluster source à désactiver.

   i. Sélectionnez le snapshot à utiliser pour restaurer l'application sur place, qui restaure l'application vers une version antérieure de lui-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.

   iii. Consultez les détails de l'action de restauration, saisissez "restaurer" et sélectionnez **Restaurer**.
   - **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. Choisissez le cluster de destination pour l'application que vous souhaitez restaurer.
     ii. 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.

iii. Sélectionnez **Suivant**.

iv. Sélectionnez le snapshot à utiliser pour restaurer l'application.

v. Sélectionnez **Suivant**.

vi. Consultez les détails de l'action de restauration et sélectionnez **Restaurer**.

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 la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

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

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

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

Vous pouvez répliquer des applications dans différents scénarios, comme : uniquement sur site, environnements hybrides et multicloud :

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

vers des fournisseurs de cloud différents)

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

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

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

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

Conditions préalables à la réplication

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

- Pour assurer une reprise après incident transparente, nous vous recommandons de déployer Astra Control Center dans un troisième domaine de pannes ou un troisième site secondaire.
- Le cluster Kubernetes hôte de l'application et un cluster Kubernetes de destination doivent être gérés avec leurs clusters ONTAP, dans l'idéal dans différents domaines ou sites de défaillance.
- Les clusters ONTAP et le SVM hôte doivent être associés. Voir "Présentation du cluster et de SVM peering".
- Le SVM distant couplé doit être disponible avec Astra Trident sur le cluster de destination.
- La version 22.07 ou ultérieure d'Astra Trident doit exister sur les clusters ONTAP source et de destination.
- Les licences asynchrones ONTAP SnapMirror via le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Voir "Présentation des licences SnapMirror dans ONTAP".
- Lorsque vous ajoutez un système de stockage back-end ONTAP à Astra Control Center, appliquez les identifiants de l'utilisateur avec le rôle « admin » qui possède des méthodes d'accès `http` et `ontapi` Activation sur les clusters ONTAP source et de destination Voir "Gérer les comptes utilisateur dans la documentation ONTAP" pour en savoir plus.
- Les clusters Kubernetes source et destination et les clusters ONTAP doivent être gérés par Astra Control.

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

- **Configuration de l'Astra Trident / ONTAP** : le Centre de contrôle Astra requiert la création et la définition d'une classe de stockage comme classe de stockage par défaut. Astra Control Center prend en charge les pilotes ONTAP suivants fournis par Astra Trident pour la réplication :

- ontap-nas
- ontap-nas-flexgroup
- ontap-san

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

Configuration d'une relation de réplication

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

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

Étapes

1. Dans le menu de navigation gauche Astra Control, sélectionnez **applications**.
2. Dans la page application, sélectionnez l'onglet **Data protection** > **Replication**.
3. Dans l'onglet protection des données > réplication, sélectionnez **configurer la stratégie de réplication**. Ou, dans la zone protection des applications, sélectionnez l'option actions et sélectionnez **configurer la stratégie de réplication**.
4. Entrez ou sélectionnez les informations suivantes :
   - **Grappe de destination** : saisissez un cluster de destination différent de la source.
   - **Classe de stockage de destination** : sélectionnez ou entrez la classe de stockage qui utilise le SVM apparié sur le cluster ONTAP de destination.
   - **Type de réplication**: "Asynchrone" est actuellement le seul type de réplication disponible.
   - **Espace de noms de destination** : saisissez 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 instantané et le réplique à sa destination.
   - **Décalage**: Définissez le nombre de minutes à partir du haut de l'heure que vous voulez que le contrôle Astra prenne un instantané. Vous pouvez utiliser un décalage afin qu'il ne coïncide pas avec d'autres opérations planifiées. Par exemple, si vous voulez prendre l'instantané toutes les 5 minutes à partir de 10:02, entrez "02" comme minutes de décalage. Le résultat serait 10:02, 10:07, 10:12, etc
5. Sélectionnez **Suivant**, examinez le résumé et sélectionnez **Enregistrer**.

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

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

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

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

Résultat

Cela crée la relation de réplication.

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

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

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

Par exemple : normal | établi

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. Dans la page application, sélectionnez l'onglet **Data protection** > **Replication**.
3. Dans l'onglet protection des données > réplication, dans le menu actions, sélectionnez **basculer**.
4. Dans la page basculement, consultez les informations et sélectionnez **basculer**.

Résultat

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

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

Resynchroniser un basculement de réplication impossible

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

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

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

Étapes

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

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

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

Résultat

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

Réplication inverse des applications

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

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

Étapes

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

Résultat

Les actions suivantes se produisent suite à la réplication inverse :

- Une copie Snapshot est réalisée des ressources Kubernetes de l'application source d'origine.

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

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

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

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

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

Étapes

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

Résultat

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

Supprime une relation de réplication d'application

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

Étapes

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

diagramme de relations, sélectionnez **Supprimer la relation de réplication**.

Résultat

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

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

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

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

États d'intégrité des relations de réplication

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

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

États du cycle de vie de la réplication

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

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

supprime l'application Kubernetes. Pendant le processus de resynchronisation, l'état indique « établissement ».

- **Reversing** : l' est l'opération planifiée pour déplacer l'application vers le cluster de destination tout en continuant à effectuer la réplication vers le cluster source d'origine. Astra Control arrête l'application du cluster source. Il réplique les données vers la destination avant de basculer l'application vers le cluster de destination. Pendant la réplication inverse, l'état indique « établissement ».
- **Suppression** :
  - Si la relation de réplication a été établie mais n'a pas encore été rétablie, Astra Control supprime les demandes de volume persistant qui ont été créées pendant la réplication et supprime l'application gérée de destination.
  - Si la réplication a déjà échoué, Astra Control conserve les ESV et l'application de destination.

Cloner et migrer les applications

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.

Ce dont vous avez besoin

- 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.
- **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 la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

- **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.

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.
   - Entrer 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**.
- Indiquez si vous souhaitez créer le clone à partir d'un snapshot ou d'une sauvegarde existant. Si vous ne sélectionnez pas cette option, Astra Control Center crée le clone à partir de l'état actuel de l'application.
  - Si vous avez choisi de cloner à partir d'un snapshot ou d'une sauvegarde existant, choisissez le snapshot ou la sauvegarde que vous souhaitez utiliser.

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 la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.

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 des crochets d'exécution pour interrompre toutes les transactions de base de données avant un instantané et reprendre les transactions une fois l'instantané terminé. Les snapshots sont ainsi cohérents au niveau des applications.

Types de crochets d'exécution

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

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

Remarques importantes sur les crochets d'exécution personnalisés

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

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

- Si vous créez un crochet d'exécution pour une application qui participe à un maillage de service Istio, assurez-vous que le crochet s'exécute contre le conteneur d'application d'origine, et non pas le conteneur de maillage de service. Vous pouvez exclure les conteneurs de maillage de service Istio en appliquant un filtre regex à chaque crochet d'exécution qui s'exécute pour les applications qui utilisent un maillage de service Istio.
- Puisque les crochets d'exécution réduisent souvent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils sont en cours d'exécution, vous devez toujours essayer de réduire le temps d'exécution de vos crochets d'exécution personnalisés.
- Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Autrement dit, un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde est terminée.

Ordre d'exécution

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

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

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

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

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

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

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

Déterminez si un crochet va courir

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

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

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

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

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

Exemples de crochet d'exécution

Consultez le "Projet GitHub NetApp Verda" pour voir des exemples et obtenir une idée de la façon de structurer vos crochets d'exécution. Vous pouvez utiliser ces exemples comme modèles ou scripts de test.

Afficher les crochets d'exécution existants

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

Étapes

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

   Vous pouvez afficher tous les crochets d'exécution activés ou désactivés dans la liste résultante. Vous pouvez voir l'état d'un crochet, sa source et le moment où il est exécuté (pré ou post-opération). Pour afficher les journaux d'événements entourant les crochets d'exécution, accédez à la page **activité** dans la zone de navigation de gauche.

Afficher les scripts existants

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

Étapes

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

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

Ajouter un script

Vous pouvez ajouter un ou plusieurs scripts que les crochets d'exécution peuvent référencer. De nombreux crochets d'exécution peuvent référencer le même script ; cela vous permet de mettre à jour de nombreux crochets d'exécution en ne changeant qu'un seul script.

Étapes

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

Résultat

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

Supprimer un script

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

Étapes

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

3. Choisissez un script à supprimer et sélectionnez le menu dans la colonne **actions**.
4. Sélectionnez **Supprimer**.

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

Créer un crochet d'exécution personnalisé

Vous pouvez créer un crochet d'exécution personnalisé pour une application. Voir Exemples de crochet d'exécution pour des exemples de crochet. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour créer des crochets d'exécution.

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

Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
2. Sélectionnez l'onglet **crochets d'exécution**.
3. Sélectionnez **Ajouter**.
4. Dans la zone **Détails du crochet**, déterminez quand le crochet doit fonctionner en sélectionnant un type d'opération dans le menu déroulant **opération**.
5. Saisissez un nom unique pour le crochet.
6. (Facultatif) saisissez les arguments à transmettre au crochet pendant l'exécution, en appuyant sur la touche entrée après chaque argument que vous entrez pour enregistrer chacun.
7. Dans la zone **Images conteneur**, si le crochet doit être exécuté sur toutes les images de conteneur contenues dans l'application, activez la case à cocher **appliquer à toutes les images de conteneur**. Si, à la place, le crochet ne doit agir que sur une ou plusieurs images de conteneur spécifiées, entrez les noms d'image de conteneur dans le champ **noms d'image de conteneur à associer**.
8. Dans la zone **script**, effectuez l'une des opérations suivantes :
   - Ajouter un nouveau script.
     i. Sélectionnez **Ajouter**.
     ii. Effectuez l'une des opérations suivantes :
       - Charger un script personnalisé.
         I. Sélectionnez l'option **Télécharger le fichier**.
         II. Accédez à un fichier et téléchargez-le.
         III. Donnez un nom unique au script.
         IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
         V. Sélectionnez **Enregistrer le script**.
       - Coller dans un script personnalisé à partir du presse-papiers.
         I. Sélectionnez l'option **Coller ou type**.

II. Sélectionnez le champ de texte et collez le texte du script dans le champ.

III. Donnez un nom unique au script.

IV. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.

- Sélectionnez un script existant dans la liste.

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

9. Sélectionnez **Ajouter crochet**.

Vérifier l'état d'un crochet d'exécution

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

Étapes

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

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

Afficher l'utilisation du script

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

Étapes

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

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

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

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

Désactivez un crochet d'exécution

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

Étapes

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

Supprimer un crochet d'exécution

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

Étapes

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

Pour en savoir plus

- "Projet GitHub NetApp Verda"

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 (qu'il s'agisse d'une application en bon état), son état de protection (qu'il soit entièrement protégé en cas de défaillance), les pods, le stockage persistant, et bien plus encore.

Étapes

1. Dans l'interface utilisateur du Centre de contrôle Astra, sélectionnez **applications**, puis le nom d'une application.
2. Vérifiez les informations.
   - **App Status** : fournit un état qui reflète l'état de l'application dans Kubernetes. Par exemple, les pods et les volumes persistants sont-ils en ligne ? Si une application est défectueuse, vous devez chercher à résoudre le problème sur le cluster en consultant les journaux Kubernetes. Astra ne fournit pas d'informations pour vous aider à réparer une application défaillante.
   - **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'adresse e-mail de l'attribut LDAP "mail" pour rechercher et garder le suivi des utilisateurs distants. Cet attribut peut être un champ facultatif ou vide dans votre répertoire. Une adresse électronique doit exister dans ce champ pour tous les utilisateurs distants que vous souhaitez afficher dans Astra Control Center. Cette adresse e-mail est utilisée comme nom d'utilisateur dans Astra Control Center pour l'authentification.

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.

Ce dont vous avez besoin

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 **User Match**, entrez le nom unique de base et un filtre de recherche d'utilisateur approprié à utiliser lors de la récupération des informations utilisateur à partir du serveur LDAP.
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.

> 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.

> Vous ne pouvez pas ajouter un utilisateur distant si un utilisateur local avec la même adresse e-mail existe déjà sur le système. Pour ajouter l'utilisateur en tant qu'utilisateur distant, supprimez d'abord l'utilisateur local du système.

> Astra Control Center utilise l'adresse e-mail de l'attribut LDAP "mail" pour rechercher et garder le suivi des utilisateurs distants. Cet attribut peut être un champ facultatif ou vide dans votre répertoire. Une adresse électronique doit exister dans ce champ pour tous les utilisateurs distants que vous souhaitez afficher dans Astra Control Center. Cette adresse e-mail est utilisée comme nom d'utilisateur dans Astra Control Center pour l'authentification.

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 sont ajoutés à Astra Control et héritent du même rôle.

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 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 et tous les utilisateurs distants de ce groupe

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

Supprimer les informations d'identification

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

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

Étapes

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

Résultat

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

Surveillez l'activité des comptes

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

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

Afficher toutes les activités du compte dans Astra Control

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

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

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

Afficher l'activité des comptes pour les clusters

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

Prenez des mesures pour résoudre les événements qui nécessitent votre attention

1. Sélectionnez **activité**.

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

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

Mettre à jour une licence existante

Vous pouvez convertir une licence d'évaluation en licence complète, ou mettre à jour une évaluation existante ou une licence complète avec une nouvelle licence. Si vous ne disposez pas d'une licence complète, contactez votre contact commercial NetApp pour obtenir une licence complète et un numéro de série. Vous pouvez utiliser l'interface utilisateur 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.

Ce dont vous avez besoin

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

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

Étapes

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

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

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

Trouvez plus d'informations

- "Utilisez l'API de contrôle Astra"

Gérer le stockage back-end

La gestion des clusters de stockage d'Astra Control en tant que backend de stockage vous permet d'obtenir des liens entre les volumes persistants (PVS) et le back-end de stockage, ainsi que des metrics de stockage supplémentaires. Il est possible de surveiller la capacité du stockage et les informations concernant son état, y compris les performances si le centre de contrôle Astra est connecté à Cloud Insights.

Pour obtenir des instructions sur la gestion des systèmes back-end avec l'API Astra Control, consultez le "Informations sur l'automatisation et les API d'Astra".

Vous pouvez effectuer les tâches suivantes liées à la gestion d'un système back-end :

- "Ajout d'un système back-end"
- Afficher les détails du système back-end
- Annuler la gestion d'un système back-end
- 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

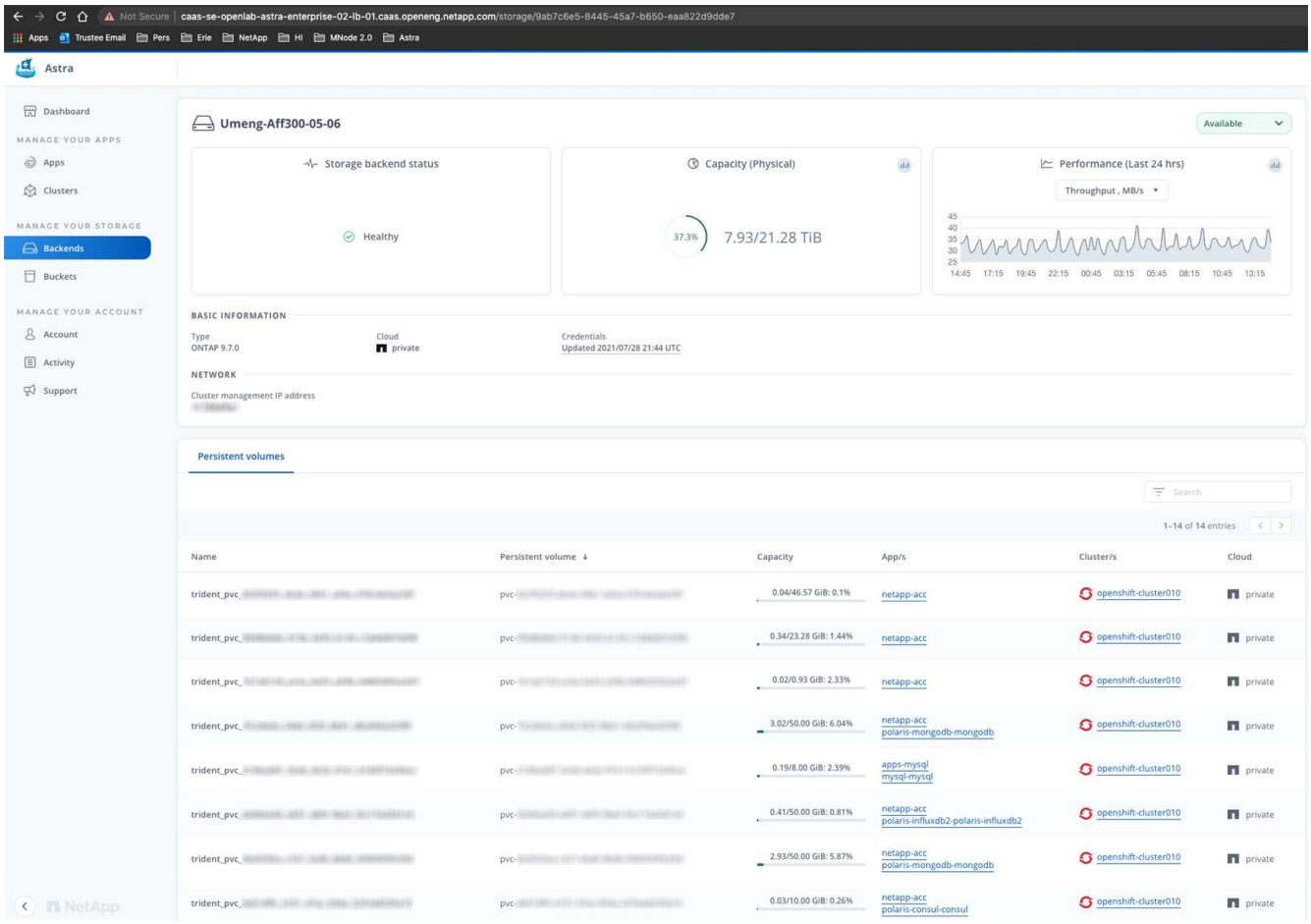
Affichez des informations sur l'état du système back-end, la capacité et les performances (débit et/ou latence des IOPS).

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.



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

Annuler la gestion d'un système back-end

Vous pouvez annuler la gestion du système back-end.

Étapes

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

Retirer un système back-end

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

Ce dont vous avez besoin

- Assurez-vous que le système de stockage back-end n'est pas géré.
- Assurez-vous que le système back-end ne 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.

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

Résultat

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

Modifier les paramètres du serveur proxy

Vous pouvez modifier les paramètres du serveur proxy.

Étapes

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

Désactiver la connexion au serveur proxy

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

Étapes

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

Connectez-vous à Cloud Insights

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

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

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

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

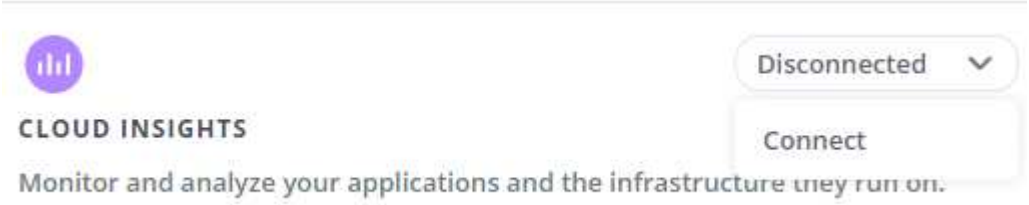
Ce dont vous avez besoin

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

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

Étapes

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

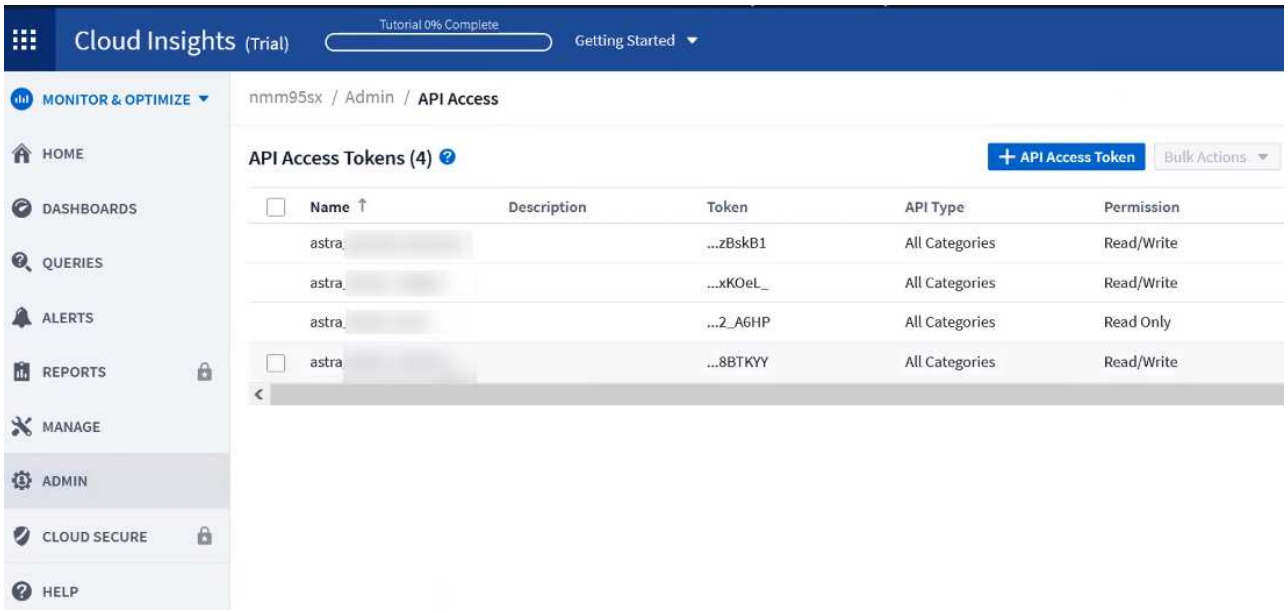


4. Entrez les jetons de l'API Cloud Insights et l'URL du locataire. L'URL du locataire a le format suivant, par exemple :

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

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

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



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

d. Copiez la clé **lecture/écriture**. Vous devrez le coller dans la fenêtre Centre de contrôle Astra **connexion Cloud Insights**. Pour les autorisations de 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.

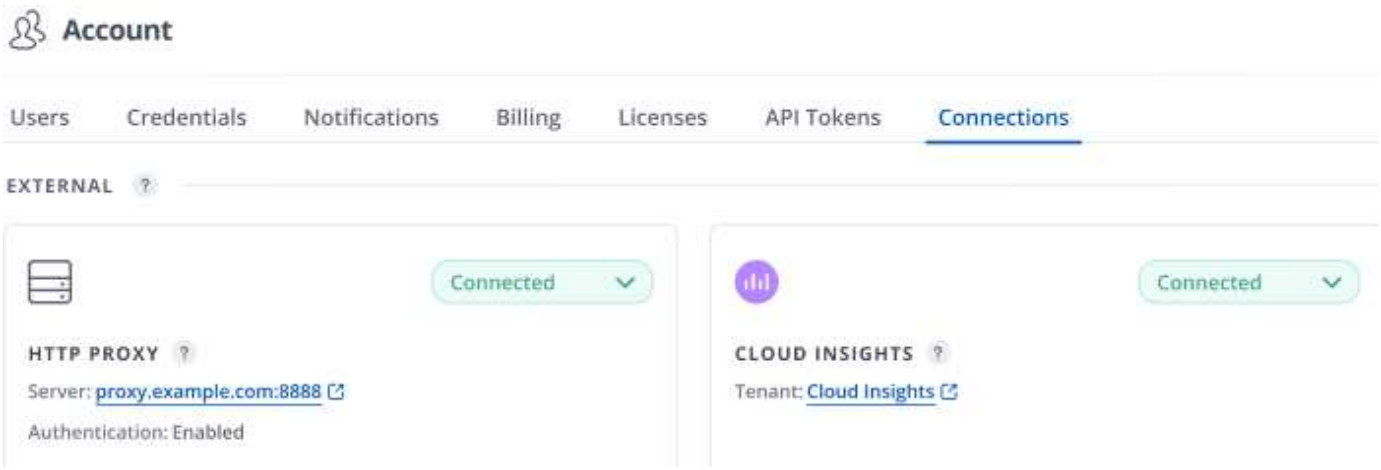
5. Sélectionnez **connexion**.

> 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**.

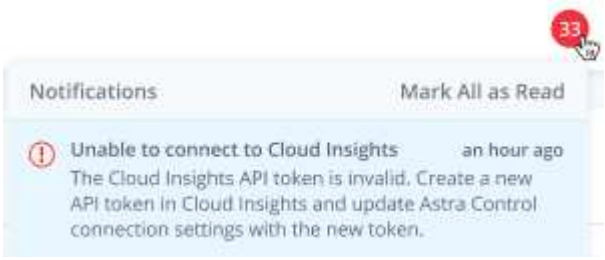
> Pour passer facilement entre le centre de contrôle Astra et les interfaces utilisateur Cloud Insights, assurez-vous d'être connecté aux deux.

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.

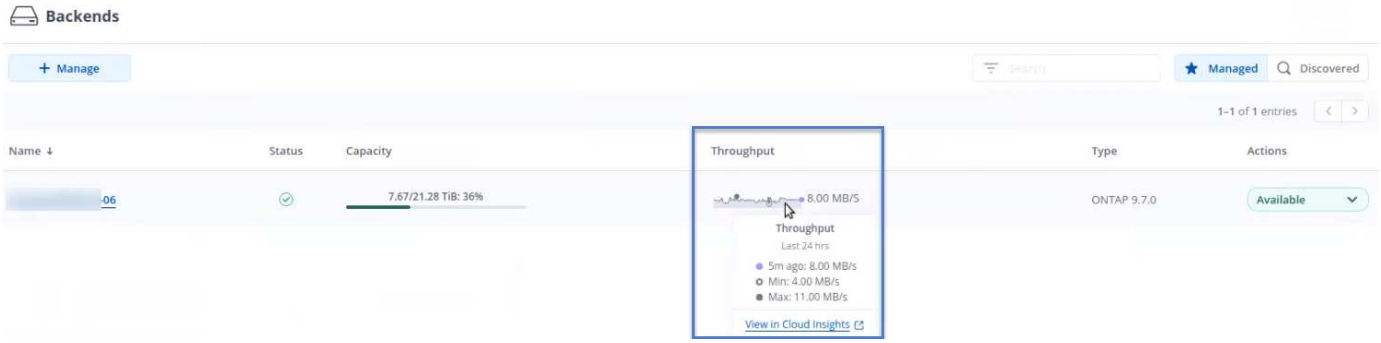


Si la connexion a échoué pour une raison quelconque, l'état indique **FAILED**. Vous pouvez trouver la raison de l'échec sous **Notifications** en haut à droite de l'interface utilisateur.



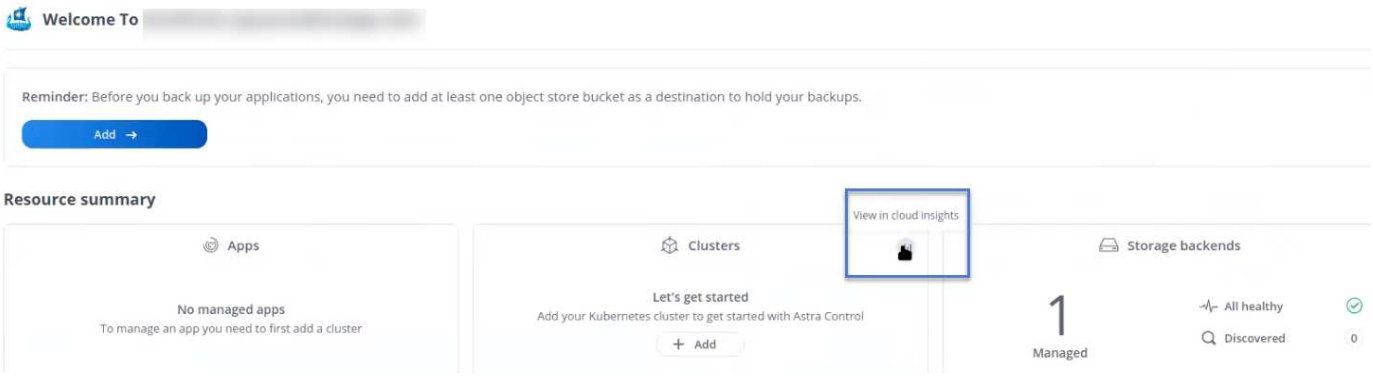
Vous pouvez également trouver les mêmes informations sous **compte** > **Notifications**.

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



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

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



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

Modifier la connexion Cloud Insights

Vous pouvez modifier la connexion Cloud Insights.

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

Étapes

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

Désactiver la connexion Cloud Insights

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

Étapes

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

Connectez-vous à 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 aurez 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.

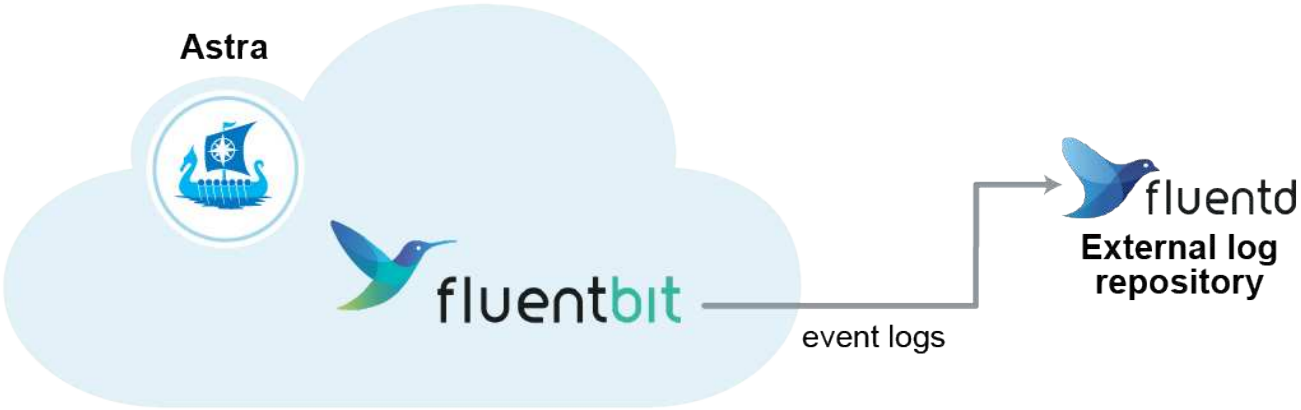
Étapes

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) depuis le 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.

Ce dont vous avez besoin

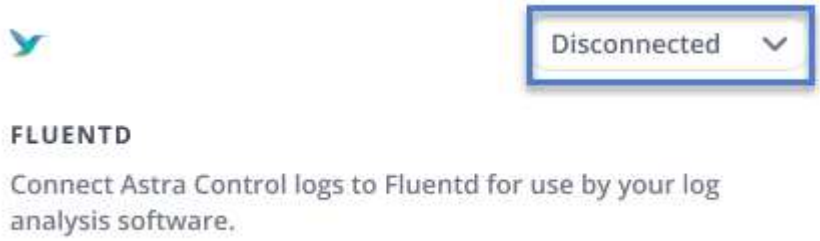
- Un compte Astra Control Center avec **admin**/**propriétaire** privilèges.
- Astra Control Center est installé et exécuté sur un cluster Kubernetes.

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

Étapes

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

3. Sélectionnez **Connect** dans la liste déroulante où apparaît **déconnecté** pour ajouter la connexion.



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

Résultat

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

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

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

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

Modifiez la connexion Fluentd

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

Étapes

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

Désactivez la connexion Fluentd

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

Étapes

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

Annuler la gestion des applications et des clusters

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

Annuler la gestion d'une application

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

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.
- Trident ne sera pas désinstallé du cluster. "Découvrez comment désinstaller 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.

Ce dont vous avez besoin

- Avant de procéder à la mise à niveau, reportez-vous à la section "De l'environnement opérationnel" Pour garantir que votre environnement respecte les exigences minimales en matière de déploiement d'Astra Control Center. Votre environnement doit disposer des éléments suivants :
  - Une version d'Astra Trident prise en charge pour déterminer la version que vous exécutez, exécutez la commande suivante contre votre Astra Control Center existant :

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

    Reportez-vous à la section "Documentation Astra Trident" pour effectuer une mise à niveau à partir d'une ancienne version.

    > Vous devez effectuer une mise à niveau vers Astra Trident 22.10 * AVANT* pour la mise à niveau vers Kubernetes 1.25.

  - Une distribution Kubernetes prise en charge pour déterminer la version que vous exécutez, exécutez la commande suivante par rapport à votre Astra Control Center existant : `kubectl get nodes -o wide`
  - Suffisamment de ressources de cluster pour déterminer les ressources de cluster, exécutez la commande suivante dans votre cluster Astra Control Center existant : `kubectl describe node <node name>`
  - Registre que vous pouvez utiliser pour diffuser et télécharger des images Astra Control Center
  - Une classe de stockage par défaut pour déterminer votre classe de stockage par défaut, exécutez la commande suivante avec votre Astra Control Center existant : `kubectl get storageclass`
- (OpenShift uniquement) Assurez-vous que tous les opérateurs de cluster sont en bon état et disponibles.

  ```
  kubectl get clusteroperators
  ```

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

```
kubectl get apiservices
```

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

Description de la tâche

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

- Téléchargez 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

1. Accédez au "Page de téléchargement des produits Astra Control Center" Sur le site de support NetApp. Vous pouvez sélectionner la dernière version ou une autre version souhaitée dans le menu déroulant.
2. Téléchargez le pack contenant Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (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 :

```
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.

4. Extraire les images du pack Astra Control Center :

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

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

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

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. Pour supprimer une version existante de kubectl-astra, exécutez la commande suivante : `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 ce fichier et ce répertoire:

   ```
   acc.manifest.bundle.yaml
   acc/
   ```

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.manifest.bundle.yaml
   acc/
   ```

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=22.11.0-82
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
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
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://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/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_or_custom_name_of_secret>
```

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

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

d. Ajoutez les valeurs suivantes à la `env` section :

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  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: [your_registry_path]/kube-rbac-proxy:v4.8.0
      name: kube-rbac-proxy
      ports:
      - containerPort: 8443
        name: https
    - args:
      - --health-probe-bind-address=:8081
      - --metrics-bind-address=127.0.0.1:8080
      - --leader-elect
      env:
      - name: ACCOP_LOG_LEVEL
        value: "2"
      - name: ACCOP_HELM_UPGRADETIMEOUT
        value: 300m
      image: [your_registry_path]/acc-operator:[version x.y.z]
      imagePullPolicy: IfNotPresent
      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.astra.
netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

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

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

Mettez à niveau Astra Control Center

1. 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`) vers la version que vous mettez à niveau vers :

```
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
```

Une fois que vous avez enregistré et quitté l'éditeur de fichiers, les modifications seront appliquées et la mise à niveau commencera.

6. (Facultatif) Vérifiez que les modules se terminent et deviennent disponibles à nouveau :

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

7. 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   22.11.0-82
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.

Désinstaller Astra Control Center

Vous devrez peut-être retirer les composants du centre de contrôle Astra si vous effectuez une mise à niveau d'un essai vers une version complète du produit. Pour déposer le centre de commande Astra et le conducteur du centre de commande Astra, exécuter les commandes décrites dans cette procédure dans l'ordre.

Si vous rencontrez des problèmes avec la désinstallation, reportez-vous à la section Dépannage des problèmes de désinstallation.

Ce dont vous avez besoin

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

Étapes

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

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

Résultat :

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

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

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

Résultat :

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

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

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

Résultat :

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

Dépannage des problèmes de désinstallation

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

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

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

Étapes

1. Supprimer `acc-monitoring` agent :

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

Résultat :

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

2. Supprimez le namespace :

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

Résultat :

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

3. Confirmer la suppression des ressources :

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

Résultat :

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

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

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

Résultat de l'échantillon :

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

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

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

Résultat :

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

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

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

Étapes

1. Lister les CRD Traefik installés sur le cluster :

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

   Réponse

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Supprimez les CRD :

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

Trouvez plus d'informations

- "Problèmes connus de désinstallation"