Utilisez le service Astra Control

Astra Control Service

NetApp
May 30, 2023

Table des matières

Utilisez le service Astra Control

Connectez-vous au service Astra Control

Le service Astra Control est accessible par le biais d'une interface utilisateur SaaS https://astra.netapp.io.

Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). Pour en savoir plus, consultez le "Centre d'aide de Cloud Central" Puis sélectionnez **Options de connexion à Cloud Central**.

Avant de commencer

- "ID d'utilisateur Cloud Central".
- "Un nouveau compte Astra Control" ou "invitation à un compte existant".
- Un navigateur Web pris en charge.

  Astra Control Service prend en charge les versions récentes de Firefox, Safari et Chrome avec une résolution minimale de 1280 x 720.

Étapes

1. Ouvrez un navigateur Web et accédez à https://astra.netapp.io.
2. Connectez-vous à l'aide de vos identifiants NetApp Cloud Central.

Gestion et protection des applications

Commencez à gérer les applications

Après vous "Ajoutez un cluster Kubernetes à 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.

Besoins en termes de gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer plus de 10 espaces de noms, vous avez besoin d'un abonnement à Astra Control.
- **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 les ressources Kubernetes non collectées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control collecte les ressources Kubernetes suivantes :

ClusterRole	ClusterRoleBinding	ConfigMap
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.

Astra Control ne gère les applications avec état que si le stockage est placé sur une classe de stockage prise en charge par Astra Control. Astra Control Service prend en charge toutes les classes de stockage prises en charge par Astra Trident ou un pilote CSI générique.

- "Découvrez les classes de stockage pour les clusters GKE"
- "Découvrez les classes de stockage pour les clusters AKS"
- "Découvrir les classes de stockage pour les clusters AWS"

Définir les applications

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

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

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

Avant de commencer

- Un cluster Kubernetes ajouté à Astra Control.
- Une ou plusieurs applications installées sur le cluster. En savoir plus sur les méthodes d'installation d'applications prises en charge.
- Espaces de noms existants sur le cluster Kubernetes que vous avez ajouté à Astra Control.
- (Facultatif) 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, envisagez "modification des rôles utilisateur avec des contraintes d'espace de noms" avant de définir des applications.

- 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 des ressources Kubernetes peut provoquer des conflits de données.

En savoir plus sur 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 Rechercher pour voir les ressources supplémentaires comprises dans la portée du cluster.

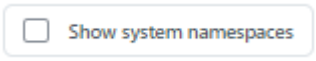
Définissez un espace de noms à gérer en tant qu'application

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 la définition individuelle des applications si vous "ont l'intention de gérer et de protéger toutes les ressources d'un namespace 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. 

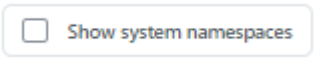
"En savoir plus".

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.

Protéger les applications avec les snapshots et les sauvegardes

Protégez vos applications en effectuant des copies Snapshot et des sauvegardes à l'aide d'une stratégie de protection automatisée ou ad hoc. Vous pouvez utiliser l'interface

utilisateur Astra ou "API de contrôle Astra" pour protéger les applications.

En savoir plus sur "Protection des données dans Astra Control".

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".

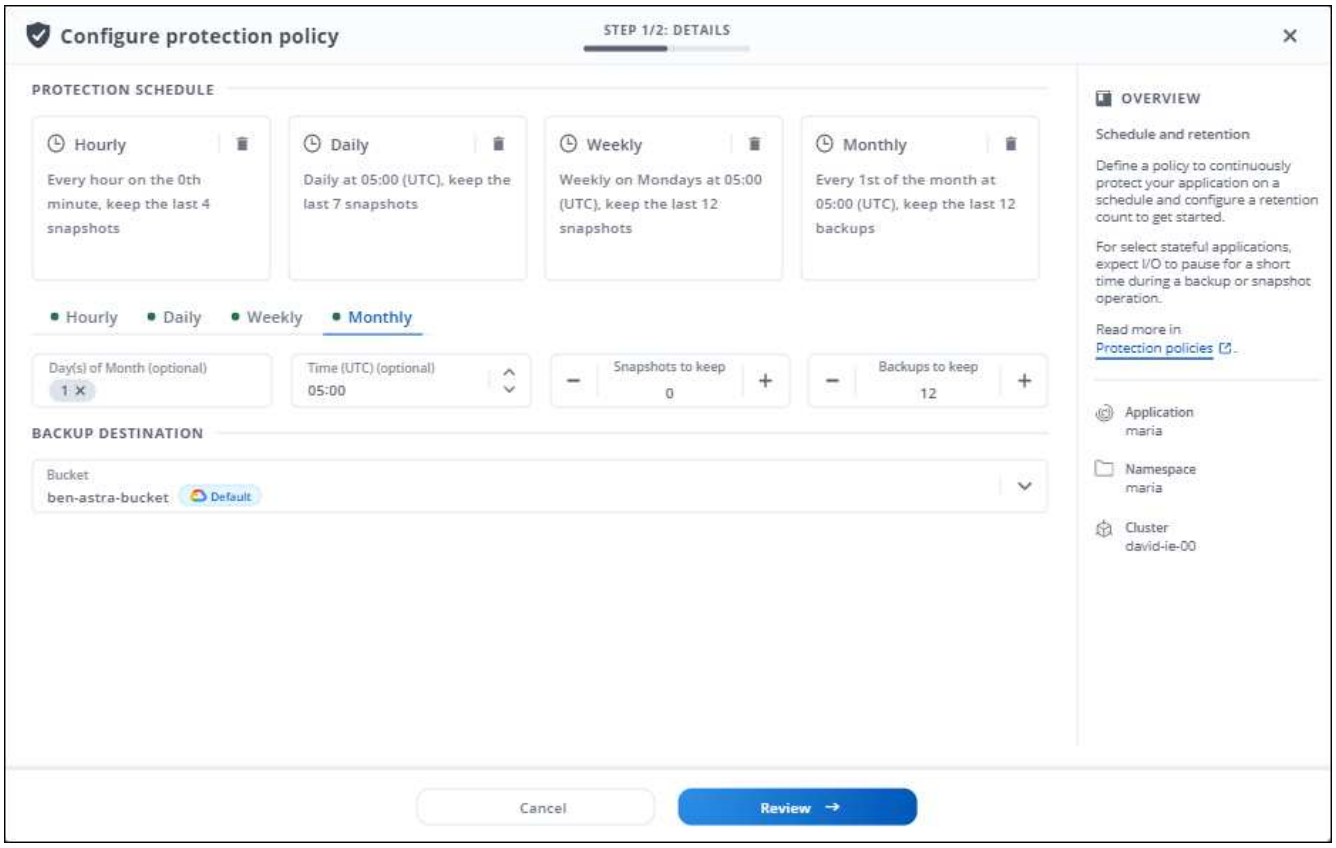
Étapes

1. Sélectionnez **applications**, puis le nom d'une application gérée.
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 à conserver pour les horaires, quotidiens, hebdomadaires et mensuels.

   Vous pouvez définir les horaires horaires, quotidiens, hebdomadaires et mensuels simultanément. Un programme ne sera pas activé tant que vous n'aurez pas défini un niveau de rétention pour les snapshots et les sauvegardes.

   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.

Soyez conscient du traitement de l'espace de stockage lors de la sauvegarde d'une application hébergée sur un système de stockage Azure NetApp Files. Reportez-vous à la section "Sauvegardes d'applications" pour en savoir plus.

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 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.

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 gérée.
2. Sélectionnez **protection des données**.

   Les snapshots s'affichent par défaut.

3. Sélectionnez **backups** pour faire référence à la liste des sauvegardes.

Supprimer les instantanés

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

Étapes

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

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

Description de la tâche

- **Protéger vos applications en premier** : il est fortement recommandé de prendre un instantané ou une

sauvegarde de 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.
- **Planifier les besoins en espace** : lorsque vous effectuez une restauration sur place d'une application utilisant un stockage NetApp ONTAP, l'espace utilisé par l'application restaurée peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.

> 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.

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.
3. Choisissez le type de restauration :
   - **Restaurer les espaces de noms d'origine** : utilisez cette procédure pour restaurer l'app sur place dans le cluster d'origine.
     i. Sélectionnez le snapshot ou la sauvegarde à utiliser pour restaurer l'application sur place, ce qui restaure l'application à une version antérieure de elle-même.
     ii. Sélectionnez **Suivant**.

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

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

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

     iv. Sélectionnez **Suivant**.
     v. Sélectionnez le snapshot ou la sauvegarde à utiliser pour restaurer l'application.
     vi. Sélectionnez **Suivant**.
     vii. Options au choix :

- **Restaurer à l'aide des classes de stockage d'origine** : l'application utilise la classe de stockage associée à l'origine, sauf si elle n'existe pas sur le cluster cible. Dans ce cas, la classe de stockage par défaut du cluster sera utilisée.
- **Restaurer à l'aide d'une classe de stockage différente** : sélectionnez une classe de stockage qui existe sur le cluster cible. Tous les volumes d'application, quelles que soient les classes de stockage qui leur sont associées à l'origine, seront migrés vers cette classe de stockage différente dans le cadre de la restauration.

viii. Sélectionnez **Suivant**.

4. Sélectionnez les ressources à filtrer :
   - **Restaurer toutes les ressources** : restaurez toutes les ressources associées à l'application d'origine.
   - **Filtrer les ressources** : spécifiez des règles pour restaurer un sous-ensemble des ressources d'application d'origine :
     i. Choisissez d'inclure ou d'exclure des ressources de l'application restaurée.
     ii. Sélectionnez **Ajouter une règle d'inclusion** ou **Ajouter une règle d'exclusion** et configurez la règle pour filtrer les ressources appropriées lors de la restauration de l'application. Vous pouvez modifier une règle ou la supprimer et créer une nouvelle règle jusqu'à ce que la configuration soit correcte.

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

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

Résultat

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

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

> Tout utilisateur membre aux contraintes de namespace par nom/ID d'espace de noms ou par libellés de namespace peut cloner ou restaurer une application vers un nouvel espace de noms sur le même cluster ou vers tout autre cluster du compte de son entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après 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.

Filtrer les ressources pendant la restauration d'une application

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

En savoir plus sur les scénarios d'inclusion et d'exclusion

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

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

Étapes

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

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

2. Configurez la règle de filtre :

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

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

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

b. (Facultatif) Entrez un nom de ressource.

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

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

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

i. (Facultatif) **Group** : dans la liste déroulante, sélectionnez le groupe API Kubernetes.

ii. **Type** : dans la liste déroulante, sélectionnez le schéma d'objet du type de ressource Kubernetes à utiliser dans le filtre.

iii. **Version** : sélectionnez la version de l'API Kubernetes.

3. Vérifiez la règle créée en fonction de vos entrées.
4. Sélectionnez **Ajouter**.

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

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.

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

Avant de commencer

- Pour cloner des applications sur un autre cluster, vérifiez que vous avez attribué un compartiment par défaut à l'instance cloud contenant le cluster source. Si l'instance de cloud source ne dispose pas d'un ensemble de compartiments par défaut, l'opération de clonage inter-cluster échoue.
- 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.

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 ou d'une restauration d'application, vous pouvez spécifier un compartiment à utiliser. Vous devez spécifier un compartiment par défaut lors du clonage des clusters, mais en spécifiant un compartiment est facultatif lorsque vous effectuez le clonage au sein du même cluster.
  - Lorsque vous clonez les clusters, l'instance cloud contenant le cluster source de l'opération de clonage doit disposer d'un ensemble de compartiments par défaut.
  - 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.

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 un espace de noms de destination.

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

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

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

Résultat

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

Après 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.

Gérer les crochets d'exécution de l'application

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

Types de crochets d'exécution

Astra Control 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

Filtres de crochet d'exécution

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

Chaque filtre que vous ajoutez à un crochet d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un crochet correspond à un conteneur, le crochet exécute son script associé sur ce conteneur.

Les expressions régulières pour les filtres utilisent la syntaxe de l'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre qui exclut les conteneurs de la liste des correspondances.

Pour plus d'informations sur la syntaxe prise en charge par Astra Control pour les expressions régulières dans les filtres de crochet d'exécution, voir "Prise en charge de la syntaxe de l'expression régulière 2 (RE2)".

Remarques importantes sur les crochets d'exécution personnalisés

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

Puisque les crochets d'exécution réduisent 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. Cela signifie que la logique utilisée dans un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde a été effectuée.

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

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	N	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	N	S/O

Exemples de crochet d'exécution

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

Afficher les crochets d'exécution existants

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

Étapes

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

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

Afficher les scripts existants

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

Étapes

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

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

Ajouter un script

Chaque crochet d'exécution doit utiliser un script pour effectuer des actions. Vous pouvez ajouter un ou plusieurs scripts que les crochets d'exécution peuvent référencer. De nombreux crochets d'exécution peuvent référencer le même script ; 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. Reportez-vous à la section Exemples de crochet d'exécution pour des exemples de crochet. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour créer des crochets d'exécution.

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

Étapes

1. 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** :
   a. Déterminez quand le crochet doit fonctionner en sélectionnant un type d'opération dans le menu déroulant **opération**.
   b. Saisissez un nom unique pour le crochet.
   c. (Facultatif) saisissez les arguments à transmettre au crochet pendant l'exécution, en appuyant sur la touche entrée après chaque argument que vous entrez pour enregistrer chacun.
5. (Facultatif) dans la zone **Détails du filtre de crochet**, vous pouvez ajouter des filtres pour contrôler les conteneurs sur lesquels le crochet d'exécution s'exécute :
   a. Sélectionnez **Ajouter filtre**.
   b. Dans la colonne Type de filtre **Hook**, choisissez un attribut sur lequel filtrer dans le menu déroulant.

c. Dans la colonne **Regex**, entrez une expression régulière à utiliser comme filtre. Astra Control utilise le "Expression régulière 2 (RE2) syntaxe regex".

> Si vous filtrez le nom exact d'un attribut (comme un nom de pod) sans autre texte dans le champ expression régulière, une correspondance de sous-chaîne est effectuée. Pour faire correspondre un nom exact et ce nom uniquement, utilisez la syntaxe de correspondance de chaîne exacte (par exemple, `^exact_podname$`).

d. Pour ajouter d'autres filtres, sélectionnez **Ajouter filtre**.

> Plusieurs filtres pour un crochet d'exécution sont combinés à un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.

6. Lorsque vous avez terminé, sélectionnez **Suivant**.
7. 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.
8. Sélectionnez **Suivant**.
9. Vérifiez la configuration du crochet d'exécution.
10. Sélectionnez **Ajouter**.

Vérifier l'état d'un crochet d'exécution

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

Étapes

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

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

Afficher l'utilisation du script

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

Étapes

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

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

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

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

Modifier un crochet d'exécution

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

Étapes

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

Désactivez un crochet d'exécution

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

Étapes

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

Supprimer un crochet d'exécution

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

Étapes

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

Pour en savoir plus

- "Projet GitHub NetApp Verda"

Affichez l'état des applications et des ressources de calcul

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

Cliquez sur **Dashboard** pour afficher une vue de haut niveau de vos applications, clusters et leur état de santé.

La mosaïque applications vous aide à identifier les éléments suivants :

- Nombre d'applications que vous gérez actuellement.
- Si ces applications gérées sont en bon état.
- Que les applications soient entièrement protégées (elles sont protégées si des sauvegardes récentes sont disponibles).

Notez qu'il ne s'agit pas uniquement de chiffres ou d'États, vous pouvez approfondir ces informations. 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.

La mosaïque clusters fournit des informations similaires sur l'état de santé du cluster et vous pouvez accéder à des informations plus détaillées comme vous le pouvez avec une application.

Afficher l'état de santé et les détails des clusters

Une fois que vous avez ajouté des clusters Kubernetes à Astra Control, vous pouvez afficher des informations détaillées sur le cluster, notamment son emplacement, les

nœuds de travail, les volumes persistants et les classes de stockage.

Étapes

1. Dans l'interface utilisateur du service 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** : activités liées au cluster.

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

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

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. Sélectionnez **applications**, puis le nom d'une application.
2. Trouvez les informations que vous recherchez :

Statut de l'application
Fournit un état qui reflète l'état de l'application dans Kubernetes.

État de la protection des applications
Fournit un état de protection de l'application :

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

Vous ne pouvez pas être entièrement protégé tant que vous n'avez pas une sauvegarde récente.

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

Présentation

Informations sur l'état des modules associés à l'application.

Protection des données

Vous permet de configurer une règle de protection des données et d'afficher les snapshots et les sauvegardes existants.

Stockage

Vous indique les volumes persistants au niveau de l'application. L'état d'un volume persistant est du point de vue du cluster Kubernetes.

Ressources

Vous permet de vérifier quelles ressources sont sauvegardées et gérées.

Activité

Les activités Astra Control liées à l'application.

Gestion des compartiments

Vous pouvez gérer les compartiments qu'Astra utilise pour la sauvegarde et le clonage. Vous pouvez ajouter des compartiments supplémentaires, supprimer des compartiments existants et modifier le compartiment par défaut des clusters Kubernetes dans une instance cloud.

Seuls les propriétaires et les administrateurs peuvent gérer les compartiments.

Utilisation des seaux par Astra Control

Lorsque vous commencez à gérer votre premier cluster Kubernetes pour une instance cloud, Astra Control Service crée le compartiment initial pour cette instance "instance cloud".

Vous pouvez désigner manuellement un compartiment comme compartiment par défaut pour une instance cloud. Dans ce cas, Astra Control Service utilise ce compartiment par défaut pour les sauvegardes et les clones que vous créez sur n'importe quel cluster géré de cette instance cloud (vous pouvez sélectionner un compartiment différent pour les sauvegardes). Si vous effectuez un clone dynamique d'une application depuis l'un des clusters gérés d'une instance cloud vers un autre cluster, Astra Control Service utilise le compartiment par défaut de l'instance cloud source pour effectuer l'opération de clonage.

Vous pouvez définir le même compartiment que le compartiment par défaut pour plusieurs instances cloud.

Vous pouvez faire votre choix parmi les compartiments lorsque vous créez une stratégie de protection ou que vous démarrez une sauvegarde ad hoc.

Le service de contrôle Astra vérifie si un compartiment de destination est accessible avant de démarrer une sauvegarde ou un clone.

Afficher les compartiments existants

Affichez la liste des compartiments disponibles pour Astra Control Service pour déterminer leur état et identifier le compartiment par défaut (si défini) de votre instance cloud.

Un godet peut avoir l'un des États suivants :

En attente
: Une fois que vous avez ajouté un compartiment, celui-ci commence à l'état en attente tandis qu'Astra Control le découvre.

Disponibilité
: Le godet peut être utilisé par Astra Control.

Supprimé
: Le godet n'est pas opérationnel actuellement. Passez votre souris sur l'icône d'état pour identifier le problème.

  Si un compartiment est retiré, vous pouvez toujours le définir comme compartiment par défaut et l'affecter à une planification de protection. Mais si le compartiment n'est pas disponible au moment où une opération de protection des données démarre, cette opération échoue.

Étape

1. Aller à **seaux**.

   La liste des compartiments disponibles pour Astra Control Service s'affiche.

Ajouter un godet supplémentaire

Vous pouvez ajouter des compartiments supplémentaires à tout moment. Vous avez ainsi le choix entre compartiments lors de la création d'une règle de protection ou du démarrage d'une sauvegarde ad hoc. Vous pouvez également modifier le compartiment par défaut utilisé par une instance cloud.

Vous pouvez ajouter les types de compartiments suivants :

- Amazon Web Services
- S3 générique
- Google Cloud Platform
- Microsoft Azure
- NetApp ONTAP S3
- NetApp StorageGRID S3

Avant de commencer

- Nom d'un compartiment existant.
- Identifiants du compartiment qui fournit à Astra Control Service les autorisations dont le service IT a besoin pour gérer le compartiment.
- Si votre compartiment est dans Microsoft Azure :
  - Le compartiment doit appartenir au groupe de ressources nommé *astra-backup-rg*.
  - Si le paramètre de performance de l'instance de compte de stockage Azure est défini sur « Premium »,

le paramètre « Type de compte Premium » doit être défini sur « blobs de bloc ».

Étapes

1. Aller à **seaux**.
2. Sélectionnez **Ajouter** et suivez les invites pour ajouter le compartiment.
   - **Type** : Choisissez votre fournisseur cloud.
   - **Nom de compartiment existant** : saisissez le nom du compartiment.
   - **Description** : saisissez éventuellement une description du godet.
     - **Compte de stockage** (Azure uniquement) : saisissez le nom de votre compte de stockage Azure. Ce compartiment doit appartenir au groupe de ressources nommé *astra-backup-rg*.
     - **Nom du serveur S3 ou adresse IP** (types de compartiment AWS et S3 uniquement) : entrez le nom de domaine complet du terminal S3 correspondant à votre région, sans `https://`. Reportez-vous à la section "La documentation Amazon" pour en savoir plus.
     - **Sélectionner les informations d'identification** : entrez les informations d'identification qui fournissent à Astra Control Service les autorisations dont il a besoin pour gérer le compartiment. Les informations à fournir varient en fonction du type de godet.
       a. Sélectionnez **Ajouter** pour ajouter le compartiment.

Résultat

ASTRA Control Service ajoute le compartiment. Vous pouvez désormais choisir ce compartiment lors de la création d'une règle de protection ou de l'exécution d'une sauvegarde ad hoc. Vous pouvez également définir ce compartiment comme compartiment par défaut pour une instance cloud.

Modifier le compartiment par défaut

Vous pouvez modifier le compartiment par défaut d'une instance cloud. ASTRA Control Service utilisera ce compartiment par défaut pour les sauvegardes et les clones. Chaque instance cloud dispose de son propre compartiment par défaut.

Astra Control n'attribue pas automatiquement de compartiment par défaut à une instance de cloud. Vous devez définir manuellement un compartiment par défaut pour une instance de cloud avant d'effectuer des opérations de clonage d'applications entre deux clusters.

Étapes

1. Accédez à **Cloud instances**.
2. Sélectionnez le menu de configuration dans la colonne **actions** pour l'instance de Cloud que vous souhaitez modifier.
3. Sélectionnez **Modifier**.
4. Dans la liste des compartiments, sélectionnez le compartiment par défaut pour cette instance cloud.
5. Sélectionnez **mettre à jour**.

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.

Avant de commencer

- Avant de commencer, assurez-vous qu'aucune sauvegarde n'est en cours d'exécution ou terminée pour ce compartiment.
- Vérifiez que le compartiment n'est pas utilisé pour les sauvegardes planifiées.

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

Étapes

1. Aller à **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"

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".

Gérez votre compte

Configurez la facturation

Vous pouvez utiliser plusieurs méthodes pour gérer la facturation de votre compte Astra Control Service. Si vous utilisez Azure ou Amazon AWS, vous pouvez vous abonner à un plan de service Astra Control via Microsoft Azure Marketplace ou AWS Marketplace. Dans ce cas, vous pouvez gérer vos données de facturation via Marketplace. Vous pouvez également vous abonner directement à NetApp. Si vous vous inscrivez directement à NetApp, vous pouvez gérer vos données de facturation via Astra Control Service. Si vous utilisez le service Astra Control sans abonnement, vous êtes automatiquement abonné au programme gratuit.

Le plan gratuit de service de contrôle d'Astra vous permet de gérer jusqu'à 10 espaces de noms dans votre compte. Si vous souhaitez gérer plus de 10 espaces de noms, vous devrez configurer la facturation en mettant à niveau le plan gratuit vers le plan Premium, ou en vous inscrivant sur Azure Marketplace ou AWS Marketplace.

Présentation de la facturation

Il existe deux types de coûts associés au service Astra Control : les frais de NetApp pour le service Astra Control et les frais de votre fournisseur cloud pour les volumes persistants et le stockage objet.

Facturation des services de contrôle Astra

Le service Astra Control propose trois plans :

Plan gratuit
: Gérer jusqu'à 10 espaces de noms gratuits.

Prime à l'utilisation
: Gérer un nombre illimité de namespaces à un taux spécifique par heure, par espace de noms.

Abonnement Premium
: Prépayez à un tarif réduit avec un abonnement annuel qui vous permet de gérer jusqu'à 10 espaces de noms par *Namespace pack*. Contactez le service commercial NetApp pour acheter autant de packs que nécessaire à votre entreprise. Par exemple, achetez 3 paquets pour gérer 30 espaces de noms auprès d'Astra Control Service. Si vous gérez plus de espaces de noms que ceux autorisés par votre abonnement annuel, vous serez facturé au taux de dépassement dépendant de l'abonnement par espace de noms supplémentaire.

  Si vous n'avez pas encore de compte Astra Control, l'achat de l'abonnement Premium crée automatiquement un compte Astra Control pour vous. Si vous disposez d'un plan gratuit existant, vous êtes automatiquement converti en abonnement Premium.

Lorsque vous créez un compte Astra Control, vous êtes automatiquement abonné au Plan gratuit. Le tableau de bord d'Astra Control vous indique le nombre d'espaces de noms que vous gérez actuellement à partir des

10 espaces de noms gratuits que vous êtes autorisé. La facturation commence pour un espace de noms lorsque la première application contenant l'espace de noms est gérée et s'arrête pour cet espace de noms lorsque la dernière application contenant l'espace de noms n'est pas gérée.

Si vous essayez de gérer un 11e espace de noms, Astra Control vous avertit que vous avez atteint la limite du Plan libre. Il vous invite ensuite à passer du plan gratuit à un plan Premium. Vous serez facturé au taux de dépassement dépendant de l'abonnement par espace de noms supplémentaire.

Vous pouvez passer à un abonnement Premium à tout moment. Après la mise à niveau, Astra Control commence à vous charger pour *All* namespaces dans le compte. Les 10 premiers espaces de noms ne restent pas dans le Plan libre.

Facturation Google Cloud

Lorsque vous gérez des clusters GKE avec Astra Control Service, les volumes persistants sont sauvegardés par NetApp Cloud Volumes Service et les sauvegardes de vos applications sont stockées dans un compartiment Google Cloud Storage.

- "Consultez les détails de tarification pour Cloud Volumes Service".

  Notez que le service Astra Control prend en charge tous les types de service et tous les niveaux de service. Le type de service que vous utilisez dépend de votre "Région Google Cloud".

- "Consultez les détails des prix des compartiments de stockage Google Cloud".

Facturation Microsoft Azure

Lorsque vous gérez des clusters AKS avec Astra Control Service, les volumes persistants sont sauvegardés par Azure NetApp Files et les sauvegardes de vos applications sont stockées dans un conteneur Azure Blob.

- "Consultez les détails de tarification pour Azure NetApp Files".
- "Consultez les détails des prix du stockage Microsoft Azure Blob".
- "Consultez les plans et les tarifs d'Astra Control Service dans Azure Marketplace"

Facturation d'Amazon Web Services

Lorsque vous gérez des clusters AWS avec Astra Control Service, les volumes persistants sont sauvegardés par EBS ou FSX pour NetApp ONTAP et les sauvegardes de vos applications sont stockées dans un compartiment AWS.

- "Voir les détails de tarification pour Amazon Web Services".

Abonnez-vous à Astra Control Service dans Azure Marketplace

Vous pouvez vous abonner au service Astra Control à l'aide d'Azure Marketplace. Vos informations de compte et de facturation sont gérées via Marketplace.

Pour visionner une vidéo de présentation du processus d'abonnement à Azure Marketplace, rendez-vous sur "NetApp TV".

Étapes

1. Accédez au "Azure Marketplace".
2. Sélectionnez **obtenir maintenant**.

3. Suivez les instructions pour vous abonner à un plan.

Abonnez-vous à Astra Control Service sur AWS Marketplace

Vous pouvez vous abonner au service Astra Control avec AWS Marketplace. Vos informations de compte et de facturation sont gérées via Marketplace.

Étapes

1. Accédez au "AWS Marketplace".
2. Sélectionnez **Afficher les options d'achat**.
3. Si vous y êtes invité, connectez-vous à votre compte AWS ou créez un nouveau compte.
4. Suivez les instructions pour vous abonner à un plan.

Abonnez-vous à Astra Control Service directement avec NetApp

Vous pouvez vous abonner au service de contrôle Astra depuis l'interface utilisateur du service de contrôle Astra ou en contactant le service commercial de NetApp.

Passez du Plan gratuit au Plan Premium PayGo

Mettez à niveau votre plan de facturation à tout moment pour commencer à gérer plus de 10 espaces de noms d'Astra Control en payant au fur et à mesure. Vous n'avez besoin que d'une carte de crédit valide.

Étapes

1. Sélectionnez **compte**, puis **facturation**.
2. Sous **plans**, accédez à **Premium PayGo** et sélectionnez **Upgrade Now**.
3. Fournissez les détails de paiement d'une carte de crédit valide et sélectionnez **mise à niveau vers le plan Premium**.

   Astra Control vous enverra un e-mail si la carte de crédit arrive à expiration.

Résultat

Vous pouvez désormais gérer plus de 10 espaces de noms. Astra Control commence à vous charger pour *tous* namespaces que vous gérez actuellement.

Passez du Plan gratuit à l'abonnement Premium

Contactez l'équipe commerciale de NetApp pour bénéficier d'un tarif préférentiel et d'un abonnement annuel.

Étapes

1. Sélectionnez **compte**, puis **facturation**.
2. Sous **plans**, accédez à **abonnement Premium** et sélectionnez **Contact ventes**.
3. Fournissez des détails à l'équipe commerciale pour démarrer le processus.

Résultat

Un ingénieur commercial NetApp vous contactera pour traiter votre bon de commande. Une fois la commande terminée, Astra Control reflétera votre plan actuel dans l'onglet **facturation**.

Afficher les coûts actuels et l'historique de facturation

Astra Control vous montre vos coûts mensuels actuels, ainsi qu'un historique détaillé de facturation par espace de noms. Si vous vous êtes abonné à un plan via un Marketplace, l'historique de facturation n'est pas visible (mais vous pouvez l'afficher en vous connectant au Marketplace).

Étapes

1. Sélectionnez **compte**, puis **facturation**.

   Vos coûts actuels apparaissent sous la vue d'ensemble de la facturation.

2. Pour afficher l'historique de facturation par espace de noms, sélectionnez **Historique de facturation**.

   Astra Control vous indique l'utilisation des minutes et le coût de chaque espace de noms. La minute d'utilisation correspond au nombre de minutes pendant lesquelles Astra Control a géré votre espace de noms au cours d'une période de facturation.

3. Sélectionnez la liste déroulante pour sélectionner un mois précédent.

Changez la carte de crédit pour Premium PayGo

Si nécessaire, vous pouvez changer la carte de crédit qu'Astra Control a en dossier pour la facturation.

Étapes

1. Sélectionnez **compte > facturation > mode de paiement**.
2. Sélectionnez l'icône configurer.
3. Modifier la carte de crédit.

Remarques importantes

- Votre plan de facturation est conforme au compte Astra Control.

  Si vous avez plusieurs comptes, chacun a son propre plan de facturation.

- Votre facture de contrôle Astra comprend des frais pour la gestion de vos espaces de noms. Votre fournisseur cloud vous facture séparément pour le back-end de stockage des volumes persistants.

  "En savoir plus sur la tarification Astra Control".

- Chaque période de facturation se termine le dernier jour du mois.
- Vous ne pouvez pas rétrograder d'un plan Premium à un plan gratuit.

Inviter et supprimer des utilisateurs

Invitez les utilisateurs à rejoindre votre compte Astra Control et supprimez les utilisateurs qui ne devraient plus avoir accès au compte.

Inviter des utilisateurs

Les propriétaires et administrateurs de comptes peuvent inviter d'autres utilisateurs à rejoindre le compte Astra Control.

Étapes

1. Assurez-vous que l'utilisateur dispose d'un "Connexion à Cloud Central".
2. Sélectionnez **compte**.
3. Dans l'onglet **utilisateurs**, sélectionnez **inviter**.
4. Entrez le nom, l'adresse e-mail et le rôle de l'utilisateur.

   Notez ce qui suit :

   - L'adresse e-mail doit correspondre à l'adresse que l'utilisateur a utilisée pour s'inscrire à Cloud Central.
   - Chaque rôle offre les autorisations suivantes :
     - Un **propriétaire** possède des autorisations d'administration et peut supprimer des comptes.
     - Un **Admin** dispose des autorisations de membre et peut inviter d'autres utilisateurs.
     - Un **membre** peut gérer entièrement les applications et les clusters.
     - Un **Viewer** peut afficher les ressources.
5. Pour ajouter des contraintes à un utilisateur avec un rôle membre ou visualiseur, activez la case à cocher **restreindre le rôle aux contraintes**.

   Pour plus d'informations sur l'ajout de contraintes, voir "Gérez les rôles".
6. Pour inviter un autre utilisateur, sélectionnez **Ajouter un autre utilisateur** et entrez les informations pour le nouvel utilisateur.

   Vous pouvez inviter jusqu'à 10 utilisateurs à la fois. Vous pouvez naviguer entre les utilisateurs que vous invitez sur le côté gauche de la boîte de dialogue **inviter utilisateurs**.
7. Sélectionnez **inviter des utilisateurs**.

Résultat

L'utilisateur ou les utilisateurs recevront un e-mail les invitant à rejoindre votre compte.

Modifier le rôle d'un utilisateur

Un propriétaire de compte peut modifier le rôle de tous les utilisateurs, tandis qu'un administrateur de compte peut modifier le rôle des utilisateurs qui ont le rôle Admin, Member ou Viewer.

Étapes

1. Sélectionnez **compte**.
2. Dans l'onglet **utilisateurs**, sélectionnez le menu dans la colonne **actions** de l'utilisateur.
3. Sélectionnez **Modifier le rôle**.
4. Sélectionnez un nouveau rôle.
5. Pour ajouter des contraintes à un utilisateur avec un rôle membre ou visualiseur, activez la case à cocher **restreindre le rôle aux contraintes**.

   Pour plus d'informations sur l'ajout de contraintes, voir "Gérez les rôles".
6. Sélectionnez **confirmer**.

Résultat

Astra Control met à jour les autorisations de l'utilisateur en fonction du nouveau rôle que vous avez

sélectionné.

Supprimer des utilisateurs

Un utilisateur ayant le rôle propriétaire peut à tout moment supprimer d'autres utilisateurs du compte.

Étapes

1. Sélectionnez **compte**.
2. Dans l'onglet **utilisateurs**, sélectionnez les utilisateurs que vous souhaitez supprimer.
3. Sélectionnez le menu dans la colonne **actions** et sélectionnez **Supprimer l'utilisateur**.
4. Lorsque vous y êtes invité, confirmez la suppression en tapant « Supprimer », puis sélectionnez **Oui, Supprimer l'utilisateur**.

Résultat

Astra Control supprime l'utilisateur du compte.

Gérez les rôles

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

Ajoutez une contrainte d'espace de noms à un rôle

Un administrateur ou un propriétaire peut ajouter des contraintes d'espace de noms.

Étapes

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

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

6. Sélectionnez **Ajouter une contrainte**.

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

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

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

10. Sélectionnez **confirmer**.

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

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

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

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

Étapes

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

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

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

Pour en savoir plus

- "Rôles et espaces de noms d'utilisateur"

Ajouter et supprimer des informations d'identification

Ajoutez et supprimez des informations d'identification du fournisseur cloud de votre compte à tout moment. Astra Control utilise ces identifiants pour détecter un cluster Kubernetes et les applications sur le cluster, et provisionner les ressources en votre nom.

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

Ajouter des informations d'identification

La façon la plus courante d'ajouter des informations d'identification à Astra Control est de gérer les clusters, mais vous pouvez également ajouter des informations d'identification à partir de la page compte. Les identifiants seront ensuite disponibles pour choisir lors de la gestion de clusters Kubernetes supplémentaires.

Avant de commencer

- Pour Amazon Web Services, vous devez disposer de la sortie JSON des informations d'identification du compte IAM utilisé pour créer le cluster. "Découvrez comment configurer un utilisateur IAM".
- Pour GKE, vous devez disposer du fichier de clé de compte de service pour un compte de service disposant des autorisations requises. "Découvrez comment configurer un compte de service".

- Pour AKS, vous devez disposer du fichier JSON qui contient la sortie de l'interface de ligne de commande Azure lorsque vous avez créé le principal de service. "Découvrez comment configurer un principal de service".

  Vous aurez également besoin de votre ID d'abonnement Azure, si vous n'avez pas ajouté le fichier JSON.

Étapes

1. Sélectionnez **compte > informations d'identification**.
2. Sélectionnez **Ajouter des informations d'identification**.
3. Sélectionnez **Microsoft Azure**.
4. Sélectionnez **Google Cloud Platform**.
5. Sélectionnez **Amazon Web Services**.
6. Saisissez un nom pour les informations d'identification qui les distinguent des autres informations d'identification dans Astra Control.
7. Indiquez les informations d'identification requises.
8. **Microsoft Azure**: Fournissez Astra Control avec des détails sur votre principal de service Azure en téléchargeant un fichier JSON ou en collant le contenu de ce fichier JSON à partir de votre presse-papiers.

   Le fichier JSON doit contenir la sortie de l'interface de ligne de commandes Azure lorsque vous avez créé le principal de service. Il peut également inclure votre identifiant d'abonnement afin qu'il soit automatiquement ajouté à Astra Control. Sinon, vous devez saisir manuellement l'ID après avoir fourni le fichier JSON.

9. **Google Cloud Platform**: Fournir le fichier de clé de compte de service Google Cloud soit en téléchargeant le fichier soit en collant le contenu à partir de votre presse-papiers.
10. **Amazon Web Services** : fournissez les informations d'identification utilisateur Amazon Web Services IAM en téléchargeant le fichier ou en collant le contenu à partir de votre presse-papiers.
11. Sélectionnez **Ajouter des informations d'identification**.

Résultat

Vous pouvez maintenant sélectionner les informations d'identification lorsque vous ajoutez un cluster à Astra Control.

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", sauf si vous faites pivoter des informations d'identification (voir Faire pivoter les informations d'identification).

> 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 s'authentifier auprès du compartiment de secours. Il est préférable de ne pas supprimer ces informations d'identification.

Étapes

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

3. Sélectionnez **Supprimer**.
4. Saisissez le nom des informations d'identification pour confirmer la suppression, puis sélectionnez **Oui, Supprimer les informations d'identification**.

Résultat

Astra Control supprime les informations d'identification du compte.

Faire pivoter les informations d'identification

Vous pouvez faire pivoter les informations d'identification de votre compte. 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).

Étapes

1. Supprimez les informations d'identification existantes en suivant les étapes de la section Supprimer les informations d'identification.
2. Ajoutez les nouvelles informations d'identification en suivant les étapes de la section Ajouter des informations d'identification.
3. Mettez à jour toutes les rubriques pour utiliser les nouvelles informations d'identification :
   a. Dans le menu de navigation de gauche, sélectionnez **seaux**.
   b. Sélectionnez la liste déroulante dans la colonne **actions** pour le compartiment que vous souhaitez modifier.
   c. Sélectionnez **Modifier**.
   d. Dans la section **Sélectionner les informations d'identification**, choisissez les nouvelles informations d'identification que vous avez ajoutées à Astra Control.
   e. Sélectionnez **mettre à jour**.
   f. Répétez les étapes **b** à **e** pour les compartiments restants de votre système.

Résultat

Astra Control commence à utiliser les nouveaux identifiants du fournisseur cloud.

Surveillez l'activité des comptes

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

Afficher toutes les activités du compte dans Astra Control

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

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

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

2. Sélectionnez **activité**.

Afficher l'activité des comptes pour les clusters

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

Afficher et gérer les notifications

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

Le nombre de notifications non lues est disponible en haut à droite de l'interface.

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

Étapes

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

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

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

Fermez votre compte

Si vous n'avez plus besoin de votre compte Astra Control, vous pouvez le fermer à tout moment.

> Les compartiments créés automatiquement par Astra Control seront automatiquement supprimés lorsque vous fermez votre compte.

Étapes

1. "Annuler la gestion de toutes les applications et clusters".
2. "Supprimer les informations d'identification de l'Astra Control".
3. Sélectionnez **compte > facturation > mode de paiement**.
4. Sélectionnez **Fermer le compte**.
5. Entrez votre nom de compte et confirmez la fermeture du compte.

Gérer les instances cloud

Une instance de cloud est un domaine unique au sein d'un fournisseur de cloud. Vous pouvez créer plusieurs instances cloud pour chaque fournisseur cloud, et chaque instance cloud possède son propre nom, ses identifiants et ses clusters associés.

Vous créez une instance de Cloud lorsque vous ajoutez un nouveau cluster à Astra Control. Vous pouvez modifier une instance de Cloud pour changer son nom ou son compartiment par défaut à l'aide de l'interface

utilisateur Astra Control et effectuer d'autres actions avec l'instance de Cloud à l'aide de l'API Astra Control.

Ajouter une instance de cloud

Vous pouvez ajouter une nouvelle instance de Cloud lorsque vous ajoutez un nouveau cluster à Astra Control. Reportez-vous à la section "Commencez à gérer les clusters Kubernetes à partir d'Astra Control Service" pour en savoir plus.

Modifier une instance de nuage

Vous pouvez modifier une instance de cloud existante pour un fournisseur de cloud.

Étapes

1. Accédez à **Cloud instances**.
2. Dans la liste des instances de Cloud, sélectionnez le menu **actions** pour l'instance de Cloud que vous souhaitez modifier.
3. Sélectionnez **Modifier**.

   Sur cette page, vous pouvez mettre à jour le nom et le compartiment par défaut de l'instance de cloud.

   Chaque instance de cloud d'Astra Control doit avoir un nom unique.

Faites pivoter les informations d'identification d'une instance de Cloud

Vous pouvez utiliser l'API Astra Control pour faire pivoter les informations d'identification pour une instance de Cloud. Pour en savoir plus, "Accédez à la documentation sur l'automatisation d'Astra".

Supprimez une instance de Cloud

Vous pouvez utiliser l'API Astra Control pour supprimer une instance cloud d'un fournisseur cloud. Pour en savoir plus, "Accédez à la documentation sur l'automatisation d'Astra".

Annuler la gestion des applications et des clusters

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

Arrêtez la gestion d'une application

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

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 cesse de gérer l'application.

Arrêtez la gestion d'un cluster

Arrêtez de gérer le cluster que vous ne souhaitez plus gérer avec Astra Control.

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

Il est recommandé de supprimer le cluster d'Astra Control avant de le supprimer via GCP.

Lorsque vous dégérez un cluster :

- Cette action empêche la gestion de votre cluster par Astra Control. Elle ne modifie pas la configuration du cluster et ne supprime pas le cluster.
- Astra Trident ne sera pas désinstallé du cluster. "Découvrez comment désinstaller Astra Trident".

Étapes

1. 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.

Suppression de clusters de votre fournisseur de cloud

Avant de supprimer un cluster Kubernetes contenant des volumes persistants (PV) résidant sur des classes de stockage NetApp, vous devez d'abord supprimer les demandes de volume persistant suivant l'une des méthodes ci-dessous. La suppression de la demande de volume persistant et du volume persistant avant la suppression du cluster vous permet de ne pas recevoir de factures inattendues de votre fournisseur de cloud.

- **Méthode #1** : supprimez les espaces de noms de charge de travail de l'application du cluster. Do *not* delete l'espace de noms Trident.
- **Méthode #2** : supprimez les demandes de volume persistant et les modules, ou le déploiement où les volumes persistants sont montés.

Lorsque vous gérez un cluster Kubernetes à partir d'Astra Control, les applications qui ce cluster utilisent votre fournisseur cloud comme back-end de stockage pour les volumes persistants. Si vous supprimez le cluster de votre fournisseur cloud sans supprimer au préalable les volumes persistants, les volumes back-end sont *non*

supprimés avec le cluster.

L’utilisation de l’une des méthodes ci-dessus supprimera le PVS correspondant de votre cluster. Assurez-vous qu’aucun volume persistant ne réside dans les classes de stockage NetApp du cluster avant de les supprimer.

Si vous n’avez pas supprimé les volumes persistants avant de supprimer le cluster, vous devrez supprimer manuellement les volumes back-end de votre fournisseur de cloud.