Protégez vos applications

Astra Control Center

NetApp
November 27, 2023

Sommaire

Protégez vos applications

Présentation de la protection

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

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

Workflow de protection des applications

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

[Une seule] Protégez toutes vos applications

Pour être sûr que vos applications sont immédiatement protégées, "créez une sauvegarde manuelle de toutes les applications".

[Deux] Configurez une stratégie de protection pour chaque application

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

[Trois] Ajuster les règles de protection

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

[Quatre] Répliquer les applications sur un cluster distant

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

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

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

Protéger les applications avec les snapshots et les sauvegardes

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

Description de la tâche

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

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

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

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

Configurer une règle de protection

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

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

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

Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` conducteur, les politiques de protection ne peuvent pas être utilisées. Migrez vers une classe de stockage prise en charge par Astra Control si vous souhaitez planifier des sauvegardes et des snapshots.

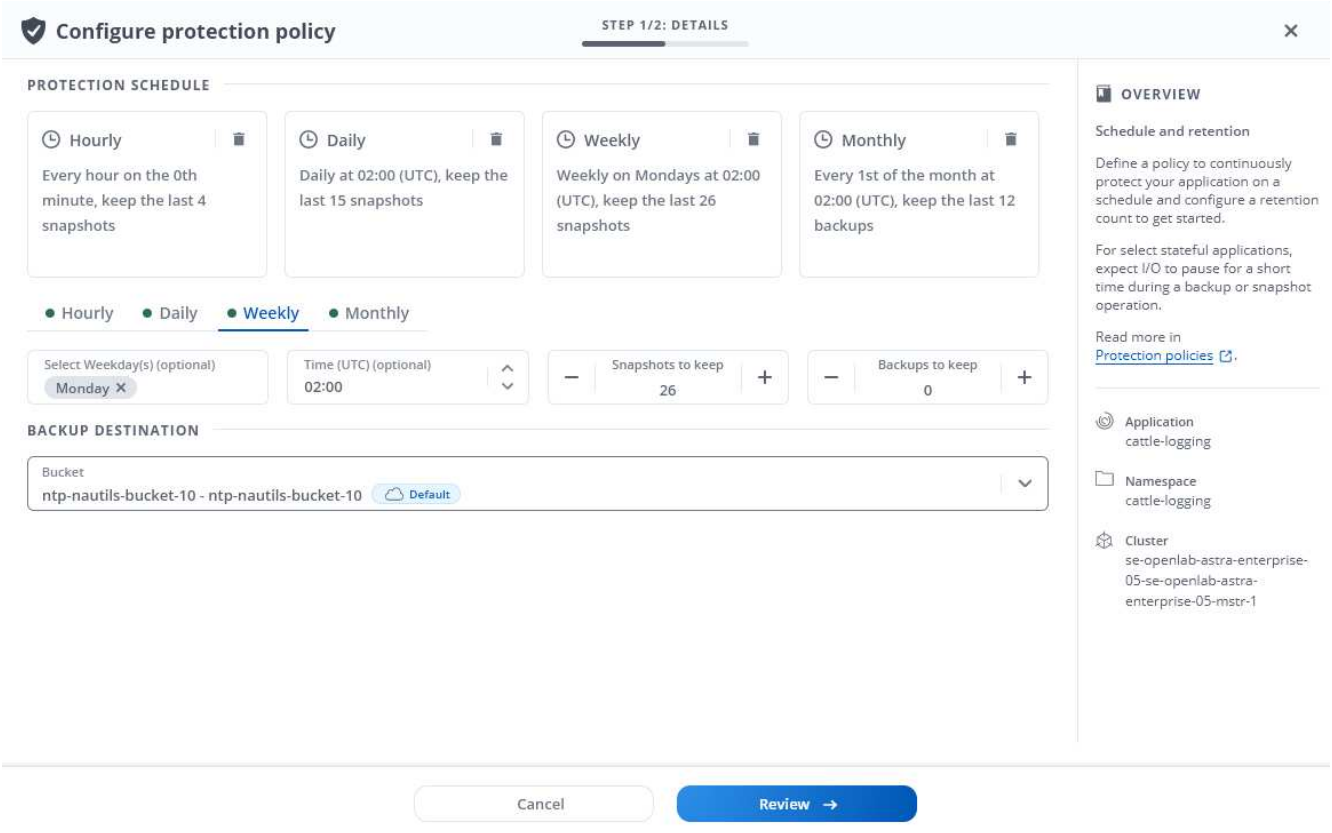
Étapes

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

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

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

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



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

Résultat

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

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

Créer un snapshot

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

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

Étapes

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

Résultat

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

Créer une sauvegarde

Vous pouvez également sauvegarder une application à tout moment.

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

> Si votre application utilise une classe de stockage soutenue par `ontap-nas-economy` vérifiez que vous avez défini un `backendType` dans votre "Objet de stockage Kubernetes" avec une valeur de `ontap-nas-economy` avant d'effectuer toute opération de protection. Sauvegardes des applications sauvegardées par `ontap-nas-economy` sont perturbateurs et l'application sera indisponible jusqu'à la fin de l'opération de sauvegarde.

Étapes

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

Résultat

Astra Control crée une sauvegarde de l'application.

Si votre réseau est en panne ou anormalement lent, une opération de sauvegarde risque d'être terminée. Ceci entraîne l'échec de la sauvegarde.

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

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

Afficher les snapshots et les sauvegardes

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

Étapes

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

   Les snapshots s'affichent par défaut.

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

Supprimer les instantanés

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

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

Étapes

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

Résultat

Astra Control supprime le snapshot.

Annuler les sauvegardes

Vous pouvez annuler une sauvegarde en cours.

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

Étapes

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

Supprimer les sauvegardes

Supprimez les sauvegardes planifiées ou à la demande qui ne vous sont plus nécessaires.

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

Étapes

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

Résultat

Astra Control supprime la sauvegarde.

Restaurez les applications

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

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.
- **Vérifier les volumes de destination** : si vous restaurez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, ReadWriteMaly). L'opération de restauration échoue si le mode d'accès au volume persistant de destination est différent. Par exemple, si votre volume persistant source utilise le mode d'accès RWX, en sélectionnant une classe de stockage de destination qui ne peut pas fournir RWX, comme les disques gérés Azure, AWS EBS, Google persistent Disk ou `ontap-san`, provoque l'échec de l'opération de restauration. Pour plus d'informations sur les modes d'accès aux volumes persistants, reportez-vous au "Kubernetes" documentation :
- **Planifier les besoins en espace** : lorsque vous effectuez une restauration sur place d'une application

utilisant un stockage NetApp ONTAP, l'espace utilisé par l'application restaurée peut doubler. Une fois la restauration sur place effectuée, supprimez les snapshots indésirables de l'application restaurée pour libérer de l'espace de stockage.

- **(clusters OpenShift uniquement) Ajouter des règles** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, un UID SecurityContext est affecté au projet (ou à l'espace de noms Kubernetes). Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

- **Les applications déployées par Helm** : les applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement prises en charge. Les applications déployées avec Helm 2 ne sont pas prises en charge.

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

Étapes

1. Sélectionnez **applications**, puis le nom d'une application.
2. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.
3. Choisissez le type de restauration :
   - **Restaurer les espaces de noms d'origine** : utilisez cette procédure pour restaurer l'app sur place dans le cluster d'origine.

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

     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 utiliser cette procédure pour à une classe de stockage soutenue par `ontap-nas` Sur le même cluster **OU**, copiez l'application sur un autre cluster avec une classe de stockage soutenue par `ontap-nas-economy` conducteur.

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.

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

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

Migrez du stockage ontap-nas-Economy vers le stockage ontap-nas

Vous pouvez utiliser un système Astra Control "restauration des applications" ou "clone de l'application" opération de migration des volumes d'application à partir d'une classe de stockage soutenue par `ontap-nas-economy`, qui autorise des options limitées de protection des applications, à une classe de stockage soutenue par `ontap-nas` Grâce à sa gamme complète d'options de protection Astra Control. L'opération de clonage ou de restauration migre les volumes basés sur Qtree qui utilisent un `ontap-nas-economy` back-end aux volumes standard sauvegardés par `ontap-nas`. Des volumes, qu'ils soient `ontap-nas-economy` sauvegardé uniquement ou mixte, sera migré vers la classe de stockage cible. Une fois la migration terminée, les options de protection ne sont plus limitées.

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

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

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

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

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

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

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

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

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

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

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

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

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

Conditions préalables à la réplication

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

- **Clusters ONTAP** :
  - **Astra Trident** : Astra Trident version 22.10 ou ultérieure doit exister sur les clusters Kubernetes source et de destination qui utilisent ONTAP en tant que back-end.
  - **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Reportez-vous à la section "Présentation des licences SnapMirror dans ONTAP" pour en savoir plus.
- **Peering** :
  - **Cluster et SVM** : les systèmes back-end de stockage ONTAP doivent être peering. Reportez-vous à la section "Présentation du cluster et de SVM peering" pour en savoir plus.

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

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

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

  - **Clusters gérés** : les clusters suivants doivent être ajoutés et gérés par Astra Control, idéalement sur différents sites ou domaines de défaillance :
    - Cluster Kubernetes source
    - Cluster Kubernetes de destination
    - Clusters ONTAP associés
  - **Comptes d'utilisateur** : lorsque vous ajoutez un back-end de stockage ONTAP à Astra Control Center, appliquez les informations d'identification de l'utilisateur avec le rôle « admin ». Ce rôle a des méthodes d'accès `http` et `ontapi` Activation sur les clusters ONTAP source et de destination Reportez-vous à la section "Gérer les comptes utilisateur dans la documentation ONTAP" pour en savoir plus.
- **Configuration d'Astra Trident / ONTAP** : Astra Control Center exige que vous configuriez au moins un back-end de stockage qui prend en charge la réplication pour les clusters source et de destination. Si les clusters source et cible sont identiques, l'application de destination doit utiliser un back-end de stockage

différent de l'application source pour une résilience optimale.

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

Configuration d'une relation de réplication

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

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

Étapes

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

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

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

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

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

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

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

Résultat

Cela crée la relation de réplication.

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

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

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

Par exemple :
Normal | établi

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

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

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

Étapes

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

Résultat

La procédure de basculement entraîne les actions suivantes :

- L'application de destination démarre sur la base du dernier snapshot répliqué.
- Le cluster source et l'app (si opérationnel) ne sont pas arrêtés et continuent à fonctionner.

- L'état de réplication passe à « basculement » puis à « basculement » une fois terminé.
- La règle de protection de l'application source est copiée vers l'application de destination en fonction des plannings présents sur l'application source au moment du basculement.
- Si un ou plusieurs crochets d'exécution post-restauration sont activés dans l'application source, ces crochets d'exécution sont exécutés pour l'application de destination.
- Astra Control affiche l'application sur les clusters source et de destination et son état de santé respectif.

Resynchroniser un basculement de réplication impossible

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

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

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

Étapes

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

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

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

Résultat

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

Réplication inverse des applications

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

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

Étapes

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

Résultat

Les actions suivantes se produisent suite à la réplication inverse :

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

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

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

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

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

Étapes

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

Résultat

Cette action associe les résultats des opérations de resynchronisation et de « relation inversée » pour que

l'application soit en ligne sur le cluster source d'origine et que la réplication reprend au cluster de destination d'origine.

Supprime une relation de réplication d'application

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

Étapes

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

Résultat

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

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

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

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

États d'intégrité des relations de réplication

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

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

États du cycle de vie de la réplication

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

- **Établissement**: Une nouvelle relation de réplication est en cours de création. Astra Control crée un espace de noms si nécessaire, crée des demandes de volume persistant sur les nouveaux volumes du cluster de destination et crée des relations SnapMirror. Cet état peut également indiquer que la réplication est resynchronyée ou inversée.

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

Cloner et migrer les applications

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

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

Avant de commencer

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

- Lors des opérations de clonage, les applications nécessitant une ressource IngressClass ou des crochets Web ne doivent pas avoir ces ressources déjà définies sur le cluster de destination.

> Lors du clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour cela, il faut configurer une policy d'exportation de volume ONTAP afin de permettre ces opérations. Pour ce faire, utilisez les commandes suivantes :
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limites des clones

- **Classes de stockage explicites** : si vous déployez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **ONTAP-nas-Economy-reed Storage class**: Si votre application utilise une classe de stockage soutenue par le `ontap-nas-economy` driver, la partie sauvegarde d'une opération de clonage est perturbatrice. L'application source n'est pas disponible tant que la sauvegarde n'est pas terminée. La partie restauration du clone ne perturbe pas les opérations.
- **Clones et contraintes utilisateur** : tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par étiquette d'espace de noms peut cloner ou restaurer une application dans un nouvel espace de noms sur le même cluster ou sur tout autre cluster du compte de son organisation. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un espace de noms par une opération de clonage ou de restauration, l'administrateur/propriétaire du compte peut modifier le compte d'utilisateur membre et mettre à jour les contraintes de rôle pour l'utilisateur affecté afin d'autoriser l'accès au nouvel espace de noms.
- **Les clones utilisent des compartiments par défaut** : lors d'une sauvegarde d'application ou d'une restauration d'application, vous pouvez éventuellement spécifier un ID de compartiment. Cependant, une opération de clonage d'application utilise toujours le compartiment par défaut défini. Il n'existe aucune option pour modifier les compartiments d'un clone. Si vous souhaitez contrôler le godet utilisé, vous pouvez l'un des deux "modifiez les paramètres par défaut du compartiment" ou faites un "sauvegarde" suivi d'un "restaurer" séparément.
- **Avec Jenkins ci** : si vous clonez une instance déployée par l'opérateur de Jenkins ci, vous devez restaurer manuellement les données persistantes. Il s'agit d'une limitation du modèle de déploiement de l'application.
- **Avec les compartiments S3**: Les compartiments S3 dans Astra Control Center n'indiquent pas la capacité disponible. Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.
- **Avec une version spécifique de PostgreSQL** : les clones d'applications dans le même cluster échouent systématiquement avec le graphique Bitnami PostgreSQL 11.5.0. Pour effectuer un clonage réussi, utilisez une version antérieure ou ultérieure du graphique.

Considérations d'OpenShift

- **Clusters et versions OpenShift** : si vous clonez une application entre les clusters, les clusters source et cible doivent être de la même distribution qu'OpenShift. Par exemple, si vous clonez une application depuis un cluster OpenShift 4.7, utilisez un cluster de destination qui est également OpenShift 4.7.

- **Projets et UID** : lorsque vous créez un projet pour héberger une application sur un cluster OpenShift, le projet (ou l'espace de noms Kubernetes) est affecté à un UID SecurityContext. Pour permettre à Astra Control Center de protéger votre application et de la déplacer vers un autre cluster ou projet dans OpenShift, vous devez ajouter des règles qui permettent à l'application de s'exécuter comme un UID. Par exemple, les commandes OpenShift CLI suivantes octroient les règles appropriées à une application WordPress.

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

Étapes

1. Sélectionnez **applications**.
2. Effectuez l'une des opérations suivantes :
   - Sélectionnez le menu Options dans la colonne **actions** pour l'application souhaitée.
   - Sélectionnez le nom de l'application souhaitée et sélectionnez la liste déroulante d'état en haut à droite de la page.
3. Sélectionnez **Clone**.
4. Spécifiez les détails du clone :
   - Entrez un nom.
   - Choisissez un cluster de destination pour le clone.
   - Entrer les espaces de noms de destination du clone. Chaque espace de noms source associé à l'application est mappé à l'espace de noms de destination que vous définissez.

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

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

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

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

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

Résultat

Astra Control clone l'application en fonction des informations que vous avez fournies. L'opération de clonage a

réussi lorsque le nouveau clone d'application est dans `Healthy` Indiquez la page **applications**.

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

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

Gérer les crochets d'exécution de l'application

Un crochet d'exécution est une action personnalisée que vous pouvez configurer pour s'exécuter conjointement avec une opération de protection des données d'une application gérée. Par exemple, si vous disposez d'une application de base de données, vous pouvez utiliser 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
- Après le basculement

Filtres de crochet d'exécution

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

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

l'expression régulière 2 (RE2)".

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

Remarques importantes sur les crochets d'exécution personnalisés

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

> Puisque les crochets d'exécution réduisent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils s'exécutent, vous devez toujours essayer de réduire le temps d'exécution de vos crochets personnalisés.
> Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Cela signifie que la logique utilisée dans un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde a été effectuée.

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

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

Ordre d'exécution

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

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

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

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

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

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

Déterminez si un crochet va courir

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

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

d’exécution d’une opération de clonage varient.

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

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

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

Scénario	Fonctionnement	Snapshot existant	Sauvegarde existante	Espace de noms	Cluster	Les crochets de snapshot sont exécutés	Les crochets de secours sont en place	Restaurer la course des crochets	Les crochets de basculement s'exécutent
13	Basculement	Y	S/O	Créé par réplication	Identique	N	N	N	Y

Exemples de crochet d'exécution

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

Afficher les crochets d'exécution existants

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

Étapes

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

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

Afficher les scripts existants

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

Étapes

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

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

Ajouter un script

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

Étapes

1. 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 et l'ajouter à Astra Control. Reportez-vous à la section Exemples de crochet d'exécution pour des exemples de crochet. Vous devez disposer d'autorisations propriétaire, administrateur ou membre pour créer des crochets d'exécution.

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

Étapes

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

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

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

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"

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

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

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

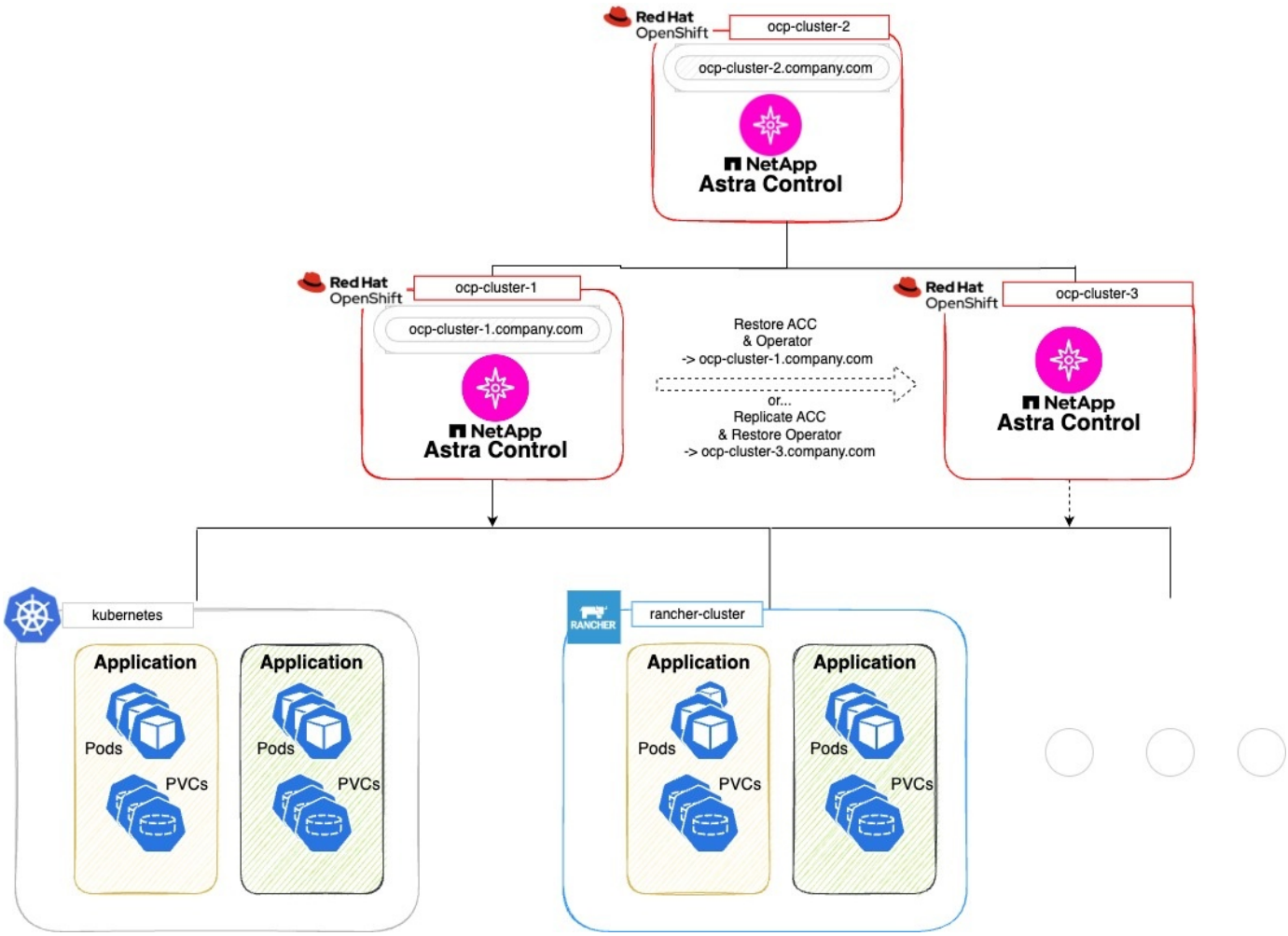
Avant de commencer

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

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

Description de la tâche

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



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

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

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

Non représenté dans le schéma :

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

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

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

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

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

Avant de commencer

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

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire (s'exécutant sur le système `ocp-cluster-2` cluster) :
   a. Connectez-vous à l'instance Astra Control Center secondaire.
   b. "Ajoutez le cluster Astra Control Center principal" (`ocp-cluster-1`).
   c. "Ajouter le troisième cluster de destination" (`ocp-cluster-3`) qui sera utilisé pour la restauration.
2. Gérez Astra Control Center et l'opérateur Astra Control Center sur l'Astra Control Center secondaire :
   a. Dans la page applications, sélectionnez **définir**.
   b. Dans la fenêtre **Define application**, entrez le nom de la nouvelle application (`netapp-acc`).
   c. Choisissez le cluster qui exécute le principal Astra Control Center (`ocp-cluster-1`) Dans la liste déroulante **Cluster**.
   d. Choisissez le `netapp-acc` Espace de noms pour Astra Control Center dans la liste déroulante **namespace**.
   e. Sur la page Ressources du cluster, cochez **inclure des ressources supplémentaires de cluster-scoped**.
   f. Sélectionnez **Ajouter inclure règle**.
   g. Sélectionnez ces entrées et sélectionnez **Ajouter** :
      - Sélecteur d'étiquettes : acc-crds
      - Groupe : apiextensions.k8s.io

- Version : v1
- Type : CustomResourceDefinition

h. Confirmez les informations de l'application.

i. Sélectionnez **définir**.

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

3. Sauvegardez Astra Control Center et l'opérateur :

a. Sur le centre de contrôle Astra secondaire, accédez à la page applications en sélectionnant l'onglet applications.

b. "Sauvegarde" L'application Astra Control Center (`netapp-acc`).

c. "Sauvegarde" l'opérateur (`netapp-acc-operator`).

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

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

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

a. Sélectionnez **applications**, puis sélectionnez le nom de l'application Astra Control Center.

b. Dans le menu Options de la colonne actions, sélectionnez **Restaurer**.

c. Choisissez le type de restauration **Restaurer vers les nouveaux espaces de noms**.

d. Entrez le nom de la restauration (`netapp-acc`).

e. Choisissez le troisième cluster de destination (`ocp-cluster-3`).

f. Mettez à jour l'espace de noms de destination de sorte qu'il s'agisse du même espace de noms que l'espace de noms d'origine.

g. Sur la page Source de restauration, sélectionnez la sauvegarde d'application qui sera utilisée comme source de restauration.

h. Sélectionnez **Restaurer à l'aide des classes de stockage d'origine**.

i. Sélectionnez **Restaurer toutes les ressources**.

j. Examinez les informations de restauration, puis sélectionnez **Restore** pour démarrer le processus de restauration qui restaure Astra Control Center sur le cluster de destination (`ocp-cluster-3`). La restauration est terminée lorsque l'application entre `available` état.

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

a. Ouvrez un terminal et connectez-le au cluster de destination à l'aide du kubeconfig (`ocp-cluster-3`) Qui contient l'Astra Control Center restaurée.

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

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

Réponse :

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.07.0-24 ocp-cluster-
1.company.com           True
```

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

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

i. Modifiez le `astraAddress` sous `spec:` Au FQDN (`ocp-cluster-1.company.com` Dans cet exemple) de l'instance principale d'Astra Control Center.

ii. Enregistrez la configuration.

iii. Vérifiez que l'adresse a été mise à jour :

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

b. Accédez au Restaurez l'opérateur Astra Control Center de ce document pour terminer le processus de restauration.

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

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

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

Avant de commencer

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

Étapes

1. Gérez l'application Astra Control Center principale et le cluster de destination à partir de l'instance Astra Control Center secondaire :
   a. Connectez-vous à l'instance Astra Control Center secondaire.
   b. "Ajoutez le cluster Astra Control Center principal" (`ocp-cluster-1`).
   c. "Ajouter le troisième cluster de destination" (`ocp-cluster-3`) qui sera utilisé pour la réplication.

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

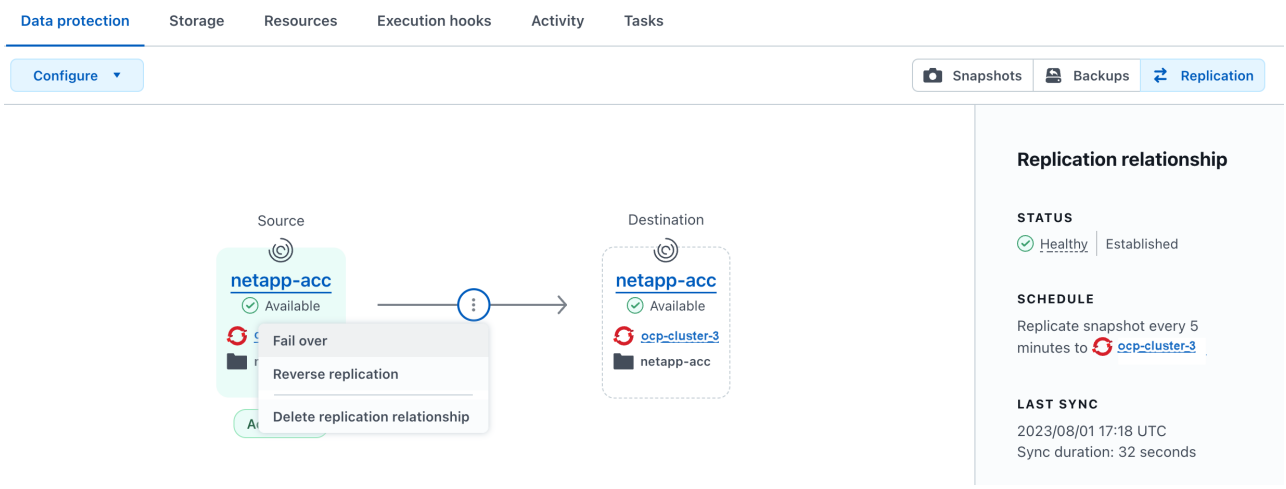
   La réplication nécessite le cluster principal Astra Control Center et le cluster de destination (`ocp-cluster-3`) Utiliser des systèmes back-end de stockage ONTAP peering différents. Une fois chaque back-end ajouté à Astra Control, le back-end apparaît dans l'onglet **découvert** de la page Backends.

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

      La relation de réplication passe de `Establishing` à `Established`. Lorsqu'elle est active, cette réplication se produit toutes les cinq minutes jusqu'à ce que la configuration de réplication soit supprimée.
5. Basculez la réplication vers l'autre cluster si le système principal est corrompu ou n'est plus accessible :

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

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



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

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

6. Compléter la configuration de basculement :

   a. Ouvrez un terminal et connectez-le à l'aide du kubeconfig du troisième cluster (`ocp-cluster-3`). Ce cluster est désormais équipé d'Astra Control Center.

   b. Déterminez le nom de domaine complet d'Astra Control Center sur le troisième cluster (`ocp-cluster-3`).

   c. Mettez à jour la configuration pour référencer le DNS Astra Control Center :

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

      i. Modifiez le `astraAddress` sous `spec:` Avec le FQDN (`ocp-cluster-3.company.com`) du troisième cluster de destination.

      ii. Enregistrez la configuration.

      iii. Vérifiez que l'adresse a été mise à jour :

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

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

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

   CRDS de traefik requis :

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

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

   i. Accédez à "documentation de traefik".

   ii. Copiez la zone « Définitions » dans un fichier.

   iii. Appliquer les modifications :

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

   iv. Redémarrer le traefik :

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

b. Accédez au Restaurez l'opérateur Astra Control Center de ce document pour terminer le processus de restauration.

Étape 2 : restaurez l'opérateur Astra Control Center

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

Étapes

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

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

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

Résultat

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

Dépannage

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

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

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

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

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

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

  Réponse :

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.07.0-24 ocp-cluster-
  1.company.com           True
  ```

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

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

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

Informations sur le copyright

Informations sur les marques commerciales