Gestion et protection des applications

Astra Control Service

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-service/use/manage-apps.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommaire

Gestion et protection des applications . . . 1
Commencez à gérer les applications . . . 1
Protéger les applications avec les snapshots et les sauvegardes . . . 9
[Aperçu technique] protège l’ensemble d’un cluster . . . 21
Restaurez les applications . . . 22
Cloner et migrer les applications . . . 31
Gérer les crochets d’exécution de l’application . . . 33

Gestion et protection des applications

Commencez à gérer les applications

Après vous "Ajoutez un cluster Kubernetes à Astra Control", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour définir les applications.

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

Besoins en termes de gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licence** : pour gérer plus de 10 espaces de noms, vous avez besoin d'un abonnement à Astra Control.
- **Espaces de noms** : les applications peuvent être définies au sein d'un ou plusieurs espaces de noms spécifiés sur un même cluster à l'aide d'Astra Control. Une application peut contenir des ressources couvrant plusieurs espaces de noms au sein d'un même cluster. Astra Control ne prend pas en charge la possibilité de définir des applications entre plusieurs clusters.
- **Classe de stockage** : si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Ressources Kubernetes** : les applications qui utilisent les ressources Kubernetes non collectées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control collecte les ressources Kubernetes suivantes :

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

Méthodes d'installation d'applications prises en charge

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

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

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

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

  Voici quelques applications opérateur qui suivent ces modèles :

  - "Apache K8ssandra"

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

  - "IC Jenkins"
  - "Cluster Percona XtraDB"

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

Installez les applications sur votre cluster

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

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

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

Définir les applications

Une fois qu'Astra Control détecte les espaces de noms sur vos clusters, vous pouvez définir les applications

que vous souhaitez gérer. Vous pouvez choisir gérer une application couvrant un ou plusieurs espaces de noms ou gérer la totalité d'un namespace comme une seule application. La granularité est en effet au niveau de granularité requis pour les opérations de protection des données.

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

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

Avant de commencer

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

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

Description de la tâche

- Avant de commencer, vous devez également comprendre "gestion des espaces de noms standard et système".
- Si vous prévoyez d'utiliser plusieurs espaces de noms avec vos applications dans Astra Control, envisagez "modification des rôles utilisateur avec des contraintes d'espace de noms" avant de définir des applications.
- Pour obtenir des instructions sur la gestion des applications à l'aide de l'API Astra Control, reportez-vous au "Informations sur l'automatisation et les API d'Astra".

Options de gestion des applications

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

Définissez les ressources à gérer en tant qu'application

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

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

Lors de la définition d'applications, assurez-vous de ne pas inclure de ressource Kubernetes dans plusieurs applications avec des règles de protection. Le chevauchement des règles de protection sur des ressources Kubernetes peut provoquer des conflits de données.

En savoir plus sur l'ajout de ressources cluster-scoped à vos espaces de noms d'applications.

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

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

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

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

Étapes

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

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

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

   Pour en savoir plus sur les étiquettes Kubernetes, "Consultez la documentation officielle Kubernetes".

6. (Facultatif) Ajouter des espaces de noms supplémentaires pour l'application en sélectionnant **Ajouter un espace de noms** et en choisissant l'espace de noms dans la liste déroulante.

7. (Facultatif) Entrez des critères de sélection d'étiquette ou d'étiquette pour tout espace de noms supplémentaire que vous ajoutez.
8. (Facultatif) pour inclure des ressources à périmètre de cluster en plus de celles qu'Astra Control inclut automatiquement, cochez **inclure des ressources supplémentaires à périmètre de cluster** et complétez les éléments suivants :
   a. Sélectionnez **Ajouter inclure règle**.
   b. **Groupe** : dans la liste déroulante, sélectionnez le groupe de ressources API.
   c. **Type** : dans la liste déroulante, sélectionnez le nom du schéma d'objet.
   d. **Version** : saisissez la version de l'API.
   e. **Sélecteur d'étiquettes** : si vous le souhaitez, incluez un libellé à ajouter à la règle. Cette étiquette est utilisée pour récupérer uniquement les ressources correspondant à cette étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe.
   f. Vérifiez la règle créée en fonction de vos entrées.
   g. Sélectionnez **Ajouter**.

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

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

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

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

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

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

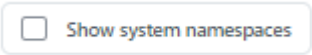
Définissez un espace de noms à gérer en tant qu'application

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

Étapes

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

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

Cochez la case **Afficher les espaces de noms système** pour afficher les espaces de noms système qui ne sont généralement pas utilisés dans la gestion des applications par défaut. 

"En savoir plus".

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

[Aperçu technique] définissez une application à l'aide d'une ressource personnalisée Kubernetes

Vous pouvez spécifier les ressources Kubernetes que vous souhaitez gérer avec Astra Control en les définissant comme une application à l'aide d'une ressource personnalisée (CR). Vous pouvez ajouter des ressources définies dans le cluster si vous souhaitez gérer ces ressources individuellement ou toutes les ressources Kubernetes d'un namespace si, par exemple, vous avez l'intention de gérer et de protéger toutes les ressources d'un namespace spécifique de la même manière et à intervalles réguliers.

Étapes

1. Créer le fichier de ressource personnalisée (CR) et le nommer (par exemple, `astra_mysql_app.yaml`).
2. Nommez l'application dans `metadata.name`.
3. Définissez les ressources d'application à gérer :

spec.includedClusterScopedResources

Incluez les types de ressources cluster-scoped en plus de celles qu'Astra Control inclut automatiquement :

- **spec.includedClusterScopedResources**: *(Facultatif)* Une liste des types de ressource cluster-scoped à inclure.
  - **GroupVersionKind**: *(Facultatif)* identifie sans ambiguïté un type.
    - **Group**: *(requis si groupVersionKind est utilisé)* groupe API de la ressource à inclure.
    - **Version**: *(requis si groupVersionKind est utilisé)* version API de la ressource à inclure.
    - **Kind**: *(requis si groupVersionKind est utilisé)* type de la ressource à inclure.
  - **LabelSelector**: *(Facultatif)* Une requête d'étiquette pour un ensemble de ressources. Il est utilisé pour récupérer uniquement les ressources correspondant à l'étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe. Le résultat des matchLabels et des expressions matchExpressions est ANDed.
    - **MatchLabels**: *(Facultatif)* Une carte de {key,value} paires. Un {key,value} unique dans la carte matchLabels est équivalent à un élément de matchExpressions qui a un champ clé de "key", un opérateur de "in" et un tableau de valeurs contenant uniquement "Value". Les exigences sont ANDed.
    - **MatchExpressions**: *(Facultatif)* Une liste des exigences du sélecteur d'étiquettes. Les exigences sont ANDed.
      - **Key**: *(requis si matchExpressions est utilisé)* la clé de libellé associée au sélecteur de libellé.
      - **Operator**: *(requis si matchExpressions est utilisé)* représente la relation d'une clé à un ensemble de valeurs. Les opérateurs valides sont `In`, `NotIn`, `Exists` et `DoesNotExist`.
      - **Valeurs**: *(obligatoire si matchExpressions est utilisé)_un tableau de valeurs de chaîne. Si l'opérateur est `In` ou `NotIn`, le tableau de valeurs doit être _not* vide. Si l'opérateur est `Exists` ou `DoesNotExist`, le tableau de valeurs doit être vide.

spec.includedNamespaces

Inclure les espaces de noms et les ressources dans ces ressources dans l'application :

- **spec.includedNamespaces**: _(required)_définit l'espace de noms et les filtres facultatifs pour la sélection des ressources.
  - **Namespace**: *(obligatoire)* l'espace de noms qui contient les ressources d'applications que vous souhaitez gérer avec Astra Control.
  - **LabelSelector**: *(Facultatif)* Une requête d'étiquette pour un ensemble de ressources. Il est utilisé pour récupérer uniquement les ressources correspondant à l'étiquette. Si vous ne fournissez pas d'étiquette, Astra Control collecte toutes les instances du type de ressource spécifié pour ce groupe. Le résultat des matchLabels et des expressions matchExpressions est ANDed.
    - **MatchLabels**: *(Facultatif)* Une carte de {key,value} paires. Un {key,value} unique dans la carte matchLabels est équivalent à un élément de matchExpressions qui a un champ clé de "key", un opérateur de "in" et un tableau de valeurs contenant uniquement "Value". Les exigences sont ANDed.

- **MatchExpressions**: *(Facultatif)* Une liste des exigences du sélecteur d'étiquettes. `key` et `operator` sont obligatoires. Les exigences sont ANDed.
  - **Key**: *(requis si matchExpressions est utilisé)* la clé de libellé associée au sélecteur de libellé.
  - **Operator**: *(requis si matchExpressions est utilisé)* représente la relation d'une clé à un ensemble de valeurs. Les opérateurs valides sont `In`, `NotIn`, `Exists` et `DoesNotExist`.
  - **Valeurs**: *(obligatoire si matchExpressions est utilisé)* un tableau de valeurs de chaîne. Si l'opérateur est `In` ou `NotIn`, le tableau de valeurs doit être *not* vide. Si l'opérateur est `Exists` ou `DoesNotExist`, le tableau de valeurs doit être vide.

Exemple YAML :

```yaml
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

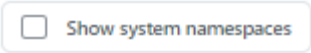
4. Après avoir renseigné le `astra_mysql_app.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

Qu'en est-il des espaces de noms système

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

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



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

Protéger les applications avec les snapshots et les sauvegardes

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

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

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

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

Configurer une règle de protection

Une règle de protection protège une application en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Vous pouvez choisir de créer des snapshots et des sauvegardes toutes les heures, tous les jours, toutes les semaines et tous les mois, et vous pouvez spécifier le nombre de copies à conserver. Vous pouvez définir une règle de protection à l'aide de l'interface utilisateur Web d'Astra Control ou d'un fichier de ressource personnalisée (CR).

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

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

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

Configurez une stratégie de protection à l'aide de l'interface utilisateur Web

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 à conserver pour les horaires, quotidiens, hebdomadaires et mensuels.

   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.

   [Capture d'écran d'un exemple de stratégie de configuration dans laquelle vous pouvez choisir de réaliser des snapshots et des sauvegardes toutes les heures, tous les jours, toutes les semaines ou tous les mois.]

5. [**Tech Preview**] Choisissez un compartiment de destination pour les sauvegardes ou les instantanés dans la liste des compartiments de stockage.
6. Sélectionnez **Revue**.
7. Sélectionnez **définir la stratégie de protection.**

[Aperçu technique] configurez une stratégie de protection à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-schedule-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour répondre à vos besoins en matière d'environnement Astra Control, de configuration de cluster et de protection des données :
   - <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
   - <APPLICATION_NAME> : nom Kubernetes de l'application à sauvegarder.
   - <APPVAULT_NAME> : nom du coffre-fort dans lequel le contenu de la sauvegarde doit être stocké.
   - <BACKUPS_RETAINED> : nombre de sauvegardes à conserver. Zéro indique qu'aucune sauvegarde ne doit être créée.
   - <SNAPSHOTS_RETAINED> : nombre de snapshots à conserver. Zéro indique qu'aucun snapshot ne doit être créé.
   - <GRANULARITY> : fréquence à laquelle le programme doit être exécuté. Valeurs possibles, ainsi que les champs associés obligatoires :
     - `hourly` (nécessite que vous spécifiiez `spec.minute`)
     - `daily` (nécessite que vous spécifiiez `spec.minute` et `spec.hour`)
     - `weekly` (nécessite que vous spécifiiez `spec.minute`, `spec.hour`, et `spec.dayOfWeek`)

    - `monthly` (nécessite que vous spécifiiez `spec.minute`, `spec.hour`, et `spec.dayOfMonth`)
  - <DAY_OF_MONTH> : *(Facultatif)* le jour du mois (1 - 31) que l'horaire doit exécuter. Ce champ est obligatoire si la granularité est définie sur `monthly`.
  - <DAY_OF_WEEK> : *(Facultatif)* le jour de la semaine (0 - 7) que l'horaire doit exécuter. Les valeurs 0 ou 7 indiquent dimanche. Ce champ est obligatoire si la granularité est définie sur `weekly`.
  - <HOUR_OF_DAY> : *(Facultatif)* l'heure du jour (0 - 23) que le programme doit exécuter. Ce champ est obligatoire si la granularité est définie sur `daily`, `weekly`, ou `monthly`.
  - <MINUTE_OF_HOUR> : *(Facultatif)* la minute de l'heure (0 - 59) que le programme doit exécuter. Ce champ est obligatoire si la granularité est définie sur `hourly`, `daily`, `weekly`, ou `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Après avoir renseigné le `astra-control-schedule-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Résultat

Astra Control implémente la règle de protection des données en créant et en conservant des snapshots et des sauvegardes à l'aide du calendrier et de la règle de conservation que vous avez définis.

Créer un snapshot

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

Description de la tâche

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

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

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

Créez un instantané à l'aide de l'interface utilisateur Web

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. [**Tech Preview**] Choisissez un compartiment de destination pour le snapshot dans la liste des compartiments de stockage.
5. Examinez le résumé de l'instantané et sélectionnez **instantané**.

[Aperçu technique] Créez un instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
   - <APPLICATION_NAME> : nom Kubernetes de l'application à snapshot.
   - <APPVAULT_NAME> : nom du coffre-fort d'applications où le contenu de l'instantané doit être stocké.
   - <RECLAIM_POLICY> : *(Facultatif)* définit ce qui arrive à un instantané lorsque le snapshot CR est supprimé. Options valides :
     - `Retain`
     - `Delete` (valeur par défaut)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Après avoir renseigné le `astra-control-snapshot-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

Résultat

Le processus d'instantané commence. Un instantané a réussi lorsque l'état est **Healthy** dans la colonne **State**

de la page **Data protection** > **snapshots**.

Créer une sauvegarde

Vous pouvez également sauvegarder une application à tout moment.

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

> ASTRA Control prend en charge la création de sauvegardes à l'aide de classes de stockage basées sur les pilotes suivants :
>
> - `ontap-nas`
> - `ontap-nas-economy`
> - `ontap-san`
> - `ontap-san-economy`

Description de la tâche

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

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

Créez une sauvegarde à l'aide de l'interface utilisateur Web

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. [**Tech Preview**] Choisissez 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**.

[Aperçu technique] Créez une sauvegarde à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette ressource personnalisée ; choisissez un nom unique et sensible pour votre environnement.
   - <APPLICATION_NAME> : nom Kubernetes de l'application à sauvegarder.
   - <APPVAULT_NAME> : nom du coffre-fort dans lequel le contenu de la sauvegarde doit être stocké.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Après avoir renseigné le `astra-control-backup-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Résultat

Astra Control crée une sauvegarde de l'application.

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

Sauvegardez et restaurez les opérations ontap-nas

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

Avant de commencer

- Vous avez activé Astra Control Provisioner ou Astra Trident.
- Vous avez défini une application dans Astra Control. Cette application aura une fonctionnalité de protection limitée jusqu'à ce que vous ayez terminé cette procédure.
- Vous avez `ontap-nas-economy` sélectionné comme classe de stockage par défaut pour votre système back-end de stockage.

Développez pour les étapes de configuration

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

   a. Trouver le SVM qui héberge `ontap-nas-economy`volumes de l'application basés sur.

   b. Connectez-vous à un terminal connecté à ONTAP où les volumes sont créés.

   c. Masquer le répertoire Snapshot pour le SVM :

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

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

+

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

2. Effectuez les opérations suivantes dans Astra Control Provisioner ou Astra Trident :

   a. Activez le répertoire Snapshot pour chaque volume persistant reposant sur ontap-nas-Economy et associé à l'application :

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

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

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

   Réponse :

```
snapshotDirectory: "true"
```

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

Résultat

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

Créez une sauvegarde immuable

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

Avant de commencer

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

- **Amazon Web Services** : "Activez le verrouillage objet S3 lors de la création du compartiment et définissez un mode de conservation par défaut de « gouvernance » avec une période de conservation par défaut".
- **Google Cloud** : "Configurez un compartiment avec une règle de conservation et spécifiez une période de conservation".
- **Microsoft Azure** : "Configuration d'un compartiment de stockage d'objets blob avec une règle de conservation basée sur le temps concernant l'étendue au niveau du conteneur".
- **NetApp StorageGRID** : "Activez le verrouillage objet S3 lors de la création du compartiment et définissez un mode de conservation par défaut de « conformité » avec une période de conservation par défaut".

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

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

Étapes

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

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

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

Résultat

ASTRA Control crée une sauvegarde immuable de l'application.

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

Afficher les snapshots et les sauvegardes

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

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

Étapes

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

   Les snapshots s'affichent par défaut.

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

Supprimer les instantanés

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

Étapes

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

Résultat

Astra Control supprime le snapshot.

Annuler les sauvegardes

Vous pouvez annuler une sauvegarde en cours.

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

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

Étapes

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

Supprimer les sauvegardes

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

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.

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

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.

[Aperçu technique] protège l'ensemble d'un cluster

Vous pouvez créer une sauvegarde automatique planifiée de tout ou partie des espaces de noms non gérés sur un cluster. NetApp fournit ces workflows en tant que compte de service Kubernetes, liaisons de rôles et tâche cron orchestrée avec un script Python.

Comment cela fonctionne

Lorsque vous configurez et installez le flux de travail de sauvegarde de cluster complet, une tâche cron s'exécute régulièrement et protège tout espace de noms qui n'est pas déjà géré, en créant automatiquement des stratégies de protection basées sur les planifications que vous choisissez pendant l'installation.

Si vous ne souhaitez pas protéger tous les espaces de noms non gérés du cluster avec le workflow complet de sauvegarde du cluster, vous pouvez utiliser le workflow de sauvegarde basé sur des libellés. Le flux de travail de sauvegarde basé sur des étiquettes utilise également une tâche cron, mais au lieu de protéger tous les espaces de noms non gérés, il identifie les espaces de noms par des étiquettes que vous fournissez pour protéger éventuellement les espaces de noms en fonction de stratégies de sauvegarde Bronze, Silver ou Gold.

Lorsqu'un nouvel espace de noms est créé et entre dans le cadre du workflow de votre choix, il est automatiquement protégé, sans aucune action d'administrateur. Ces flux de travail sont implémentés par cluster. Ainsi, différents clusters peuvent utiliser les deux flux de travail avec des niveaux de protection uniques, selon l'importance du cluster.

Exemple : protection complète du cluster

Par exemple, lorsque vous configurez et installez l'intégralité du workflow de sauvegarde du cluster, toutes les applications de n'importe quel espace de noms sont régulièrement gérées et protégées sans que l'administrateur n'ait à faire appel à lui. L'espace de noms n'a pas besoin d'exister au moment de l'installation du workflow ; si un espace de noms est ajouté ultérieurement, il sera protégé.

Exemple : protection par étiquette

Pour plus de granularité, vous pouvez utiliser le flux de production basé sur des étiquettes. Par exemple, vous pouvez installer ce flux de travail et demander à vos utilisateurs d'appliquer l'une des étiquettes à tous les espaces de noms qu'ils souhaitent protéger, en fonction du niveau de protection dont ils ont besoin. Cela permet aux utilisateurs de créer l'espace de noms avec l'une de ces étiquettes et ils n'ont pas à en avertir l'administrateur. Le nouveau namespace et toutes les applications qu'il contient sont automatiquement protégés.

Créer une sauvegarde planifiée de tous les espaces de noms

Vous pouvez créer une sauvegarde planifiée de tous les espaces de noms sur un cluster à l'aide du workflow complet de sauvegarde du cluster.

Étapes

1. Téléchargez les fichiers suivants sur un ordinateur disposant d'un accès réseau à votre cluster :
   - "Components.yaml fichier CRD"
   - "protectCluster.py script Python"
2. Pour configurer et installer la boîte à outils, "suivez les instructions fournies".

Créer une sauvegarde planifiée d'espaces de noms spécifiques

Vous pouvez créer une sauvegarde planifiée d'espaces de noms spécifiques en utilisant leurs étiquettes à l'aide du flux de travail de sauvegarde basé sur des étiquettes.

Étapes

1. Téléchargez les fichiers suivants sur un ordinateur disposant d'un accès réseau à votre cluster :
   - "Components.yaml fichier CRD"
   - "protectCluster.py script Python"
2. Pour configurer et installer la boîte à outils, "suivez les instructions fournies".

Restaurez les applications

Astra Control peut restaurer votre application à partir d'un snapshot ou d'une

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

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

Avant de commencer

- **Protéger vos applications en premier** : il est fortement recommandé de prendre un instantané ou une sauvegarde de votre application avant de la restaurer. Vous pourrez ainsi cloner à partir de l'instantané ou de la sauvegarde si la restauration échoue.
- **Vérifier les volumes de destination** : si vous restaurez vers une classe de stockage différente, assurez-vous que la classe de stockage utilise le même mode d'accès au volume persistant (par exemple, 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.
- **Pilotes de classe de stockage pris en charge** : Astra Control prend en charge la restauration des sauvegardes à l'aide de classes de stockage soutenues par les pilotes suivants :
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- * (Pilote ontap-nas-Economy uniquement) sauvegardes et restaurations* : avant de sauvegarder ou de restaurer une application qui utilise une classe de stockage sauvegardée par `ontap-nas-economy` pilote, vérifiez que "Le répertoire Snapshot du système back-end de stockage ONTAP est masqué". Si ce répertoire n'est pas masqué, l'accès à votre application risque d'être perdu, en particulier s'il utilise NFSv3.

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

Étapes

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

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

ii. Sélectionnez **Suivant**.

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

- **Restaurer vers de nouveaux espaces de noms** : utilisez cette procédure pour restaurer l'application vers un autre cluster ou avec des espaces de noms différents de la source. Vous pouvez également utiliser cette procédure pour migrer une application vers une autre classe de stockage.

  i. Spécifiez le nom de l'application restaurée.

  ii. Choisissez le cluster de destination pour l'application que vous souhaitez restaurer.

  iii. Entrez un espace de noms de destination pour chaque espace de noms source associé à l'application.

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

  iv. Sélectionnez **Suivant**.

  v. Sélectionnez le snapshot ou la sauvegarde à utiliser pour restaurer l'application.

  vi. Sélectionnez **Suivant**.

  vii. Options au choix :

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

  viii. Sélectionnez **Suivant**.

4. Sélectionnez les ressources à filtrer :

   - **Restaurer toutes les ressources** : restaurez toutes les ressources associées à l'application d'origine.
   - **Filtrer les ressources** : spécifiez des règles pour restaurer un sous-ensemble des ressources d'application d'origine :

     i. Choisissez d'inclure ou d'exclure des ressources de l'application restaurée.

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

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

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

[Aperçu technique] Restauration à partir d'une sauvegarde à l'aide d'une ressource personnalisée (CR)

Vous pouvez restaurer des données à partir d'une sauvegarde à l'aide d'un fichier de ressources personnalisées (CR) dans un espace de noms différent ou dans l'espace de noms source d'origine.

Restauration à partir d'une sauvegarde à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-restore-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE> : espace de noms source de l'opération de restauration.
   - <DESTINATION_NAMESPACE> : espace de noms de destination de l'opération de restauration.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directive non résolue dans <stdin> - include:../_include/selective-restore-cr.adoc[]

1. Après avoir renseigné le `astra-control-backup-restore-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

   ```
   kubectl apply -f astra-control-backup-restore-cr.yaml
   ```

Restauration à partir de la sauvegarde vers l'espace de noms d'origine à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-backup-ipr-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.

- <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
- <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Directive non résolue dans <stdin> - include:../_include/selective-restore-cr.adoc[]

1. Après avoir renseigné le `astra-control-backup-ipr-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Aperçu technique] Restauration à partir d'un instantané à l'aide d'une ressource personnalisée (CR)

Vous pouvez restaurer les données d'un instantané à l'aide d'un fichier de ressource personnalisée (CR) dans un espace de noms différent ou dans l'espace de noms source d'origine.

Restauration à partir d'un instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-restore-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.
   - <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
   - <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE> : espace de noms source de l'opération de restauration.
   - <DESTINATION_NAMESPACE> : espace de noms de destination de l'opération de restauration.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directive non résolue dans <stdin> - include:../_include/selective-restore-cr.adoc[]

1. Après avoir renseigné le `astra-control-snapshot-restore-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

   ```
   kubectl apply -f astra-control-snapshot-restore-cr.yaml
   ```

Restauration de l'instantané vers l'espace de noms d'origine à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le `astra-control-snapshot-ipr-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <CR_NAME> : nom de cette opération CR ; choisissez un nom sensible pour votre environnement.

- <APPVAULT_NAME> : nom de l'AppVault dans lequel sont stockés le contenu de la sauvegarde.
- <BACKUP_PATH> : chemin d'accès dans AppVault où sont stockés le contenu de la sauvegarde. Par exemple :

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Directive non résolue dans <stdin> - include:../_include/selective-restore-cr.adoc[]

1. Après avoir renseigné le `astra-control-snapshot-ipr-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Résultat

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

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

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

Filtrer les ressources pendant la restauration d'une application

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

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

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

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

Étapes

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

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

2. Configurez la règle de filtre :

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

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

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

b. (Facultatif) Entrez un nom de ressource.

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

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

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

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

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

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

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

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

Cloner et migrer les applications

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

Le clonage peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre. Par exemple, il peut être intéressant de déplacer les workloads dans un pipeline ci/CD et entre les espaces de noms Kubernetes.

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

Avant de commencer

- **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 des applications sur un autre cluster, vérifiez que vous avez attribué un compartiment par défaut à l'instance cloud contenant le cluster source. Si l'instance de cloud source ne dispose pas d'un

ensemble de compartiments par défaut, l'opération de clonage inter-cluster échoue.

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

Limites des clones

- **Classes de stockage explicites** : si vous déployez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera.
- **Applications économiques ontap-nas** : vous ne pouvez pas utiliser d'opérations de clonage si la classe de stockage de votre application est prise en charge par `ontap-nas-economy` conducteur. Vous pouvez cependant "sauvegardez et restaurez les opérations ontap-nas".
- **Clones et contraintes utilisateur** : tout utilisateur membre ayant des contraintes d'espace de noms par nom/ID d'espace de noms ou par étiquette d'espace de noms peut cloner ou restaurer une application dans un nouvel espace de noms sur le même cluster ou sur tout autre cluster du compte de son organisation. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après qu'une opération de clonage ou de restauration a créé un nouvel espace de noms, l'administrateur/propriétaire du compte peut modifier le compte utilisateur membre et mettre à jour les contraintes de rôle pour que l'utilisateur affecté accorde l'accès au nouvel espace de noms.
- **Les clones utilisent des compartiments par défaut** :
  - Lors d'une sauvegarde ou d'une restauration d'application, vous pouvez spécifier un compartiment à utiliser. Vous devez spécifier un compartiment par défaut lors du clonage des clusters, mais en spécifiant un compartiment est facultatif lorsque vous effectuez le clonage au sein du même cluster.
  - Lorsque vous clonez les clusters, l'instance cloud contenant le cluster source de l'opération de clonage doit disposer d'un ensemble de compartiments par défaut.
  - Il n'existe aucune option pour modifier les compartiments d'un clone. Si vous souhaitez contrôler le godet utilisé, vous pouvez l'un des deux "modifiez les paramètres par défaut du compartiment" ou faites un "sauvegarde" suivi d'un "restaurer" séparément.
- **Avec Jenkins ci** : si vous clonez une instance déployée par l'opérateur de Jenkins ci, vous devez restaurer manuellement les données persistantes. Il s'agit d'une limitation du modèle de déploiement de l'application.

Étapes

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

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

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

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

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

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

Résultat

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

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

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 Service prend en charge les types de crochets d'exécution suivants, selon le moment où ils peuvent être exécutés :

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

- Post-restauration

Filtres de crochet d'exécution

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

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

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

Remarques importantes sur les crochets d'exécution personnalisés

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

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

- La fonction crochets d'exécution est désactivée par défaut pour les nouveaux déploiements d'Astra Control.
  - Vous devez activer la fonction crochets d'exécution avant de pouvoir utiliser les crochets d'exécution.
  - Les utilisateurs propriétaires ou administrateurs peuvent activer ou désactiver la fonction crochets d'exécution pour tous les utilisateurs définis dans le compte Astra Control actuel. Reportez-vous à la section Activez la fonction crochets d'exécution et Désactivez la fonction crochets d'exécution pour obtenir des instructions.
  - Le statut d'activation de la fonctionnalité est conservé pendant les mises à niveau d'Astra Control.
- Un crochet d'exécution doit utiliser un script pour effectuer des actions. De nombreux crochets d'exécution peuvent référencer le même script.
- Astra Control exige que les scripts utilisés par les crochets d'exécution soient écrits au format de scripts shell exécutables.

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

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
1	Clonage	N	N	Nouveau	Identique	Y	N	Y
2	Clonage	N	N	Nouveau	Différente	Y	Y	Y
3	Cloner ou restaurer	Y	N	Nouveau	Identique	N	N	Y
4	Cloner ou restaurer	N	Y	Nouveau	Identique	N	N	Y
5	Cloner ou restaurer	Y	N	Nouveau	Différente	N	N	Y
6	Cloner ou restaurer	N	Y	Nouveau	Différente	N	N	Y

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
7	Restaurer	Y	N	Existant	Identique	N	N	Y
8	Restaurer	N	Y	Existant	Identique	N	N	Y
9	Snapshot	S/O	S/O	S/O	S/O	Y	S/O	S/O
10	Sauvegarde	N	S/O	S/O	S/O	Y	Y	S/O
11	Sauvegarde	Y	S/O	S/O	S/O	N	N	S/O

Exemples de crochet d'exécution

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

Activez la fonction crochets d'exécution

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

Étapes

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

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

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

Désactivez la fonction crochets d'exécution

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

Étapes

1. Accédez à **compte**, puis sélectionnez l'onglet **Paramètres de fonction**.

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

Afficher les crochets d'exécution existants

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

Étapes

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

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

Afficher les scripts existants

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

Étapes

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

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

Ajouter un script

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

Étapes

1. Assurez-vous que la fonction crochets d'exécution est activé.
2. Accédez à **compte**.
3. Sélectionnez l'onglet **scripts**.
4. Sélectionnez **Ajouter**.
5. Effectuez l'une des opérations suivantes :

- Charger un script personnalisé.
  i. Sélectionnez l'option **Télécharger le fichier**.
  ii. Accédez à un fichier et téléchargez-le.
  iii. Donnez un nom unique au script.
  iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.
  v. Sélectionnez **Enregistrer le script**.
- Coller dans un script personnalisé à partir du presse-papiers.
  i. Sélectionnez l'option **Coller ou type**.
  ii. Sélectionnez le champ de texte et collez le texte du script dans le champ.
  iii. Donnez un nom unique au script.
  iv. (Facultatif) Entrez toutes les notes que les autres administrateurs doivent connaître au sujet du script.

6. Sélectionnez **Enregistrer le script**.

Résultat

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

Supprimer un script

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

Étapes

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

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

Créer un crochet d'exécution personnalisé

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

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

Étapes

1. Assurez-vous que la fonction crochets d'exécution est activé.

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

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

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

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

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

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

- Sélectionnez un script existant dans la liste.

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

9. Sélectionnez **Suivant**.
10. Vérifiez la configuration du crochet d'exécution.
11. Sélectionnez **Ajouter**.

Vérifier l'état d'un crochet d'exécution

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

Étapes

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

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

Afficher l'utilisation du script

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

Étapes

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

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

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

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

Modifier un crochet d'exécution

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

d’exécution.

Étapes

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

Désactivez un crochet d’exécution

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

Étapes

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

Supprimer un crochet d’exécution

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

Étapes

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

Pour en savoir plus

- "Projet GitHub NetApp Verda"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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