Gérer des applications

Astra Control Center

NetApp
November 21, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-center-2112/use/manage-apps.html on November 21, 2023. Always check docs.netapp.com for the latest.

Sommaire

Gérer des applications 1
Commencez à gérer les applications 1
Définir un exemple d’application personnalisée 7

Gérer des applications

Commencez à gérer les applications

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

Besoins en termes de gestion des applications

Astra Control présente les exigences de gestion des applications suivantes :

- **Licensing**: Pour gérer des applications à l'aide d'Astra Control Center, vous devez disposer d'une licence Astra Control Center.
- **Espaces de noms** : Astra Control exige qu'une application ne couvre pas plus d'un seul espace de noms, mais qu'un espace de noms peut contenir plus d'une application.
- **StorageClass** : si vous installez explicitement une application avec une classe de stockage 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 explicitement définie sur 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
  - CustomResourceDefinition
  - Ressource CustomResource
  - Ensemble de démonstrations
  - Déploiement
  - Déploiement.Config
  - Entrée
  - MutatingWebhook
  - Demande de volume persistant
  - Pod
  - Et de réplication
  - RoleBinding
  - Rôle
  - Itinéraire
  - Secret
  - Service
  - Compte de service

- StatefulSet
- ValidétingWebhook

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 de l'espace de noms. Ces opérateurs sont généralement conçus avec une architecture « pass-by-value » plutôt qu'une architecture « pass-by-Reference ». Voici quelques applications opérateur qui suivent ces modèles :
  - "Apache K8ssandra"
  - "IC Jenkins"
  - "Cluster Percona XtraDB"

Notez qu'Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture de "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.

> 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.

Installez les applications sur votre cluster

Maintenant que vous avez ajouté votre cluster à Astra Control, vous pouvez installer des applications ou gérer des applications existantes sur le cluster. Toute application étendue à un espace de noms peut être gérée. Une fois les pods en ligne, vous pouvez gérer l'application avec Astra Control.

Pour obtenir de l'aide sur le déploiement des applications validées à partir des graphiques Helm, consultez les éléments suivants :

- "Déployer des bases de données MariaDB à partir d'un graphique Helm"
- "Déployer MySQL à partir d'un graphique Helm"
- "Déploiement de Postgres à partir d'un graphique Helm"
- "Déployez Jenkins à partir d'un graphique Helm"

Gérer des applications

Astra Control vous permet de gérer vos applications au niveau de l'espace de noms ou du label Kubernetes.

> Les applications installées avec Helm 2 ne sont pas prises en charge.

Vous pouvez effectuer les opérations suivantes pour gérer les applications :

- Gérer des applications
  - Gérer les applications par espace de noms
  - Gérer les applications par étiquette Kubernetes
- Ignorer les applications
- Annuler la gestion des applications

> 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. Pour afficher les applications système, utilisez le filtre "Afficher les applications système".

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".

> 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.

Gérer les applications par espace de noms

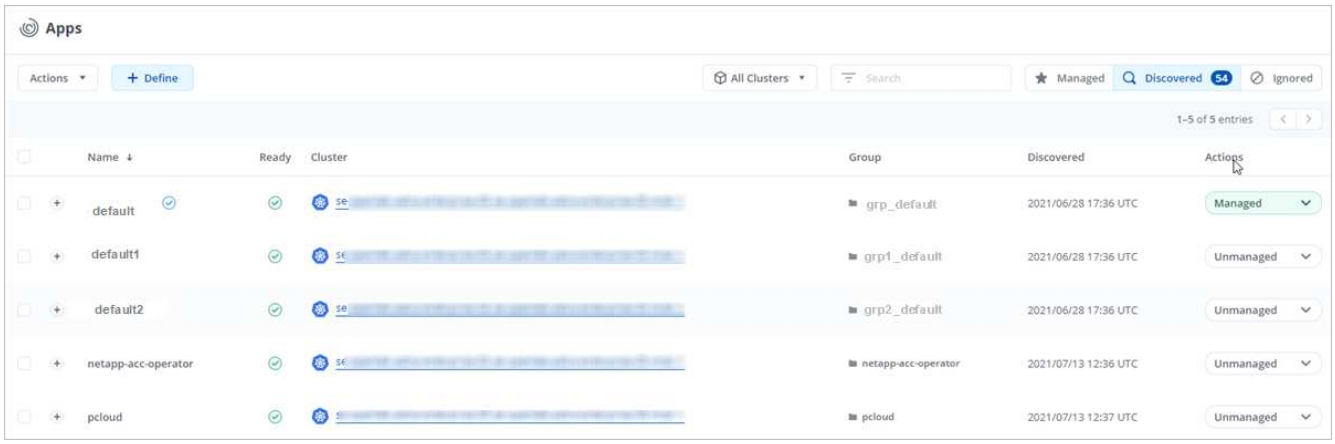
La section **découverts** de la page Apps affiche les espaces de noms et toutes les applications installées par Helm ou les applications étiquetées sur mesure dans ces espaces de noms. Vous pouvez choisir de gérer chaque application individuellement ou au niveau de l'espace de noms. La granularité est en effet au niveau de granularité requis pour les opérations de protection des données.

Par exemple, vous pouvez définir une stratégie de sauvegarde pour « maria » qui a une cadence 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 un espace de noms unique.

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), 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.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **découvert**.



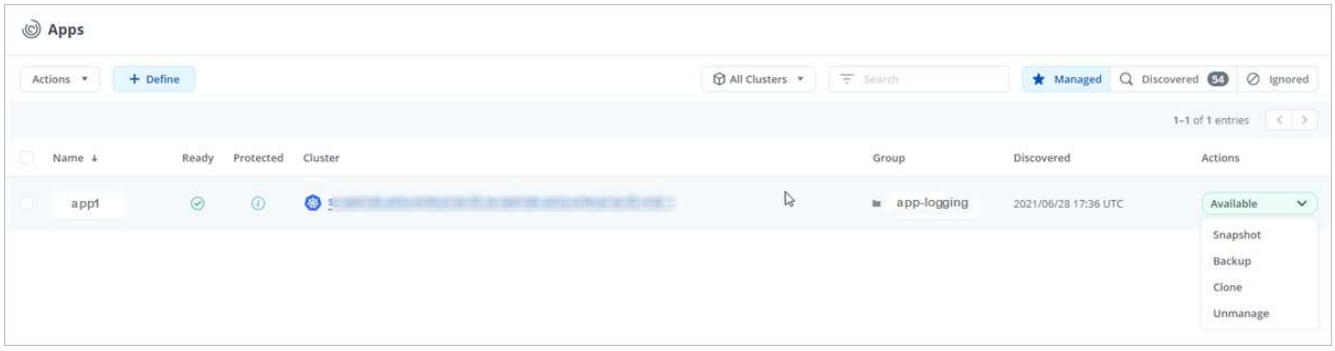
3. Afficher la liste des espaces de noms découverts. Développez l'espace de noms pour afficher les applications et les ressources associées.

   Astra Control présente les applications Helm et les applications étiquetées sur mesure dans l'espace de noms. Si des étiquettes Helm sont disponibles, elles sont désignées par une icône de balise.

4. Consultez la colonne **Groupe** pour voir dans quel espace de noms l'application s'exécute (elle est désignée par l'icône du dossier).
5. Décidez si vous souhaitez gérer chaque application individuellement ou au niveau de l'espace de noms.
6. Recherchez l'application souhaitée au niveau souhaité dans la hiérarchie, et dans le menu actions, sélectionnez **gérer**.
7. Si vous ne souhaitez pas gérer une application, sélectionnez **Ignorer** dans le menu actions situé à côté de l'application.

   Par exemple, si vous souhaitez gérer ensemble toutes les applications sous l'espace de noms « maria » afin qu'elles aient les mêmes stratégies de snapshot et de sauvegarde, vous devez gérer l'espace de noms et ignorer les applications dans l'espace de noms.

8. Pour afficher la liste des applications gérées, sélectionnez **Managed** comme filtre d'affichage.



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

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

Résultat

Les applications que vous avez choisi de gérer sont désormais disponibles dans l'onglet **Managed**. Toutes les applications ignorées seront transférées vers l'onglet **ignoré**. Idéalement, l'onglet découvert affiche zéro

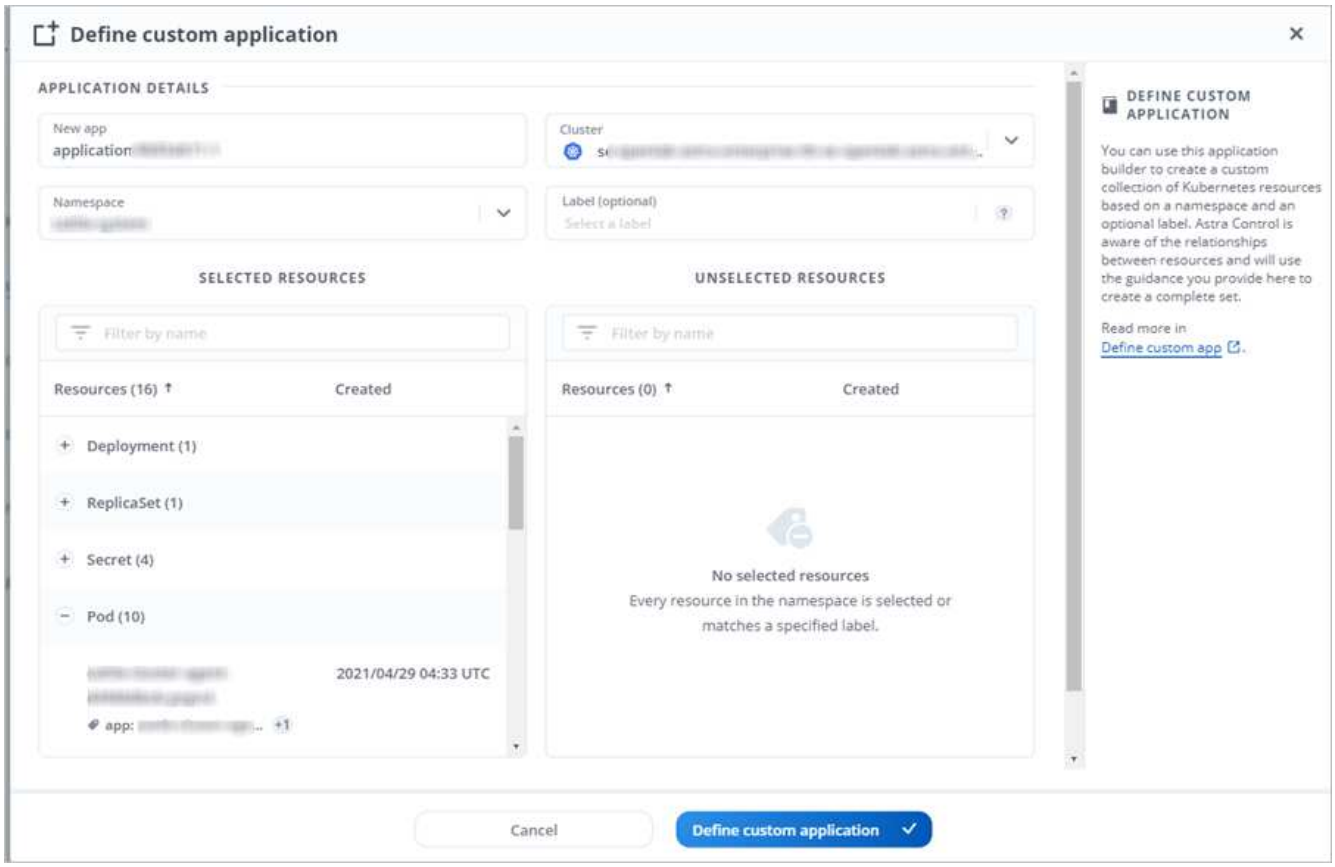
application, de sorte qu'à mesure que de nouvelles applications sont installées, elles sont plus faciles à trouver et à gérer.

Gérer les applications par étiquette Kubernetes

Astra Control inclut une action en haut de la page applications nommée **define Custom app**. Vous pouvez utiliser cette action pour gérer les applications identifiées avec une étiquette Kubernetes. "En savoir plus sur la définition d'applications personnalisées par Kubernetes label".

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **définir**.



3. Dans la boîte de dialogue **Define Custom application**, indiquez les informations requises pour gérer l'application :
   a. **Nouvelle application** : saisissez le nom d'affichage de l'application.
   b. **Cluster** : sélectionnez le cluster où réside l'application.
   c. **Espace de noms :** sélectionnez l'espace de noms de l'application.
   d. **Label:** Entrez un libellé ou sélectionnez un libellé parmi les ressources ci-dessous.
   e. **Ressources sélectionnées** : affichez et gérez les ressources Kubernetes sélectionnées que vous souhaitez protéger (pods, secrets, volumes persistants, etc.).
      - Affichez les étiquettes disponibles en développant une ressource et en sélectionnant le nombre d'étiquettes.
      - Sélectionnez l'un des libellés.

Une fois que vous avez choisi un libellé, celui-ci s'affiche dans le champ **Label**. Astra Control met également à jour la section **Ressources non sélectionnées** pour afficher les ressources qui ne correspondent pas à l'étiquette sélectionnée.

f. **Ressources non sélectionnées** : vérifiez les ressources de l'application que vous ne voulez pas protéger.

4. Sélectionnez **définir l'application personnalisée**.

Résultat

Astra Control permet de gérer l'application. Vous pouvez maintenant le trouver dans l'onglet **Managed**.

Ignorer les applications

Si une application a été découverte, elle apparaît dans la liste découverte. Dans ce cas, vous pouvez nettoyer la liste découverte afin que les nouvelles applications qui viennent d'être installées soient plus faciles à trouver. Vous pouvez aussi avoir des applications que vous gérez et décider par la suite que vous ne souhaitez plus les gérer. Si vous ne souhaitez pas gérer ces applications, vous pouvez indiquer qu'elles doivent être ignorées.

Par ailleurs, vous pouvez avoir besoin de gérer les applications sous un seul espace de noms (géré par un espace de noms). Vous pouvez ignorer les applications que vous souhaitez exclure de l'espace de noms.

Étapes

1. Dans la barre de navigation de gauche, sélectionnez **applications**.
2. Sélectionnez **découvert** comme filtre.
3. Sélectionnez l'application.
4. Dans le menu actions, sélectionnez **Ignorer**.
5. Pour annuler l'ignorer, dans le menu actions, sélectionnez **Unignore**.

Annuler la gestion des applications

Lorsque vous ne souhaitez plus sauvegarder, créer des copies Snapshot ou cloner une application, vous pouvez arrêter de la gérer.

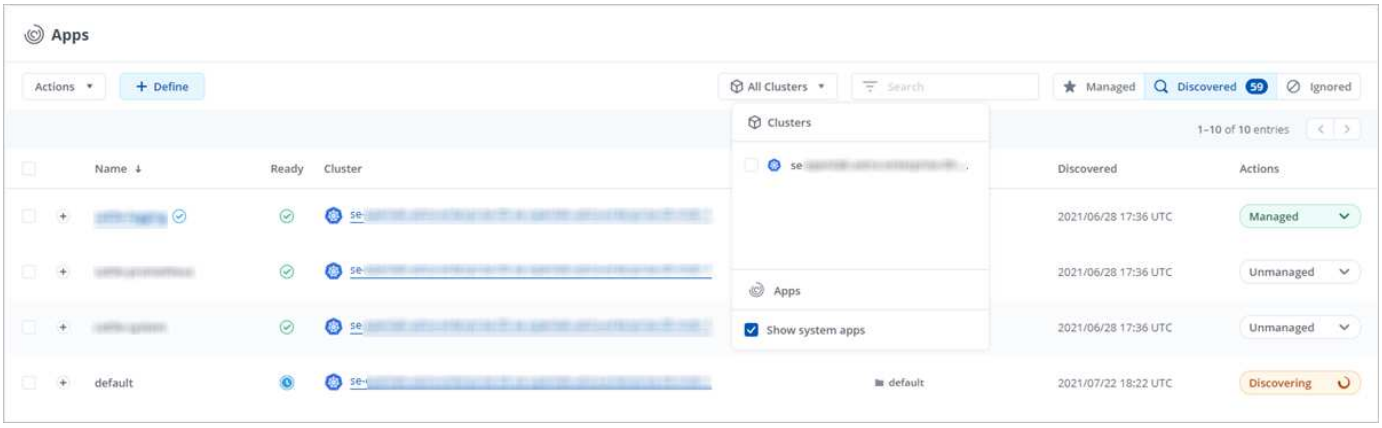
> Si vous annulez la gestion d'une application, toutes les sauvegardes ou instantanés créés précédemment seront perdus.

Étapes

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

Qu’en est-il des applications système ?

Astra Control détecte également les applications système qui s’exécutent sur un cluster Kubernetes. Vous pouvez afficher les applications système en cochant la case **Afficher les applications système** sous le filtre Cluster dans la barre d’outils.



Nous ne vous montrons pas par défaut ces applications système car il est rare que vous ayez besoin de les sauvegarder.

> 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. Pour afficher les applications système, utilisez le filtre “Afficher les applications système”.

Trouvez plus d’informations

- "Utilisez l’API de contrôle Astra"

Définir un exemple d’application personnalisée

La création d’une application personnalisée vous permet de regrouper des éléments de votre cluster Kubernetes dans une seule application.

Une application personnalisée vous offre un contrôle plus granulaire sur les éléments à inclure dans une opération Astra Control, notamment :

- Clonage
- Snapshot
- Sauvegarde
- Règle de protection

Dans la plupart des cas, vous voudrez utiliser les fonctions d’Astra Control sur l’ensemble de votre application. Toutefois, vous pouvez également créer une application personnalisée pour utiliser ces fonctionnalités par les étiquettes que vous attribuez aux objets Kubernetes dans un espace de noms.

Pour créer une application personnalisée, accédez à la page applications et sélectionnez **+ définir**.

Lorsque vous effectuez vos sélections, la fenêtre de l’application personnalisée vous indique quelles

ressources seront incluses ou exclues de votre application personnalisée. Cela vous permet de vous assurer que vous choisissez les critères appropriés pour définir votre application personnalisée.

> Les applications personnalisées ne peuvent être créées qu'au sein d'un espace de nom spécifié sur un même cluster. Astra Control ne prend pas en charge la capacité d'une application personnalisée à s'étendre sur plusieurs espaces de noms ou clusters.

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".

> Le chevauchement de stratégies pour la même ressource sous des noms différents peut entraîner des conflits de données. Si vous créez une application personnalisée pour une ressource, assurez-vous qu'elle n'est pas en cours de clonage ou de sauvegarde dans le cadre d'autres stratégies.

Exemple : politique de protection séparée pour la libération de canaris

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

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

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

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

Étapes

1. Une fois que l'équipe a ajouté le cluster à Astra Control, l'étape suivante consiste à définir une application personnalisée. Pour ce faire, l'équipe sélectionne le bouton **+ Define** sur la page Apps.
2. Dans la fenêtre contextuelle qui s'affiche, l'association est définie `devops-canary-deployment` comme nom de l'application. L'équipe choisit le cluster dans la liste déroulante **Cluster**, puis l'espace de noms de l'application dans la liste déroulante **namespace**.
3. L'association peut saisir l'une ou l'autre `deployment=canary` Dans le champ **étiquettes**, ou sélectionnez cette étiquette parmi les ressources répertoriées ci-dessous.
4. Après avoir défini l'application personnalisée pour le déploiement canary, l'équipe répète le processus pour un déploiement stable.

Lorsque l'équipe a fini de créer les deux applications personnalisées, elle peut traiter ces ressources comme n'importe quelle autre application Astra Control. Ils peuvent les cloner, créer des sauvegardes et des snapshots et créer une règle de protection personnalisée pour chaque groupe de ressources en fonction des étiquettes Kubernetes.

Informations sur le copyright

Copyright © 2023 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.