Concepts

Astra Control Center

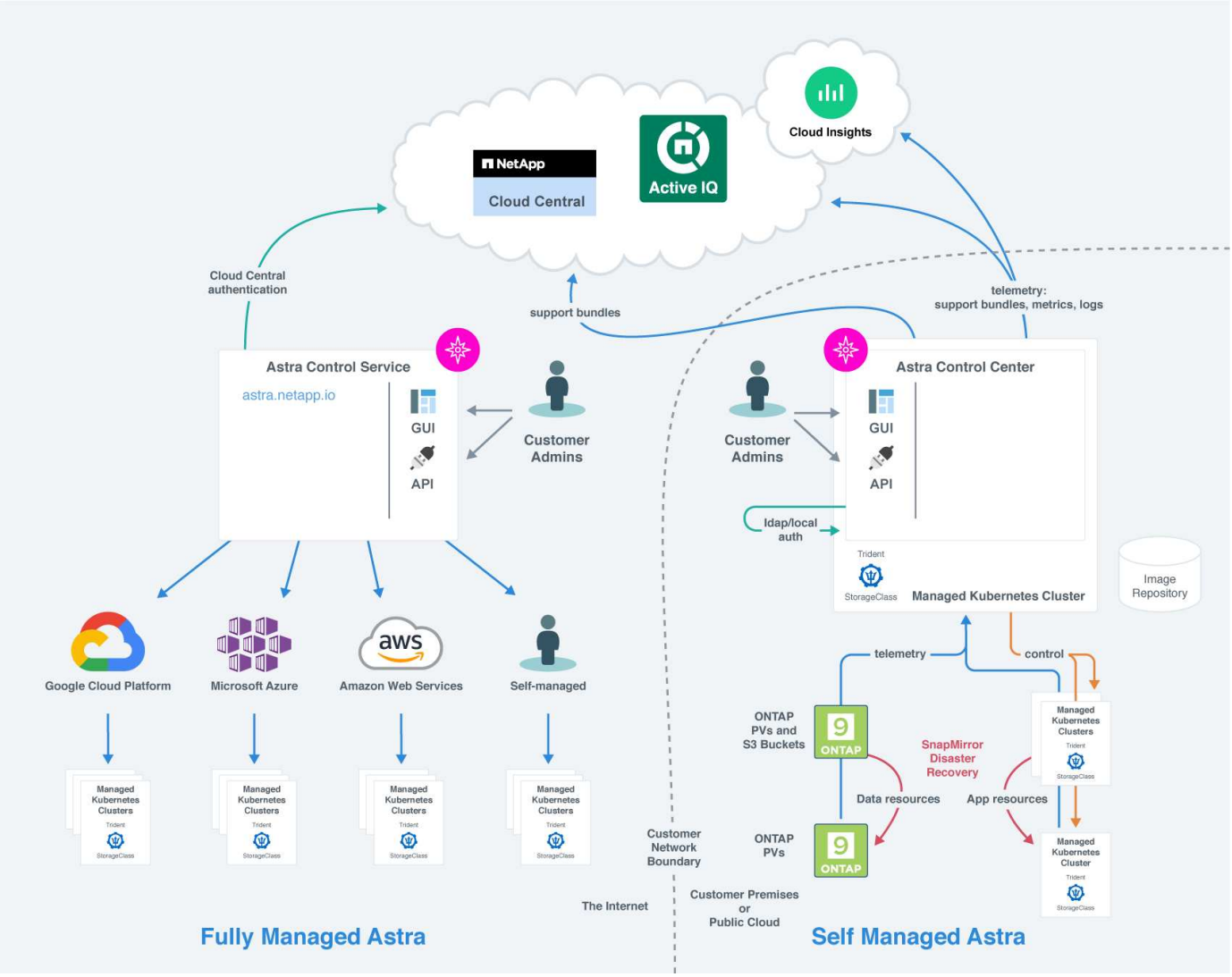
NetApp
November 21, 2023

Sommaire

Concepts

Architecture et composants

Voici un aperçu des divers composants de l'environnement Astra Control.



Composants d'Astra Control

- **Clusters Kubernetes** : Kubernetes est une plateforme portable, extensible et open source pour la gestion des workloads et des services conteneurisés, qui facilite à la fois la configuration déclarative et l'automatisation. Astra propose des services de gestion pour les applications hébergées dans un cluster Kubernetes.
- **Astra Trident** : en tant que fournisseur de stockage open source entièrement pris en charge et orchestrateur géré par NetApp, Astra Trident vous permet de créer des volumes de stockage pour les applications conteneurisées gérées par Docker et Kubernetes. Lorsqu'il est déployé avec Astra Control Center, Trident inclut un système back-end de stockage ONTAP configuré.
- **Back-end de stockage** :
  - Le service Astra Control utilise les systèmes de stockage back-end suivants :

        - "NetApp Cloud Volumes Service pour Google Cloud" Ou Google persistent Disk en tant que backend de stockage pour les clusters GKE
        - "Azure NetApp Files" Ou des disques gérés Azure en tant que système de stockage back-end pour les clusters AKS.
        - "Amazon Elastic Block Store (EBS)" ou "Amazon FSX pour NetApp ONTAP" En tant qu'options de stockage back-end pour les clusters EKS.
    - Astra Control Center utilise les systèmes back-end de stockage suivants :
        - ONTAP AFF, FAS et ASA. En tant que plateforme matérielle et logicielle de stockage, ONTAP fournit des services de stockage de base, la prise en charge de plusieurs protocoles d'accès au stockage et des fonctionnalités de gestion du stockage, telles que les snapshots et la mise en miroir.
        - Cloud Volumes ONTAP
- **Cloud Insights** : outil de surveillance de l'infrastructure cloud NetApp, Cloud Insights vous permet de contrôler les performances et l'utilisation de vos clusters Kubernetes gérés par Astra Control Center. Cloud Insights met en corrélation l'utilisation du stockage avec les charges de travail. Lorsque vous activez la connexion Cloud Insights dans le centre de contrôle Astra, les informations de télémétrie s'affichent dans les pages de l'interface utilisateur du centre de contrôle Astra.

Interfaces de contrôle Astra

Vous pouvez effectuer des tâches à l'aide de différentes interfaces :

- **Interface utilisateur Web (UI)** : Astra Control Service et Astra Control Center utilisent la même interface utilisateur Web où vous pouvez gérer, migrer et protéger des applications. Utilisez également l'interface utilisateur pour gérer les comptes utilisateur et les paramètres de configuration.
- **API** : le service de contrôle Astra et le centre de contrôle Astra utilisent la même API de contrôle Astra. L'API vous permet d'effectuer les mêmes tâches que l'interface utilisateur.

Astra Control Center vous permet également de gérer, de migrer et de protéger les clusters Kubernetes qui s'exécutent dans des environnements de machines virtuelles.

Pour en savoir plus

- "Documentation relative au service après-vente Astra Control"
- "Documentation Astra Control Center"
- "Documentation Astra Trident"
- "Utilisez l'API de contrôle Astra"
- "Documentation Cloud Insights"
- "Documentation ONTAP"

Protection des données

Découvrez les types de protection des données disponibles dans Astra Control Center, et comment il est préférable de les utiliser pour protéger vos applications.

Snapshots, sauvegardes et règles de protection

Les snapshots et les sauvegardes protègent les types de données suivants :

- L'application elle-même
- Tout volume de données persistant associé à l'application
- Tous les artefacts de ressource appartenant à l'application

Un *snapshot* est une copie ponctuelle d'une application stockée sur le même volume provisionné que l'application. Ils sont généralement rapides. Vous pouvez utiliser les snapshots locaux pour restaurer l'application à un point antérieur dans le temps. Les copies Snapshot sont utiles pour les clones rapides. Les snapshots incluent tous les objets Kubernetes de l'application, y compris les fichiers de configuration. Les snapshots sont utiles pour le clonage ou la restauration d'une application au sein du même cluster.

Une *sauvegarde* est basée sur un snapshot. Il est stocké dans le magasin d'objets externe et, par conséquent, peut être plus lent à prendre par rapport aux snapshots locaux. Vous pouvez restaurer une sauvegarde d'application sur le même cluster ou migrer une application en restaurant sa sauvegarde sur un autre cluster. Vous pouvez également choisir une période de conservation plus longue pour les sauvegardes. Les sauvegardes étant stockées dans un référentiel de stockage objet externe, il est généralement plus efficace que les copies Snapshot en cas de panne serveur ou de perte de données.

Une *stratégie de protection* est un moyen de protéger une application en créant automatiquement des snapshots, des sauvegardes ou les deux en fonction d'un planning que vous définissez pour cette application. Une règle de protection vous permet également de choisir le nombre de snapshots et de sauvegardes à conserver dans la planification, et de définir différents niveaux de granularité de planification. L'automatisation de vos sauvegardes et de vos snapshots à l'aide d'une règle de protection est la meilleure façon de garantir que chaque application est protégée en fonction des besoins de votre organisation et des exigences de votre contrat de niveau de service.

> *Vous ne pouvez pas être entièrement protégé tant que vous n'avez pas une sauvegarde récente*. Ceci est important, car les sauvegardes sont stockées dans un magasin d'objets à distance des volumes persistants. En cas de défaillance ou d'accident, le cluster et le stockage persistant qui lui est associé doivent être sauvegardées pour être restaurées. Un snapshot ne vous permettrait pas de restaurer.

Clones

Un *clone* est un doublon exact d'une application, de sa configuration et de ses volumes de données persistants. Vous pouvez créer manuellement un clone sur le même cluster Kubernetes ou sur un autre cluster. Le clonage d'une application peut être utile pour déplacer des applications et du stockage d'un cluster Kubernetes vers un autre.

Réplication sur un cluster distant

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

Astra Control réplique de façon asynchrone les copies Snapshot d'application vers un cluster distant. Le processus de réplication inclut les données des volumes persistants répliqués par SnapMirror et les métadonnées d'application protégées par Astra Control.

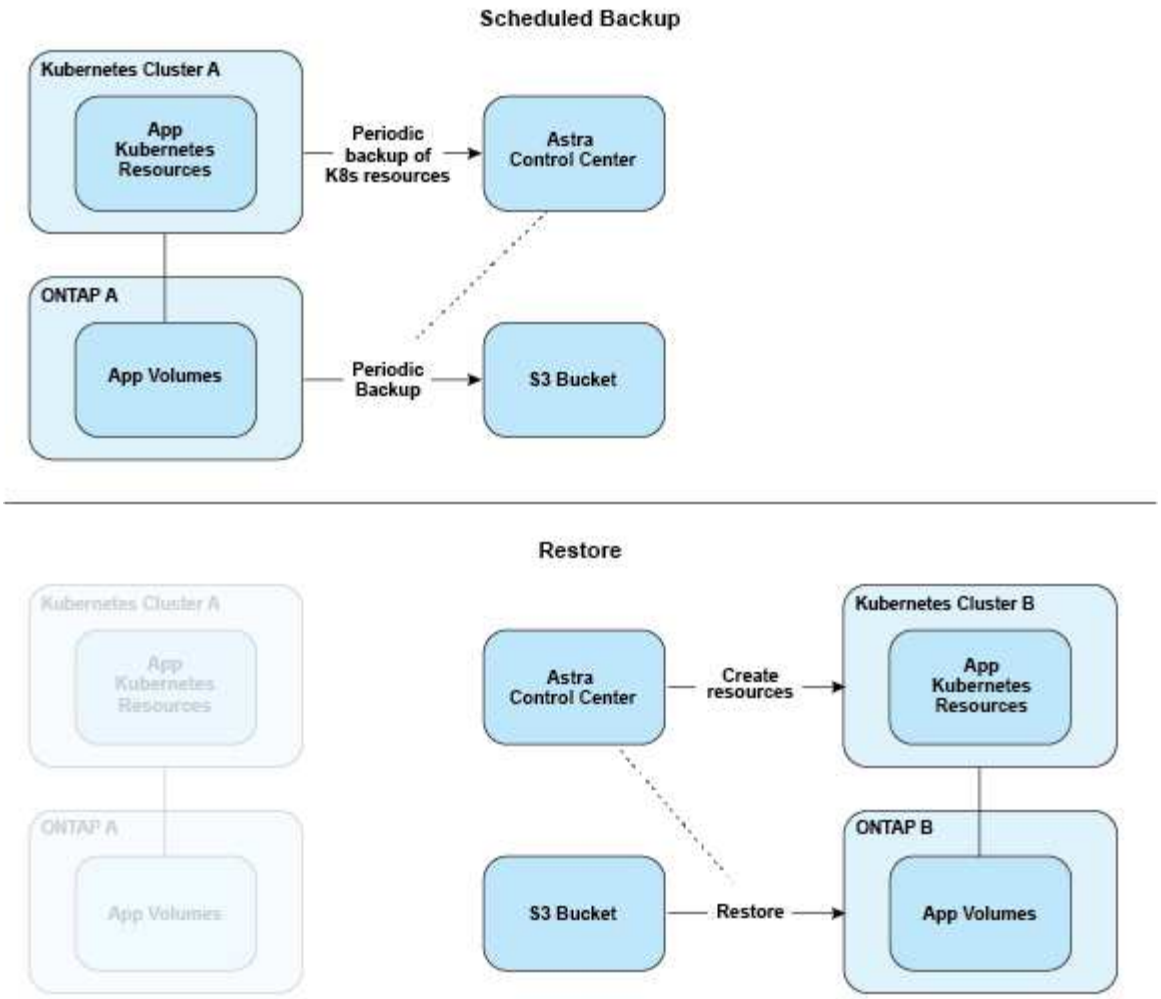
La réplication d'application est différente de la sauvegarde et de la restauration de l'application de la manière suivante :

- **Réplication d'applications** : avec Astra Control, les clusters Kubernetes source et de destination doivent être disponibles et gérés avec leurs systèmes back-end de stockage ONTAP respectifs configurés pour activer NetApp SnapMirror. ASTRA Control utilise la copie Snapshot de l'application pilotée par des règles et la réplique sur le cluster distant. La technologie SnapMirror de NetApp est utilisée pour répliquer les données de volume persistant. Pour basculer, Astra Control peut rendre l'application répliquée en ligne en recréant les objets d'application sur le cluster Kubernetes de destination avec les volumes répliqués sur le cluster ONTAP de destination. Les données du volume persistant étant déjà présentes sur le cluster ONTAP de destination, Astra Control peut offrir des délais de restauration rapides pour le basculement.
- **Sauvegarde et restauration d'applications** : lors de la sauvegarde d'applications, Astra Control crée un instantané des données d'application et le stocke dans un compartiment de stockage objet. Lorsqu'une restauration est nécessaire, les données du compartiment doivent être copiées sur un volume persistant du cluster ONTAP. Pour réaliser l'opération de sauvegarde et de restauration, le cluster Kubernetes/ONTAP secondaire ne doit pas être disponible et géré, mais la copie de données supplémentaire peut générer des délais de restauration plus longs.

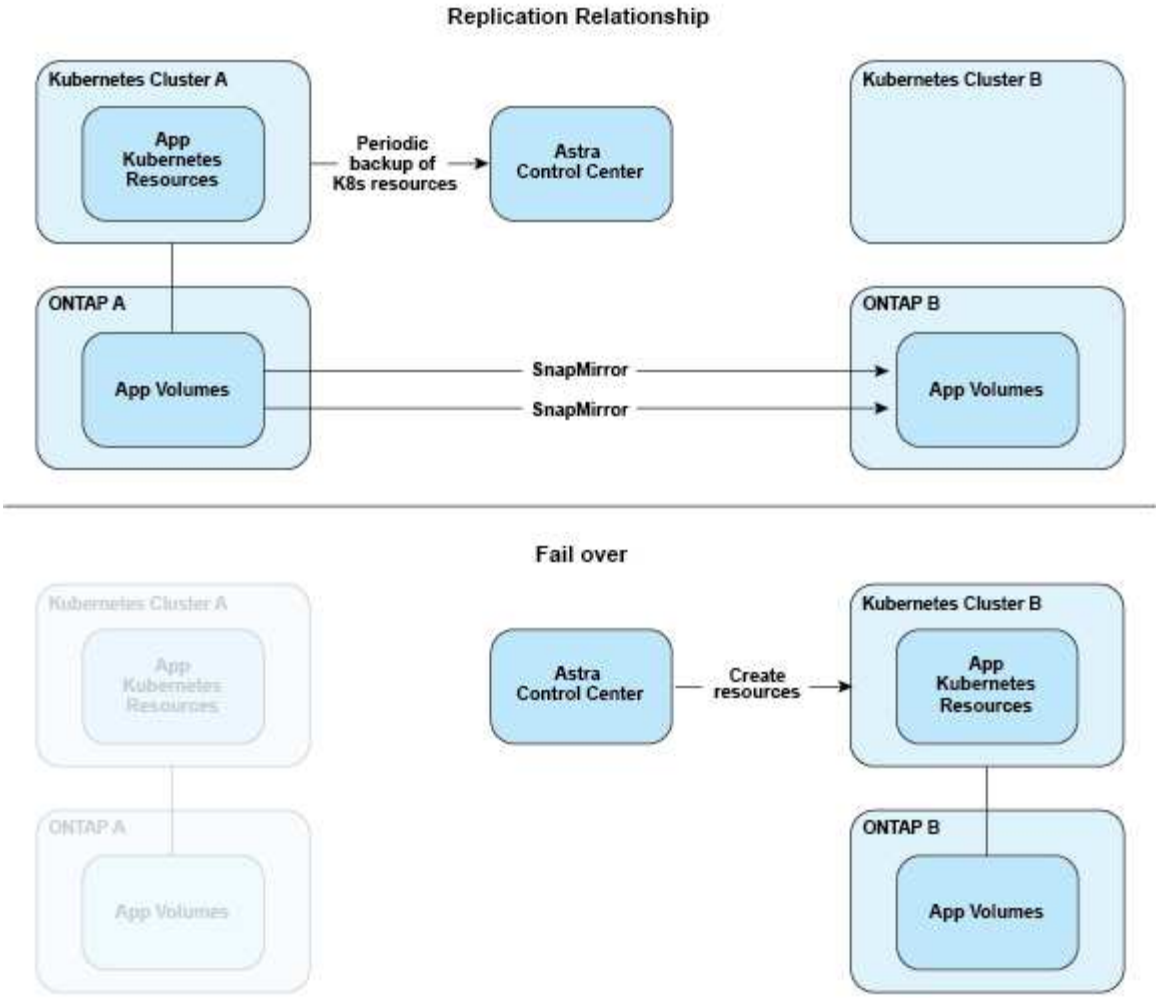
Pour savoir comment répliquer des applications, reportez-vous à la section "Répliquez vos applications sur un système distant grâce à la technologie SnapMirror".

Les images suivantes présentent le processus de sauvegarde et de restauration planifié par rapport au processus de réplication.

Le processus de sauvegarde copie les données dans des compartiments S3 et les restaure à partir de compartiments S3 :



Par contre, la réplication s'effectue via la réplication vers ONTAP, puis un basculement crée les ressources Kubernetes :



Sauvegardes, snapshots et clones avec une licence expirée

Si votre licence expire, vous pouvez ajouter une nouvelle application ou effectuer des opérations de protection des applications (telles que les copies Snapshot, les sauvegardes, les clones et les opérations de restauration) uniquement si l'application que vous ajoutez ou protégez est une autre instance d'Astra Control Center.

Licences

Lorsque vous déployez Astra Control Center, il est installé avec une licence d'évaluation intégrée de 90 jours pour 4,800 unités centrales. Si vous avez besoin de plus de capacité ou d'une période d'évaluation plus longue, ou si vous souhaitez effectuer une mise à niveau vers une licence complète, vous pouvez obtenir une autre licence d'évaluation ou une licence complète auprès de NetApp.

Vous obtenez une licence de l'une des manières suivantes :

- Si vous évaluez Astra Control Center et que vous avez besoin de termes d'évaluation différents de ceux inclus dans la licence d'évaluation intégrée, contactez NetApp pour demander un fichier de licence d'évaluation différent.
- "Si vous avez déjà acheté Astra Control Center, générez votre fichier de licence NetApp (NLF)" En vous connectant au site du support NetApp et en accédant à vos licences logicielles via le menu systèmes.

Pour plus d'informations sur les licences requises pour les systèmes de stockage back-end ONTAP, reportez-vous à la "systèmes back-end de stockage pris en charge".

> Assurez-vous que votre licence active au moins autant d'UC que nécessaire. Si le nombre d'UC actuellement gérées par Astra Control Center dépasse les UC disponibles dans la nouvelle licence en cours d'application, vous ne pourrez pas appliquer la nouvelle licence.

Licences d'évaluation et licences complètes

Une licence d'évaluation intégrée est fournie avec une nouvelle installation d'Astra Control Center. Une licence d'évaluation offre les mêmes fonctionnalités qu'une licence complète pour une période limitée (90 jours). Après la période d'évaluation, une licence complète est requise pour continuer à bénéficier de toutes les fonctionnalités.

Expiration de la licence

Si la licence Astra Control Center active expire, l'interface utilisateur et les fonctionnalités d'API des fonctionnalités suivantes ne sont pas disponibles :

- Snapshots et sauvegardes locaux manuels
- Snapshots et sauvegardes locaux programmés
- Restauration à partir d'un snapshot ou d'une sauvegarde
- Clonage à partir d'un snapshot ou état actuel
- Gestion de nouvelles applications
- Configuration des règles de réplication

Mode de calcul de la consommation des licences

Lorsque vous ajoutez un nouveau cluster à Astra Control Center, il ne prend pas en compte les licences consommées tant qu'au moins une application exécutée sur le cluster est gérée par Astra Control Center.

Lorsque vous commencez à gérer une application sur un cluster, toutes les unités de processeur de ce cluster sont incluses dans la consommation de licence Astra Control Center, à l'exception des unités de processeur de nœud de cluster Red Hat OpenShift signalées par un à l'aide du libellé `node-role.kubernetes.io/infra: ""`.

> Les nœuds d'infrastructure Red Hat OpenShift ne consomment pas de licences dans Astra Control Center. Pour marquer un nœud en tant que nœud d'infrastructure, appliquez le libellé `node-role.kubernetes.io/infra: ""` au nœud.

Trouvez plus d'informations

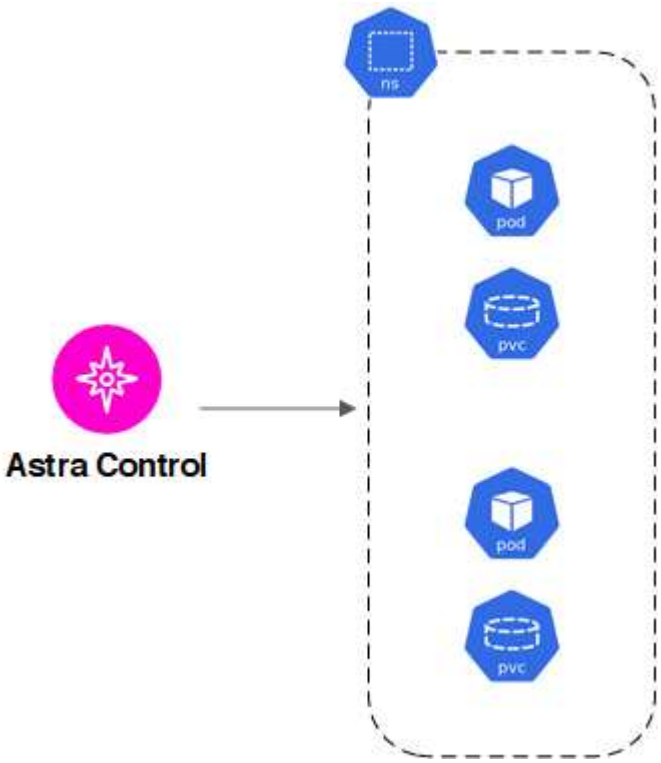
- "Ajoutez une licence lorsque vous configurez Astra Control Center pour la première fois"
- "Mettre à jour une licence existante"

Gestion des applications

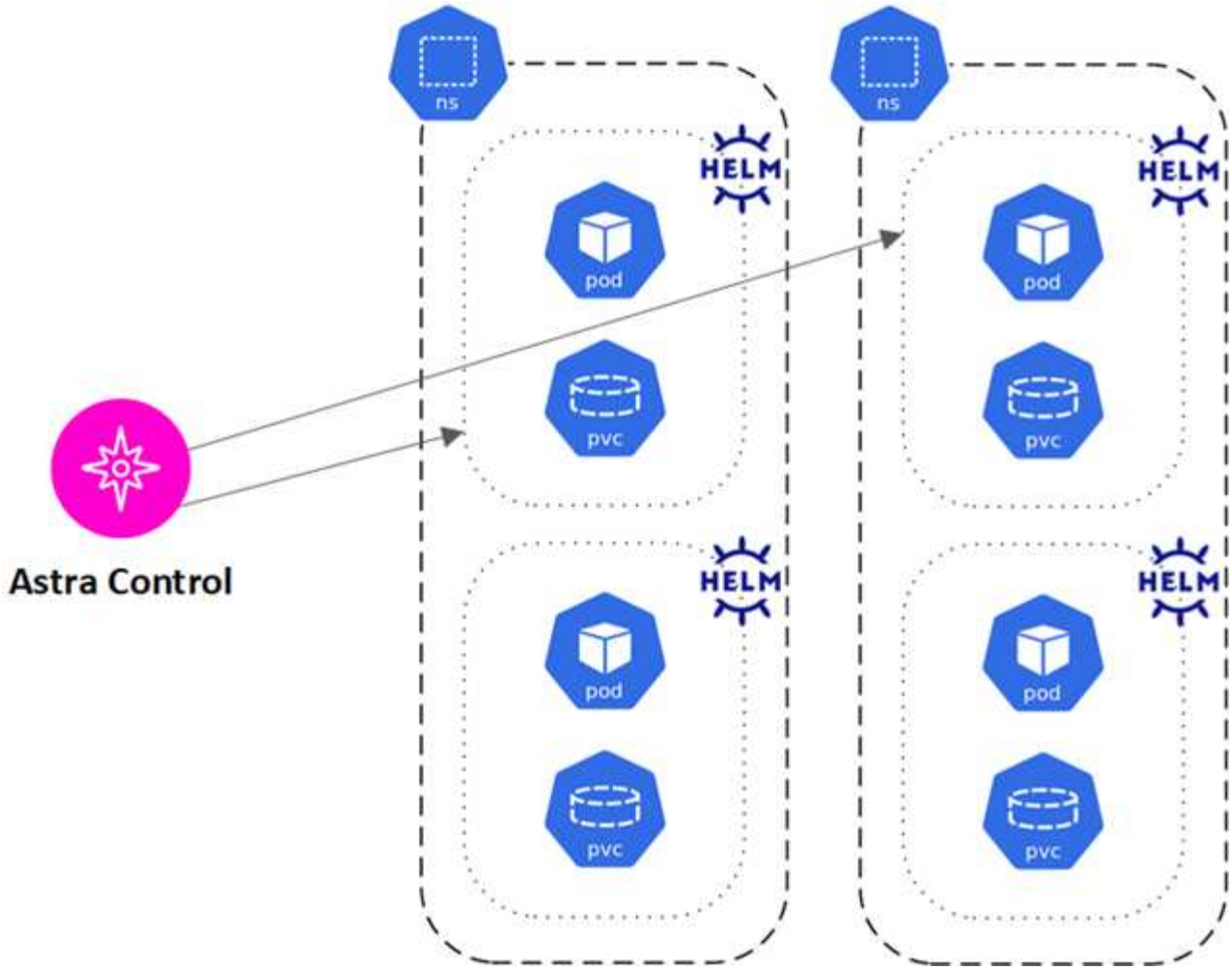
Lorsque Astra Control détecte vos clusters, les applications de ces clusters ne sont pas

gérées jusqu'à ce que vous choisissiez comment les gérer. Une application gérée d'Astra Control peut être l'une des suivantes :

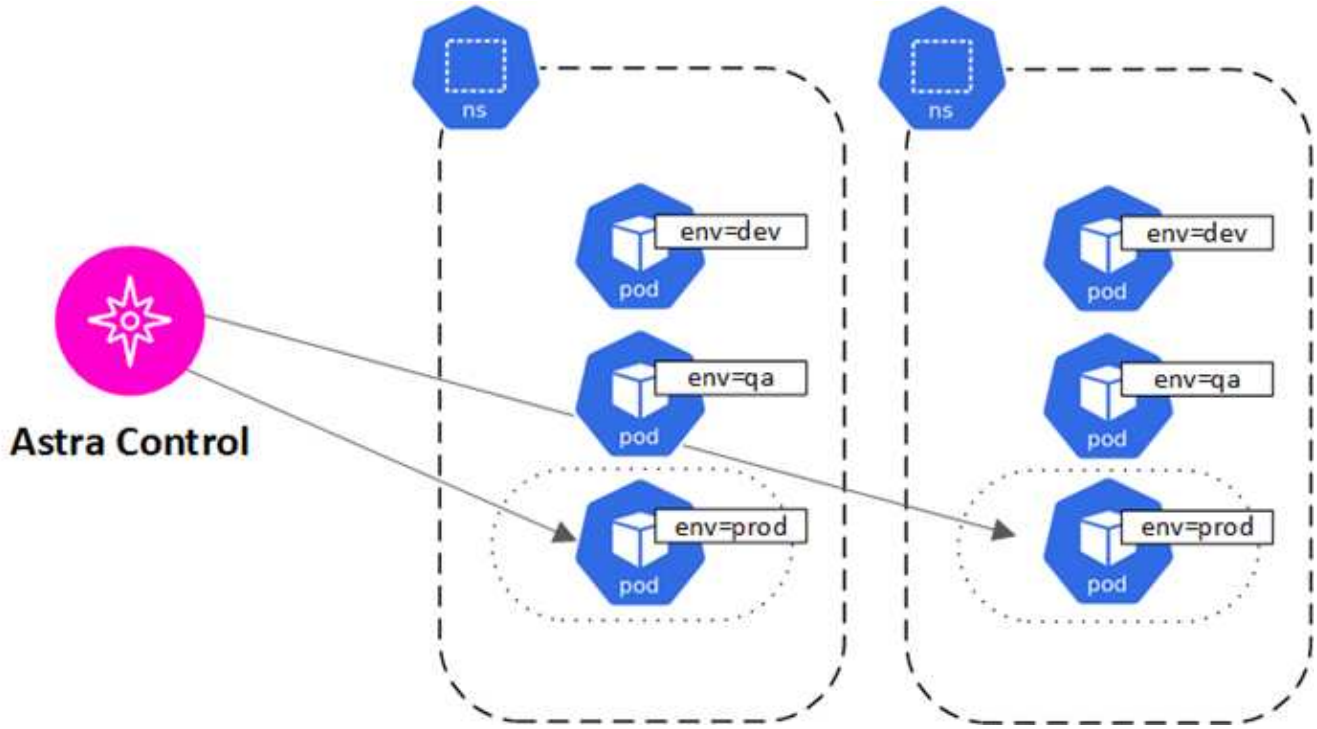
- Un espace de nom, y compris toutes les ressources de cet espace de nom



- Une application individuelle déployée au sein d'un ou plusieurs espaces de noms (helm3 est utilisé dans cet exemple)



- Groupe de ressources identifié par une étiquette Kubernetes dans un ou plusieurs espaces de noms



Classes de stockage et taille de volume persistant

Astra Control Center prend en charge ONTAP en tant que système de stockage back-end.

Présentation

Le centre de contrôle Astra est compatible avec les éléments suivants :

- **Classes de stockage Astra Trident reposant sur le stockage ONTAP** : si vous utilisez un système back-end ONTAP, Astra Control Center offre la possibilité d'importer le système back-end ONTAP pour générer des rapports sur diverses informations de surveillance.

> Les classes de stockage Astra Trident doivent être préconfigurées en dehors d'Astra Control Center.

Classes de stockage

Lorsque vous ajoutez un cluster à Astra Control Center, vous êtes invité à sélectionner une classe de stockage précédemment configurée sur ce cluster comme classe de stockage par défaut. Cette classe de stockage sera utilisée lorsqu'aucune classe de stockage n'est spécifiée dans une demande de volume persistant. La classe de stockage par défaut peut être modifiée à tout moment dans Astra Control Center et toute classe de stockage peut être utilisée à tout moment en spécifiant le nom de la classe de stockage dans le graphique ESV ou Helm. Assurez-vous de n'avoir qu'une seule classe de stockage par défaut définie pour votre cluster Kubernetes.

Pour en savoir plus

- "Documentation Astra Trident"

Rôles et espaces de noms d'utilisateur

Apprenez-en plus sur les rôles d'utilisateur et les espaces de noms d'Astra Control, et découvrez comment vous pouvez les utiliser pour contrôler l'accès aux ressources de votre entreprise.

Rôles utilisateur

Vous pouvez utiliser des rôles pour contrôler l'accès des utilisateurs aux ressources ou aux fonctionnalités d'Astra Control. Les rôles d'utilisateur dans Astra Control sont les suivants :

- Un **Viewer** peut afficher les ressources.
- Un **membre** dispose des autorisations de rôle Viewer et peut gérer les applications et les clusters, annuler la gestion des applications et supprimer des instantanés et des sauvegardes.
- Un **Admin** dispose des autorisations de rôle de membre et peut ajouter et supprimer d'autres utilisateurs, à l'exception du propriétaire.
- Un **propriétaire** possède des autorisations de rôle d'administrateur et peut ajouter et supprimer des comptes d'utilisateur.

Vous pouvez ajouter des contraintes à un membre ou à un visualiseur pour limiter l'utilisateur à un ou plusieurs

Espaces de noms.

Espaces de noms

Un espace de noms est une portée que vous pouvez attribuer à des ressources spécifiques au sein d'un cluster géré par Astra Control. Astra Control détecte les espaces de noms d'un cluster lorsque vous ajoutez le cluster à Astra Control. Une fois découverts, les espaces de noms sont disponibles pour leur attribuer en tant que contraintes. Seuls les membres ayant accès à cet espace de noms peuvent utiliser cette ressource. Vous pouvez utiliser les espaces de noms pour contrôler l'accès aux ressources à l'aide d'un paradigme adapté à votre entreprise (par exemple, par régions physiques ou par divisions au sein d'une entreprise). Lorsque vous ajoutez des contraintes à un utilisateur, vous pouvez configurer cet utilisateur pour qu'il ait accès à tous les espaces de noms ou seulement à un ensemble spécifique d'espaces de noms. Vous pouvez également affecter des contraintes d'espace de noms à l'aide d'étiquettes d'espace de noms.

Trouvez plus d'informations

"Gérez les utilisateurs et les rôles locaux"

Sécurité des pods

Astra Control Center prend en charge la limitation des privilèges via les politiques de sécurité du pod (CSP) et l'admission à la sécurité du pod (PSA). Ces frameworks vous permettent de limiter les utilisateurs ou les groupes capables d'exécuter des conteneurs et les privilèges dont ils disposent.

Certaines distributions Kubernetes peuvent disposer d'une configuration de sécurité du pod par défaut trop restrictive et entraîner des problèmes lors de l'installation d'Astra Control Center.

Vous pouvez utiliser les informations et exemples inclus ici pour comprendre les changements de sécurité apportés par Astra Control Center et utiliser une approche de sécurité de pod qui fournit la protection dont vous avez besoin sans interférer avec les fonctions du Control Center Astra.

PSA appliquée par Astra Control Center

Pendant l'installation, Astra Control Center permet d'appliquer une entrée de sécurité de pod en ajoutant l'étiquette suivante au `netapp-acc` ou un espace de noms personnalisé :

```
pod-security.kubernetes.io/enforce: privileged
```

PSP installé par Astra Control Center

Lorsque vous installez Astra Control Center sur Kubernetes 1.23 ou 1.24, plusieurs règles de sécurité du pod sont créées lors de l'installation. Certaines sont permanentes, certaines d'entre elles sont créées pendant certaines opérations et sont supprimées une fois l'opération terminée. Astra Control Center ne tente pas d'installer les PSP lorsque le cluster hôte exécute Kubernetes 1.25 ou une version ultérieure, car ils ne sont pas pris en charge sur ces versions.

PSP créé lors de l'installation

Lors de l'installation d'Astra Control Center, l'opérateur du centre de contrôle Astra installe une politique de

sécurité de pod personnalisée, a `Role` objet, et un `RoleBinding` Objet prenant en charge le déploiement des services de centre de contrôle Astra dans l'espace de noms d'Astra Control Center.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                              PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
netapp-astra-deployment-psp    false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                      CREATED AT
netapp-astra-deployment-role              2022-06-27T19:34:58Z

kubectl get rolebinding -n <namespace_name>

NAME                                      ROLE
AGE
netapp-astra-deployment-rb                Role/netapp-astra-deployment-role
32m
```

PSP créé pendant les opérations de sauvegarde

Pendant les opérations de sauvegarde, Astra Control Center crée une règle de sécurité dynamique de pod, A. `ClusterRole` objet, et un `RoleBinding` objet. Ils prennent en charge le processus de sauvegarde, qui se produit dans un espace de noms distinct.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                             PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                   CREATED AT
netapp-astra-backup   2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                   ROLE                         AGE
netapp-astra-backup   Role/netapp-astra-backup   62s
```

PSP créé lors de la gestion du cluster

Lorsque vous gérez un cluster, Astra Control Center installe l'opérateur de surveillance netapp dans le cluster géré. Cet opérateur crée une stratégie de sécurité de pod, A. `ClusterRole` objet, et un `RoleBinding` Objet permettant de déployer des services de télémétrie dans l'espace de noms Astra Control Center.

La nouvelle règle et les objets ont les attributs suivants :

```
kubectl get psp

NAME                             PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo     true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                          CREATED AT
netapp-monitoring-role-privileged             2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                                                ROLE
AGE
netapp-monitoring-role-binding-privileged           Role/netapp-
monitoring-role-privileged             2m5s
```

Informations sur le copyright

Informations sur les marques commerciales