# Concepts

## Astra Control Center

NetApp
August 11, 2025

# Sommaire

# Concepts

## Architecture et composants

Astra Control est une solution de gestion du cycle de vie des données d'application Kubernetes qui simplifie les opérations pour les applications avec état et vous aide à stocker, protéger et déplacer vos charges de travail Kubernetes dans des environnements hybrides.

### Capacités

Astra Control offre des fonctionnalités stratégiques pour la gestion du cycle de vie des données d'application Kubernetes :

**Magasin** :

- Provisionnement de stockage dynamique pour les workloads conteneurisés
- Chiffrement à la volée des données du conteneur vers les volumes persistants
- Réplication entre régions et zones

**Protéger** :

- Détection automatisée et protection respectueuse des applications pour l'ensemble d'une application et de ses données
- Restauration instantanée d'une application à partir de n'importe quelle version de snapshot en fonction des besoins de votre organisation
- Basculement rapide dans les zones, les régions et les fournisseurs de cloud

**Déplacer** :

- Mobilité complète des applications et des données dans et entre les clusters Kubernetes et les clouds
- Des clones instantanés des applications et des données entières
- Migration des applications en un clic via une interface utilisateur Web et une API cohérentes

### Architecture

L'architecture d'Astra Control permet aux équipes IT de proposer des fonctionnalités avancées de gestion des données qui améliorent à la fois les fonctionnalités et la disponibilité des applications Kubernetes, simplifient la gestion, la protection et le déplacement des workloads conteneurisés dans les clouds publics et les environnements sur site. il offre également des fonctionnalités d'automatisation via son API REST et son SDK, qui permettent un accès par programmation pour une intégration transparente avec les workflows déjà en place.

ASTRA Control est natif de Kubernetes, ce qui permet des workflows de protection des données qui utilisent des ressources personnalisées tout en restant rétrocompatible avec l'API et le kit de développement logiciel existants. La protection native des données Kubernetes offre des avantages considérables. En s'intégrant de manière transparente avec les API et les ressources Kubernetes, la protection des données peut devenir inhérente au cycle de vie des applications, via les outils ci/CD et/ou GitOps d'une entreprise.

ASTRA Control est basé sur quatre composants complémentaires :

- **Astra Control** : Astra Control est le service de gestion centralisé pour tous les clusters gérés, fournissant des charges de travail orchestrées pour la protection et la mobilité des applications sur site ainsi que les fonctionnalités suivantes :
  - Vue combinée de plusieurs clusters
  - Protection des workflows orchestrés
  - Visualisation et sélection granulaires des ressources
- **Astra Connector** : Astra Connector s'associe à Astra Control pour fournir une connexion sécurisée à chaque cluster géré, offrant ainsi une exécution locale des opérations planifiées, quel que soit l'état de la connexion, ainsi que les fonctionnalités suivantes :
  - Exécution locale des opérations planifiées quel que soit l'état de la connexion
  - Opérations locales qui distribuent et optimisent l'utilisation des ressources système d'Astra sur les clusters
  - Installation locale qui active un accès avec le moins de privilèges possible au cluster pour une sécurité améliorée
- **Astra Control Provisioner** : Astra Control Provisioner fournit des fonctionnalités de provisionnement CSI de base et des capacités de gestion de stockage avancées pour une configuration de sécurité et de reprise après incident accrue, ainsi que les fonctionnalités suivantes :
  - Provisionnement de stockage dynamique pour les workloads conteneurisés
  - Gestion avancée du stockage :
    - Chiffrement à la volée des données du conteneur vers le volume persistant
    - Fonctionnalité SnapMirror Cloud avec réplication entre régions et zones
- **Astra Ressources personnalisées** : les ressources personnalisées utilisées sur chaque cluster offrent une approche Kubernetes native pour exécuter les opérations localement, simplifier l'intégration avec d'autres outils et l'automatisation compatibles Kubernetes, ainsi que les fonctionnalités suivantes :
  - Intégration directe des outils de l'écosystème et automatisation des workflows
  - Primitives de niveau inférieur permettant d'activer des flux de travail personnalisés

## Modèles de déploiement

Astra Control est disponible dans un modèle de déploiement unique.

**Astra Control Center** : logiciel autogéré qui assure une gestion des données compatible avec les applications de clusters Kubernetes exécutés dans votre environnement sur site. Astra Control Center peut également être installé sur plusieurs environnements de fournisseur cloud avec un système back-end de stockage NetApp Cloud Volumes ONTAP.

"Documentation Astra Control Center"

| | **Centre de contrôle Astra** |
|---|---|
| **Comment est-elle proposée ?** | En tant que logiciel que vous pouvez télécharger, installer et gérer |
| **Où est-il hébergé ?** | Sur votre cluster Kubernetes |
| **Comment est-elle mise à jour ?** | Vous gérez toutes les mises à jour |

| | Centre de contrôle Astra |
|---|---|
| **Quelles sont les distributions Kubernetes prises en charge ?** | • Azure Kubernetes Service sur Azure Stack HCI<br>• Anthos de Google<br>• Kubernetes (en amont)<br>• Rancher Kubernetes Engine (RKE)<br>• Plateforme de conteneurs Red Hat OpenShift |
| **Quels sont les systèmes back-end pris en charge ?** | • Systèmes NetApp ONTAP AFF et FAS<br>• NetApp ONTAP Select<br>• "Cloud Volumes ONTAP"<br>• "Longhorn" |

### Pour en savoir plus

- "Documentation Astra Control Center"
- "Documentation Astra Trident"
- "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.

**Sauvegardes immuables**

Une sauvegarde immuable est une sauvegarde qui ne peut pas être modifiée ou supprimée au cours d'une période spécifiée. Lorsque vous créez une sauvegarde immuable, Astra Control vérifie que le compartiment que vous utilisez est un compartiment WORM (Write Once, Read Many) et, si oui, vérifie que la sauvegarde est immuable depuis Astra Control.
ASTRA Control Center prend en charge la création de sauvegardes immuables avec les plateformes et les types de compartiments suivants :

- Amazon Web Services utilisant un compartiment Amazon S3 avec le verrouillage objet S3 configuré
- NetApp StorageGRID utilisant un compartiment S3 avec verrouillage objet S3 configuré

Notez les points suivants lorsque vous travaillez avec des sauvegardes immuables :

- Si vous effectuez une sauvegarde vers un compartiment WORM sur une plateforme non prise en charge ou vers un type de compartiment non pris en charge, vous risquez d'obtenir des résultats imprévisibles, comme la suppression de la sauvegarde, même si le temps de conservation est écoulé.
- ASTRA Control ne prend pas en charge les politiques de gestion du cycle de vie des données ni la suppression manuelle d'objets dans les compartiments que vous utilisez avec des sauvegardes immuables. Assurez-vous que votre système back-end de stockage n'est pas configuré pour gérer le cycle de vie des snapshots Astra Control ou des données sauvegardées.

## 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 entre les systèmes back-end

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

Vous pouvez répliquer des données entre deux SVM ONTAP sur le même cluster ONTAP ou sur différents clusters ONTAP.

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

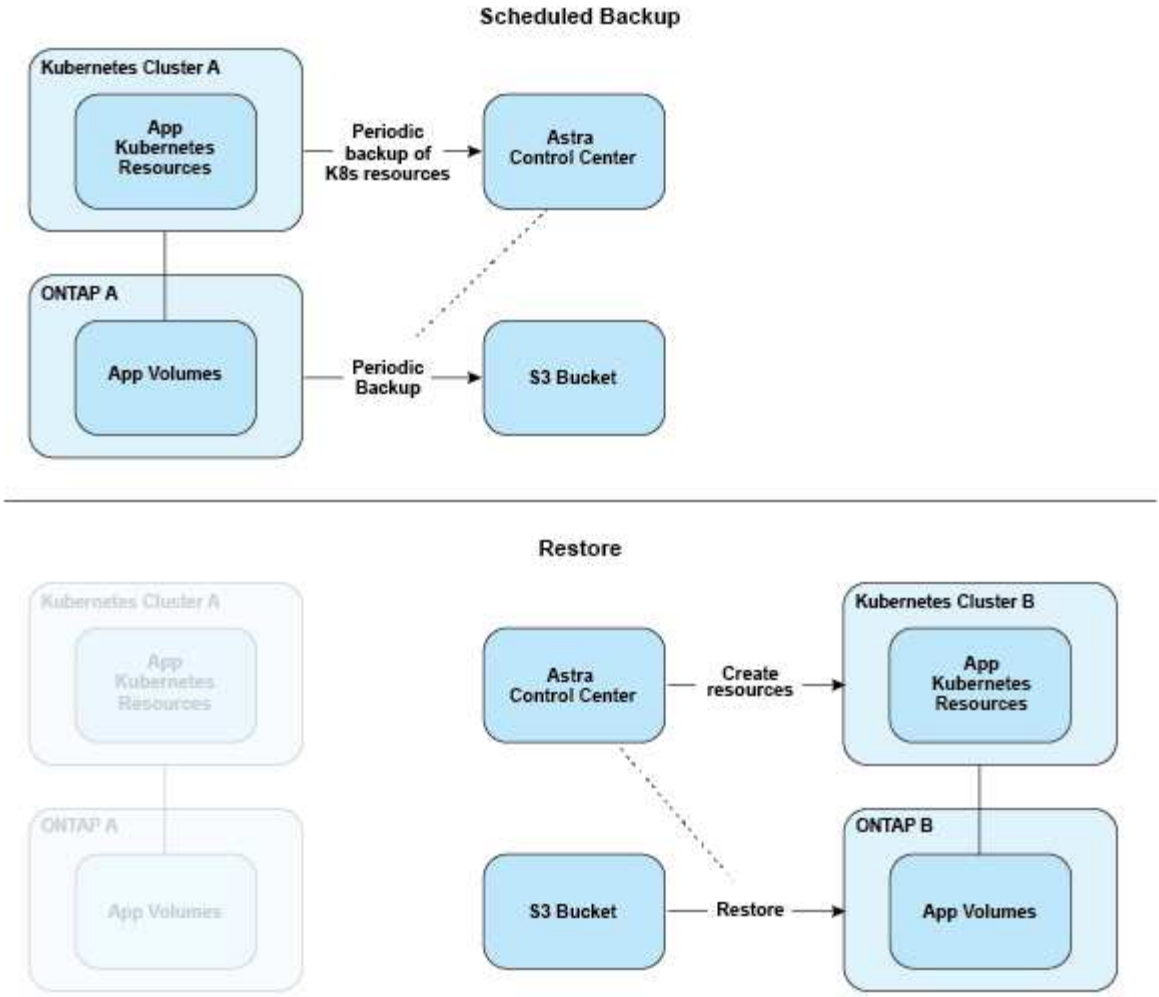
La réplication d'application est différente de la sauvegarde et de la restauration de l'application de la manière suivante :

- **Réplication d'applications** : Astra Control requiert que les clusters Kubernetes source et de destination (qui peuvent être le même cluster) soient disponibles et gérés avec leurs systèmes back-end de stockage ONTAP respectifs configurés pour activer NetApp SnapMirror. ASTRA Control utilise le Snapshot d'application piloté par des règles et le réplique vers le système de stockage back-end de destination. 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 des applications** : lors de la sauvegarde des applications, Astra Control crée un snapshot des données d'application et les 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.

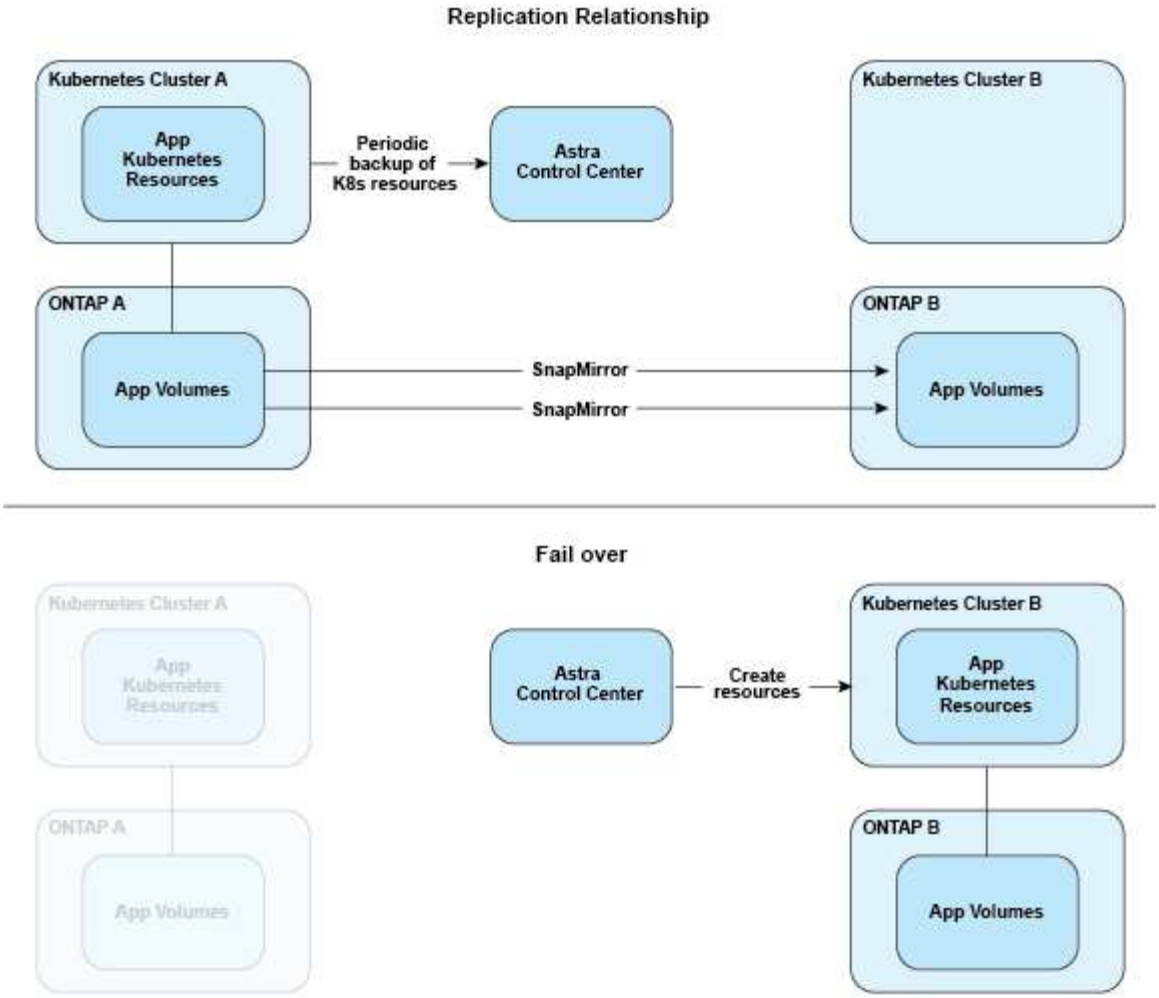
Pour savoir comment répliquer des applications, reportez-vous à la section "Répliquez vos applications sur un système distant grâce à la technologie SnapMirror".

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

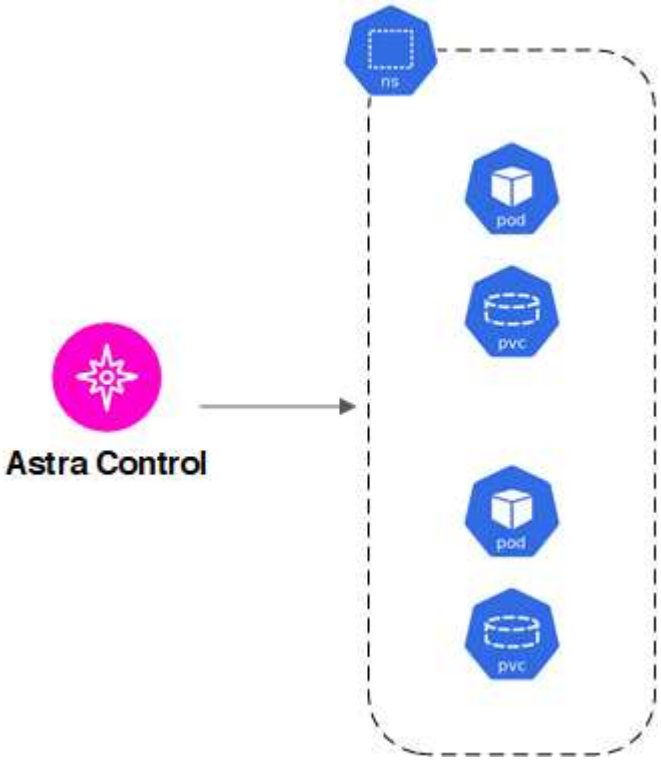
- "Ajoutez une licence lorsque vous configurez Astra Control Center pour la première fois"
- "Mettre à jour une licence existante"

# Gestion des applications

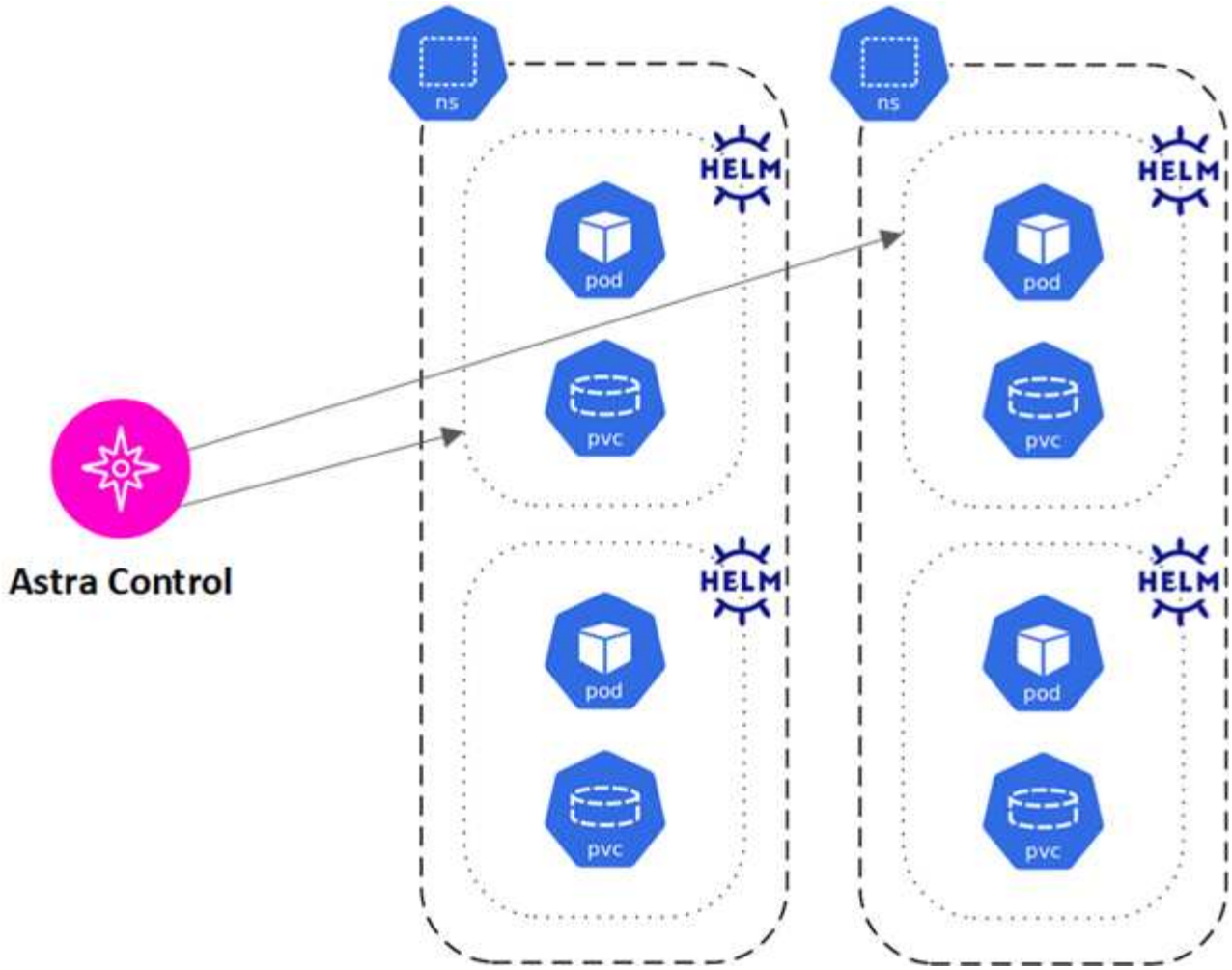
Lorsque Astra Control détecte vos clusters, les applications de ces clusters ne sont pas

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

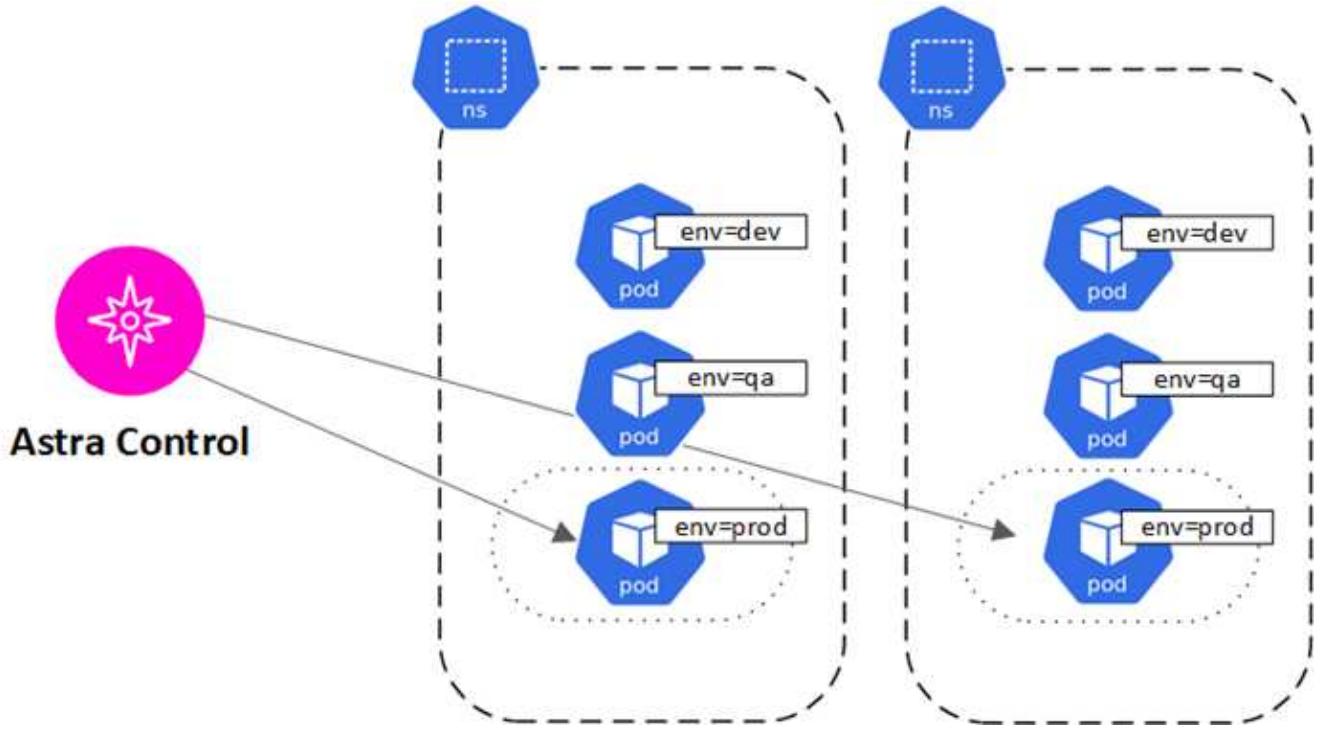
- Un espace de nom, y compris toutes les ressources de cet espace de nom




- 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 NetApp ONTAP et Longhorn en tant que systèmes back-end de stockage.

## Présentation

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

- **Classes de stockage soutenues par le stockage ONTAP** : si vous utilisez un back-end ONTAP, Astra Control Center offre la possibilité d'importer le back-end ONTAP pour générer des rapports d'informations de surveillance.
- **Classes de stockage CSI soutenues par Longhorn** : vous pouvez utiliser Longhorn avec le pilote Longhorn Container Storage interface (CSI).

Les classes de stockage doivent être "configuré" À l'aide d'Astra Control Provisioner.

## 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.

# 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"