Conceptos

Astra Control Center

NetApp
August 11, 2025

Tabla de contenidos

Conceptos

Arquitectura y componentes

Astra Control es una solución de gestión del ciclo de vida de los datos de aplicaciones Kubernetes que simplifica las operaciones de las aplicaciones con estado y lo ayuda a almacenar, proteger y mover sus cargas de trabajo de Kubernetes en entornos híbridos.

Funcionalidades

Astra Control ofrece funcionalidades cruciales para la gestión del ciclo de vida de los datos de las aplicaciones Kubernetes:

Tienda:

- Aprovisionamiento de almacenamiento dinámico para cargas de trabajo en contenedores
- Cifrado de datos en tránsito desde contenedores a volúmenes persistentes
- Replicación entre regiones y zonas

Proteger:

- Detección automatizada y protección compatible con las aplicaciones de toda una aplicación y sus datos
- Recuperación instantánea de una aplicación desde cualquier versión de snapshot según las necesidades de su organización
- Rápida recuperación tras fallos entre zonas, regiones y proveedores de cloud

Mover:

- Completa movilidad de aplicaciones y datos en y entre clústeres y clouds de Kubernetes
- Clones instantáneos de aplicaciones y datos completos
- Migración de aplicaciones con un solo clic a través de una API e IU web consistentes

Arquitectura

La arquitectura de Astra Control permite que los departamentos de tecnología proporcionen funcionalidades de gestión de datos avanzadas que mejoran tanto la funcionalidad como la disponibilidad de las aplicaciones de Kubernetes, simplifica la gestión, la protección y el movimiento de cargas de trabajo en contenedores entre clouds públicos y entornos en las instalaciones. y proporciona funcionalidades de automatización a través de su API de REST y SDK, lo que permite un acceso mediante programación para una integración perfecta con los flujos de trabajo existentes.

Astra Control es nativo de Kubernetes, lo que permite flujos de trabajo de protección de datos que utilizan recursos personalizados y siguen siendo compatibles con las API y el SDK existentes. La protección de datos nativa de Kubernetes ofrece importantes ventajas; al integrarse sin problemas con las API y los recursos de Kubernetes, la protección de datos puede convertirse en una parte inherente del ciclo de vida de la aplicación mediante las herramientas GitOps o CI/CD existentes de una organización.

Astra Control se basa en cuatro componentes complementarios:

- **Astra Control**: Astra Control es el servicio de administración centralizada para todos los clústeres administrados, que proporciona cargas de trabajo orquestadas para la protección y movilidad de aplicaciones locales, así como las siguientes capacidades:
  - Vista combinada de múltiples clústeres
  - Protección de flujos de trabajo orquestados
  - Visualización y selección granular de recursos
- **Astra Connector**: Astra Connector cuenta con Astra Control para proporcionar una conexión segura a cada clúster gestionado, ofreciendo la ejecución local de las operaciones programadas independientemente del estado de conexión, así como las siguientes capacidades:
  - Ejecución local de operaciones programadas independientemente del estado de conexión
  - Operaciones locales que distribuyen y optimizan el uso de los recursos del sistema de Astra en todos los clústeres
  - Instalación local que permite el acceso con menos privilegios al clúster para mejorar la seguridad
- **Astra Control Provisionador**: Astra Control Provisionador ofrece funcionalidad de aprovisionamiento CSI central y capacidades avanzadas de administración de almacenamiento para una mayor configuración de seguridad y recuperación ante desastres, así como las siguientes capacidades:
  - Aprovisionamiento de almacenamiento dinámico para cargas de trabajo en contenedores
  - Gestión de almacenamiento avanzada:
    - Cifrado en tránsito de datos desde contenedor a VP
    - Funcionalidad de SnapMirror Cloud con replicación entre zonas y regiones
- **Recursos personalizados de Astra**: Los recursos personalizados utilizados en cada clúster proporcionan un enfoque nativo de Kubernetes para ejecutar las operaciones localmente, simplificando la integración con otras herramientas y automatización compatibles con Kubernetes, además de proporcionar las siguientes capacidades:
  - Integración directa de herramientas del ecosistema y flujos de trabajo de automatización
  - Primitivos de nivel inferior que permiten flujos de trabajo personalizados

Modelos de puesta en marcha

Astra Control está disponible en un único modelo de implementación.

Astra Control Center: Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local. Astra Control Center también se puede instalar en entornos de varios proveedores de cloud con un entorno de administración del almacenamiento Cloud Volumes ONTAP de NetApp.

"Documentación de Astra Control Center"

	Astra Control Center
¿Cómo se ofrece?	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Usted administra cualquier actualización

	Astra Control Center
¿Cuáles son las distribuciones de Kubernetes compatibles?	• Azure Kubernetes Service en HCI de pila de Azure • Anthos de Google • Kubernetes (ascendente) • Motor Kubernetes de rancher (RKE) • OpenShift Container Platform de Red Hat
¿Cuáles son los back-ends de almacenamiento compatibles?	• Sistemas ONTAP AFF y FAS de NetApp • ONTAP Select de NetApp • "Cloud Volumes ONTAP" • "El Longhorn"

Si quiere más información

- "Documentación de Astra Control Center"
- "Documentación de Astra Trident"
- "API de control Astra"
- "Documentación de Cloud Insights"
- "Documentación de ONTAP"

Protección de datos

Conozca los tipos disponibles de protección de datos en Astra Control Center y cómo usarlos de la mejor forma para proteger sus aplicaciones.

Snapshot, backups y políticas de protección

Tanto Snapshot como los backups protegen los siguientes tipos de datos:

- La propia aplicación
- Todos los volúmenes de datos persistentes asociados con la aplicación
- Cualquier objeto de recurso que pertenezca a la aplicación

Un *snapshot* es una copia puntual de una aplicación que se almacena en el mismo volumen aprovisionado que la aplicación. Por lo general son rápidas. Es posible usar snapshots locales para restaurar la aplicación a un momento específico anterior. Las copias Snapshot son útiles para los clones rápidos; las copias Snapshot incluyen todos los objetos de Kubernetes para la aplicación, incluidos los archivos de configuración. Las copias Snapshot son útiles para clonar o restaurar una aplicación dentro del mismo clúster.

Un *backup* se basa en una instantánea. Se almacena en el almacén de objetos externo y, debido a esto, puede tardar más en hacerse en comparación con las copias Snapshot locales. Puede restaurar una copia de seguridad de aplicaciones en el mismo clúster, o puede migrar una aplicación restaurando su copia de seguridad en un clúster diferente. También es posible elegir un período de retención más largo para backups. Debido a que están almacenados en el almacén de objetos externo, los backups generalmente ofrecen mejor protección que las copias Snapshot en caso de fallo del servidor o pérdida de datos.

Una *política de protección* es una forma de proteger una aplicación mediante la creación automática de instantáneas, copias de seguridad o ambas de acuerdo con un programa definido para esa aplicación. Una política de protección también permite elegir cuántas Snapshot y backups se retendrán en la programación, y establecer diferentes niveles de granularidad de programación. Automatizar los backups y las copias Snapshot con una política de protección es la mejor forma de garantizar que cada aplicación esté protegida en función de las necesidades de la organización y los requisitos del acuerdo de nivel de servicio.

no puede estar completamente protegido hasta que tenga una copia de seguridad reciente. Esto es importante porque los backups se almacenan en un almacén de objetos lejos de los volúmenes persistentes. Si un fallo o accidente limpia el cluster y su almacenamiento persistente asociado, necesitará una copia de seguridad para recuperar. Una Snapshot no le permite recuperar.

Backups inmutables

Un backup inmutable es un backup que no se puede cambiar ni eliminar durante un periodo determinado. Cuando creas un backup inmutable, Astra Control realiza una comprobación para garantizar que el bloque que utilizas sea un bloque de escritura única y lectura múltiple (WORM), y, si es así, garantiza que el backup sea inmutable desde Astra Control.
Astra Control Center admite la creación de backups inmutables con las siguientes plataformas y tipos de bloques:

- Amazon Web Services con un bucket de Amazon S3 con S3 Object Lock configurado
- NetApp StorageGRID con un bloque de S3 con bloqueo de objetos de S3 GB configurado

Tenga en cuenta lo siguiente cuando trabaje con copias de seguridad inmutables:

- Si realiza la copia de SEGURIDAD en un bloque WORM en una plataforma no compatible o en un tipo de bloque no compatible, puede obtener resultados impredecibles, como un error en la eliminación de backups, incluso si ha transcurrido el tiempo de retención.
- Astra Control no admite políticas de gestión del ciclo de vida de los datos ni la eliminación manual de objetos en los bloques que utilizas con backups inmutables. Asegúrate de que el back-end de almacenamiento no esté configurado para gestionar el ciclo de vida de las copias Snapshot de Astra Control o de los datos que se han realizado backups.

Clones

Un *clone* es un duplicado exacto de una aplicación, su configuración y sus volúmenes de datos persistentes. Es posible crear manualmente un clon en el mismo clúster de Kubernetes o en otro clúster. El clonado de una aplicación puede ser útil si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro.

Replicación entre back-ends de almacenamiento

Con Astra Control, puede aumentar la continuidad del negocio para sus aplicaciones con un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación bajo (Recovery Time Objective) mediante funcionalidades de replicación asíncrona de la tecnología SnapMirror de NetApp. Una vez configurado, esto permite a sus aplicaciones replicar los cambios de aplicaciones y datos de un back-end de almacenamiento a otro, en el mismo clúster o entre diferentes clústeres.

Puede replicar entre dos SVM de ONTAP en el mismo clúster de ONTAP o en otros clústeres de ONTAP.

Astra Control replica de forma asíncrona las copias snapshot de las aplicaciones en un clúster de destino. El proceso de replicación incluye datos en los volúmenes persistentes replicados por SnapMirror y los metadatos

de aplicaciones protegidos por Astra Control.

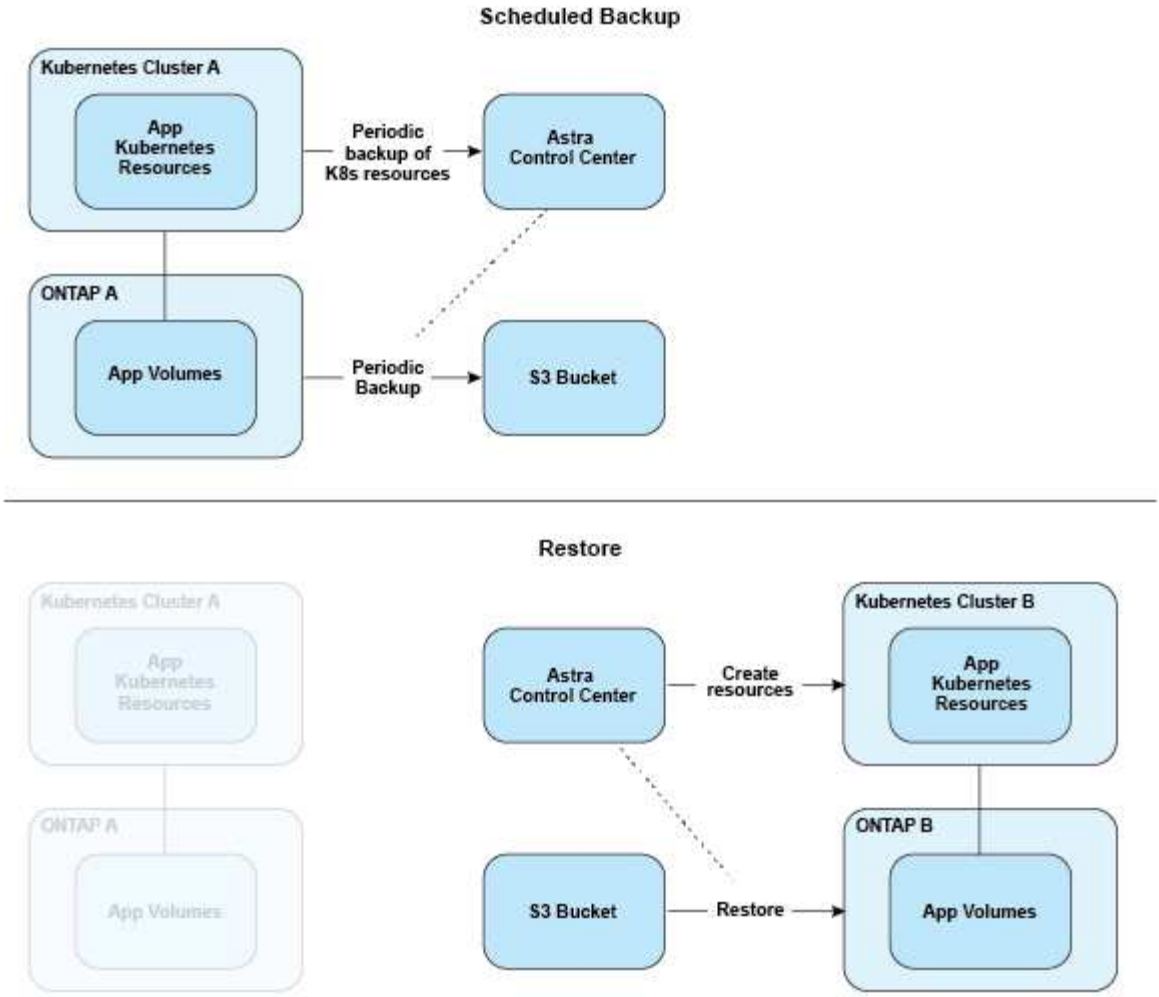
La replicación de aplicaciones es diferente de la copia de seguridad y la restauración de aplicaciones de las siguientes formas:

- **Replicación de aplicaciones**: Astra Control requiere que los clústeres de Kubernetes de origen y destino (que pueden ser el mismo clúster) estén disponibles y gestionados con sus respectivos back-ends de almacenamiento de ONTAP configurados para habilitar SnapMirror de NetApp. Astra Control toma la snapshot de la aplicación condicionada por políticas y la replica en el back-end del almacenamiento de destino. La tecnología SnapMirror de NetApp se utiliza para replicar los datos de volumen persistentes. Para conmutar al nodo de respaldo, Astra Control puede poner en línea la aplicación replicada al volver a crear los objetos de aplicación en el clúster de Kubernetes de destino con los volúmenes replicados en el clúster de ONTAP de destino. Dado que los datos de volúmenes persistentes ya están presentes en el clúster de ONTAP de destino, Astra Control puede ofrecer tiempos de recuperación rápidos para la conmutación al respaldo.
- **Copia de seguridad y restauración de aplicaciones**: Al realizar copias de seguridad de aplicaciones, Astra Control crea una instantánea de los datos de la aplicación y los almacena en un depósito de almacenamiento de objetos. Cuando se necesita una restauración, los datos del bloque deben copiarse a un volumen persistente del clúster de ONTAP. La operación de backup/restauración no requiere que el clúster de Kubernetes/ONTAP secundario esté disponible y gestionado, pero la copia de datos adicional puede provocar tiempos de restauración más prolongados.

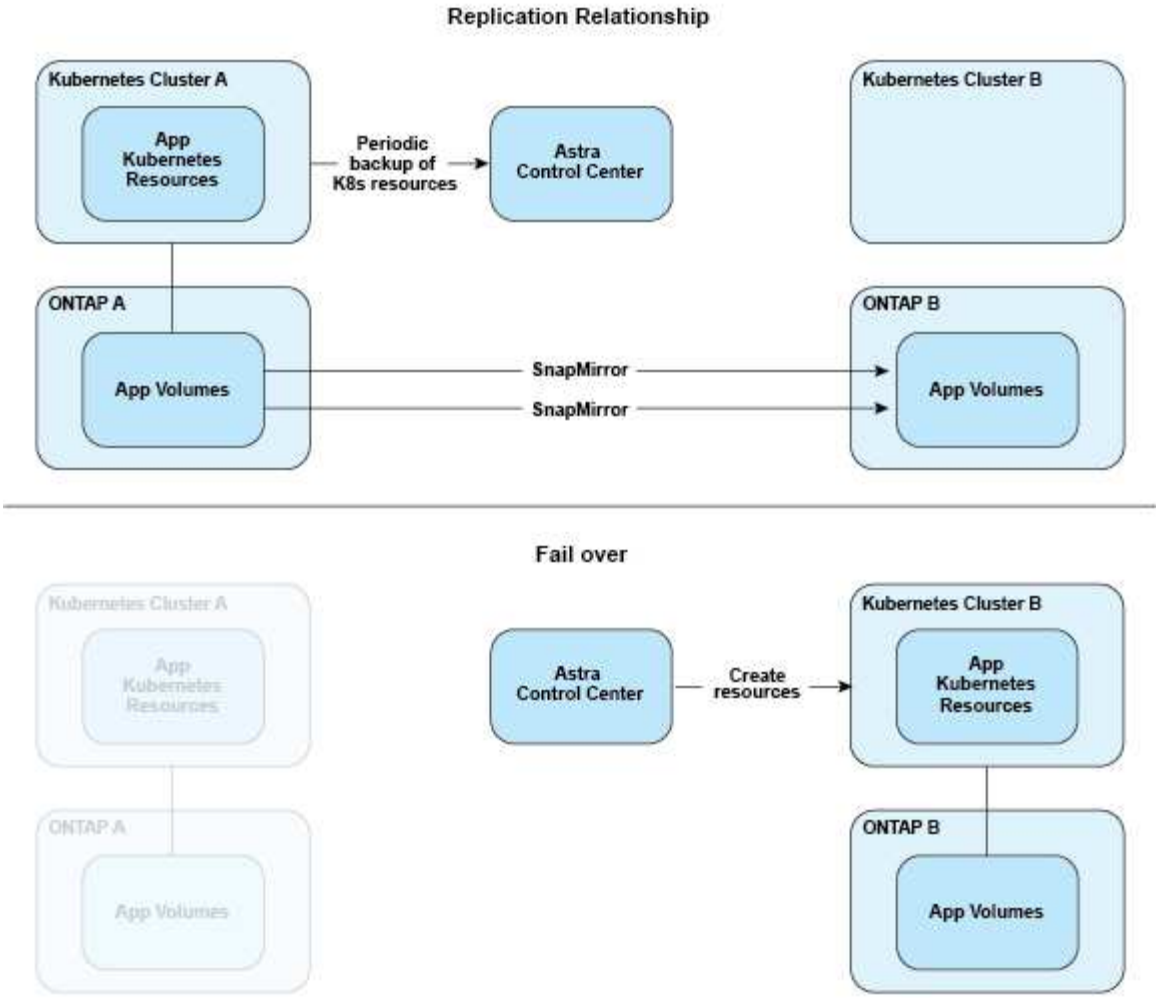
Para obtener más información sobre cómo replicar aplicaciones, consulte "Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror".

Las siguientes imágenes muestran el proceso de backup y restauración programado en comparación con el proceso de replicación.

El proceso de backup copia los datos en bloques de S3 y restaura a partir de bloques S3:



Por otro lado, la replicación se realiza replicando en ONTAP y, a continuación, una conmutación al respaldo crea los recursos de Kubernetes:



Backups, snapshots y clones con una licencia caducada

Si caduca la licencia, solo puede añadir una nueva aplicación o realizar operaciones de protección de la aplicación (como snapshots, backups, clones y operaciones de restauración) si la aplicación que está añadiendo o protegiendo es otra instancia de Astra Control Center.

Licencia

Al implementar Astra Control Center, se instala con una licencia de evaluación integrada de 90 días para 4.800 unidades CPU. Si necesita más capacidad o un período de evaluación más largo, o si desea actualizar a una licencia completa, puede obtener una licencia de evaluación diferente o una licencia completa de NetApp.

Usted obtiene una licencia de una de las siguientes maneras:

- Si va a evaluar Astra Control Center y necesita términos de evaluación distintos a los incluidos en la licencia de evaluación integrada, póngase en contacto con NetApp para solicitar un archivo de licencia de evaluación diferente.
- "Si ya ha adquirido Astra Control Center, genere su archivo de licencia de NetApp (NLF)" Al iniciar sesión en el sitio de soporte de NetApp y navegar a sus licencias de software en el menú Sistemas.

Para obtener más información sobre las licencias necesarias para los back-ends de almacenamiento de ONTAP, consulte "compatibles con los back-ends de almacenamiento".

> Asegúrese de que su licencia habilita al menos tantas unidades de CPU como necesite. Si el número de unidades de CPU que gestiona actualmente Astra Control Center supera las unidades de CPU disponibles en la nueva licencia que se está aplicando, no podrá aplicar la nueva licencia.

Licencias de evaluación y licencias completas

Se proporciona una licencia de evaluación integrada con una nueva instalación de Astra Control Center. Una licencia de evaluación habilita las mismas capacidades y funciones que una licencia completa durante un periodo limitado (90 días). Después del período de evaluación, se requiere una licencia completa para continuar con todas las funciones.

Caducidad de la licencia

Si la licencia de Astra Control Center activa caduca, la funcionalidad de interfaz de usuario y API de las siguientes funciones no están disponibles:

- Snapshots y backups locales manuales
- Snapshot y backups locales programados
- Restauración a partir de una copia de Snapshot o un backup
- Clonado desde una copia de Snapshot o estado actual
- Gestionar nuevas aplicaciones
- Configurar políticas de replicación

Cómo se calcula el consumo de licencias

Al añadir un nuevo clúster a Astra Control Center, no cuenta con licencias consumidas hasta que Astra Control Center gestione al menos una aplicación que se ejecute en el clúster.

Cuando comienza a administrar una aplicación en un clúster, todas las unidades de CPU de ese clúster se incluyen en el consumo de licencias de Astra Control Center, excepto las unidades de CPU de nodo de clúster Red Hat OpenShift que se notifican mediante un mediante la etiqueta `node-role.kubernetes.io/infra: ""`.

> Los nodos de infraestructura de Red Hat OpenShift no consumen licencias en Astra Control Center. Para marcar un nodo como un nodo de infraestructura, aplique la etiqueta `node-role.kubernetes.io/infra: ""` al nodo.

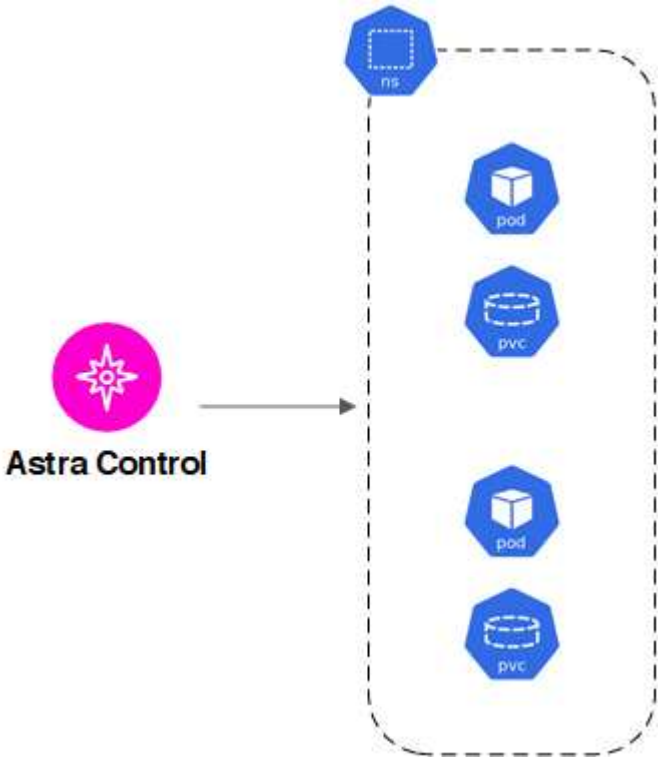
Obtenga más información

- "Agregue una licencia cuando configure por primera vez Astra Control Center"
- "Actualizar una licencia existente"

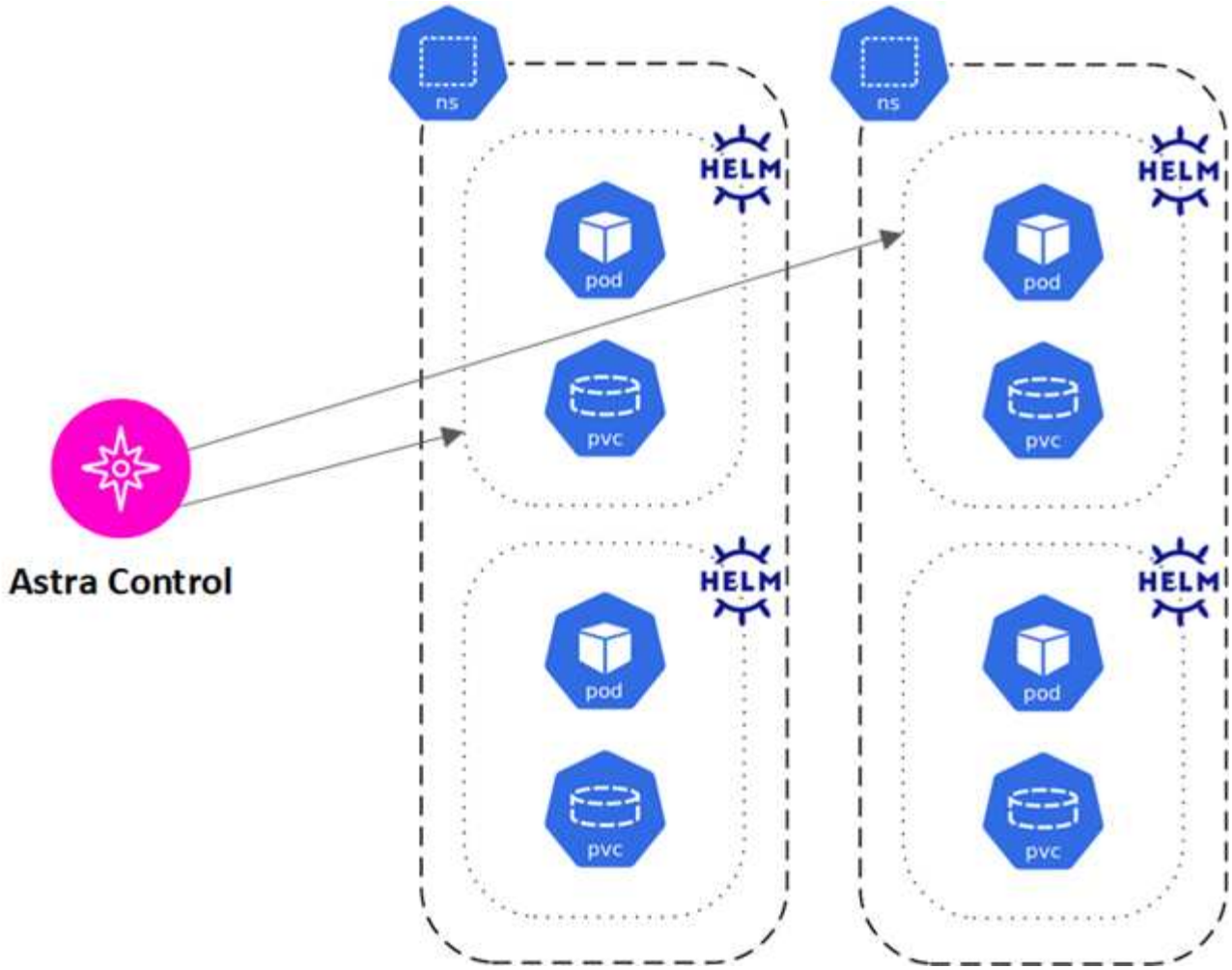
Gestión de aplicaciones

Cuando Astra Control detecta sus clústeres, las aplicaciones de esos clústeres no se gestionan hasta que elija cómo desea gestionarlas. Una aplicación administrada de Astra Control puede ser cualquiera de las siguientes:

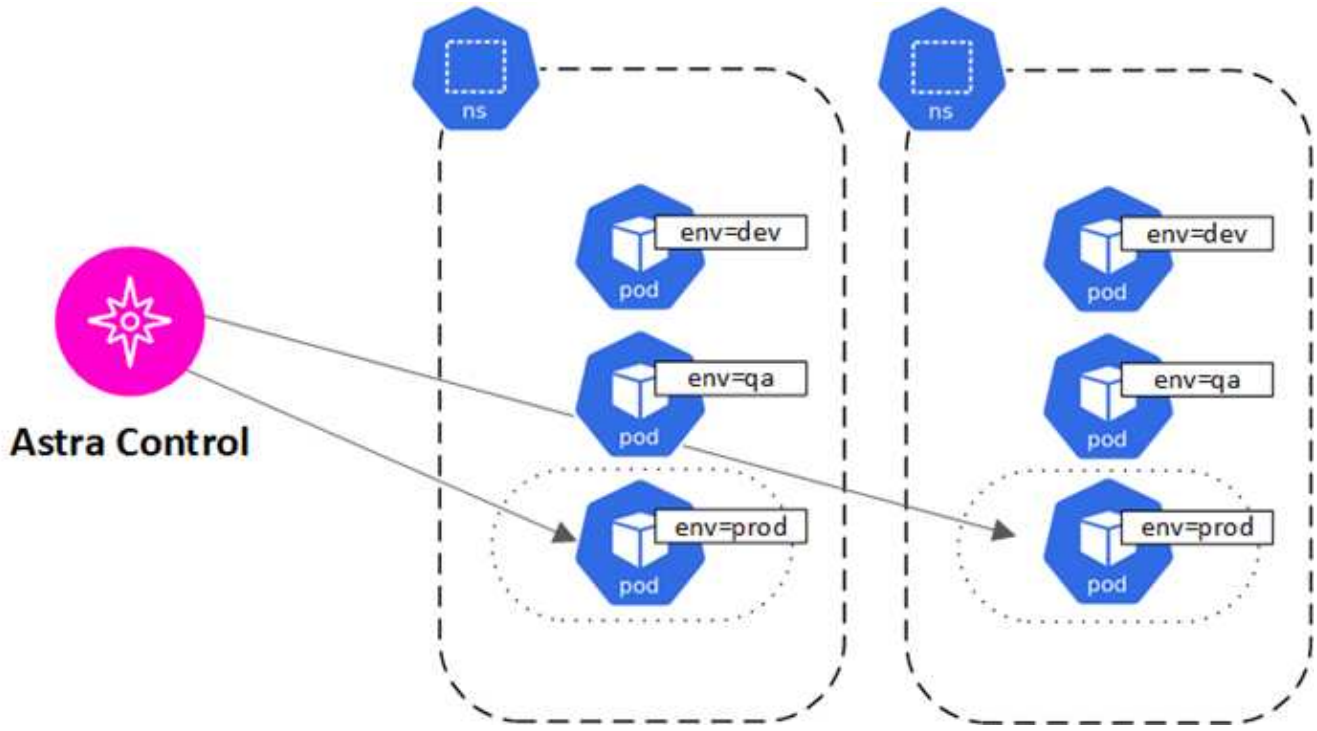
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- Una aplicación individual desplegada en uno o más espacios de nombres (se utiliza helm3 en este ejemplo)



- Un grupo de recursos que se identifica con una etiqueta de Kubernetes dentro de uno o varios espacios de nombres



Clases de almacenamiento y tamaño de volumen persistente

Astra Control Center admite NetApp ONTAP y Longhorn como back-ends de almacenamiento.

Descripción general

Astra Control Center admite lo siguiente:

- **Clases de almacenamiento respaldadas por el almacenamiento de ONTAP**: Si estás usando un backend de ONTAP, el Centro de control de Astra ofrece la capacidad de importar el backend de ONTAP para informar de la información de monitoreo.
- **Clases de almacenamiento basadas en CSI respaldadas por Longhorn**: Puedes usar Longhorn con el controlador Longhorn Container Storage Interface (CSI).

Las clases de almacenamiento deberían ser "configurado" Con el aprovisionador de Astra Control.

Clases de almacenamiento

Cuando agregue un clúster a Astra Control Center, se le pedirá que seleccione una clase de almacenamiento previamente configurada en ese clúster como la clase de almacenamiento predeterminada. Este tipo de almacenamiento se usará cuando no se especifique ningún tipo de almacenamiento en una reclamación de volumen persistente (RVP). La clase de almacenamiento predeterminada se puede cambiar en cualquier momento dentro de Astra Control Center y cualquier clase de almacenamiento se puede usar en cualquier momento especificando el nombre de la clase de almacenamiento dentro del gráfico PVC o Helm. Compruebe que solo tiene una única clase de almacenamiento predeterminada definida para el clúster de Kubernetes.

Roles de usuario y espacios de nombres

Obtenga información acerca de las funciones de usuario y los espacios de nombres en Astra Control y cómo puede utilizarlas para controlar el acceso a los recursos de la organización.

Roles de usuario

Puede utilizar las funciones para controlar el acceso de los usuarios a los recursos o capacidades de Astra Control. Las siguientes son las funciones de usuario de Astra Control:

- Un **Visor** puede ver los recursos.
- Un **Miembro** tiene permisos de función de Viewer y puede administrar aplicaciones y clústeres, anular la administración de aplicaciones y eliminar instantáneas y copias de seguridad.
- Un **Admin** tiene permisos de rol de miembro y puede agregar y quitar cualquier otro usuario excepto el propietario.
- **Owner** tiene permisos de función de administrador y puede agregar y eliminar cualquier cuenta de usuario.

Puede agregar restricciones a un usuario Miembro o Visor para restringir el usuario a uno o más Espacios de

nombres.

Espacios de nombres

Un espacio de nombres es un ámbito que puede asignar a recursos específicos de un clúster gestionado por Astra Control. Astra Control detecta los espacios de nombres de un clúster cuando agrega el clúster a Astra Control. Una vez detectados, los espacios de nombres están disponibles para asignarlos como restricciones a los usuarios. Sólo los miembros que tienen acceso a ese espacio de nombres pueden usar ese recurso. Puede utilizar espacios de nombres para controlar el acceso a los recursos mediante un paradigma que tenga sentido para la organización; por ejemplo, por regiones físicas o divisiones dentro de una empresa. Cuando agrega restricciones a un usuario, puede configurarlo para que tenga acceso a todos los espacios de nombres o sólo a un conjunto específico de espacios de nombres. También es posible asignar restricciones de espacio de nombres usando etiquetas de espacio de nombres.

Obtenga más información

"Gestione usuarios locales y roles"