Conceptos

Astra Control Center

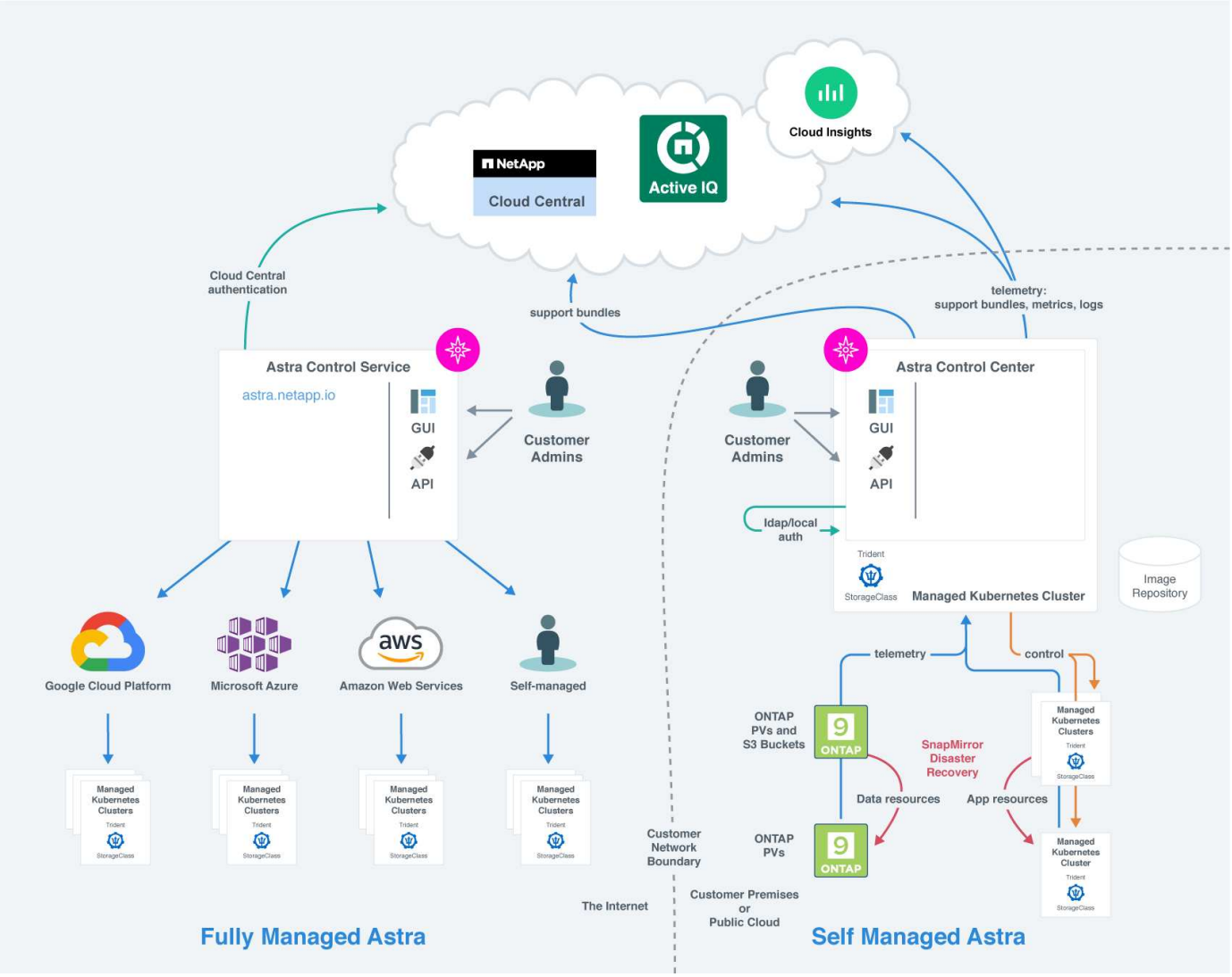
NetApp
November 21, 2023

Tabla de contenidos

Conceptos

Arquitectura y componentes

A continuación se ofrece una descripción general de los distintos componentes del entorno de Astra Control.



Componentes de Astra Control

- **Clústeres de Kubernetes**: Kubernetes es una plataforma portátil, extensible y de código abierto para gestionar cargas de trabajo y servicios en contenedores, que facilita la configuración y la automatización declarativas. Astra proporciona servicios de gestión para aplicaciones alojadas en un clúster de Kubernetes.
- **Astra Trident**: Como orquestador y gestor de aprovisionamiento de código abierto totalmente compatible y mantenido por NetApp, Astra Trident le permite crear volúmenes de almacenamiento para aplicaciones en contenedores gestionadas por Docker y Kubernetes. Cuando se pone en marcha con Astra Control Center, Astra Trident incluye un back-end de almacenamiento configurado para ONTAP.
- **Sistema de almacenamiento**:

    - Astra Control Service utiliza los siguientes back-ends de almacenamiento:
        - "Cloud Volumes Service de NetApp para Google Cloud" O Google Persistent Disk como back-end de almacenamiento para clústeres GKE
        - "Azure NetApp Files" O discos gestionados de Azure como back-end de almacenamiento para clústeres de AKS.
        - "Elastic Block Store (EBS) de Amazon" o. "Amazon FSX para ONTAP de NetApp" Como opciones de almacenamiento de back-end para clústeres EKS.
    - Astra Control Center utiliza los siguientes back-ends de almacenamiento:
        - ONTAP AFF, FAS y ASA. Como plataforma de hardware y software de almacenamiento, ONTAP proporciona servicios de almacenamiento básicos, compatibilidad con varios protocolos de acceso a almacenamiento y funcionalidad de gestión del almacenamiento, como copias Snapshot y mirroring.
        - Cloud Volumes ONTAP
- **Cloud Insights**: Una herramienta de supervisión de infraestructura de nube de NetApp, Cloud Insights te permite supervisar el rendimiento y la utilización de tus clústeres de Kubernetes gestionados por el Centro de control de Astra. Cloud Insights relaciona el uso del almacenamiento con las cargas de trabajo. Cuando activa la conexión Cloud Insights en Astra Control Center, la información de telemetría se muestra en las páginas de interfaz de usuario de Astra Control Center.

Interfaces Astra Control

Puede completar tareas utilizando diferentes interfaces:

- **Interfaz de usuario web (UI)**: Tanto Astra Control Service como Astra Control Center utilizan la misma interfaz de usuario basada en web en la que puede gestionar, migrar y proteger aplicaciones. Use también la interfaz de usuario para gestionar las cuentas de usuario y las opciones de configuración.
- **API**: Tanto el Servicio de control Astra como el Centro de control Astra utilizan la misma API de control Astra. Con la API, puede realizar las mismas tareas que utilizaría la interfaz de usuario.

Astra Control Center también le permite gestionar, migrar y proteger los clústeres de Kubernetes que se ejecutan en entornos de VM.

Si quiere más información

- "Documentación de Astra Control Service"
- "Documentación de Astra Control Center"
- "Documentación de Astra Trident"
- "Utilice la API Astra Control"
- "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.

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.

La replicación en un clúster remoto

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 que se ha configurado, esto permite a sus aplicaciones replicar los cambios de aplicaciones y datos de un clúster a otro.

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

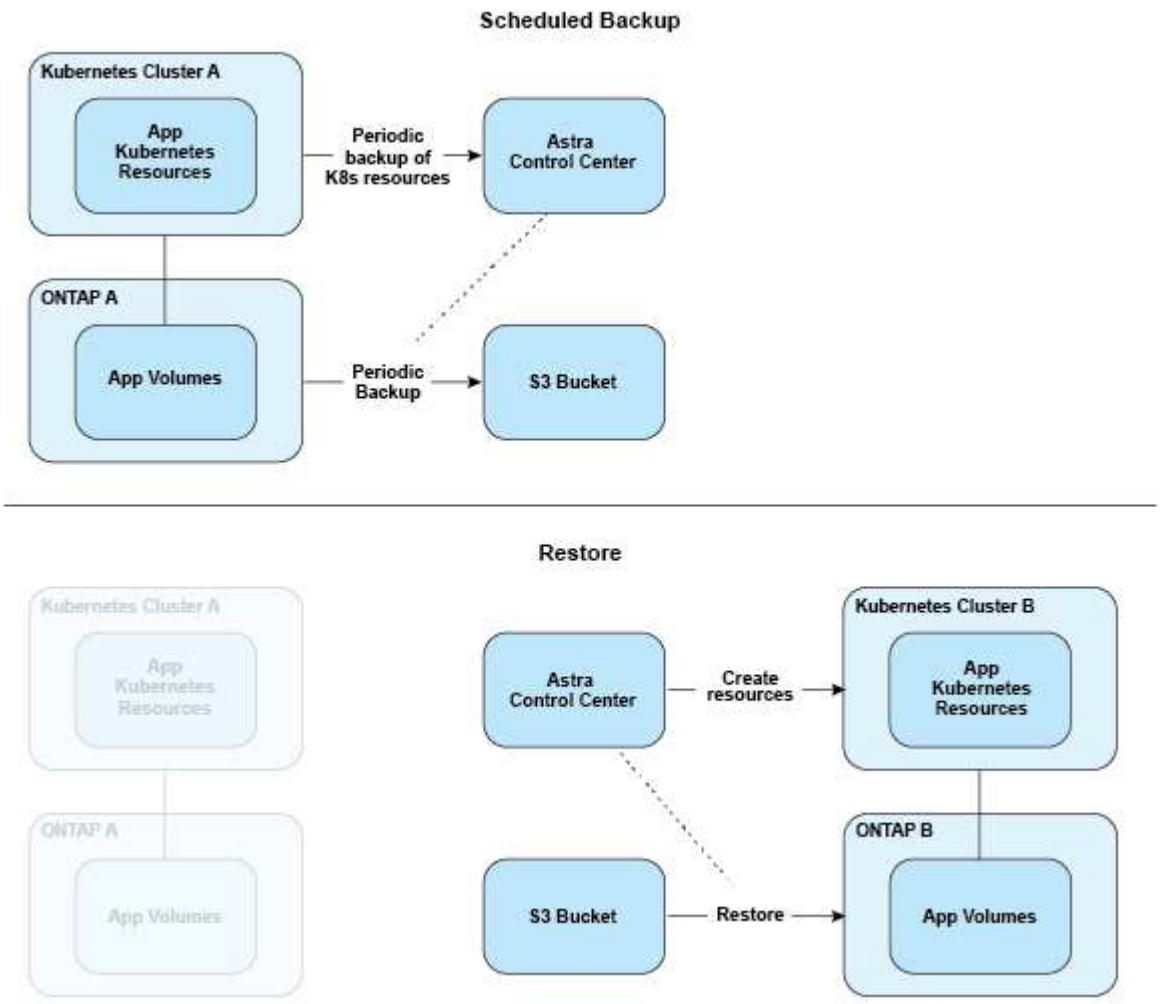
La replicación de aplicaciones es diferente de la copia de seguridad y la restauración de aplicaciones de las siguientes formas:

- **Replicación de aplicaciones**: Astra Control requiere que los clústeres de Kubernetes de origen y destino estén disponibles y gestionados con sus respectivos back-ends de almacenamiento de ONTAP configurados para habilitar SnapMirror de NetApp. Astra Control toma la copia Snapshot de la aplicación basada en políticas y la replica en el clúster remoto. 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 hacer copias de seguridad de aplicaciones, Astra Control crea una instantánea de los datos de la aplicación y los almacena en un bloque 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.

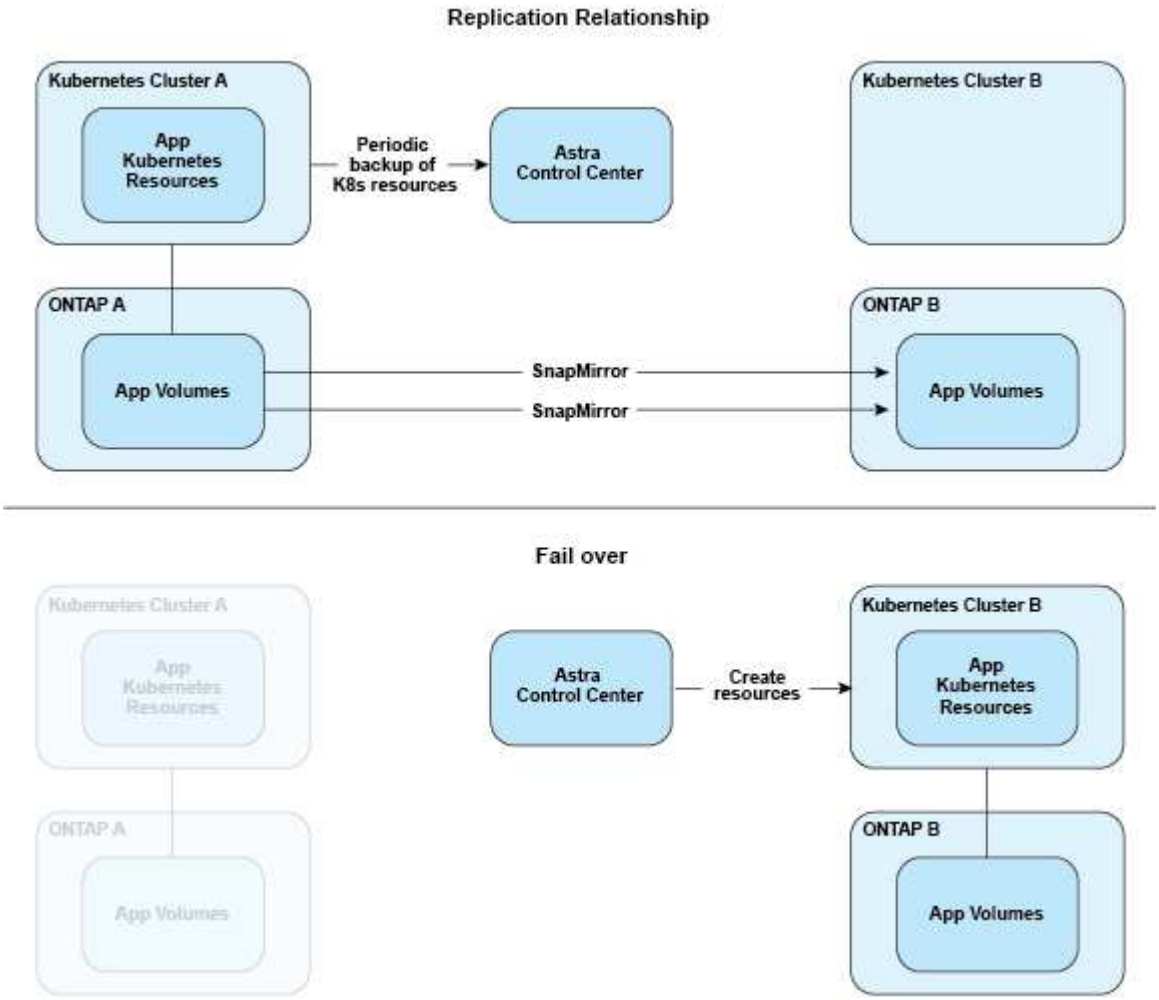
Para obtener más información sobre cómo replicar aplicaciones, consulte "Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror".

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 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.

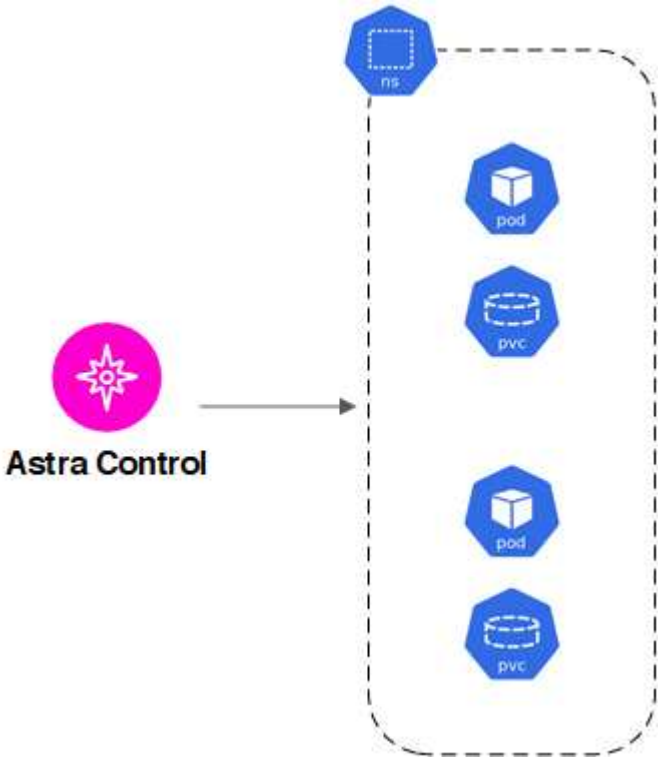
Obtenga más información

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

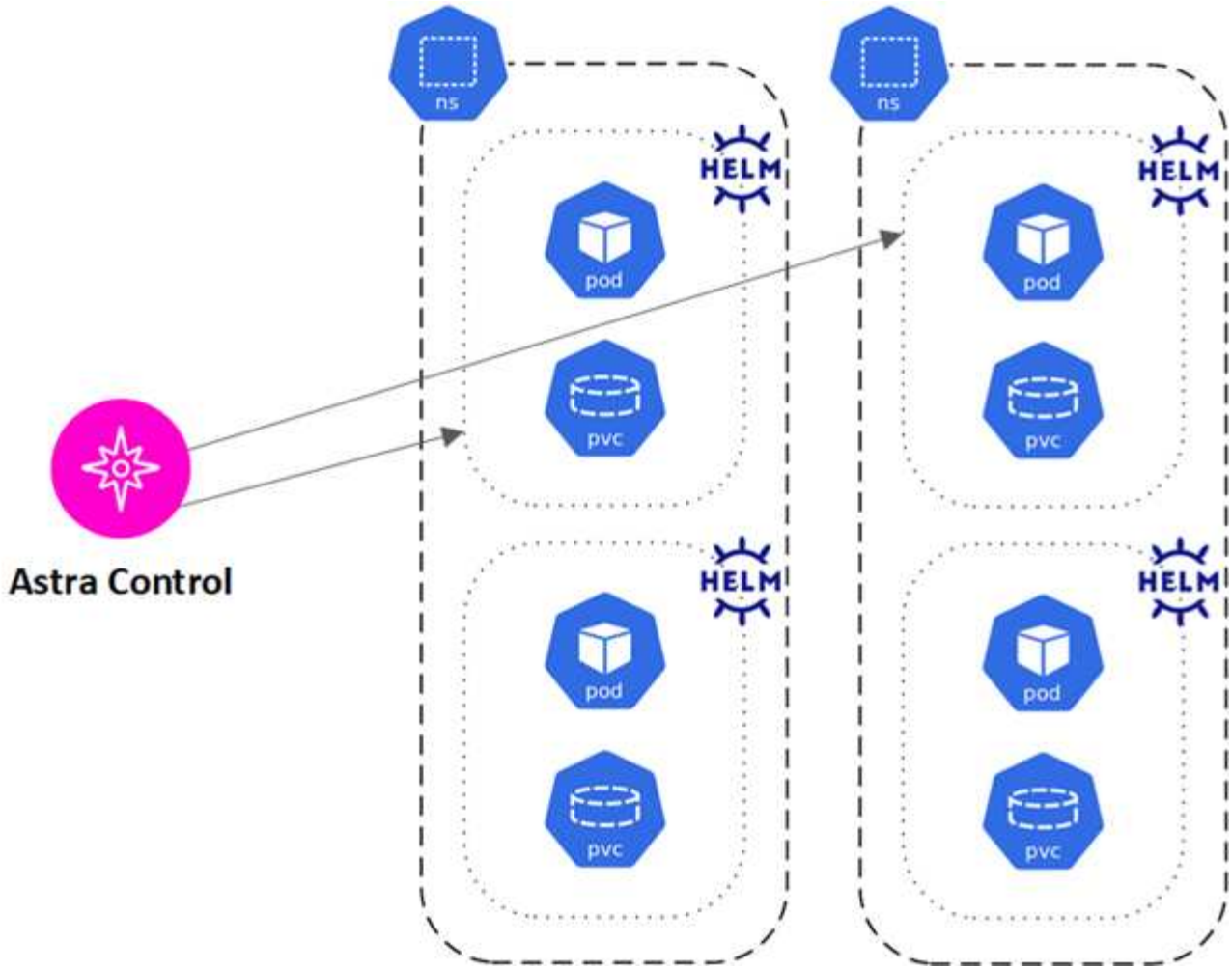
Gestión de aplicaciones

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:

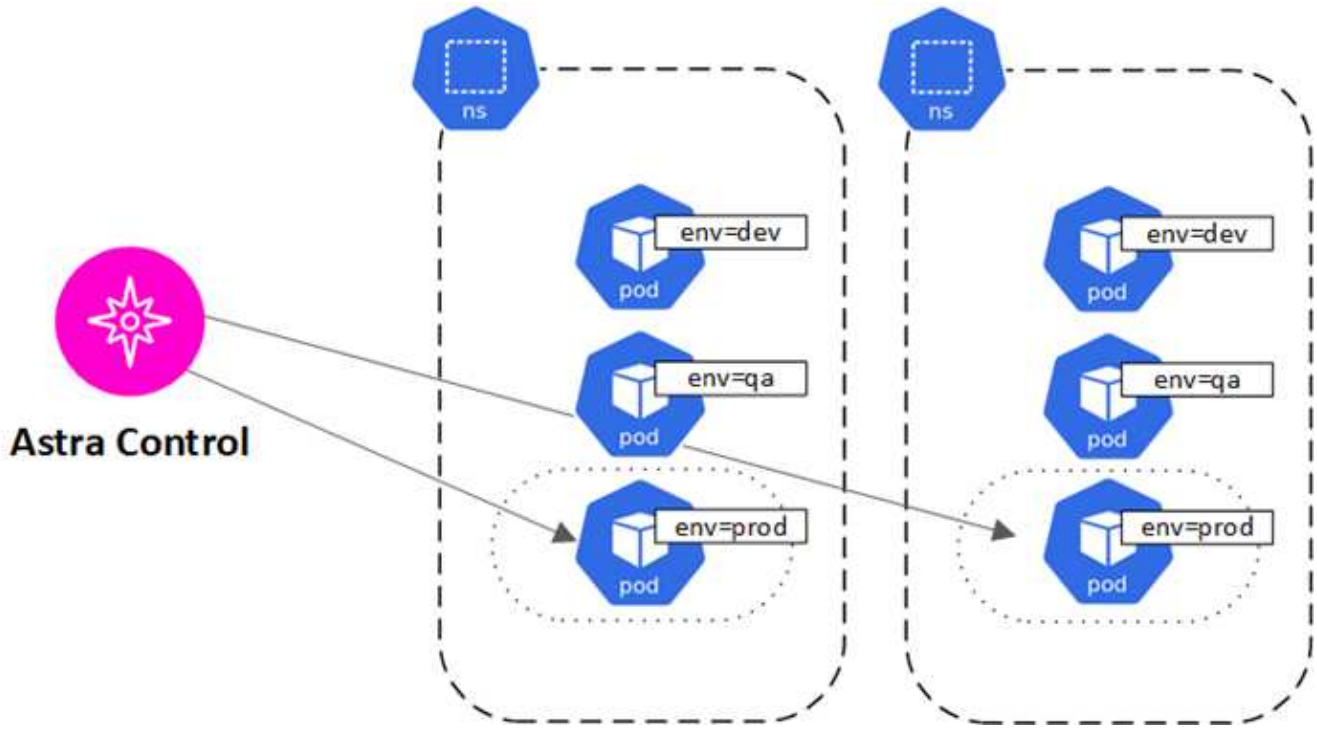
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- 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 es compatible con ONTAP como back-end de almacenamiento.

Descripción general

Astra Control Center admite lo siguiente:

- **Clases de almacenamiento de Astra Trident respaldadas por el almacenamiento de ONTAP**: Si estás usando un backend de ONTAP, Astra Control Center ofrece la capacidad de importar el backend de ONTAP para reportar información de monitoreo diversa.

> Las clases de almacenamiento de Astra Trident deben preconfigurarse fuera de Astra Control Center.

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.

Si quiere más información

- "Documentación de Astra Trident"

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"

Seguridad de POD

Astra Control Center admite la limitación de privilegios mediante directivas de seguridad de POD (PSP) y la admisión de seguridad de POD (PSA). Estos marcos le permiten limitar qué usuarios o grupos pueden ejecutar contenedores y qué privilegios pueden tener dichos contenedores.

Algunas distribuciones de Kubernetes pueden tener una configuración de seguridad en POD predeterminada que es demasiado restrictiva y causa problemas al instalar Astra Control Center.

Puede utilizar la información y los ejemplos que se incluyen aquí para comprender los cambios de seguridad del POD que realiza Astra Control Center, y utilizar un método de seguridad de POD que proporcione la protección que necesita sin interferir con las funciones de Astra Control Center.

El Servicio de Seguridad y Seguridad de la Seguridad y la Seguridad en el Control Center

Durante la instalación, Astra Control Center permite la aplicación de una admisión de seguridad de POD agregando la siguiente etiqueta a la `netapp-acc` o un espacio de nombres personalizado:

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

PSP instalado por Astra Control Center

Al instalar Astra Control Center en Kubernetes 1.23 o 1.24, se crean varias directivas de seguridad para POD durante la instalación. Algunas de ellas son permanentes y algunas se crean durante ciertas operaciones y se eliminan una vez que se completa la operación. Astra Control Center no intenta instalar PSP cuando el clúster de hosts ejecuta Kubernetes 1.25 o posterior, ya que no son compatibles con estas versiones.

Se crean PSP durante la instalación

Durante la instalación de Astra Control Center, el operador Astra Control Center instala una directiva de seguridad de POD personalizada, a. `Role` y un `RoleBinding` Objeto compatible con la implementación de los servicios Astra Control Center en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
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
```

Se crean PSP durante las operaciones de backup

Durante las operaciones de copia de seguridad, Astra Control Center crea una directiva de seguridad dinámica de POD, a. `ClusterRole` y un `RoleBinding` objeto. Estos permiten utilizar el proceso de backup, que se produce en un espacio de nombres aparte.

La política y los objetos nuevos tienen los siguientes atributos:

```
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
```

Se crean PSP durante la gestión del clúster

Cuando gestiona un clúster, Astra Control Center instala el operador de supervisión de netapp en el clúster gestionado. Este operador crea una directiva de seguridad de POD, a. `ClusterRole` y un `RoleBinding` Objeto para implementar servicios de telemetría en el espacio de nombres de Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
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
```