



Conceptos

Astra Control Center

NetApp
June 06, 2024

Tabla de contenidos

- Conceptos 1
- Más información sobre Astra Control 1
- Arquitectura y componentes 4
- Protección de datos 6
- Licencia 8
- Descripción de la gestión de aplicaciones 9
- Clases de almacenamiento y tamaño de volumen persistente 10
- Roles de usuario y espacios de nombres 11

Conceptos

Más información sobre Astra Control

Astra Control es una solución de gestión del ciclo de vida de los datos de las aplicaciones de Kubernetes que simplifica las operaciones para aplicaciones con estado. Proteja, cree backups, replique y migre cargas de trabajo de Kubernetes con facilidad y cree instantáneamente clones de aplicaciones en funcionamiento.

Funciones

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

- Gestione automáticamente el almacenamiento persistente
- Crear copias Snapshot y backups bajo demanda que se tienen en cuenta las aplicaciones
- Automatice las operaciones de backup y Snapshot condicionadas por políticas
- Replique una aplicación en un sistema remoto mediante la tecnología SnapMirror de NetApp
- Migre aplicaciones y datos de un clúster de Kubernetes a otro
- Clonar fácilmente una aplicación desde la producción hasta la configuración provisional
- Visualizar el estado de la protección y el estado de la aplicación
- Utilice una interfaz de usuario o una API para implementar los flujos de trabajo de backup y migración

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de implementación:

- **Astra Control Service:** Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en Google Kubernetes Engine (GKE) y Azure Kubernetes Service (AKS).
- **Astra Control Center:** Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local.

	Servicio de control Astra	Astra Control Center
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se descarga, se instala y se gestiona
¿Dónde está alojado?	En un cloud público que elija NetApp	En el clúster de Kubernetes que se suministra
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización
¿Cuáles son las funcionalidades de gestión de datos de aplicaciones?	Mismas funcionalidades en ambas plataformas, con excepciones en los back-end de almacenamiento o a servicios externos	Mismas funcionalidades en ambas plataformas, con excepciones en los back-end de almacenamiento o a servicios externos

	Servicio de control Astra	Astra Control Center
¿Cuál es el soporte del back-end de almacenamiento?	Ofertas de servicios cloud de NetApp	<ul style="list-style-type: none"> • Sistemas ONTAP AFF y FAS de NetApp • Astra Data Store como back-end de almacenamiento • Entorno de administración del almacenamiento de Cloud Volumes ONTAP

Funcionamiento del servicio Astra Control

Astra Control Service es un servicio cloud gestionado por NetApp que siempre está activo y actualizado con las últimas funcionalidades. Utiliza varios componentes para habilitar la gestión del ciclo de vida de los datos de aplicaciones.

En un nivel superior, Astra Control Service funciona de esta manera:

- Para comenzar a trabajar con Astra Control Service, configure su proveedor de cloud y inscribese para obtener una cuenta Astra.
 - Para los clústeres GKE, el servicio Astra Control utiliza ["Cloud Volumes Service de NetApp para Google Cloud"](#) O discos persistentes de Google como back-end de almacenamiento para sus volúmenes persistentes.
 - Para clústeres AKS, el servicio de control Astra utiliza ["Azure NetApp Files"](#) O almacenamiento en disco de Azure como back-end de almacenamiento para sus volúmenes persistentes.
 - Para clústeres de Amazon EKS, utiliza Astra Control Service ["Amazon Elastic Block Store"](#) o ["Amazon FSX para ONTAP de NetApp"](#) como back-end de almacenamiento para sus volúmenes persistentes.
- Agregue su primera tecnología Kubernetes al servicio Astra Control. A continuación, el servicio de control de Astra realiza lo siguiente:
 - Crea un almacén de objetos en su cuenta de proveedor de cloud, que es donde se almacenan las copias de backup.

En Azure, Astra Control Service también crea un grupo de recursos, una cuenta de almacenamiento y claves para el contenedor Blob.
 - Crea un nuevo rol de administrador y una cuenta de servicio de Kubernetes en el clúster.
 - Utiliza la nueva función de administración para instalar ["Astra Trident"](#) en el clúster y para crear una o varias clases de almacenamiento.
 - Si utiliza Azure NetApp Files o Cloud Volumes Service de NetApp para Google Cloud como back-end de almacenamiento, el servicio Astra Control utiliza Astra Trident para aprovisionar volúmenes persistentes para sus aplicaciones.
- En este momento, puede añadir aplicaciones al clúster. Se aprovisionan volúmenes persistentes en la nueva clase de almacenamiento predeterminada.
- A continuación, utilice Astra Control Service para gestionar estas aplicaciones y empiece a crear copias Snapshot, copias de seguridad y clones.

El plan gratuito de Astra Control le permite gestionar hasta 10 aplicaciones en su cuenta. Si desea gestionar más de 10 aplicaciones, tendrá que configurar la facturación mediante la actualización del plan gratuito al plan

Premium.

Cómo funciona Astra Control Center

Astra Control Center se ejecuta en forma local en su propia nube privada.

Astra Control Center es compatible con clústeres de Kubernetes con:

- Back-ends de almacenamiento de Trident con ONTAP 9.5 y versiones posteriores
- Astra Data Store back-ends

En un entorno conectado a la nube, Astra Control Center utiliza Cloud Insights para proporcionar supervisión y telemetría avanzadas. Ante la ausencia de una conexión con Cloud Insights, la telemetría y la supervisión limitadas (7 días de métricas) están disponibles en Astra Control Center y también se exportan a herramientas de supervisión nativas de Kubernetes (como Prometheus y Grafana) mediante puntos finales de métricas abiertas.

Astra Control Center está totalmente integrado en el ecosistema de AutoSupport y Active IQ para proporcionar a los usuarios y el soporte de NetApp información sobre solución de problemas y uso.

Puede probar Astra Control Center con una licencia de evaluación de 90 días. La versión de evaluación se admite a través de opciones de correo electrónico y comunidad (canal Slack). Además, tendrá acceso a los artículos de la base de conocimientos y a la documentación desde la consola de soporte del producto.

Para instalar y utilizar Astra Control Center, tendrá que estar seguro "[requisitos](#)".

En un nivel superior, Astra Control Center funciona de esta manera:

- Instala Astra Control Center en su entorno local. Obtenga más información sobre cómo "[Instalar Astra Control Center](#)".
- Puede realizar algunas tareas de configuración como las siguientes:
 - Configurar la licencia.
 - Añada el primer clúster.
 - Añada el back-end de almacenamiento que se detecta al añadir el clúster.
 - Agregue un bloque de almacenamiento de objetos que almacenará las copias de seguridad de la aplicación.

Obtenga más información sobre cómo "[Configure Astra Control Center](#)".

El Centro de Control de Astra hace lo siguiente:

- Detecta detalles del clúster, incluidos los espacios de nombres, y permite definir y proteger las aplicaciones.
- Descubre la configuración de Astra Trident o Astra Data Store en los clústeres que desea gestionar y le permite supervisar los back-ends de almacenamiento.

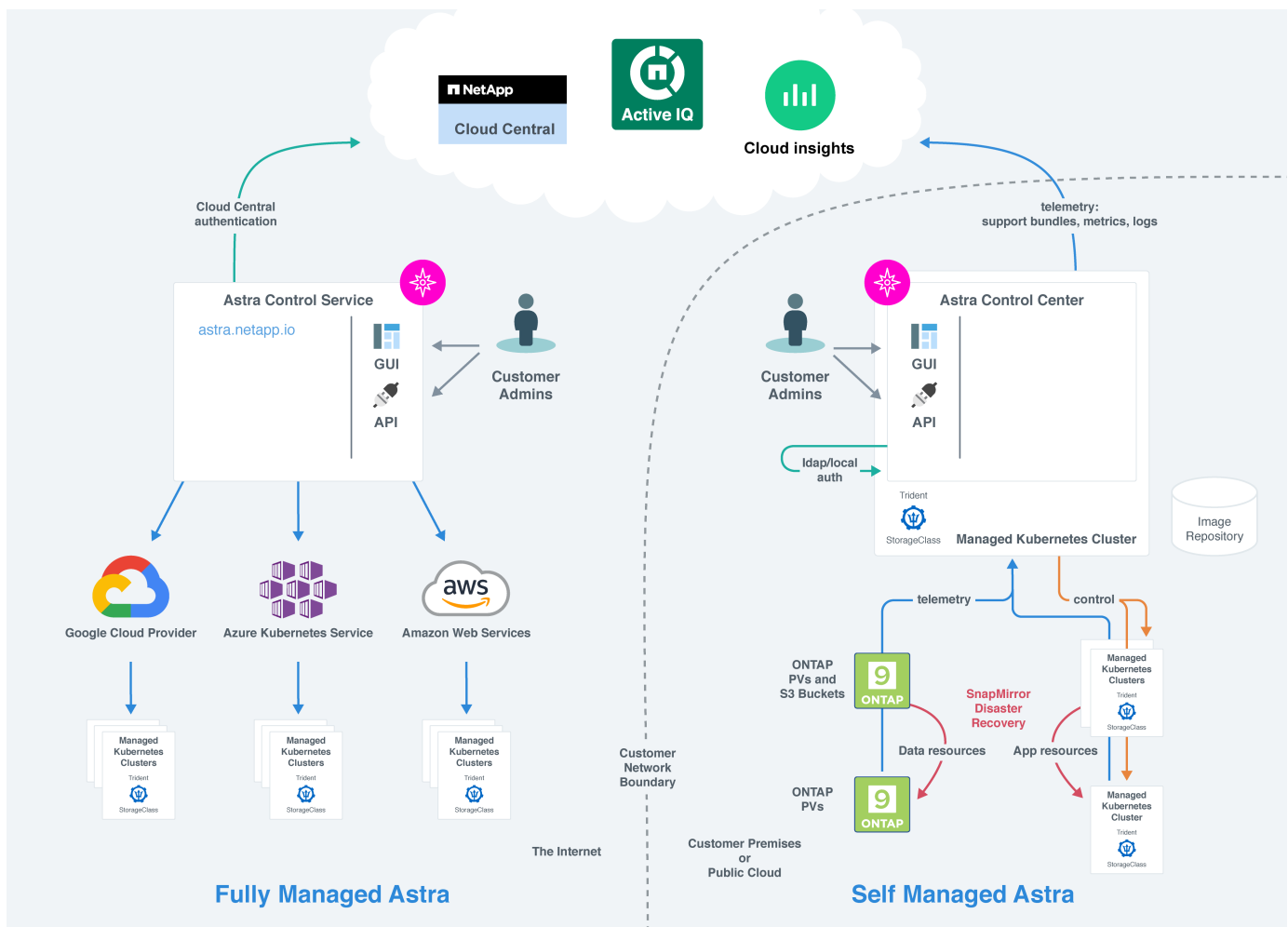
Puede añadir aplicaciones al clúster. O bien, si ya tiene algunas aplicaciones en el clúster que se están gestionando, puede utilizar Astra Control Center para gestionarlas. A continuación, utilice Astra Control Center para crear copias Snapshot, backups, clones y relaciones de replicación.

Si quiere más información

- "Documentación de Astra Control Service"
- "Documentación de Astra Control Center"
- "Documentación de Astra Data Store"
- "Documentación de Astra Trident"
- "Utilice la API Astra Control"
- "Documentación de Cloud Insights"
- "Documentación de ONTAP"

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, 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, 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 y FAS. 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 cloud de NetApp, Cloud Insights le permite supervisar el rendimiento y la utilización de sus clústeres de Kubernetes gestionados por Astra Control Center. 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

Un *snapshot* es una copia puntual de una aplicación que se almacena en el mismo volumen provisionado 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.

Un *backup* se almacena en el almacén de objetos externo y puede tardar más en tomarse en comparación con las instantáneas 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. Automatizar los backups y las copias Snapshot con una política de protección es la mejor manera de garantizar que cada aplicación esté protegida en función de las necesidades de la organización.



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 su almacenamiento persistente. 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

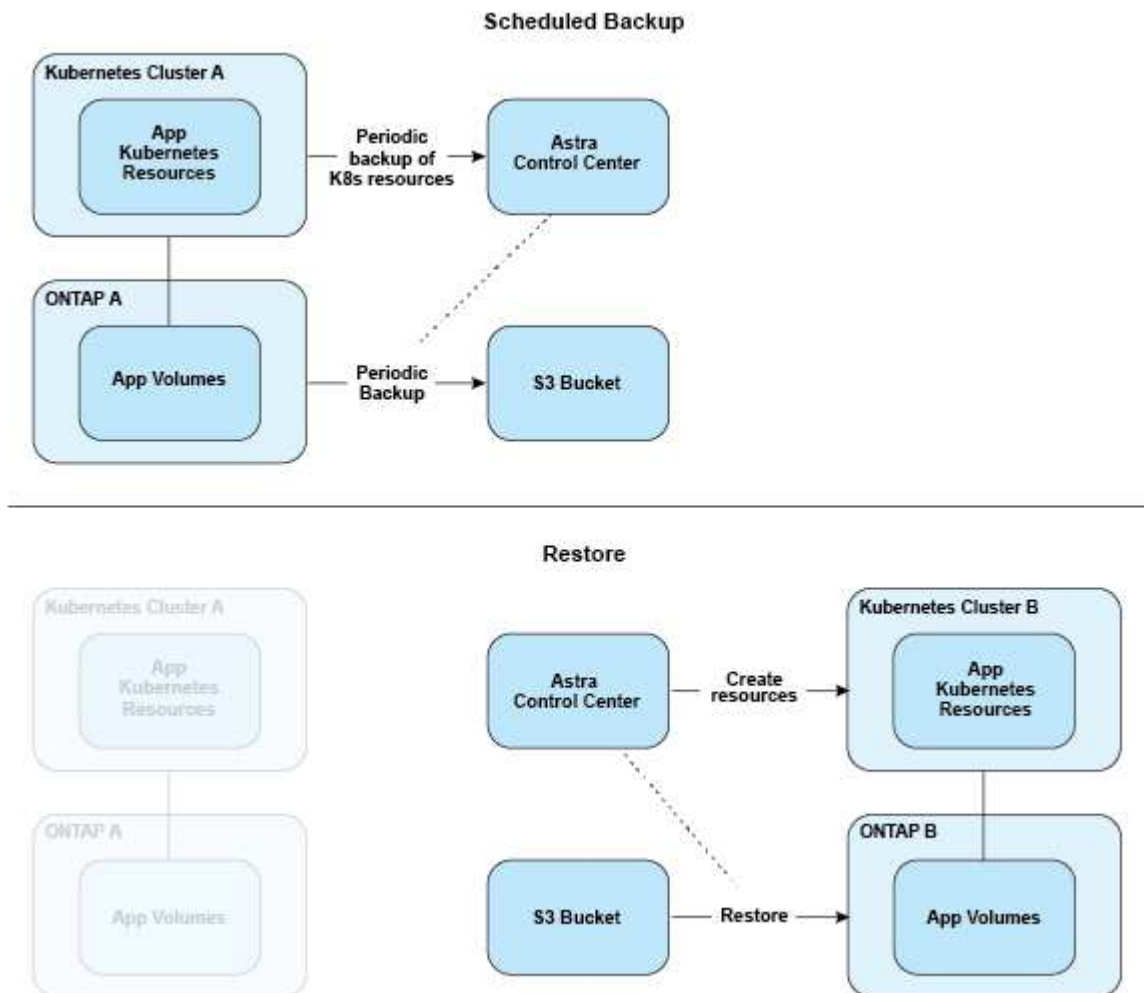
configurados para habilitar SnapMirror de NetApp. Astra Control toma la instantánea de las aplicaciones basadas en normativas y la replica en el clúster remoto. La tecnología SnapMirror de NetApp se usa para replicar los datos de volúmenes persistentes. Para conmutar al nodo de respaldo, Astra Control 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 en caso de fallo.

- **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 saber cómo replicar aplicaciones, consulte ["Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror"](#).

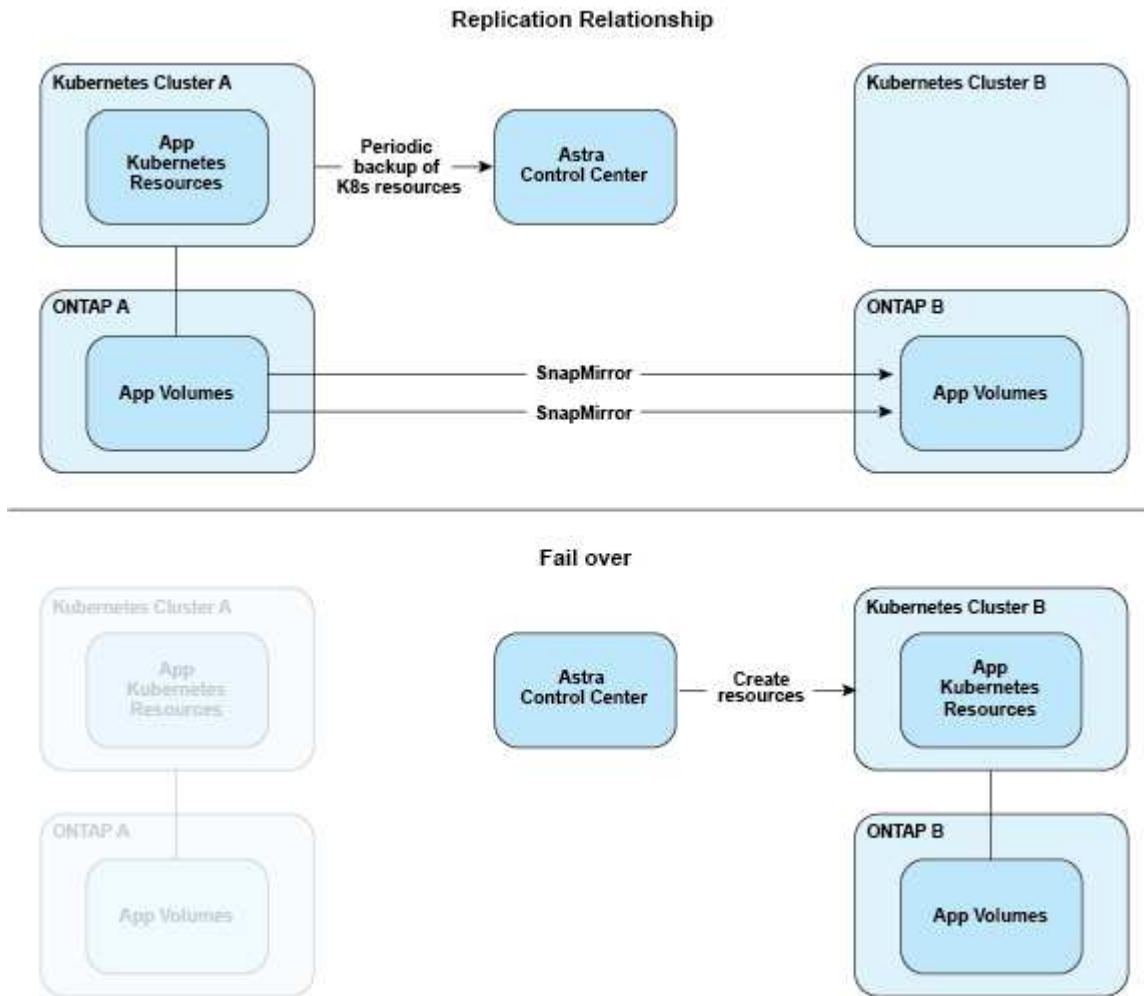
Las siguientes imágenes muestran el proceso de backup y restauración programado en comparación con el proceso de replicación.

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 para después crear el relevo de funciones en los

recursos de Kubernetes:



Licencia

Astra Control Center requiere la instalación de una licencia para habilitar la funcionalidad completa de gestión de datos de aplicaciones. Cuando se implementa Astra Control Center sin una licencia, se muestra un banner en la interfaz de usuario web, con la advertencia de que la funcionalidad del sistema es limitada.

Necesita una licencia para proteger sus aplicaciones y datos. Consulte Astra Control Center ["funciones"](#) para obtener más detalles.

Después de adquirir el producto, recibirá un número de serie y una licencia. Es posible generar el archivo de licencia de NetApp (NLF) a partir de ["Sitio de soporte de NetApp"](#).

También puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Para obtener más información, consulte ["Requisitos"](#).

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



Puede añadir un clúster, añadir un bloque y gestionar un back-end de almacenamiento sin una licencia.

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 se empieza a gestionar una aplicación en un clúster, todas las unidades CPU del clúster se incluyen en el consumo de licencia de Astra Control Center.

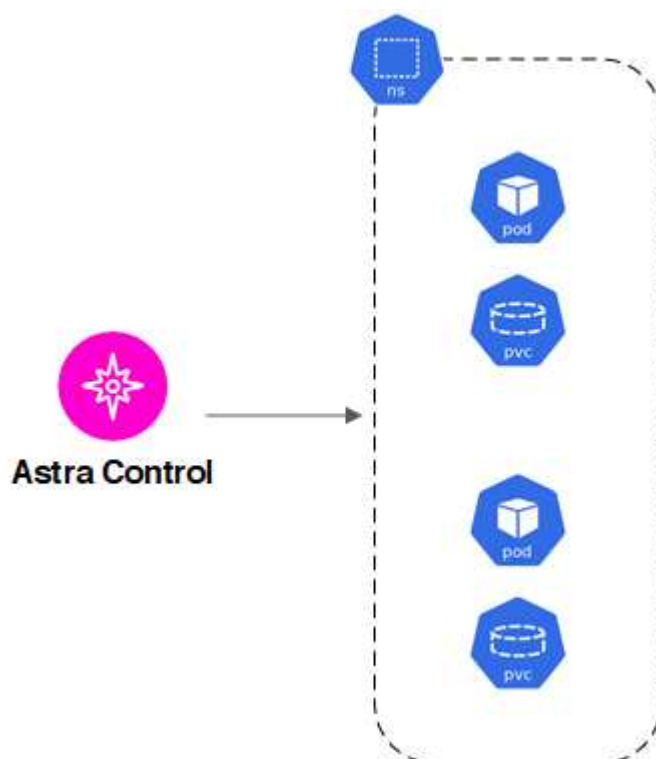
Obtenga más información

- ["Actualizar una licencia existente"](#)

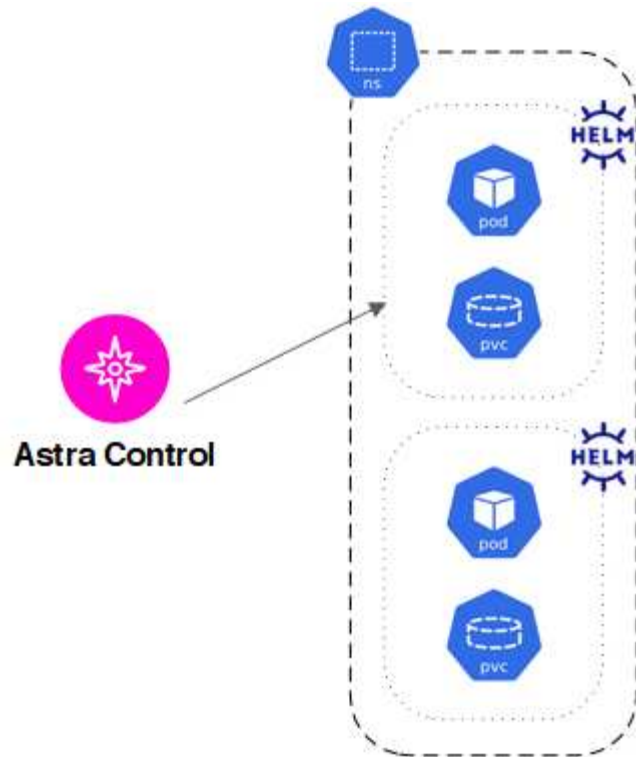
Descripción de la gestión de aplicaciones

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:

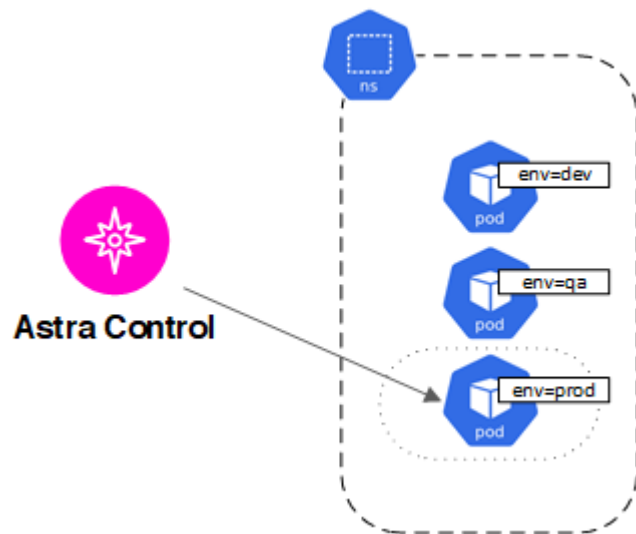
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- Una aplicación individual implementada en un espacio de nombres (en este ejemplo se utiliza helm3)



- Un grupo de recursos que se identifican mediante una etiqueta de Kubernetes dentro de un espacio de nombres



Clases de almacenamiento y tamaño de volumen persistente

Astra Control Center es compatible con ONTAP o Astra Data Store como back-end de almacenamiento.

Descripción general

Astra Control Center admite lo siguiente:

- * Clases de almacenamiento Trident respaldadas por Astra Data Store Storage*: Si ha instalado uno o varios clústeres de Astra Data Store manualmente, Astra Control Center ofrece la capacidad de importar estos y recuperar su topología (nodos, discos), así como varios Estados.

Astra Control Center muestra el clúster de Kubernetes subyacente de la configuración de Astra Data Store, la nube a la que pertenece el clúster de Kubernetes, los volúmenes persistentes aprovisionados por Astra Data Store, el nombre del volumen interno correspondiente, la aplicación que utiliza el volumen persistente y el clúster que contiene la aplicación.

- * Clases de almacenamiento Trident respaldadas por almacenamiento ONTAP*: Si utiliza un back-end de ONTAP, Astra Control Center ofrece la capacidad de importar el back-end de ONTAP para informar sobre diversos datos de supervisión.



Las clases de almacenamiento de 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.

Cuando utiliza Astra Control Center integrado con un back-end de almacenamiento de Astra Data Store, después de la instalación, no se definen clases de almacenamiento. Deberá crear la clase de almacenamiento predeterminada de Trident y aplicarla al back-end de almacenamiento. Consulte "[Introducción a Astra Data Store](#)" Para crear una clase de almacenamiento Astra Data Store predeterminada.

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

["Gestionar roles"](#)

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.