Documentación de Astra Control Center 24,02

Astra Control Center

NetApp
April 25, 2024

Tabla de contenidos

Documentación de Astra Control Center 24,02

Notas de la versión

Nos complace anunciar la última versión de Astra Control Center.

- "¿Qué hay en esta versión de Astra Control Center"
- "Problemas conocidos"
- "Limitaciones conocidas"

Envíe sus comentarios sobre la documentación convirtiéndose en una "Colaborador de GitHub" o enviar un correo electrónico a doccomments@netapp.com.

Novedades de esta versión de Astra Control Center

Nos complace anunciar la última versión de Astra Control Center.

15 de marzo de 2024 (24.02.0)

Nuevas funciones y soporte

- **Implementar Astra Control Center sin un registro privado**: Ya no es necesario enviar imágenes de Astra Control Center a un registro privado o usar uno como parte de su entorno de Astra Control.
- **Correcciones de errores menores**

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

(Vista previa técnica) Flujos de trabajo declarativos de Kubernetes

Esta versión de Astra Control Center contiene la funcionalidad declarativa de Kubernetes que le permite realizar una gestión de datos desde un recurso personalizado de Kubernetes nativo (CR).

Después de instalar el "Conector Astra" En el clúster que desee gestionar, podrá realizar las siguientes operaciones de clúster basadas en CR en la interfaz de usuario o desde un CR:

- "Defina una aplicación mediante un recurso personalizado"
- "Defina el período"
- "Proteja todo un clúster"
- "Realice una copia de seguridad de su aplicación"
- "Crear una copia de Snapshot"
- "Crear programaciones para Snapshot o backups"
- "Restaure una aplicación desde una copia Snapshot o un backup"

7 de noviembre de 2023 (23.10.0)

Nuevas funciones y soporte

- * Capacidades de copia de seguridad y restauración para aplicaciones con backends de almacenamiento respaldados por controladores de economía ontap-nas*: Permite operaciones de copia de seguridad y restauración para `ontap-nas-economy` con algunos "sencillos pasos".

- **Copias de seguridad inmutables**: Astra Control ahora es compatible "backups de solo lectura que se pueden modificar" como capa de seguridad adicional contra el malware y otras amenazas.
- **Presentamos Astra Control Provisionador**

  Con el lanzamiento 23,10, Astra Control introduce un nuevo componente de software llamado Astra Control Provisioning que estará disponible para todos los usuarios con licencia de Astra Control. Astra Control Provisioning ofrece acceso a un superconjunto de funciones avanzadas de aprovisionamiento de almacenamiento y gestión más allá de las que ofrece Astra Trident. Estas funciones están disponibles para todos los clientes de Astra Control sin coste adicional.

  - **Empieza con Astra Control Provisioner**
    Puede hacerlo "Habilita el aprovisionador de Astra Control" Si ha instalado y configurado su entorno de modo que utilice Astra Trident 23,10.
  - **La funcionalidad de Astra Control Provisionador**

    Las siguientes funciones están disponibles en la versión Astra Control Provisioner 23,10:

    - * Seguridad de backend de almacenamiento mejorada con cifrado Kerberos 5*: Puede mejorar la seguridad del almacenamiento "habilitar cifrado" para el tráfico entre el clúster gestionado y el back-end de almacenamiento. El aprovisionador de control de Astra admite el cifrado de Kerberos 5 a través de conexiones NFSv4,1 GbE desde clústeres de Red Hat OpenShift a volúmenes Azure NetApp Files y ONTAP en las instalaciones
    - **Recuperar datos usando una instantánea**: Astra Control Provisioner proporciona una restauración de volumen rápida y en el lugar desde una instantánea usando el `TridentActionSnapshotRestore` (TASR) CR.
    - **Mejoras de SnapMirror**: Utilice la función de replicación de aplicaciones en entornos en los que Astra Control no tenga conectividad directa a un clúster de ONTAP ni acceso a credenciales de ONTAP. Esta función te permite utilizar la replicación sin tener que gestionar un back-end de almacenamiento ni sus credenciales en Astra Control.
    - * Capacidades de copia de seguridad y restauración para aplicaciones con `ontap-nas-economy` Back-ends de almacenamiento respaldados por el conductor*: Como se describe anterior.
- **Soporte para la gestión de aplicaciones que utilizan almacenamiento NVMe/TCP**
  Astra Control ahora puede gestionar aplicaciones respaldadas por volúmenes persistentes que están conectados mediante NVMe/TCP.
- * Ganchos de ejecución desactivados por defecto*: A partir de esta versión, la funcionalidad de los ganchos de ejecución puede ser "activado" o desactivado para seguridad adicional (está desactivado de forma predeterminada). Si todavía no has creado enlaces de ejecución para usarlos con Astra Control, debes hacerlo "active la función de enlaces de ejecución" para empezar a crear ganchos. Si ha creado enlaces de ejecución antes de esta versión, la funcionalidad de enlaces de ejecución permanece activada y puede utilizar los enlaces como lo haría normalmente.

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

31 de julio de 2023 (23.07.0)

Nuevas funciones y soporte

- "Soporte para el uso de NetApp MetroCluster en una configuración de ampliación como back-end de almacenamiento"

- "Soporte para el uso de Longhorn como back-end de almacenamiento"
- "Ahora las aplicaciones se pueden replicar entre back-ends de ONTAP desde el mismo clúster de Kubernetes"
- "Astra Control Center ahora admite 'userPrincipalName' como atributo de inicio de sesión alternativo para usuarios remotos (LDAP)"
- "Se puede ejecutar un nuevo tipo de gancho de ejecución 'post-failover' después de la conmutación al nodo de respaldo de la replicación con Astra Control Center"
- Los flujos de trabajo de clonado ahora solo admiten clones activos (el estado actual de las aplicaciones gestionadas). Para clonar desde una copia Snapshot o un backup, utilice "flujo de trabajo de restauración".

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

18 de mayo de 2023 (23.04.2)

Esta versión de revisión (23.04.2) de Astra Control Center (23.04.0) ofrece compatibilidad para "Snapshotter externo CSI de Kubernetes v6,1.0" y corrige lo siguiente:

- Un error con la restauración de la aplicación in situ al utilizar los ganchos de ejecución
- Problemas de conexión con el servicio de depósito

25 de abril de 2023 (23.04.0)

Nuevas funciones y soporte

- "Licencia de evaluación de 90 días habilitada de forma predeterminada para nuevas instalaciones de Astra Control Center"
- "Funciones mejoradas de enlaces de ejecución con opciones de filtrado adicionales"
- "Ahora se pueden ejecutar ganchos de ejecución después de la conmutación al nodo de respaldo de la replicación con Astra Control Center"
- "Soporte para la migración de volúmenes de la clase «almacenamiento económico ontap-nas» al tipo de almacenamiento «ontap-nas»"
- "Soporte para incluir o excluir recursos de aplicaciones durante las operaciones de restauración"
- "Compatibilidad para la gestión de aplicaciones solo de datos"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

22 de noviembre de 2022 (22.11.0)

Nuevas funciones y soporte

- "Compatibilidad con aplicaciones que abarcan varios espacios de nombres"
- "Soporte para incluir recursos de clúster en una definición de aplicación"
- "Autenticación LDAP mejorada con integración de control de acceso basado en roles (RBAC)"
- "Compatibilidad añadida para Kubernetes 1.25 y admisión de seguridad en Pod (PSA)"

- "Generación de informes de progreso mejorado para sus operaciones de backup, restauración y clonado"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

8 de septiembre de 2022 (22.08.1)

Esta versión de revisión (22.08.1) para Astra Control Center (22.08.0) soluciona errores menores en la replicación de aplicaciones mediante SnapMirror de NetApp.

10 de agosto de 2022 (22.08.0)

Nuevas funciones y soporte

- "Replicación de aplicaciones con la tecnología SnapMirror de NetApp"
- "Flujo de trabajo de gestión de aplicaciones mejorado"
- "Mejora la funcionalidad de enlaces de ejecución propios"

> En esta versión, NetApp proporcionó los enlaces predeterminados de ejecución de copias Snapshot y posteriores a ellas para aplicaciones específicas. Si actualiza a esta versión y no proporciona sus propios enlaces de ejecución para instantáneas, Astra Control sólo realizará instantáneas coherentes con los fallos. Visite la "Verda de NetApp" Repositorio de GitHub para secuencias de comandos de gancho de ejecución de muestra que puede modificar para ajustarse a su entorno.

- "Soporte para VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)"
- "Compatibilidad con Google Anthos"
- "Configuración de LDAP (mediante la API Astra Control)"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

26 de abril de 2022 (22.04.0)

Nuevas funciones y soporte

- "Control de acceso basado en roles (RBAC) del espacio de nombres"
- "Compatibilidad con Cloud Volumes ONTAP"
- "Habilitación de entrada genérica para Astra Control Center"
- "Desmontaje de la cuchara del control Astra"
- "Soporte para la cartera de tanzu de VMware"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

14 de diciembre de 2021 (21.12)

Nuevas funciones y soporte

- "Restauración de aplicaciones"
- "Ganchos de ejecución"
- "Soporte para aplicaciones implementadas con operadores con ámbito de espacio de nombres"
- "Compatibilidad adicional para upstream Kubernetes y Rancher"
- "Actualizaciones de Astra Control Center"
- "Opción Red Hat OperatorHub para la instalación"

Problemas resueltos

- "Se han resuelto problemas para esta versión"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

5 de agosto de 2021 (21.08)

Lanzamiento inicial de Astra Control Center.

- "Qué es"
- "Comprensión de la arquitectura y los componentes"
- "Qué se necesita para empezar"
- "Instale" y.. "configuración"
- "Gestione" y.. "proteger" aplicaciones
- "Gestionar bloques" y.. "back-ends de almacenamiento"
- "Gestionar cuentas"
- "Automatización con API"

Obtenga más información

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"
- "Versiones anteriores de la documentación de Astra Control Center"

Problemas conocidos

Los problemas conocidos identifican problemas por los que el uso correcto de esta versión del producto puede resultar imposible.

Los siguientes problemas conocidos afectan a la versión actual:

- Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster

- Se produce un error en la gestión de un clúster con Astra Control Center cuando el archivo kubeconfig contiene más de un contexto
- Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión
- Las operaciones de restauración sin movimiento a las clases de almacenamiento económico ontap-nas fallan
- Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos
- Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida

Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster

Los backups y las Snapshot fallan con un `UI 500 error` en este escenario. Como solución alternativa, actualice la lista de aplicaciones.

Se produce un error en la gestión de un clúster con Astra Control Center cuando el archivo kubeconfig contiene más de un contexto

No puede utilizar una imagen de kubeconfig con más de un clúster y contexto en él. Consulte "artículo de base de conocimientos" si quiere más información.

Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión

Si Astra Trident se desconecta (y se vuelve a conectar) y se producen 500 errores internos de servicio al intentar gestionar los datos de las aplicaciones, reinicie todos los nodos de Kubernetes del clúster de aplicaciones para restaurar la funcionalidad.

Las operaciones de restauración sin movimiento a las clases de almacenamiento económico ontap-nas fallan

Si realiza una restauración sin movimiento de una aplicación (restaura la aplicación en su espacio de nombres original) y la clase de almacenamiento de la aplicación utiliza el `ontap-nas-economy` controlador, se puede producir un error en la operación de restauración si el directorio snapshot no está oculto. Antes de restaurar en el lugar, siga las instrucciones de "Habilite el backup y la restauración para las operaciones económicas de ontap-nas" para ocultar el directorio de instantáneas.

Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos

Cuando se restaura una aplicación desde un backup a un back-end de almacenamiento que utiliza el cifrado en tránsito de Kerberos, se puede producir un error en la operación de restauración. Este problema no afecta a la restauración de una copia Snapshot ni a la replicación de los datos de la aplicación mediante SnapMirror de NetApp.

> Cuando use el cifrado en tránsito de Kerberos con volúmenes NFSv4, asegúrese de que los volúmenes NFSv4 estén utilizando la configuración correcta. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida

Si elimina el backup inmutable de una aplicación después de que la política de retención del bloque haya caducado, el backup se eliminará de Astra Control, pero no del bloque. Este problema se solucionará en una próxima versión.

Obtenga más información

- "Limitaciones conocidas"

Limitaciones conocidas

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

Limitaciones de gestión de clústeres

- Dos instancias de Astra Control Center no pueden gestionar el mismo clúster
- Astra Control Center no puede gestionar dos clústeres con el mismo nombre

Limitaciones de control de acceso basado en roles (RBAC)

- Un usuario con restricciones de RBAC de espacio de nombres puede añadir y anular la gestión de un clúster
- Un miembro con restricciones de espacio de nombres no puede acceder a las aplicaciones clonadas o restauradas hasta que el administrador agregue el espacio de nombres a la restricción
- Las restricciones de rol restrictivas se pueden ignorar para los recursos en clusters que no son de conector

Limitaciones en la gestión de aplicaciones

- No es posible restaurar varias aplicaciones en un espacio de nombres único de forma colectiva en un espacio de nombres diferente
- Astra Control no es compatible con aplicaciones que usan varias clases de almacenamiento por espacio de nombres
- Astra Control no asigna automáticamente bloques predeterminados para las instancias de la nube
- Se pueden producir errores en los clones de aplicaciones instaladas con operadores de paso a referencia
- No se admiten las operaciones de restauración in situ de las aplicaciones que utilizan un administrador de certificados
- No se admiten aplicaciones puestas en marcha de operadores con OLM y ámbito de clúster
- Las aplicaciones implementadas con Helm 2 no son compatibles
- 25 o posteriores con ciertas versiones de controladoras Snapshot

- Es posible que no se conserven las copias de Snapshot durante la eliminación de una instancia de Astra Control Center

Limitaciones generales

- Limitaciones de usuarios y grupos LDAP
- Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible
- Astra Control Center no valida los detalles introducidos para su servidor proxy
- Las conexiones existentes a un pod Postgres provocan fallos
- La página Actividad muestra hasta 100000 eventos
- SnapMirror no admite aplicaciones que utilizan NVMe over TCP para back-ends de almacenamiento

Dos instancias de Astra Control Center no pueden gestionar el mismo clúster

Si desea gestionar un clúster en otra instancia de Astra Control Center, primero debe hacerlo "anule la gestión del clúster" desde la instancia en la que se gestiona antes de administrarla en otra instancia. Después de quitar el clúster de la administración, compruebe que el clúster no se administre ejecutando este comando:

```
oc get pods n -netapp-monitoring
```

No debe haber ningún POD que se ejecuten en ese espacio de nombres o no debe existir el espacio de nombres. Si alguno de ellos es verdadero, el clúster no se gestiona.

Astra Control Center no puede gestionar dos clústeres con el mismo nombre

Si intenta añadir un clúster con el mismo nombre de un clúster que ya existe, la operación fallará. Este problema se produce más a menudo en un entorno Kubernetes estándar si no se ha cambiado el nombre predeterminado del clúster en los archivos de configuración de Kubernetes.

Para solucionar este problema, haga lo siguiente:

1. Edite su `kubeadm-config` Mapa de ConfigMap:

   ```
   kubectl edit configmaps -n kube-system kubeadm-config
   ```

2. Cambie el `clusterName` valor de campo desde `kubernetes` (El nombre predeterminado de Kubernetes) a un nombre personalizado único.
3. Editar imagen de kubeconfig (`.kube/config`).
4. Actualice el nombre del clúster desde `kubernetes` a un nombre personalizado único (`xyz-cluster` se utiliza en los siguientes ejemplos). Realice la actualización en ambos `clusters` y.. `contexts` secciones como se muestra en este ejemplo:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

Un usuario con restricciones de RBAC de espacio de nombres puede añadir y anular la gestión de un clúster

No se debe permitir que un usuario con restricciones de RBAC de espacio de nombres añada o anule la gestión de clústeres. Debido a una limitación actual, Astra no impide que estos usuarios desgestionen los clústeres.

Un miembro con restricciones de espacio de nombres no puede acceder a las aplicaciones clonadas o restauradas hasta que el administrador agregue el espacio de nombres a la restricción

Cualquiera `member` El usuario con limitaciones de RBAC por nombre/ID de espacio de nombres puede clonar o restaurar una aplicación en un espacio de nombres nuevo en el mismo clúster o en cualquier otro clúster de la cuenta de la organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Una vez que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar el `member` cuenta de usuario y restricciones de función de actualización para que el usuario afectado conceda acceso al nuevo espacio de nombres.

Las restricciones de rol restrictivas se pueden ignorar para los recursos en clusters que no son de conector

- **Si los recursos a los que se accede pertenecen a clusters que tienen instalado el último Astra Connector**: Cuando se asignan varios roles a un usuario a través de la pertenencia a un grupo LDAP, se combinan las restricciones de los roles. Por ejemplo, si un usuario con un rol de visor local une tres grupos vinculados al rol de miembro, el usuario ahora tendrá acceso al rol de visor a los recursos originales, así como acceso al rol de miembro a los recursos obtenidos mediante la pertenencia al grupo.
- **Si los recursos a los que se accede pertenecen a clusters que no tienen instalado Astra Connector**: Cuando se asignan varios roles a un usuario a través de la pertenencia a un grupo LDAP, las restricciones del rol más permisivo son las únicas que surten efecto.

No es posible restaurar varias aplicaciones en un espacio de nombres único de forma colectiva en un espacio de nombres diferente

Si administra varias aplicaciones en un espacio de nombres único (mediante la creación de varias definiciones de aplicaciones en Astra Control), no podrá restaurar todas las aplicaciones en un espacio de nombres único diferente. Es necesario restaurar cada aplicación a su propio espacio de nombres independiente.

Astra Control no es compatible con aplicaciones que usan varias clases de almacenamiento por espacio de nombres

Astra Control admite aplicaciones que utilizan una única clase de almacenamiento por espacio de nombres. Al agregar una aplicación a un espacio de nombres, asegúrese de que la aplicación tenga la misma clase de almacenamiento que otras aplicaciones del espacio de nombres.

Astra Control no asigna automáticamente bloques predeterminados para las instancias de la nube

Astra Control no asigna automáticamente un bloque predeterminado para ninguna instancia de cloud. Debe establecer manualmente un bloque predeterminado para una instancia de cloud. Si no se ha establecido un bloque predeterminado, no se podrán realizar operaciones de clonado de aplicaciones entre dos clústeres.

Se pueden producir errores en los clones de aplicaciones instaladas con operadores de paso a referencia

Astra Control admite las aplicaciones instaladas con operadores con ámbito de espacio de nombres. Estos operadores están diseñados generalmente con una arquitectura "pasada por valor" en lugar de "pasada por referencia". Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

- "Apache K8ssandra"

> Para K8ssandra, se admiten operaciones de restauración in situ. Una operación de restauración a un nuevo espacio de nombres o clúster requiere que se apague la instancia original de la aplicación. Esto es para garantizar que la información del grupo de pares no conduzca a la comunicación entre instancias. No se admite la clonación de la aplicación.

- "Jenkins CI"
- "Clúster Percona XtraDB"

Es posible que Astra Control no pueda clonar a un operador diseñado con una arquitectura "pase por referencia" (por ejemplo, el operador CockroachDB). Durante estos tipos de operaciones de clonado, el operador clonado intenta hacer referencia a los secretos de Kubernetes del operador de origen a pesar de tener su propio secreto nuevo como parte del proceso de clonado. Es posible que se produzca un error en la operación de clonado porque Astra Control no conoce los secretos de Kubernetes en el operador de origen.

> Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.

No se admiten las operaciones de restauración in situ de las aplicaciones que utilizan un administrador de certificados

Esta versión de Astra Control Center no admite la restauración local de aplicaciones con gestores de certificados. Se admiten las operaciones de restauración en otro espacio de nombres y operaciones de clonado.

No se admiten aplicaciones puestas en marcha de operadores con OLM y ámbito de clúster

Astra Control Center no admite las actividades de gestión de aplicaciones con operadores con ámbito de clúster.

Las aplicaciones implementadas con Helm 2 no son compatibles

Si utiliza Helm para implantar aplicaciones, Astra Control Center requiere Helm versión 3. Es totalmente compatible con la gestión y clonación de aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Para obtener más información, consulte "Requisitos del Centro de Control de Astra".

Es posible que las copias de Snapshot fallen en clústeres de Kubernetes 1,25 o posteriores con ciertas versiones de controladoras Snapshot

Las snapshots de los clústeres de Kubernetes que ejecutan la versión 1,25 o posterior pueden fallar si la versión v1beta1 de las API del controlador de snapshots se instala en el clúster.

Como solución alternativa, haga lo siguiente al actualizar instalaciones existentes de Kubernetes 1,25 o posteriores:

1. Elimine cualquier CRD de Snapshot existente y cualquier controlador de instantánea existente.
2. "Desinstale Astra Trident".
3. "Instale los CRD de instantánea y el controlador de instantánea".
4. "Instala la versión más reciente de Astra Trident".
5. "Cree una instancia de VolumeSnapshotClass".

Es posible que no se conserven las copias de Snapshot durante la eliminación de una instancia de Astra Control Center

Si dispone de una licencia de evaluación, asegúrese de almacenar su ID de cuenta para evitar la pérdida de datos en caso de que se produzca un error en Astra Control Center si no envía los ASUP.

Limitaciones de usuarios y grupos LDAP

Astra Control Center admite hasta 5,000 grupos remotos y 10,000 usuarios remotos.

Astra Control no admite una entidad LDAP (usuario o grupo) que tenga un DN que contenga un RDN con un espacio '\' o final.

Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible

Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Astra Control Center no valida los detalles introducidos para su servidor proxy

Asegúrese de que usted "introduzca los valores correctos" al establecer una conexión.

Las conexiones existentes a un pod Postgres provocan fallos

Cuando realice operaciones en pods Postgres, no debe conectarse directamente dentro del pod para utilizar el comando psql. Astra Control requiere acceso psql para congelar y descongelar las bases de datos. Si existe una conexión preexistente, se producirá un error en la snapshot, el backup o el clon.

La página Actividad muestra hasta 100000 eventos

La página Actividad de Astra Control puede mostrar hasta 100.000 eventos. Para ver todos los eventos registrados, recupere los eventos mediante "API de control Astra".

SnapMirror no admite aplicaciones que utilizan NVMe over TCP para back-ends de almacenamiento

Astra Control Center no admite la replicación de SnapMirror de NetApp para back-ends de almacenamiento que utilizan el protocolo NVMe over TCP.

Obtenga más información

- "Problemas conocidos"

Manos a la obra

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
- Migre aplicaciones y datos de un clúster de Kubernetes a otro
- Replicar aplicaciones en un sistema remoto mediante la tecnología SnapMirror de NetApp (Astra Control Center)
- Clone aplicaciones de almacenamiento provisional a producción
- Visualizar el estado de la protección y el estado de la aplicación
- Trabaje con una interfaz de usuario web o una API para implementar sus 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 varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.
- **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.

	Servicio de control Astra	**Astra Control Center**
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En un cloud público que elija NetApp	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización

	Servicio de control Astra	Astra Control Center

¿Cuáles son las distribuciones de Kubernetes compatibles?	• * Proveedores en la nube*
	  ◦ Amazon Web Services
	  ▪ Amazon Elastic Kubernetes Service (EKS)
	  ◦ Google Cloud
	  ▪ Google Kubernetes Engine (GKE)
	  ◦ Microsoft Azure
	  ▪ Azure Kubernetes Service (AKS)
	• **Clusters autogestionados**
	  ◦ Kubernetes (ascendente)
	  ◦ Motor Kubernetes de rancher (RKE)
	  ◦ OpenShift Container Platform de Red Hat
	• * Clústeres locales*
	  ◦ Red Hat OpenShift Container Platform en las instalaciones
		• 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

	Servicio de control Astra	Astra Control Center
¿Cuáles son los back-ends de almacenamiento compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX para ONTAP de NetApp ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disco persistente de Google ▪ Cloud Volumes Service de NetApp ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Discos gestionados de Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Clusters autogestionados** ◦ Amazon EBS ◦ Discos gestionados de Azure ◦ Disco persistente de Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "El Longhorn" • * Clústeres locales* ◦ NetApp MetroCluster ◦ Sistemas ONTAP AFF y FAS de NetApp ◦ ONTAP Select de NetApp ◦ "Cloud Volumes ONTAP" ◦ "El Longhorn"	• Sistemas ONTAP AFF y FAS de NetApp • ONTAP Select de NetApp • "Cloud Volumes ONTAP" • "El Longhorn"

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 inscríbase 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 Azure gestionó discos 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 el nuevo rol de administrador para instalar el enlace../concepts/architecture#astra-control-components[Astra Control Provisioner^] en el clúster y crear una o varias clases de almacenamiento.
    - Si utilizas una oferta de almacenamiento de servicios en la nube de NetApp como back-end de almacenamiento, el servicio Astra Control utiliza el aprovisionador de control de Astra para aprovisionar volúmenes persistentes para tus aplicaciones. Si utiliza discos administrados de Amazon EBS o Azure como back-end de almacenamiento, deberá instalar un controlador CSI específico del proveedor. Se proporcionan instrucciones de instalación en "Configure Amazon Web Services" y.. "Configure Microsoft Azure con discos gestionados de Azure".
- 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 espacios de nombres en su cuenta. Si desea gestionar más de 10, deberá configurar la facturación actualizando 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 admite los clústeres de Kubernetes con un tipo de almacenamiento configurado por el aprovisionador de Astra Control con un back-end de almacenamiento de ONTAP.

La supervisión y la telemetría 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) a través de 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.

Puedes probar Astra Control Center con una licencia de evaluación integrada de 90 días. Mientras estás evaluando Astra Control Center, puedes obtener soporte a través del correo electrónico y las opciones de la comunidad. 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".

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 Trident"
- "Documentación de la API de Astra Control"
- "Documentación de ONTAP"

Requisitos del Centro de Control de Astra

Comience verificando la preparación de su entorno operativo, clústeres de aplicaciones, aplicaciones, licencias y explorador web. Asegúrate de que tu entorno cumpla con estos requisitos para poner en marcha y operar Astra Control Center.

Entornos de Kubernetes de clústeres host admitidos

Astra Control Center se ha validado con los siguientes entornos de host de Kubernetes:

> Compruebe que el entorno de Kubernetes que elijas para alojar Astra Control Center cumpla con los requisitos básicos de recursos que se describen en la documentación oficial del entorno.

Distribución de Kubernetes en clúster de hosts	Versiones compatibles
Azure Kubernetes Service en HCI de pila de Azure	Azure Stack HCI 21H2 y 22H2 con AKS 1.24.11 a 1.26.6
Anthos de Google	1,15 a 1,16 (consulte Requisitos de incorporación de Google Anthos)

Distribución de Kubernetes en clúster de hosts	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

Requisitos de recursos del clúster de hosts

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

> Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

- **Extensiones de CPU**: Las CPU de todos los nodos del entorno de alojamiento deben tener habilitadas las extensiones AVX.
- * Nodos de trabajo*: Al menos 3 nodos de trabajo en total, con 4 núcleos de CPU y 12GB RAM cada uno
- **Requisitos de clúster de VMware Tanzu Kubernetes Grid**: Al alojar Astra Control Center en un clúster de VMware Tanzu Kubernetes Grid (TKG) o Tanzu Kubernetes Grid Integrated Edition (TKGi), tenga en cuenta las siguientes consideraciones.
  - El token predeterminado del archivo de configuración de VMware TKG y TKGi caduca diez horas después de la implementación. Si utiliza productos de la cartera de Tanzu, debe generar un archivo de configuración de tanzu Kubernetes Cluster con un token que no caduca para evitar problemas de conexión entre Astra Control Center y clústeres de aplicaciones administradas. Si desea obtener instrucciones, visite "La documentación de producto del centro de datos NSX-T de VMware."
  - Utilice la `kubectl get nsxlbmonitors -A` comando para ver si ya tiene un monitor de servicio configurado para aceptar tráfico de entrada. Si existe una, no debe instalar MetalLB, ya que el monitor de servicio existente anulará cualquier nueva configuración de equilibrador de carga.
  - Desactive la implementación predeterminada de la clase de almacenamiento TKG o TKGi en cualquier cluster de aplicaciones que Astra Control deba gestionar. Para ello, edite la `TanzuKubernetesCluster` recurso en el clúster de espacio de nombres.
  - Ten en cuenta los requisitos específicos para el aprovisionador de Astra Control al implementar Astra Control Center en un entorno TKG o TKGi:
    - El clúster debe admitir cargas de trabajo con privilegios.
    - La `--kubelet-dir` el indicador se debe establecer en la ubicación del directorio kubelet. De forma predeterminada, esta es `/var/vcap/data/kubelet`.
    - Especificación de la ubicación del kubelet mediante `--kubelet-dir` Sabe que funciona para el operador, Helm y. `tridentctl` implementaciones.

Requisitos de malla de servicio

Se recomienda instalar una versión vanilla compatible de la malla de servicio de Istio en el clúster de hosts de

Astra Control Center. Consulte "versiones compatibles" Para versiones compatibles de Istio. Los lanzamientos de marca de la malla de servicio de Istio, como OpenShift Service Mesh, no están validados con Astra Control Center.

Para integrar Astra Control Center con la malla de servicio de Istio instalada en el clúster de hosts, es necesario hacer la integración como parte de un Astra Control Center "instalación" y no independiente de este proceso.

> La instalación y el uso de Astra Control Center sin configurar una malla de servicio en el clúster de host tiene implicaciones de seguridad potencialmente graves.

Astra Trident

Si piensa utilizar Astra Trident en lugar de Astra Control Provisioner con esta versión, se admiten Astra Trident 23,04 y las versiones posteriores. Astra Control Center requerirá Aprovisionador de Astra Control en futuras versiones.

Aprovisionador de Astra Control

Para usar la funcionalidad de almacenamiento avanzada del aprovisionador de Astra Control, debe instalar Astra Trident 23,10 o una versión posterior y habilitarla "Funcionalidad de aprovisionamiento Astra Control". Para utilizar las funcionalidades del aprovisionador de control de Astra más recientes, necesitarás las versiones más recientes de Astra Trident y Astra Control Center.

- **Versión mínima de Astra Control Provisionador para usar con Astra Control Center**: Astra Control Provisionador 23,10 o posterior instalado y configurado.

Configuración de ONTAP con Astra Trident

- **Clase de almacenamiento**: Configure al menos una clase de almacenamiento en el clúster. Si se configura una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento con la designación predeterminada.
- **Controladores de almacenamiento y nodos de trabajo**: Asegúrese de configurar los nodos de trabajo en su clúster con los controladores de almacenamiento adecuados para que los pods puedan interactuar con el almacenamiento de backend. Astra Control Center es compatible con los siguientes controladores de ONTAP proporcionados por Astra Trident:
  - `ontap-nas`
  - `ontap-san`
  - `ontap-san-economy` (la replicación de aplicaciones no está disponible con este tipo de clase de almacenamiento)
  - `ontap-nas-economy` (las instantáneas y las políticas de replicación de aplicaciones no están disponibles con este tipo de clase de almacenamiento)

Back-ends de almacenamiento

Asegúrese de tener un backend soportado con capacidad suficiente.

- * Capacidad de almacenamiento de backend requerida*: Al menos 500GB disponibles
- **Backends soportados**: Astra Control Center soporta los siguientes backends de almacenamiento:

- Sistemas NetApp ONTAP 9.9.1 o posteriores AFF, FAS y ASA
- NetApp ONTAP Select 9.9.1 o posterior
- NetApp Cloud Volumes ONTAP 9.9.1 o posterior
- (Para la vista previa técnica de Centro de control de Astra) NetApp ONTAP 9.10.1 o posterior para operaciones de protección de datos que se proporcionan como versión preliminar técnica
- Longhorn 1.5.0 o posterior
  - Requiere la creación manual de un objeto VolumeSnapshotClass. Consulte la "Documentación de Longhorn" si desea obtener instrucciones.
- NetApp MetroCluster
  - Los clústeres de Kubernetes gestionados deben tener una configuración con ampliación.
- Back-ends de almacenamiento disponibles con proveedores de cloud admitidos

Licencias ONTAP

Para utilizar Astra Control Center, compruebe que dispone de las siguientes licencias de ONTAP, en función de lo que necesite:

- FlexClone
- SnapMirror: Opcional. Solo es necesario para la replicación en sistemas remotos mediante la tecnología SnapMirror. Consulte "Información sobre licencias de SnapMirror".
- Licencia de S3: Opcional. Solo se necesita para bloques ONTAP S3

Para comprobar si su sistema ONTAP tiene las licencias necesarias, consulte "Gestione licencias de ONTAP".

NetApp MetroCluster

Cuando usa NetApp MetroCluster como back-end de almacenamiento, tiene que hacer lo siguiente:

- Especifique una LIF de gestión de SVM como opción de back-end en el controlador de Astra Trident que utilice
- Asegúrese de tener la licencia de ONTAP adecuada

Para configurar el LIF MetroCluster, consulte estas opciones y ejemplos de cada controlador:

- "SAN"
- "NAS"

Licencia de Astra Control Center

Se requiere una licencia de Astra Control Center. Al instalar Astra Control Center, ya está activada una licencia de evaluación de 90 días para 4.800 CPU. Si necesita más capacidad o diferentes términos de evaluación, o si desea actualizar a una licencia completa, puede obtener otra licencia de evaluación o una licencia completa de NetApp. Necesita una licencia para proteger sus aplicaciones y datos.

Para probar Astra Control Center, regístrate para obtener una prueba gratuita. Puede registrarse registrándose "aquí".

Para configurar la licencia, consulte "utilice una licencia de evaluación de 90 días".

Para obtener más información sobre cómo funcionan las licencias, consulte "Licencia".

Requisitos de red

Configura tu entorno operativo para garantizar que Astra Control Center se pueda comunicar correctamente. Se requieren las siguientes configuraciones de red:

- **Dirección FQDN**: Debes tener una dirección FQDN para Astra Control Center.
- **Acceso a internet**: Debes determinar si tienes acceso externo a internet. Si no lo hace, es posible que algunas funcionalidades se vean limitadas, por ejemplo, enviar paquetes de soporte al "Sitio de soporte de NetApp".
- **Acceso al puerto**: El entorno operativo que aloja Astra Control Center se comunica mediante los siguientes puertos TCP. Debe asegurarse de que estos puertos estén permitidos a través de cualquier firewall y configurar firewalls para permitir que cualquier tráfico de salida HTTPS que se origine en la red Astra. Algunos puertos requieren conectividad de ambos modos entre el entorno que aloja Astra Control Center y cada clúster gestionado (se indica si procede).

> Puede poner en marcha Astra Control Center en un clúster de Kubernetes de doble pila y Astra Control Center puede gestionar las aplicaciones y los back-ends de almacenamiento que se hayan configurado para un funcionamiento de doble pila. Para obtener más información sobre los requisitos de los clústeres de doble pila, consulte "Documentación de Kubernetes".

Origen	Destino	Puerto	Protocolo	Específico
PC cliente	Astra Control Center	443	HTTPS	Acceso IU/API: Asegúrese de que este puerto esté abierto en ambas direcciones entre Astra Control Center y el sistema utilizado para acceder a Astra Control Center
Consumidor de métricas	Nodo de trabajo de Astra Control Center	9090	HTTPS	Comunicación de datos de métricas: Asegúrese de que cada clúster gestionado pueda acceder a este puerto en el clúster que aloja a Astra Control Center (se requiere una comunicación bidireccional)
Astra Control Center	Proveedor de bloques de almacenamiento Amazon S3	443	HTTPS	Comunicación del almacenamiento de Amazon S3

Origen	Destino	Puerto	Protocolo	Específico
Astra Control Center	AutoSupport de NetApp	443	HTTPS	Comunicación AutoSupport de NetApp
Astra Control Center	Clúster de Kubernetes gestionado	443/6443 **NOTA**: El puerto que utiliza el clúster administrado puede variar dependiendo del clúster. Consulte la documentación del proveedor de software del clúster.	HTTPS	Comunicación con el clúster gestionado: Asegúrese de que este puerto esté abierto en ambos sentidos entre el clúster que aloja Astra Control Center y cada clúster gestionado

Entrada para clústeres de Kubernetes en las instalaciones

Puede elegir el tipo de entrada de red que utiliza Astra Control Center. De forma predeterminada, Astra Control Center implementa la puerta de enlace Astra Control Center (service/trafik) como un recurso para todo el clúster. Astra Control Center también admite el uso de un equilibrador de carga de servicio, si están permitidos en su entorno. Si prefiere utilizar un equilibrador de carga de servicio y aún no tiene uno configurado, puede utilizar el equilibrador de carga de MetalLB para asignar automáticamente una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga.

> El equilibrador de carga debe utilizar una dirección IP ubicada en la misma subred que las direcciones IP del nodo de trabajo de Astra Control Center.

Para obtener más información, consulte "Configure la entrada para el equilibrio de carga".

Requisitos de incorporación de Google Anthos

Cuando alojes Astra Control Center en un clúster Anthos de Google, ten en cuenta que Google Anthos incluye de forma predeterminada el equilibrador de carga MetalLB y el servicio Istio Ingress, lo que te permite usar simplemente las capacidades genéricas de ingreso de Astra Control Center durante la instalación. Consulte "Documentación de instalación de Astra Control Center" para obtener más detalles.

Exploradores web compatibles

Astra Control Center es compatible con las versiones recientes de Firefox, Safari y Chrome con una resolución mínima de 1280 x 720.

Requisitos adicionales para clusters de aplicaciones

Tenga en cuenta estos requisitos si planea utilizar estas funciones de Astra Control Center:

- **Requisitos del clúster de aplicaciones**: "Requisitos de gestión de clústeres"
  - **Requisitos de aplicación gestionada**: "Y gestión de aplicaciones"
  - **Requisitos adicionales para la replicación de aplicaciones**: "Requisitos previos de replicación"

El futuro

Vea la "inicio rápido" descripción general.

Inicio rápido para Astra Control Center

A continuación se ofrece una descripción general de los pasos necesarios para empezar con Astra Control Center. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

1 Revise los requisitos del clúster de Kubernetes

Asegúrese de que su entorno cumple estos requisitos:

Clúster de Kubernetes

- "Asegúrese de que el clúster de hosts cumple los requisitos de entorno operativo"
- "Configure el ingreso para el balanceo de carga en los clústeres de Kubernetes de las instalaciones"

Integración de almacenamiento

- "Compruebe que tu entorno incluye el aprovisionador de Astra Control"
- "Habilita las funciones avanzadas de gestión y aprovisionamiento de almacenamiento de Astra Control Provisioner"
- "Preparar nodos de trabajo de cluster"
- "Configurar los back-ends de almacenamiento"
- "Configure las clases de almacenamiento"
- "Instale una controladora Snapshot de volumen"
- "Cree una clase de snapshot de volumen"

Credenciales de ONTAP

- "Configure las credenciales de ONTAP"

2 Descargue e instale Astra Control Center

Complete estas tareas de instalación:

- "Descargue Astra Control Center desde la página de descargas del sitio de soporte de NetApp"
- Obtenga el archivo de licencia de NetApp:
  - Si está evaluando Astra Control Center, ya hay una licencia de evaluación integrada incluida
  - "Si ya ha adquirido Astra Control Center, genere su archivo de licencia"
- "Instalar Astra Control Center"
- "Realice pasos de configuración opcionales adicionales"

Complete algunas tareas de configuración inicial

Complete algunas tareas básicas para comenzar:

- "Añadir una licencia"
- "Preparar el entorno para la gestión de clústeres"
- "Añadir un clúster"
- "Añada un back-end de almacenamiento"
- "Añadir un bucket"

Utilice Astra Control Center

Cuando termine de configurar Astra Control Center, utiliza la interfaz de usuario de Astra Control o el "API de control Astra" para comenzar a administrar y proteger aplicaciones:

- "Gestionar cuentas": Usuarios, roles, LDAP, credenciales y más.
- "Gestionar notificaciones"
- "Gestionar aplicaciones": Definir recursos para gestionar.
- "Proteja sus aplicaciones": Configurar directivas de protección y replicar, clonar y migrar aplicaciones.

Si quiere más información

- "Utilice la API Astra Control"
- "Actualice Astra Control Center"
- "Obtenga ayuda con Astra Control"

Información general de la instalación

Elija y complete uno de los siguientes procedimientos de instalación de Astra Control Center:

- "Instale Astra Control Center mediante el proceso estándar"
- "(Si utiliza Red Hat OpenShift) instale Astra Control Center mediante OpenShift OperatorHub"
- "Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP"

En función de su entorno, es posible que se necesite una configuración adicional después de instalar Astra Control Center:

- "Configurar Astra Control Center después de la instalación"

Instale Astra Control Center mediante el proceso estándar

Para instalar Astra Control Center, descargue las imágenes de instalación y siga estos pasos. Puede utilizar este procedimiento para instalar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Para ver una demostración del proceso de instalación de Astra Control Center, consulte "este vídeo".

Antes de empezar

- **Cumplir con los requisitos ambientales**: "Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center".

  Pon en marcha Astra Control Center en un tercer dominio de fallo o sitio secundario. Esto se recomienda para la replicación de aplicaciones y la recuperación ante desastres fluida.

- **Asegurar servicios saludables**: Comprueba que todos los servicios API estén en buen estado y disponibles:

```
kubectl get apiservices
```

- **Asegúrese de que un FQDN enrutable**: El FQDN de Astra que planea utilizar se puede enrutar al clúster. Esto significa que tiene una entrada DNS en el servidor DNS interno o que está utilizando una ruta URL principal que ya está registrada.
- **Configurar gestor de cert**: Si ya existe un gestor de cert en el clúster, debe realizar algunos "requisitos previos" Por lo tanto, Astra Control Center no intenta instalar su propio administrador de certificados. De forma predeterminada, Astra Control Center instala su propio administrador de certificados durante la instalación.
- **(Solo controlador SAN de ONTAP) Habilitar acceso múltiple**: Si está utilizando un controlador SAN de ONTAP, asegúrese de que la opción multivía esté habilitada en todos sus clústeres de Kubernetes.

También debe tener en cuenta lo siguiente:

- **Acceda al registro de imágenes de NetApp Astra Control**:

  Tiene la opción de obtener imágenes de instalación y mejoras de funcionalidades para Astra Control, como Astra Control Provisioner, desde el registro de imágenes de NetApp.

  a. Registra tu ID de cuenta de Astra Control que tendrás que iniciar sesión en el registro.

     Puedes ver tu ID de cuenta en la interfaz de usuario web de Astra Control Service. Selecciona el icono de la figura en la parte superior derecha de la página, selecciona **Acceso API** y escribe tu ID de cuenta.

  b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.

  c. Inicia sesión en el Registro de Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Instale una malla de servicio para comunicaciones seguras**: Se recomienda encarecidamente que los canales de comunicaciones del clúster host de Astra Control estén protegidos mediante un "malla de servicio compatible".

> La integración de Astra Control Center con una malla de servicios solo puede llevarse a cabo durante Astra Control Center "instalación" y no independiente de este proceso. No se admite el cambio de un entorno mallado a otro sin mallado.

Para el uso de la malla de servicio de Istio, deberá hacer lo siguiente:

- Agregue un `istio-injection:enabled` etiqueta En el espacio de nombres de Astra antes de poner en marcha Astra Control Center.
- Utilice la `Generic` ajuste de entrada y proporcionar una entrada alternativa para equilibrio de carga externo.
- Para los clústeres de Red Hat OpenShift, debe definirlos `NetworkAttachmentDefinition` En todos los espacios de nombres del Centro de control de Astra asociados (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` para clusters de aplicaciones o cualquier espacio de nombres personalizado que se haya sustituido).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

Pasos

Para instalar Astra Control Center, lleve a cabo los siguientes pasos:

- Descargue y extraiga Astra Control Center
- Complete los pasos adicionales si utiliza un registro local
- Configurar espacio de nombres y secreto para registros con requisitos de autenticación
- Instale el operador de Astra Control Center
- Configurar Astra Control Center

- Complete la instalación del centro de control de Astra y del operador
- Comprobar el estado del sistema
- Configure la entrada para el equilibrio de carga
- Inicie sesión en la interfaz de usuario de Astra Control Center

> No elimine el operador Astra Control Center (por ejemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) En cualquier momento durante la instalación o el funcionamiento de Astra Control Center para evitar la eliminación de las dosis.

Descargue y extraiga Astra Control Center

Descargue las imágenes del Centro de control de Astra de una de las siguientes ubicaciones:

- **Registro de imágenes del Servicio de control de Astra**: Utilice esta opción si no utiliza un registro local con las imágenes del Centro de control de Astra o si prefiere este método a la descarga del paquete desde el Sitio de soporte de NetApp.
- **Sitio de soporte de NetApp**: Utilice esta opción si utiliza un registro local con las imágenes del Centro de control de Astra.

Registro de imágenes de Astra Control

1. Inicia sesión en el servicio Astra Control.
2. En el Dashboard, selecciona **Desplegar una instancia autogestionada de Astra Control**.
3. Sigue las instrucciones para iniciar sesión en el registro de imágenes de Astra Control, extraer la imagen de instalación de Astra Control Center y extraer la imagen.

Sitio de soporte de NetApp

1. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete.

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig astra-
   control-center-[version].tar.gz
   ```

   Se mostrará la salida `Verified OK` después de una verificación correcta.

3. Extraiga las imágenes del paquete Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Complete los pasos adicionales si utiliza un registro local

Si tiene pensado enviar el paquete Centro de control de Astra a su registro local, debe usar el complemento de la línea de comandos kubectl de Astra de NetApp.

Instale el complemento Astra kubectl de NetApp

Complete estos pasos para instalar el plugin de línea de comandos kubectl de NetApp Astra más reciente.

Antes de empezar

NetApp proporciona binarios de complementos para diferentes arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea.

Si ya tiene instalado el plugin desde una instalación anterior, "asegúrese de tener la versión más reciente" antes de realizar estos pasos.

Pasos

1. Enumera los binarios para complementos de kubectl de Astra de NetApp disponibles:

> La biblioteca de complementos kubectl forma parte del paquete tar y se extrae en la carpeta `kubectl-astra`.

```
ls kubectl-astra/
```

2. Mueva el archivo que necesita para su sistema operativo y la arquitectura de CPU a la ruta actual y cámbiele el nombre a. `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Agregue las imágenes a su registro

1. Si planeas enviar el paquete Astra Control Center a tu registro local, completa la secuencia de pasos apropiada para tu motor de contenedores:

Docker

a. Cambie al directorio raíz del tarball. Debería ver el `acc.manifest.bundle.yaml` archivo y estos directorios:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:

- Sustituya <BUNDLE_FILE> por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
- Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio de Docker; por ejemplo, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
- Reemplace <MY_REGISTRY_USER> por el nombre de usuario.
- Sustituya <MY_REGISTRY_TOKEN> por un token autorizado para el registro.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

a. Cambie al directorio raíz del tarball. Debería ver este archivo y directorio:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

c. Prepare y ejecute una de las siguientes secuencias de comandos personalizadas para la versión de Podman que utilice. Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio que incluye cualquier subdirectorio.

```
<strong>Podman 4</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

La ruta de acceso de imagen que crea el script debe parecerse a la siguiente, dependiendo de la configuración del Registro:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Cambie el directorio:

```
cd manifests
```

Configurar espacio de nombres y secreto para registros con requisitos de autenticación

1. Exporte el comando kubeconfig del clúster de hosts de Astra Control Center:

```
export KUBECONFIG=[file path]
```

> Antes de completar la instalación, asegúrese de que su kubeconfig apunte al clúster donde desea instalar Astra Control Center.

2. Si utiliza un registro que requiere autenticación, debe hacer lo siguiente:

   a. Cree el `netapp-acc-operator` espacio de nombres:

```
kubectl create ns netapp-acc-operator
```

   b. Cree un secreto para `netapp-acc-operator` espacio de nombres. Añada información sobre Docker y ejecute el siguiente comando:

> El marcador de posición `your_registry_path` debe coincidir con la ubicación de las imágenes que ha cargado anteriormente (por ejemplo, `[Registry_URL]/netapp/astra/astracc/24.02.0-69`).

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-
operator --docker-server=cr.astra.netapp.io --docker
-username=[astra_account_id] --docker-password=[astra_api_token]
```

+

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-
operator --docker-server=[your_registry_path] --docker
-username=[username] --docker-password=[token]
```

+

> Si elimina el espacio de nombres después de que se genere el secreto, vuelva a crear el espacio de nombres y, a continuación, vuelva a generar el secreto para el espacio de nombres.

   a. Cree el `netapp-acc` (o nombre personalizado).

```
kubectl create ns [netapp-acc or custom namespace]
```

   b. Cree un secreto para `netapp-acc` (o nombre personalizado). Agregue información de Docker y

ejecute uno de los comandos adecuados en función de sus preferencias de registro:

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-
acc or custom namespace] --docker-server=cr.astra.netapp.io --docker
-username=[astra_account_id] --docker-password=[astra_api_token]
```

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-
acc or custom namespace] --docker-server=[your_registry_path]
--docker-username=[username] --docker-password=[token]
```

Instale el operador de Astra Control Center

1. (Solo registros locales) Si está utilizando un registro local, complete estos pasos:

   a. Abra el YAML de implementación del operador de Astra Control Center:

   ```
   vim astra_control_center_operator_deploy.yaml
   ```

   Una muestra anotada de AYLMA sigue estos pasos.

   b. Si utiliza un registro que requiere autenticación, reemplace la línea predeterminada de `imagePullSecrets: []` con lo siguiente:

   ```
   imagePullSecrets: [{name: astra-registry-cred}]
   ```

   c. Cambiar `ASTRA_IMAGE_REGISTRY` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

   d. Cambiar `ASTRA_IMAGE_REGISTRY` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
```

```
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_INSTALLTIMEOUT
          value: 5m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:24.02.68
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
```

```
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

2. Instale el operador de Astra Control Center:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Ampliar para respuesta de muestra:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

3. Verifique que los pods se estén ejecutando:

```
kubectl get pods -n netapp-acc-operator
```

Configurar Astra Control Center

1. Edite el archivo de recursos personalizados (CR) del Centro de control de Astra (`astra_control_center.yaml`) para realizar las configuraciones de cuenta, soporte, registro y otras necesarias:

```
vim astra_control_center.yaml
```

> Una muestra anotada de AYLMA sigue estos pasos.

2. Modifique o confirme los siguientes ajustes:

Nombre de cuenta

Ajuste	Orientación	Tipo	Ejemplo
`accountName`	Cambie el `accountName` Cadena con el nombre que desea asociar a la cuenta Astra Control Center. Sólo puede haber un nombre de cuenta.	cadena	`Example`

Versión astraVersion

Ajuste	Orientación	Tipo	Ejemplo
`astraVersion`	La versión de Astra Control Center para implementar. No se necesita ninguna acción para este ajuste, ya que el valor se rellenará previamente.	cadena	`24.02.0-69`

Dirección de astern

Ajuste	Orientación	Tipo	Ejemplo
`astraAddress`	Cambie el `astraAddress` Cadena al FQDN (recomendado) o dirección IP que desea utilizar en su navegador para acceder a Astra Control Center. Esta dirección define cómo se encontrará Astra Control Center en su centro de datos y es el mismo FQDN o la dirección IP que ha aprovisionado desde su equilibrador de carga cuando ha finalizado "Requisitos del Centro de Control de Astra". NOTA: No utilizar `http://` o. `https://` en la dirección. Copie este FQDN para utilizarlo en un paso posterior.	cadena	`astra.example.com`

AutoSupport

Sus selecciones en esta sección determinan si participará en la aplicación de soporte proactivo de NetApp, NetApp Active IQ y dónde se envían los datos. Se requiere una conexión a Internet (puerto 442) y todos los datos de soporte se anóniman.

Ajuste	Uso	Orientación	Tipo	Ejemplo
`autoSupport.enrolled`	Uno de los dos `enrolled` o. `url` los campos deben seleccionarse	Cambiar `enrolled` Para AutoSupport a. `false` para sitios sin conexión a internet o retención `true` para sitios conectados. Un valor de `true` Permite enviar datos anónimos a NetApp con fines de soporte. La elección predeterminada es `false` E indica que no se enviará ningún dato de soporte a NetApp.	Booleano	`false` (este valor es el predeterminado)
`autoSupport.url`	Uno de los dos `enrolled` o. `url` los campos deben seleccionarse	Esta URL determina dónde se enviarán los datos anónimos.	cadena	`https://support.netapp.com/asupprod/post/1.0/postAsup`

correo electrónico

Ajuste	Orientación	Tipo	Ejemplo
`email`	Cambie el `email` cadena en la dirección inicial predeterminada del administrador. Copie esta dirección de correo electrónico para su uso en un paso posterior. Esta dirección de correo electrónico se utilizará como nombre de usuario de la cuenta inicial para iniciar sesión en la interfaz de usuario y se le notificarán los eventos de Astra Control.	cadena	`admin@example.com`

Nombre

Ajuste	Orientación	Tipo	Ejemplo
`firstName`	El nombre del administrador inicial predeterminado asociado con la cuenta Astra. El nombre utilizado aquí aparecerá en un encabezado de la interfaz de usuario después del primer inicio de sesión.	cadena	`SRE`

Apellidos

Ajuste	Orientación	Tipo	Ejemplo
`lastName`	Apellido del administrador inicial predeterminado asociado con la cuenta Astra. El nombre utilizado aquí aparecerá en un encabezado de la interfaz de usuario después del primer inicio de sesión.	cadena	`Admin`

ImageRegistry

Las selecciones realizadas en esta sección definen el registro de imágenes del contenedor que aloja las imágenes de la aplicación Astra, el operador del centro de control Astra y el repositorio de Astra Control Center Helm.

Ajuste	Uso	Orientación	Tipo	Ejemplo
`imageRegistry.name`	Obligatorio	El nombre del registro de imágenes de Astra Control, que aloja todas las imágenes necesarias para implementar Astra Control Center. El valor se rellenará previamente y no será necesario realizar ninguna acción a menos que haya configurado un registro local. Para un registro local, reemplace este valor existente por el nombre del registro de imágenes donde insertó las imágenes en el paso anterior. No utilizar `http://` o. `https://` en el nombre del registro.	cadena	`cr.astra.netapp.io` (predeterminado) `example.registry.com/astra` (ejemplo de registro local)

Ajuste	Uso	Orientación	Tipo	Ejemplo
`imageRegistry.secret`	Opcional	El nombre del secreto Kubernetes utilizado para autenticarse con el registro de imágenes. El valor se rellenará previamente y no será necesario realizar ninguna acción a menos que haya configurado un registro local y la cadena que haya introducido para ese registro en `imageRegistry.name` requiere un secreto. IMPORTANTE: Si está utilizando un registro local que no requiere autorización, debe eliminarlo `secret` línea dentro `imageRegistry` o se producirá un error en la instalación.	cadena	`astra-registry-cred`

Clase de almacenamiento

Ajuste	Orientación	Tipo	Ejemplo
`storageClass`	Cambie el `storageClass` valor desde `ontap-gold` A otro recurso de Storage Class según lo requiera la instalación. Ejecute el comando `kubectl get sc` para determinar las clases de almacenamiento configuradas existentes. Una de las clases de almacenamiento configuradas por el aprovisionador de Astra Control debe introducirse en el archivo de manifiesto (`astra-control-center-<version>.manifest`) Y se utilizará para Astra PVs. Si no está establecida, se utilizará la clase de almacenamiento predeterminada. NOTA: Si se ha configurado una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento que tiene la anotación predeterminada.	cadena	`ontap-gold`

VolumeReclaimPolicy

Ajuste	Orientación	Tipo	Opciones
`volumeReclaimPolicy`	De esta forma se establece la política de reclamaciones para los vehículos de Astra. Configuración de esta directiva como `Retain` Conserva los volúmenes persistentes una vez que Astra se elimina. Configuración de esta directiva como `Delete` elimina los volúmenes persistentes después de eliminar astra. Si no se establece este valor, se conservan los VP.	cadena	• `Retain` (Este es el valor predeterminado) • `Delete`

IngresType

Ajuste	Orientación	Tipo	Opciones
`ingressType`	Utilice uno de los siguientes tipos de entrada: **Genérico** (`ingressType: "Generic"`) (Predeterminado) Utilice esta opción cuando tenga otro controlador de entrada en uso o prefiera utilizar su propio controlador de entrada. Después de poner en marcha Astra Control Center, será necesario configurar el "controlador de entrada" Para exponer Astra Control Center con una URL. IMPORTANTE: Si va a utilizar una malla de servicio con Astra Control Center, debe seleccionar `Generic` como tipo de ingreso y configure el suyo propio "controlador de entrada". **AccTraefik** (`ingressType: "AccTraefik"`) Utilice esta opción cuando prefiera no configurar un controlador de entrada. Esto despliega el Astra Control Center `traefik` Puerta de enlace como servicio de tipo Kubernetes LoadBalancer. Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le	cadena	• `Generic` (este es el valor predeterminado) • `AccTraefik`

Tamaño escalonado

Ajuste	Orientación	Tipo	Opciones
`scaleSize`	De forma predeterminada, Astra utilizará la alta disponibilidad (HA) `scaleSize` de `Medium`, Que despliega la mayoría de los servicios en HA y despliega múltiples réplicas para redundancia. Con `scaleSize` como `Small`, Astra reducirá el número de réplicas para todos los servicios excepto los servicios esenciales para reducir el consumo. CONSEJO: `Medium` las puestas en marcha constan de unos 100 pods (sin incluir cargas de trabajo transitorias. 100 pod se basa en la configuración de tres nodos principales y tres nodos de trabajador). Tenga en cuenta las limitaciones de límites de red por pod que pueden ser un problema en su entorno, sobre todo cuando tenga en cuenta situaciones de recuperación ante desastres.	cadena	• `Small` • `Medium` (Este es el valor predeterminado)

Recursos astrarScaler

Ajuste	Orientación	Tipo	Opciones
`astraResourcesScaler`	Opciones de escalado para los límites de recursos de AstraControlCenter. De forma predeterminada, Astra Control Center se despliega con solicitudes de recursos establecidas para la mayoría de los componentes de Astra. Esta configuración permite que la pila de software de Astra Control Center tenga un mejor rendimiento en entornos con un mayor nivel de carga y escalabilidad de las aplicaciones. Sin embargo, en situaciones que utilizan grupos de desarrollo o pruebas más pequeños, el campo CR `astraResourcesScalar` se puede establecer en `Off`. De este modo se deshabilitan las solicitudes de recursos y se puede implementar en clústeres más pequeños.	cadena	• `Default` (Este es el valor predeterminado) • `Off`

Valores adicionales

Añada los siguientes valores adicionales a Astra Control Center CR para evitar un problema conocido en la instalación:

```
additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

crds

Sus selecciones en esta sección determinan cómo Astra Control Center debe manejar los CRD.

Ajuste	Orientación	Tipo	Ejemplo
`crds.externalCertManager`	Si utiliza un administrador de certificados externo, cambie `externalCertManager` para `true`. El valor predeterminado `false` Hace que Astra Control Center instale sus propios CRD de administrador de certificados durante la instalación. Los crds son objetos de todo el clúster y su instalación podría tener un impacto en otras partes del clúster. Puede utilizar este indicador para indicar a Astra Control Center que el administrador del clúster instalará y gestionará estos CRD fuera de Astra Control Center.	Booleano	`False` (este valor es el predeterminado)
`crds.externalTraefik`	De forma predeterminada, Astra Control Center instalará los CRD de Traefik necesarios. Los crds son objetos de todo el clúster y su instalación podría tener un impacto en otras partes del clúster. Puede utilizar este indicador para indicar a Astra Control Center que el administrador del clúster instalará y gestionará estos CRD fuera de Astra Control Center.	Booleano	`False` (este valor es el predeterminado)

Asegúrese de haber seleccionado la clase de almacenamiento y el tipo de entrada correctos para la configuración antes de completar la instalación.

muestra astrara_control_center.yaml

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[cr.astra.netapp.io or your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
  crds:
    externalTraefik: false
    externalCertManager: false
```

Complete la instalación del centro de control de Astra y del operador

1. Si todavía no lo ha hecho en un paso anterior, cree el `netapp-acc` espacio de nombres (o personalizado):

   ```
   kubectl create ns [netapp-acc or custom namespace]
   ```

2. Si usas una malla de servicio con Astra Control Center, agrega la siguiente etiqueta a la `netapp-acc` o espacio de nombres personalizado:

Su tipo de ingreso (`ingressType`) debe establecerse en `Generic` En Astra Control Center CR antes de continuar con este comando.

```
kubectl label ns [netapp-acc or custom namespace] istio-
injection:enabled
```

3. (Recomendado) "Activar MTLS estricto" Para la malla de servicio de Istio:

```
kubectl apply -n istio-system -f - <<EOF
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
spec:
  mtls:
    mode: STRICT
EOF
```

4. Instale Astra Control Center en `netapp-acc` (o su espacio de nombres personalizado):

```
kubectl apply -f astra_control_center.yaml -n [netapp-acc or custom
namespace]
```

El operador del Centro de control de Astra realizará una comprobación automática de los requisitos del entorno. Ausente "requisitos" Puede provocar que falle la instalación o que Astra Control Center no funcione correctamente. Consulte siguiente sección para comprobar si hay mensajes de advertencia relacionados con la comprobación automática del sistema.

Comprobar el estado del sistema

Puede verificar el estado del sistema con comandos kubectl. Si prefiere utilizar OpenShift, puede utilizar comandos de OC comparables para realizar los pasos de verificación.

Pasos

1. Compruebe que el proceso de instalación no ha generado mensajes de advertencia relacionados con las comprobaciones de validación:

```
kubectl get acc [astra or custom Astra Control Center CR name] -n
[netapp-acc or custom namespace] -o yaml
```

También se notifican mensajes de advertencia adicionales en los registros del operador de Astra Control Center.

2. Corrija cualquier problema del entorno que se notifique mediante las comprobaciones automatizadas de requisitos.

> Puede corregir problemas garantizando que su entorno cumple con los "requisitos" Para Astra Control Center.

3. Compruebe que todos los componentes del sistema se han instalado correctamente.

```
kubectl get pods -n [netapp-acc or custom namespace]
```

Cada pod debe tener el estado de `Running`. Pueden tardar varios minutos en implementar los pods del sistema.

Amplíe para obtener una respuesta de muestra

```
acc-helm-repo-5bd77c9ddd-8wxm2             1/1     Running     0
1h
activity-5bb474dc67-8l9ss                  1/1     Running     0
1h
activity-5bb474dc67-qbrtq                  1/1     Running     0
1h
api-token-authentication-6wbj2             1/1     Running     0
1h
api-token-authentication-9pgw6             1/1     Running     0
1h
api-token-authentication-tqf6d             1/1     Running     0
1h
asup-5495f44dbd-z4kft                      1/1     Running     0
1h
authentication-6fdd899858-5x45s            1/1     Running     0
1h
bucketservice-84d47487d-n9xgp              1/1     Running     0
1h
bucketservice-84d47487d-t5jhm              1/1     Running     0
1h
cert-manager-5dcb7648c4-hbldc              1/1     Running     0
1h
cert-manager-5dcb7648c4-nr9qf              1/1     Running     0
1h
cert-manager-cainjector-59b666fb75-bk2tf   1/1     Running     0
1h
cert-manager-cainjector-59b666fb75-pfnck   1/1     Running     0
1h
cert-manager-webhook-c6f9b6796-ngz2x       1/1     Running     0
1h
cert-manager-webhook-c6f9b6796-rwtbn       1/1     Running     0
1h
certificates-5f5b7b4dd-52tnj               1/1     Running     0
1h
certificates-5f5b7b4dd-gtjbx               1/1     Running     0
1h
certificates-expiry-check-28477260-dz5vw   0/1     Completed   0
1h
cloud-extension-6f58cc579c-lzfmv           1/1     Running     0
1h
cloud-extension-6f58cc579c-zw2km           1/1     Running     0
1h
cluster-orchestrator-79dd5c8d95-qjg92      1/1     Running     0
1h
```

```
composite-compute-85dc84579c-nz82f         1/1     Running     0
1h
composite-compute-85dc84579c-wx2z2         1/1     Running     0
1h
composite-volume-bff6f4f76-789nj           1/1     Running     0
1h
composite-volume-bff6f4f76-kwnd4           1/1     Running     0
1h
credentials-79fd64f788-m7m8f               1/1     Running     0
1h
credentials-79fd64f788-qnc6c               1/1     Running     0
1h
entitlement-f69cdbd77-4p2kn                1/1     Running     0
1h
entitlement-f69cdbd77-hswm6                1/1     Running     0
1h
features-7b9585444c-7xd7m                  1/1     Running     0
1h
features-7b9585444c-dcqwc                  1/1     Running     0
1h
fluent-bit-ds-crq8m                        1/1     Running     0
1h
fluent-bit-ds-gmgq8                        1/1     Running     0
1h
fluent-bit-ds-gzr4f                        1/1     Running     0
1h
fluent-bit-ds-j6sf6                        1/1     Running     0
1h
fluent-bit-ds-v4t9f                        1/1     Running     0
1h
fluent-bit-ds-x7j59                        1/1     Running     0
1h
graphql-server-6cc684fb46-2x8lr            1/1     Running     0
1h
graphql-server-6cc684fb46-bshbd            1/1     Running     0
1h
hybridauth-84599f79fd-fjc7k                1/1     Running     0
1h
hybridauth-84599f79fd-s9pmn                1/1     Running     0
1h
identity-95df98cb5-dvlmz                   1/1     Running     0
1h
identity-95df98cb5-krf59                   1/1     Running     0
1h
influxdb2-0                                1/1     Running     0
1h
```

```
keycloak-operator-6d4d688697-cfq8b         1/1     Running     0
1h
krakend-5d5c8f4668-7bq8g                   1/1     Running     0
1h
krakend-5d5c8f4668-t8hbn                   1/1     Running     0
1h
license-689cdd4595-2gsc8                   1/1     Running     0
1h
license-689cdd4595-g6vwk                   1/1     Running     0
1h
login-ui-57bb599956-4fwgz                  1/1     Running     0
1h
login-ui-57bb599956-rhztb                  1/1     Running     0
1h
loki-0                                     1/1     Running     0
1h
metrics-facade-846999bdd4-f7jdm            1/1     Running     0
1h
metrics-facade-846999bdd4-lnsxl            1/1     Running     0
1h
monitoring-operator-6c9d6c4b8c-ggkrl       2/2     Running     0
1h
nats-0                                     1/1     Running     0
1h
nats-1                                     1/1     Running     0
1h
nats-2                                     1/1     Running     0
1h
natssync-server-6df7d6cc68-9v2gd           1/1     Running     0
1h
nautilus-64b7fbdd98-bsgwb                  1/1     Running     0
1h
nautilus-64b7fbdd98-djlhw                  1/1     Running     0
1h
openapi-864584bccc-75nlv                   1/1     Running     0
1h
openapi-864584bccc-zh6bx                   1/1     Running     0
1h
polaris-consul-consul-server-0             1/1     Running     0
1h
polaris-consul-consul-server-1             1/1     Running     0
1h
polaris-consul-consul-server-2             1/1     Running     0
1h
polaris-keycloak-0                         1/1     Running     2 (1h
ago)      1h
```

```
polaris-keycloak-1                          1/1     Running     0
1h
polaris-keycloak-db-0                       1/1     Running     0
1h
polaris-keycloak-db-1                       1/1     Running     0
1h
polaris-keycloak-db-2                       1/1     Running     0
1h
polaris-mongodb-0                           1/1     Running     0
1h
polaris-mongodb-1                           1/1     Running     0
1h
polaris-mongodb-2                           1/1     Running     0
1h
polaris-ui-66476dcf87-f6s8j                 1/1     Running     0
1h
polaris-ui-66476dcf87-ztjk7                 1/1     Running     0
1h
polaris-vault-0                             1/1     Running     0
1h
polaris-vault-1                             1/1     Running     0
1h
polaris-vault-2                             1/1     Running     0
1h
public-metrics-bfc4fc964-x4m79              1/1     Running     0
1h
storage-backend-metrics-7dbb88d4bc-g78cj    1/1     Running     0
1h
storage-provider-5969b5df5-hjvcm            1/1     Running     0
1h
storage-provider-5969b5df5-r79ld            1/1     Running     0
1h
task-service-5fc9dc8d99-4q4f4               1/1     Running     0
1h
task-service-5fc9dc8d99-8l5zl               1/1     Running     0
1h
task-service-task-purge-28485735-fdzkd      1/1     Running     0
12m
telegraf-ds-2rgm4                           1/1     Running     0
1h
telegraf-ds-4qp6r                           1/1     Running     0
1h
telegraf-ds-77frs                           1/1     Running     0
1h
telegraf-ds-bc725                           1/1     Running     0
1h
```

```
telegraf-ds-cvmxf                          1/1     Running     0
1h
telegraf-ds-tqzgj                          1/1     Running     0
1h
telegraf-rs-5wtd8                          1/1     Running     0
1h
telemetry-service-6747866474-5djnc         1/1     Running     0
1h
telemetry-service-6747866474-thb7r         1/1     Running     1 (1h
ago)      1h
tenancy-5669854fb6-gzdzf                   1/1     Running     0
1h
tenancy-5669854fb6-xvsm2                   1/1     Running     0
1h
traefik-8f55f7d5d-4lgfw                    1/1     Running     0
1h
traefik-8f55f7d5d-j4wt6                    1/1     Running     0
1h
traefik-8f55f7d5d-p6gcq                    1/1     Running     0
1h
trident-svc-7cb5bb4685-54cnq               1/1     Running     0
1h
trident-svc-7cb5bb4685-b28xh               1/1     Running     0
1h
vault-controller-777b9bbf88-b5bqt          1/1     Running     0
1h
vault-controller-777b9bbf88-fdfd8          1/1     Running     0
1h
```

4. (Opcional) Vea el `acc-operator` registros para supervisar el progreso:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

> `accHost` el registro del clúster es una de las últimas operaciones y, si no se produce un error en la implementación, no provocará un error. En el caso de que se produzca un error de registro del clúster que se indica en los registros, puede volver a intentar realizar el registro a través de la "Añada el flujo de trabajo del clúster en la interfaz de usuario de" O API.

5. Cuando todos los pods estén en ejecución, verifique que la instalación se haya realizado correctamente (`READY` es `True`) Y obtén la contraseña de configuración inicial que usarás cuando inicies sesión en Astra Control Center:

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Respuesta:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  24.02.0-69
10.111.111.111  True
```

> Copie el valor de UUID. La contraseña es `ACC-` Seguido del valor UUID (`ACC-[UUID]` o, en este ejemplo, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Configure la entrada para el equilibrio de carga

Puede configurar un controlador de entrada de Kubernetes que gestione el acceso externo a los servicios. Estos procedimientos proporcionan ejemplos de configuración para un controlador de entrada si utilizó el valor predeterminado de `ingressType: "Generic"` En el recurso personalizado Astra Control Center (`astra_control_center.yaml`). No es necesario utilizar este procedimiento si se ha especificado `ingressType: "AccTraefik"` En el recurso personalizado Astra Control Center (`astra_control_center.yaml`).

Después de poner en marcha Astra Control Center, deberás configurar la controladora de entrada para exponer Astra Control Center con una URL.

Los pasos de configuración varían en función del tipo de controlador de entrada que utilice. Astra Control Center admite muchos tipos de controladores Ingress. Estos procedimientos de configuración proporcionan pasos de ejemplo para algunos tipos de controladores de entrada comunes.

Antes de empezar

- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.

Pasos para la entrada de Istio

1. Configurar la entrada de Istio.

   > En este procedimiento se asume que Istio se implementa utilizando el perfil de configuración "predeterminado".

2. Recopile o cree el certificado y el archivo de claves privadas deseados para la puerta de enlace de entrada.

   Es posible usar un certificado firmado por CA o autofirmado. El nombre común debe ser la dirección Astra (FQDN).

   Comando de ejemplo:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

3. Cree un secreto `tls secret name` de tipo `kubernetes.io/tls` Para una clave privada TLS y un certificado en `istio-system namespace` Tal como se describe en los secretos TLS.

   Comando de ejemplo:

```
kubectl create secret tls [tls secret name] --key="tls.key"
--cert="tls.crt" -n istio-system
```

> El nombre del secreto debe coincidir con el `spec.tls.secretName` proporcionado en `istio-ingress.yaml` archivo.

4. Implemente un recurso de entrada en `netapp-acc` espacio de nombres (o con nombre personalizado) mediante el tipo de recurso v1 para un esquema (`istio-Ingress.yaml` se utiliza en este ejemplo):

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Aplicar los cambios:

```
kubectl apply -f istio-Ingress.yaml
```

6. Compruebe el estado de la entrada:

```
kubectl get ingress -n [netapp-acc or custom namespace]
```

Respuesta:

```
NAME    CLASS HOSTS             ADDRESS         PORTS   AGE
ingress istio astra.example.com 172.16.103.248  80, 443 1h
```

7. Finalice la instalación de Astra Control Center.

Pasos para el controlador de entrada Nginx

1. Cree un secreto de tipo `kubernetes.io/tls` Para una clave privada TLS y un certificado en `netapp-acc` (o nombre personalizado) como se describe en "Secretos TLS".
2. Implemente un recurso de entrada en `netapp-acc` espacio de nombres (o con nombre personalizado) mediante el tipo de recurso v1 para un esquema (`nginx-Ingress.yaml` se utiliza en este ejemplo):

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

3. Aplicar los cambios:

```
kubectl apply -f nginx-Ingress.yaml
```

> NetApp recomienda la instalación de la controladora nginx como una puesta en marcha en lugar de como una `daemonSet`.

Pasos para el controlador de entrada de OpenShift

1. Obtenga su certificado y consiga los archivos de clave, certificado y CA listos para su uso por la ruta OpenShift.
2. Cree la ruta OpenShift:

```
oc create route edge --service=traefik --port=web -n [netapp-acc or
custom namespace] --insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

Inicie sesión en la interfaz de usuario de Astra Control Center

Tras instalar Astra Control Center, cambiará la contraseña del administrador predeterminado e iniciará sesión en la consola de interfaz de usuario de Astra Control Center.

Pasos

1. En un navegador, introduzca el FQDN (incluido el `https://` prefijo) que utilizó en el `astraAddress` en la `astra_control_center.yaml` CR cuando Ha instalado Astra Control Center.
2. Acepte los certificados autofirmados si se le solicita.

   > Se puede crear un certificado personalizado después de iniciar sesión.

3. En la página de inicio de sesión de Astra Control Center, introduzca el valor utilizado `email` pulg `astra_control_center.yaml` CR cuando Ha instalado Astra Control Center, seguido de la contraseña de configuración inicial (`ACC-[UUID]`).

   > Si introduce una contraseña incorrecta tres veces, la cuenta de administrador se bloqueará durante 15 minutos.

4. Seleccione **Iniciar sesión**.
5. Cambie la contraseña cuando se le solicite.

   > Si éste es su primer inicio de sesión y olvida la contraseña y no se han creado otras cuentas de usuario administrativas, póngase en contacto con "Soporte de NetApp" para obtener ayuda para la recuperación de contraseñas.

6. (Opcional) quite el certificado TLS autofirmado existente y sustitúyalo por un "Certificado TLS personalizado firmado por una entidad de certificación (CA)".

Solucione los problemas de instalación

Si alguno de los servicios está en `Error` puede inspeccionar los registros. Busque códigos de respuesta API en la gama 400 a 500. Esos indican el lugar donde ocurrió un fracaso.

Opciones

- Para inspeccionar los registros del operador de Astra Control Center, introduzca lo siguiente:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

- Para comprobar el resultado de Astra Control Center CR:

```
kubectl get acc -n [netapp-acc or custom namespace] -o yaml
```

Procedimientos de instalación alternativos

- **Instalar con Red Hat OpenShift OperatorHub**: Utilice esto "procedimiento alternativo" Para instalar Astra Control Center en OpenShift mediante OperatorHub.
- **Instalar en la nube pública con Cloud Volumes ONTAP backend**: Uso "estos procedimientos" Para instalar Astra Control Center en Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure con un back-end de almacenamiento de Cloud Volumes ONTAP.

El futuro

- (Opcional) en función de su entorno, post-instalación completa "pasos de configuración".
- "Después de instalar Astra Control Center, iniciar sesión en la interfaz de usuario y cambiar la contraseña, querrá configurar una licencia, añadir clústeres, habilitar la autenticación, gestionar el almacenamiento y añadir buckets".

Configure un administrador de certificados externo

Si ya existe un administrador de certificados en su clúster de Kubernetes, deberá realizar algunos pasos previos para que Astra Control Center no instale su propio administrador de certificados.

Pasos

1. Confirme que tiene instalado un administrador de certificados:

   ```
   kubectl get pods -A | grep 'cert-manager'
   ```

   Respuesta de ejemplo:

   ```
   cert-manager   essential-cert-manager-84446f49d5-sf2zd              1/1
   Running    0     6d5h
   cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
   Running    0     6d5h
   cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq      1/1
   Running    0     6d5h
   ```

2. Cree un certificado/pareja de claves para `astraAddress` FQDN:

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
   tls.crt
   ```

   Respuesta de ejemplo:

```
Generating a 2048 bit RSA private key
..................+++
.......................................+++
writing new private key to 'tls.key'
```

3. Crear un secreto con archivos generados previamente:

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Respuesta de ejemplo:

```
secret/selfsigned-tls created
```

4. Cree un `ClusterIssuer` archivo que es **exactamente** el siguiente pero que incluye la ubicación del espacio de nombres donde el `cert-manager` los pods están instalados:

```yaml
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Respuesta de ejemplo:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Compruebe que el `ClusterIssuer` ha surgido correctamente. `Ready` debe ser `True` antes de poder continuar:

```
kubectl get ClusterIssuer
```

Respuesta de ejemplo:

```
NAME                        READY   AGE
astra-ca-clusterissuer      True    9s
```

6. Complete el "Proceso de instalación de Astra Control Center". Hay una "Paso de configuración necesario para el clúster YAML de Astra Control Center" En el que cambia el valor CRD para indicar que el administrador de certificados está instalado externamente. Debe completar este paso durante la instalación para que Astra Control Center reconozca al gestor de certificados externo.

Instale Astra Control Center utilizando OpenShift OperatorHub

Si utiliza Red Hat OpenShift, puede instalar Astra Control Center mediante el operador certificado de Red Hat. Utilice este procedimiento para instalar Astra Control Center desde "Catálogo de Red Hat Ecosystem" O con Red Hat OpenShift Container Platform.

Después de completar este procedimiento, debe volver al procedimiento de instalación para completar el "pasos restantes" para verificar que la instalación se ha realizado correctamente e iniciar sesión.

Antes de empezar

- **Cumplir con los requisitos ambientales**: "Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center".

> Pon en marcha Astra Control Center en un tercer dominio de fallo o sitio secundario. Esto se recomienda para la replicación de aplicaciones y la recuperación ante desastres fluida.

- * Asegurar operadores de clúster saludables y servicios API*:
  - En el clúster de OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado:

    ```
    oc get clusteroperators
    ```

  - En el clúster OpenShift, asegúrese de que todos los servicios API se encuentran en buen estado:

    ```
    oc get apiservices
    ```

- **Asegúrese de que un FQDN enrutable**: El FQDN de Astra que planea utilizar se puede enrutar al clúster. Esto significa que tiene una entrada DNS en el servidor DNS interno o que está utilizando una ruta URL principal que ya está registrada.
- **Obtenga permisos de OpenShift**: Necesitará todos los permisos necesarios y acceso a Red Hat OpenShift Container Platform para realizar los pasos de instalación descritos.
- **Configurar un administrador de cert**: Si ya existe un administrador de cert en el clúster, debe realizar algunos "requisitos previos" Por lo tanto, Astra Control Center no instala su propio administrador de certificados. De forma predeterminada, Astra Control Center instala su propio administrador de certificados durante la instalación.
- **Configurar el controlador de ingreso de Kubernetes**: Si tienes un controlador de ingreso de Kubernetes que administre el acceso externo a los servicios, como el balanceo de carga en un clúster, debes

configurarlo para usarlo con Astra Control Center:

a. Crear el espacio de nombres del operador:

```
oc create namespace netapp-acc-operator
```

b. "Completar la configuración" para el tipo de controlador de entrada.

- **(Solo controlador SAN de ONTAP) Habilitar acceso múltiple**: Si está utilizando un controlador SAN de ONTAP, asegúrese de que la opción multivía esté habilitada en todos sus clústeres de Kubernetes.

También debe tener en cuenta lo siguiente:

- **Acceda al registro de imágenes de NetApp Astra Control**:

  Tiene la opción de obtener imágenes de instalación y mejoras de funcionalidades para Astra Control, como Astra Control Provisioner, desde el registro de imágenes de NetApp.

  a. Registra tu ID de cuenta de Astra Control que tendrás que iniciar sesión en el registro.

     Puedes ver tu ID de cuenta en la interfaz de usuario web de Astra Control Service. Selecciona el icono de la figura en la parte superior derecha de la página, selecciona **Acceso API** y escribe tu ID de cuenta.

  b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.

  c. Inicia sesión en el Registro de Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Instale una malla de servicio para comunicaciones seguras**: Se recomienda encarecidamente que los canales de comunicaciones del clúster host de Astra Control estén protegidos mediante un "malla de servicio compatible".

  > La integración de Astra Control Center con una malla de servicios solo puede llevarse a cabo durante Astra Control Center "instalación" y no independiente de este proceso. No se admite el cambio de un entorno mallado a otro sin mallado.

  Para el uso de la malla de servicio de Istio, deberá hacer lo siguiente:

  - Agregue un `istio-injection:enabled` Etiqueta en el espacio de nombres de Astra antes de implementar Astra Control Center.
  - Utilice la `Generic` ajuste de entrada y proporcionar una entrada alternativa para "equilibrio de carga externo".
  - Para los clústeres de Red Hat OpenShift, deberá definirlos `NetworkAttachmentDefinition` En todos los espacios de nombres del Centro de control de Astra asociados (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` para clusters de aplicaciones o cualquier espacio de nombres personalizado que se haya sustituido).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

Pasos

- Descargue y extraiga Astra Control Center
- Complete los pasos adicionales si utiliza un registro local
- Busque la página de instalación del operador
- Instale el operador
- Instalar Astra Control Center

> No elimine el operador Astra Control Center (por ejemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) En cualquier momento durante la instalación o el funcionamiento de Astra Control Center para evitar la eliminación de las dosis.

Descargue y extraiga Astra Control Center

Descargue las imágenes del Centro de control de Astra de una de las siguientes ubicaciones:

- **Registro de imágenes del Servicio de control de Astra**: Utilice esta opción si no utiliza un registro local con las imágenes del Centro de control de Astra o si prefiere este método a la descarga del paquete desde el Sitio de soporte de NetApp.
- **Sitio de soporte de NetApp**: Utilice esta opción si utiliza un registro local con las imágenes del Centro de control de Astra.

Registro de imágenes de Astra Control

1. Inicia sesión en el servicio Astra Control.
2. En el Dashboard, selecciona **Desplegar una instancia autogestionada de Astra Control**.
3. Sigue las instrucciones para iniciar sesión en el registro de imágenes de Astra Control, extraer la imagen de instalación de Astra Control Center y extraer la imagen.

Sitio de soporte de NetApp

1. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete.

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig astra-
   control-center-[version].tar.gz
   ```

   Se mostrará la salida `Verified OK` después de una verificación correcta.

3. Extraiga las imágenes del paquete Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Complete los pasos adicionales si utiliza un registro local

Si tiene pensado enviar el paquete Centro de control de Astra a su registro local, debe usar el complemento de la línea de comandos kubectl de Astra de NetApp.

Instale el complemento Astra kubectl de NetApp

Complete estos pasos para instalar el plugin de línea de comandos kubectl de NetApp Astra más reciente.

Antes de empezar

NetApp proporciona binarios de complementos para diferentes arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea.

Si ya tiene instalado el plugin desde una instalación anterior, "asegúrese de tener la versión más reciente" antes de realizar estos pasos.

Pasos

1. Enumere los binarios disponibles del complemento Astra kubectl de NetApp, y anote el nombre del archivo que necesita para el sistema operativo y la arquitectura de CPU:

> La biblioteca de complementos kubectl forma parte del paquete tar y se extrae en la carpeta `kubectl-astra`.

```
ls kubectl-astra/
```

2. Mueva el binario correcto a la ruta actual y cambie el nombre a. `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Agregue las imágenes a su registro

1. Si planeas enviar el paquete Astra Control Center a tu registro local, completa la secuencia de pasos apropiada para tu motor de contenedores:

Docker

a. Cambie al directorio raíz del tarball. Debería ver el `acc.manifest.bundle.yaml` archivo y estos directorios:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:

- Sustituya <BUNDLE_FILE> por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
- Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio de Docker; por ejemplo, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
- Reemplace <MY_REGISTRY_USER> por el nombre de usuario.
- Sustituya <MY_REGISTRY_TOKEN> por un token autorizado para el registro.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

a. Cambie al directorio raíz del tarball. Debería ver este archivo y directorio:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

c. Prepare y ejecute una de las siguientes secuencias de comandos personalizadas para la versión de Podman que utilice. Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio que incluye cualquier subdirectorio.

```
<strong>Podman 4</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

La ruta de acceso de imagen que crea el script debe parecerse a la siguiente, dependiendo de la configuración del Registro:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Cambie el directorio:

```
cd manifests
```

Busque la página de instalación del operador

1. Realice uno de los siguientes procedimientos para acceder a la página de instalación del operador:

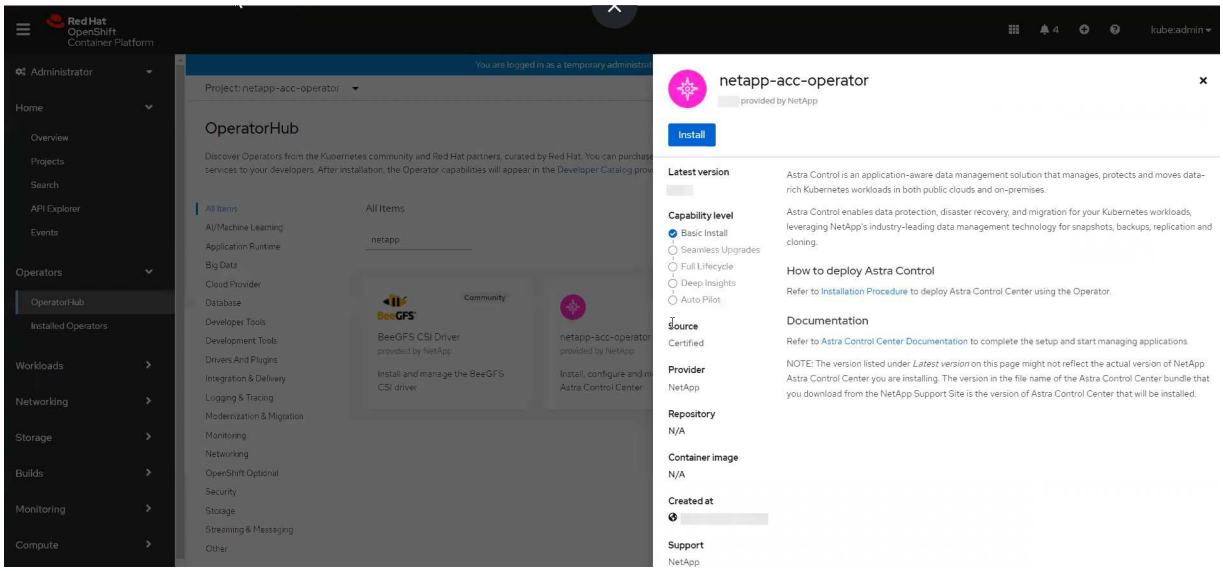
Consola web de Red Hat OpenShift

a. Inicie sesión en la IU de OpenShift Container Platform.

b. En el menú lateral, seleccione **operadores > OperatorHub**.

> Solo se puede actualizar a la versión actual de Astra Control Center con este operador.

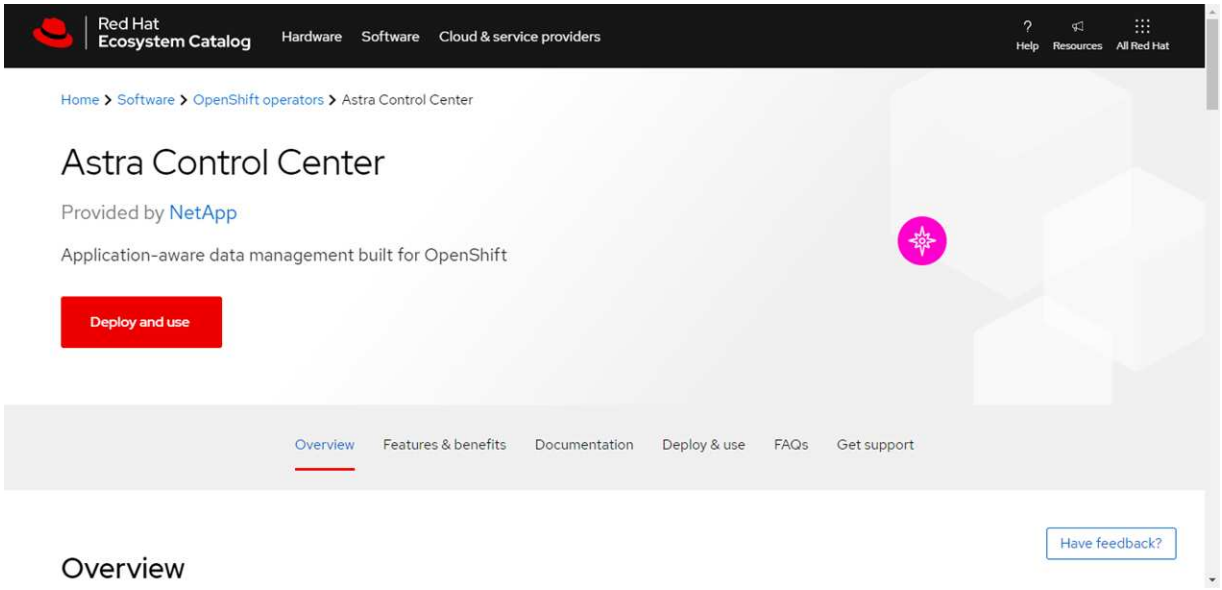
c. Busque `netapp-acc` Y selecciona el operador Centro de control de Astra de NetApp.



Catálogo de Red Hat Ecosystem

a. Seleccione Astra Control Center de NetApp "operador".

b. Seleccione **Desplegar y usar**.



Instale el operador

1. Complete la página **Install Operator** e instale el operador:

   El operador estará disponible en todos los espacios de nombres del clúster.

   a. Seleccione el espacio de nombres del operador o. `netapp-acc-operator` el espacio de nombres se creará automáticamente como parte de la instalación del operador.

   b. Seleccione una estrategia de aprobación manual o automática.

      Se recomienda la aprobación manual. Solo debe tener una instancia de operador en ejecución por clúster.

   c. Seleccione **instalar**.

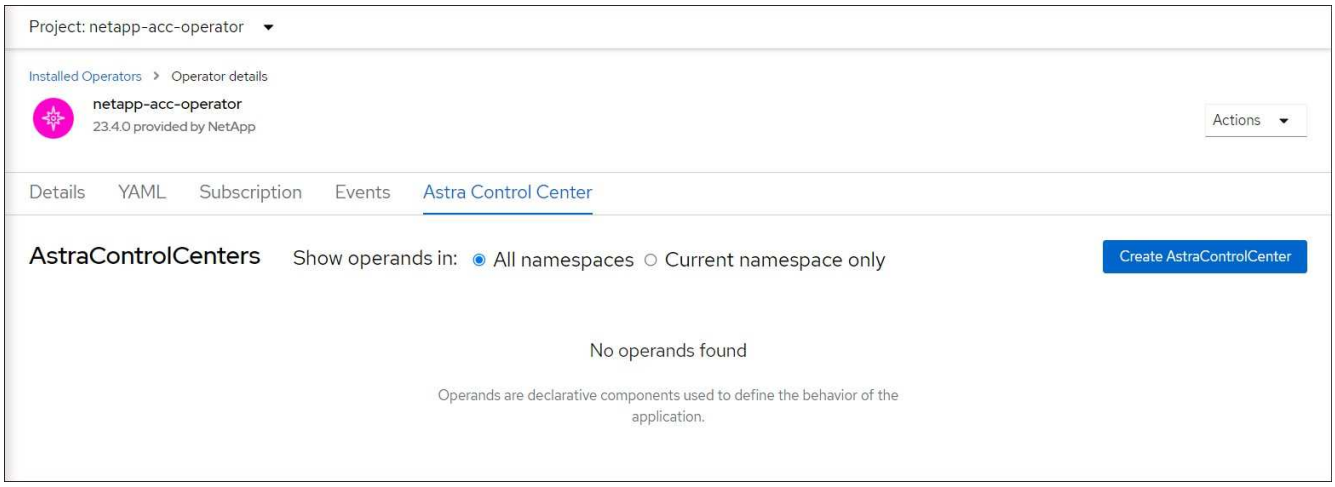
      Si ha seleccionado una estrategia de aprobación manual, se le pedirá que apruebe el plan de instalación manual para este operador.

2. Desde la consola, vaya al menú OperatorHub y confirme que el operador se ha instalado correctamente.

Instalar Astra Control Center

1. Desde la consola de la pestaña **Astra Control Center** del operador Astra Control Center, seleccione **Crear AstraControlCenter**

   .



2. Complete el `Create AstraControlCenter` campo de formulario:

   a. Mantenga o ajuste el nombre del Centro de control de Astra.

   b. Agregue etiquetas para Astra Control Center.

   c. Habilitar o deshabilitar AutoSupport. Se recomienda conservar la funcionalidad de AutoSupport.

   d. Introduzca el FQDN o la dirección IP de Astra Control Center. No entre `http://` o. `https://` en el campo de dirección.

   e. Introduce la versión de Astra Control Center; por ejemplo, 24.02.0-69.

   f. Introduzca un nombre de cuenta, una dirección de correo electrónico y un apellido de administrador.

   g. Seleccione una política de reclamaciones de volumen de `Retain`, `Recycle`, o. `Delete`. El valor

predeterminado es `Retain`.

h. Seleccione el tamaño de escala de la instalación.

> De forma predeterminada, Astra utilizará la alta disponibilidad (HA) `scaleSize` de `Medium`, Que despliega la mayoría de los servicios en HA y despliega múltiples réplicas para redundancia. Con `scaleSize` como `Small`, Astra reducirá el número de réplicas para todos los servicios excepto los servicios esenciales para reducir el consumo.

i. Seleccione el tipo de entrada:

- **Genérico** (`ingressType: "Generic"`) (Predeterminado)

  Utilice esta opción cuando tenga otro controlador de entrada en uso o prefiera utilizar su propio controlador de entrada. Después de poner en marcha Astra Control Center, será necesario configurar el "controlador de entrada" Para exponer Astra Control Center con una URL.

- **AccTraefik** (`ingressType: "AccTraefik"`)

  Utilice esta opción cuando prefiera no configurar un controlador de entrada. Esto despliega el Astra Control Center `traefik` Puerta de enlace como servicio de tipo "LoadBalancer" de Kubernetes.

Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y aún no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga.

> Para obtener detalles sobre el tipo de servicio de “LoadBalancer” e Ingress, consulte "Requisitos".

a. En **Image Registry**, utilice el valor predeterminado a menos que configure un registro local. Para un registro local, reemplace este valor por la ruta del registro de imágenes local donde insertó las imágenes en un paso anterior. No entre `http://` o. `https://` en el campo de dirección.

b. Si utiliza un registro de imágenes que requiere autenticación, introduzca el secreto de imagen.

> Si utiliza un registro que requiere autenticación, cree un secreto en el clúster.

c. Introduzca el nombre del administrador.

d. Configure el escalado de recursos.

e. Proporcione la clase de almacenamiento predeterminada.

> Si se configura una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento que tiene la anotación predeterminada.

f. Defina las preferencias de manejo de CRD.

3. Seleccione la vista YAML para revisar los ajustes seleccionados.

4. Seleccione `Create`.

Cree un secreto de registro

Si utiliza un registro que requiere autenticación, cree un secreto en el clúster de OpenShift e introduzca el nombre secreto en el `Create AstraControlCenter` campo de formulario.

1. Cree un espacio de nombres para el operador Astra Control Center:

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. Cree un secreto en este espacio de nombres:

```
oc create secret docker-registry astra-registry-cred -n [netapp-acc-
operator or custom namespace] --docker-server=[your_registry_path]
--docker username=[username] --docker-password=[token]
```

> Astra Control sólo admite secretos de registro Docker.

3. Complete los campos restantes en El campo de formulario Create AstraControlCenter.

El futuro

Complete el "pasos restantes" Para verificar que Astra Control Center se ha instalado correctamente, configure un controlador de entrada (opcional) e inicie sesión en la interfaz de usuario. Además, deberá realizar el trabajo "tareas de configuración" tras completar la instalación.

Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP

Con Astra Control Center, puede gestionar sus aplicaciones en un entorno de cloud híbrido con clústeres de Kubernetes e instancias de Cloud Volumes ONTAP autogestionados. Puedes poner en marcha Astra Control Center en tus clústeres de Kubernetes on-premises o en uno de los clústeres de Kubernetes autogestionados del entorno de nube.

Con una de estas puestas en marcha, puede realizar operaciones de gestión de datos de aplicaciones utilizando Cloud Volumes ONTAP como back-end de almacenamiento. También es posible configurar un bloque de S3 como destino de backup.

Para instalar Astra Control Center en Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure con una back-end de almacenamiento de Cloud Volumes ONTAP, realice los siguientes pasos en función de su entorno de cloud.

- Ponga en marcha Astra Control Center en Amazon Web Services
- Ponga en marcha Astra Control Center en Google Cloud Platform
- Ponga en marcha Astra Control Center en Microsoft Azure

Puede gestionar sus aplicaciones en distribuciones con clústeres de Kubernetes autogestionados, como OpenShift Container Platform (OCP). Sólo se validan los clústeres OCP autogestionados para la implantación

de Astra Control Center.

Ponga en marcha Astra Control Center en Amazon Web Services

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Amazon Web Services (AWS).

Lo que necesitará para AWS

Antes de implementar Astra Control Center en AWS, necesitarás los siguientes elementos:

- Licencia Astra Control Center. Consulte "Requisitos de licencia de Astra Control Center".
- "Cumpla los requisitos de Astra Control Center".
- Cuenta de Cloud Central de NetApp
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de AWS, Access ID y Secret Key con permisos que permiten crear cubos y conectores
- Acceso e inicio de sesión del Elastic Container Registry (ECR) de la cuenta de AWS
- Se necesitan la zona alojada de AWS y la entrada de Amazon Route 53 para acceder a la interfaz de usuario de Astra Control

Requisitos de los entornos operativos para AWS

Astra Control Center requiere los siguientes entornos operativos para AWS:

- Red Hat OpenShift Container Platform 4,11 a 4,13

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere recursos específicos además de los requisitos de recursos del entorno. Consulte "Requisitos del entorno operativo del Centro de control de Astra".

> El token de registro de AWS caduca en 12 horas, después de lo cual tendrá que renovar el secreto del registro de imágenes de Docker.

Información general sobre la implementación para AWS

He aquí una descripción general del proceso de instalación de Astra Control Center para AWS con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. Compruebe que dispone de suficientes permisos IAM.
2. Instale un clúster RedHat OpenShift en AWS.
3. Configure AWS.
4. Configuración de BlueXP de NetApp para AWS.
5. Instale Astra Control Center para AWS.

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM que le permiten instalar un clúster RedHat OpenShift y un conector BlueXP de NetApp (anteriormente Cloud Manager).

Consulte "Credenciales iniciales de AWS".

Instale un clúster RedHat OpenShift en AWS

Instale un clúster RedHat OpenShift Container Platform en AWS.

Para obtener instrucciones de instalación, consulte "Instalación de un clúster en AWS en OpenShift Container Platform".

Configure AWS

A continuación, configure AWS para crear una red virtual, configurar EC2 instancias de computación y crear un bucket de AWS S3. Si no puede acceder al registro de imágenes del Centro de control de Astra de NetApp, también deberá crear un registro de contenedores elásticos (ECR) para alojar las imágenes del Centro de control de Astra e insertar las imágenes en este registro.

Siga la documentación de AWS para completar los pasos siguientes. Consulte "Documentación de instalación de AWS".

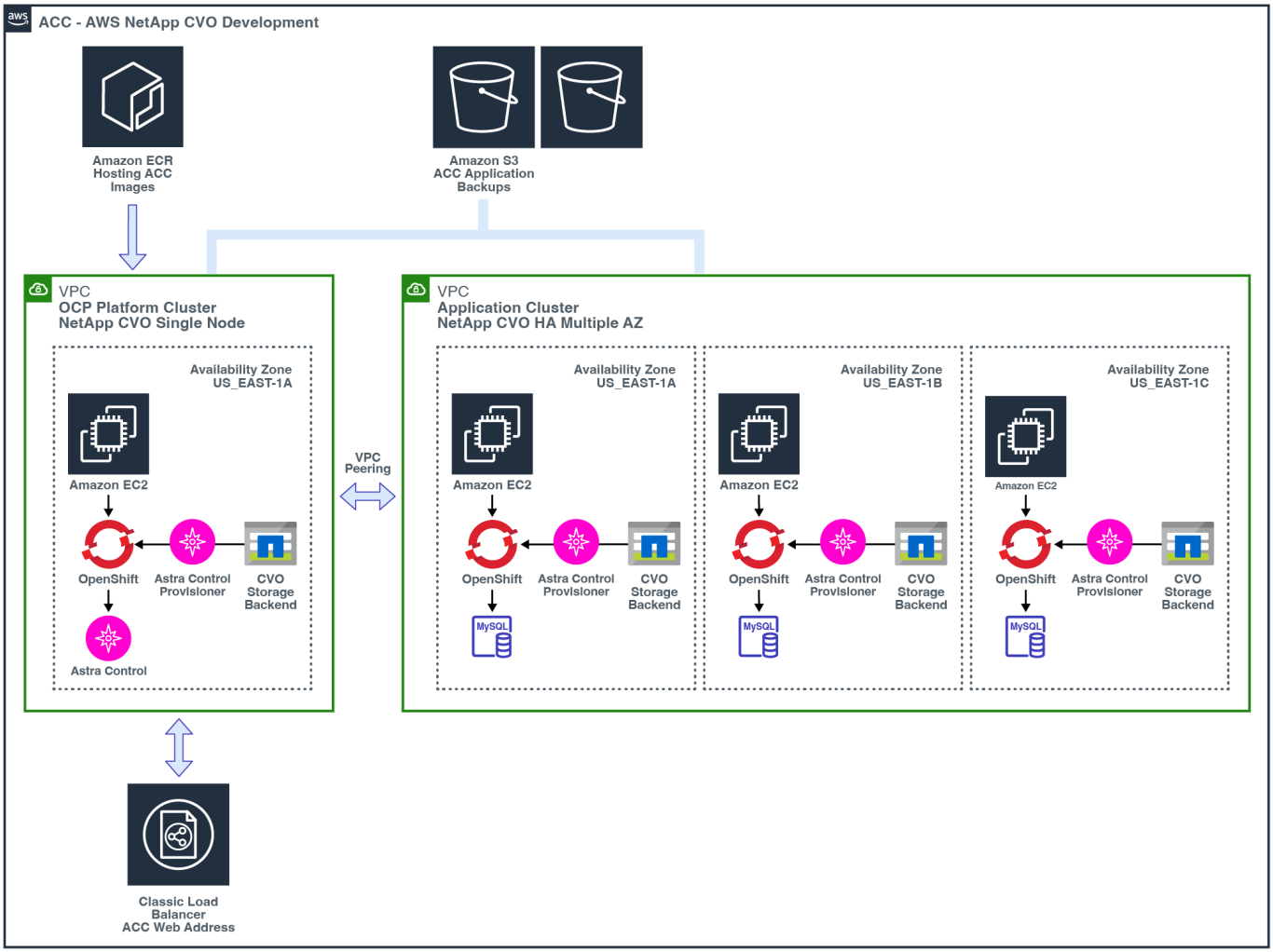
1. Cree una red virtual AWS.
2. Revise las instancias de computación EC2. Puede ser un servidor con configuración básica o máquinas virtuales en AWS.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en AWS para cumplir los requisitos de Astra. Consulte "Requisitos del Centro de Control de Astra".
4. Cree al menos un bloque de AWS S3 para almacenar los backups.
5. (Opcional) Si no puede acceder al registro de imágenes NetApp, haga lo siguiente:
   a. Cree un AWS Elastic Container Registry (ECR) para alojar todas las imágenes de Astra Control Center.

      Si no crea la ECR, Astra Control Center no puede acceder a los datos de supervisión de un clúster que contenga Cloud Volumes ONTAP con un back-end de AWS. El problema se produce cuando el clúster que intenta detectar y gestionar mediante Astra Control Center no tiene acceso a AWS ECR.

   b. Envía las imágenes del Centro de control de Astra al registro definido.

El token del registro de contenedor elástico de AWS (ECR) caduca al cabo de 12 horas y provoca errores en las operaciones de clonado de varios clústeres. Este problema ocurre cuando se gestiona un back-end de almacenamiento desde Cloud Volumes ONTAP configurado para AWS. Para corregir este problema, vuelva a autenticarse con la ECR y genere un nuevo secreto para que las operaciones de clonación se reanuden correctamente.

A continuación mostramos un ejemplo de una puesta en marcha de AWS:



Configuración de BlueXP de NetApp para AWS

Con NetApp BlueXP (anteriormente Cloud Manager), cree un espacio de trabajo, añada un conector a AWS, cree un entorno de trabajo e importe el clúster.

Siga la documentación de BlueXP para completar los siguientes pasos. Consulte lo siguiente:

- "Introducción a Cloud Volumes ONTAP en AWS".
- "Cree un conector en AWS mediante BlueXP"

Pasos

1. Agregue sus credenciales a BlueXP.
2. Crear un área de trabajo.
3. Agregue un conector para AWS. Elija AWS como proveedor.
4. Cree un entorno de trabajo para su entorno de cloud.
   a. Ubicación: "Amazon Web Services (AWS)"
   b. Tipo: "Cloud Volumes ONTAP ha"
5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
   a. Consulte los detalles del clúster de NetApp seleccionando **K8s** > **Lista de clústeres** > **Detalles del clúster**.

b. En la esquina superior derecha, observa la versión de aprovisionamiento de Astra Control.

c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el aprovisionador.

   Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento.
   Astra Control Provisioning se instala automáticamente como parte del proceso de importación y detección.

6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.

> Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de implementación del nodo que se ejecutan en AWS.

Instale Astra Control Center para AWS

Siga la norma "Instrucciones de instalación de Astra Control Center".

> AWS utiliza el tipo de bloque Generic S3.

Ponga en marcha Astra Control Center en Google Cloud Platform

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Google Cloud Platform (GCP).

Qué necesitará para GCP

Antes de implementar Astra Control Center en GCP, necesitarás los siguientes elementos:

- Licencia Astra Control Center. Consulte "Requisitos de licencia de Astra Control Center".
- "Cumpla los requisitos de Astra Control Center".
- Cuenta de Cloud Central de NetApp
- Si utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4,11 a 4,13
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Cuenta de servicio de GCP con permisos que le permiten crear cubos y conectores

Requisitos del entorno operativo para GCP

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere recursos específicos además de los requisitos de recursos del entorno. Consulte "Requisitos del entorno operativo del Centro de control de Astra".

Información general de puesta en marcha para GCP

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center en un clúster OCP autogestionado en GCP con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. Instale un clúster RedHat OpenShift en GCP.
2. Cree un proyecto de GCP y una nube privada virtual.
3. Compruebe que dispone de suficientes permisos IAM.
4. Configure GCP.
5. Configuración de NetApp BlueXP para GCP.
6. Instale Astra Control Center para GCP.

Instale un clúster RedHat OpenShift en GCP

El primer paso es instalar un clúster RedHat OpenShift en GCP.

Para obtener instrucciones de instalación, consulte lo siguiente:

- "Instalar un clúster OpenShift en GCP"
- "Creación de una cuenta de servicio de GCP"

Cree un proyecto de GCP y una nube privada virtual

Cree al menos un proyecto de GCP y una nube privada virtual (VPC).

> OpenShift podría crear sus propios grupos de recursos. Además de ellas, debe definir también un VPC de GCP. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM que le permiten instalar un clúster RedHat OpenShift y un conector BlueXP de NetApp (anteriormente Cloud Manager).

Consulte "Credenciales y permisos iniciales de GCP".

Configure GCP

A continuación, configure GCP para crear una VPC, configurar instancias de computación y crear un almacenamiento de objetos de Google Cloud. Si no puedes acceder al registro de imágenes del Centro de control de Astra de NetApp, también tendrás que crear un Registro de contenedores de Google para alojar las imágenes del Centro de control de Astra e insertar las imágenes en este registro.

Siga la documentación de GCP para completar los siguientes pasos. Consulte instalación del clúster OpenShift en GCP.

1. Cree un proyecto de GCP y VPC en el GCP que planea utilizar para el clúster de OCP con el back-end de CVO.
2. Revise las instancias de computación. Puede tratarse de un servidor de configuración básica o máquinas virtuales en GCP.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestro y trabajador, cambie el tipo de instancia de GCP para que cumpla los requisitos de Astra. Consulte

"Requisitos del Centro de Control de Astra".

4. Cree al menos un bloque de almacenamiento en cloud de GCP para almacenar sus backups.
5. Crear un secreto, que es necesario para el acceso a bloques.
6. (Opcional) Si no puede acceder al registro de imágenes NetApp, haga lo siguiente:
   a. Crea un registro de contenedores de Google para alojar las imágenes del Centro de control de Astra.
   b. Configure el acceso al registro de contenedores de Google para inserción/extracción de Docker para todas las imágenes de Astra Control Center.

      Ejemplo: Las imágenes del Centro de control de Astra se pueden enviar a este registro introduciendo el siguiente script:

      ```
      gcloud auth activate-service-account <service account email address>
      --key-file=<GCP Service Account JSON file>
      ```

      Este script requiere un archivo de manifiesto de Astra Control Center y su ubicación del Registro de imágenes de Google. Ejemplo:

```
manifestfile=acc.manifest.bundle.yaml
GCP_CR_REGISTRY=<target GCP image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < acc.manifest.bundle.yaml
```

7. Configure zonas DNS.

Configuración de NetApp BlueXP para GCP

Con NetApp BlueXP (anteriormente Cloud Manager), cree un espacio de trabajo, añada un conector a GCP, cree un entorno de trabajo e importe el clúster.

Siga la documentación de BlueXP para completar los siguientes pasos. Consulte "Introducción a Cloud Volumes ONTAP en GCP".

Antes de empezar

- Acceso a la cuenta de servicio de GCP con los permisos y roles de IAM necesarios

Pasos

1. Agregue sus credenciales a BlueXP. Consulte "Adición de cuentas de GCP".

2. Agregue un conector para GCP.
   a. Elija "GCP" como el proveedor.
   b. Introduzca las credenciales de GCP. Consulte "Creación de un conector en GCP desde BlueXP".
   c. Asegúrese de que el conector está en marcha y cambie a dicho conector.
3. Cree un entorno de trabajo para su entorno de cloud.
   a. Ubicación: "GCP"
   b. Tipo: "Cloud Volumes ONTAP ha"
4. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
   a. Consulte los detalles del clúster de NetApp seleccionando **K8s** > **Lista de clústeres** > **Detalles del clúster**.
   b. En la esquina superior derecha, observa la versión de aprovisionamiento de Astra Control.
   c. Tenga en cuenta las clases de almacenamiento del clúster de Cloud Volumes ONTAP que muestran "NetApp" como el aprovisionador.

      Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento.
      Astra Control Provisioning se instala automáticamente como parte del proceso de importación y detección.
5. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.

> Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en GCP.

Instale Astra Control Center para GCP

Siga la norma "Instrucciones de instalación de Astra Control Center".

> GCP utiliza el tipo de bloque Generic S3.

1. Genere el secreto Docker para obtener imágenes de la instalación de Astra Control Center:

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

Ponga en marcha Astra Control Center en Microsoft Azure

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado que se aloja en un cloud público de Microsoft Azure.

Lo que necesitará para Azure

Antes de implementar Astra Control Center en Azure, necesitarás los siguientes elementos:

- Licencia Astra Control Center. Consulte "Requisitos de licencia de Astra Control Center".
- "Cumpla los requisitos de Astra Control Center".
- Cuenta de Cloud Central de NetApp
- Si utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4,11 a 4,13
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de Azure con permisos que le permiten crear cubos y conectores

Requisitos del entorno operativo para Azure

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere recursos específicos además de los requisitos de recursos del entorno. Consulte "Requisitos del entorno operativo del Centro de control de Astra".

Información general sobre la implementación para Azure

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center para Azure.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. Instale un clúster RedHat OpenShift en Azure.
2. Cree grupos de recursos de Azure.
3. Compruebe que dispone de suficientes permisos IAM.
4. Configure Azure.
5. Configuración de NetApp BlueXP (anteriormente Cloud Manager) para Azure.
6. Instalar y configurar Astra Control Center para Azure.

Instale un clúster RedHat OpenShift en Azure

El primer paso es instalar un clúster RedHat OpenShift en Azure.

Para obtener instrucciones de instalación, consulte lo siguiente:

- "Instalando el clúster de OpenShift en Azure".
- "Instalar una cuenta de Azure".

Cree grupos de recursos de Azure

Cree al menos un grupo de recursos de Azure.

> OpenShift podría crear sus propios grupos de recursos. Además de estos, también debe definir los grupos de recursos de Azure. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos IAM para poder instalar un clúster RedHat OpenShift y un conector BlueXP de NetApp.

Consulte "Credenciales y permisos de Azure".

Configure Azure

A continuación, configure Azure para crear una red virtual, configurar instancias de computación y crear un contenedor de Azure Blob. Si no puede acceder al registro de imágenes del Centro de control de Astra de NetApp, también deberá crear un Registro de contenedores de Azure (ACR) para alojar las imágenes del Centro de control de Astra e insertar las imágenes en este registro.

Siga la documentación de Azure para completar los siguientes pasos. Consulte "Instalando el clúster de OpenShift en Azure".

1. Cree una red virtual de Azure.
2. Revise las instancias de computación. Puede ser un servidor con configuración básica o máquinas virtuales en Azure.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en Azure para cumplir los requisitos de Astra. Consulte "Requisitos del Centro de Control de Astra".
4. Cree al menos un contenedor de Azure Blob para almacenar los backups.
5. Cree una cuenta de almacenamiento. Necesitarás una cuenta de almacenamiento para crear un contenedor que se utilice como bloque en Astra Control Center.
6. Crear un secreto, que es necesario para el acceso a bloques.
7. (Opcional) Si no puede acceder al registro de imágenes NetApp, haga lo siguiente:

    a. Cree un registro de contenedores de Azure (ACR) para alojar las imágenes del Centro de control de Astra.

    b. Configura el acceso de ACR para la inserción/extracción de Docker para todas las imágenes del Centro de control de Astra.

    c. Envíe las imágenes del Centro de control de Astra a este registro mediante el siguiente script:

    ```
    az acr login -n <AZ ACR URL/Location>
    This script requires the Astra Control Center manifest file and your
    Azure ACR location.
    ```

    Ejemplo:

```
manifestfile=acc.manifest.bundle.yaml
AZ_ACR_REGISTRY=<target Azure ACR image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < acc.manifest.bundle.yaml
```

8. Configure zonas DNS.

Configuración de NetApp BlueXP (anteriormente Cloud Manager) para Azure

Con BlueXP (anteriormente Cloud Manager), cree un espacio de trabajo, añada un conector a Azure, cree un entorno de trabajo e importe el clúster.

Siga la documentación de BlueXP para completar los siguientes pasos. Consulte "Introducción a BlueXP en Azure".

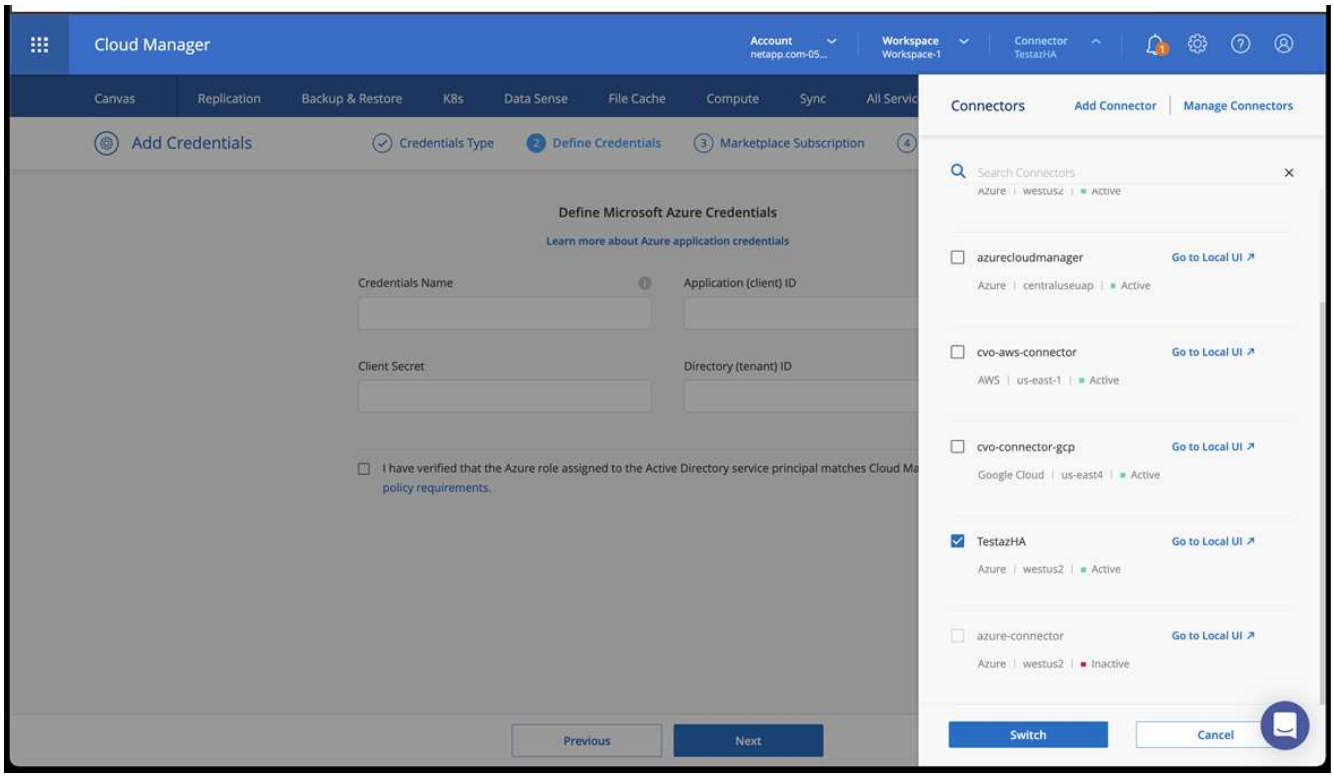
Antes de empezar

Acceso a la cuenta de Azure con los permisos y roles de IAM necesarios

Pasos

1. Agregue sus credenciales a BlueXP.
2. Agregue un conector para Azure. Consulte "Políticas de BlueXP".
   a. Elija **Azure** como proveedor.
   b. Introduzca las credenciales de Azure, incluidos el ID de aplicación, el secreto de cliente y el ID del directorio (inquilino).

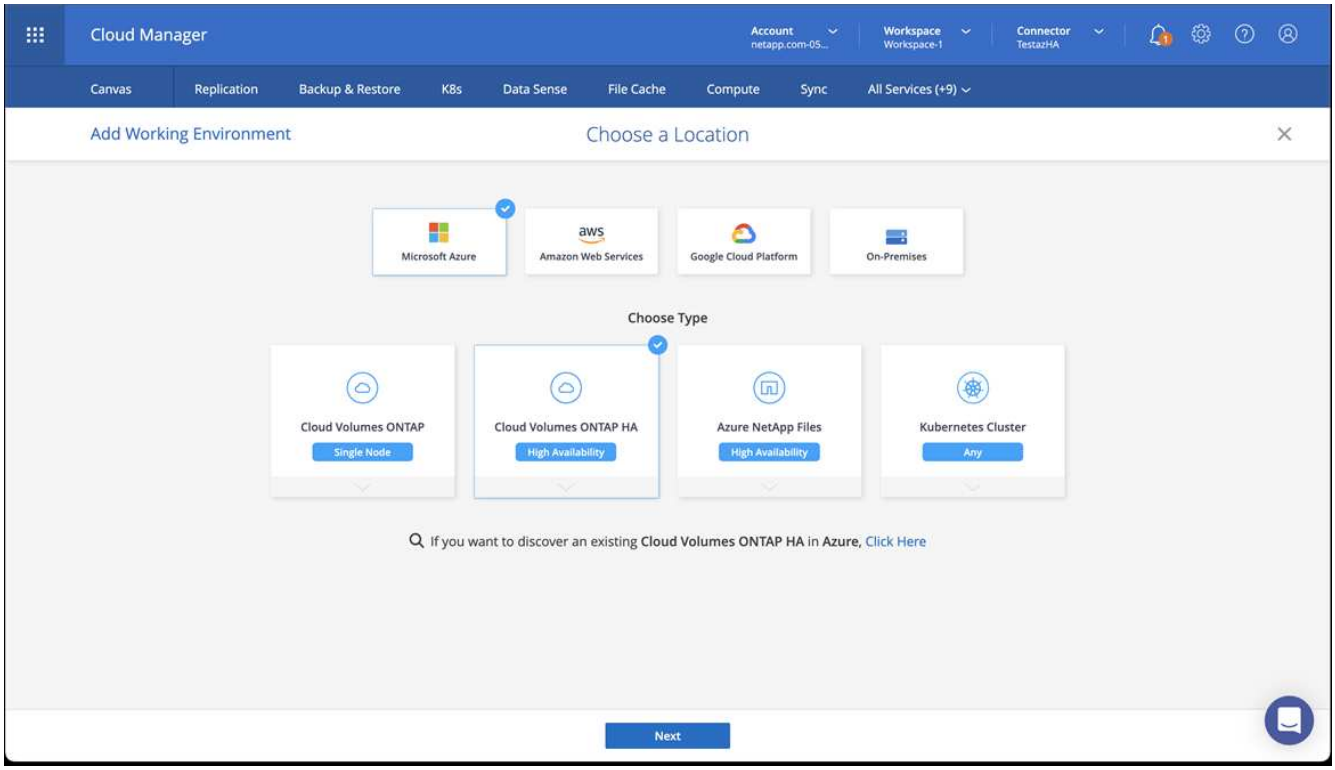
      Consulte "Creación de un conector en Azure desde BlueXPr".
3. Asegúrese de que el conector está en marcha y cambie a dicho conector.



4. Cree un entorno de trabajo para su entorno de cloud.

   a. Ubicación: "Microsoft Azure".

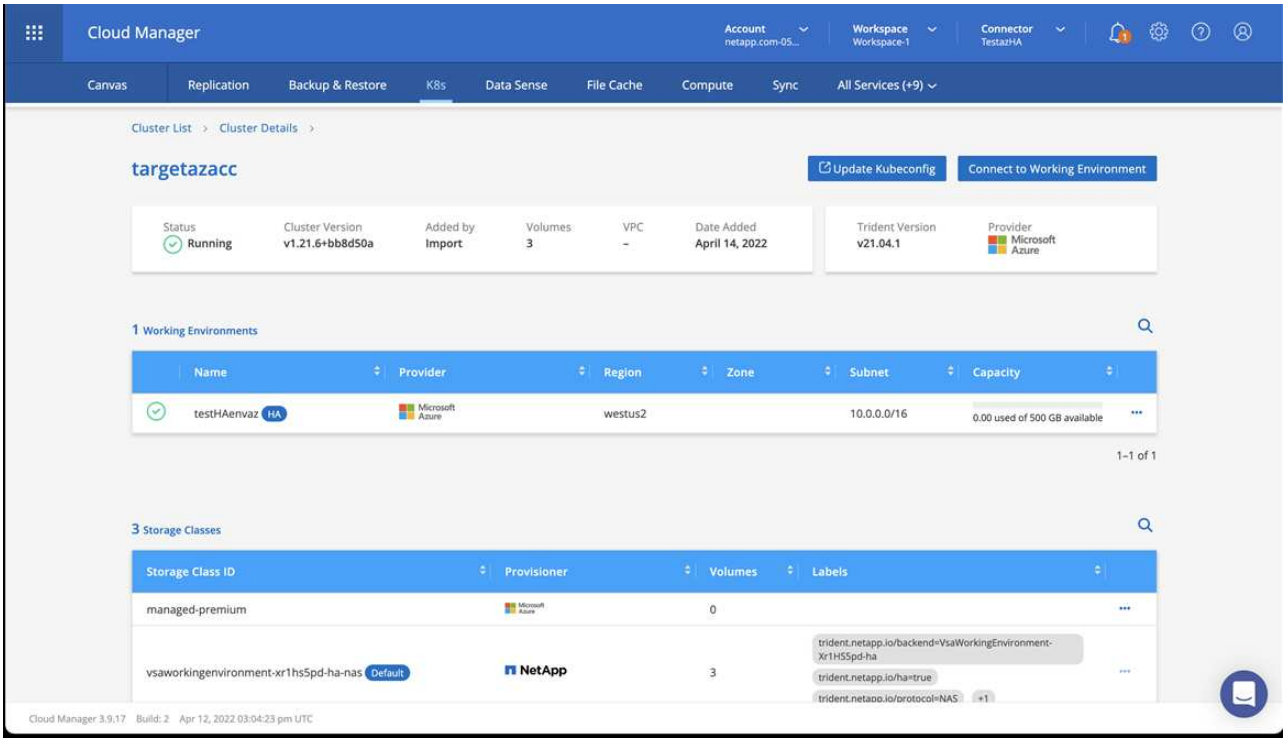
   b. Tipo: "Cloud Volumes ONTAP ha".



5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.

   a. Consulte los detalles del clúster de NetApp seleccionando **K8s** > **Lista de clústeres** > **Detalles del**

clúster.



b. En la esquina superior derecha, observa la versión de aprovisionamiento de Astra Control.

c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el aprovisionador.

Esto importa su clúster de Red Hat OpenShift y asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento.
Astra Control Provisioning se instala automáticamente como parte del proceso de importación y detección.

6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.
7. Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si ha está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en Azure.

Instalar y configurar Astra Control Center para Azure

Instale Astra Control Center con el estándar "instrucciones de instalación".

Con Astra Control Center, añada un bucket de Azure. Consulte "Configure Astra Control Center y añada cucharones".

Configurar Astra Control Center después de la instalación

En función de su entorno, es posible que se necesite una configuración adicional después de instalar Astra Control Center.

Quite las limitaciones de recursos

Algunos entornos utilizan los objetos ResourceQuotas y LimitRanges para evitar que los recursos de un espacio de nombres consuman toda la CPU y memoria disponibles en el clúster. Astra Control Center no

establece límites máximos, por lo que no se ajusta a esos recursos. Si su entorno se configura de esta forma, debe eliminar esos recursos de los espacios de nombres en los que planea instalar Astra Control Center.

Puede utilizar los siguientes pasos para recuperar y eliminar estas cuotas y límites. En estos ejemplos, el resultado del comando se muestra inmediatamente después del comando.

Pasos

1. Obtenga las cuotas de recursos en la `netapp-acc` espacio de nombres (o con nombre personalizado):

```
kubectl get quota -n [netapp-acc or custom namespace]
```

Respuesta:

```
NAME          AGE   REQUEST                                          LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. Elimine todas las cuotas de recursos por nombre:

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom
namespace]
```

3. Obtenga los rangos de límites en la `netapp-acc` espacio de nombres (o con nombre personalizado):

```
kubectl get limits -n [netapp-acc or custom namespace]
```

Respuesta:

```
NAME              CREATED AT
cpu-limit-range   2022-06-27T19:01:23Z
```

4. Eliminar los rangos de límites por nombre:

```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom
namespace]
```

Agregue un certificado TLS personalizado

Astra Control Center utiliza un certificado TLS autofirmado de forma predeterminada para el tráfico del controlador de entrada (solo en determinadas configuraciones) y la autenticación de la interfaz de usuario web con exploradores web. Para el uso en producción, debe quitar el certificado TLS autofirmado existente y reemplazarlo por un certificado TLS firmado por una entidad de certificación (CA).

> El certificado autofirmado predeterminado se utiliza para dos tipos de conexiones:
>
> - Conexiones HTTPS a la interfaz de usuario web de Astra Control Center
> - Tráfico del controlador de entrada (sólo si el `ingressType: "AccTraefik"` la propiedad se estableció en `astra_control_center.yaml` Archivo durante la instalación de Astra Control Center)
>
> Al reemplazar el certificado TLS predeterminado, se reemplaza el certificado utilizado para la autenticación de estas conexiones.

Antes de empezar

- Clúster Kubernetes con Astra Control Center instalado
- Acceso administrativo a un shell de comandos en el clúster para ejecutar `kubectl` comandos
- Archivos de claves privadas y certificados de la CA

Quite el certificado autofirmado

Quite el certificado TLS autofirmado existente.

1. Con SSH, inicie sesión en el clúster Kubernetes que aloja Astra Control Center como usuario administrativo.
2. Busque el secreto TLS asociado con el certificado actual mediante el comando siguiente, reemplazo `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Elimine el secreto y certificado instalados actualmente con los comandos siguientes:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
```

```
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Añada un nuevo certificado mediante la línea de comandos

Añada un nuevo certificado TLS firmado por una CA.

1. Utilice el siguiente comando para crear el nuevo secreto TLS con la clave privada y los archivos de certificado de la CA, reemplazando los argumentos entre paréntesis <> con la información adecuada:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Utilice el siguiente comando y el ejemplo para editar el archivo de definición de recursos personalizados (CRD) del clúster y cambiar el `spec.selfSigned` valor a. `spec.ca.secretName` Para hacer referencia al secreto TLS que ha creado anteriormente:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
```

   CRD:

```
#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Utilice el siguiente comando y el resultado de ejemplo para validar que los cambios son correctos y que el clúster está listo para validar certificados, sustituir `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
```

   Respuesta:

```
Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. Cree el `certificate.yaml` archivo utilizando el ejemplo siguiente, reemplazando los valores de marcador de posición entre corchetes <> con la información apropiada:

> En este ejemplo se utiliza el `dnsNames` Propiedad para especificar la dirección DNS de Astra Control Center. Astra Control Center no admite el uso de la propiedad Common Name (CN) para especificar la dirección DNS.

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  <strong>name: <certificate-name></strong>
  namespace: <ACC-deployment-namespace>
spec:
  <strong>secretName: <certificate-secret-name></strong>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  <strong>- <astra.dnsname.example.com></strong> #Replace with the
correct Astra Control Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Cree el certificado con el comando siguiente:

```
kubectl apply -f certificate.yaml
```

6. Con el siguiente comando y el resultado de ejemplo, valide que el certificado se ha creado correctamente y con los argumentos especificados durante la creación (como nombre, duración, plazo de renovación y nombres DNS).

```
kubectl describe certificate -n <ACC-deployment-namespace>
```

Respuesta:

```
Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. Edite el almacén de CRD de TLS para que apunte al nuevo nombre de secreto de certificado mediante el siguiente comando y por ejemplo, sustituyendo los valores de marcador de posición entre paréntesis <> por la información adecuada

```
kubectl edit tlsstores.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
spec:
  defaultCertificate:
    secretName: <certificate-secret-name>
```

8. Edite la opción Ingress CRD TLS para que apunte al nuevo secreto de certificado utilizando el siguiente comando y ejemplo, reemplazando los valores de marcador de posición entre paréntesis <> con la información adecuada:

```
kubectl edit ingressroutes.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
 tls:
    secretName: <certificate-secret-name>
```

9. Con un explorador web, vaya a la dirección IP de implementación de Astra Control Center.
10. Compruebe que los detalles del certificado coinciden con los detalles del certificado que ha instalado.
11. Exporte el certificado e importe el resultado en el administrador de certificados en su navegador web.

Configure Astra Control Center

Agregue una licencia de Astra Control Center

Al instalar Astra Control Center, ya hay una licencia de evaluación integrada instalada. Si estás evaluando Astra Control Center, puedes omitir este paso.

Puede añadir una nueva licencia con la interfaz de usuario de Astra Control o. "API de control Astra".

Las licencias de Astra Control Center miden los recursos de CPU mediante unidades de CPU de Kubernetes y representan los recursos de CPU asignados a los nodos de trabajo de todos los clústeres de Kubernetes gestionados. Las licencias se basan en el uso de vCPU. Para obtener más información sobre cómo se calculan las licencias, consulte "Licencia".

> Si su instalación crece para superar el número de unidades CPU con licencia, Astra Control Center le impide gestionar nuevas aplicaciones. Se muestra una alerta cuando se supera la capacidad.

> Para actualizar una evaluación existente o una licencia completa, consulte "Actualizar una licencia existente".

Antes de empezar

- Acceso a una instancia de Astra Control Center recién instalada.
- Permisos del rol de administrador.
- A. "Archivo de licencia de NetApp" (NLF).

Pasos

1. Inicie sesión en la interfaz de usuario de Astra Control Center.
2. Seleccione **cuenta** > **Licencia**.
3. Seleccione **Agregar licencia**.
4. Busque el archivo de licencia (NLF) que descargó.
5. Seleccione **Agregar licencia**.

La página **cuenta** > **Licencia** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

Si tiene una licencia de evaluación y no envía datos a AutoSupport, asegúrese de almacenar su ID de cuenta para evitar la pérdida de datos en caso de un fallo en Astra Control Center.

Habilita el aprovisionador de Astra Control

Las versiones 23,10 y posteriores de Astra Trident incluyen la opción de usar Astra Control Provisioning, que permite a los usuarios de Astra Control con licencia acceder a funcionalidades avanzadas de aprovisionamiento del almacenamiento. El aprovisionador Astra Control ofrece esta funcionalidad ampliada, además de la funcionalidad estándar basada en CSI de Astra Trident.

En las próximas actualizaciones de Astra Control, el aprovisionador de Astra Control reemplazará a Astra Trident como aprovisionador de almacenamiento y orquestador y será obligatorio para su uso en Astra Control. Por este motivo, se recomienda encarecidamente que los usuarios de Astra Control habiliten el aprovisionador de Astra Control. Astra Trident seguirá siendo de código abierto y se seguirá lanzando, manteniendo, admitiendo y actualizando con las nuevas funciones CSI y otras de NetApp.

Acerca de esta tarea

Debes seguir este procedimiento si eres un usuario del Centro de control de Astra con licencia y quieres utilizar la funcionalidad de aprovisionamiento de Astra Control. También debes seguir este procedimiento si eres usuario de Astra Trident y quieres utilizar la funcionalidad adicional que proporciona el aprovisionador de Astra Control sin utilizar también Astra Control.

En cada caso, la funcionalidad de aprovisionador no está habilitada de manera predeterminada en Astra Trident 24,02 y debe estar habilitada.

Antes de empezar

Si habilita el aprovisionador de Astra Control, primero haga lo siguiente:

Astra Control proporciona a los usuarios aprovisionamiento con Astra Control Center

- **Obtén una licencia de Astra Control Center**: Necesitarás una "Licencia de Astra Control Center" Para habilitar el aprovisionador de Astra Control y acceder a las funcionalidades que ofrece.
- **Instalar o actualizar a Astra Control Center 23,10 o posterior**: Necesitarás la última versión de Astra Control Center (24,02) si planeas usar la última funcionalidad de Astra Control Provisionador (24,02) con Astra Control.
- **Confirme que su clúster tiene una arquitectura de sistema AMD64**: La imagen del aprovisionador de Astra Control se proporciona en las arquitecturas de CPU AMD64 y ARM64, pero solo AMD64 es compatible con Astra Control Center.
- **Obtén una cuenta del Servicio de control de Astra para acceder al registro**: Si tienes la intención de usar el Registro de control de Astra en lugar del Sitio de soporte de NetApp para descargar la imagen del aprovisionador de control de Astra, completa el registro para un "Cuenta de Astra Control Service". Después de completar, enviar el formulario y crear una cuenta de BlueXP, recibirás un correo electrónico de bienvenida de Astra Control Service.
- **Si tienes Astra Trident instalado, confirma que su versión está dentro de una ventana de cuatro versiones**: Puedes realizar una actualización directa a Astra Trident 24,02 con el aprovisionador de control de Astra si tu Astra Trident está dentro de una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a 24,02.

El aprovisionador de Astra Control solo para los usuarios

- **Obtén una licencia de Astra Control Center**: Necesitarás una "Licencia de Astra Control Center" Para habilitar el aprovisionador de Astra Control y acceder a las funcionalidades que ofrece.
- **Si tienes Astra Trident instalado, confirma que su versión está dentro de una ventana de cuatro versiones**: Puedes realizar una actualización directa a Astra Trident 24,02 con el aprovisionador de control de Astra si tu Astra Trident está dentro de una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a 24,02.
- **Obtén una cuenta de Astra Control Service para acceder al registro**: Necesitarás acceder al registro para descargar imágenes de Astra Control Provisionador. Para comenzar, complete el registro para una "Cuenta de Astra Control Service". Después de completar, enviar el formulario y crear una cuenta de BlueXP, recibirás un correo electrónico de bienvenida de Astra Control Service.

(Paso 1) Obtén la imagen del aprovisionador de Astra Control

Los usuarios de Astra Control Center pueden obtener la imagen del aprovisionador de control de Astra mediante el registro de Astra Control o el método del sitio de soporte de NetApp. Los usuarios de Astra Trident que deseen utilizar el aprovisionador de control de Astra sin Astra Control deben utilizar el método de registro.

Registro de imágenes de Astra Control

> Puede utilizar Podman en lugar de Docker para los comandos de este procedimiento. Si se utiliza un entorno de Windows, se recomienda PowerShell.

1. Acceda al registro de imágenes de Astra Control de NetApp:
   a. Inicie sesión en la interfaz de usuario web de Astra Control Service y seleccione el icono de figura situado en la parte superior derecha de la página.
   b. Seleccione **acceso API**.
   c. Escriba su ID de cuenta.
   d. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.
   e. Inicia sesión en el registro de Astra Control usando el método que prefieras:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-
token>
```

2. (Solo registros personalizados) Siga estos pasos para mover la imagen a su registro personalizado. Si no está utilizando un registro, siga los pasos del operador Trident en la "siguiente sección".
   a. Extrae la imagen del aprovisionador de Astra Control del registro:

> La imagen extraída no soportará múltiples plataformas y solo soportará la misma plataforma que el host que sacó la imagen, como Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Ejemplo:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0 --platform
linux/amd64
```

   a. Etiquete la imagen:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

   b. Introduzca la imagen en el registro personalizado:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

> Puede utilizar Crane copy como alternativa a la ejecución de estos comandos Docker: `crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0 <my_custom_registry>/trident-acp:24.02.0`

Sitio de soporte de NetApp

1. Descarga el bundle Astra Control Provisioner (`trident-acp-[version].tar`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (astra-control-center-certs-[version].tar.gz) para verificar la firma del paquete tar trident-acp-[version].

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
   ```

3. Cargue la imagen del aprovisionador de Astra Control:

   ```
   docker load < trident-acp-24.02.0.tar
   ```

   Respuesta:

   ```
   Loaded image: trident-acp:24.02.0-linux-amd64
   ```

4. Etiquete la imagen:

   ```
   docker tag trident-acp:24.02.0-linux-amd64 <my_custom_registry>/trident-acp:24.02.0
   ```

5. Introduzca la imagen en el registro personalizado:

   ```
   docker push <my_custom_registry>/trident-acp:24.02.0
   ```

(Paso 2) Habilitar el aprovisionador de Astra Control en Astra Trident

Determine si el método de instalación original ha utilizado un "Operador (manualmente o con Helm) o tridentctl" y complete los pasos apropiados de acuerdo con su método original.

Operador Astra Trident

1. "Descarga el instalador de Astra Trident y extráigalo".
2. Complete estos pasos si todavía no ha instalado Astra Trident o si ha quitado el operador de la implementación original de Astra Trident:
   a. Cree el CRD:

   ```
   kubectl create -f
   deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
   aml
   ```

   b. Cree el espacio de nombres trident (`kubectl create namespace trident`) o confirme que el espacio de nombres trident sigue existiendo (`kubectl get all -n trident`). Si el espacio de nombres se ha eliminado, vuelva a crearlo.
3. Actualice Astra Trident a 24.02.0:

   > Para los clústeres que ejecutan Kubernetes 1,24 o una versión anterior, utilice `bundle_pre_1_25.yaml`. Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice `bundle_post_1_25.yaml`.

   ```
   kubectl -n trident apply -f trident-installer/deploy/<bundle-
   name.yaml>
   ```

4. Compruebe que Astra Trident está ejecutando:

   ```
   kubectl get torc -n trident
   ```

   Respuesta:

   ```
   NAME      AGE
   trident   21m
   ```

5. Si tienes un registro que usa secretos, crea un secreto para extraer la imagen del aprovisionador de Astra Control:

   ```
   kubectl create secret docker-registry <secret_name> -n trident
   --docker-server=<my_custom_registry> --docker-username=<username>
   --docker-password=<token>
   ```

6. Edite el CR de TridentOrchestrator y realice las siguientes modificaciones:

```
kubectl edit torc trident -n trident
```

a. Establezca una ubicación de registro personalizada para la imagen de Astra Trident o extráigala del registro de Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0` o. `tridentImage: netapp/trident:24.02.0`).

b. Habilita el aprovisionador de Astra Control (`enableACP: true`).

c. Establezca la ubicación de registro personalizada para la imagen del aprovisionador de Astra Control o sáquela del registro de Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0` o. `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).

d. Si estableció la imagen descubre los secretos anteriormente en este procedimiento, puede establecerlos aquí (`imagePullSecrets: - <secret_name>`). Utilice el mismo nombre secreto que estableció en los pasos anteriores.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

7. Guarde y salga del archivo. El proceso de despliegue comenzará automáticamente.
8. Compruebe que se han creado el operador, el despliegue y los replicasets.

```
kubectl get all -n trident
```

> Solo debe haber **una instancia** del operador en un clúster de Kubernetes. No cree varias implementaciones del operador Trident de Astra.

9. Compruebe el `trident-acp` container se está ejecutando y eso `acpVersion` es `24.02.0` con el estado de `Installed`:

```
kubectl get torc -o yaml
```

Respuesta:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

1. "Descarga el instalador de Astra Trident y extráigalo".
2. "Si ya tiene un Astra Trident existente, desinstálelo del clúster que lo aloja".
3. Instale Astra Trident con el aprovisionador de control de Astra habilitado (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

4. Confirme que se ha habilitado el aprovisionador de Astra Control:

```
./tridentctl -n trident version
```

Respuesta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 24.02.0 | 24.02.0 | 24.02.0. | +----------------
+----------------+-------------+
```

Timón

1. Si tiene Astra Trident 23.07.1 o anterior instalado, "desinstalar" el operador y otros componentes.
2. Si tu clúster de Kubernetes ejecuta la versión 1,24 o anterior, elimina psp:

```
kubectl delete psp tridentoperatorpod
```

3. Añada el repositorio de Astra Trident Helm:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-
chart
```

4. Actualice el gráfico Helm:

```
helm repo update netapp-trident
```

Respuesta:

```
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. □Happy Helming!□
```

5. Enumere las imágenes:

```
./tridentctl images -n trident
```

Respuesta:

```
| v1.28.0            | netapp/trident:24.02.0|
|                    | docker.io/netapp/trident-autosupport:24.02|
|                    | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                    | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                    | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                    | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                    | registry.k8s.io/sig-storage/csi-node-driver-
registrar:v2.10.0 |
|                    | netapp/trident-operator:24.02.0 (optional)
```

6. Asegúrese de que el trident-operator 24.02.0 esté disponible:

```
helm search repo netapp-trident/trident-operator --versions
```

Respuesta:

```
NAME                            CHART VERSION   APP VERSION
DESCRIPTION
netapp-trident/trident-operator 100.2402.0      24.02.0         A
```

7. Uso `helm install` y ejecute una de las siguientes opciones que incluyen estos ajustes:
   - Un nombre para la ubicación de despliegue
   - La versión de Trident de Astra
   - El nombre de la imagen del aprovisionador de Astra Control
   - La marca para habilitar el aprovisionador
   - (Opcional) Una ruta de registro local. Si está utilizando un registro local, su "Imágenes de Trident" Se pueden ubicar en un registro o en diferentes registros, pero todas las imágenes CSI deben estar ubicadas en el mismo registro.
   - El espacio de nombres de Trident

Opciones

- Imágenes sin registro

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-acp:24.02.0
--set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Imágenes en uno o más registros

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Puede utilizar `helm list` para revisar detalles de la instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación, y el número de revisión.

Si tiene problemas para poner en marcha Trident mediante Helm, ejecute este comando para desinstalar completamente Astra Trident:

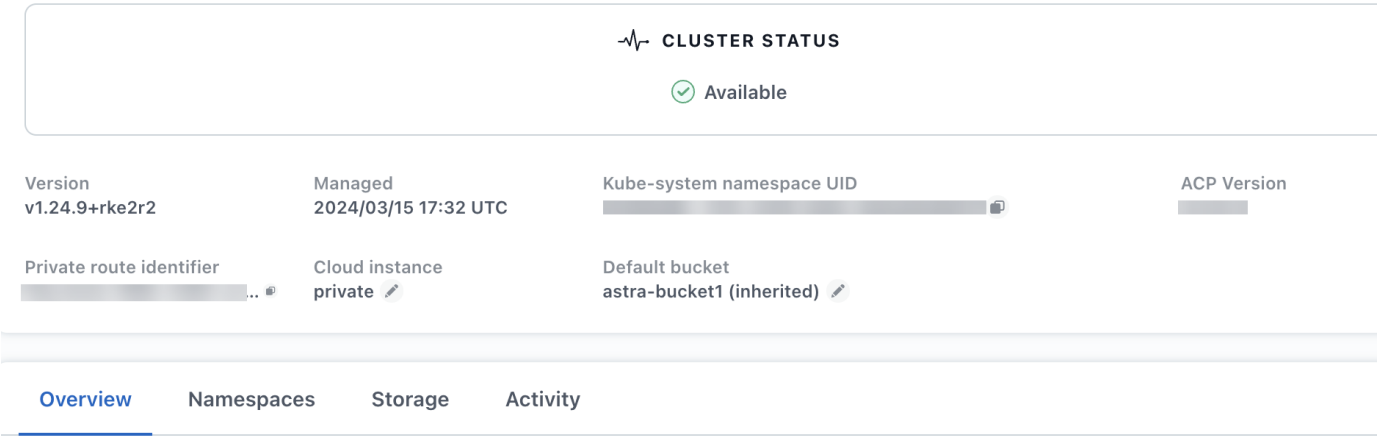
```
./tridentctl uninstall -n trident
```

No "Elimina por completo los CRD de Astra Trident" Como parte de la desinstalación antes de intentar habilitar de nuevo Astra Control Provisioner.

Resultado

Está habilitada la funcionalidad de aprovisionamiento de Astra Control y es posible usar cualquier función disponible para la versión que esté ejecutando.

(Solo para usuarios de Astra Control Center) Después de instalar Astra Control Provisioner, el clúster que aloja el aprovisionador en la interfaz de usuario de Astra Control Center mostrará un `ACP version` en lugar de `Trident version` campo y núm. de versión instalada actual.



Si quiere más información

- "Documentación sobre actualizaciones de Astra Trident"

Prepare su entorno para la gestión de clústeres con Astra Control

Antes de añadir un clúster, debe asegurarse de que se cumplen las siguientes condiciones previas. También debe realizar comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para añadirse a Astra Control Center y crear roles de clúster kubeconfig según sea necesario.

Astra Control le permite añadir clústeres gestionados mediante recurso personalizado (CR) o kubeconfig, en función de su entorno y sus preferencias.

Antes de empezar

- **Cumplir con los requisitos ambientales**: Su entorno cumple "requisitos del entorno operativo" Para Astra Control Center.
- * Configurar nodos de trabajador*: Asegúrese de que usted "configure los nodos de trabajo" en su clúster con los controladores de almacenamiento adecuados para que los pods puedan interactuar con el almacenamiento back-end.
- **Habilitar restricciones PSA**: Si su clúster tiene activada la aplicación de admisión de seguridad de pod, que es estándar para los clústeres de Kubernetes 1,25 y posteriores, debe habilitar las restricciones PSA en estos espacios de nombres:
  - `netapp-acc-operator` espacio de nombres:

```
kubectl label --overwrite ns netapp-acc-operator pod-
security.kubernetes.io/enforce=privileged
```

- `netapp monitoring` espacio de nombres:

```
kubectl label --overwrite ns netapp-monitoring pod-
security.kubernetes.io/enforce=privileged
```

- **Credenciales de ONTAP**: Necesita credenciales de ONTAP y un superusuario e ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center.

  Ejecute los siguientes comandos en la línea de comandos de la ONTAP:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

- **Requisitos de clúster gestionados por kubeconfig**: Estos requisitos son específicos para los clusters de aplicaciones gestionados por kubeconfig.
  - **Hacer kubeconfig accesible**: Usted tiene acceso a la "kubeconfig de cluster por defecto" eso "ha configurado durante la instalación".
  - **Consideraciones de la autoridad de certificación**: Si está agregando el clúster usando un archivo kubeconfig que hace referencia a una autoridad de certificación (CA) privada, agregue la siguiente línea a la `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

```
insecure-skip-tls-verify: true
```

  - **Sólo rancher**: Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.
- **Requisitos del aprovisionador de Astra Control**: Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident**: Antes de instalar o actualizar el aprovisionador de Astra Control, revise el "compatibles con front-ends, back-ends y configuraciones de host".
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control**: Se recomienda instalar Astra Trident 23,10 o posterior y activar "Funcionalidad de almacenamiento avanzada de Astra Control Provisioning". En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento**: Al menos un backend de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster.

- **Configure una clase de almacenamiento**: Al menos una clase de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster. Si se configura una clase de almacenamiento predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.
- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen**: "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

Ejecutar las comprobaciones de elegibilidad

Ejecute las siguientes comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

Pasos

1. Determine la versión de Astra Trident que ejecuta:

   ```
   kubectl get tridentversion -n trident
   ```

   Si existe Astra Trident, obtendrá un resultado similar al siguiente:

   ```
   NAME      VERSION
   trident   24.02.0
   ```

   Si Astra Trident no existe, obtendrá un resultado similar al siguiente:

   ```
   error: the server doesn't have a resource type "tridentversions"
   ```

2. Debe realizar una de las siguientes acciones:
   - Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos "instrucciones" Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede hacerlo "realice una actualización directa" Para Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.
   - Si utiliza Astra Trident 23,10 o una versión posterior, compruebe que el aprovisionador de Astra Control haya sido "activado". El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. "Actualiza tu aprovisionador de Astra Control" De modo que tiene la misma versión que Astra Control Center que vas a actualizar para acceder a la funcionalidad más reciente.
3. Asegúrese de que todos los pods (incluidos `trident-acp`) se están ejecutando:

   ```
   kubectl get pods -n trident
   ```

4. Determine si las clases de almacenamiento están utilizando los controladores Astra Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get sc
```

Respuesta de ejemplo:

```
NAME                   PROVISIONER            RECLAIMPOLICY
VOLUMEBINDINGMODE  ALLOWVOLUMEEXPANSION  AGE
ontap-gold (default)  csi.trident.netapp.io  Delete         Immediate
true                   5d23h
```

Crear un rol de cluster kubeconfig

En el caso de los clústeres que se gestionan mediante kubeconfig, puede crear una función de administrador de permisos limitados o de permisos ampliados para Astra Control Center. Este no es un procedimiento obligatorio para la configuración de Astra Control Center, ya que ya configuró un kubeconfig como parte de la "proceso de instalación".

Este procedimiento le ayuda a crear un kubeconfig independiente si cualquiera de los siguientes escenarios se aplica a su entorno:

- Deseas limitar los permisos de Astra Control a los clústeres que gestiona
- Usas varios contextos y no puedes usar el comando predeterminado de Astra Control configurado durante la instalación o un rol limitado con un solo contexto no funcionará en tu entorno

Antes de empezar

Asegúrese de que tiene lo siguiente para el clúster que tiene intención de administrar antes de completar los pasos del procedimiento:

- kubectl v1.23 o posterior instalado
- Acceda con atención al clúster que pretende añadir y gestionar con Astra Control Center

> Para este procedimiento, no necesita acceso kubectl al clúster que ejecuta Astra Control Center.

- Una imagen de referencia activa para el clúster que pretende gestionar con derechos de administrador del clúster para el contexto activo

Pasos

1. Cree una cuenta de servicio:
   a. Cree un archivo de cuenta de servicio llamado `astracontrol-service-account.yaml`.

```
<strong>astracontrol-service-account.yaml</strong>
```

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

b. Aplicar la cuenta de servicio:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. Cree uno de los siguientes roles de clúster con permisos suficientes para que Astra Control gestione un clúster:

Rol de clúster limitado

Este rol contiene los permisos mínimos necesarios para que Astra Control gestione un clúster:

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```
    - horizontalpodautoscalers
    - ingresses
    - jobs
    - namespaces
    - networkpolicies
    - persistentvolumeclaims
    - poddisruptionbudgets
    - pods
    - podtemplates
    - replicasets
    - replicationcontrollers
    - replicationcontrollers/scale
    - rolebindings
    - roles
    - secrets
    - serviceaccounts
    - services
    - statefulsets
    - tridentmirrorrelationships
    - tridentsnapshotinfos
    - volumesnapshots
    - volumesnapshotcontents
    verbs:
    - delete

  # Watch resources
  # Necessary to monitor progress
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    verbs:
    - watch

  # Update resources
  - apiGroups:
    - ""
    - build.openshift.io
    - image.openshift.io
    resources:
    - builds/details
    - replicationcontrollers
    - replicationcontrollers/scale
    - imagestreams/layers
```

```
  - imagestreamtags
  - imagetags
  verbs:
  - update
```

b. (Solo para clústeres de OpenShift) Añada lo siguiente al final del `astra-admin-account.yaml` archivo:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

c. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

Rol del clúster ampliado

Este rol contiene permisos ampliados para que un clúster lo gestione Astra Control. Puedes usar este rol si utilizas varios contextos y no puedes utilizar el comando kubeconfig predeterminado de Astra Control configurado durante la instalación o un rol limitado con un único contexto no funcionará en tu entorno:

> Lo siguiente `ClusterRole` Los pasos son un ejemplo general de Kubernetes. Consulte la documentación de la distribución de Kubernetes para obtener instrucciones específicas de su entorno.

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Cree el enlace de rol de clúster para el rol del clúster a la cuenta de servicio:

a. Cree un `ClusterRoleBinding` archivo llamado `astracontrol-clusterrolebinding.yaml`.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

b. Aplique el enlace de roles del clúster:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. Crear y aplicar el secreto de token:
   a. Cree un archivo secreto de token llamado `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

   b. Aplique el secreto de token:

```
kubectl apply -f secret-astracontrol-service-account.yaml
```

5. Agregue el secreto de token a la cuenta de servicio agregando su nombre a la `secrets` array (la última línea del siguiente ejemplo):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

6. Enumere los secretos de la cuenta de servicio, reemplazando `<context>` con el contexto correcto para su instalación:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

El final de la salida debe ser similar a lo siguiente:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-48xhx` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

7. Genere la kubeconfig de la siguiente manera:
   a. Cree un `create-kubeconfig.sh` archivo.
   b. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  *-o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token-
user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

c. Origen de los comandos para aplicarlos al clúster de Kubernetes.

```
source create-kubeconfig.sh
```

8. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

(Vista previa técnica) Instale Astra Connector para clústeres gestionados

Los clústeres gestionados por Astra Control Center utilizan Astra Connector para permitir la comunicación entre el clúster gestionado y Astra Control Center. Debe instalar Astra Connector en todos los clústeres que desee gestionar.

Instala Astra Connector

Instalas Astra Connector con comandos de Kubernetes y archivos de recursos personalizados (CR).

Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster que desee gestionar con Astra Control.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

Antes de empezar

- Necesitas acceder al clúster que quieras gestionar con Astra Control.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

> Si el clúster está configurado con la aplicación de admisión de seguridad de POD, que es el valor predeterminado para los clústeres de Kubernetes 1,25 y posteriores, tiene que habilitar las restricciones PSA en los espacios de nombres correspondientes. Consulte "Prepare su entorno para la gestión de clústeres con Astra Control" si desea obtener instrucciones.

Pasos

1. Instala el operador Astra Connector en el clúster que quieras gestionar con Astra Control. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la "Documentación de Astra Automation" si desea obtener instrucciones.
4. Cree un secreto con el token. Reemplaza <API_TOKEN> por el token que has recibido de Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crea un secreto de Docker para extraer la imagen de Astra Connector. Sustituya los valores entre paréntesis <> por información de su entorno:

> Puedes encontrar la instancia de <ASTRA_CONTROL_ACCOUNT_ID> en la interfaz de usuario web de Astra Control. En la interfaz de usuario web, seleccione el icono de figura en la parte superior derecha de la página y seleccione **Acceso API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <ASTRA_CONTROL_ACCOUNT_ID>: Obtenida de la interfaz de usuario web de Astra Control durante el paso anterior.

- <CLUSTER_NAME>: El nombre que se debe asignar este clúster en Astra Control.
- <ASTRA_CONTROL_URL>: La URL de interfaz de usuario web de Astra Control. Por ejemplo:

```
https://astra.control.url
```

```yaml
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

9. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

Debería ver una salida similar a la siguiente:

```
NAMESPACE          NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    astra-connector    true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Compruebe que el clúster aparezca en la lista de clústeres gestionados de la página **Clusters** de la interfaz de usuario web de Astra Control.

Añadir un clúster

Para comenzar a gestionar las aplicaciones, añada un clúster de Kubernetes y gestiónelo como un recurso de computación. Es necesario añadir un clúster para Astra Control Center para descubrir sus aplicaciones Kubernetes.

> Le recomendamos que Astra Control Center gestione el clúster en el que se implementa primero antes de añadir otros clústeres a Astra Control Center para su gestión. Disponer del cluster inicial en administración es necesario para enviar datos Kubemetrics y datos asociados al cluster para mediciones y resolución de problemas.

Antes de empezar

- Antes de añadir un clúster, revise y realice la operación necesaria "requisitos previos".
- Si utiliza un controlador de SAN de ONTAP, asegúrese de que multivía esté habilitado en todos los clústeres de Kubernetes.

Pasos

1. Acceda desde el menú Dashboard o Clusters:
   - En **Panel** en Resumen de recursos, seleccione **Agregar** en el panel Clusters.
   - En el área de navegación de la izquierda, seleccione **Clusters** y, a continuación, seleccione **Add Cluster** en la página Clusters.
2. En la ventana **Agregar clúster** que se abre, cargue un `kubeconfig.yaml` archivar o pegar el contenido de un `kubeconfig.yaml` archivo.

   > La `kubeconfig.yaml` el archivo debe incluir **sólo la credencial de cluster para un cluster**.

   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "Documentación de Kubernetes" para obtener información acerca de cómo crear `kubeconfig` archivos. Si creó una imagen de kubeconfig para una función de clúster limitada mediante "este proceso", asegúrese de cargar o pegar esa kubeconfig en este paso.

3. Introduzca un nombre de credencial. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
4. Seleccione **Siguiente**.
5. Seleccione la clase de almacenamiento predeterminada que se utilizará para este clúster de Kubernetes y seleccione **Siguiente**.

> Debe seleccionar una clase de almacenamiento que esté configurada en el aprovisionador de control de Astra y que esté respaldada por el almacenamiento de ONTAP.

6. Revise la información y si todo parece bien, seleccione **Agregar**.

Resultado

El clúster entra en el estado **descubriendo** y luego cambia a **saludable**. Ahora está gestionando el clúster con Astra Control Center.

> Después de agregar un clúster para administrarlo en Astra Control Center, puede que el operador de supervisión tarde unos minutos en implementar. Hasta entonces, el icono de notificación se vuelve rojo y registra un evento **Comprobación de estado del agente de supervisión fallida**. Puede ignorar esto porque el problema se resuelve cuando Astra Control Center obtiene el estado correcto. Si el problema no se resuelve en unos minutos, vaya al clúster y ejecute `oc get pods -n netapp-monitoring` como punto de partida. Tendrá que buscar en los registros del operador de supervisión para depurar el problema.

Habilite la autenticación en el back-end de almacenamiento ONTAP

El Centro de control de Astra ofrece dos modos de autenticación de un back-end de ONTAP:

- **Autenticación basada en credenciales**: El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos requeridos. Debe utilizar un rol de inicio de sesión de seguridad predefinido, como admin o vsadmin, para garantizar la máxima compatibilidad con las versiones de ONTAP.
- **Autenticación basada en certificados**: Astra Control Center también puede comunicarse con un clúster de ONTAP utilizando un certificado instalado en el backend. Debe usar el certificado de cliente, la clave y el certificado de CA de confianza si se utilizan (recomendado).

Más adelante, puede actualizar los back-ends existentes para pasar de un tipo de autenticación a otro método. Solo se admite un método de autenticación a la vez.

Habilite la autenticación basada en credenciales

Astra Control Center requiere las credenciales para un ámbito del clúster `admin` Para comunicarse con el backend de ONTAP. Debe utilizar roles estándar predefinidos como `admin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones para que las utilicen en futuras versiones del Centro de control de Astra.

> Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Astra Control Center, pero no es recomendable.

Una definición de backend de ejemplo tiene el siguiente aspecto:

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

La definición de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. De este modo, se trata de una operación exclusiva para administrador que realiza el administrador de Kubernetes o de almacenamiento.

Habilite la autenticación basada en certificados

Astra Control Center puede utilizar certificados para comunicarse con back-ends de ONTAP nuevos y existentes. Debe introducir la siguiente información en la definición de backend.

- `clientCertificate`: Certificado de cliente.
- `clientPrivateKey`: Clave privada asociada.
- `trustedCACertificate`: Certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Es posible usar uno de los siguientes tipos de certificados:

- Certificado autofirmado
- Certificado de terceros

Habilite la autenticación con un certificado autofirmado

Un flujo de trabajo típico implica los pasos siguientes.

Pasos

1. Genere una clave y un certificado de cliente. Al generar, defina el nombre común (CN) en el usuario ONTAP para autenticarse como.

   ```
   openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
   -out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
   ```

2. Instale el certificado de cliente de tipo `client-ca` Y el clúster de ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Confirme que el rol de inicio de sesión de seguridad de ONTAP admite el método de autenticación de certificado.

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

4. Pruebe la autenticación mediante el certificado generado. Sustituya <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre SVM. Debe asegurarse de que la LIF tiene su política de servicio establecida en `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-
name>"><vserver-get></vserver-get></netapp>
```

5. Con los valores obtenidos del paso anterior, añada el back-end del almacenamiento en la interfaz de usuario de Astra Control Center.

Active la autenticación con un certificado de terceros

Si tiene un certificado de terceros, puede configurar la autenticación basada en certificados con estos pasos.

Pasos

1. Genere la clave privada y CSR:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem
-out ontap_cert_request.csr -keyout ontap_cert_request.key -addext
"subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>”
```

2. Transfiera la CSR a la CA de Windows (CA de terceros) y emita el certificado firmado.
3. Descargue el certificado firmado y asígnele el nombre `ontap_signed_cert.crt'
4. Exporte el certificado raíz de Windows CA (CA de terceros).
5. Asigne un nombre a este archivo `ca_root.crt`

   Ahora tiene los siguientes tres archivos:

- **Clave privada**: `ontap_signed_request.key` (Esta es la clave correspondiente para el certificado de servidor en ONTAP. Se necesita al instalar el certificado de servidor.)
- **Certificado firmado**: `ontap_signed_cert.crt` (Esto también se denomina *server certificate* en ONTAP.)
- **Certificado de CA raíz**: `ca_root.crt` (Esto también se denomina *server-ca certificate* en ONTAP.)

6. Instale estos certificados en ONTAP. Generar e instalar `server` y.. `server-ca` Certificados en ONTAP.

Expanda para sample.yaml

```
# Copy the contents of ca_root.crt and use it here.

security certificate install -type server-ca

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:

CA:
serial:

The certificate's generated name for reference:


===

# Copy the contents of ontap_signed_cert.crt and use it here. For
key, use the contents of ontap_cert_request.key file.
security certificate install -type server
Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN PRIVATE KEY-----
<private key details>
-----END PRIVATE KEY-----

Enter certificates of certification authorities (CA) which form the
certificate chain of the server certificate. This starts with the
issuing CA certificate of the server certificate and can range up to
the root CA certificate.
Do you want to continue entering root and/or intermediate
```

```
certificates {y|n}: n

The provided certificate does not have a common name in the subject
field.
Enter a valid common name to continue installation of the
certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
The installed certificate's CA and serial number for reference:
CA:
serial:
The certificate's generated name for reference:


==
# Modify the vserver settings to enable SSL for the installed
certificate

ssl modify -vserver <vserver_name> -ca <CA>  -server-enabled true
-serial <serial number>       (security ssl modify)

==
# Verify if the certificate works fine:

openssl s_client -CAfile ca_root.crt -showcerts -servername server
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
CONNECTED(00000005)
depth=1 DC = local, DC = umca, CN = <CA>
verify return:1
depth=0
verify return:1
write W BLOCK
---
Certificate chain
0 s:
   i:/DC=local/DC=umca/<CA>

-----BEGIN CERTIFICATE-----
<Certificate details>
```

7. Cree el certificado de cliente para el mismo host para la comunicación sin contraseña. Astra Control Center utiliza este proceso para comunicarse con ONTAP.
8. Genere e instale los certificados de cliente en ONTAP:

Expanda para sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"

Copy the content of ontap_test_client.pem file and use it in the
below command:
security certificate install -type client-ca -vserver <vserver_name>

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<Certificate details>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
The installed certificate's CA and serial number for reference:

CA:
serial:
The certificate's generated name for reference:


==

ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)

# Setting permissions for certificates
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>

security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>

==

#Verify passwordless communication works fine with the use of only
certificates:

curl --cacert ontap_signed_cert.crt  --key ontap_test_client.key
--cert ontap_test_client.pem
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
{
```

```
"records": [
{
"uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
"name": "<aggr_name>",
"node": {
"uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
"name": "<node_name>",
"_links": {
"self": {
"href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
}
}
},
"_links": {
"self": {
"href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-
4bf5378b41bd"
}
}
}
],
"num_records": 1,
"_links": {
"self": {
"href": "/api/storage/aggregates"
}
}
}%
```


9. Añada el back-end de almacenamiento en la interfaz de usuario de Astra Control Center y proporcione los siguientes valores:
   - **Certificado de cliente**: ontap_test_client.pem
   - **Clave privada**: ontap_test_client.key
   - **Certificado de CA de confianza**: ontap_signed_cert.crt

Añada un back-end de almacenamiento

Después de configurar las credenciales o la información de autenticación de certificados, puede añadir un back-end de almacenamiento de ONTAP existente a Astra Control Center para gestionar sus recursos.

Gestionar los clústeres de almacenamiento en Astra Control como back-end de almacenamiento le permite obtener vínculos entre los volúmenes persistentes (VP) y el back-end de almacenamiento, así como mediciones de almacenamiento adicionales.

Añadir y gestionar back-ends de almacenamiento de ONTAP en Astra Control Center es opcional cuando se

utiliza la tecnología SnapMirror de NetApp si has habilitado el aprovisionador de control de Astra.

Pasos

1. En el panel de control del área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione **Agregar**.
3. En la sección Usar existente de la página Agregar backend de almacenamiento, seleccione **ONTAP**.
4. Seleccione una de las siguientes opciones:
   - **Usar credenciales de administrador**: Ingrese la dirección IP de administración del clúster de ONTAP y las credenciales de administración. Las credenciales deben ser credenciales para todo el clúster.

     > El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, aplique las credenciales de usuario con el rol "admin", que tiene los métodos de acceso `ontapi` y.. `http`, En clústeres ONTAP de origen y destino. Consulte "Gestionar cuentas de usuario en la documentación de ONTAP" si quiere más información.

   - **Utilice un certificado**: Cargue el certificado `.pem` archivo, la clave de certificado `.key` archivo y, opcionalmente, el archivo de entidad de certificación.
5. Seleccione **Siguiente**.
6. Confirme los detalles del backend y seleccione **Administrar**.

Resultado

El back-end aparece en la `online` estado en la lista con información resumida.

> Es posible que deba actualizar la página para que se muestre el back-end.

Añadir un bucket

Puede añadir un bloque con la interfaz de usuario de Astra Control o. "API de control Astra". Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina.

No necesita un bloque de Astra Control si clona la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster. La funcionalidad de snapshots de aplicaciones no requiere un bloque.

Antes de empezar

- Asegúrese de tener un bloque al que se puede acceder desde los clústeres que gestiona Astra Control Center.
- Asegúrese de tener credenciales para el bloque.
- Asegúrese de que el cucharón es uno de los siguientes tipos:
  - ONTAP S3 de NetApp
  - StorageGRID S3 de NetApp
  - Microsoft Azure

- Genérico S3

> Amazon Web Services (AWS) y Google Cloud Platform (GCP) utilizan el tipo de bloque Generic S3.

> Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Pasos

1. En el área de navegación de la izquierda, seleccione **Cuchos**.
2. Seleccione **Agregar**.
3. Seleccione el tipo de bloque.

> Cuando agregue un bloque, seleccione el proveedor de segmento correcto y proporcione las credenciales correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como tipo y acepta credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los futuros backups de aplicaciones y restauraciones usando este bucket.

4. Introduzca un nombre de bloque existente y una descripción opcional.

> El nombre y la descripción del bloque aparecen como una ubicación de backup que se puede elegir más adelante al crear un backup. El nombre también aparece durante la configuración de la política de protección.

5. Introduzca el nombre o la dirección IP del extremo de S3.
6. En **Seleccionar credenciales**, elija la ficha **Agregar** o **utilizar existente**.
   - Si ha elegido **Agregar**:
     i. Introduzca un nombre para la credencial que la distingue de otras credenciales en Astra Control.
     ii. Escriba el identificador de acceso y la clave secreta pegando el contenido del portapapeles.
   - Si ha elegido **utilizar existente**:
     i. Seleccione las credenciales existentes que desea utilizar con el bloque.
7. Seleccione `Add`.

> Cuando se agrega un bloque, Astra Control Marca un bloque con el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado. A medida que se añaden bloques, más adelante se puede decidir a. "establecer otro bloque predeterminado".

Conceptos

Arquitectura y componentes

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

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

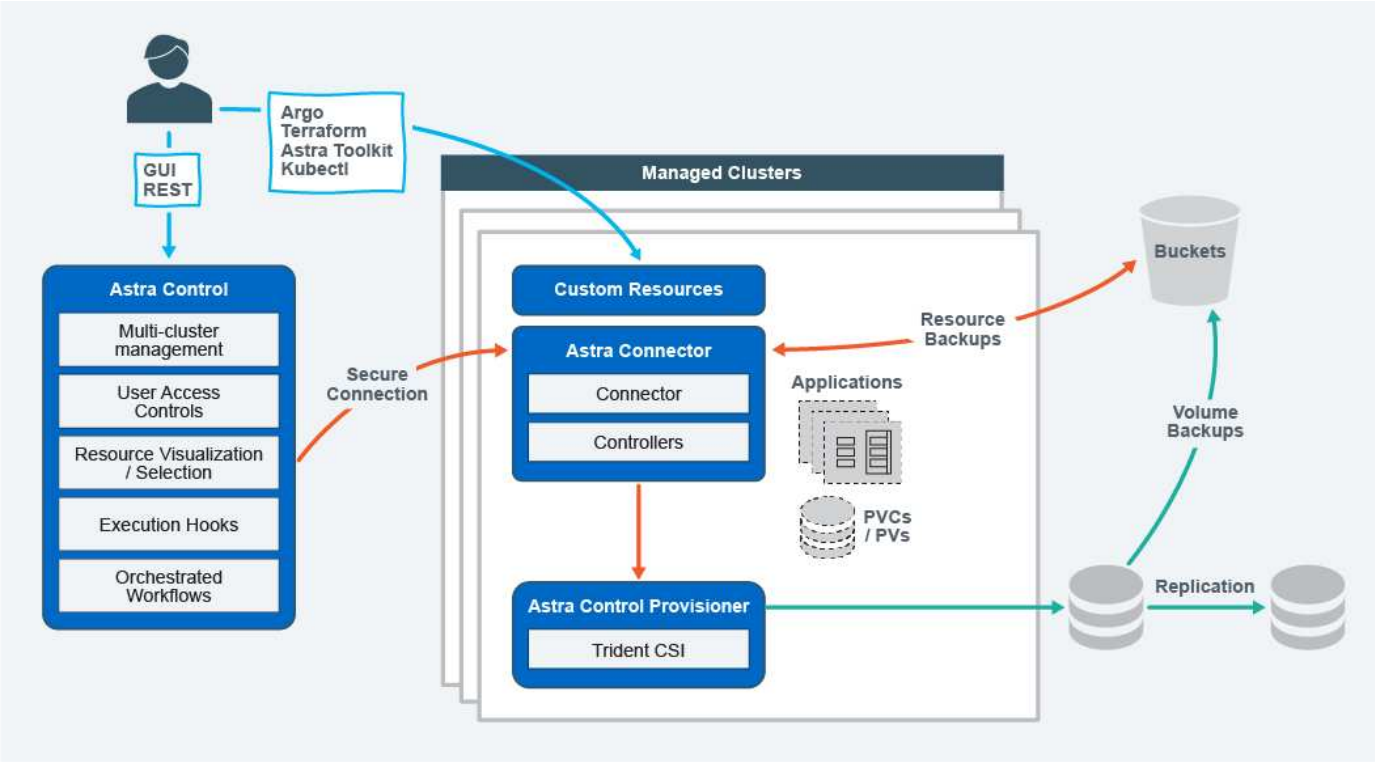
Mover:

- 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:

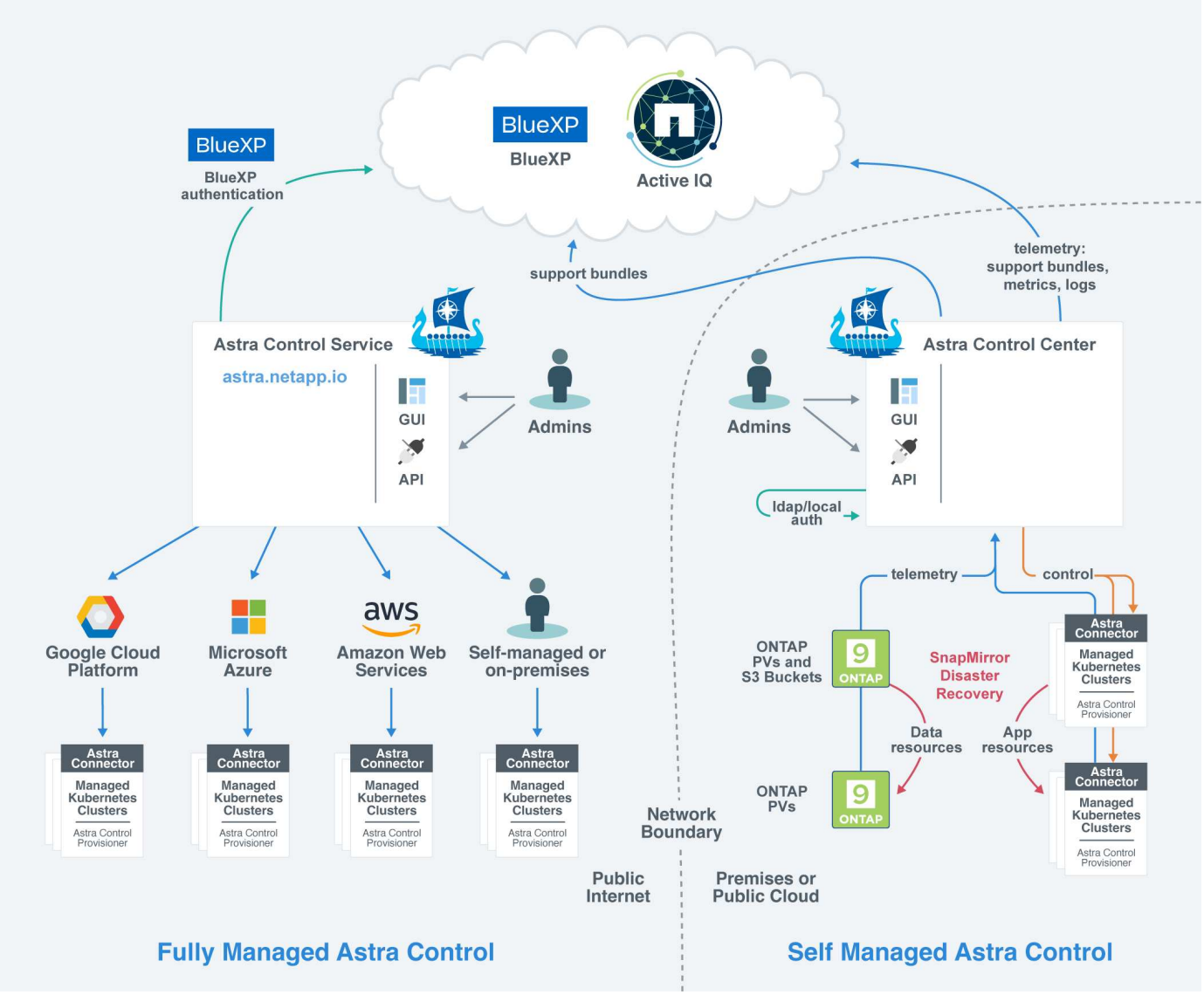
- **Astra Control**: Astra Control es el servicio de gestión centralizado para todos los clústeres gestionados, proporcionando cargas de trabajo orquestadas para la protección y movilidad de aplicaciones en la nube y on-premises, así como las siguientes capacidades:
  - Vista combinada de varios clústeres y clouds
  - 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 dos modelos de puesta en marcha.



- **Astra Control Service**: Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.

  "Documentación de Astra Control Service"

- **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"

	Servicio de control Astra	Astra Control Center
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En un cloud público que elija NetApp	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización
¿Cuáles son las distribuciones de Kubernetes compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure ▪ Azure Kubernetes Service (AKS) • **Clusters autogestionados** ◦ Kubernetes (ascendente) ◦ Motor Kubernetes de rancher (RKE) ◦ OpenShift Container Platform de Red Hat • * Clústeres locales* ◦ Red Hat OpenShift Container Platform en las instalaciones	• 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

	Servicio de control Astra	Astra Control Center

¿Cuáles son los back-ends de almacenamiento compatibles?	• * Proveedores en la nube*
	  ◦ Amazon Web Services
	  ▪ Amazon EBS
	  ▪ Amazon FSX para ONTAP de NetApp
	  ▪ "Cloud Volumes ONTAP"
	  ◦ Google Cloud
	  ▪ Disco persistente de Google
	  ▪ Cloud Volumes Service de NetApp
	  ▪ "Cloud Volumes ONTAP"
	  ◦ Microsoft Azure
	  ▪ Discos gestionados de Azure
	  ▪ Azure NetApp Files
	  ▪ "Cloud Volumes ONTAP"
	• **Clusters autogestionados**
	  ◦ Amazon EBS
	  ◦ Discos gestionados de Azure
	  ◦ Disco persistente de Google
	  ◦ "Cloud Volumes ONTAP"
	  ◦ NetApp MetroCluster
	  ◦ "El Longhorn"
	• * Clústeres locales*
	  ◦ NetApp MetroCluster
	  ◦ Sistemas ONTAP AFF y FAS de NetApp
	  ◦ ONTAP Select de NetApp
	  ◦ "Cloud Volumes ONTAP"
	  ◦ "El Longhorn"
		• Sistemas ONTAP AFF y FAS de NetApp
		• ONTAP Select de NetApp
		• "Cloud Volumes ONTAP"
		• "El Longhorn"

Si quiere más información

- "Documentación de Astra Control Service"
- "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:

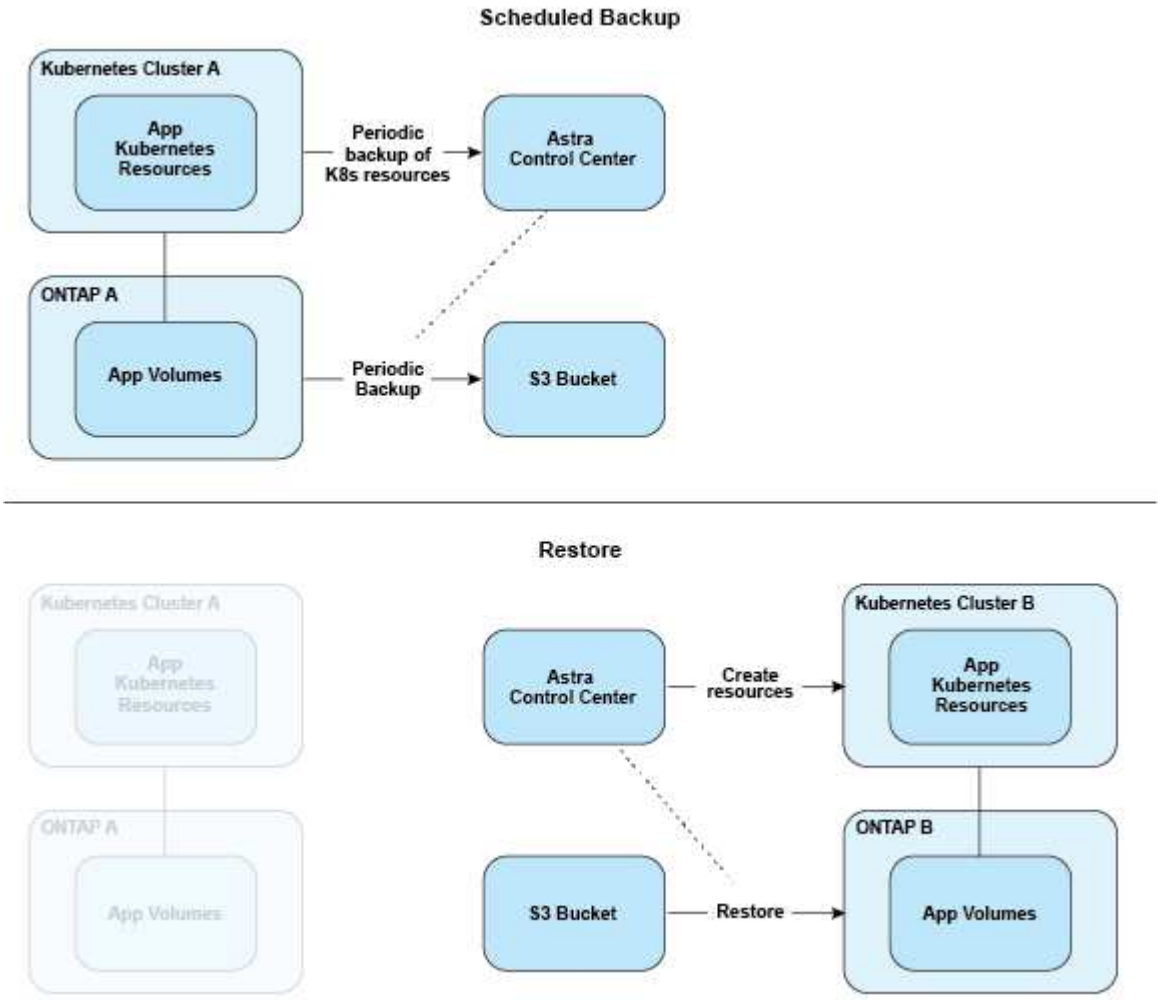
- **Replicación de aplicaciones**: Astra Control requiere que los clústeres de Kubernetes de origen y destino (que pueden ser el mismo clúster) estén disponibles y gestionados con sus respectivos back-ends de almacenamiento de ONTAP configurados para habilitar SnapMirror de NetApp. Astra Control toma 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

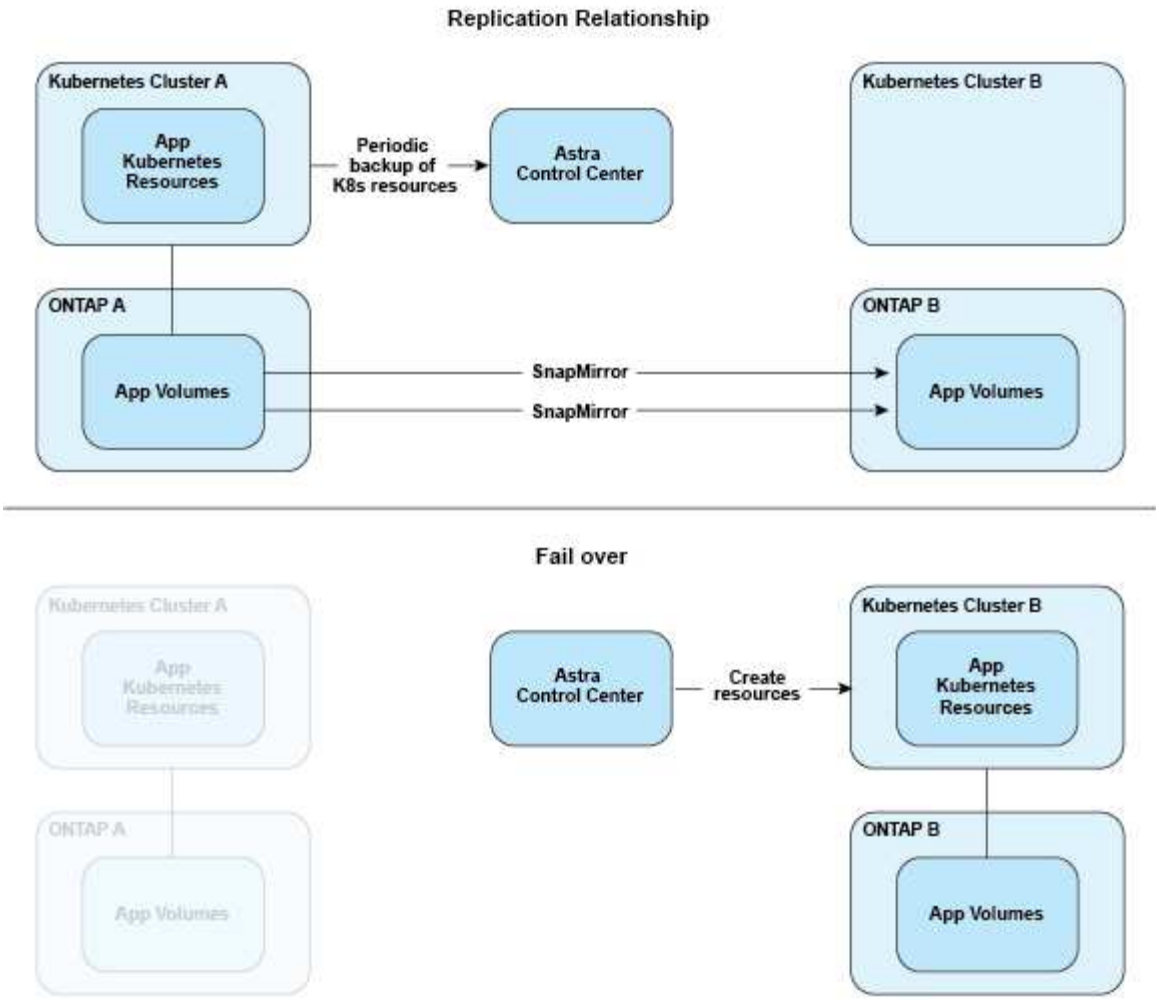
sistema remoto mediante la tecnología SnapMirror".

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.

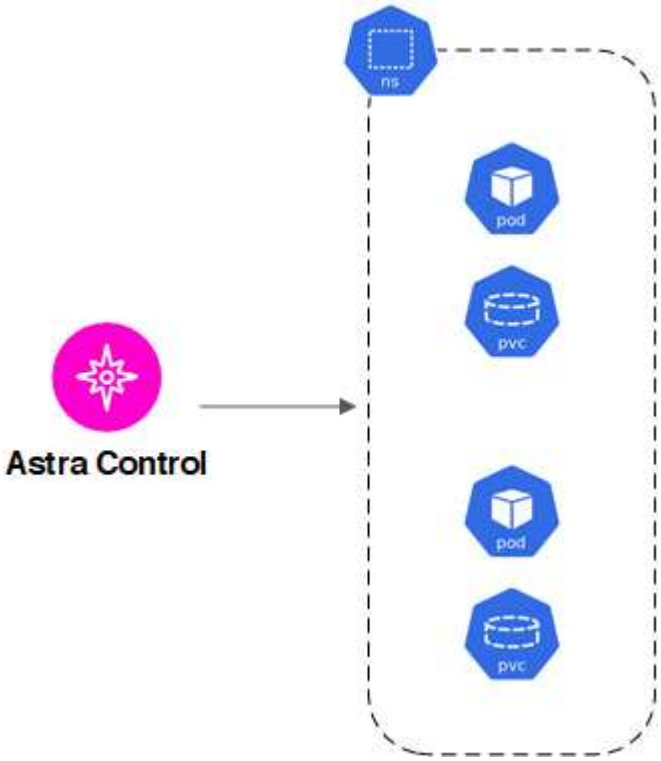
Obtenga más información

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

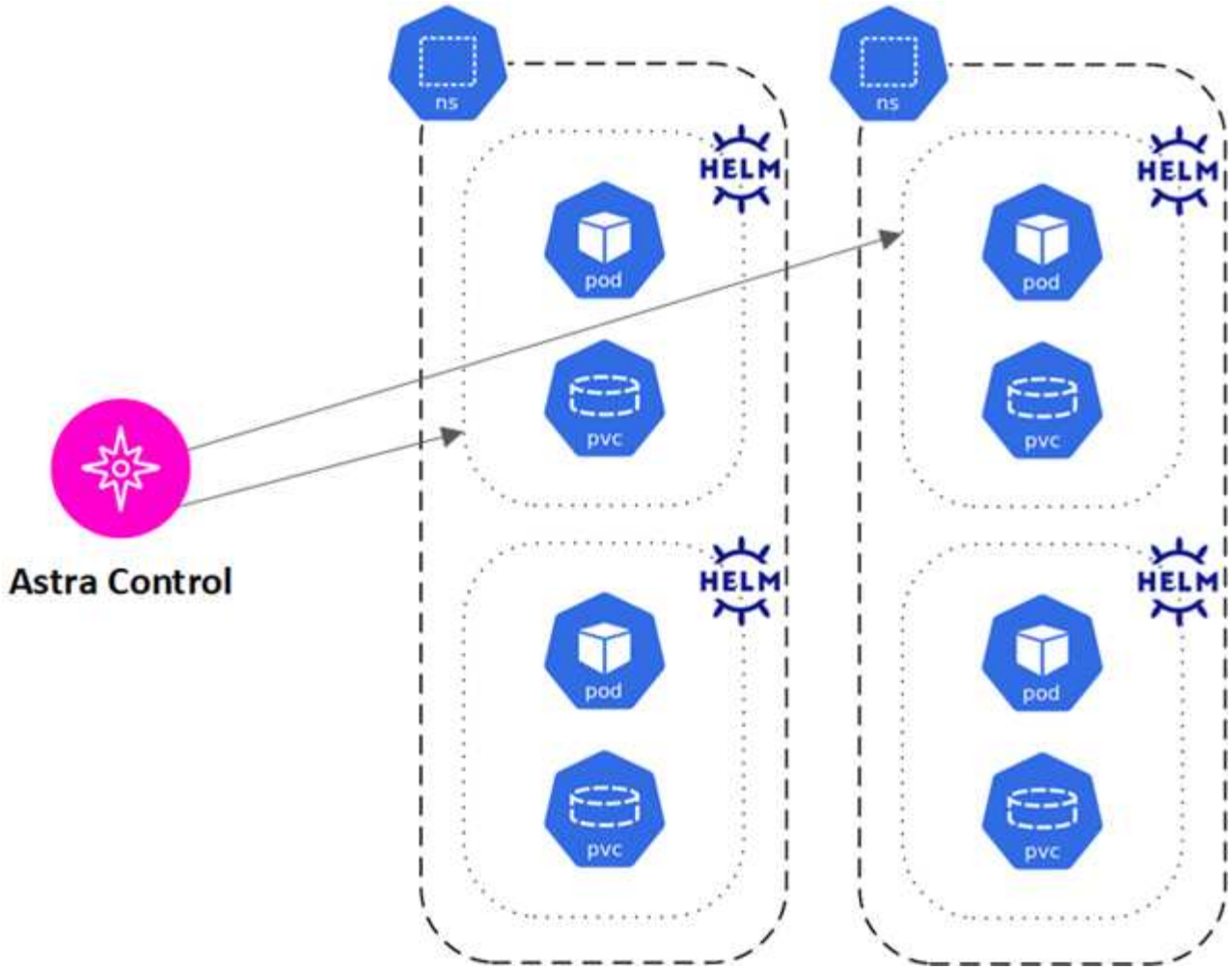
Gestión de aplicaciones

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:

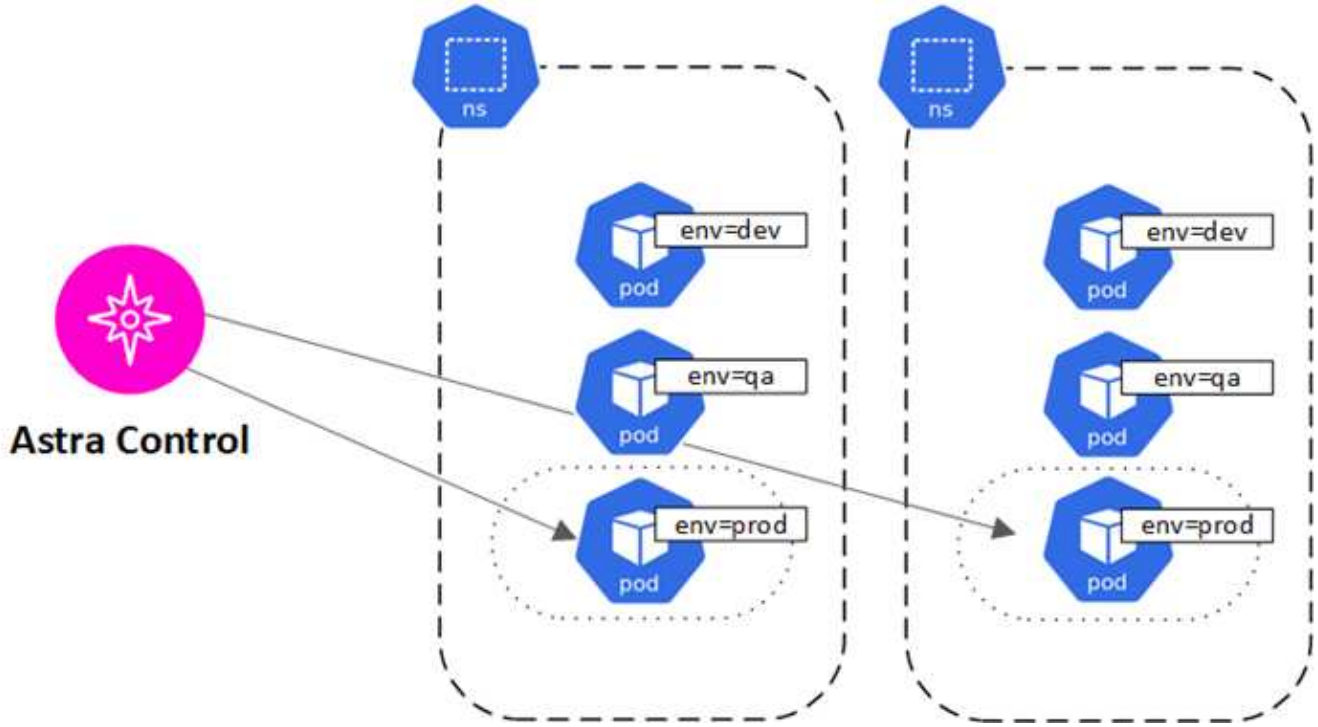
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- 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"

Utilice Astra Control Center

Inicie la gestión de aplicaciones

Usted primero "Añada un clúster a la gestión de Astra Control", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para definir las aplicaciones y sus recursos.

Puede definir y gestionar aplicaciones que incluyan recursos de almacenamiento con pods en ejecución o aplicaciones que incluyan recursos de almacenamiento sin ningún pods en ejecución. Las aplicaciones que no tienen pods en ejecución se conocen como aplicaciones de solo datos.

Y gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencias**: Para administrar aplicaciones con Astra Control Center, necesitas la licencia de evaluación integrada de Astra Control Center o una licencia completa.
- **Namespaces**: Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.
- **Clase de almacenamiento**: Si instala una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Recursos de Kubernetes**: Las aplicaciones que usan recursos de Kubernetes no recopilados por Astra Control podrían no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

Métodos de instalación de aplicaciones compatibles

Astra Control es compatible con los siguientes métodos de instalación de aplicaciones:

- **Fichero manifiesto**: Astra Control admite aplicaciones instaladas desde un archivo manifiesto mediante kubectl. Por ejemplo:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. Es totalmente compatible con la gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3). No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador**: Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres que, en general, están diseñadas con una arquitectura “pass-by-value” en lugar de “pass-by-reference”. Un operador y la aplicación que instala deben usar el mismo espacio de nombres; es posible que deba modificar el archivo YAML de implementación para que el operador se asegure de que este es el caso.

  Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

  - "Apache K8ssandra"

    > Para K8ssandra, se admiten operaciones de restauración in situ. Una operación de restauración a un nuevo espacio de nombres o clúster requiere que se apague la instancia original de la aplicación. Esto es para garantizar que la información del grupo de pares no conduzca a la comunicación entre instancias. No se admite la clonación de la aplicación.

  - "Jenkins CI"
  - "Clúster Percona XtraDB"

  Es posible que Astra Control no pueda clonar a un operador diseñado con una arquitectura "pase por referencia" (por ejemplo, el operador CockroachDB). Durante estos tipos de operaciones de clonado, el operador clonado intenta hacer referencia a los secretos de Kubernetes del operador de origen a pesar de tener su propio secreto nuevo como parte del proceso de clonado. Es posible que se produzca un error en la operación de clonado porque Astra Control no conoce los secretos de Kubernetes en el operador de origen.

Instale las aplicaciones en el clúster

La tienes "ha agregado el clúster" A Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Cualquier aplicación que se limita a uno o más espacios de nombres se puede gestionar.

Defina las aplicaciones

Una vez que Astra Control detecta espacios de nombres en sus clústeres, puede definir las aplicaciones que desea administrar. Puede elegir administrar una aplicación que abarque uno o más espacios de nombres o. gestione un espacio de nombres completo como una única aplicación. Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Aunque Astra Control le permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones en ese espacio de nombres o espacio de nombres expansivo), la práctica recomendada es elegir uno u otro. Las acciones que realice en Astra Control pueden fallar si las acciones se llevan a cabo al mismo tiempo tanto en el espacio de nombres como en el nivel de la aplicación.

A modo de ejemplo, puede que desee establecer una normativa de backup para «maria» con una cadencia semanal, pero es posible que deba realizar backups de «mariadb» (que se encuentra en el mismo espacio de nombres) con mayor frecuencia que esta. Según estas necesidades, debería gestionar las aplicaciones por separado, no como una aplicación de espacio de nombres único.

Antes de empezar

- Se añadió un clúster de Kubernetes a Astra Control.
- Una o más aplicaciones instaladas en el clúster. Obtenga más información sobre los métodos de instalación de aplicaciones compatibles.
- Espacios de nombres existentes en el clúster Kubernetes que se añadió a Astra Control.
- (Opcional) una etiqueta de Kubernetes en cualquiera "Recursos de Kubernetes compatibles".

Una etiqueta es una pareja clave/valor que se puede asignar a objetos de Kubernetes para su identificación. Las etiquetas facilitan la ordenación, la organización y la búsqueda de los objetos de Kubernetes. Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

Acerca de esta tarea

- Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".
- Si planea utilizar varios espacios de nombres con sus aplicaciones en Astra Control, "modificar los roles de usuario con restricciones de espacio de nombres" Tras actualizar a una versión de Astra Control Center compatible con varios espacios de nombres.
- Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte "Información sobre API y automatización de Astra".

Opciones de gestión de aplicaciones

- Defina los recursos que se van a administrar como una aplicación
- Defina un espacio de nombres para administrar como una aplicación
- "(Vista previa técnica) Definir una aplicación utilizando un recurso personalizado de Kubernetes"

Defina los recursos que se van a administrar como una aplicación

Puede especificar el "Los recursos de Kubernetes forman una aplicación" Que desea gestionar con Astra Control. Definir una aplicación le permite agrupar elementos de su clúster de Kubernetes en una única aplicación. Esta colección de recursos de Kubernetes está organizada por criterios de espacio de nombres y selector de etiquetas.

Definir una aplicación le proporciona un control más granular de lo que se debe incluir en una operación Astra Control, que incluye clonado, copias Snapshot y backups.

Al definir aplicaciones, asegúrese de no incluir un recurso de Kubernetes en varias aplicaciones con políticas de protección. La superposición de políticas de protección en recursos de Kubernetes puede provocar conflictos de datos. Más información en un ejemplo.

Amplíe para obtener más información sobre cómo agregar recursos de ámbito de cluster a los espacios de nombres de aplicaciones.

Puede importar recursos de clúster asociados a los recursos de espacio de nombres además de los que se incluyen automáticamente Astra Control. Puede agregar una regla que incluirá recursos de un grupo específico, tipo, versión y, opcionalmente, etiqueta. Es posible que desee hacer esto si hay recursos que Astra Control no incluye automáticamente.

No puede excluir ninguno de los recursos con ámbito de clúster que Astra Control incluya automáticamente.

Puede agregar lo siguiente `apiVersions` (Que son los grupos combinados con la versión API):

Tipo de recursos	ApiVersions (grupo + versión)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admissionregistration.k8s.io/v1
`ValidatingWebhookConfiguration`	admissionregistration.k8s.io/v1

Pasos

1. En la página aplicaciones, seleccione **definir**.
2. En la ventana **definir aplicación**, introduzca el nombre de la aplicación.
3. Seleccione el clúster en el que se ejecuta la aplicación en la lista desplegable **Cluster**.
4. Elija un espacio de nombres para su aplicación en la lista desplegable **espacio de nombres**.

   Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.

5. (Opcional) Introduzca una etiqueta para los recursos de Kubernetes en cada espacio de nombres. Puede especificar una sola etiqueta o un criterio de selector de etiquetas (consulta).

   Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

6. (Opcional) Añada espacios de nombres adicionales para la aplicación seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
7. (Opcional) Introduzca los criterios de etiqueta única o selector de etiquetas para los espacios de nombres adicionales que añada.
8. (Opcional) para incluir recursos de ámbito de clúster además de los que Astra Control incluye

automáticamente, marque **incluir recursos adicionales de ámbito de clúster** y complete lo siguiente:

a. Seleccione **Agregar regla de inclusión**.

b. **Grupo**: En la lista desplegable, seleccione el grupo API de recursos.

c. **Kind**: En la lista desplegable, seleccione el nombre del esquema de objetos.

d. **Versión**: Introduzca la versión API.

e. **Selector de etiquetas**: Opcionalmente, incluya una etiqueta que se agregará a la regla. Esta etiqueta se utiliza para recuperar solo los recursos que coincidan con esta etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster.

f. Revise la regla que se crea en función de las entradas.

g. Seleccione **Agregar**.

> Puede crear tantas reglas de recursos con ámbito de clúster como desee. Las reglas aparecen en definir resumen de la aplicación.

9. Seleccione **definir**.
10. Después de seleccionar **definir**, repita el proceso para otras aplicaciones, según sea necesario.

Cuando termine de definir una aplicación, la aplicación aparecerá en `Healthy` estado en la lista de aplicaciones de la página aplicaciones. Ahora puede clonarla y crear backups y copias Snapshot.

> Es posible que la aplicación que acaba de agregar tenga un icono de advertencia en la columna protegido, lo que indica que no se ha realizado una copia de seguridad y que aún no está programada para las copias de seguridad.

> Para ver los detalles de una aplicación en particular, seleccione el nombre de la aplicación.

Para ver los recursos agregados a esta aplicación, seleccione la ficha **Recursos**. Seleccione el número después del nombre del recurso en la columna Resource o introduzca el nombre del recurso en la búsqueda para ver los recursos adicionales con ámbito del clúster incluidos.

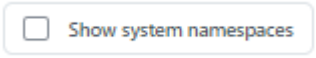
Defina un espacio de nombres para administrar como una aplicación

Puede añadir todos los recursos de Kubernetes en un espacio de nombres a la gestión de Astra Control al definir los recursos de ese espacio de nombres como una aplicación. Este método es preferible a definir las aplicaciones individualmente si piensa administrar y proteger todos los recursos de un espacio de nombres determinado de una manera similar y en intervalos comunes.

Pasos

1. En la página Clusters, seleccione un clúster.
2. Seleccione la ficha **Namespaces**.
3. Seleccione el menú acciones del espacio de nombres que contiene los recursos de aplicación que desea administrar y seleccione **definir como aplicación**.

> Si desea definir varias aplicaciones, seleccione en la lista de espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **definir como aplicación**. Esto definirá varias aplicaciones individuales en sus espacios de nombres individuales. Para aplicaciones con varios espacios de nombres, consulte Defina los recursos que se van a administrar como una aplicación.

Active la casilla de verificación **Mostrar espacios de nombres del sistema** para mostrar los espacios de nombres del sistema que normalmente no se usan en la administración de aplicaciones de forma predeterminada. 

"Leer más".

Una vez completado el proceso, las aplicaciones asociadas al espacio de nombres aparecen en la `Associated applications` columna.

[Vista PREVIA TÉCNICA] Defina una aplicación utilizando un recurso personalizado de Kubernetes

Puede especificar los recursos de Kubernetes que desee gestionar con Astra Control definiéndolos como aplicación mediante un recurso personalizado (CR). Puede añadir recursos de ámbito en clúster si desea gestionar esos recursos individualmente o todos los recursos de Kubernetes en un espacio de nombres si, por ejemplo, tiene la intención de gestionar y proteger todos los recursos de un espacio de nombres particular de una forma similar y con intervalos comunes.

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `astra_mysql_app.yaml`).
2. Asigne un nombre a la aplicación en `metadata.name`.
3. Defina los recursos de aplicación que se van a gestionar:

spec.includedClusterScopedResources

Incluye los tipos de recursos de ámbito del clúster además de los que Astra Control incluye automáticamente:

- **spec.includedClusterScopedResources**: *(Opcional)* Una lista de tipos de recursos de ámbito de cluster que se incluirán.
  - **GroupVersionKind**: *(Opcional)* identifica inequívocamente un tipo.
    - **GROUP**: *(requerido si se usa groupVersionKind)* Grupo API del recurso a incluir.
    - **VERSIÓN**: *(requerido si se usa groupVersionKind)* Versión API del recurso a incluir.
    - **Kind**: *(requerido si se usa groupVersionKind)* tipo de recurso a incluir.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. Los requisitos son ANDed.
      - **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
      - **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
      - **VALORES**: *(requerido si se utiliza matchExpressions)_Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe _not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

spec.includedNamespaces

Incluya espacios de nombres y recursos dentro de esos recursos en la aplicación:

- **spec.includedNamespaces**: _(required)_Define el espacio de nombres y los filtros opcionales para la selección de recursos.
  - **Namespace**: *(required)* El espacio de nombres que contiene los recursos de la aplicación que desea administrar con Astra Control.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. `key` y.. `operator` son obligatorios. Los requisitos son ANDed.

- **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
- **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
- **Valores**: *(requerido si se usa matchExpressions)* Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe *not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

Ejemplo YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

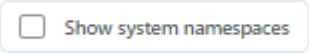
4. Después de rellenar el `astra_mysql_app.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

¿Qué ocurre con los espacios de nombres del sistema?

Astra Control también detecta espacios de nombres de sistemas en un clúster de Kubernetes. No le mostramos estos espacios de nombres del sistema de forma predeterminada porque es raro que necesite realizar backups de los recursos de la aplicación del sistema.

Puede visualizar los espacios de nombres del sistema desde la ficha espacios de nombres de un clúster seleccionado activando la casilla de verificación **Mostrar espacios de nombres del sistema** .



Astra Control Center no se muestra de forma predeterminada como una aplicación que puedes gestionar, pero puedes crear backups y restaurar una instancia de Astra Control Center mediante otra instancia de Astra Control Center.

Ejemplo: Separar la normativa de protección para diferentes versiones

En este ejemplo, el equipo de devops gestiona una puesta en marcha de versiones «canaria». El grupo del equipo tiene tres pods que se ejecutan nginx. Dos de los pods están dedicados a la versión estable. El tercer pod es para el lanzamiento canario.

El administrador de Kubernetes del equipo de devops añade la etiqueta `deployment=stable` a los pods de liberación estables. El equipo agrega la etiqueta `deployment=canary` a la cápsula de liberación canaria.

La versión estable del equipo incluye los requisitos de snapshots cada hora y backups diarios. la liberación canaria es más efímera, por lo que quieren crear una Política de Protección a corto plazo menos agresiva para cualquier cosa etiquetada `deployment=canary`.

Para evitar posibles conflictos de datos, el administrador creará dos aplicaciones: Una para el lanzamiento "canario" y otra para el lanzamiento "estable". De este modo, los backups, las snapshots y las operaciones de clonado se mantienen independientes para los dos grupos de objetos de Kubernetes.

Obtenga más información

- "Utilice la API Astra Control"
- "Desgestionar una aplicación"

Proteja sus aplicaciones

Información general sobre la protección

Puede crear backups, clones, snapshots y políticas de protección para sus aplicaciones con Astra Control Center. El backup de sus aplicaciones ayuda a que los servicios y los datos asociados estén disponibles lo más posible; durante un desastre, la restauración a partir de una copia de seguridad puede garantizar la recuperación completa de una aplicación y sus datos asociados con una interrupción mínima. Los backups, clones y copias Snapshot pueden ayudar a protegerse frente a amenazas comunes como el ransomware, la pérdida accidental de datos y los desastres medioambientales. "Conozca los tipos disponibles de protección de datos en Astra Control Center y cuándo utilizarlas".

Además, puede replicar aplicaciones en un clúster remoto como preparación para la recuperación ante desastres.

Flujo de trabajo de protección de aplicaciones

Puede utilizar el siguiente ejemplo de flujo de trabajo para empezar a proteger las aplicaciones.

[Uno] Proteja todas las aplicaciones

Para asegurarse de que sus aplicaciones están protegidas inmediatamente, "cree una copia de seguridad manual de todas las aplicaciones".

[Dos] Configure una política de protección para cada aplicación

Para automatizar futuros backups y copias Snapshot, "configure una política de protección para cada aplicación". A modo de ejemplo, puede comenzar con backups semanales y snapshots diarias, con una retención de un mes para ambos. La automatización de backups y snapshots con una política de protección es muy recomendada con respecto a copias de Snapshot y backups manuales.

[Tres] Ajuste las políticas de protección

A medida que cambian las aplicaciones y sus patrones de uso, ajuste las políticas de protección según sea necesario para proporcionar la mejor protección.

[Cuatro] Replicar aplicaciones en un clúster remoto

"Replicar aplicaciones" A un clúster remoto mediante la tecnología NetApp SnapMirror. Astra Control replica las instantáneas en un clúster remoto, lo que proporciona una función asíncrona y de recuperación ante desastres.

[Cinco] En caso de desastre, restaure sus aplicaciones con la última copia de seguridad o replicación en el sistema remoto

Si se produce la pérdida de datos, puede recuperarlo "restaurar la copia de seguridad más reciente" la primera para cada aplicación. Luego puede restaurar la snapshot más reciente (si está disponible). O bien, puede utilizar la replicación en un sistema remoto.

Proteja las aplicaciones con snapshots y backups

Proteger todas las aplicaciones mediante la toma de snapshots y backups a través de una política de protección automatizada o de manera ad hoc. Puede utilizar la interfaz de usuario de Astra Control Center o "La API de control Astra" para proteger aplicaciones.

Acerca de esta tarea

- **Helm implementó aplicaciones**: Si utiliza Helm para implementar aplicaciones, Astra Control Center requiere Helm versión 3. Se admite por completo la gestión y clonación de las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Las aplicaciones implementadas con Helm 2 no son compatibles.
- **(Solo clústeres de OpenShift) Agregar políticas**: Cuando crea un proyecto para alojar una aplicación en un clúster de OpenShift, al proyecto (o espacio de nombres de Kubernetes) se le asigna un UID de SecurityContext. Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

  ```
  oc new-project wordpress
  oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
  oc adm policy add-scc-to-user privileged -z default -n wordpress
  ```

Puede realizar las siguientes tareas relacionadas con la protección de los datos de la aplicación:

- Configure una política de protección
- Crear una copia de Snapshot
- Cree un backup

- Habilite el backup y la restauración para las operaciones económicas de ontap-nas
- Cree un backup inmutable
- Ver Snapshot y backups
- Eliminar snapshots
- Cancelar backups
- Eliminar backups

Configure una política de protección

La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener. Puede definir una política de protección con la interfaz de usuario web de Astra Control o un archivo de recursos personalizados (CR).

Si necesita que backups o snapshots se ejecuten con más frecuencia de una vez por hora, puede hacerlo "Utilice la API REST de Astra Control para crear copias Snapshot y copias de seguridad".

Si va a definir una política de protección que crea backups inmutables para escribir bloques WORM (escritura única y lectura múltiple), asegúrese de que el tiempo de retención de los backups no sea más corto que el período de retención configurado para el bloque.

Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

Configure una política de protección con la interfaz de usuario web

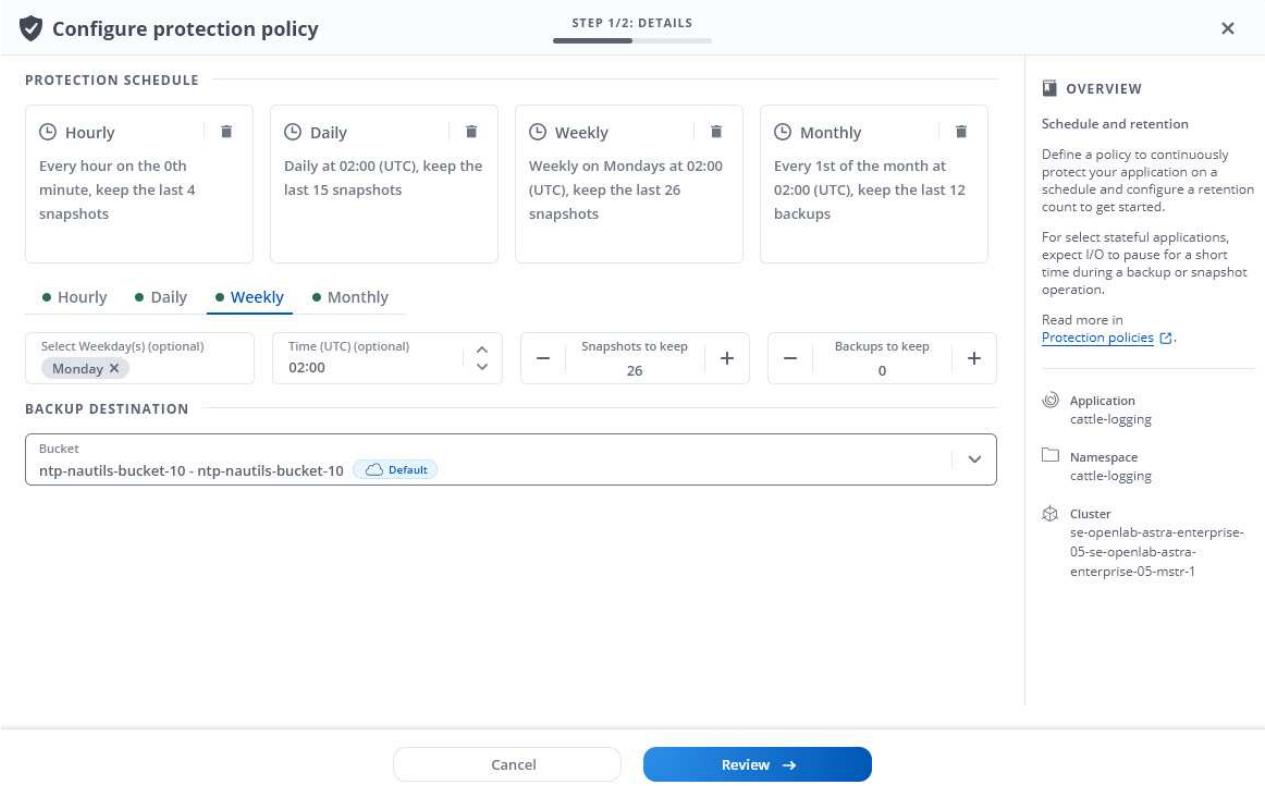
Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **Configurar política de protección**.
4. Defina una programación de protección eligiendo la cantidad de snapshots y backups que se mantendrán por hora, día, semana y mes.

   Puede definir las programaciones por hora, por día, por semana y por mes de forma simultánea. Una programación no se activa hasta que se establece un nivel de retención.

   Al establecer un nivel de retención para backups, puede elegir el bloque en el que desea almacenar los backups.

   En el siguiente ejemplo, se establecen cuatro programaciones de protección: Por hora, día, semana y mes para las copias Snapshot y los backups.



5. [**Vista previa tecnológica**] Elija un depósito de destino para las copias de seguridad o instantáneas de la lista de depósitos de almacenamiento.
6. Seleccione **Revisión**.
7. Seleccione **Configurar política de protección.**

[Tech preview] Configurar una política de protección con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-schedule-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tus

necesidades de entorno de Astra Control, configuración del clúster y protección de datos:

- <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
- <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
- <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.
- <BACKUPS_RETAINED>: La cantidad de backups que se retendrán. Cero indica que no se debe crear ningún backup.
- <SNAPSHOTS_RETAINED>: La cantidad de snapshots que se retendrán. Cero indica que no se debe crear ninguna instantánea.
- <GRANULARITY>: La frecuencia con la que debe ejecutarse la programación. Los posibles valores, junto con los campos asociados necesarios:
  - `hourly` (requiere que especifique `spec.minute`)
  - `daily` (requiere que especifique `spec.minute` y.. `spec.hour`)
  - `weekly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfWeek`)
  - `monthly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfMonth`)
- <DAY_OF_MONTH>: *(Opcional)* el día del mes (1 - 31) en el que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `monthly`.
- <DAY_OF_WEEK>: *(Opcional)* El día de la semana (0 - 7) en el que se debe ejecutar la programación. Los valores de 0 o 7 indican el domingo. Este campo es necesario si la granularidad se establece en `weekly`.
- <HOUR_OF_DAY>: *(Opcional)* La hora del día (0 - 23) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `daily`, `weekly`, o. `monthly`.
- <MINUTE_OF_HOUR>: *(Opcional)* El minuto de la hora (0 - 59) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `hourly`, `daily`, `weekly`, o. `monthly`.

```yaml
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Después de rellenar el `astra-control-schedule-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Resultado

Astra Control implementa la política de protección de datos mediante la creación y retención de copias Snapshot y copias de seguridad con la política de programación y retención que haya definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

Acerca de esta tarea

Astra Control permite la creación de copias Snapshot con clases de almacenamiento respaldadas por los siguientes controladores:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, no se pueden crear instantáneas. Utilice una clase de almacenamiento alternativa para las instantáneas.

Cree una copia Snapshot de con la interfaz de usuario web de

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **Snapshot**.
3. Personalice el nombre de la instantánea y, a continuación, seleccione **Siguiente**.
4. [**Vista previa tecnológica**] Elija un cubo de destino para la instantánea de la lista de cubos de almacenamiento.
5. Revise el resumen de la instantánea y seleccione **Snapshot**.

[Vista previa técnica] Crear una instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación que se va a realizar la instantánea.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la instantánea.
   - <RECLAIM_POLICY>: *(Opcional)* define lo que ocurre con una instantánea cuando se elimina la CR de instantánea. Opciones válidas:
     - `Retain`
     - `Delete` (predeterminado)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Después de rellenar el `astra-control-snapshot-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

Resultado

Se inicia el proceso Snapshot. Una instantánea se realiza correctamente cuando el estado es **saludable** en la columna **Estado** de la página **Protección de datos** > **instantáneas**.

Cree un backup

Puede realizar una copia de seguridad de una aplicación en cualquier momento.

Acerca de esta tarea

Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` conductor, usted necesita habilite el backup y la restauración funcionalidad. Asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

> Astra Control permite la creación de backups mediante clases de almacenamiento respaldadas por los siguientes controladores:
>
> - `ontap-nas`
> - `ontap-nas-economy`
> - `ontap-san`
> - `ontap-san-economy`

Cree un backup con la interfaz de usuario web de

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. [**Tech preview**] Elija un depósito de destino para la copia de seguridad de la lista de depósitos de almacenamiento.
6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

[Vista previa técnica] Cree un backup con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Después de rellenar el `astra-control-backup-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Resultado

Astra Control crea una copia de seguridad de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice las instrucciones de Eliminar backups.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Habilite el backup y la restauración para las operaciones económicas de ontap-nas

Astra Control Provisioning ofrece funcionalidad de backup y restauración que puede habilitarse para los back-ends de almacenamiento que utilicen el `ontap-nas-economy` clase de almacenamiento.

Antes de empezar

- Ya tienes "Habilitado Astra Control Provisioning".
- Has definido una aplicación en Astra Control. Esta aplicación tendrá funcionalidad de protección limitada hasta que complete este procedimiento.
- Ya tienes `ontap-nas-economy` se ha seleccionado como la clase de almacenamiento predeterminada para el back-end del almacenamiento.

Pasos

1. Realice lo siguiente en el back-end de almacenamiento de ONTAP:

   a. Busque la SVM donde aloja el `ontap-nas-economy`-basado en volúmenes de la aplicación.

   b. Inicie sesión en un terminal conectado a ONTAP donde se crean los volúmenes.

   c. Oculte el directorio de snapshots para la SVM:

   Este cambio afecta a toda la SVM. El directorio oculto seguirá siendo accesible.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+

   Compruebe que el directorio de snapshots del back-end de almacenamiento de ONTAP esté oculto. Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.

2. Haga lo siguiente en Astra Control Provisioner:

   a. Active el directorio de instantáneas para cada VP que sea `ontap-nas-economy` basado y asociado con la aplicación:

```
tridentctl update volume <pv name> --snapshot-dir=true --pool-level
=true -n trident
```

b. Confirme que el directorio de snapshots se haya habilitado para cada VP asociado:

```
tridentctl get volume <pv name> -n trident -o yaml | grep snapshotDir
```

Respuesta:

```
snapshotDirectory: "true"
```

3. En Astra Control, actualiza la aplicación después de habilitar todos los directorios Snapshot asociados para que Astra Control reconozca el valor modificado.

Resultado

La aplicación está lista para realizar backups y restauraciones con Astra Control. Otras aplicaciones también pueden utilizar cada RVP para realizar backups y restauraciones de datos.

Cree un backup inmutable

No se puede modificar, eliminar ni sobrescribir una copia de seguridad inmutable siempre que la política de retención del depósito que almacena la copia de seguridad la prohíba. Puede crear backups inmutables mediante el backup de aplicaciones en bloques que tengan configurada una política de retención. Consulte "Protección de datos" para obtener información importante sobre cómo trabajar con backups inmutables.

Antes de empezar

Debe configurar el bucket de destino con una política de retención. La forma de hacerlo variará en función del proveedor de almacenamiento que utilice. Consulte la documentación del proveedor de almacenamiento para obtener más información:

- **Amazon Web Services**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «gobierno» con un período de retención predeterminado".
- **NetApp StorageGRID**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «cumplimiento» con un período de retención predeterminado".

> Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

Pasos

1. Seleccione **aplicaciones**.

2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. Seleccione un bucket de destino para el backup en la lista de bloques de almacenamiento. Se indica un depósito de escritura única y lectura múltiple (WORM) con el estado «bloqueado» junto al nombre del depósito.

   Si el depósito es de tipo no admitido, se indica cuando pasa el ratón por encima o selecciona el depósito.

6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control crea un backup inmutable de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si intentas crear dos backups inmutables de la misma aplicación en el mismo bloque a la vez, Astra Control impide que se inicie el segundo backup. Espere hasta que se complete la primera copia de seguridad antes de iniciar otra.
- No es posible cancelar una copia de seguridad inmutable en ejecución.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Ver Snapshot y backups

Puede ver las instantáneas y las copias de seguridad de una aplicación desde la pestaña Data Protection.

Se indica una copia de seguridad inmutable con el estado «Locked» junto al bloque que está utilizando.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.

   Las instantáneas se muestran de forma predeterminada.

3. Seleccione **copias de seguridad** para ver la lista de copias de seguridad.

Eliminar snapshots

Elimine las snapshots programadas o bajo demanda que ya no necesite.

No es posible eliminar una copia de Snapshot que se está replicando actualmente.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione **Protección de datos**.
3. En el menú Opciones de la columna **acciones** de la instantánea deseada, seleccione **Eliminar instantánea**.
4. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete snapshot**.

Resultado

Astra Control elimina la instantánea.

Cancelar backups

Es posible cancelar una copia de seguridad que esté en curso.

Para cancelar una copia de seguridad, la copia de seguridad debe estar en `Running` estado. No puede cancelar una copia de seguridad que esté en `Pending` estado.

No es posible cancelar una copia de seguridad inmutable en ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** para la copia de seguridad deseada, seleccione **Cancelar**.
5. Escriba la palabra "cancelar" para confirmar la operación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

Eliminar backups

Elimine los backups programados o bajo demanda que ya no necesita. No puede eliminar un backup realizado en un bloque inmutable hasta que la política de retención del bloque lo permita.

No se puede eliminar un backup inmutable antes de que caduque el período de retención.

Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice estas instrucciones.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** de la copia de seguridad deseada, seleccione **Eliminar**

copia de seguridad.

5. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete backup**.

Resultado

Astra Control elimina la copia de seguridad.

[Tech preview] Proteger todo un clúster

Es posible crear un backup automático programado de cualquiera de los espacios de nombres no gestionados de un clúster o de todos ellos. Estos flujos de trabajo los proporciona NetApp como una cuenta de servicio de Kubernetes, enlaces de roles y un trabajo cron orquestado con un script de Python.

Cómo funciona

Cuando configura e instala el flujo de trabajo de backup de clúster completo, un trabajo con cron se ejecuta periódicamente y protege cualquier espacio de nombres que aún no esté gestionado, lo que crea automáticamente políticas de protección basadas en los programas que elija durante la instalación.

Si no desea proteger todos los espacios de nombres no administrados en el clúster con el flujo de trabajo de backup de clúster completo, en su lugar, puede utilizar el flujo de trabajo de backup basado en etiquetas. El flujo de trabajo de backup basado en etiquetas también usa una tarea CRON, pero, en lugar de proteger todos los espacios de nombres no gestionados, identifica los espacios de nombres por etiquetas que se proporcionan para proteger, opcionalmente, los espacios de nombres según políticas de backup bronce, plata o oro.

Cuando se crea un nuevo espacio de nombres que se ajusta al alcance del flujo de trabajo elegido, se protege automáticamente, sin necesidad de que el administrador realice ninguna acción. Estos flujos de trabajo se implementan por clúster, de modo que diferentes clústeres pueden utilizar cualquier flujo de trabajo con niveles de protección únicos, según la importancia del clúster.

Ejemplo: Protección de clúster completa

Como ejemplo, cuando configura e instala el flujo de trabajo de backup completo del clúster, las aplicaciones en cualquier espacio de nombres se gestionan periódicamente y se protegen sin que el administrador intervenga. El espacio de nombres no tiene que existir en el momento de instalar el flujo de trabajo; si se agrega un espacio de nombres en el futuro, se protegerá.

Ejemplo: Protección basada en etiquetas

Para obtener más granularidad, puede utilizar el flujo de trabajo basado en etiquetas. Por ejemplo, puede instalar este flujo de trabajo y decirle a los usuarios que apliquen una de varias etiquetas a cualquier espacio de nombres que quieran proteger, según el nivel de protección que necesiten. Esto permite a los usuarios crear el espacio de nombres con una de estas etiquetas, y no tienen que notificar a un administrador. Su nuevo espacio de nombres y todas las aplicaciones que contiene quedan protegidas de forma automática.

Cree una copia de seguridad programada de todos los espacios de nombres

Es posible crear un backup programado de todos los espacios de nombres en un clúster mediante el flujo de trabajo de backup de clúster completo.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:

- "Archivo CRD Components.yaml"
- "protectCluster.py Script Python"

2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Crear una copia de seguridad programada de espacios de nombres específicos

Puede crear un backup programado de espacios de nombres específicos mediante sus etiquetas mediante el flujo de trabajo de backup basado en etiquetas.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:
   - "Archivo CRD Components.yaml"
   - "protectCluster.py Script Python"
2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Restaurar aplicaciones

Astra Control puede restaurar su aplicación a partir de una instantánea o una copia de seguridad. La restauración a partir de una snapshot existente será más rápida cuando se restaure la aplicación en el mismo clúster. Puede utilizar la interfaz de usuario de Astra Control o. "API de control Astra" para restaurar aplicaciones.

Antes de empezar

- **Proteja sus aplicaciones primero**: Se recomienda encarecidamente que tome una instantánea o una copia de seguridad de su aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup si la restauración no se realiza correctamente.
- **Comprobar volúmenes de destino**: Si restaura a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de restauración si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que falle la operación de restauración. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- **Planificar necesidades de espacio**: Cuando se realiza una restauración in situ de una aplicación que utiliza almacenamiento ONTAP de NetApp, el espacio utilizado por la aplicación restaurada puede duplicarse. Después de realizar una restauración sin movimiento, elimine las instantáneas no deseadas de la aplicación restaurada para liberar espacio de almacenamiento.
- **(Solo clústeres de Red Hat OpenShift) Agregar políticas**: Cuando crea un proyecto para alojar una aplicación en un clúster de OpenShift, al proyecto (o espacio de nombres de Kubernetes) se le asigna un UID de SecurityContext. Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- **Controladores de clase de almacenamiento compatibles**: Astra Control admite la restauración de copias de seguridad mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(Solo controlador económico de ontap-nas) Copias de seguridad y restauraciones**: Antes de realizar copias de seguridad o restaurar una aplicación que utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, compruebe que el "El directorio Snapshot del sistema de administración de almacenamiento de ONTAP está oculto". Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.
- * Aplicaciones implementadas de Helm*: Las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. Las aplicaciones implementadas con Helm 2 no son compatibles.

> La ejecución de una operación de restauración sin movimiento en una aplicación que comparte recursos con otra aplicación puede tener resultados no intencionados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones. Para obtener más información, consulte este ejemplo.

Realice los siguientes pasos, según el tipo de archivo que desee restaurar:

Restaure los datos de un backup o una copia Snapshot mediante la interfaz de usuario web

Puede restaurar datos con la interfaz de usuario web de Astra Control.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.
3. Elija el tipo de restauración:
   - **Restaurar en espacios de nombres originales**: Utilice este procedimiento para restaurar la aplicación en su sitio al cluster original.

     > Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` driver, debe restaurar la aplicación utilizando las clases de almacenamiento originales. No puede especificar una clase de almacenamiento diferente si va a restaurar la aplicación en el mismo espacio de nombres.

     i. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación en el lugar, lo que revierte la aplicación a una versión anterior de sí misma.

     ii. Seleccione **Siguiente**.

     > Si se restaura en un espacio de nombres que se eliminó previamente, se crea un espacio de nombres nuevo con el mismo nombre como parte del proceso de restauración. Cualquier usuario que tenga derechos para administrar aplicaciones en el espacio de nombres previamente eliminado debe restaurar manualmente los derechos en el espacio de nombres recién creado.

- **Restaurar en nuevos espacios de nombres**: Utilice este procedimiento para restaurar la aplicación en otro clúster o con diferentes espacios de nombres desde el origen.
  i. Especifique el nombre de la aplicación restaurada.
  ii. Elija el clúster de destino de la aplicación que desea restaurar.
  iii. Introduzca un espacio de nombres de destino para cada espacio de nombres de origen asociado a la aplicación.

  > Astra Control crea nuevos espacios de nombres de destino como parte de esta opción de restauración. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

  iv. Seleccione **Siguiente**.
  v. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación.
  vi. Seleccione **Siguiente**.
  vii. Elija una de las siguientes opciones:
    - **Restaurar usando clases de almacenamiento originales**: La aplicación utiliza la clase de almacenamiento asociada originalmente a menos que no exista en el clúster de destino. En este caso, se utilizará la clase de almacenamiento predeterminada para el clúster.
    - **Restaurar usando una clase de almacenamiento diferente**: Seleccione una clase de almacenamiento que exista en el clúster de destino. Todos los volúmenes de aplicaciones, independientemente de sus tipos de almacenamiento asociados originalmente, se migrarán a esta clase de almacenamiento diferente como parte de la restauración.
  viii. Seleccione **Siguiente**.

4. Elija cualquier recurso para filtrar:
   - **Restaurar todos los recursos**: Restaurar todos los recursos asociados con la aplicación original.
   - **Filtrar recursos**: Especificar reglas para restaurar un subconjunto de los recursos originales de la aplicación:
     i. Seleccione incluir o excluir recursos de la aplicación restaurada.
     ii. Seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión** y configure la regla para filtrar los recursos correctos durante la restauración de la aplicación. Puede editar una regla o eliminarla y volver a crear una regla hasta que la configuración sea correcta.

     > Para obtener más información sobre la configuración de reglas de inclusión y exclusión, consulte Filtre recursos durante una restauración de aplicación.

5. Seleccione **Siguiente**.
6. Revise los detalles sobre la acción de restauración cuidadosamente, escriba “restaurar” (si se le solicita) y seleccione **Restaurar**.

[Vista previa técnica] Restaurar a partir del backup mediante un recurso personalizado (CR)

Es posible restaurar datos desde un backup con un archivo de recurso personalizado (CR) en otro espacio de nombres o en el espacio de nombres de origen original.

Restaurar desde una copia de seguridad con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Opcional) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas concretas:
   - "<INCLUDE-EXCLUDE>": *(requerido para filtrar)* use `include` o. `exclude` Para incluir o excluir un recurso definido en resourceMatchers. Agregue los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
     - <GROUP>: *(Opcional)* Grupo del recurso que se va a filtrar.
     - <KIND>: *(Opcional)* Tipo de recurso que se va a filtrar.
     - <VERSION>: *(Opcional)* Versión del recurso que se va a filtrar.
     - <NAMES>: *(Opcional)* Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <NAMESPACES>: *(Opcional)* Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <SELECTORS>: *(Optional)* Cadena de selector de etiquetas en el campo Kubernetes

metadata.name del recurso, tal como se define en "Documentación de Kubernetes". Ejemplo: `"trident.netapp.io/os=linux"`.

Ejemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Después de rellenar el `astra-control-backup-restore-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

Restaure desde un backup al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

```
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

2. (Opcional) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas concretas:

   - "<INCLUDE-EXCLUDE>": *(requerido para filtrar)* use `include` o. `exclude` Para incluir o excluir un recurso definido en resourceMatchers. Agregue los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
     - <GROUP>: *(Opcional)* Grupo del recurso que se va a filtrar.
     - <KIND>: *(Opcional)* Tipo de recurso que se va a filtrar.
     - <VERSION>: *(Opcional)* Versión del recurso que se va a filtrar.
     - <NAMES>: *(Opcional)* Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <NAMESPACES>: *(Opcional)* Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <SELECTORS>: *(Optional)* Cadena de selector de etiquetas en el campo Kubernetes metadata.name del recurso, tal como se define en "Documentación de Kubernetes". Ejemplo: `"trident.netapp.io/os=linux"`.

       Ejemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Después de rellenar el `astra-control-backup-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Vista PREVIA TÉCNICA] Restauración a partir de una instantánea con un recurso personalizado (CR)

Puede restaurar datos desde una copia Snapshot con un archivo de recurso personalizado (CR) en un espacio de nombres diferente o en el espacio de nombres de origen original.

Restaurar desde instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Opcional) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas concretas:
   - "<INCLUDE-EXCLUDE>": *(requerido para filtrar)* use `include` o. `exclude` Para incluir o excluir un recurso definido en resourceMatchers. Agregue los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
     - <GROUP>: *(Opcional)* Grupo del recurso que se va a filtrar.
     - <KIND>: *(Opcional)* Tipo de recurso que se va a filtrar.
     - <VERSION>: *(Opcional)* Versión del recurso que se va a filtrar.
     - <NAMES>: *(Opcional)* Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <NAMESPACES>: *(Opcional)* Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <SELECTORS>: *(Optional)* Cadena de selector de etiquetas en el campo Kubernetes

metadata.name del recurso, tal como se define en "Documentación de Kubernetes". Ejemplo: `"trident.netapp.io/os=linux"`.

Ejemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Después de rellenar el `astra-control-snapshot-restore-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

Restauración de una snapshot al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

2. (Opcional) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas concretas:

   - "<INCLUDE-EXCLUDE>": *(requerido para filtrar)* use `include` o. `exclude` Para incluir o excluir un recurso definido en resourceMatchers. Agregue los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
     - <GROUP>: *(Opcional)* Grupo del recurso que se va a filtrar.
     - <KIND>: *(Opcional)* Tipo de recurso que se va a filtrar.
     - <VERSION>: *(Opcional)* Versión del recurso que se va a filtrar.
     - <NAMES>: *(Opcional)* Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <NAMESPACES>: *(Opcional)* Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
     - <SELECTORS>: *(Optional)* Cadena de selector de etiquetas en el campo Kubernetes metadata.name del recurso, tal como se define en "Documentación de Kubernetes". Ejemplo: `"trident.netapp.io/os=linux"`.

       Ejemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Después de rellenar el `astra-control-snapshot-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Resultado

Astra Control restaura la aplicación en función de la información proporcionada. Si restauró la aplicación en un lugar, el contenido de los volúmenes persistentes existentes se reemplaza por el contenido de los volúmenes persistentes de la aplicación restaurada.

> Después de una operación de protección de datos (clonado, backup o restauración) y un posterior tamaño de volumen persistente, se produce un retraso de hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario web. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

> Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Filtre recursos durante una restauración de aplicación

Puede agregar una regla de filtro a un "restaurar" operación que especificará los recursos de aplicación existentes que se incluirán o excluirán de la aplicación restaurada. Puede incluir o excluir recursos basados en un espacio de nombres, etiqueta o GVK (GroupVersionKind) especificado.

Amplíe para obtener más información sobre Incluir y excluir escenarios

- **Selecciona una regla de inclusión con espacios de nombres originales (restauración in situ)**: Los recursos de aplicación existentes que definas en la regla se eliminarán y reemplazarán por aquellos de la instantánea o copia de seguridad seleccionada que estés utilizando para la restauración. Cualquier recurso que no especifique en la regla Incluir permanecerá sin cambios.
- **Selecciona una regla de inclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas en la aplicación restaurada. Los recursos que no especifique en la regla Incluir no se incluirán en la aplicación restaurada.
- **Selecciona una regla de exclusión con espacios de nombres originales (restauración in situ)**: Los recursos que especifiques para ser excluidos no se restaurarán y permanecerán sin cambios. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup. Todos los datos de los volúmenes persistentes se eliminarán y volverán a crear si el StatefulSet correspondiente forma parte de los recursos filtrados.
- **Selecciona una regla de exclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas eliminar de la aplicación restaurada. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup.

Las reglas son tipos de inclusión o exclusión. Las reglas que combinan la inclusión y exclusión de recursos no están disponibles.

Pasos

1. Una vez que haya elegido filtrar recursos y seleccionado una opción Incluir o Excluir en el asistente

Restaurar aplicación, seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión**.

> No puede excluir ningún recurso en el ámbito del clúster que Astra Control incluya automáticamente.

2. Configure la regla de filtro:

> Debe especificar al menos un espacio de nombres, una etiqueta o un GVK. Asegúrese de que los recursos que retenga después de aplicar las reglas de filtro sean suficientes para mantener la aplicación restaurada en buen estado.

   a. Seleccione un espacio de nombres específico para la regla. Si no hace una selección, se usarán todos los espacios de nombres en el filtro.

   > Si la aplicación contenía originalmente varios espacios de nombres y la restauraba en nuevos espacios de nombres, todos los espacios de nombres se crearán incluso si no contienen recursos.

   b. (Opcional) Introduzca un nombre de recurso.
   c. (Opcional) **Selector de etiquetas**: Incluye a. "selector de etiquetas" para agregar a la regla. El selector de etiquetas se utiliza para filtrar sólo los recursos que coincidan con la etiqueta seleccionada.
   d. (Opcional) Seleccione **Usar GVK (GroupVersionKind) configurado para filtrar recursos** para opciones de filtrado adicionales.

   > Si utiliza un filtro GVK, debe especificar Versión y Tipo.

      i. (Opcional) **Grupo**: En la lista desplegable, seleccione el grupo API de Kubernetes.
      ii. **Kind**: En la lista desplegable, seleccione el esquema de objeto para el tipo de recurso de Kubernetes a utilizar en el filtro.
      iii. **Versión**: Seleccione la versión de la API de Kubernetes.
3. Revise la regla que se crea en función de las entradas.
4. Seleccione **Agregar**.

> Puede crear tantas reglas de inclusión y exclusión de recursos como desee. Las reglas aparecen en el resumen de la aplicación de restauración antes de iniciar la operación.

Complicaciones de restauración in situ para una aplicación que comparte recursos con otra aplicación

Puede realizar una operación de restauración in situ en una aplicación que comparta recursos con otra aplicación y produzca resultados no deseados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones.

A continuación se muestra un ejemplo que crea una situación no deseable cuando se usa la replicación SnapMirror de NetApp para una restauración:

1. Defina la aplicación `app1` uso del espacio de nombres `ns1`.
2. Puede configurar una relación de replicación para `app1`.

3. Defina la aplicación `app2` (en el mismo clúster) mediante los espacios de nombres `ns1` y.. `ns2`.
4. Puede configurar una relación de replicación para `app2`.
5. La replicación se invierte para `app2`. Esto provoca la `app1` en el clúster de origen que se va a desactivar.

Replicar aplicaciones entre back-ends de almacenamiento mediante la tecnología SnapMirror

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.

Si quiere ver una comparación entre backups/restauraciones y replicación, consulte "Conceptos de protección de datos".

Puede replicar aplicaciones en diferentes situaciones, como las siguientes situaciones de solo en las instalaciones, de cloud híbrido y multicloud:

- Del sitio local A al sitio local A
- De sitio en las instalaciones A al sitio en las instalaciones B
- De las instalaciones al cloud con Cloud Volumes ONTAP
- Cloud con Cloud Volumes ONTAP a las instalaciones
- Cloud con Cloud Volumes ONTAP al cloud (entre distintas regiones del mismo proveedor de cloud o a distintos proveedores de cloud)

Astra Control puede replicar aplicaciones en clústeres locales, de las instalaciones al cloud (mediante Cloud Volumes ONTAP) o entre clouds (Cloud Volumes ONTAP a Cloud Volumes ONTAP).

> Puede replicar simultáneamente una aplicación diferente en la dirección opuesta. Por ejemplo, las aplicaciones A, B, C se pueden replicar del centro de datos 1 al centro de datos 2 y las aplicaciones X, y y, Z se pueden replicar del centro de datos 2 al centro de datos 1.

Con Astra Control, puede realizar las siguientes tareas relacionadas con la replicación de aplicaciones:

- Configurar una relación de replicación
- Ponga una aplicación replicada en línea en el clúster de destino (conmutación por error)
- Se ha producido un error al sincronizar una replicación
- Replicación de aplicaciones inversa
- Conmutación tras error de las aplicaciones al clúster de origen original
- Eliminar una relación de replicación de aplicaciones

Requisitos previos de replicación

La replicación de aplicaciones de Astra Control requiere que se cumplan los siguientes requisitos previos antes de empezar:

Clústeres ONTAP

- **El aprovisionador de control de Astra o Astra Trident**: El aprovisionador de control de Astra o Astra Trident deben existir en los clústeres de Kubernetes de origen y destino que utilicen ONTAP como back-end. Astra Control admite la replicación con la tecnología SnapMirror de NetApp mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-san`
- **Licencias**: Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP" si quiere más información.

Interconexión

- **Cluster y SVM**: Los back-ends de almacenamiento ONTAP deben ser peered. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM" si quiere más información.

  Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **El aprovisionador de Astra Control o Astra Trident y SVM**: Las SVM remotas entre iguales deben estar disponibles para el aprovisionador de Astra Control o Astra Trident en el clúster de destino.

  Astra Control Center

  "Pon en marcha Astra Control Center" en un tercer dominio de fallo o centro secundario para proporcionar una recuperación ante desastres sin problemas.

- **Backends administrados**: Necesitas agregar y administrar backends de almacenamiento de ONTAP en el Centro de control de Astra para crear una relación de replicación.

  Añadir y gestionar back-ends de almacenamiento de ONTAP en Astra Control Center es opcional si has habilitado el aprovisionador de Astra Control.

- **Clusters administrados**: Agregue y administre los siguientes clusters con Astra Control, idealmente en diferentes dominios o sitios de falla:
  - Clúster de Kubernetes de origen
  - Clúster de Kubernetes de destino
  - Clústeres de ONTAP asociados
- **Cuentas de usuario**: Cuando añades un backend de almacenamiento de ONTAP al Centro de control de Astra, aplica las credenciales de usuario con el rol “admin”. Este rol tiene métodos de acceso `http` y.. `ontapi` Se habilitó en los clústeres de origen y destino de ONTAP. Consulte "Gestionar cuentas de usuario en la documentación de ONTAP" si quiere más información.

  Con la funcionalidad de aprovisionamiento de Astra Control, no es necesario definir específicamente un rol de administrador para gestionar clústeres en Astra Control Center, ya que estas credenciales no son necesarias para Astra Control Center.

Astra Control Center no admite la replicación de SnapMirror de NetApp para back-ends de almacenamiento que utilizan el protocolo NVMe over TCP.

Configuración de Astra Trident/ONTAP

Astra Control Center requiere que configure al menos un back-end de almacenamiento que admita replicación para los clústeres de origen y destino. Si los clústeres de origen y destino son los mismos, la aplicación de destino debe usar un back-end de almacenamiento diferente al de la aplicación de origen para obtener la mejor resiliencia.

> La replicación de Astra Control admite aplicaciones que utilicen una única clase de almacenamiento. Al agregar una aplicación a un espacio de nombres, asegúrese de que la aplicación tenga la misma clase de almacenamiento que otras aplicaciones del espacio de nombres. Cuando agregue una RVP a una aplicación replicada, asegúrese de que la nueva RVP tenga la misma clase de almacenamiento que otras RVP del espacio de nombres.

Configurar una relación de replicación

La configuración de una relación de replicación implica lo siguiente:

- Selección de la frecuencia con la que quieres que Astra Control tome una instantánea de una aplicación (que incluye los recursos de Kubernetes de la aplicación, así como las instantáneas de volumen de cada uno de los volúmenes de la aplicación)
- Elegir la programación de replicación (se incluyen recursos de Kubernetes, así como datos de volúmenes persistentes)
- Establecer la hora para que se realice la snapshot

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. Seleccione **Configurar política de replicación**. O bien, en el cuadro Protección de aplicaciones, seleccione la opción acciones y seleccione **Configurar directiva de replicación**.
4. Introduzca o seleccione la siguiente información:
    - **Cluster de destino**: Introduzca un cluster de destino (puede ser el mismo que el cluster de origen).
    - **Clase de almacenamiento de destino**: Seleccione o introduzca la clase de almacenamiento que utiliza la SVM con pares en el clúster de ONTAP de destino. Como práctica recomendada, la clase de almacenamiento de destino debe apuntar a un back-end de almacenamiento distinto al de la clase de almacenamiento de origen.
    - **Tipo de replicación**: `Asynchronous` actualmente es el único tipo de replicación disponible.
    - **Espacio de nombres de destino**: Introduzca espacios de nombres de destino nuevos o existentes para el clúster de destino.
    - (Opcional) Añada espacios de nombres adicionales seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
    - **Frecuencia de replicación**: Establece la frecuencia con la que quieres que Astra Control tome una instantánea y la replique en el destino.
    - **Offset**: Establece el número de minutos desde la parte superior de la hora en que quieres que Astra Control tome una instantánea. Es posible que desee utilizar un offset para no coincidir con otras operaciones programadas.

> Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

5. Seleccione **Siguiente**, revise el resumen y seleccione **Guardar**.

   > Al principio, el estado muestra "app-mirror" antes de que se produzca la primera programación.

   Astra Control crea una snapshot de aplicación utilizada para la replicación.

6. Para ver el estado de la instantánea de la aplicación, seleccione la pestaña **Aplicaciones** > **Snapshots**.

   El nombre de la snapshot usa el formato de `replication-schedule-<string>`. Astra Control conserva la última snapshot utilizada para la replicación. Cualquier instantánea de replicación más antigua se elimina una vez que la replicación se completa correctamente.

Resultado

De este modo se crea la relación de replicación.

Astra Control realiza las siguientes acciones como resultado de establecer la relación:

- Crea un espacio de nombres en el destino (si no existe).
- Crea un PVC en el espacio de nombres de destino correspondiente a las RVP de la aplicación de origen.
- Realiza una instantánea inicial coherente con las aplicaciones.
- Establece la relación de SnapMirror para volúmenes persistentes mediante la snapshot inicial.

La página **Protección de datos** muestra el estado y el estado de la relación de replicación:
<Health status> | <Relationship life cycle state>

Por ejemplo: Normal | establecido

Obtenga más información acerca de los estados y el estado de replicación al final de este tema.

Ponga una aplicación replicada en línea en el clúster de destino (conmutación por error)

Mediante Astra Control, puede conmutar al respaldo las aplicaciones replicadas en un clúster de destino. Este procedimiento detiene la relación de replicación y conecta la aplicación en el clúster de destino. Este procedimiento no detiene la aplicación en el clúster de origen si estaba operativa.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, seleccione **Error**.
4. En la página de conmutación por error, revise la información y seleccione **failover**.

Resultado

Las siguientes acciones se producen como resultado del procedimiento de failover:

- La aplicación de destino se inicia en función de la última instantánea replicada.
- El clúster de origen y la aplicación (si están operativas) no se han detenido y se seguirá ejecutando.
- El estado de replicación cambia a "recuperación tras fallos" y luego a "recuperación tras fallos" cuando ha finalizado.
- La política de protección de la aplicación de origen se copia en la aplicación de destino según los horarios presentes en la aplicación de origen en el momento de la conmutación por error.
- Si la aplicación de origen tiene uno o más ganchos de ejecución posteriores a la restauración habilitados, esos ganchos de ejecución se ejecutan para la aplicación de destino.
- Astra Control muestra la aplicación tanto en los clústeres de origen como de destino y su estado respectivo.

Se ha producido un error al sincronizar una replicación

La operación de resincronización vuelve a establecer la relación de replicación. Puede elegir el origen de la relación para conservar los datos en el clúster de origen o de destino. Esta operación vuelve a establecer las relaciones de SnapMirror para iniciar la replicación de volúmenes en la dirección que se desee.

El proceso detiene la aplicación en el nuevo clúster de destino antes de volver a establecer la replicación.

> Durante el proceso de resincronización, el estado del ciclo de vida muestra como "establecer".

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, selecciona **Resincronizar**.
4. En la página Resync, seleccione la instancia de aplicación de origen o de destino que contenga los datos que desea conservar.

   > Elija el origen de resincronización con cuidado, ya que los datos del destino se sobrescribirán.

5. Seleccione **Resync** para continuar.
6. Escriba "Resync" para confirmar.
7. Seleccione **Sí, resincronización** para finalizar.

Resultado

- La página Replication muestra el estado de "establecimiento".
- Astra Control detiene la aplicación en el nuevo clúster de destino.
- Astra Control vuelve a establecer la replicación de volúmenes persistentes en la dirección seleccionada mediante la resincronización de SnapMirror.
- La página Replication muestra la relación actualizada.

Replicación de aplicaciones inversa

Esta es la operación planificada para mover la aplicación al back-end del almacenamiento de destino y continuar replicando de nuevo al back-end del almacenamiento de origen original. Astra Control detiene la aplicación de origen y replica los datos en el destino antes de conmutar por error a la aplicación de destino.

En esta situación, está intercambiando el origen y el destino.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, seleccione **Replicación inversa**.
4. En la página replicación inversa, revise la información y seleccione **replicación inversa** para continuar.

Resultado

Las siguientes acciones ocurren como resultado de la replicación inversa:

- Se toma una instantánea de los recursos de Kubernetes de la aplicación de origen original.
- Los pods de la aplicación de origen originales se detienen con dignidad al eliminar los recursos de Kubernetes de la aplicación (dejando las RVP y los VP en funcionamiento).
- Después de que los pods se cierran, se toman y replican instantáneas de los volúmenes de la aplicación.
- Las relaciones de SnapMirror se rompen, lo que hace que los volúmenes de destino estén listos para la lectura/escritura.
- Los recursos de Kubernetes de la aplicación se restauran a partir de la instantánea previa al cierre, utilizando los datos del volumen replicados después de que se cerró la aplicación de origen original.
- La replicación se restablece en la dirección inversa.

Conmutación tras error de las aplicaciones al clúster de origen original

Con Astra Control, puede conseguir un «retorno tras la recuperación» después de una operación de conmutación por error utilizando la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Astra Control replica (resincroniza) cualquier cambio de aplicación en la aplicación de origen original antes de revertir la dirección de la replicación.

Este proceso se inicia desde una relación que ha completado una conmutación al nodo de respaldo a un destino e implica los siguientes pasos:

- Comience con un estado de conmutación al respaldo.
- Volver a sincronizar la relación.
- Invierta la replicación.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, selecciona **Resincronizar**.
4. Para una operación de conmutación por error, seleccione la aplicación con error como origen de la operación de resincronización (conservando los datos escritos después de la conmutación por error).
5. Escriba "Resync" para confirmar.
6. Seleccione **Sí, resincronización** para finalizar.
7. Una vez finalizada la resincronización, en la ficha Protección de datos > replicación, en el menú acciones, seleccione **replicación inversa**.
8. En la página replicación inversa, revise la información y seleccione **replicación inversa**.

Resultado

Esto combina los resultados de las operaciones de "resincronización" y "relación inversa" para conectar la aplicación en el clúster de origen original con la reanudación de la replicación al clúster de destino original.

Eliminar una relación de replicación de aplicaciones

La eliminación de la relación da como resultado dos aplicaciones independientes sin relación entre ellas.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el cuadro Protección de aplicaciones o en el diagrama de relaciones, seleccione **Eliminar relación de replicación**.

Resultado

Las siguientes acciones ocurren como resultado de eliminar una relación de replicación:

- Si se establece la relación pero la aplicación aún no se ha conectado en el clúster de destino (se ha producido un error al respecto), Astra Control conserva las RVP creadas durante la inicialización, deja una aplicación gestionada "vacía" en el clúster de destino y conserva la aplicación de destino para mantener las copias de seguridad que se hayan creado.
- Si la aplicación se ha conectado en el clúster de destino (con errores), Astra Control conserva las RVP y las aplicaciones de destino. Las aplicaciones de origen y destino se tratan ahora como aplicaciones independientes. Las programaciones de backup permanecen en ambas aplicaciones, pero no se asocian entre sí.

estado de la relación de replicación y estados del ciclo de vida de la relación

Astra Control muestra el estado de la relación y los estados del ciclo de vida de la relación de replicación.

Estados de la relación de replicación

Los siguientes Estados indican el estado de la relación de replicación:

- **Normal**: La relación se establece o se ha establecido, y la instantánea más reciente se ha transferido con éxito.
- **Advertencia**: La relación está fallando o ya falló (y por lo tanto ya no protege la aplicación de origen).
- **Crítico**
  - La relación se ha establecido o se ha realizado una conmutación por error, y el último intento de reconciliación ha fallado.
  - Se establece la relación y se produce un error en el último intento de reconciliar la adición de una nueva RVP.
  - Se establece la relación (por lo que una instantánea se ha replicado correctamente y es posible la recuperación tras fallos), pero la instantánea más reciente ha fallado o no se ha podido replicar.

estados de ciclo de vida de replicación

Los siguientes estados reflejan las diferentes etapas del ciclo de vida de la replicación:

- **Establecer**: Se está creando una nueva relación de replicación. Astra Control crea un espacio de nombres

en caso necesario, crea reclamaciones de volúmenes persistentes (RVP) en los nuevos volúmenes en el clúster de destino y crea relaciones con SnapMirror. Este estado también puede indicar que la replicación está resincronizada o invirtiendo la replicación.

- **Establecido**: Existe una relación de replicación. Astra Control comprueba periódicamente que los RVP estén disponibles, comprueba la relación de replicación, crea snapshots de la aplicación periódicamente e identifica cualquier RVP de origen nuevo en la aplicación. Si es así, Astra Control crea los recursos para incluirlos en la replicación.
- **Fallo**: Astra Control rompe las relaciones de SnapMirror y restaura los recursos de Kubernetes de la aplicación a partir de la última instantánea de la aplicación replicada con éxito.
- **Fallo de más**: Astra Control deja de replicar desde el clúster de origen, utiliza la instantánea de la aplicación replicada más reciente (exitosa) en el destino y restaura los recursos de Kubernetes.
- **Resyncing**: Astra Control reenvía los nuevos datos del origen de resincronización al destino de resincronización mediante SnapMirror resync. Es posible que esta operación sobrescriba algunos de los datos del destino en función de la dirección de la sincronización. Astra Control detiene la aplicación que se ejecuta en el espacio de nombres de destino y elimina la aplicación Kubernetes. Durante el proceso de resincronización, el estado muestra como "establecer".
- **Inversión**: Es la operación planificada para mover la aplicación al clúster de destino mientras continúa la réplica al clúster de origen original. Astra Control detiene la aplicación en el clúster de origen y replica los datos en el destino antes de conmutar por error la aplicación al clúster de destino. Durante la replicación inversa, el estado aparece como "establecer".
- **Eliminación**:
  - Si la relación de replicación se ha establecido pero aún no se ha realizado una conmutación por error, Astra Control elimina las RVP que se crearon durante la replicación y elimina la aplicación administrada de destino.
  - Si la replicación ya ha fallado, Astra Control conserva las EVs y la aplicación de destino.

Clone y migre aplicaciones

Puede clonar una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control clona una aplicación, crea un clon de la configuración de la aplicación y del almacenamiento persistente.

El clonado puede ayudarle si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro. Por ejemplo, es posible que desee mover cargas de trabajo mediante una canalización de CI/CD y entre espacios de nombres Kubernetes. Puede utilizar la interfaz de usuario de Astra Control Center o "API de control Astra" para clonar y migrar aplicaciones.

Antes de empezar

- **Comprobar volúmenes de destino**: Si clona a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de clonado si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que se produzca un error en la operación de clonado. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- Para clonar aplicaciones en un clúster diferente, debe asegurarse de que las instancias de cloud que contienen los clústeres de origen y destino (si no son iguales) tienen un bloque predeterminado. Deberá asignar un bloque predeterminado para cada instancia de cloud.

- Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.

> Durante la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Por este motivo, es necesario configurar una política de exportación de volúmenes ONTAP para permitir estas operaciones. Puede hacerlo con los siguientes comandos:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limitaciones de clones

- **Clases de almacenamiento explícitas**: Si implementa una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Aplicaciones respaldadas por la economía de ontap-nas**: No puede usar operaciones de clonación si la clase de almacenamiento de su aplicación está respaldada por el `ontap-nas-economy` controlador. Sin embargo, usted puede "habilite el backup y la restauración para las operaciones económicas de ontap-nas".
- **Clones y restricciones de usuario**: Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación a un nuevo espacio de nombres en el mismo clúster o a cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.
- **Los clones utilizan cubos predeterminados**: Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar opcionalmente un ID de bloque. Sin embargo, en una operación de clonado de aplicaciones, siempre se utiliza el bloque predeterminado que se ha definido. No existe ninguna opción para cambiar bloques para un clon. Si desea controlar qué segmento se utiliza, puede hacer lo mismo "cambiar el valor predeterminado del segmento" o haga un "Backup" seguido de un "restaurar" por separado.
- **Con Jenkins CI**: Si clona una instancia de Jenkins CI desplegada por el operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.
- **Con bloques S3**: Los bloques S3 de Astra Control Center no informan de la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.
- **Con una versión específica de PostgreSQL**: Los clones de aplicaciones dentro del mismo clúster fallan constantemente con el gráfico BitNami PostgreSQL 11.5.0. Para clonar correctamente, utilice una versión anterior o posterior del gráfico.

Consideraciones sobre OpenShift

- **Clusters y OpenShift versiones**: Si clona una aplicación entre clústeres, los clústeres de origen y destino deben ser la misma distribución de OpenShift. Por ejemplo, si clona una aplicación de un clúster de OpenShift 4.7, utilice un clúster de destino que también sea OpenShift 4.7.

- **Proyectos y UID**: Cuando se crea un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Pasos

1. Seleccione **aplicaciones**.
2. Debe realizar una de las siguientes acciones:
   - Seleccione el menú Opciones de la columna **acciones** de la aplicación deseada.
   - Seleccione el nombre de la aplicación deseada y seleccione la lista desplegable de estado en la parte superior derecha de la página.
3. Seleccione **Clonar**.
4. Especifique los detalles del clon:
   - Introduzca un nombre.
   - Elija un clúster de destino para el clon.
   - Introduzca los espacios de nombres de destino para el clon. Cada espacio de nombres de origen asociado a la aplicación se asigna al espacio de nombres de destino que defina.

     Astra Control crea nuevos espacios de nombres de destino como parte de la operación de clonación. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

   - Seleccione **Siguiente**.
   - Elija mantener la clase de almacenamiento original asociada a la aplicación o seleccionar una clase de almacenamiento diferente.

     Puedes migrar una clase de almacenamiento de una aplicación a una clase de almacenamiento de proveedor de nube nativo u otro tipo de almacenamiento compatible, y migrar una aplicación desde una clase de almacenamiento respaldada por `ontap-nas-economy` a una clase de almacenamiento respaldada por `ontap-nas` en el mismo clúster o copie la aplicación en otro clúster con una clase de almacenamiento respaldada por `ontap-nas-economy` controlador.

   Si selecciona otra clase de almacenamiento y esta clase de almacenamiento no existe en el momento de la restauración, se devolverá un error.

5. Seleccione **Siguiente**.
6. Revise la información sobre el clon y seleccione **Clonar**.

Resultado

Astra Control clona la aplicación en función de la información proporcionada. La operación de clonado se

realiza correctamente cuando se encuentra el nuevo clon de la aplicación `Healthy` en la página **aplicaciones**.

Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

> Después de una operación de protección de datos (clonado, backup o restauración) y un posterior cambio de tamaño de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Gestione los enlaces de ejecución de aplicaciones

Un enlace de ejecución es una acción personalizada que puede configurar para que se ejecute junto con una operación de protección de datos de una aplicación gestionada. Por ejemplo, si dispone de una aplicación de base de datos, puede utilizar un enlace de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez completada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Tipos de enlaces de ejecución

Astra Control Center admite los siguientes tipos de ganchos de ejecución, basados en el momento en el que se pueden ejecutar:

- Copia previa de Snapshot
- Possnapshot
- Previo al backup
- Después del backup
- Después de la restauración
- Después de la conmutación al respaldo

Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución a una aplicación, puede agregar filtros a un enlace de ejecución para gestionar los contenedores que coincidirá el enlace. Los filtros son útiles para aplicaciones que usan la misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito diferente (como Elasticsearch). Los filtros le permiten crear escenarios donde los enlaces de ejecución se ejecutan en algunos, pero no necesariamente todos los contenedores idénticos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agregue a un enlace de ejecución utiliza una expresión regular para hacer coincidir los contenedores del clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor. Las expresiones regulares para los filtros utilizan la sintaxis expresión regular 2 (RE2), que no admite la creación de un filtro que excluye contenedores de la lista de coincidencias. Para obtener información sobre la sintaxis que admite Astra Control para las expresiones regulares en los filtros de

enlace de ejecución, consulte "Soporte de sintaxis de expresión regular 2 (RE2)".

> Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Notas importantes sobre los enlaces de ejecución personalizados

Tenga en cuenta lo siguiente al planificar enlaces de ejecución para sus aplicaciones.

> Debido a que los enlaces de ejecución a menudo reducen o desactivan por completo la funcionalidad de la aplicación con la que se ejecutan, siempre debe intentar minimizar el tiempo que tardan los enlaces de ejecución personalizados.
> Si inicia una operación de copia de seguridad o de instantánea con los enlaces de ejecución asociados pero, a continuación, la cancela, los ganchos pueden ejecutarse si ya se ha iniciado la operación de copia de seguridad o de Snapshot. Esto significa que la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

- La función de enlaces de ejecución está deshabilitada de forma predeterminada para las nuevas implementaciones de Astra Control.
  - Debe activar la función de enlaces de ejecución antes de poder utilizar los enlaces de ejecución.
  - Los usuarios propietario o administrador pueden habilitar o deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en la cuenta de Astra Control actual. Consulte Active la función de enlaces de ejecución y.. Desactive la función de enlaces de ejecución si desea obtener instrucciones.
  - El estado de habilitación de la función se preserva durante las actualizaciones de Astra Control.
- Un enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Muchos enlaces de ejecución pueden hacer referencia al mismo script.
- Astra Control requiere que las secuencias de comandos que utilizan los enlaces de ejecución se escriban en el formato de secuencias de comandos de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Astra Control utiliza la configuración del enlace de ejecución y cualquier criterio coincidente para determinar qué ganchos se aplican a una operación de instantánea, copia de seguridad o restauración.
- Todos los fallos del enlace de ejecución son fallos de software; otros ganchos y la operación de protección de datos se siguen intentando incluso si falla un gancho. Sin embargo, cuando falla un gancho, se registra un suceso de advertencia en el registro de eventos de la página **Activity**.
- Para crear, editar o eliminar enlaces de ejecución, debe ser un usuario con permisos de propietario, administrador o miembro.
- Si un enlace de ejecución tarda más de 25 minutos en ejecutarse, el enlace fallará, creando una entrada de registro de eventos con un código de retorno de "N/A". Se agotará el tiempo de espera de todas las instantáneas afectadas y se marcarán como errores, con una entrada de registro de eventos resultante que tenga en cuenta el tiempo de espera.
- Para las operaciones de protección de datos bajo demanda, todos los eventos de enlace se generan y guardan en el registro de eventos de la página **Actividad**. Sin embargo, en el caso de las operaciones de protección de datos programadas, solo se registran los eventos de fallo de enlace en el registro de eventos (los eventos generados por las propias operaciones de protección de datos programadas aún se

registran).

- Si Astra Control Center conmuta por error una aplicación de origen replicada a la aplicación de destino, todos los ganchos de ejecución posteriores a la conmutación al nodo de respaldo que estén habilitados para la aplicación de origen se ejecutan para la aplicación de destino una vez completada la conmutación por error.

> Si has ejecutado ganchos posteriores a la restauración con Astra Control Center 23,04 y actualizado tu Astra Control Center a la versión 23,07 o posterior, los ganchos de ejecución posteriores a la restauración ya no se ejecutarán tras una replicación de conmutación al respaldo. Necesitas crear nuevos ganchos de ejecución posteriores a la conmutación por error para tus aplicaciones. También puede cambiar el tipo de operación de los ganchos posteriores a la restauración existentes destinados a recuperaciones tras fallos de «post-restore» a «post-failover».

Orden de ejecución

Cuando se ejecuta una operación de protección de datos, los eventos de enlace de ejecución tienen lugar en el siguiente orden:

1. Los ganchos de ejecución de preoperación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos ganchos de prefuncionamiento personalizados como necesite, pero el orden de ejecución de estos enlaces antes de la operación no está garantizado ni configurable.
2. Se realiza la operación de protección de datos.
3. Los enlaces de ejecución de post-operación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces de post-operación personalizados como necesite, pero el orden de ejecución de estos enlaces después de la operación no está garantizado ni configurable.

Si crea varios enlaces de ejecución del mismo tipo (por ejemplo, presnapshot), no se garantiza el orden de ejecución de esos enlaces. Sin embargo, el orden de ejecución de ganchos de diferentes tipos está garantizado. Por ejemplo, el orden de ejecución de una configuración que tiene todos los diferentes tipos de ganchos se vería así:

1. Ganchos de precopia de seguridad ejecutados
2. Ganchos presnapshot ejecutados
3. Ganchos posteriores a la instantánea ejecutados
4. Se han ejecutado los enlaces posteriores a la copia de seguridad
5. Ganchos posteriores a la restauración ejecutados

Puede ver un ejemplo de esta configuración en el número de escenario 2 de la tabla de la Determine si se ejecutará un gancho.

> Siempre debe probar sus secuencias de comandos de ejecución de enlace antes de habilitarlas en un entorno de producción. Puede utilizar el comando 'kubectl exec' para probar cómodamente los scripts. Después de habilitar los enlaces de ejecución en un entorno de producción, pruebe las copias Snapshot y backups resultantes para garantizar que sean coherentes. Para ello, puede clonar la aplicación en un espacio de nombres temporal, restaurar la instantánea o la copia de seguridad y, a continuación, probar la aplicación.

Determine si se ejecutará un gancho

Utilice la siguiente tabla para determinar si se ejecutará un enlace de ejecución personalizado para su aplicación.

Tenga en cuenta que todas las operaciones de aplicaciones de alto nivel consisten en ejecutar una de las operaciones básicas de copia Snapshot, backup o restauración. Según el supuesto, una operación de clonado puede consistir en diversas combinaciones de estas operaciones, de modo que lo que enlaza la ejecución de una operación de clonado será diferente.

Las operaciones de restauración sin movimiento requieren una snapshot o un backup existentes, por lo que estas operaciones no ejecutan datos instantáneos ni enlaces de backup.

> Si comienza pero luego cancela una copia de seguridad que incluye una instantánea y hay enlaces de ejecución asociados, es posible que se ejecuten algunos enlaces y es posible que otros no. Esto significa que un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado. Tenga en cuenta los siguientes puntos para realizar backups cancelados con enlaces de ejecución asociados:
>
> - Los enlaces de copia de seguridad previa y posterior siempre se ejecutan.
> - Si la copia de seguridad incluye una nueva instantánea y se ha iniciado la instantánea, se ejecutan los enlaces de preinstantánea y posterior a la instantánea.
> - Si la copia de seguridad se cancela antes del inicio de la instantánea, no se ejecutan los enlaces presnapshot y post snapshot.

Situación	Funcionamiento	Snapshot existente	Backup existente	Espacio de nombres	Clúster	Funcionan los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos	Se ejecutan los ganchos de failover
1	Clonar	N	N	Nuevo	Igual	Y	N	Y	N
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y	N
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y	N
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y	N
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	N	Y	N
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y	N
7	Restaurar	Y	N	Existente	Igual	N	N	Y	N
8	Restaurar	N	Y	Existente	Igual	N	N	Y	N
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.	N
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.	N
11	Backup	Y	N.A.	N.A.	N.A.	N	N	N.A.	N

Situación	Funcionamiento	Snapshot existente	Backup existente	Espacio de nombres	Clúster	Funcionan los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos	Se ejecutan los ganchos de failover
12	Conmutación al respaldo	Y	N.A.	Creado por replicación	Diferente	N	N	N	Y
13	Conmutación al respaldo	Y	N.A.	Creado por replicación	Igual	N	N	N	Y

Ejemplos de gancho de ejecución

Visite la "Proyecto Verda GitHub de NetApp" Para descargar enlaces de ejecución real para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios enlaces de ejecución personalizados.

Active la función de enlaces de ejecución

Si es un usuario propietario o administrador, puede activar la función de enlaces de ejecución. Cuando habilita la función, todos los usuarios definidos en esta cuenta de Astra Control pueden usar ganchos de ejecución y ver los ganchos de ejecución y los scripts de enlace existentes.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione **Enable execution hooks**.

   Aparece la pestaña **Cuenta** > **Ajustes de función**.

4. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
5. Selecciona **Activar**.
6. Observe la advertencia de seguridad que aparece.
7. Seleccione **Sí, habilite los ganchos de ejecución**.

Desactive la función de enlaces de ejecución

Si eres un usuario propietario o administrador, puedes deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en esta cuenta de Astra Control. Debe suprimir todos los enlaces de ejecución existentes antes de desactivar la función de enlaces de ejecución. Consulte Eliminar un gancho de ejecución para obtener instrucciones sobre cómo eliminar un enlace de ejecución existente.

Pasos

1. Vaya a **Cuenta** y luego seleccione la pestaña **Ajustes de función**.
2. Seleccione la ficha **ganchos de ejecución**.

3. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
4. Seleccione **Desactivar**.
5. Observe la advertencia que aparece.
6. Tipo `disable` para confirmar que desea deshabilitar la función para todos los usuarios.
7. Seleccione **Sí, desactivar**.

Ver los enlaces de ejecución existentes

Puede ver los enlaces de ejecución personalizados existentes para una aplicación.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.

   Puede ver todos los enlaces de ejecución habilitados o desactivados en la lista resultante. Puede ver el estado de un gancho, cuántos contenedores coinciden, la hora de creación y cuándo se ejecuta (antes o después de la operación). Puede seleccionar la + icono junto al nombre del gancho para expandir la lista de contenedores en los que se ejecutará. Para ver los registros de eventos que rodean los enlaces de ejecución de esta aplicación, vaya a la ficha **actividad**.

Ver los scripts existentes

Puede ver los scripts cargados existentes. También puede ver qué scripts están en uso, y qué enlaces los están utilizando, en esta página.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.

   En esta página puede ver una lista de los scripts cargados existentes. La columna **Used by** muestra los enlaces de ejecución que utilizan cada script.

Agregar un script

Cada enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos ganchos de ejecución pueden hacer referencia al mismo script; esto le permite actualizar muchos ganchos de ejecución cambiando solo un script.

Pasos

1. Asegúrese de que la función de enlaces de ejecución es activado.
2. Vaya a **cuenta**.
3. Seleccione la ficha **Scripts**.
4. Seleccione **Agregar**.
5. Debe realizar una de las siguientes acciones:
   - Cargue un script personalizado.
     i. Seleccione la opción **cargar archivo**.

    ii. Navegue hasta un archivo y cárguelo.
    iii. Asigne al script un nombre único.
    iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
    v. Seleccione **Guardar script**.
  - Pegar en un script personalizado desde el portapapeles.
    i. Seleccione la opción **Pegar o Tipo**.
    ii. Seleccione el campo de texto y pegue el texto del script en el campo.
    iii. Asigne al script un nombre único.
    iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
6. Seleccione **Guardar script**.

Resultado

La nueva secuencia de comandos aparece en la lista de la ficha **Scripts**.

Eliminar un script

Puede eliminar una secuencia de comandos del sistema si ya no es necesaria y no se utiliza en ningún anzuelo de ejecución.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Elija la secuencia de comandos que desee quitar y seleccione el menú en la columna **acciones**.
4. Seleccione **Eliminar**.

> Si la secuencia de comandos está asociada con uno o más enlaces de ejecución, la acción **Eliminar** no estará disponible. Para eliminar la secuencia de comandos, primero edite los enlaces de ejecución asociados y asócielos a una secuencia de comandos diferente.

Cree un enlace de ejecución personalizado

Puedes crear un gancho de ejecución personalizado para una aplicación y añadirlo a Astra Control. Consulte Ejemplos de gancho de ejecución para ejemplos de gancho. Necesita tener permisos de propietario, administrador o miembro para crear enlaces de ejecución.

> Cuando cree un script de shell personalizado para utilizarlo como un enlace de ejecución, recuerde especificar el shell adecuado al principio del archivo, a menos que esté ejecutando comandos específicos o proporcionando la ruta completa a un ejecutable.

Pasos

1. Asegúrese de que la función de enlaces de ejecución es activado.
2. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
3. Seleccione la ficha **ganchos de ejecución**.
4. Seleccione **Agregar**.
5. En el área **Detalles del gancho**:

a. Determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.

b. Introduzca un nombre único para el gancho.

c. (Opcional) Introduzca cualquier argumento para pasar al gancho durante la ejecución, pulsando la tecla Intro después de cada argumento que introduzca para grabar cada uno.

6. (Opcional) en el área **Detalles de filtro de gancho**, puede añadir filtros para controlar en qué contenedores se ejecuta el gancho de ejecución:

   a. Seleccione **Agregar filtro**.

   b. En la columna **Tipo de filtro Hook**, elija un atributo en el que filtrar en el menú desplegable.

   c. En la columna **Regex**, introduzca una expresión regular que se utilizará como filtro. Astra Control utiliza "Sintaxis de regex de expresión regular 2 (RE2)".

   > Si filtra el nombre exacto de un atributo (como un nombre de POD) sin ningún otro texto en el campo de expresión normal, se realizará una coincidencia de subcadena. Para que coincida con un nombre exacto y sólo con ese nombre, utilice la sintaxis de coincidencia de cadena exacta (por ejemplo, `^exact_podname$`).

   d. Para añadir más filtros, seleccione **Agregar filtro**.

   > Se combinan varios filtros para un enlace de ejecución con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

7. Cuando termine, seleccione **Siguiente**.

8. En el área **Script**, siga uno de estos procedimientos:

   - Agregue un nuevo script.

     i. Seleccione **Agregar**.

     ii. Debe realizar una de las siguientes acciones:

       - Cargue un script personalizado.

         I. Seleccione la opción **cargar archivo**.

         II. Navegue hasta un archivo y cárguelo.

         III. Asigne al script un nombre único.

         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.

         V. Seleccione **Guardar script**.

       - Pegar en un script personalizado desde el portapapeles.

         I. Seleccione la opción **Pegar o Tipo**.

         II. Seleccione el campo de texto y pegue el texto del script en el campo.

         III. Asigne al script un nombre único.

         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.

   - Seleccione un script existente de la lista.

     Esto indica al enlace de ejecución que utilice esta secuencia de comandos.

9. Seleccione **Siguiente**.
10. Revise la configuración del gancho de ejecución.
11. Seleccione **Agregar**.

Compruebe el estado de un enlace de ejecución

Después de que una operación de instantánea, backup o restauración finalice la ejecución, puede comprobar el estado de los enlaces de ejecución que se ejecutan como parte de la operación. Puede utilizar esta información de estado para determinar si desea mantener el enlace de ejecución, modificarlo o eliminarlo.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **Protección de datos**.
3. Seleccione **instantáneas** para ver las instantáneas en ejecución, o **copias de seguridad** para ver las copias de seguridad en ejecución.

   El estado * gancho* muestra el estado de la ejecución del gancho de ejecución una vez completada la operación. Puede pasar el ratón sobre el estado para obtener más detalles. Por ejemplo, si hay fallos de enlace de ejecución durante una instantánea, pasar el ratón sobre el estado de enlace de esa instantánea proporciona una lista de los enlaces de ejecución fallidos. Para ver las razones de cada fallo, puede consultar la página **actividad** en el área de navegación del lado izquierdo.

Ver el uso de las secuencias de comandos

Puede ver qué enlaces de ejecución utilizan una secuencia de comandos determinada en la interfaz de usuario web de Astra Control.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **Scripts**.

   La columna **usado por** de la lista de scripts contiene detalles sobre qué ganchos están utilizando cada script de la lista.

3. Seleccione la información de la columna **utilizado por** para un script que le interese.

   Aparece una lista más detallada, con los nombres de los ganchos que utilizan la secuencia de comandos y el tipo de operación con la que están configurados para ejecutarse.

Edite un gancho de ejecución

Puede editar un enlace de ejecución si desea cambiar sus atributos, filtros o la secuencia de comandos que utiliza. Necesita tener permisos de propietario, administrador o miembro para editar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para un gancho que desee editar.
4. Seleccione **Editar**.

5. Haga los cambios necesarios, seleccione **Siguiente** después de completar cada sección.
6. Seleccione **Guardar**.

Desactivar un gancho de ejecución

Puede desactivar un gancho de ejecución si desea impedir temporalmente que se ejecute antes o después de una instantánea de una aplicación. Necesita tener permisos de propietario, administrador o miembro para desactivar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea desactivar.
4. Seleccione **Desactivar**.

Eliminar un gancho de ejecución

Puede eliminar un enlace de ejecución por completo si ya no lo necesita. Necesita tener permisos de propietario, administrador o miembro para eliminar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea eliminar.
4. Seleccione **Eliminar**.
5. En el cuadro de diálogo que aparece, escriba "delete" para confirmar.
6. Seleccione **Sí, elimine el enlace de ejecución**.

Si quiere más información

- "Proyecto Verda GitHub de NetApp"

Protege Astra Control Center con Astra Control Center

A fin de garantizar mejor la resiliencia frente a errores graves en el clúster de Kubernetes donde se ejecuta Astra Control Center, protege la aplicación de Astra Control Center en sí misma. Puedes realizar backups y restauraciones de Astra Control Center con una instancia secundaria del Astra Control Center o utilizar la replicación de Astra si el almacenamiento subyacente utiliza ONTAP.

En estos casos, se pone en marcha y se configura una segunda instancia de Astra Control Center en un dominio de fallos diferente y se ejecuta en un segundo clúster de Kubernetes distinto al de la instancia principal del Astra Control Center. La segunda instancia de Astra Control se usa para crear backups y restaurar potencialmente la instancia principal de Astra Control Center. Una instancia del Astra Control Center, restaurada o replicada, seguirá proporcionando la gestión de los datos de aplicaciones para las aplicaciones del cluster de aplicaciones y restaurará la accesibilidad a los backups y copias Snapshot de esas aplicaciones.

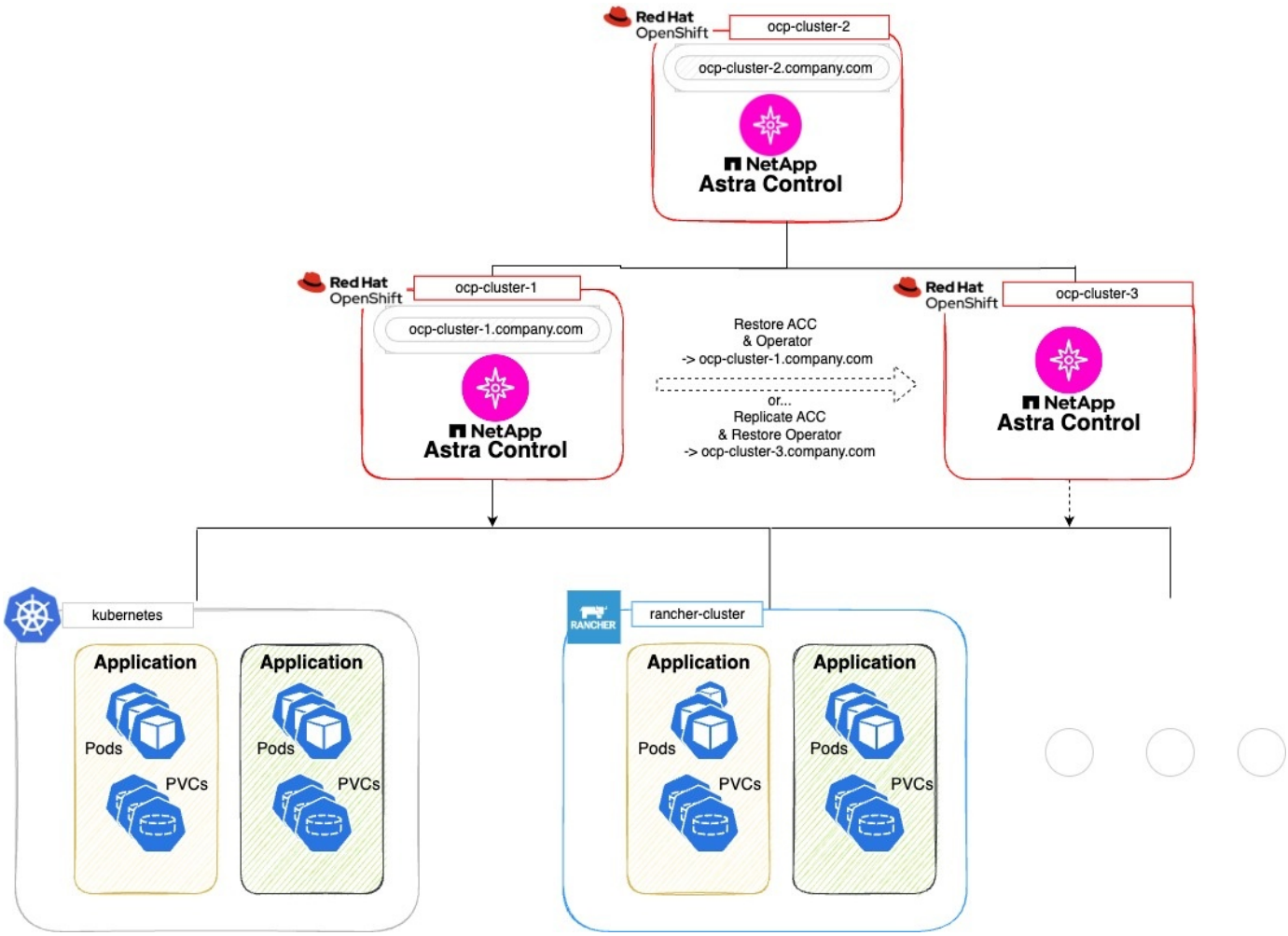
Antes de empezar

Asegúrate de tener lo siguiente antes de configurar las situaciones de protección para Astra Control Center:

- **Un clúster de Kubernetes que ejecuta la instancia principal de Astra Control Center**: Este clúster aloja la instancia principal de Astra Control Center que gestiona los clústeres de aplicaciones.
- **Un segundo clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que ejecuta la instancia secundaria de Astra Control Center**: Este clúster aloja la instancia de Astra Control Center que gestiona la instancia principal de Astra Control Center.
- **Un tercer clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal**: Este clúster alojará la instancia restaurada o replicada de Astra Control Center. Debe tener disponible el mismo espacio de nombres de Astra Control Center que actualmente se pone en marcha en el volumen principal. Por ejemplo, si Astra Control Center se pone en marcha en un espacio de nombres `netapp-acc` en el clúster de origen, el espacio de nombres `netapp-acc` Debe estar disponible y no lo deben usar ninguna aplicación del clúster de Kubernetes de destino.
- **Cubetas compatibles con S3**: Cada instancia de Astra Control Center tiene un cubo de almacenamiento de objetos accesible compatible con S3.
- **Un equilibrador de carga configurado**: El equilibrador de carga proporciona una dirección IP para Astra y debe tener conectividad de red con los clústeres de aplicaciones y los dos buckets S3.
- **Los clústeres cumplen con los requisitos del Centro de control de Astra**: Cada clúster utilizado en la protección del Centro de control de Astra cumple "requisitos generales de Astra Control Center".

Acerca de esta tarea

Estos procedimientos describen los pasos necesarios para restaurar Astra Control Center en un clúster nuevo mediante uno de ellos backup y restauración o. replicación. Los pasos se basan en la configuración de ejemplo que se describe a continuación:



En esta configuración de ejemplo, se muestra lo siguiente:

- **Un clúster de Kubernetes que ejecuta la instancia principal de Astra Control Center**:
  - Clúster de OpenShift: `ocp-cluster-1`
  - Instancia primaria de Astra Control Center: `ocp-cluster-1.company.com`
  - Este cluster gestiona los clusters de aplicaciones.
- **El segundo clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que ejecuta la instancia secundaria de Astra Control Center**:
  - Clúster de OpenShift: `ocp-cluster-2`
  - Instancia secundaria de Astra Control Center: `ocp-cluster-2.company.com`
  - Este clúster se utilizará para crear una copia de seguridad de la instancia principal de Astra Control Center o configurar la replicación en un clúster diferente (en este ejemplo, la `ocp-cluster-3` clúster).
- **Un tercer clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que se utilizará para las operaciones de restauración**:
  - Clúster de OpenShift: `ocp-cluster-3`
  - Tercera instancia de Astra Control Center: `ocp-cluster-3.company.com`
  - Este clúster se utilizará para la restauración o replicación de conmutación al nodo de respaldo de Astra

Control Center.

> Lo ideal sería que el clúster de aplicaciones se situara fuera de los tres clústeres de Astra Control Center, tal y como muestran los clústeres de kubernetes y rancher en la imagen anterior.

No se muestra en el diagrama:

- Todos los clústeres tienen back-ends de ONTAP con Astra Trident o el aprovisionador de Astra Control instalado.
- En esta configuración, los clusters de OpenShift utilizan MetalLB como equilibrador de carga.
- La controladora Snapshot y VolumeSnapshotClass también se instalan en todos los clústeres, como se describe en la "requisitos previos".

Paso 1 Opción: Realizar copias de seguridad y restaurar Astra Control Center

Este procedimiento describe los pasos necesarios para restaurar Astra Control Center en un nuevo clúster mediante el backup y la restauración.

En este ejemplo, Astra Control Center siempre se instala en la `netapp-acc` el espacio de nombres y el operador se instalan en la `netapp-acc-operator` espacio de nombres.

> Aunque no se describe, el operador de Astra Control Center también puede ponerse en marcha en el mismo espacio de nombres que Astra CR.

Antes de empezar

- Ha instalado el Astra Control Center principal en un clúster.
- Ha instalado el Astra Control Center secundario en un clúster diferente.

Pasos

1. Gestiona la aplicación principal del Centro de control de Astra y el clúster de destino desde la instancia del Centro de control de Astra secundaria (ejecutándose en `ocp-cluster-2` clúster):
   a. Inicia sesión en la instancia secundaria de Astra Control Center.
   b. "Añada el clúster de Astra Control Center principal" (`ocp-cluster-1`).
   c. "Añada el tercer clúster de destino" (`ocp-cluster-3`) que se utilizará para la restauración.
2. Gestiona Astra Control Center y el operador del Astra Control Center en el Astra Control Center secundario:
   a. En la página aplicaciones, seleccione **definir**.
   b. En la ventana **Definir aplicación**, introduzca el nombre de la nueva aplicación (`netapp-acc`).
   c. Elige el clúster que ejecuta el Astra Control Center principal (`ocp-cluster-1`) De la lista desplegable **Cluster**.
   d. Elija la `netapp-acc` Espacio de nombres para Astra Control Center en la lista desplegable **Namespace**.
   e. En la página Recursos de Cluster, seleccione **Incluir recursos adicionales de ámbito de cluster**.
   f. Seleccione **Agregar regla de inclusión**.
   g. Seleccione estas entradas y seleccione **Agregar**:

- Selector de etiquetas: <label name>
- Grupo: Apiextensions.k8s.io
- Versión: V1
- Clase: CustomResourceDefinition

h. Confirme la información de la aplicación.

i. Seleccione **definir**.

Después de seleccionar **Definir**, repita el proceso Definir solicitud para el operador `netapp-acc-operator`) y seleccione `netapp-acc-operator` Espacio de nombres en el Asistente de Definición de Aplicación.

3. Crea backups de Astra Control Center y el operador:

   a. En el Astra Control Center secundario, accede a la página Applications seleccionando la pestaña Applications.

   b. "Realice un backup" La aplicación Astra Control Center (`netapp-acc`).

   c. "Realice un backup" el operador (`netapp-acc-operator`).

4. Después de haber realizado el backup de Astra Control Center y el operador, simular un escenario de recuperación ante desastres mediante "Desinstalación de Astra Control Center" del clúster principal.

> Restaurarás Astra Control Center en un nuevo clúster (el tercer clúster de Kubernetes descrito en este procedimiento) y usarás el mismo DNS que el clúster principal para el Astra Control Center recién instalado.

5. Mediante el centro secundario de Astra Control Center, "restaurar" La instancia principal de la aplicación Astra Control Center desde su backup:

   a. Selecciona **Aplicaciones** y luego selecciona el nombre de la aplicación Astra Control Center.

   b. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.

   c. Elija el **Restaurar a nuevos espacios de nombres** como el tipo de restauración.

   d. Introduzca el nombre de la restauración (`netapp-acc`).

   e. Elija el tercer clúster de destino (`ocp-cluster-3`).

   f. Actualice el espacio de nombres de destino para que sea el mismo espacio de nombres que el original.

   g. En la página Restore Source, seleccione la copia de seguridad de la aplicación que se utilizará como origen de la restauración.

   h. Seleccione **Restaurar usando clases de almacenamiento originales**.

   i. Seleccione **Restaurar todos los recursos**.

   j. Revise la información de restauración y, a continuación, seleccione **Restaurar** para iniciar el proceso de restauración que restaura Astra Control Center al clúster de destino (`ocp-cluster-3`). La restauración se completa cuando la aplicación entra `available` estado.

6. Configure Astra Control Center en el clúster de destino:

   a. Abra un terminal y conéctese usando kubeconfig al clúster de destino (`ocp-cluster-3`) Que contiene el Astra Control Center restaurado.

b. Confirme que el `ADDRESS` La columna de la configuración de Astra Control Center hace referencia al nombre DNS del sistema principal:

```
kubectl get acc -n netapp-acc
```

Respuesta:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
1.company.com           True
```

a. Si la `ADDRESS` En la respuesta anterior no tiene el FQDN de la instancia principal de Astra Control Center, actualice la configuración para hacer referencia a los DNS de Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

i. Cambie el `astraAddress` inferior `spec:` Al FQDN (`ocp-cluster-1.company.com` En este ejemplo) de la instancia principal de Astra Control Center.

ii. Guarde la configuración.

iii. Confirme que la dirección se ha actualizado:

```
kubectl get acc -n netapp-acc
```

b. Vaya a la Restaure el operador del centro de control de Astra sección de este documento para completar el proceso de restauración.

Paso 1 Opción: Protección del centro de control Astra con replicación

Este procedimiento describe los pasos necesarios para configurar "Replicación de Astra Control Center" Para proteger la instancia principal de Astra Control Center.

En este ejemplo, Astra Control Center siempre se instala en la `netapp-acc` el espacio de nombres y el operador se instalan en la `netapp-acc-operator` espacio de nombres.

Antes de empezar

- Ha instalado el Astra Control Center principal en un clúster.
- Ha instalado el Astra Control Center secundario en un clúster diferente.

Pasos

1. Gestione la aplicación principal del Centro de Astra Control y el clúster de destino desde la instancia de Astra Control Center secundaria:

   a. Inicia sesión en la instancia secundaria de Astra Control Center.

b. "Añada el clúster de Astra Control Center principal" (`ocp-cluster-1`).

c. "Añada el tercer clúster de destino" (`ocp-cluster-3`) que se utilizará para la replicación.

2. Gestiona Astra Control Center y el operador del Astra Control Center en el Astra Control Center secundario:

   a. Selecciona **Clusters** y selecciona el clúster que contiene el Astra Control Center principal (`ocp-cluster-1`).

   b. Seleccione la ficha **Namespaces**.

   c. Seleccione `netapp-acc` y.. `netapp-acc-operator` espacios de nombres.

   d. Seleccione el menú Acciones y seleccione **Definir como aplicaciones**.

   e. Seleccione **Ver en aplicaciones** para ver las aplicaciones definidas.

3. Configurar Backends para Replicación:

   > La replicación requiere que el clúster principal de Astra Control Center y el clúster de destino (`ocp-cluster-3`) Utilice back-ends de almacenamiento ONTAP con diferentes pares.
   > Después de que cada backend se encuentre y se agregue a Astra Control, el backend aparecerá en la pestaña **Descubierto** de la página Backends.

   a. "Agregue un backend con pares" A Astra Control Center en el clúster principal.

   b. "Agregue un backend con pares" A Astra Control Center en el clúster de destino.

4. Configurar replicación:

   a. En la pantalla Aplicaciones, seleccione `netapp-acc` cliente más.

   b. Seleccione **Configurar política de replicación**.

   c. Seleccione `ocp-cluster-3` como el clúster de destino.

   d. Seleccione la clase de almacenamiento.

   e. Introduzca `netapp-acc` como espacio de nombres de destino.

   f. Cambie la frecuencia de replicación si lo desea.

   g. Seleccione **Siguiente**.

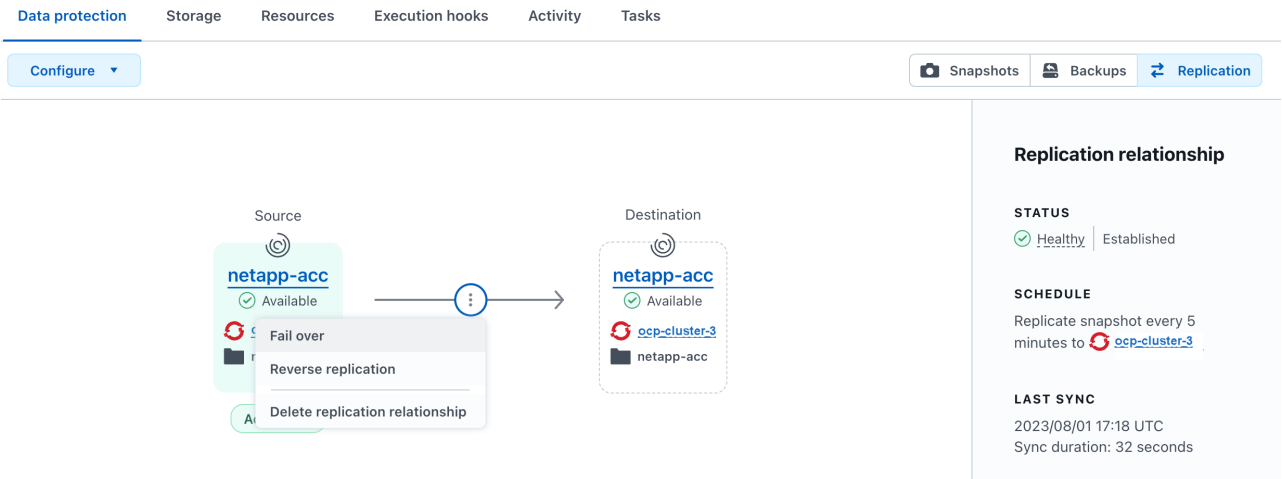
   h. Confirme que la configuración es correcta y seleccione **Guardar**.

      La relación de replicación de `Establishing` para `Established`. Cuando está activa, esta replicación se producirá cada cinco minutos hasta que se elimine la configuración de replicación.

5. Realice una conmutación al nodo de respaldo de la replicación en el otro clúster si el sistema principal está dañado o ya no se puede acceder a él:

   > Asegúrate de que el clúster de destino no tenga Astra Control Center instalado para garantizar una conmutación al nodo de respaldo correcta.

   a. Seleccione el icono de elipses verticales y seleccione **fail over**.



b. Confirme los detalles y seleccione **fail over** para comenzar el proceso de failover.

   El estado de la relación de replicación cambia a. `Failing over` y después `Failed over` cuando finalice.

6. Complete la configuración de failover:

   a. Abra un terminal y conéctelo usando el kubeconfig del tercer grupo (`ocp-cluster-3`). Este clúster ahora tiene Astra Control Center instalado.

   b. Determinar el nombre de dominio completo de Astra Control Center en el tercer clúster (`ocp-cluster-3`).

   c. Actualiza la configuración para hacer referencia a los DNS de Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

      i. Cambie el `astraAddress` inferior `spec:` Con el FQDN (`ocp-cluster-3.company.com`) del tercer cluster de destino.

      ii. Guarde la configuración.

      iii. Confirme que la dirección se ha actualizado:

```
kubectl get acc -n netapp-acc
```

   d. Confirme que todos los CRD de traefik necesarios están presentes:

```
kubectl get crds | grep traefik
```

   CRD DE traefik requeridos:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Si faltan algunos de los CRD anteriores:
   i. Vaya a. "documentación de traefik".
   ii. Copie el área Definiciones en un archivo.
   iii. Aplicar cambios:

```
kubectl apply -f <file name>
```

   iv. Reiniciar traefik:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Vaya a la Restaure el operador del centro de control de Astra sección de este documento para completar el proceso de restauración.

Paso 2: Restaure el operador del centro de control de Astra

Mediante el Astra Control Center secundario, restaure el operador principal del Astra Control Center desde el backup. El espacio de nombres de destino debe ser el mismo que el de origen. En caso de que Astra Control Center se eliminara del clúster de origen principal, seguirán existiendo backups para realizar los mismos pasos de restauración.

Pasos

1. Selecciona **Aplicaciones** y luego selecciona el nombre de la app del operador (`netapp-acc-operator`).

2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**
3. Elija el **Restaurar a nuevos espacios de nombres** como el tipo de restauración.
4. Elija el tercer clúster de destino (`ocp-cluster-3`).
5. Cambie el espacio de nombres para que sea el mismo que el asociado al clúster de origen principal (`netapp-acc-operator`).
6. Seleccione la copia de seguridad realizada anteriormente como origen de restauración.
7. Seleccione **Restaurar usando clases de almacenamiento originales**.
8. Seleccione **Restaurar todos los recursos**.
9. Revise los detalles y haga clic en **Restaurar** para iniciar el proceso de restauración.

   La página Aplicaciones muestra el operador del Centro de control de Astra que se está restaurando en el tercer clúster de destino (`ocp-cluster-3`). Cuando el proceso se completa, el estado se muestra como `Available`. En un plazo de diez minutos, la dirección DNS debería resolverse en la página.

Resultado

Astra Control Center, sus clústeres registrados y las aplicaciones gestionadas con sus copias Snapshot y backups ahora están disponibles en el tercer clúster de destino (`ocp-cluster-3`). Cualquier política de protección que tuviera en el original también está ahí en la nueva instancia. Puede seguir realizando copias Snapshot y backups programadas o bajo demanda.

Resolución de problemas

Determine el estado del sistema y si los procesos de protección se han realizado correctamente.

- **Los pods no están funcionando**: Confirma que todos los pods están activos y en funcionamiento:

  ```
  kubectl get pods -n netapp-acc
  ```

  Si hay algunos pods en la `CrashLookBackOff` estado, reinícielos y deben realizar la transición a. `Running` estado.

- **Confirmar el estado del sistema**: Confirma que el sistema Astra Control Center está en `ready` provincia:

  ```
  kubectl get acc -n netapp-acc
  ```

  Respuesta:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
  1.company.com           True
  ```

- **Confirmar el estado de implementación**: Muestra la información de implementación de Astra Control Center para confirmarlo `Deployment State` es `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **La interfaz de usuario restaurada de Astra Control Center devuelve un error 404**: Si esto sucede cuando lo has seleccionado `AccTraefik` como opción de entrada, marque la CRD de traefik para asegurarse de que todos están instalados.

Supervise el estado de las aplicaciones y del clúster

Ver un resumen del estado de las aplicaciones y el clúster

Seleccione * Dashboard* para ver una vista de alto nivel de sus aplicaciones, clusters, back-ends de almacenamiento y su estado.

No se trata sólo de números o Estados estáticos, sino que se puede profundizar en cada uno de ellos. Por ejemplo, si las aplicaciones no están completamente protegidas, puede pasar el ratón sobre el icono para identificar qué aplicaciones no están completamente protegidas, lo que incluye un motivo.

Aplicaciones

El mosaico **aplicaciones** le ayuda a identificar lo siguiente:

- Cuántas aplicaciones gestiona actualmente con Astra.
- Si esas aplicaciones gestionadas están en buen estado.
- Si las aplicaciones están totalmente protegidas (están protegidas si hay backups recientes disponibles).
- El número de aplicaciones que se han detectado, pero que aún no se han administrado.

  Lo ideal sería que este número fuera cero porque gestionaría o ignoraría aplicaciones después de que se descubrieran. Y, a continuación, supervisaría el número de aplicaciones detectadas en el Panel de control para identificar cuándo los desarrolladores añaden nuevas aplicaciones a un clúster.

Icono de clústeres

El mosaico **Clusters** proporciona detalles similares sobre el estado de los clústeres que está administrando utilizando Astra Control Center, y puede profundizar para obtener más detalles como usted puede con una app.

Icono de los back-ends de almacenamiento

El mosaico **back-ends** de almacenamiento proporciona información para ayudarle a identificar el estado de los back-ends de almacenamiento, incluidos:

- Cuántos back-ends de almacenamiento se gestionan
- Si estos back-ends administrados son en buen estado
- Si los back-ends están totalmente protegidos
- La cantidad de back-ends que se detectan, pero todavía no se gestionan.

Consulte el estado del clúster y gestione las clases de almacenamiento

Después de añadir clústeres que debe gestionar Astra Control Center, puede ver detalles sobre el clúster, como su ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento. También es posible cambiar la clase de almacenamiento predeterminada para los clústeres gestionados.

Ver el estado y los detalles del clúster

Puede ver detalles sobre el clúster, como la ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento.

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster cuyos detalles desea ver.

> Si hay un clúster en `removed` estado aunque la conectividad del clúster y de la red parece correcta (los intentos externos de acceder al clúster mediante las API de Kubernetes se han realizado correctamente), es posible que la imagen que proporcionó a Astra Control ya no sea válida. Esto puede deberse a la rotación o a la caducidad del certificado en el clúster. Para corregir este problema, actualice las credenciales asociadas con el clúster en Astra Control mediante "API de control Astra".

3. Consulte la información en las pestañas **Descripción general**, **almacenamiento** y **actividad** para encontrar la información que busca.
   - **Descripción general**: Detalles sobre los nodos de trabajo, incluido su estado.
   - **almacenamiento**: Los volúmenes persistentes asociados con el cálculo, incluyendo la clase de almacenamiento y el estado.
   - **Actividad**: Muestra las actividades relacionadas con el cluster.

> También puede ver la información del clúster a partir de Astra Control Center **Dashboard**. En la ficha **Clusters** de **Resumen de recursos**, puede seleccionar los clústeres administrados, que le llevará a la página **Clusters**. Después de llegar a la página **Clusters**, siga los pasos descritos anteriormente.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de. Cuando Astra Control gestiona un clúster, realiza un seguimiento de la clase de almacenamiento predeterminada del clúster.

> No cambie la clase de almacenamiento con comandos kubectl. Utilice este procedimiento en su lugar. Astra Control revertirá los cambios si se realizan con kubectl.

Pasos

1. En la interfaz de usuario web de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.

5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Ver el estado y los detalles de una aplicación

Después de empezar a gestionar una aplicación, Astra Control proporciona detalles sobre la aplicación que te permiten identificar el estado de comunicación (si Astra Control puede comunicarse con la aplicación), su estado de protección (si está totalmente protegido en caso de fallo), los pods, el almacenamiento persistente y mucho más.

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Revise la información.

   Estado de la aplicación

   Proporciona un estado que refleja si Astra Control puede comunicarse con la aplicación.

   - **App Protection Status**: Proporciona un estado de la protección de la aplicación:
     - **totalmente protegido**: La aplicación tiene una programación de copia de seguridad activa y una copia de seguridad exitosa que tiene menos de una semana de antigüedad
     - **parcialmente protegido**: La aplicación tiene una programación de copia de seguridad activa, una programación de instantáneas activa o una copia de seguridad o instantánea correcta
     - **desprotegido**: Aplicaciones que no están completamente protegidas o parcialmente protegidas.

       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 es almacenamiento persistente, necesitará una copia de seguridad para recuperar. Una Snapshot no le permite recuperar.
   - **Descripción general**: Información sobre el estado de los pods que están asociados con la aplicación.
   - **Protección de datos**: Permite configurar una directiva de protección de datos y ver las instantáneas y copias de seguridad existentes.
   - **Almacenamiento**: Muestra los volúmenes persistentes a nivel de aplicación. El estado de un volumen persistente es desde el punto de vista del clúster de Kubernetes.
   - **Recursos**: Permite verificar qué recursos se están haciendo copias de seguridad y gestionando.
   - **Actividad**: Muestra las actividades relacionadas con la aplicación.

   > También puede ver la información de la aplicación, empezando por Astra Control Center **Dashboard**. En la ficha **aplicaciones** de **Resumen de recursos**, puede seleccionar las aplicaciones administradas, que le llevará a la página **aplicaciones**. Después de llegar a la página **aplicaciones**, siga los pasos descritos anteriormente.

Gestione su cuenta

Gestione usuarios locales y roles

Puede añadir, eliminar y editar usuarios de la instalación de Astra Control Center mediante la interfaz de usuario de Astra Control. Puede utilizar la interfaz de usuario de Astra Control o. "API de control Astra" para gestionar usuarios.

También se puede utilizar LDAP para realizar autenticación para los usuarios seleccionados.

Utilice LDAP

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra Control. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP. En la siguiente documentación, se ofrece más información:

- "Utilice la API Astra Control para gestionar la autenticación y los usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar grupos y usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar la autenticación remota"

Añadir usuarios

Los propietarios y administradores de cuentas pueden agregar más usuarios a la instalación de Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Agregar usuario**.
4. Introduzca el nombre del usuario, la dirección de correo electrónico y una contraseña temporal.

   El usuario deberá cambiar la contraseña en el primer inicio de sesión.

5. Seleccione una función de usuario con los permisos de sistema adecuados.

   Cada rol proporciona los siguientes permisos:

   - 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.
6. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones** .

Para obtener más información sobre cómo agregar restricciones, consulte "Gestione usuarios locales y roles".

7. Seleccione **Agregar**.

Gestionar contraseñas

Puede gestionar las contraseñas de las cuentas de usuario en Astra Control Center.

Cambie la contraseña

Puede cambiar la contraseña de su cuenta de usuario en cualquier momento.

Pasos

1. Seleccione el icono Usuario situado en la parte superior derecha de la pantalla.
2. Seleccione **Perfil**.
3. En el menú Opciones de la columna **acciones** y seleccione **Cambiar contraseña**.
4. Introduzca una contraseña que se ajuste a los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.
6. Seleccione **Cambiar contraseña**.

Restablecer la contraseña de otro usuario

Si su cuenta tiene permisos de rol de administrador o propietario, puede restablecer las contraseñas de otras cuentas de usuario así como las suyas propias. Al restablecer una contraseña, asigna una contraseña temporal que el usuario tendrá que cambiar al iniciar sesión.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la lista desplegable **acciones**.
3. Seleccione **Restablecer contraseña**.
4. Introduzca una contraseña temporal que cumpla los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.

   La próxima vez que el usuario inicie sesión, se le pedirá que cambie la contraseña.

6. Seleccione **Restablecer contraseña**.

Quitar usuarios

Los usuarios con el rol propietario o administrador pueden eliminar otros usuarios de la cuenta en cualquier momento.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios** , active la casilla de verificación en la fila de cada usuario que desee quitar.
3. En el menú Opciones de la columna **acciones**, seleccione **Eliminar usuario/s**.
4. Cuando se le solicite, confirme la eliminación escribiendo la palabra "eliminar" y, a continuación,

seleccione **Sí, Eliminar usuario**.

Resultado

Astra Control Center elimina al usuario de la cuenta.

Gestionar roles

Es posible gestionar roles si se añaden restricciones de espacio de nombres y se restringen los roles del usuario a dichas restricciones. Esto le permite controlar el acceso a los recursos de su organización. Puede utilizar la interfaz de usuario de Astra Control o. "API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Administrador o propietario puede agregar restricciones de espacio de nombres a las funciones de miembro o de visor.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor.
4. Seleccione **Editar rol**.
5. Active la casilla de verificación **restringir rol a restricciones**.

   La casilla de verificación sólo está disponible para funciones de miembro o de visor. Puede seleccionar un rol diferente de la lista desplegable **rol**.

6. Seleccione **Agregar restricción**.

   Se puede ver la lista de restricciones disponibles por espacio de nombres o por etiqueta de espacio de nombres.

7. En la lista desplegable **Tipo de restricción**, seleccione **espacio de nombres Kubernetes** o **etiqueta de espacio de nombres Kubernetes** dependiendo de cómo estén configurados los espacios de nombres.
8. Seleccione uno o más espacios de nombres o etiquetas de la lista para redactar una restricción que restrinja las funciones a esos espacios de nombres.
9. Seleccione **Confirmar**.

   La página **Editar función** muestra la lista de restricciones que ha elegido para esta función.

10. Seleccione **Confirmar**.

    En la página **cuenta**, puede ver las restricciones de cualquier rol de miembro o de visor en la columna **rol**.

> Si habilita restricciones para una función y selecciona **Confirmar** sin agregar restricciones, se considera que la función tiene restricciones completas (se deniega el acceso a cualquier recurso asignado a espacios de nombres).

Quitar una restricción de espacio de nombres de una función

Un usuario Admin o Owner puede eliminar una restricción de espacio de nombres de una función.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor que tiene restricciones activas.
4. Seleccione **Editar rol**.

   El cuadro de diálogo **Editar función** muestra las restricciones activas para la función.

5. Seleccione **X** a la derecha de la restricción que debe eliminar.
6. Seleccione **Confirmar**.

Si quiere más información

- "Roles de usuario y espacios de nombres"

Administrar la autenticación remota

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra Control.

En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP.

> Astra Control Center usa el atributo de inicio de sesión de usuario, configurado cuando la autenticación remota está habilitada, para buscar usuarios remotos y hacer un seguimiento de ellos. En este campo debe existir un atributo de una dirección de correo electrónico («correo») o nombre principal de usuario («userPrincipalName») para cualquier usuario remoto que desee aparecer en Astra Control Center. Este atributo se utiliza como nombre de usuario en Astra Control Center para la autenticación y en búsquedas de usuarios remotos.

Añada un certificado para la autenticación LDAPS

Agregue el certificado TLS privado del servidor LDAP para que Astra Control Center pueda autenticarse con el servidor LDAP cuando utilice una conexión LDAPS. Sólo tiene que hacerlo una vez o cuando caduque el certificado que ha instalado.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **certificados**.
3. Seleccione **Agregar**.
4. Cargue el `.pem` archiva o pega el contenido del archivo desde el portapapeles.
5. Seleccione la casilla de verificación **Trusted**.
6. Seleccione **Agregar certificado**.

Habilite la autenticación remota

Puede habilitar la autenticación LDAP y configurar la conexión entre Astra Control y el servidor LDAP remoto.

Antes de empezar

Si planea utilizar LDAPS, asegúrese de que el certificado TLS privado del servidor LDAP está instalado en Astra Control Center para que Astra Control Center pueda autenticarse con el servidor LDAP. Consulte Añada un certificado para la autenticación LDAPS si desea obtener instrucciones.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **conectar**.
4. Introduzca la dirección IP del servidor, el puerto y el protocolo de conexión preferido (LDAP o LDAPS).

   > Como práctica recomendada, use LDAPS al conectarse con el servidor LDAP. Debe instalar el certificado TLS privado del servidor LDAP en Astra Control Center antes de conectarse con LDAPS.

5. Introduzca las credenciales de la cuenta de servicio en formato de correo electrónico (administrator@example.com). Astra Control utilizará estas credenciales al conectar con el servidor LDAP.
6. En la sección **Coincidencia de usuario**, haz lo siguiente:
   a. Introduzca el DN base y un filtro de búsqueda de usuario adecuado que se utilizará al recuperar la información de usuario del servidor LDAP.
   b. (Opcional) Si el directorio utiliza el atributo de inicio de sesión del usuario `userPrincipalName` en lugar de `mail`, entre `userPrincipalName` En el atributo correcto en el campo **Atributo de inicio de sesión de usuario**.
7. En la sección **coincidencia de grupo**, introduzca el DN base de búsqueda de grupo y un filtro de búsqueda de grupo personalizado adecuado.

   > Asegúrese de utilizar el nombre completo (DN) de base correcto y un filtro de búsqueda apropiado para **coincidencia de usuario** y **coincidencia de grupo**. El DN base indica a Astra Control en qué nivel del árbol de directorios iniciar la búsqueda, y el filtro de búsqueda limita las partes del árbol de directorios de las búsquedas de Astra Control.

8. Seleccione **Enviar**.

Resultado

El estado del panel **autenticación remota** pasa a **pendiente** y a **conectado** cuando se establece la conexión con el servidor LDAP.

Desactivar la autenticación remota

Puede deshabilitar temporalmente una conexión activa con el servidor LDAP.

> Cuando se deshabilita una conexión a un servidor LDAP, se guardan todas las opciones y se conservan todos los usuarios y grupos remotos que se agregaron a Astra Control desde ese servidor LDAP. Puede volver a conectarse a este servidor LDAP en cualquier momento.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Desactivar**.

Resultado

El estado del panel **autenticación remota** pasa a **Desactivada**. Se conservan todos los ajustes de autenticación remota, usuarios remotos y grupos remotos, y se puede volver a habilitar la conexión en cualquier momento.

Edite la configuración de autenticación remota

Si ha desactivado la conexión al servidor LDAP o el panel **autenticación remota** se encuentra en el estado "error de conexión", puede editar los valores de configuración.

> No puede editar la dirección IP o la dirección URL del servidor LDAP cuando el panel **autenticación remota** está en estado "Desactivada". Necesita hacerlo Desconecte la autenticación remota primero.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Editar**.
4. Realice los cambios necesarios y seleccione **Editar**.

Desconecte la autenticación remota

Puede desconectarse de un servidor LDAP y eliminar los ajustes de configuración de Astra Control.

> Si es un usuario LDAP y se desconecta, la sesión finalizará inmediatamente Cuando se desconecta del servidor LDAP, todas las opciones de configuración de ese servidor LDAP se eliminan de Astra Control, así como todos los usuarios y grupos remotos que se hayan agregado de ese servidor LDAP.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **desconectar**.

Resultado

El estado del panel **autenticación remota** pasa a **desconectado**. La configuración de autenticación remota, los usuarios remotos y los grupos remotos se eliminan de Astra Control.

Administrar grupos y usuarios remotos

Si ha activado la autenticación LDAP en el sistema Astra Control, puede buscar usuarios y grupos LDAP e incluirlos en los usuarios aprobados del sistema.

Agregar un usuario remoto

Los propietarios y administradores de cuentas pueden agregar usuarios remotos a Astra Control. Astra Control Center admite hasta 10.000 usuarios remotos de LDAP.

> Astra Control Center usa el atributo de inicio de sesión de usuario, configurado cuando la autenticación remota está habilitada, para buscar usuarios remotos y hacer un seguimiento de ellos. En este campo debe existir un atributo de una dirección de correo electrónico («correo») o nombre principal de usuario («userPrincipalName») para cualquier usuario remoto que desee aparecer en Astra Control Center. Este atributo se utiliza como nombre de usuario en Astra Control Center para la autenticación y en búsquedas de usuarios remotos.

> No puede agregar un usuario remoto si ya existe en el sistema un usuario local con la misma dirección de correo electrónico (basada en el atributo de correo o nombre principal de usuario). Para agregar el usuario como usuario remoto, elimine primero el usuario local del sistema.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **usuarios remotos**.
4. Seleccione **Agregar**.
5. Opcionalmente, busque un usuario LDAP introduciendo la dirección de correo electrónico del usuario en el campo **Filtrar por correo electrónico**.
6. Seleccione uno o varios usuarios de la lista.
7. Asigne un rol al usuario.

   > Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este usuario y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   > Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo usuario aparece en la lista de usuarios remotos. En esta lista, puede ver restricciones activas en el usuario, así como administrar el usuario desde el menú **acciones**.

Agregar un grupo remoto

Para agregar muchos usuarios remotos a la vez, los propietarios de cuentas y los administradores pueden agregar grupos remotos a Astra Control. Cuando se añade un grupo remoto, todos los usuarios remotos de

ese grupo están disponibles para iniciar sesión en Astra Control y heredarán el mismo rol que el grupo.

Astra Control Center admite hasta 5.000 grupos remotos LDAP.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **grupos remotos**.
4. Seleccione **Agregar**.

   En esta ventana, puede ver una lista de los nombres comunes y nombres distintivos de los grupos LDAP que Astra Control ha recuperado del directorio.

5. Opcionalmente, busque un grupo LDAP introduciendo el nombre común del grupo en el campo **filtro por nombre común**.
6. Seleccione uno o varios grupos de la lista.
7. Asigne un rol a los grupos.

   El rol que seleccione se asigna a todos los usuarios de este grupo. Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este grupo y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   - **Si los recursos a los que se accede pertenecen a clusters que tienen instalado el último Astra Connector**: Cuando se asignan varios roles a un usuario a través de la pertenencia a un grupo LDAP, se combinan las restricciones de los roles. Por ejemplo, si un usuario con un rol de visor local une tres grupos vinculados al rol de miembro, el usuario ahora tendrá acceso al rol de visor a los recursos originales, así como acceso al rol de miembro a los recursos obtenidos mediante la pertenencia al grupo.
   - **Si los recursos a los que se accede pertenecen a clusters que no tienen instalado Astra Connector**: Cuando se asignan varios roles a un usuario a través de la pertenencia a un grupo LDAP, las restricciones del rol más permisivo son las únicas que surten efecto.

9. Seleccione **Agregar**.

Resultado

El nuevo grupo aparece en la lista de grupos remotos. Los usuarios remotos de este grupo no aparecen en la lista de usuarios remotos hasta que cada usuario remoto inicia sesión. En esta lista, puede ver detalles sobre el grupo, así como administrar el grupo desde el menú **acciones**.

Ver y gestionar notificaciones

Astra le notifica cuando las acciones se han completado o han fallado. Por ejemplo, verá una notificación si una copia de seguridad de una aplicación se ha completado correctamente.

Puede gestionar estas notificaciones desde la parte superior derecha de la interfaz:

Pasos

1. Seleccione el número de notificaciones sin leer en la parte superior derecha.
2. Revise las notificaciones y seleccione **Marcar como leído** o **Mostrar todas las notificaciones**.

   Si ha seleccionado **Mostrar todas las notificaciones**, se cargará la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, seleccione **Acción** y seleccione **Marcar como leído**.

Añada y elimine credenciales

Añada y elimine credenciales de proveedores de cloud privado local como ONTAP S3, clústeres de Kubernetes gestionados con OpenShift o clústeres de Kubernetes no gestionados de su cuenta en cualquier momento. Astra Control Center utiliza estas credenciales para descubrir los clústeres y las aplicaciones de Kubernetes en los clústeres, y para aprovisionar recursos en su nombre.

Tenga en cuenta que todos los usuarios de Astra Control Center comparten los mismos conjuntos de credenciales.

Añada credenciales

Puede agregar credenciales a Astra Control Center cuando gestiona los clústeres. Para añadir credenciales al añadir un clúster nuevo, consulte "Añada un clúster de Kubernetes".

> Si creas tu propio archivo kubeconfig, debes definir solo **one** elemento de contexto en él. Consulte "Documentación de Kubernetes" para obtener información sobre la creación de archivos kubeconfig.

Quite las credenciales

Eliminar credenciales de una cuenta en cualquier momento. Solo debe quitar credenciales después de "desgestione todos los clústeres asociados".

> El primer conjunto de credenciales que agregue a Astra Control Center está siempre en uso porque Astra Control Center utiliza las credenciales para autenticarse en el bloque de copia de seguridad. Lo mejor es no eliminar estas credenciales.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **credenciales**.
3. Seleccione el menú Opciones de la columna **Estado** para obtener las credenciales que desea quitar.
4. Seleccione **Quitar**.
5. Escriba la palabra "quitar" para confirmar la eliminación y, a continuación, seleccione **Sí, Eliminar credenciales**.

Resultado

Astra Control Center elimina las credenciales de la cuenta.

Controlar la actividad de la cuenta

Puede ver los detalles de las actividades en su cuenta de Astra Control. Por ejemplo, cuando se invitó a nuevos usuarios, cuando se agregaba un clúster o cuando se tomaba una snapshot. También puede exportar la actividad de su cuenta a un archivo CSV.

Ver toda la actividad de la cuenta en Astra Control

1. Seleccione **actividad**.
2. Utilice los filtros para restringir la lista de actividades o utilice el cuadro de búsqueda para encontrar exactamente lo que busca.
3. Seleccione **Exportar a CSV** para descargar la actividad de su cuenta en un archivo CSV.

Ver la actividad de la cuenta de una aplicación específica

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **actividad**.

Ver la actividad de la cuenta de los clústeres

1. Seleccione **Clusters** y, a continuación, seleccione el nombre del clúster.
2. Seleccione **actividad**.

Tome la acción para resolver eventos que requieren atención

1. Seleccione **actividad**.
2. Seleccione un evento que requiera atención.
3. Seleccione la opción desplegable **tomar acción**.

   En esta lista, puede ver las posibles acciones correctivas que puede adoptar, ver la documentación relacionada con el problema y obtener soporte para ayudar a resolver el problema.

Actualizar una licencia existente

Puede convertir una licencia de evaluación a una licencia completa, o puede actualizar una evaluación existente o una licencia completa con una nueva licencia. Si no tiene una licencia completa, trabaje con su contacto de ventas de NetApp para obtener un número de serie y una licencia completa. Puede utilizar la interfaz de usuario de Astra Control Center o "API de control Astra" para actualizar una licencia existente.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp".
2. Acceda a la página de descarga de Astra Control Center, introduzca el número de serie y descargue el archivo de licencia completo de NetApp (NLF).
3. Inicie sesión en la interfaz de usuario de Astra Control Center.
4. En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.

5. En la página **cuenta** > **Licencia**, seleccione el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta** > **licencias** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

Si quiere más información

- "Licencias de Astra Control Center"

Gestionar bloques

Un proveedor de bloques de almacenamiento de objetos es esencial si desea realizar backups de las aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Con Astra Control Center, agregue un proveedor de almacenes de objetos como destino de copia de seguridad fuera del clúster para sus aplicaciones.

No necesita un bucket si va a clonar su configuración de aplicaciones y almacenamiento persistente en el mismo clúster.

Use uno de los siguientes proveedores de bloques de Amazon simple Storage Service (S3):

- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp
- Microsoft Azure
- Genérico S3

> Amazon Web Services (AWS) y Google Cloud Platform (GCP) utilizan el tipo de bloque Generic S3.

> Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Un cubo puede estar en uno de estos estados:

- Pending: Se ha programado la detección del bloque.
- Disponible: El cucharón está disponible para su uso.
- Eliminado: No se puede acceder al depósito actualmente.

Para obtener instrucciones sobre cómo gestionar los cubos con la API Astra Control, consulte "Información sobre API y automatización de Astra".

Puede realizar estas tareas relacionadas con la gestión de bloques:

- "Añadir un bucket"
- Editar un bloque
- Establecer el bloque predeterminado
- Gire o elimine las credenciales del cucharón
- Retirar un cucharón
- "[Vista PREVIA TÉCNICA Gestione un bloque con un recurso personalizado"]

> Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Editar un bloque

Puede cambiar la información de credenciales de acceso de un bloque y cambiar si un bloque seleccionado es el bloque predeterminado.

> Cuando agregue un bloque, seleccione el proveedor de segmento correcto y proporcione las credenciales correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como tipo y acepta credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los futuros backups de aplicaciones y restauraciones usando este bucket. Consulte "Notas de la versión".

Pasos

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú de la columna **acciones**, seleccione **Editar**.
3. Cambie cualquier información que no sea el tipo de segmento.

   > No puede modificar el tipo de segmento.

4. Seleccione **Actualizar**.

Establecer el bloque predeterminado

Cuando se realiza un clon entre clústeres, Astra Control requiere un bloque predeterminado. Siga estos pasos para establecer un bloque predeterminado para todos los clústeres.

Pasos

1. Vaya a **instancias de cloud**.
2. Seleccione el menú en la columna **acciones** para la instancia de nube de la lista.
3. Seleccione **Editar**.
4. En la lista **bloque**, seleccione el segmento que desea que sea el predeterminado.
5. Seleccione **Guardar**.

Gire o elimine las credenciales del cucharón

Astra Control utiliza las credenciales de bloque para obtener acceso y proporcionar claves secretas para un bloque de S3, de forma que Astra Control Center pueda comunicarse con el cucharón.

Rotar las credenciales del cucharón

Si gira las credenciales, gírelos durante una ventana de mantenimiento cuando no haya copias de seguridad en curso (programadas o bajo demanda).

Pasos para editar y girar credenciales

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú Opciones de la columna **acciones**, seleccione **Editar**.
3. Cree la nueva credencial.
4. Seleccione **Actualizar**.

Quitar las credenciales del bloque

Debe eliminar las credenciales de bloque solo si se han aplicado credenciales nuevas a un bloque o si ya no se utiliza el bloque de forma activa.

> El primer conjunto de credenciales que agregue a Astra Control siempre está en uso porque Astra Control utiliza las credenciales para autenticar el bloque de copia de seguridad. No elimine estas credenciales si el bloque está en uso activo, ya que esto dará lugar a fallos de copia de seguridad y a falta de disponibilidad de copia de seguridad.

> Si elimina las credenciales de bloque activas, consulte "solución de problemas de eliminación de credenciales del bloque".

Para obtener instrucciones sobre cómo eliminar credenciales de S3 mediante la API Astra Control, consulte "Información sobre API y automatización de Astra".

Retirar un cucharón

Puede eliminar un cubo que ya no esté en uso o que no esté sano. Se recomienda hacer esto para mantener la configuración del almacén de objetos sencilla y actualizada.

> - No se puede eliminar un bloque predeterminado. Si desea eliminar ese bloque, seleccione primero otro bloque como predeterminado.
> - No puede quitar un depósito de escritura única y lectura múltiple (WORM) antes de que haya caducado el período de retención del proveedor de cloud del depósito. Los depósitos WORM están marcados con «bloqueados» junto al nombre del bloque.

- No se puede eliminar un bloque predeterminado. Si desea eliminar ese bloque, seleccione primero otro bloque como predeterminado.

Antes de empezar

- Antes de empezar, debe comprobar que no hay copias de seguridad en ejecución o completadas para este bloque.
- Debe comprobar que el bloque no se esté utilizando en ninguna política de protección activa.

Si hay, no podrá continuar.

Pasos

1. En la navegación de la izquierda, seleccione **Cuchos**.

2. En el menú **acciones**, seleccione **Quitar**.

> Astra Control garantiza en primer lugar que no existan normativas de programación utilizando el bloque para copias de seguridad y que no haya copias de seguridad activas en el bloque que va a eliminar.

3. Escriba "eliminar" para confirmar la acción.
4. Seleccione **Sí, retire la cuchara**.

[Vista PREVIA TÉCNICA] Gestione un bloque con un recurso personalizado

Puede añadir un bloque con un recurso personalizado de Astra Control (CR) en el clúster de aplicaciones. Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina. Si utiliza el método de recursos personalizado, la funcionalidad de snapshots de aplicaciones requiere un bloque.

No necesita un bloque de Astra Control si clona la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster.

El recurso personalizado de bloque para Astra Control se conoce como AppVault. Este CR contiene las configuraciones necesarias para que un cucharón se utilice en operaciones de protección.

Antes de empezar

- Asegúrese de tener un bloque al que se puede acceder desde los clústeres que gestiona Astra Control Center.
- Asegúrese de tener credenciales para el bloque.
- Asegúrese de que el cucharón es uno de los siguientes tipos:
  - ONTAP S3 de NetApp
  - StorageGRID S3 de NetApp
  - Microsoft Azure
  - Genérico S3

> Amazon Web Services (AWS) utiliza el tipo de bloque S3 genérico.

> Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `astra-appvault.yaml`).
2. Configure los siguientes atributos:
   - **metadata.name**: *(required)* El nombre del recurso personalizado de AppVault.
   - **Spec.prefix**: *(Opcional)* Una ruta que tiene el prefijo de los nombres de todas las entidades almacenadas en AppVault.

- **spec.providerConfig**: *(required)* Almacena la configuración necesaria para acceder a AppVault utilizando el proveedor especificado.
- **spec.providerCredentials**: *(required)* Almacena referencias a cualquier credencial necesaria para acceder a AppVault utilizando el proveedor especificado.
  - **spec.providerCredentials.valueFromSecret**: *(Opcional)* indica que el valor de la credencial debe provenir de un secreto.
    - **KEY**: *(requerido si se usa valueFromSecret)* La clave válida del secreto para seleccionar.
    - **Name**: *(requerido si se usa valueFromSecret)* Nombre del secreto que contiene el valor de este campo. Debe estar en el mismo espacio de nombres.
- **spec.providerType**: *(required)* Determina qué proporciona la copia de seguridad; por ejemplo, NetApp ONTAP S3 o Microsoft Azure.

  Ejemplo YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Después de rellenar el `astra-appvault.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```

> Cuando se agrega un bloque, Astra Control Marca un bloque con el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado. A medida que se añaden bloques, más adelante se puede decidir a. "establecer otro bloque predeterminado".

Obtenga más información

- "Utilice la API Astra Control"

Gestione el entorno de administración del almacenamiento

Gestionar los clústeres de almacenamiento en Astra Control como back-end de almacenamiento le permite obtener vínculos entre los volúmenes persistentes (VP) y el back-end de almacenamiento, así como mediciones de almacenamiento adicionales.

Para obtener instrucciones sobre cómo gestionar los back-ends de almacenamiento con la API Astra Control, consulte "Información sobre API y automatización de Astra".

Es posible completar las siguientes tareas relacionadas con la gestión de un back-end de almacenamiento:

- "Añada un back-end de almacenamiento"
- Ver detalles del back-end de almacenamiento
- Editar los detalles de autenticación del back-end de almacenamiento
- Gestionar un back-end de almacenamiento detectado
- Desgestione un back-end de almacenamiento
- Quite un back-end de almacenamiento

Ver detalles del back-end de almacenamiento

Puede ver la información del back-end de almacenamiento desde Dashboard o desde la opción Backends.

Consulte los detalles del back-end de almacenamiento en la Consola

Pasos

1. En la navegación de la izquierda, seleccione **Tablero**.
2. Revise el panel del back-end de almacenamiento de Dashboard que muestra el estado:
    - **Insalubre**: El almacenamiento no está en un estado óptimo. Esto puede deberse a un problema de latencia o a que una aplicación está degradada debido a un problema de contenedor, por ejemplo.
    - **Todo sano**: El almacenamiento ha sido gestionado y se encuentra en un estado óptimo.
    - **Descubierto**: El almacenamiento ha sido descubierto, pero no gestionado por Astra Control.

Consulte los detalles del backends de almacenamiento en la opción Backends

Vea información sobre el estado, la capacidad y el rendimiento del back-end (rendimiento de IOPS y/o latencia).

Puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado.

Pasos

1. En el área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.

Editar los detalles de autenticación del back-end de almacenamiento

El Centro de control de Astra ofrece dos modos de autenticación de un back-end de ONTAP.

- **Autenticación basada en credenciales**: El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos requeridos. Debe utilizar un rol de inicio de sesión de seguridad predefinido, como admin, para garantizar la máxima compatibilidad con las versiones de ONTAP.
- **Autenticación basada en certificados**: Astra Control Center también puede comunicarse con un clúster de ONTAP utilizando un certificado instalado en el backend. Debe usar el certificado de cliente, la clave y el certificado de CA de confianza si se utilizan (recomendado).

Puede actualizar los back-ends existentes para pasar de un tipo de autenticación a otro método. Solo se admite un método de autenticación a la vez.

Para obtener más información sobre la activación de la autenticación basada en certificados, consulte "Habilite la autenticación en el back-end de almacenamiento de ONTAP".

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el campo Credenciales, seleccione el icono **Editar**.
4. En la página Editar, seleccione una de las siguientes opciones.
   - **Usar credenciales de administrador**: Ingrese la dirección IP de administración del clúster de ONTAP y las credenciales de administración. Las credenciales deben ser credenciales para todo el clúster.

     > El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, aplique las credenciales de usuario con el rol "admin", que tiene los métodos de acceso `ontapi` y.. `http`, En clústeres ONTAP de origen y destino. Consulte "Gestionar cuentas de usuario en la documentación de ONTAP" si quiere más información.

   - **Utilice un certificado**: Cargue el certificado `.pem` archivo, la clave de certificado `.key` archivo y, opcionalmente, el archivo de entidad de certificación.
5. Seleccione **Guardar**.

Gestionar un back-end de almacenamiento detectado

Puede seleccionar gestionar un back-end de almacenamiento no gestionado pero detectado. Cuando gestionas un back-end de almacenamiento, Astra Control indica si ha caducado un certificado para la autenticación.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione la opción **Descubrido**.
3. Seleccione el back-end de almacenamiento.
4. En el menú Opciones de la columna **Acciones**, selecciona **Administrar**.
5. Realice los cambios.

6. Seleccione **Guardar**.

Desgestione un back-end de almacenamiento

Puede anular la gestión del back-end.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el menú Opciones de la columna **acciones**, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar la acción.
5. Seleccione **Sí, anular la administración del backend de almacenamiento**.

Quite un back-end de almacenamiento

Puede eliminar un back-end de almacenamiento que ya no se esté utilizando. Se recomienda hacer esto para mantener su configuración sencilla y actualizada.

Antes de empezar

- Asegúrese de que el back-end de almacenamiento no esté gestionado.
- Compruebe que el back-end de almacenamiento no tenga ningún volumen asociado con el clúster.

Pasos

1. En la navegación izquierda, seleccione **Backends**.
2. Si se gestiona el back-end, desgestione.
   a. Seleccione **gestionado**.
   b. Seleccione el back-end de almacenamiento.
   c. En la opción **acciones**, seleccione **Unmanage**.
   d. Escriba "desgestionar" para confirmar la acción.
   e. Seleccione **Sí, anular la administración del backend de almacenamiento**.
3. Seleccione **descubierto**.
   a. Seleccione el back-end de almacenamiento.
   b. En la opción **acciones**, seleccione **Quitar**.
   c. Escriba "eliminar" para confirmar la acción.
   d. Seleccione **Sí, quite el backend de almacenamiento**.

Obtenga más información

- "Utilice la API Astra Control"

Supervisar tareas en ejecución

Puede ver detalles sobre las tareas en ejecución y las tareas que se han completado, han fallado o han sido canceladas en las últimas 24 horas en Astra Control. Por ejemplo,

puede ver el estado de una operación de backup, restauración o clonado en ejecución, y ver detalles como un porcentaje completado y el tiempo restante estimado. Es posible ver el estado de una operación programada que se haya ejecutado o una operación que se inició manualmente.

Mientras ve una tarea en ejecución o completada, puede expandir los detalles de la tarea para ver el estado de cada una de las subtareas. La barra de progreso de la tarea es verde para las tareas en curso o completadas, azul para las tareas canceladas y rojo para las tareas que han fallado debido a un error.

> Para las operaciones de clonado, las subtareas consisten en una operación de restauración de Snapshot y de Snapshot.

Para ver más información sobre las tareas fallidas, consulte "Controlar la actividad de la cuenta".

Pasos

1. Mientras se está ejecutando una tarea, vaya a **aplicaciones**.
2. Seleccione el nombre de una aplicación de la lista.
3. En los detalles de la aplicación, seleccione la ficha **tareas**.

   Puede ver detalles de tareas actuales o pasadas y filtrar por estado de tarea.

> Las tareas se conservan en la lista **tareas** durante un máximo de 24 horas. Puede configurar este límite y otros ajustes del monitor de tareas mediante "API de control Astra".

[Tech preview] Gestionar las aplicaciones de Astra Control mediante CRS

Gestione sus aplicaciones de Astra Control usando recursos personalizados de Kubernetes (CR). Están disponibles las siguientes opciones:

- "Defina una aplicación con un recurso personalizado de Kubernetes"
- "Gestione un bloque utilizando un recurso personalizado"

Supervise la infraestructura con conexiones de Prometheus o Fluentd

Puede configurar varios ajustes opcionales para mejorar su experiencia con Astra Control Center. Para supervisar y obtener información sobre toda su infraestructura, configure Prometheus o agregue una conexión de Fluentd.

Si la red en la que ejecuta Astra Control Center requiere un proxy para conectarse a Internet (para cargar paquetes de soporte al sitio de soporte de NetApp), debe configurar un servidor proxy en Centro de control de Astra.

- Conéctese a Prometheus
- Conectar a Fluentd

Añada un servidor proxy para las conexiones al sitio de soporte de NetApp

Si la red en la que ejecuta Astra Control Center requiere un proxy para conectarse a Internet (para cargar paquetes de soporte al sitio de soporte de NetApp), debe configurar un servidor proxy en Centro de control de Astra.

> Astra Control Center no valida los detalles introducidos para su servidor proxy. Asegúrese de introducir los valores correctos.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** en la lista desplegable para agregar un servidor proxy.

4. Introduzca el nombre o la dirección IP del servidor proxy y el número de puerto del proxy.
5. Si su servidor proxy requiere autenticación, active la casilla de verificación e introduzca el nombre de usuario y la contraseña.
6. Seleccione **conectar**.

Resultado

Si se guardó la información de proxy introducida, la sección **proxy HTTP** de la página **cuenta** > **conexiones** indica que está conectada y muestra el nombre del servidor.

Edite la configuración del servidor proxy

Puede editar la configuración del servidor proxy.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** de la lista desplegable para editar la conexión.
4. Edite los detalles del servidor y la información de autenticación.

5. Seleccione **Guardar**.

Desactive la conexión del servidor proxy

Puede desactivar la conexión del servidor proxy. Se le advertirá antes de deshabilitar que se podría producir una interrupción potencial a otras conexiones.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación.

Conéctese a Prometheus

Puede supervisar los datos del Centro de control de Astra con Prometheus. Puede configurar Prometheus para recopilar métricas desde el extremo de métricas del clúster de Kubernetes, y también puede utilizar Prometheus para visualizar los datos de métricas.

Para obtener más información sobre el uso de Prometheus, consulte su documentación en "Introducción a Prometheus".

Lo que necesitará

Asegúrese de que ha descargado e instalado el paquete Prometheus en el clúster Astra Control Center o en un clúster diferente que pueda comunicarse con el clúster Astra Control Center.

Siga las instrucciones de la documentación oficial para "Instale Prometheus".

Prometheus debe poder comunicarse con el clúster Kubernetes de Astra Control Center. Si Prometheus no está instalado en el clúster de Astra Control Center, debe asegurarse de que puede comunicarse con el servicio de métricas que se ejecuta en el clúster de Astra Control Center.

Configure Prometheus

Astra Control Center expone un servicio de mediciones en el puerto TCP 9090 del clúster de Kubernetes. Debe configurar Prometheus para recopilar métricas de este servicio.

Pasos

1. Inicie sesión en el servidor Prometheus.
2. Añada la entrada del clúster en el `prometheus.yml` archivo. En la `yml` file, añada una entrada similar a la siguiente para su clúster en el `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Si establece la `tls_config insecure_skip_verify` para `true`, El protocolo de cifrado TLS no es necesario.

3. Reinicie el servicio Prometheus:

```
sudo systemctl restart prometheus
```

Prometheus de acceso

Acceda a la URL de Prometheus.

Pasos

1. En un explorador, introduzca la URL Prometheus con el puerto 9090.
2. Compruebe su conexión seleccionando **Estado** > **objetivos**.

Ver datos en Prometheus

Puede utilizar Prometheus para ver los datos de Astra Control Center.

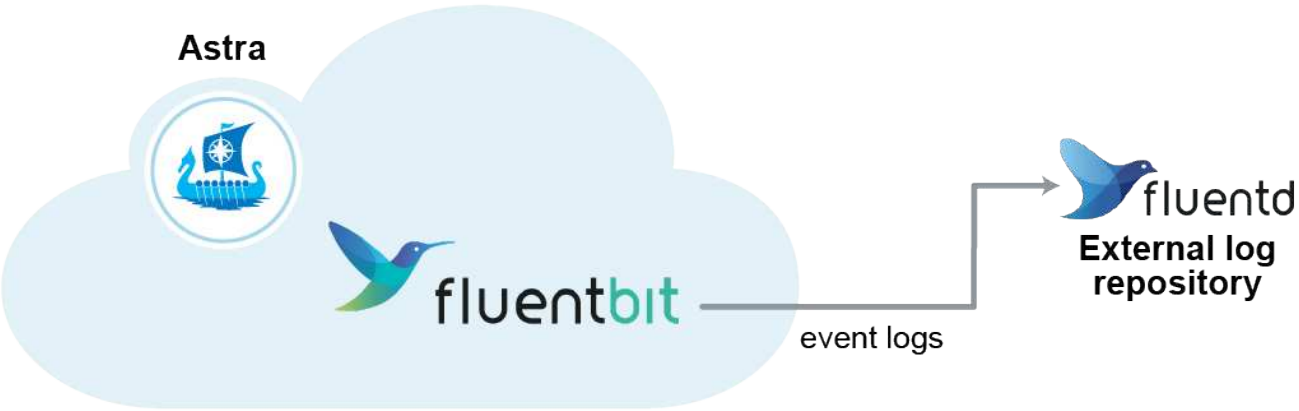
Pasos

1. En un navegador, introduzca la URL de Prometheus.
2. En el menú Prometheus, seleccione **Gráfico**.
3. Para utilizar el Explorador de métricas, seleccione el icono situado junto a **Ejecutar**.
4. Seleccione `scrape_samples_scraped` Y seleccione **Ejecutar**.
5. Para ver el raspado de muestras a lo largo del tiempo, seleccione **Gráfico**.

> Si se recopilaron varios datos de clúster, las métricas de cada clúster aparecen en un color diferente.

Conectar a Fluentd

Puede enviar registros (eventos de Kubernetes) desde un sistema supervisado por Astra Control Center a su extremo de Fluentd. La conexión fluentd está desactivada de forma predeterminada.



Sólo se reenvían a Fluentd los registros de eventos de los clusters gestionados.

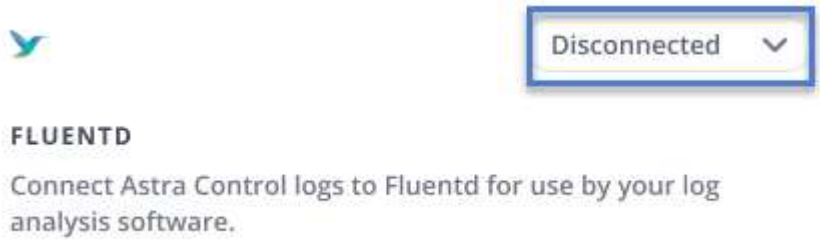
Antes de empezar

- Una cuenta de Astra Control Center con privilegios **admin**/**owner**.
- Astra Control Center se ha instalado y se ejecuta en un clúster de Kubernetes.

Astra Control Center no valida los detalles que introduzca para su servidor Fluentd. Asegúrese de introducir los valores correctos.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** en la lista desplegable en la que aparece **Desconectado** para agregar la conexión.



4. Introduzca la dirección IP del host, el número de puerto y la clave compartida para el servidor Fluentd.
5. Seleccione **conectar**.

Resultado

Si se guardaron los datos introducidos para el servidor Fluentd, la sección **Fluentd** de la página **cuenta** > **conexiones** indica que está conectado. Ahora puede visitar el servidor Fluentd que ha conectado y ver los registros de eventos.

Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.

También puede encontrar la misma información en **cuenta** > **Notificaciones**.

Si tiene problemas con la recopilación de registros, debe iniciar sesión en el nodo de trabajo y asegurarse de que los registros están disponibles en `/var/log/containers/`.

Edite la conexión fluentd

Puede editar la conexión Fluentd a su instancia de Astra Control Center.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** de la lista desplegable para editar la conexión.
4. Cambie la configuración del extremo fluentd.
5. Seleccione **Guardar**.

Desactive la conexión fluentd

Puede desactivar la conexión Fluentd a la instancia de Astra Control Center.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación.

Desgestione aplicaciones y clústeres

Elimine las aplicaciones o clústeres que ya no desee gestionar desde Astra Control Center.

Desgestionar una aplicación

Detenga la gestión de las aplicaciones de las que ya no desee realizar copias de seguridad, copias Snapshot o clones de Astra Control Center.

Al anular la gestión de una aplicación:

- Se eliminarán todos los backups y las snapshots existentes.
- Las aplicaciones y los datos siguen estando disponibles.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione la aplicación.
3. En el menú Opciones de la columna acciones, seleccione **Unmanage**.
4. Revise la información.
5. Escriba "desgestionar" para confirmar.

6. Seleccione **Sí, anular administración de la aplicación**.

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

Deje de gestionar el clúster que ya no desea gestionar desde Astra Control Center.

> Antes de anular la administración del clúster, debe anular la administración de las aplicaciones asociadas al clúster.

Cuando se desadministra un clúster:

- Con esta acción, Astra Control Center no gestiona su clúster. No realiza cambios en la configuración del clúster y no elimina el clúster.
- El aprovisionador Astra Control o Astra Trident no se desinstalarán del clúster. "Descubra cómo desinstalar Astra Trident".

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla de comprobación del clúster que ya no desee administrar.
3. En el menú Opciones de la columna **acciones**, seleccione **Unmanage**.
4. Confirme que desea anular la administración del clúster y, a continuación, seleccione **Sí, anular la administración del clúster**.

Resultado

El estado del clúster cambia a **Extracción**. Después de eso, el clúster se eliminará de la página **Clusters** y ya no será gestionado por Astra Control Center.

> Al anular la gestión del clúster se eliminan todos los recursos que se instalaron para enviar datos de telemetría.

Actualice Astra Control Center

Para actualizar Astra Control Center, descargue las imágenes de instalación y complete estas instrucciones. Puede utilizar este procedimiento para actualizar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Estas instrucciones describen el proceso de actualización de Astra Control Center desde la segunda versión más reciente a esta versión actual. No puede actualizar directamente desde una versión que tenga dos o más versiones de la versión actual. Si la versión de Astra Control Center que tienes instalada es varias versiones detrás de la última versión, es posible que debas realizar actualizaciones en cadena a versiones más recientes hasta que el Astra Control Center instalado esté a solo una versión de la última versión. Para obtener una lista completa de las versiones lanzadas, consulte "notas de la versión".

Antes de empezar

Antes de actualizar, asegúrese de que su entorno siga cumpliendo con el "Requisitos mínimos para la puesta en marcha de Astra Control Center". Su entorno debe tener lo siguiente:

- **Un habilitado "Aprovisionador de Astra Control" Con Astra Trident Running**
  a. Determine la versión de Astra Trident que ejecuta:

```
kubectl get tridentversion -n trident
```

> Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos "instrucciones" Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede realizar una actualización directa a Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.

  b. Comprueba que el aprovisionador de Astra Control se ha realizado "activado". El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. Actualiza tu aprovisionador de Astra Control para que tenga la misma versión que Astra Control Center que actualizas para acceder a la funcionalidad más reciente.

- **Una distribución de Kubernetes soportada**

  Determine la versión de Kubernetes que ejecuta:

```
kubectl get nodes -o wide
```

- **Recursos suficientes del cluster**

  Determine los recursos de clúster disponibles:

```
kubectl describe node <node name>
```

- **Una clase de almacenamiento predeterminada**

  Determine su clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

- **Servicios API saludables y disponibles**

  Asegúrese de que todos los servicios de API se encuentren en buen estado y estén disponibles:

```
kubectl get apiservices
```

- **(Solo registros locales) Un registro local que puedes usar para insertar y cargar imágenes de Astra Control Center**
- **(Solo OpenShift) Operadores de clúster sanos y disponibles**

Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

```
kubectl get clusteroperators
```

También debe tener en cuenta lo siguiente:

> Realice actualizaciones en una ventana de mantenimiento cuando no se estén ejecutando las programaciones, los backups y las snapshots.

- **Acceso al registro de imágenes de NetApp Astra Control**:
  Tiene la opción de obtener imágenes de instalación y mejoras de funcionalidades para Astra Control, como Astra Control Provisioner, desde el registro de imágenes de NetApp.
  a. Registra tu ID de cuenta de Astra Control que tendrás que iniciar sesión en el registro.

     Puedes ver tu ID de cuenta en la interfaz de usuario web de Astra Control Service. Selecciona el icono de la figura en la parte superior derecha de la página, selecciona **Acceso API** y escribe tu ID de cuenta.

  b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.
  c. Inicia sesión en el Registro de Astra Control:

     ```
     docker login cr.astra.netapp.io -u <account-id> -p <api-token>
     ```

- **Istio service mesh despliegues**
  Si instalaste una malla de servicio de Istio durante la instalación de Astra Control Center, esta actualización de Astra Control Center incluirá la malla de servicio de Istio. Si aún no tiene una malla de servicio, sólo puede instalar una durante un "puesta en marcha inicial" De Astra Control Center.

Acerca de esta tarea

El proceso de actualización del Centro de control de Astra le guiará por los siguientes pasos de alto nivel:

> Cierre la sesión de la interfaz de usuario de Astra Control Center antes de comenzar la actualización.

- Descargue y extraiga Astra Control Center
- Complete los pasos adicionales si utiliza un registro local
- Instale el operador actualizado de Astra Control Center
- Actualice Astra Control Center
- Comprobar el estado del sistema

> No elimine el operador Astra Control Center (por ejemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) En cualquier momento durante la actualización o el funcionamiento de Astra Control Center para evitar la eliminación de las dosis.

Descargue y extraiga Astra Control Center

Descargue las imágenes del Centro de control de Astra de una de las siguientes ubicaciones:

- **Registro de imágenes del Servicio de control de Astra**: Utilice esta opción si no utiliza un registro local con las imágenes del Centro de control de Astra o si prefiere este método a la descarga del paquete desde el Sitio de soporte de NetApp.
- **Sitio de soporte de NetApp**: Utilice esta opción si utiliza un registro local con las imágenes del Centro de control de Astra.

Registro de imágenes de Astra Control

1. Inicia sesión en el servicio Astra Control.
2. En el Dashboard, selecciona **Desplegar una instancia autogestionada de Astra Control**.
3. Sigue las instrucciones para iniciar sesión en el registro de imágenes de Astra Control, extraer la imagen de instalación de Astra Control Center y extraer la imagen.

Sitio de soporte de NetApp

1. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete.

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig astra-
   control-center-[version].tar.gz
   ```

   Se mostrará la salida `Verified OK` después de una verificación correcta.

3. Extraiga las imágenes del paquete Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Complete los pasos adicionales si utiliza un registro local

Si tiene pensado enviar el paquete Centro de control de Astra a su registro local, debe usar el complemento de la línea de comandos kubectl de Astra de NetApp.

Elimine el complemento Astra kubectl de NetApp y vuelva a instalarlo

Debes usar la versión más reciente del complemento de línea de comandos kubectl de Astra de NetApp para insertar imágenes en un repositorio local de Docker.

1. Determine si tiene instalado el plugin:

```
kubectl astra
```

2. Realice una de estas acciones:
   - Si el plugin está instalado, el comando debe devolver la ayuda del plugin kubectl y puede eliminar la versión existente de kubectl-astra: `delete /usr/local/bin/kubectl-astra`.
   - Si el comando devuelve un error, el plugin no está instalado y puede continuar con el siguiente paso para instalarlo.
3. Instale el complemento:

   a. Enumere los binarios disponibles del complemento Astra kubectl de NetApp, y anote el nombre del archivo que necesita para el sistema operativo y la arquitectura de CPU:

   > La biblioteca de complementos kubectl forma parte del paquete tar y se extrae en la carpeta `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Mueva el binario correcto a la ruta actual y cambie el nombre a. `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Agregue las imágenes a su registro

1. Si planeas enviar el paquete Astra Control Center a tu registro local, completa la secuencia de pasos apropiada para tu motor de contenedores:

Docker

a. Cambie al directorio raíz del tarball. Debería ver el `acc.manifest.bundle.yaml` archivo y estos directorios:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:

- Sustituya <BUNDLE_FILE> por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
- Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio de Docker; por ejemplo, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
- Reemplace <MY_REGISTRY_USER> por el nombre de usuario.
- Sustituya <MY_REGISTRY_TOKEN> por un token autorizado para el registro.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

Podman

a. Cambie al directorio raíz del tarball. Debería ver este archivo y directorio:

```
acc/
kubectl-astra/
acc.manifest.bundle.yaml
```

b. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

c. Prepare y ejecute una de las siguientes secuencias de comandos personalizadas para la versión de Podman que utilice. Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio que incluye cualquier subdirectorio.

```
<strong>Podman 4</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

La ruta de acceso de imagen que crea el script debe parecerse a la siguiente, dependiendo de la configuración del Registro:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version
```

2. Cambie el directorio:

```
cd manifests
```

Instale el operador actualizado de Astra Control Center

1. (Solo registros locales) Si está utilizando un registro local, complete estos pasos:

   a. Abra el YAML de implementación del operador de Astra Control Center:

   ```
   vim astra_control_center_operator_deploy.yaml
   ```

   Una muestra anotada de AYLMA sigue estos pasos.

   b. Si utiliza un registro que requiere autenticación, reemplace o edite la línea predeterminada de `imagePullSecrets: []` con lo siguiente:

   ```
   imagePullSecrets: [{name: astra-registry-cred}]
   ```

   c. Cambiar `ASTRA_IMAGE_REGISTRY` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

   d. Cambiar `ASTRA_IMAGE_REGISTRY` para la `acc-operator` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

   e. Añada los siguientes valores a la `env` sección:

   ```
   - name: ACCOP_HELM_UPGRADETIMEOUT
     value: 300m
   ```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
```

```
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:24.02.68
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
```

```
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

2. Instale el operador actualizado de Astra Control Center:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Respuesta de ejemplo:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

3. Verifique que los pods se estén ejecutando:

```
kubectl get pods -n netapp-acc-operator
```

Actualice Astra Control Center

1. Edite el recurso personalizado de Astra Control Center (CR):

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

Una muestra anotada de AYLMA sigue estos pasos.

2. Cambie el número de versión de Astra (`astraVersion` dentro de `spec`) de `23.10.0` para `24.02.0`:

No puede actualizar directamente desde una versión que tenga dos o más versiones de la versión actual. Para obtener una lista completa de las versiones lanzadas, consulte "notas de la versión".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Cambie el registro de imágenes:
   - (Sólo registros locales) Si está utilizando un registro local, compruebe que la ruta de acceso del registro de imágenes coincide con la ruta de registro en la que ha insertado las imágenes en un paso anterior. Actualizar `imageRegistry` dentro de `spec` si el registro local ha cambiado desde la última instalación.
   - (Registro de imágenes de Astra Control) Utiliza el registro de imágenes de Astra Control (`cr.astra.netapp.io`) Utilizó para descargar el bundle de Astra Control actualizado.

```
  imageRegistry:
    name: "[cr.astra.netapp.io or your_registry_path]"
```

4. Añada lo siguiente a su `crds` configuración dentro de `spec`:

```
crds:
  shouldUpgrade: true
```

5. Añada las siguientes líneas dentro de `additionalValues` dentro de `spec` En el Centro de control de Astra CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Guarde y salga del editor de archivos. Se aplicarán los cambios y comenzará la actualización.
7. (Opcional) Verifique que los POD terminan y estén disponibles de nuevo:

```
watch kubectl get pods -n [netapp-acc or custom namespace]
```

8. Espere a que las condiciones de estado de Astra Control indiquen que la actualización está completa y lista (`True`):

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Respuesta:

```
NAME    UUID                                      VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f      24.02.0-69
10.111.111.111  True
```

Para supervisar el estado de actualización durante la operación, ejecute el siguiente comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Para inspeccionar los registros del operador de Astra Control Center, ejecute el siguiente comando:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Comprobar el estado del sistema

1. Inicie sesión en Astra Control Center.
2. Compruebe que la versión se ha actualizado. Consulte la página **Soporte** de la interfaz de usuario.
3. Compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.

Actualiza Astra Control Center con OpenShift OperatorHub

Si ha instalado Astra Control Center con su operador certificado por Red Hat, puede actualizar Astra Control Center con un operador actualizado de OperatorHub. Use este procedimiento para actualizar Astra Control Center desde la "Catálogo de Red Hat Ecosystem" O con Red Hat OpenShift Container Platform.

Antes de empezar

- **Cumplir con los requisitos ambientales**: Antes de actualizar, asegúrese de que su entorno aún cumple con el "Requisitos mínimos para la puesta en marcha de Astra Control Center".

- * Asegúrese de que ha habilitado "Aprovisionador de Astra Control" Con Astra Trident Running*
  a. Determine la versión de Astra Trident que ejecuta:

```
kubectl get tridentversion -n trident
```

> Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos "instrucciones" Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede realizar una actualización directa a Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.

  b. Comprueba que el aprovisionador de Astra Control se ha realizado "activado". El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. Actualiza tu aprovisionador de Astra Control para que tenga la misma versión que Astra Control Center que actualizas para acceder a la funcionalidad más reciente.
- * Asegurar operadores de clúster saludables y servicios API*:
  - En el clúster de OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado:

```
oc get clusteroperators
```

  - En el clúster OpenShift, asegúrese de que todos los servicios API se encuentran en buen estado:

```
oc get apiservices
```

- **Permisos OpenShift**: Tiene todos los permisos necesarios y acceso a Red Hat OpenShift Container Platform para realizar los pasos de actualización descritos.
- **(Solo controlador SAN de ONTAP) Habilitar acceso múltiple**: Si está utilizando un controlador SAN de ONTAP, asegúrese de que la opción multivía esté habilitada en todos sus clústeres de Kubernetes.

También debe tener en cuenta lo siguiente:

- **Acceda al registro de imágenes de NetApp Astra Control**:

  Tiene la opción de obtener imágenes de instalación y mejoras de funcionalidades para Astra Control, como Astra Control Provisioner, desde el registro de imágenes de NetApp.

  a. Registra tu ID de cuenta de Astra Control que tendrás que iniciar sesión en el registro.

     Puedes ver tu ID de cuenta en la interfaz de usuario web de Astra Control Service. Selecciona el icono de la figura en la parte superior derecha de la página, selecciona **Acceso API** y escribe tu ID de cuenta.

  b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.

c. Inicia sesión en el Registro de Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

Pasos

- Acceda a la página de instalación del operador
- Desinstale el operador existente
- Instale el operador más reciente
- Actualice Astra Control Center

Acceda a la página de instalación del operador

1. Complete el procedimiento correspondiente para OpenShift Container Platform o Ecosystem Catalog:

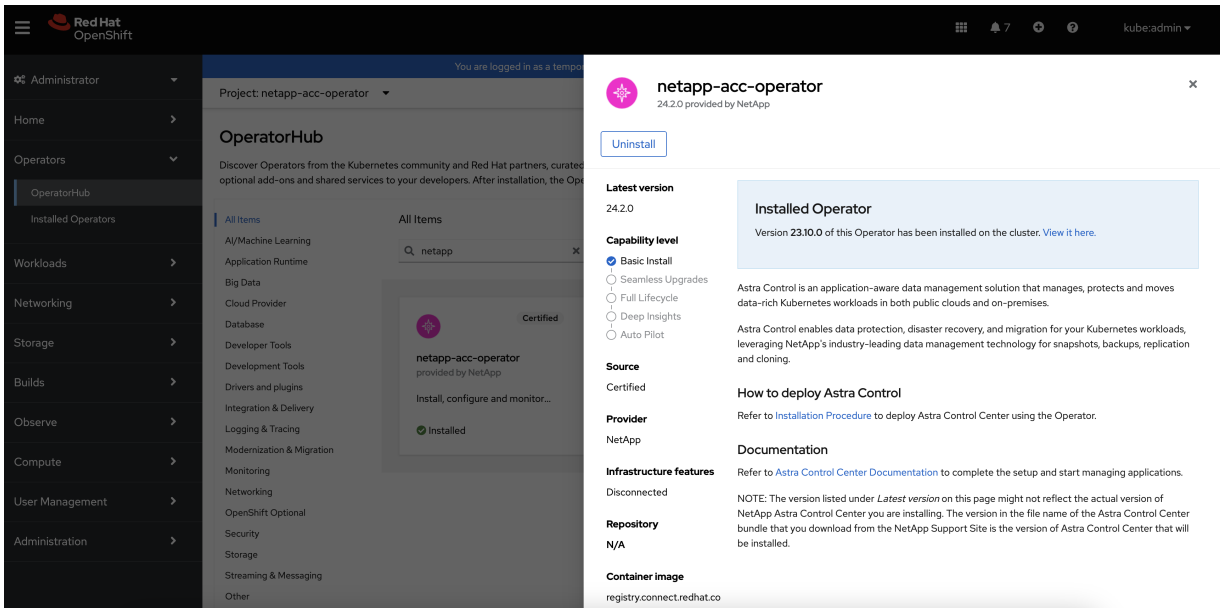
Consola web de Red Hat OpenShift

a. Inicie sesión en la IU de OpenShift Container Platform.

b. En el menú lateral, seleccione **operadores > OperatorHub**.

> Solo se puede actualizar a la versión actual de Astra Control Center con este operador.

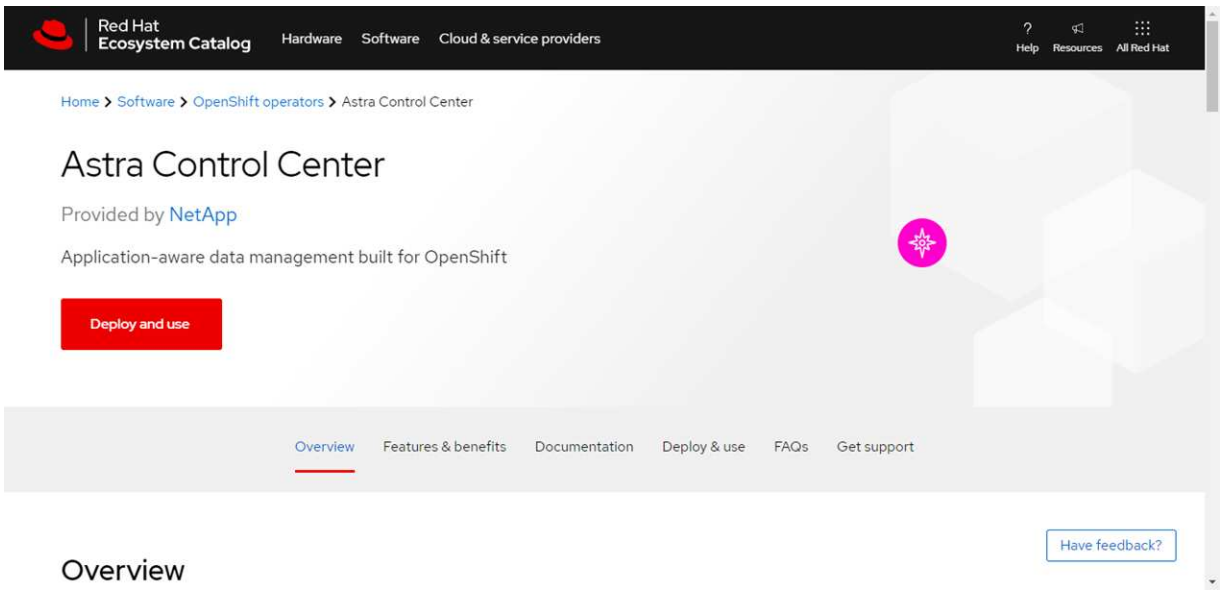
c. Busque `netapp-acc` Y selecciona el operador Centro de control de Astra de NetApp.



Catálogo de Red Hat Ecosystem

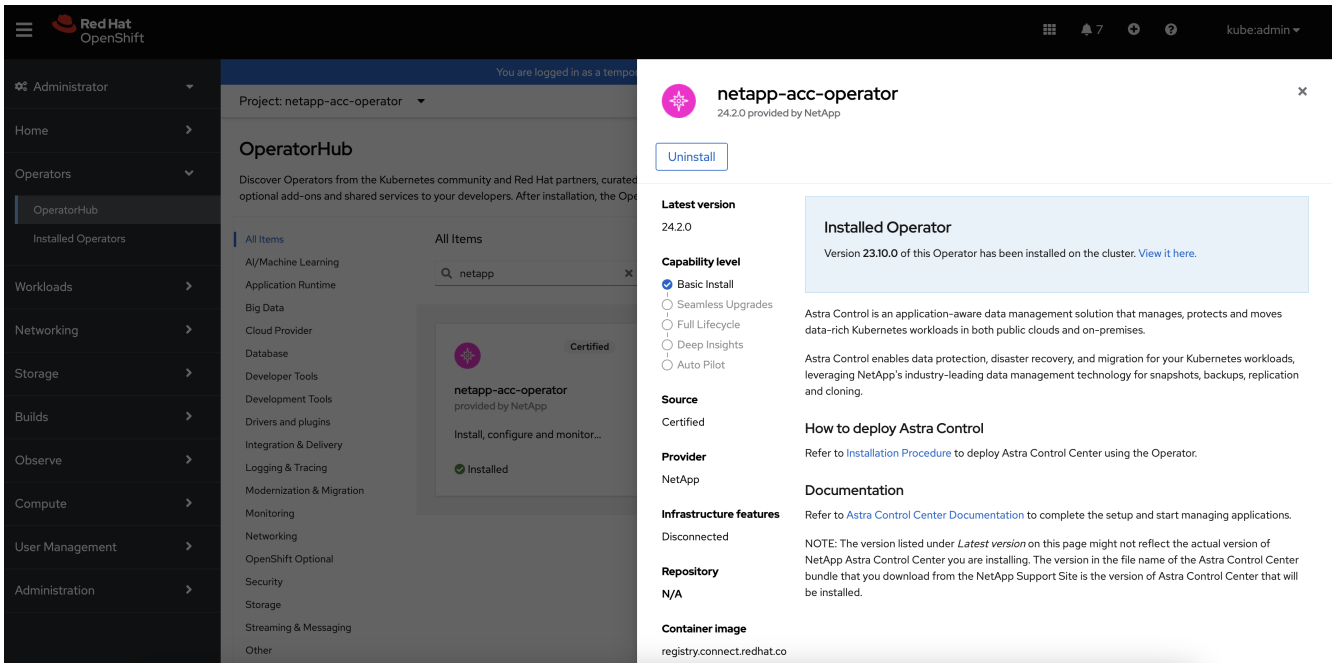
a. Seleccione Astra Control Center de NetApp "operador".

b. Seleccione **Desplegar y usar**.



Desinstale el operador existente

1. En la página **netapp-acc-operator**, seleccione **Uninstall** para eliminar su operador existente.

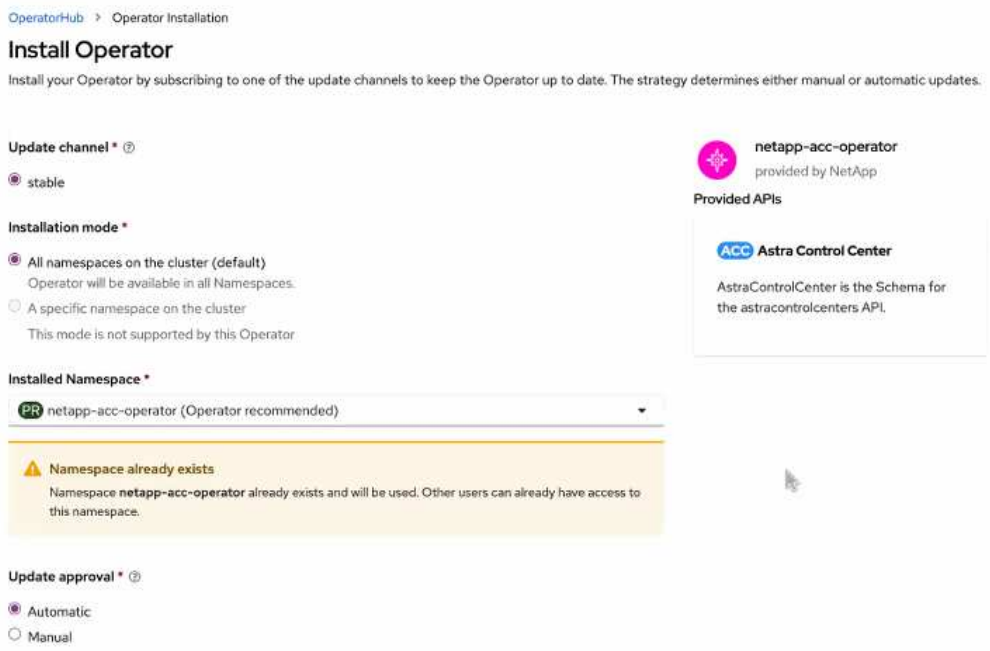


2. Confirme la operación.

> Esta operación elimina el operador netapp-acc-pero conserva el espacio de nombres y los recursos asociados originales, como los secretos.

Instale el operador más reciente

1. Desplácese hasta la `netapp-acc` página del operador de nuevo.
2. Completa la página **Install Operator** e instala el operador más reciente:



> El operador estará disponible en todos los espacios de nombres del clúster.

a. Seleccione el operador `netapp-acc-operator` espacio de nombres (o espacio de nombres personalizado) que permanece de la instalación anterior del operador eliminado.

b. Seleccione una estrategia de aprobación manual o automática.

> Se recomienda la aprobación manual. Solo debe tener una instancia de operador en ejecución por clúster.

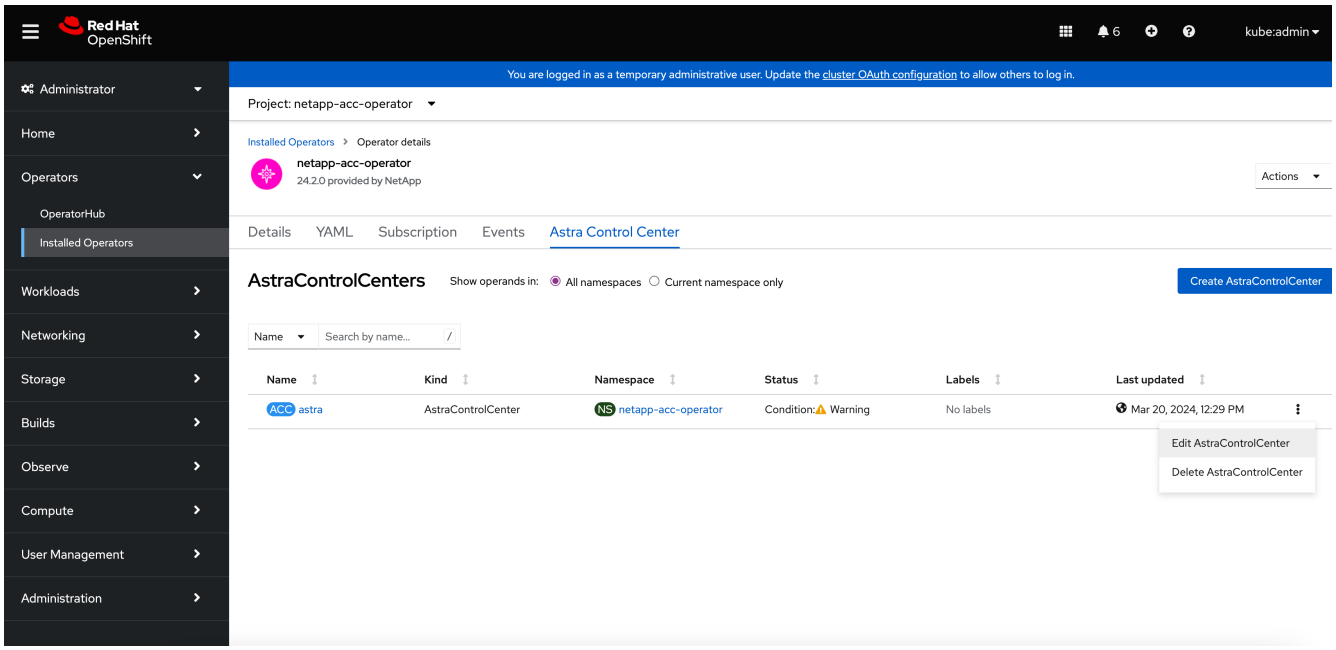
c. Seleccione **instalar**.

> Si ha seleccionado una estrategia de aprobación manual, se le pedirá que apruebe el plan de instalación manual para este operador.

3. Desde la consola, vaya al menú OperatorHub y confirme que el operador se ha instalado correctamente.

Actualice Astra Control Center

1. En la pestaña del operador de Astra Control Center, selecciona el Astra Control Center que queda de la instalación anterior y selecciona **Editar AstraControlCenter**.



2. Actualice el `AstraControlCenter` YAML:
   a. Introduce la versión más reciente de Astra Control Center, por ejemplo, 24.02.0-69.
   b. Pulg `imageRegistry.name`, actualice la ruta del registro de imágenes según sea necesario:
      - Si utiliza la opción de registro de Astra Control, cambie la ruta a. `cr.astra.netapp.io`.
      - Si configuró un registro local, cambie o conserve la ruta de acceso del registro de imágenes local donde insertó las imágenes en un paso anterior.

        No entre `http://` o. `https://` en el campo de dirección.

   c. Actualice el `imageRegistry.secret` según se necesite.

      El proceso de desinstalación del operador no elimina los secretos existentes. Solo necesita actualizar este campo si crea un nuevo secreto con un nombre diferente del secreto existente.

   d. Añada lo siguiente a su `crds` configuración:

```
crds:
  shouldUpgrade: true
```

3. Guarde los cambios.
4. La interfaz de usuario confirma que la actualización se ha realizado correctamente.

Desinstale Astra Control Center

Es posible que necesite eliminar los componentes de Astra Control Center si va a actualizar de una versión de prueba a una versión completa del producto. Para retirar el Centro de control Astra y el operador del Centro de control Astra, ejecute las

instrucciones descritas en este procedimiento en secuencia.

Si tiene algún problema con la desinstalación, consulte Solución de problemas de desinstalación.

Antes de empezar

1. "Anular la gestión de todas las aplicaciones" en los clústeres.
2. "Anule la gestión de todos los clústeres".

Pasos

1. Eliminar Astra Control Center. El comando de ejemplo siguiente se basa en una instalación predeterminada. Modifique el comando si ha realizado configuraciones personalizadas.

   ```
   kubectl delete -f astra_control_center.yaml -n netapp-acc
   ```

   Resultado:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utilice el siguiente comando para eliminar la `netapp-acc` espacio de nombres (o con nombre personalizado):

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Resultado de ejemplo:

   ```
   namespace "netapp-acc" deleted
   ```

3. Utilice el siguiente comando para eliminar los componentes del sistema del operador de Astra Control Center:

   ```
   kubectl delete -f astra_control_center_operator_deploy.yaml
   ```

   Resultado:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

Solución de problemas de desinstalación

Utilice las siguientes soluciones alternativas para solucionar cualquier problema que tenga al desinstalar Astra Control Center.

La desinstalación de Astra Control Center no puede limpiar el módulo de control del operador de supervisión en el clúster gestionado

Si no ha desgestionar los clústeres antes de desinstalar Astra Control Center, puede eliminar manualmente los POD del espacio de nombres para la supervisión de netapp y el espacio de nombres con los siguientes comandos:

Pasos

1. Eliminar `acc-monitoring` agente:

   ```
   kubectl delete agents acc-monitoring -n netapp-monitoring
   ```

   Resultado:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Elimine el espacio de nombres:

   ```
   kubectl delete ns netapp-monitoring
   ```

Resultado:

```
namespace "netapp-monitoring" deleted
```

3. Confirme los recursos eliminados:

```
kubectl get pods -n netapp-monitoring
```

Resultado:

```
No resources found in netapp-monitoring namespace.
```

4. Confirme que se ha eliminado el agente de supervisión:

```
kubectl get crd|grep agent
```

Resultado de la muestra:

```
agents.monitoring.netapp.com                      2021-07-21T06:08:13Z
```

5. Eliminar información de definición de recursos personalizada (CRD):

```
kubectl delete crds agents.monitoring.netapp.com
```

Resultado:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La desinstalación de Astra Control Center no limpia los CRD de Traefik

Puede eliminar manualmente los CRD de Traefik. Los CRD son recursos globales y su eliminación podría afectar a otras aplicaciones del cluster.

Pasos

1. Enumere los CRD de Traefik instalados en el clúster:

```
kubectl get crds |grep -E 'traefik'
```

Respuesta

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Eliminar CRD:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

Obtenga más información

- "Problemas conocidos para la desinstalación"

Use el aprovisionador de Astra Control

Configurar el cifrado de backend de almacenamiento

Con Astra Control Provisioning, puede mejorar la seguridad de acceso a los datos al habilitar el cifrado del tráfico entre su clúster gestionado y el back-end de almacenamiento.

Astra Control Provisioning admite el cifrado Kerberos para dos tipos de back-ends de almacenamiento:

- **ONTAP en las instalaciones** - El aprovisionador de control de Astra admite el cifrado de Kerberos a través de conexiones NFSv3 y NFSv4 desde Red Hat OpenShift y los clústeres de Kubernetes ascendentes a volúmenes ONTAP locales.
- **Azure NetApp Files** - El aprovisionador de control de Astra admite el cifrado de Kerberos a través de conexiones NFSv4,1 desde clústeres de Kubernetes anteriores a volúmenes de Azure NetApp Files.

Puede crear, eliminar, cambiar el tamaño, copiar, clonar, Clone de solo lectura e importe volúmenes que usen cifrado NFS.

Configure el cifrado de Kerberos en tránsito con volúmenes de ONTAP en las instalaciones

Puede habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre su clúster gestionado y un back-end de almacenamiento de ONTAP en las instalaciones.

> El cifrado de Kerberos para el tráfico NFS con back-ends de almacenamiento de ONTAP en las instalaciones solo se admite mediante el `ontap-nas` controlador de almacenamiento.

Antes de empezar

- Asegúrese de que tiene "Habilitado Astra Control Provisioning" en el clúster gestionado.
- Asegúrese de tener acceso al `tridentctl` utilidad.
- Asegúrese de tener acceso de administrador al back-end de almacenamiento de ONTAP.
- Asegúrese de conocer el nombre del volumen o los volúmenes que compartirá desde el back-end de almacenamiento de ONTAP.
- Asegúrese de haber preparado la máquina virtual de almacenamiento de ONTAP para admitir el cifrado de Kerberos para los volúmenes de NFS. Consulte "Habilite Kerberos en una LIF de datos" si desea obtener instrucciones.
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Añada o modifique las políticas de exportación de ONTAP

Tiene que agregar reglas a políticas de exportación de ONTAP existentes o crear nuevas políticas de exportación que sean compatibles con el cifrado de Kerberos para el volumen raíz de la máquina virtual de almacenamiento de ONTAP, así como para cualquier volumen de ONTAP compartido con el clúster de Kubernetes ascendente. Las reglas de políticas de exportación que añada, o las nuevas políticas de exportación que cree, deben admitir los siguientes protocolos de acceso y permisos de acceso:

Protocolos de acceso

Configure la directiva de exportación con los protocolos de acceso NFS, NFSv3 y NFSv4.

Detalles de acceso

Puede configurar una de tres versiones diferentes de cifrado de Kerberos, según las necesidades del volumen:

- **Kerberos 5** - (autenticación y cifrado)
- **Kerberos 5i** - (autenticación y encriptación con protección de identidad)
- **Kerberos 5p** - (autenticación y encriptación con protección de identidad y privacidad)

Configure la regla de política de exportación de ONTAP con los permisos de acceso adecuados. Por ejemplo, si los clústeres montarán los volúmenes NFS con una combinación de Kerberos 5i y cifrado Kerberos 5p, utilice los siguientes ajustes de acceso:

Tipo	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de superusuario
UNIX	Activado	Activado	Activado
Kerberos 5i	Activado	Activado	Activado
Kerberos 5p	Activado	Activado	Activado

Consulte la siguiente documentación para saber cómo crear políticas de exportación de ONTAP y reglas de políticas de exportación:

- "Cree una política de exportación"
- "Añada una regla a una política de exportación"

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Astra Control Provisioner que incluya la funcionalidad de cifrado Kerberos.

Acerca de esta tarea

Al crear un archivo de configuración de backend de almacenamiento que configure el cifrado Kerberos, puede especificar una de las tres versiones diferentes del cifrado Kerberos mediante el `spec.nfsMountOptions` parámetro:

- `spec.nfsMountOptions: sec=krb5` (autenticación y cifrado)
- `spec.nfsMountOptions: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `spec.nfsMountOptions: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si especifica más de un nivel de cifrado de Kerberos en la lista de parámetros, sólo se utilizará la primera opción.

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento utilizando el ejemplo siguiente. Sustituya los valores entre paréntesis <> por información de su entorno:

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con el cifrado de Kerberos.

Acerca de esta tarea

Al crear un objeto de clase de almacenamiento, puede especificar una de las tres versiones diferentes del cifrado de Kerberos mediante el `mountOptions` parámetro:

- `mountOptions: sec=krb5` (autenticación y cifrado)
- `mountOptions: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `mountOptions: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si especifica más de un nivel de cifrado de Kerberos en la lista de parámetros, sólo se utilizará la primera opción. Si el nivel de cifrado especificado en la configuración de backend de almacenamiento es diferente al nivel especificado en el objeto de clase de almacenamiento, el objeto de clase de almacenamiento tiene prioridad.

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Cree la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Asegúrese de que se ha creado la clase de almacenamiento:

```
kubectl get sc ontap-nas-sc
```

Debería ver una salida similar a la siguiente:

```
NAME            PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar

un volumen. Consulte estas instrucciones para "aprovisionamiento de un volumen".

Configure el cifrado de Kerberos en tránsito con volúmenes Azure NetApp Files

Puede habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre su clúster gestionado y un solo back-end de almacenamiento de Azure NetApp Files o un pool virtual de back-ends de almacenamiento de Azure NetApp Files.

Antes de empezar

- Asegúrese de haber habilitado el aprovisionador de Astra Control en el clúster Red Hat OpenShift gestionado. Consulte "Habilita el aprovisionador de Astra Control" si desea obtener instrucciones.
- Asegúrese de tener acceso al `tridentctl` utilidad.
- Asegúrese de haber preparado el back-end de almacenamiento de Azure NetApp Files para cifrado Kerberos siguiendo los requisitos y siguiendo las instrucciones de "Documentación de Azure NetApp Files".
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Azure NetApp Files que incluya la funcionalidad de cifrado de Kerberos.

Acerca de esta tarea

Cuando crea un archivo de configuración de backend de almacenamiento que configura el cifrado Kerberos, puede definirlo para que se aplique en uno de los dos niveles posibles:

- El **storage backend level** usando el `spec.kerberos` campo
- El **nivel de grupo virtual** usando el `spec.storage.kerberos` campo

Cuando se define la configuración en el nivel del pool virtual, el pool se selecciona con la etiqueta de la clase de almacenamiento.

En cualquier nivel, puede especificar una de las tres versiones diferentes del cifrado Kerberos:

- `kerberos: sec=krb5` (autenticación y cifrado)
- `kerberos: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `kerberos: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento mediante uno de los siguientes ejemplos, en función del lugar donde necesite definir el back-end de almacenamiento (nivel de back-end de almacenamiento o nivel de pool virtual). Sustituya los valores entre paréntesis <> por información de su entorno:

Ejemplo de nivel de back-end de almacenamiento

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Ejemplo de nivel de pool virtual

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con el cifrado de Kerberos.

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Cree la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Asegúrese de que se ha creado la clase de almacenamiento:

```
kubectl get sc anf-sc-nfs
```

Debería ver una salida similar a la siguiente:

```
NAME          PROVISIONER              AGE
anf-sc-nfs     csi.trident.netapp.io   15h
```

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Consulte estas instrucciones para "aprovisionamiento de un volumen".

Recuperar datos de volumen mediante una copia Snapshot

Astra Control Provisioning permite restaurar volúmenes rápidamente sin movimiento a partir de una copia Snapshot mediante el `TridentActionSnapshotRestore` (TASR) CR. Esta CR funciona como una acción imprescindible de Kubernetes y no persiste una

vez que finaliza la operación.

Astra Control Provisioner admite la restauración de copias Snapshot en el `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, y. `solidfire-san` de windows

Antes de empezar

Debe tener una snapshot de volumen disponible y la RVP vinculada.

- Compruebe que el estado de la RVP es de enlace.

```
kubectl get pvc
```

- Compruebe que la copia de Snapshot de volumen esté lista para utilizarse.

```
kubectl get vs
```

Pasos

1. Cree el CR de TASR. En este ejemplo se crea una CR para la RVP `pvc1` y copia de snapshot de volumen `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: trident.netapp.io/v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Aplique el CR para restaurar a partir de la instantánea. En este ejemplo se restaura a partir de una copia Snapshot `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Resultados

El aprovisionador de Astra Control restaura los datos a partir de la snapshot. Es posible verificar el estado de restauración de la Snapshot.

```
kubectl get tasr -o yaml

apiVersion: trident.netapp.io/v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- En la mayoría de los casos, el aprovisionador de Astra Control no volverá a intentar automáticamente la operación en caso de fallo. Deberá realizar la operación de nuevo.
- Es posible que el administrador deba conceder permiso al usuario de Kubernetes sin acceso de administrador para crear una CR TASR en su espacio de nombres de la aplicación.

Replicar volúmenes mediante SnapMirror

Con Astra Control Provisioning, puede crear relaciones de mirroring entre un volumen de origen en un clúster y el volumen de destino en el clúster con relación de paridad para replicar datos para la recuperación de desastres. Puede utilizar una definición de recursos personalizados (CRD) con nombre para realizar las siguientes operaciones:

- Crear relaciones de mirroring entre volúmenes (RVP)
- Elimine las relaciones de reflejo entre volúmenes
- Rompa las relaciones de reflejo
- Promocionar el volumen secundario durante condiciones de desastre (conmutaciones al respaldo).
- Realice una transición de las aplicaciones sin pérdidas de un clúster a otro (durante las migraciones y las conmutaciones al respaldo planificadas).

Requisitos previos de replicación

Asegúrese de que se cumplen los siguientes requisitos previos antes de comenzar:

Clústeres ONTAP

- **Astra Control Provisionador**: Astra Control Provisionador versión 23,10 o posterior o A "Astra Trident compatible" Debe existir en los clústeres de Kubernetes de origen y de destino que utilicen ONTAP como back-end.
- **Licencias**: Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP" si quiere más información.

Interconexión

- **Cluster y SVM**: Los back-ends de almacenamiento ONTAP deben ser peered. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM" si quiere más información.

> Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **Astra Control Provisionador y SVM**: Las SVM remotas entre iguales deben estar disponibles para Astra Control Provisionador en el clúster de destino.

Controladores compatibles

- La replicación de volúmenes es compatible con los controladores ontap-nas y ontap-san.

Cree una RVP reflejada

Siga estos pasos y utilice los ejemplos de CRD para crear una relación de reflejo entre los volúmenes primario y secundario.

Pasos

1. Realice los siguientes pasos en el clúster de Kubernetes principal:
   a. Cree un objeto StorageClass con `trident.netapp.io/replication: true` parámetro.

      Ejemplo

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        backendType: "ontap-nas"
        fsType: "nfs"
        trident.netapp.io/replication: "true"
      ```

   b. Cree una RVP con el tipo de almacenamiento creado anteriormente.

Ejemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Cree un CR de MirrorRelationship con información local.

Ejemplo

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provisioner obtiene la información interna del volumen y el estado actual de protección de datos (DP) del volumen y, a continuación, rellena el campo de estado del MirrorRelationship.

d. Obtenga el TridentMirrorRelationship CR para obtener el nombre interno y SVM de la PVC.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Realice los siguientes pasos en el clúster de Kubernetes secundario:
   a. Cree una StorageClass con el parámetro trident.netapp.io/replication: true.

      Ejemplo

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Cree un CR de MirrorRelationship con información de destino y origen.

      Ejemplo

      ```
      kind: TridentMirrorRelationship
      apiVersion: trident.netapp.io/v1
      metadata:
        name: csi-nas
      spec:
        state: established
        volumeMappings:
        - localPVCName: csi-nas
          remoteVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      ```

El aprovisionador de control de Astra creará una relación de SnapMirror con el nombre de la política de relaciones configurada (o predeterminado para ONTAP) e inicializarla.

c. Crear una RVP con StorageClass creado anteriormente para que actúe como secundario (destino de SnapMirror).

Ejemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

El aprovisionador de control de Astra comprobará el CRD de TridentMirrorRelationship y no podrá crear el volumen si la relación no existe. Si existe la relación, el aprovisionador de Astra Control se asegurará de que el nuevo volumen de FlexVol se coloque en una SVM vinculada con la SVM remota definida en MirrorRelationship.

Estados de replicación de volúmenes

Una relación de mirroring de Trident (TMR) es un CRD que representa un extremo de una relación de replicación entre RVP. El TMR de destino tiene un estado, que le dice a Astra Control Provisioner cuál es el estado deseado. El TMR de destino tiene los siguientes estados:

- **Establecido**: El PVC local es el volumen de destino de una relación de espejo, y esta es una nueva relación.
- **Promocionado**: El PVC local es ReadWrite y montable, sin relación de espejo actualmente en vigor.
- **Reestablecido**: El PVC local es el volumen de destino de una relación de espejo y también estaba anteriormente en esa relación de espejo.
  - El estado reestablecido se debe usar si el volumen de destino alguna vez mantuvo una relación con el volumen de origen debido a que sobrescribe el contenido del volumen de destino.
  - El estado reestablecido generará un error si el volumen no mantuvo una relación anteriormente con el origen.

Promocione la RVP secundaria durante una conmutación al respaldo no planificada

Realice el siguiente paso en el clúster de Kubernetes secundario:

- Actualice el campo *spec.state* de TridentMirrorRelationship a. `promoted`.

Promocione la RVP secundaria durante una conmutación al respaldo planificada

Durante una conmutación al respaldo planificada (migración), realice los siguientes pasos para promocionar la RVP secundaria:

Pasos

1. En el clúster de Kubernetes principal, cree una snapshot de la RVP y espere hasta que se cree la snapshot.
2. En el clúster de Kubernetes principal, cree SnapshotInfo CR para obtener información interna.

   Ejemplo

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. En el clúster de Kubernetes secundario, actualice el campo *spec.state* de *TridentMirrorRelationship* CR a *promoted* y *spec.promotedSnapshotHandle* para que sea InternalName de la snapshot.
4. En un clúster de Kubernetes secundario, confirme el estado (campo status.state) de TridentMirrorRelationship a Promoted.

Restaure una relación de mirroring después de una conmutación al nodo de respaldo

Antes de restaurar una relación de reflejo, elija el lado que desea realizar como el nuevo primario.

Pasos

1. En el clúster de Kubernetes secundario, compruebe que se actualicen los valores del campo *spec.remoteVolumeHandle* del TridentMirrorRelationship.
2. En el clúster de Kubernetes secundario, actualice el campo *spec.mirror* de TridentMirrorRelationship a `reestablished`.

Operaciones adicionales

Astra Control Provisioning admite las siguientes operaciones en los volúmenes primarios y secundarios:

Replica la PVC primaria a una nueva PVC secundaria

Asegúrese de que ya tiene un PVC primario y un PVC secundario.

Pasos

1. Elimine los CRD de PersistentVolumeClaim y TridentMirrorRelationship del clúster secundario (destino) establecido.
2. Elimine el CRD de TridentMirrorRelationship del clúster primario (origen).

3. Cree un nuevo CRD de TridentMirrorRelationship en el clúster primario (de origen) para la nueva PVC secundaria (de destino) que desea establecer.

Cambie el tamaño de una RVP reflejada, primaria o secundaria

El PVC se puede cambiar de tamaño como normal, ONTAP expandirá automáticamente cualquier flevxols de destino si la cantidad de datos excede el tamaño actual.

Elimine la replicación de una RVP

Para eliminar la replicación, realice una de las siguientes operaciones en el volumen secundario actual:

- Elimine el MirrorRelationship en la RVP secundaria. Esto interrumpe la relación de replicación.
- O bien, actualice el campo spec.state a *Promoted*.

Eliminar una RVP (que se había duplicado previamente)

Astra Control Provisioning comprueba si existen las RVP replicadas y libera la relación de replicación antes de intentar eliminar el volumen.

Eliminar un TMR

Al eliminar un TMR en un lado de una relación reflejada, el TMR restante pasará al estado *Promoted* antes de que Astra Control Provisioner complete la eliminación. Si el TMR seleccionado para eliminación ya se encuentra en el estado *Promoted*, no existe ninguna relación de reflejo y el TMR se eliminará y el aprovisionador de Astra Control promoverá la RVP local a *ReadWrite*. Esta eliminación libera los metadatos de SnapMirror del volumen local en ONTAP. Si este volumen se utiliza en una relación de reflejo en el futuro, debe utilizar un nuevo TMR con un estado de replicación de volumen *established* al crear la nueva relación de reflejo.

Actualice las relaciones de reflejo cuando el ONTAP esté en línea

Las relaciones de reflejos se pueden actualizar en cualquier momento una vez establecidas. Puede utilizar el `state: promoted` o. `state: reestablished` campos para actualizar las relaciones.
Al promocionar un volumen de destino a un volumen de ReadWrite normal, se puede usar *promotedSnapshotHandle* para especificar una snapshot específica a la que restaurar el volumen actual.

Actualice las relaciones de reflejo cuando la ONTAP esté sin conexión

Puede utilizar un CRD para realizar una actualización de SnapMirror sin Astra Control para tener conectividad directa con el clúster de ONTAP. Consulte el siguiente formato de ejemplo de TridentActionMirrorUpdate:

Ejemplo

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Refleja el estado del CRD TridentActionMirrorUpdate. Puede tomar un valor de *succeeded*, *in progress* o *failed*.

Automatice con la API REST de Astra Control

Automatización mediante la API REST de Astra Control

Astra Control dispone de una API REST que le permite acceder directamente a la funcionalidad Astra Control mediante un lenguaje de programación o una utilidad como Curl. También puede gestionar las puestas en marcha de Astra Control con Ansible y otras tecnologías de automatización.

Para configurar y gestionar sus aplicaciones Kubernetes, puede utilizar la interfaz de usuario de Astra Control Center o la API de Astra Control.

Para obtener más información, visite la "Documentos de automatización de Astra".

Conocimiento y apoyo

Resolución de problemas

Aprenda a solucionar algunos problemas comunes que puede encontrar.

"Base de conocimientos de NetApp para Astra Control"

Obtenga más información

- "Cómo cargar un archivo en NetApp (se requiere inicio de sesión)"
- "Cómo cargar manualmente un archivo en NetApp (se requiere inicio de sesión)"

Obtenga ayuda

NetApp ofrece compatibilidad con Astra Control de varias formas. Hay disponibles amplias opciones de soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un canal Discord. Su cuenta de Astra Control incluye soporte técnico remoto mediante emisión de boletos web.

> Si dispone de una licencia de evaluación para Astra Control Center, puede obtener asistencia técnica. Sin embargo, la creación de casos a través del sitio de soporte de NetApp (NSS) no está disponible. Puede ponerse en contacto con el servicio de asistencia técnica a través de la opción de comentarios o utilizar el canal Discord para el autoservicio.

Usted debe primero "Active el soporte para su número de serie de NetApp" para poder utilizar estas opciones de soporte no autoservicio. Se necesita una cuenta de SSO del sitio de soporte de NetApp (NSS) para el chat y los efectos de la emisión de boletos web junto con la gestión de casos.

Opciones de autosoporte

Puede acceder a las opciones de soporte desde la interfaz de usuario del Centro de control de Astra seleccionando la pestaña **Soporte** del menú principal.

Estas opciones están disponibles de forma gratuita las 24 horas del día, los 7 días de la semana

- "**Utilice la base de conocimientos** (se requiere login)": Buscar artículos, preguntas frecuentes o romper información relacionada con Astra Control.
- **Consulte la documentación del producto**: Este es el sitio de documentos que está viendo actualmente.
- "**Obtenga ayuda a través de Discord**": Ve a Astra en la categoría Pub para conectarte con colegas y expertos.
- **Crear un caso de soporte**: Generar paquetes de soporte que se proporcionarán al soporte de NetApp para la solución de problemas.
- **Danos tu opinión sobre Astra Control**: Envía un correo electrónico a astra.feedback@netapp.com para que sepamos tus pensamientos, ideas o preocupaciones.

Habilite la carga diaria programada del bundle de soporte al soporte de NetApp

Durante la instalación de Astra Control Center, si lo especifica `enrolled: true` para `autoSupport` En el archivo Astra Control Center Custom Resource (CR) (`astra_control_center.yaml`), los paquetes de soporte diario se cargan automáticamente en el "Sitio de soporte de NetApp".

Genere el paquete de soporte para suministrar soporte de NetApp

Astra Control Center permite al usuario administrador generar paquetes, que incluyen información útil para el soporte de NetApp, incluidos registros, eventos para todos los componentes de la implementación, métricas e información de topología sobre los clústeres y las aplicaciones que se están gestionando. Si está conectado a Internet, puede cargar los paquetes de soporte en el sitio de soporte de NetApp (NSS) directamente desde la interfaz de usuario de Astra Control Center.

> El tiempo que tarda Astra Control Center en generar el paquete depende del tamaño de la instalación de Astra Control Center, así como de los parámetros del paquete de soporte solicitado. La duración especificada al solicitar un bundle de soporte determina el tiempo que se tarda en generar el paquete (por ejemplo, un periodo de tiempo más corto provoca una generación más rápida de los paquetes).

Antes de empezar

Determine si se necesitará una conexión proxy para cargar paquetes en NSS. Si se necesita una conexión proxy, compruebe que Astra Control Center se ha configurado para utilizar un servidor proxy.

1. Seleccione **Cuentas** > **conexiones**.
2. Compruebe la configuración del proxy en **Ajustes de conexión**.

Pasos

1. Cree un caso en el portal NSS utilizando el número de serie de la licencia que aparece en la página **Soporte** de la interfaz de usuario de Astra Control Center.
2. Realice los siguientes pasos para generar el paquete de soporte con la interfaz de usuario de Astra Control Center:

   a. En la página **Soporte**, en el icono paquete de soporte, seleccione **generar**.

   b. En la ventana **generar un paquete de soporte**, seleccione el periodo de tiempo.

      Puede elegir entre períodos de tiempo rápidos o personalizados.

      > Puede elegir un intervalo de fechas personalizado, así como especificar un período de tiempo personalizado durante el intervalo de fechas.

   c. Después de realizar las selecciones, seleccione **Confirmar**.

   d. Active la casilla de comprobación **Upload el paquete en el sitio de soporte de NetApp cuando se genere**.

   e. Seleccione **generar paquete**.

      Cuando el paquete de soporte esté listo, aparecerá una notificación en la página **Cuentas** > **notificación** del área Alertas, en la página **actividad** y también en la lista de notificaciones (accesible seleccionando el icono en la parte superior derecha de la interfaz de usuario).

Si la generación ha fallado, aparecerá un icono en la página generar paquete. Seleccione el icono para ver

el mensaje.

> El icono de notificaciones en el lado superior derecho de la interfaz de usuario proporciona información sobre los eventos relacionados con el paquete de soporte, como cuando se crea correctamente el paquete, cuando se produce un error en la creación del paquete, cuando no se pudo cargar el paquete, cuando no se pudo descargar el paquete, etc.

Si tiene una instalación con problemas de aire

Si tiene una instalación con problemas de aire, realice los siguientes pasos después de que se genere el paquete de soporte. Cuando el paquete está disponible para descarga, el icono Descargar aparece junto a **generar** en la sección **Paquetes de soporte** de la página **Soporte**.

Pasos

1. Seleccione el icono Descargar para descargar el paquete localmente.
2. Cargue manualmente el paquete en NSS.

   Puede utilizar uno de los siguientes métodos para ello:

   - Uso "Carga de archivos autenticados de NetApp (se requiere inicio de sesión)".
   - Adjunte el paquete al caso directamente en NSS.
   - Utilice Active IQ de NetApp.

Obtenga más información

- "Cómo cargar un archivo en NetApp (se requiere inicio de sesión)"
- "Cómo cargar manualmente un archivo en NetApp (se requiere inicio de sesión)"

Versiones anteriores de la documentación de Astra Control Center

Hay documentación disponible sobre versiones anteriores.

- "Documentación de Astra Control Center 23,10"
- "Documentación de Astra Control Center 23,07"
- "Documentación de Astra Control Center 23,04"
- "Documentación de Astra Control Center 22.11"
- "Documentación de Astra Control Center 22.08"
- "Documentación de Astra Control Center 22.04"
- "Documentación de Astra Control Center 21.12"
- "Documentación de Astra Control Center 21.08"

Preguntas frecuentes

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Descripción general

En las siguientes secciones se ofrecen respuestas a algunas preguntas adicionales que puede encontrar a medida que utiliza Astra Control Center. Para obtener más aclaraciones, por favor, diríjase a astra.feedback@netapp.com

Acceso a Astra Control Center

¿Qué es la URL de Astra Control?

Astra Control Center utiliza autenticación local y una dirección URL específica para cada entorno.

Para la URL, en un explorador, introduzca el nombre de dominio completo (FQDN) que haya establecido en el campo spec.astraAddress del archivo astra_control_Center.yaml custom resource (CR) cuando instaló Astra Control Center. El mensaje de correo electrónico es el valor que se ha establecido en el campo SPEC.Email del astra_control_Center.ylma CR.

Licencia

Estoy usando una licencia de evaluación. ¿Cómo cambio a la licencia completa?

Puede cambiar fácilmente a una licencia completa si obtiene el archivo de licencia de NetApp (NLF) de NetApp.

- Pasos*
  1. En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
  2. En la descripción general de la licencia, a la derecha de la información de la licencia, seleccione el menú Opciones.
  3. Selecciona **Reemplazar**.
  4. Busque el archivo de licencia que ha descargado y seleccione **Agregar**.

Estoy usando una licencia de evaluación. ¿Puedo seguir administrando aplicaciones?

Sí, puede probar la funcionalidad de administración de aplicaciones con una licencia de evaluación (incluida la licencia de evaluación integrada que se instala de forma predeterminada). No hay diferencia en las capacidades o características entre una licencia de evaluación y una licencia completa; la licencia de evaluación simplemente tiene una vida útil más corta. Consulte "Licencia" si quiere más información.

Registrar clústeres de Kubernetes

Necesito añadir nodos de trabajador a mi clúster de Kubernetes después de agregarlos a Astra Control. ¿Qué debo hacer?

Los nodos de trabajo nuevos se pueden agregar a los pools existentes. Estos serán descubiertos automáticamente por Astra Control. Si los nuevos nodos no están visibles en Astra Control, compruebe si los nuevos nodos de trabajo están ejecutando el tipo de imagen admitido. También puede verificar el estado de los nuevos nodos de trabajo mediante el `kubectl get nodes` comando.

¿Cómo puedo anular correctamente un clúster?

1. "Desgestione las aplicaciones desde Astra Control".
2. "Desgestione el clúster desde Astra Control".

¿Qué ocurre con mis aplicaciones y datos después de quitar el clúster de Kubernetes de Astra Control?

La eliminación de un clúster de Astra Control no realizará ningún cambio en la configuración del clúster (aplicaciones y almacenamiento persistente). Las instantáneas de Astra Control o las copias de seguridad tomadas de las aplicaciones en ese clúster no estarán disponibles para restaurar. Los backups de almacenamiento persistentes creados por Astra Control permanecen en Astra Control, pero no están disponibles para la restauración.

> Quite siempre un clúster de Astra Control antes de eliminarlo mediante cualquier otro método. La eliminación de un clúster con otra herramienta mientras Astra Control sigue gestionando puede causar problemas para su cuenta Astra Control.

¿Astra Control Provisioner (o Astra Trident) se desinstala automáticamente de un clúster cuando cancelo este proceso?

Cuando se desgestiona un clúster de Astra Control Center, el aprovisionador de Astra Control o Astra Trident no se desinstalan automáticamente del clúster. Para desinstalar Astra Control Provisioner y sus componentes o Astra Trident, deberá hacerlo "Siga estos pasos para desinstalar la instancia de Astra Trident que contiene el servicio de aprovisionamiento Astra Control".

Gestionar aplicaciones

¿Puede Astra Control implementar una aplicación?

Astra Control no implementa aplicaciones. Las aplicaciones deben implementarse fuera de Astra Control.

¿Qué sucede con las aplicaciones después de dejar de gestionarlas desde Astra Control?

Se eliminarán todos los backups o las snapshots existentes. Las aplicaciones y los datos siguen estando disponibles. Las operaciones de administración de datos no estarán disponibles para aplicaciones no administradas o para cualquier copia de seguridad o copia Snapshot que pertenezcan a él.

¿Puede Astra Control gestionar una aplicación que se encuentre en almacenamiento de otros proveedores?

No Aunque Astra Control puede detectar aplicaciones que usan almacenamiento de otros proveedores, no puede gestionar una aplicación que use almacenamiento de otros proveedores.

¿Debería gestionar el propio Astra Control?

Astra Control Center no se muestra de forma predeterminada como una aplicación que puedes gestionar, pero sí que puedes "realizar una copia de seguridad y restaurar" Una instancia de Astra Control Center mediante otra instancia de Astra Control Center.

¿Los pods no saludables afectan a la gestión de la aplicación?

No, el estado de los pods no afecta a la gestión de la aplicación.

Operaciones de gestión de datos

Mi aplicación utiliza varios VP. ¿Tomará Astra Control snapshots y backups de estos VP?

Sí. Una operación de instantánea en una aplicación de Astra Control incluye una instantánea de todos los VP vinculados a las RVP de la aplicación.

¿Puedo gestionar snapshots tomadas por Astra Control directamente mediante otra interfaz u otro almacenamiento de objetos?

No Las copias Snapshot y los backups que realice Astra Control solo pueden gestionarse con Astra Control.

Aprovisionador de Astra Control

¿En qué se diferencian las funciones de aprovisionamiento de almacenamiento de Astra Control Provisioner de las de Astra Trident?

Astra Control Provisioning, como parte de Astra Control, es compatible con un superconjunto de funciones de aprovisionamiento de almacenamiento que no están disponibles en Astra Trident de código abierto. Estas funciones se suman a todas las funciones que están disponibles en Trident de código abierto.

¿El aprovisionador de Astra Control está reemplazando a Astra Trident?

Astra Control Provisioning ha reemplazado a Astra Trident como aprovisionador de almacenamiento y orquestador en la arquitectura de Astra Control. Los usuarios de Astra Control deberían hacerlo "Habilita el aprovisionador de Astra Control" Para utilizar Astra Control. Astra Trident seguirá siendo compatible en esta versión, pero no será compatible en futuras versiones. Astra Trident seguirá siendo de código abierto y se lanzará, mantendrá, admitirá y actualizará con las nuevas CSI y otras funciones de NetApp. Sin embargo, solo el aprovisionador de Astra Control que contenga la funcionalidad CSI de Astra Trident junto con funcionalidades ampliadas de gestión del almacenamiento pueden usarse con próximas versiones de Astra Control.

¿Tengo que pagar por Astra Trident?

No Astra Trident seguirá siendo de código abierto y puede descargarse gratuitamente. El uso de la funcionalidad de aprovisionamiento de Astra Control ahora requiere una licencia de Astra Control.

¿Puedo usar las funciones de gestión y aprovisionamiento del almacenamiento en Astra Control sin tener que instalar y utilizar todo Astra Control?

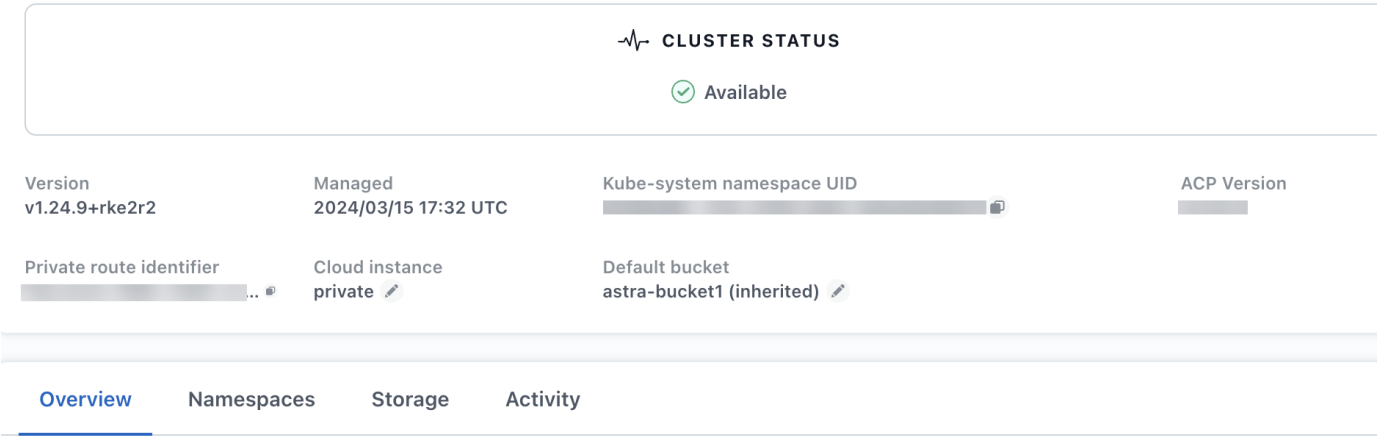
Sí, puede actualizar a Astra Control Provisioner y utilizar su funcionalidad aunque no quiera consumir el conjunto de funciones completo de la funcionalidad de gestión de datos de Astra Control.

¿Cómo puedo realizar la transición de ser un usuario existente de Astra Trident a Astra Control para usar la funcionalidad de aprovisionamiento y gestión del almacenamiento avanzada?

Si ya eres un usuario de Astra Trident (esto incluye usuarios de Astra Trident en la nube pública), primero debes adquirir una licencia de Astra Control. Cuando lo haga, podrá descargar el bundle de aprovisionamiento de Astra Control, actualizar Astra Trident y "Habilita la funcionalidad Astra Control Provisioner".

¿Cómo sé si el aprovisionador de Astra Control ha reemplazado a Astra Trident en mi clúster?

Después de instalar el aprovisionador de Astra Control, el clúster de host de la interfaz de usuario de Astra Control mostrará un `ACP version` en lugar de `Trident version` campo y núm. de versión instalada actual.



Si no tiene acceso a la interfaz de usuario, puede confirmar que la instalación se ha realizado correctamente mediante los siguientes métodos:

Operador Astra Trident

Compruebe el `trident-acp` container se está ejecutando y eso `acpVersion` es `23.10.0` o posterior (23,10 es la versión mínima) con un estado de `Installed`:

```
kubectl get torc -o yaml
```

Respuesta:

```
status:
  acpVersion: 24.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:24.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

Confirme que se ha habilitado el aprovisionador de Astra Control:

```
./tridentctl -n trident version
```

Respuesta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 24.10.0 | 24.10.0 | 24.10.0. | +----------------
+----------------+-------------+
```

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- "Aviso para Astra Control Center"

Licencia Astra Control API

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf