Documentación de Astra Control Center 22.08

Astra Control Center

NetApp
November 21, 2023

Tabla de contenidos

Documentación de Astra Control Center 22.08

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"
- "Problemas conocidos de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas"

Síganos en Twitter @NetAppDoc. 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.

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"
- "Problemas conocidos de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas de esta versión"

26 de abril de 2022 (22.04.0)

Detalles

Nuevas funciones y soporte

- "Puesta en marcha del almacén de datos de Astra desde Astra Control Center"
- "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"
- "Problemas conocidos de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas de esta versión"

14 de diciembre de 2021 (21.12)

Detalles

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"
- "Astra Data Store vista previa de la gestión y supervisión del entorno de administración"
- "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"
- "Problemas conocidos con la vista previa de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas de esta versión"

5 de agosto de 2021 (21.08)

Detalles

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"
- "Documentación de Astra Data Store"
- "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:

Aplicaciones

- La restauración de una aplicación genera un tamaño VP superior al VP original
- Los clones de aplicaciones producen un error al utilizar una versión específica de PostgreSQL
- Error en los clones de aplicaciones al utilizar restricciones de contexto de seguridad OCP de nivel de cuenta de servicio (SCC)
- Se produce un error en los clones de aplicaciones después de poner en marcha una aplicación con una clase de almacenamiento establecida
- Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster

De clúster

- La administración de un clúster con Astra Control Center falla cuando el archivo kubeconfig predeterminado contiene más de un contexto

Otros temas

- Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión
- Es posible que se produzca un error en Snapshot con la controladora Snapshot versión 4.2.0

La restauración de una aplicación genera un tamaño VP superior al VP original

Si cambia el tamaño de un volumen persistente después de crear un backup y luego se restaura a partir de ese backup, el tamaño del volumen persistente coincidiría con el nuevo tamaño del VP en lugar de usar el tamaño del backup.

Los clones de aplicaciones producen un error al utilizar 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.

Error en los clones de aplicaciones al utilizar restricciones de contexto de seguridad OCP de nivel de cuenta de servicio (SCC)

Un clon de aplicación podría fallar si las restricciones de contexto de seguridad originales están configuradas en el nivel de cuenta de servicio dentro del espacio de nombres en el clúster de OpenShift Container Platform. Cuando se produce un error en el clon de la aplicación, aparece en el área aplicaciones gestionadas del Centro de control de Astra con el estado `Removed`. Consulte "artículo de base de conocimientos" si quiere más información.

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 los clones de aplicaciones después de poner en marcha una aplicación con una clase de almacenamiento establecida

Una vez que se implementa una aplicación con una clase de almacenamiento definida explícitamente (por ejemplo, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), los intentos posteriores de clonar la aplicación requieren que el clúster de destino tenga 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. No existen pasos de recuperación en este escenario.

La administración de un clúster con Astra Control Center falla cuando el archivo kubeconfig predeterminado 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.

Es posible que se produzca un error en Snapshot con la controladora Snapshot versión 4.2.0

Cuando se usa una controladora Snapshot de Kubernetes (también conocida como copia Snapshot externa) versión 4.2.0 con Kubernetes 1.20 o 1.21, es posible que las copias Snapshot comiencen a fallar algún día. Para evitar esto, utilice otro "versión compatible" De copias Snapshot externas, como la versión 4.2.1, con las versiones 1.20 o 1.21 de Kubernetes.

1. Ejecute una llamada POSTERIOR para agregar un archivo kubeconfig actualizado al `/credentials` endpoint y recupere el asignado `id` del cuerpo de respuesta.
2. Ejecute una llamada PUT desde el `/clusters` Extremo que utiliza el ID de clúster adecuado y establece el `credentialID` para la `id` valor del paso anterior.

Después de completar estos pasos, se actualiza la credencial asociada al clúster y el clúster debe volver a conectarse y actualizar su estado a. `available`.

Obtenga más información

- "Problemas conocidos con la vista previa de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas"

Problemas conocidos de Astra Data Store y esta versión de Astra Control Center

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

"Vea estos problemas adicionales conocidos de Astra Data Store" Esta situación puede afectar a la gestión de Astra Data Store con la versión actual de Astra Control Center.

Los detalles del volumen de Astra Data Store no aparecen en la página Storage Backends de la interfaz de usuario de Astra Control Center

Detalles como la capacidad y el rendimiento no aparecen en la interfaz de usuario de. Cuando se produce este problema, anule la gestión del back-end de almacenamiento y vuelva a añadirlo.

Para desinstalar un clúster con Astra Data Store es necesario eliminar primero una aplicación de sistema gestionado

Si agregó un clúster que contiene Astra Data Store a un clúster de Astra Control Center, la aplicación astrads-System se gestiona de forma predeterminada como una aplicación oculta. Para desgestionar el clúster, primero debe desgestionar la aplicación astrads-System. No puede anular la gestión de este tipo de aplicaciones mediante la interfaz de usuario de Astra Control Center. En su lugar, utilice una solicitud de API de Astra Control para eliminar manualmente la aplicación:

Detalles

Pasos

1. Obtenga el ID del clúster gestionado mediante esta API:

```
/accounts/{account_id}/topology/v1/managedClusters
```

Respuesta:

```
{
"items": [
{
"type": "application/astra-managedCluster",
"version": "1.1",
"id": "123ab987-0bc0-00d0-a00a-1234567abd8d",
"name": "astrads-cluster-1234567",
...
```

2. Obtenga el ID de aplicación del sistema de astrads gestionado:

```
/accounts/{account_id}/topology/v2/managedClusters/{managedCluster_id}/apps
```

Respuesta:

```
{
  "items": [
    [
      "1b011d11-bb88-40c7-a1a1-ab1234c123d3",
      "astrads-system",
      "ready"
    ]
  ],
  "metadata": {}
}
```

3. Elimine la aplicación astrads-System mediante el ID de aplicación adquirido en el paso anterior (`1b011d11-bb88-40c7-a1a1-ab1234c123d3`).

```
/accounts/{account_id}/k8s/v2/apps/{astrads-system_app_id}
```

Obtenga más información

- "Problemas conocidos"
- "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

Limitaciones en la gestión de aplicaciones

- 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

Limitaciones generales

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

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 Config Map de kubeadm-config:

```
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. Cuando se crea un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador 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.

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.

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".

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.

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.

Obtenga más información

- "Problemas conocidos"
- "Problemas conocidos de Astra Data Store y esta versión de Astra Control Center"

Conceptos

Más información sobre Astra Control

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

Funciones

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

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

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de implementación:

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

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

	Servicio de control Astra	Astra Control Center
¿Cuál es el soporte del back-end de almacenamiento?	Ofertas de servicios cloud de NetApp	• Sistemas ONTAP AFF y FAS de NetApp • Astra Data Store como back-end de almacenamiento • Entorno de administración del almacenamiento de Cloud Volumes ONTAP

Funcionamiento del servicio Astra Control

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

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

- Para comenzar a trabajar con Astra Control Service, configure su proveedor de cloud y 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 almacenamiento en disco de Azure como back-end de almacenamiento para sus volúmenes persistentes.
  - Para clústeres de Amazon EKS, utiliza Astra Control Service "Amazon Elastic Block Store" o. "Amazon FSX para ONTAP de NetApp" como back-end de almacenamiento para sus volúmenes persistentes.
- Agregue su primera tecnología Kubernetes al servicio Astra Control. A continuación, el servicio de control de Astra realiza lo siguiente:
  - Crea un almacén de objetos en su cuenta de proveedor de cloud, que es donde se almacenan las copias de backup.

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

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

Premium.

Cómo funciona Astra Control Center

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

Astra Control Center es compatible con clústeres de Kubernetes con:

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

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

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

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

Para instalar y utilizar Astra Control Center, tendrá que estar seguro "requisitos".

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

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

Obtenga más información sobre cómo "Configure Astra Control Center".

El Centro de Control de Astra hace lo siguiente:

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

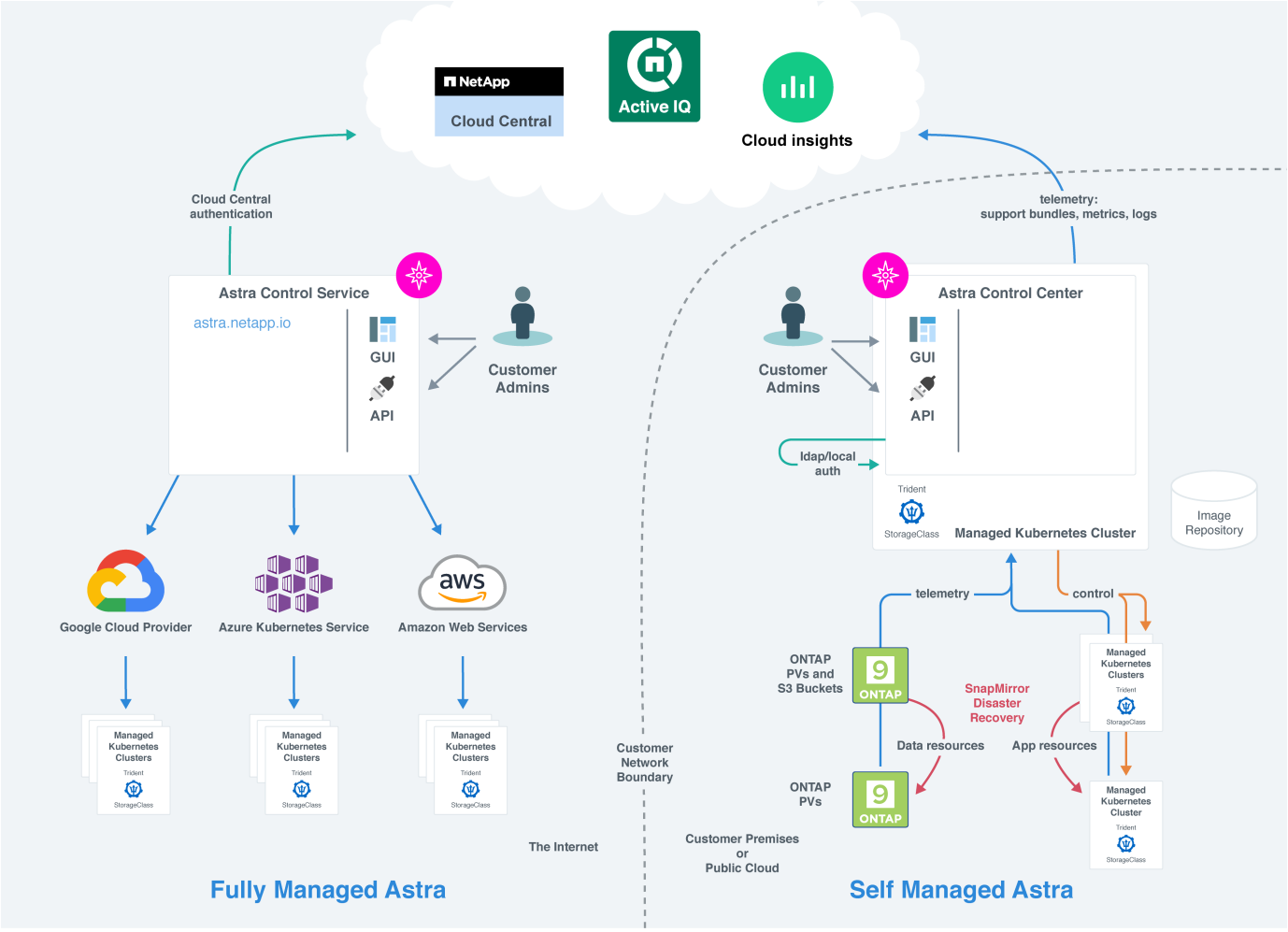
Puede añadir aplicaciones al clúster. O bien, si ya tiene algunas aplicaciones en el clúster que se están gestionando, puede utilizar Astra Control Center para gestionarlas. A continuación, utilice Astra Control Center para crear copias Snapshot, backups, clones y relaciones de replicación.

Si quiere más información

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

Arquitectura y componentes

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



Componentes de Astra Control

- **Clústeres de Kubernetes**: Kubernetes es una plataforma portátil, extensible y de código abierto para gestionar cargas de trabajo y servicios en contenedores, que facilita la configuración y la automatización declarativas. Astra proporciona servicios de gestión para aplicaciones alojadas en un clúster de Kubernetes.

- **Astra Trident**: Como orquestador y gestor de aprovisionamiento de código abierto totalmente compatible y mantenido por NetApp, Trident le permite crear volúmenes de almacenamiento para aplicaciones en contenedores gestionadas por Docker y Kubernetes. Cuando se pone en marcha con Astra Control Center, Trident incluye un back-end de almacenamiento configurado para ONTAP.
- **Sistema de almacenamiento**:
  - Astra Control Service utiliza los siguientes back-ends de almacenamiento:
    - "Cloud Volumes Service de NetApp para Google Cloud" O Google Persistent Disk como back-end de almacenamiento para clústeres GKE
    - "Azure NetApp Files" O discos gestionados de Azure como back-end de almacenamiento para clústeres de AKS.
    - "Elastic Block Store (EBS) de Amazon" o. "Amazon FSX para ONTAP de NetApp" Como opciones de almacenamiento de back-end para clústeres EKS.
  - Astra Control Center utiliza los siguientes back-ends de almacenamiento:
    - ONTAP AFF y FAS. Como plataforma de hardware y software de almacenamiento, ONTAP proporciona servicios de almacenamiento básicos, compatibilidad con varios protocolos de acceso a almacenamiento y funcionalidad de gestión del almacenamiento, como copias Snapshot y mirroring.
    - Cloud Volumes ONTAP
- **Cloud Insights**: Una herramienta de supervisión de infraestructura de cloud de NetApp, Cloud Insights le permite supervisar el rendimiento y la utilización de sus clústeres de Kubernetes gestionados por Astra Control Center. Cloud Insights relaciona el uso del almacenamiento con las cargas de trabajo. Cuando activa la conexión Cloud Insights en Astra Control Center, la información de telemetría se muestra en las páginas de interfaz de usuario de Astra Control Center.

Interfaces Astra Control

Puede completar tareas utilizando diferentes interfaces:

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

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

Si quiere más información

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

Protección de datos

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

Snapshot, backups y políticas de protección

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

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

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

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

Clones

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

La replicación en un clúster remoto

Con Astra Control, puede aumentar la continuidad del negocio para sus aplicaciones con un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación bajo (Recovery Time Objective) mediante funcionalidades de replicación asíncrona de la tecnología SnapMirror de NetApp. Una vez que se ha configurado, esto permite a sus aplicaciones replicar los cambios de aplicaciones y datos de un clúster a otro.

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

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

- **Replicación de aplicaciones**: Astra Control requiere que los clústeres de Kubernetes de origen y destino estén disponibles y gestionados con sus respectivos back-ends de almacenamiento de ONTAP

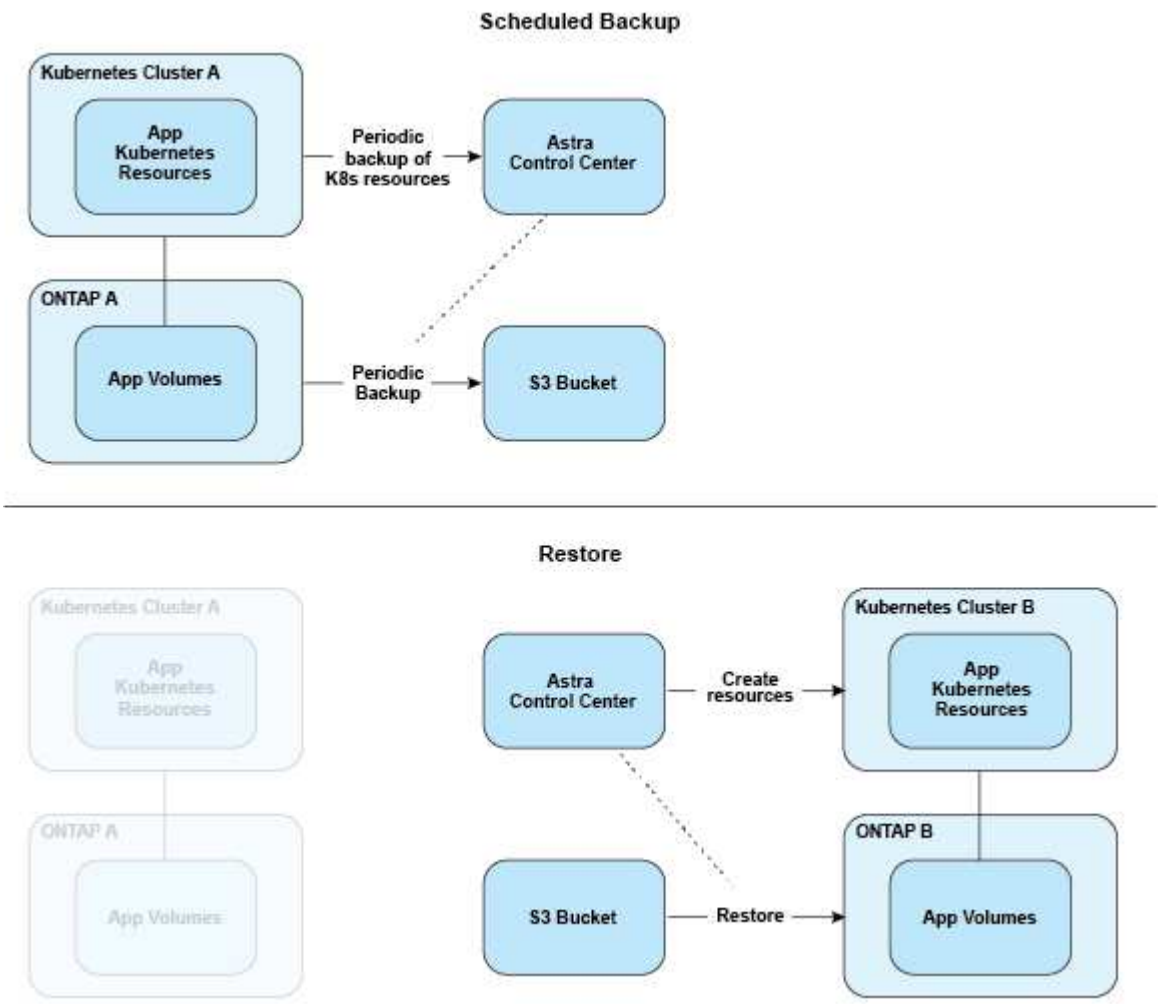
configurados para habilitar SnapMirror de NetApp. Astra Control toma la instantánea de las aplicaciones basadas en normativas y la replica en el clúster remoto. La tecnología SnapMirror de NetApp se usa para replicar los datos de volúmenes persistentes. Para conmutar al nodo de respaldo, Astra Control puede poner en línea la aplicación replicada al volver a crear los objetos de aplicación en el clúster de Kubernetes de destino con los volúmenes replicados en el clúster de ONTAP de destino. Dado que los datos de volúmenes persistentes ya están presentes en el clúster de ONTAP de destino, Astra Control puede ofrecer tiempos de recuperación rápidos en caso de fallo.

- **Copia de seguridad y restauración de aplicaciones**: Al hacer copias de seguridad de aplicaciones, Astra Control crea una instantánea de los datos de la aplicación y los almacena en un bloque de almacenamiento de objetos. Cuando se necesita una restauración, los datos del bloque deben copiarse a un volumen persistente del clúster de ONTAP. La operación de backup/restauración no requiere que el clúster de Kubernetes/ONTAP secundario esté disponible y gestionado, pero la copia de datos adicional puede provocar tiempos de restauración más prolongados.

Para saber cómo replicar aplicaciones, consulte "Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror".

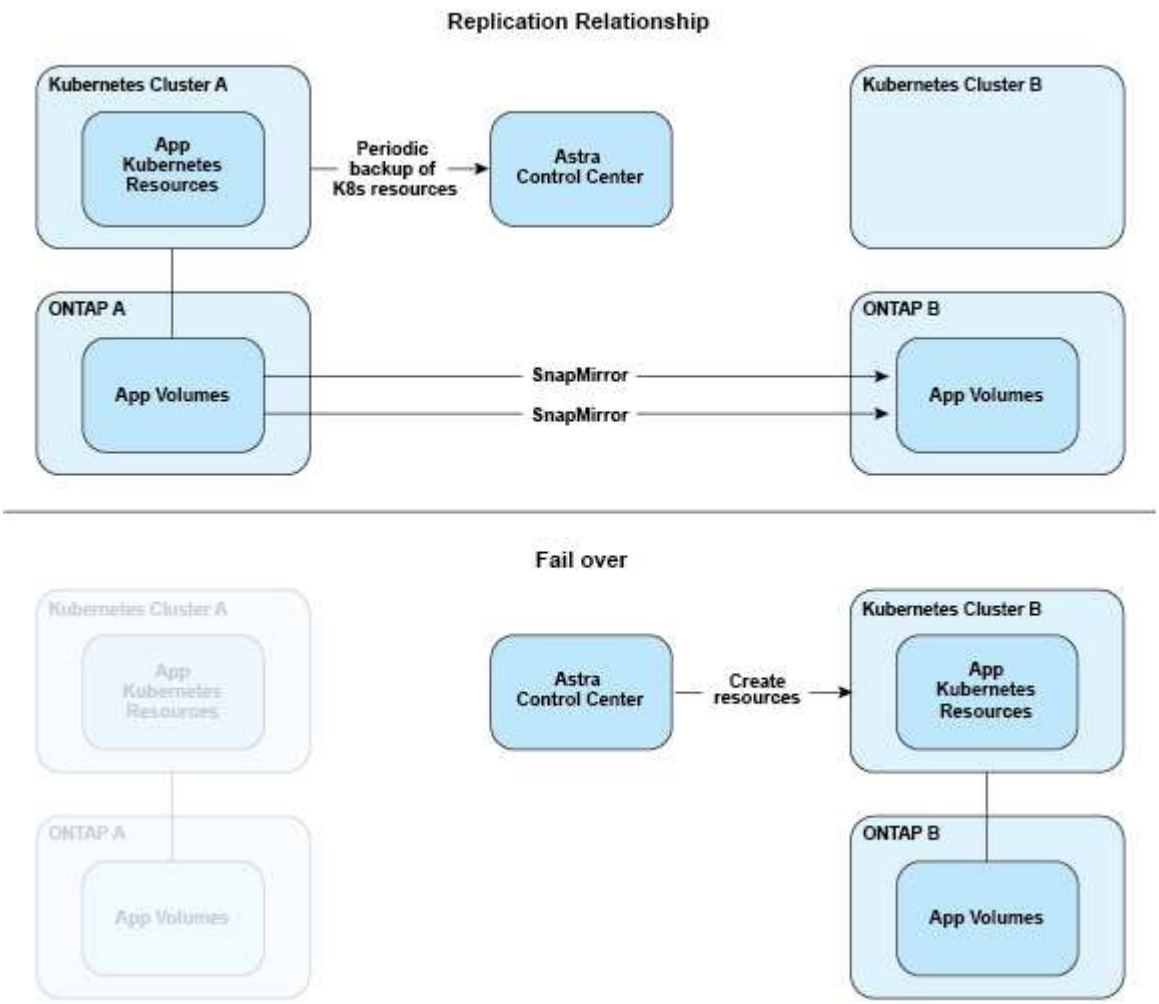
Las siguientes imágenes muestran el proceso de backup y restauración programado en comparación con el proceso de replicación.

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



Por otro lado, la replicación se realiza replicando en ONTAP para después crear el relevo de funciones en los

recursos de Kubernetes:



Licencia

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

Necesita una licencia para proteger sus aplicaciones y datos. Consulte Astra Control Center "funciones" para obtener más detalles.

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

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

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

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

Cómo se calcula el consumo de licencias

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

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

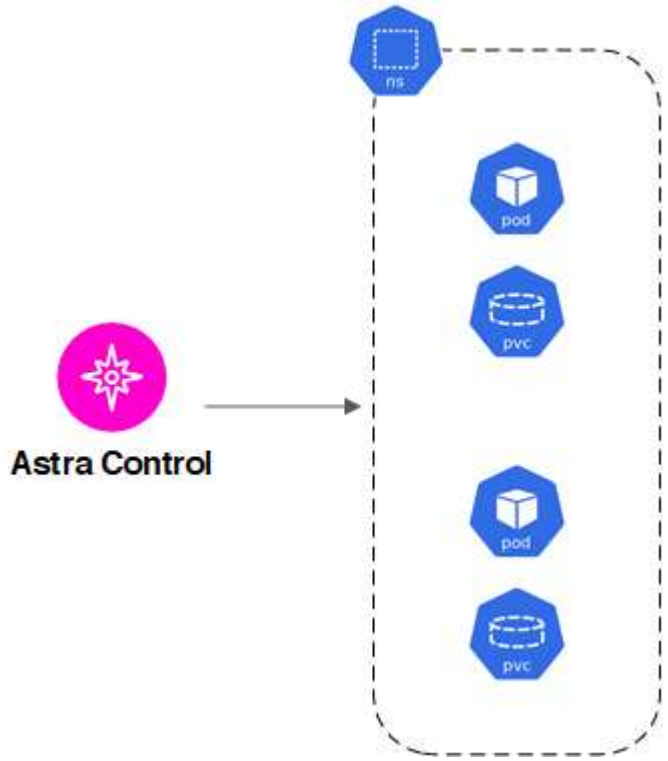
Obtenga más información

- "Actualizar una licencia existente"

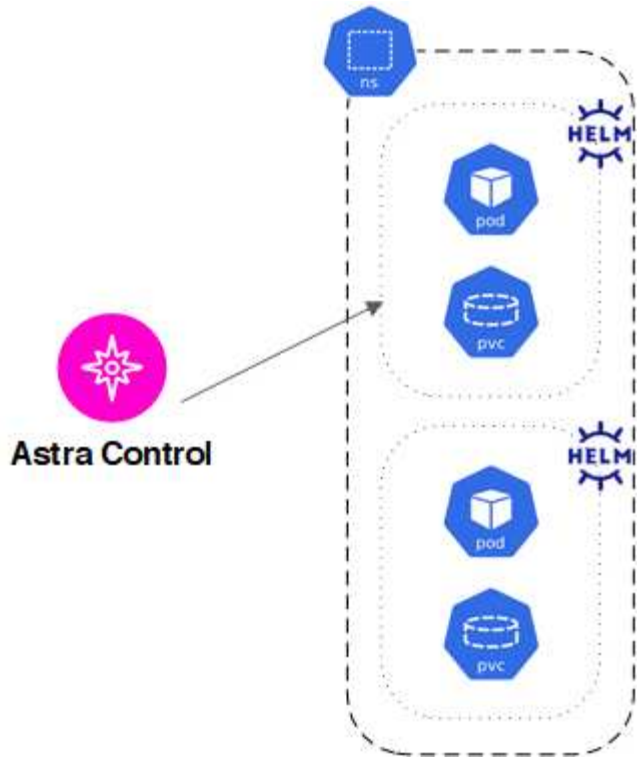
Descripción de la gestión de aplicaciones

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

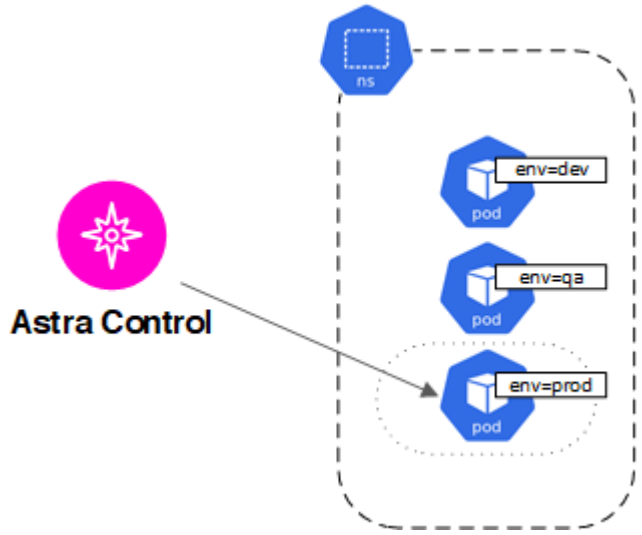
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



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



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



Clases de almacenamiento y tamaño de volumen persistente

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

Descripción general

Astra Control Center admite lo siguiente:

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

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

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

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

Clases de almacenamiento

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

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

Si quiere más información

- "Documentación de Astra Trident"

Roles de usuario y espacios de nombres

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

Roles de usuario

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

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

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

Espacios de nombres

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

Obtenga más información

"Gestionar roles"

Manos a la obra

Requisitos del Centro de Control de Astra

Comience verificando la preparación de su entorno operativo, clústeres de aplicaciones, aplicaciones, licencias y explorador web.

- Requisitos del entorno operativo
- Compatibles con los back-ends de almacenamiento
- Requisitos del clúster de aplicaciones
- Y gestión de aplicaciones
- Requisitos previos de replicación
- Acceso a Internet
- Licencia
- Entrada para clústeres de Kubernetes en las instalaciones
- Requisitos de red
- Exploradores web compatibles

Requisitos del entorno operativo

Astra Control Center se ha validado en los siguientes tipos de entornos operativos:

- Google Anthos 1.10 o 1.11
- Kubernetes 1.22 a 1.24
- Rancher Kubernetes Engine (RKE):
  - RKE 1.2.16 w/ Rancher 2.5.12 y RKE 1.3.3 w/ 2.6.3
  - RKE 2 (v1.23.6+rke2r2) con Rancher 2.6.3
- OpenShift Container Platform de Red Hat 4.8, 4.9 o 4.10
- VMware Tanzania Kubernetes Grid 1.4 o 1.5
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2 o 1.13

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 los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad del back-end de almacenamiento	500 GB disponibles como mínimo
Nodos de trabajo	Al menos 3 nodos de trabajo en total, con 4 núcleos de CPU y 12 GB de RAM cada uno
Dirección FQDN	Una dirección FQDN para Astra Control Center

Componente	Requisito
Astra Trident	Astra Trident 21.10.1 o una versión más reciente instalada y configurada Astra Trident 22.07 o más reciente para la replicación de aplicaciones basada en SnapMirror

> 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.

- **Registro de imágenes**: Debe tener un registro de imágenes Docker privado existente en el que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.
- **Configuración de Astra Trident/ONTAP**: Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con los siguientes controladores de ONTAP proporcionados por Astra Trident:
  - ontap-nas
  - san ontap
  - ontap-san-economía

> 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`

> Si tiene pensado añadir un segundo entorno operativo OpenShift como recurso informático gestionado, debe asegurarse de que la función Astra Trident Volume Snapshot esté habilitada. Para habilitar y probar copias Snapshot de volumen con Astra Trident, "Consulte las instrucciones oficiales de la Astra Trident".

Requisitos del clúster de Grid de VMware Tanzania Kubernetes

Al alojar Astra Control Center en un clúster VMware Tanzu Kubernetes Grid (TKG) o Tanzu Kubernetes Grid Integrated Edition (TKGi), tenga en cuenta las siguientes consideraciones.

- 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.
- Como parte de la instalación de Astra Control Center, los siguientes recursos se crean en un entorno restringido de directiva de seguridad de POD (PSP):
  - directiva de seguridad de pod
  - Rol de RBAC

- RBAC RoleBinding la función RBAC y los recursos RoleBinding se crean en la `netapp-acc` espacio de nombres.

- Tenga en cuenta los requisitos específicos para Astra Trident al implementar Astra Control Center en un entorno TKG o TKGi. Para obtener más información, consulte "Documentación de Astra Trident".

> 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."

Requisitos de clúster de Google Anthos

Al alojar Astra Control Center en un clúster de Google Anthos, tenga en cuenta que Google Anthos incluye de forma predeterminada el equilibrador de carga de MetalLB y el servicio de puerta de enlace de entrada Istio, lo que le permite utilizar simplemente las capacidades de entrada genéricas de Astra Control Center durante la instalación. Consulte "Configurar Astra Control Center" para obtener más detalles.

Compatibles con los back-ends de almacenamiento

Astra Control Center admite los siguientes back-ends de almacenamiento.

- NetApp ONTAP 9.5 o sistemas AFF y FAS más recientes
- ONTAP 9.8 de NetApp o sistemas AFF y FAS más recientes para la replicación de aplicaciones basadas en SnapMirror
- Cloud Volumes ONTAP de NetApp

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

Quizás desee comprobar si el sistema ONTAP tiene las licencias necesarias. Consulte "Gestione licencias de ONTAP".

Requisitos del clúster de aplicaciones

Astra Control Center tiene los siguientes requisitos para los clústeres que tiene previsto gestionar desde Astra Control Center. Estos requisitos también se aplican si el clúster que tiene previsto gestionar es el clúster de entorno operativo que aloja Astra Control Center.

- La versión más reciente de Kubernetes "componente de controladora snapshot" está instalado
- Una Astra Trident "volumesnapshotclass object" ha sido definido por un administrador
- Existe una clase de almacenamiento de Kubernetes predeterminada en el clúster
- Se configura al menos una clase de almacenamiento para que use Astra Trident

Su clúster de aplicaciones debe tener un `kubeconfig.yaml` archivo que define sólo un elemento *context*. Consulte la documentación de Kubernetes para "información sobre la creación de archivos kubeconfig".

Cuando administre clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en `kubeconfig` Archivo 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.

Y gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencia**: Para gestionar aplicaciones mediante Astra Control Center, necesita una licencia Astra Control Center.
- **Namespaces**: Astra Control requiere que una aplicación no abarque más de un único espacio de nombres, pero un espacio de nombres puede contener más de una aplicación.
- **StorageClass**: Si instala una aplicación con StorageClass definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonado debe tener el StorageClass especificado originalmente. Se producirá un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo 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:

Función de clúster	ClusterRoleBinding	ConfigMap
Cronjob	CustomResourceDefinition	Recurso personalizado
DemonSet	DeploymentConfig	HorizontalPodAutocaler
Entrada	MutatingWebhook	Política de red
Claim persistente	Pod	PodDisruptionBudget
PodTemplate	Replicaset	Función
RoleBinding	Ruta	Secreto
Servicio	ServiceAccount	Statilusionados Set
ValidadoWebhook		

Requisitos previos de replicación

La replicación de aplicaciones de Astra Control requiere que se cumplan los siguientes requisitos previos antes de comenzar:

- Para lograr una recuperación ante desastres sin problemas, le recomendamos que ponga en marcha Astra Control Center en un tercer dominio de fallo o ubicación secundaria.
- El clúster de Kubernetes host de la aplicación y un clúster de Kubernetes de destino deben estar disponibles y conectados a dos clústeres de ONTAP, lo cual es ideal para diferentes dominios de fallo o sitios.

- Los clústeres de ONTAP y la SVM de host se deben emparejar. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM".
- La SVM remota emparejada debe estar disponible para Trident en el clúster de destino.
- La versión 22.07 de Trident o superior debe existir en los clústeres ONTAP de origen y destino.
- Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben habilitarse en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP".
- Al añadir un back-end de almacenamiento de ONTAP a Astra Control Center, aplique las credenciales de usuario con la función "admin", que cuenta con métodos de acceso `http` y.. `ontapi` Habilitado en ambos clústeres de ONTAP. Consulte "Gestionar cuentas de usuario" si quiere más información.
- Astra Control debe gestionar los clústeres de Kubernetes de origen y destino, y los clústeres de ONTAP.

> Puede replicar simultáneamente una aplicación diferente (que se ejecute en el otro clúster o sitio) 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.

Aprenda cómo "Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror".

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. A continuación, se enumeran algunas aplicaciones que se han validado para este modelo de instalación:
  - "Apache K8ssandra"
  - "Jenkins CI"
  - "Clúster Percona XtraDB"

> Un operador y la aplicación que instale deben usar el mismo espacio de nombres; es posible que deba modificar el archivo .yaml de despliegue para que el operador se asegure de que así sea.

Acceso a Internet

Debe determinar si tiene acceso externo a Internet. Si no lo hace, es posible que algunas funcionalidades sean limitadas, como recibir datos de supervisión y métricas de Cloud Insights de NetApp, o enviar paquetes de soporte al "Sitio de soporte de NetApp".

Licencia

Astra Control Center requiere una licencia de Astra Control Center para obtener todas las funciones. Obtenga una licencia de evaluación o una licencia completa de NetApp. Necesita una licencia para proteger sus aplicaciones y datos. Consulte "Características de Astra Control Center" para obtener más detalles.

Puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Puede inscribirse para obtener una prueba gratuita registrándose "aquí".

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

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

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 no tiene uno configurado, puede utilizar el equilibrador de carga 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.

> Si va a alojar Astra Control Center en un clúster de cuadrícula de Tanzania Kubernetes, utilice `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.

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

Requisitos de red

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 de interfaz de usuario/API: Asegúrese de que este puerto está abierto de ambas formas entre el clúster que aloja a Astra Control Center y cada clúster gestionado
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	Servicio Cloud Insights alojado	443	HTTPS	Comunicación de Cloud Insights
Astra Control Center	Proveedor de bloques de almacenamiento Amazon S3	443	HTTPS	Comunicación del almacenamiento de Amazon S3
Astra Control Center	AutoSupport de NetApp	443	HTTPS	Comunicación AutoSupport de NetApp

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.

El futuro

Vea la "inicio rápido" descripción general.

Inicio rápido para Astra Control Center

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

¡Pruébela! Si desea probar Astra Control Center, puede utilizar una licencia de evaluación de 90 días. Consulte "información sobre licencias" para obtener más detalles.

1 Revise los requisitos del clúster de Kubernetes

- Astra funciona con clústeres de Kubernetes con un back-end de almacenamiento de ONTAP configurado para Trident o un back-end de almacenamiento de Astra Data Store.
- Los clústeres deben ejecutarse en buen estado, con al menos tres nodos de trabajo en línea.
- El clúster debe ejecutar Kubernetes.

Obtenga más información sobre la "Requisitos del Centro de Control de Astra".

2 Descargue e instale Astra Control Center

- Descargue Astra Control Center desde "Página de descargas del Centro de control de Astra del sitio de soporte de NetApp".
- Instale Astra Control Center en su entorno local.

  Opcionalmente, instale Astra Control Center utilizando Red Hat OperatorHub.

  Opcionalmente, instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP.

Más información acerca de "Instalación de Astra Control Center".

3 Complete algunas tareas de configuración inicial

- Añada una licencia de Astra Control y todas las licencias de ONTAP compatibles.
- Añada un clúster de Kubernetes y Astra Control Center descubre los detalles.
- Añada un back-end de almacenamiento de ONTAP.
- Opcionalmente, agregue un bucket de almacén de objetos que almacenará las copias de seguridad de la aplicación.

Obtenga más información sobre la "proceso de configuración inicial".

4 Utilice Astra Control Center

Cuando termine de configurar Astra Control Center, a continuación puede hacer lo siguiente:

- Gestionar una aplicación. Obtenga más información sobre cómo "gestionar aplicaciones".
- Proteja las aplicaciones configurando políticas de protección para aplicaciones, replicando aplicaciones en sistemas remotos, y clonando y migrando aplicaciones. Obtenga más información sobre cómo "proteja sus aplicaciones".
- Gestionar cuentas (incluidos usuarios, roles, LDAP para autenticación de usuarios, credenciales, conexiones de repositorio, etc.). Obtenga más información sobre cómo "gestionar usuarios".
- De manera opcional, conéctese a Cloud Insights de NetApp para mostrar métricas sobre el estado del sistema, la capacidad y el rendimiento dentro de la IU del centro de control de Astra. Más información acerca de "Conectando a Cloud Insights".

5 **Continuar desde este Inicio rápido**

"Instalar Astra Control Center".

Obtenga más información

- "Utilice la API 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"

Instale Astra Control Center mediante el proceso estándar

Para instalar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y realice los siguientes pasos para instalar Astra Control Center Operator y Astra Control Center en su entorno. Puede utilizar este procedimiento para instalar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Para entornos Red Hat OpenShift, puede utilizar un "procedimiento alternativo" Para instalar Astra Control Center con OpenShift OperatorHub.

Lo que necesitará

- "Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center".
- Si ha configurado o desea configurar directivas de seguridad de POD en su entorno, familiarícese con las directivas de seguridad de POD y cómo afectan a la instalación de Astra Control Center. Consulte "Comprender las restricciones de directivas de seguridad de POD".
- Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

  ```
  kubectl get clusteroperators
  ```

- Asegúrese de que todos los servicios de API se encuentren en buen estado y estén disponibles:

  ```
  kubectl get apiservices
  ```

- Asegúrese de que el FQDN de Astra que tiene previsto utilizar se puede enrutar a este 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.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos "requisitos previos" Por lo tanto, Astra Control Center no instala su propio cert-Manager.

Acerca de esta tarea

El proceso de instalación de Astra Control Center realiza lo siguiente:

- Instala los componentes de Astra en `netapp-acc` (o nombre personalizado).
- Crea una cuenta predeterminada.
- Establece una dirección de correo electrónico de usuario administrativo predeterminada y una contraseña única predeterminada. A este usuario se le asigna el rol de propietario del sistema que se necesita para iniciar sesión por primera vez en la interfaz de usuario.
- Le ayuda a determinar que se están ejecutando todas las pods de Astra Control Center.
- Instala la interfaz de usuario de Astra.

> (Se aplica sólo a la versión Astra Data Store Early Access Program (EAP)) Si tiene intención de gestionar Astra Data Store mediante Astra Control Center y habilitar los flujos de trabajo de VMware, implemente Astra Control Center únicamente en `pcloud` espacio de nombres y no en `netapp-acc` espacio de nombres o un espacio de nombres personalizado que se describe en los pasos de este procedimiento.

> No ejecute el siguiente comando durante todo el proceso de instalación para evitar eliminar todas las POD de Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

> Si utiliza Podman de Red Hat en lugar de Docker Engine, los comandos de Podman se pueden utilizar en lugar de los comandos de Docker.

Pasos

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

- Descargue y desembale el paquete Astra Control Center
- Instale el complemento Astra kubectl de NetApp
- Agregue las imágenes al 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

Descargue y desembale el paquete Astra Control Center

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del "Sitio de soporte de NetApp".
2. Descargue el archivo zip de los certificados y claves de Astra Control Center de "Sitio de soporte de NetApp".
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

4. Extraiga las imágenes:

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

Instale el complemento Astra kubectl de NetApp

La Astra de NetApp `kubectl` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux y Mac, puede utilizar `uname -a` comando para recopilar esta información.

Pasos

1. Enumere la Astra de NetApp disponible `kubectl` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubectl-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubectl` utilidad. En este ejemplo, la `kubectl` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

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

Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR_REGISTRY> como se indica en los comentarios:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

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

1. Exporte el KUBECONFIG para el clúster de host de Astra Control Center:

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

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
```

   Respuesta:

```
namespace/netapp-acc-operator created
```

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/22.08.1-26`).

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

Respuesta de ejemplo:

```
secret/astra-registry-cred created
```

> Si elimina el espacio de nombres después de que se genere el secreto, deberá volver a generar el secreto para el espacio de nombres después de volver a crear el espacio de nombres.

c. Cree el `netapp-acc` (o espacio de nombres personalizado).

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

Respuesta de ejemplo:

```
namespace/netapp-acc created
```

d. Cree un secreto para `netapp-acc` (o espacio de nombres personalizado). Añada información sobre Docker y ejecute el siguiente comando:

```
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]
```

Respuesta

```
secret/astra-registry-cred created
```

a. [[substep_kubeconfig_secret](opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación, asegúrese de proporcionar el kubeconfig como secreto dentro del espacio de nombres Astra Control Center que tiene intención de implementar utilizando este comando:

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret
name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom
namespace]
```

Instale el operador de Astra Control Center

1. Cambie el directorio:

```
cd manifests
```

2. Edite la implementación del operador de Astra Control Center YAML (`astra_control_center_operator_deploy.yaml`) para referirse a su registro local y secreto.

```
vim astra_control_center_operator_deploy.yaml
```

> Una muestra anotada de AYLMA sigue estos pasos.

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

```
imagePullSecrets:
- name: <astra-registry-cred>
```

b. Cambiar `[your_registry_path]` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

c. Cambiar `[your_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

d. (Para instalaciones que utilizan la vista previa de Astra Data Store) Consulte este problema conocido con respecto a "Los aprovisionadores de clases de almacenamiento y los cambios adicionales que deberá realizar en la YAML".

```
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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Instale el operador de Astra Control Center:

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

Respuesta de ejemplo:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
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
```

4. 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_min.yaml`) Para realizar las configuraciones de cuenta, AutoSupport, Registro y otras necesarias:

> `astra_control_center_min.yaml` Es la CR predeterminada y es adecuada para la mayoría de las instalaciones. Familiarícese con todos "Opciones CR y sus valores potenciales" Garantizar la puesta en marcha correcta de Astra Control Center en su entorno. Si se requieren personalizaciones adicionales para su entorno, puede utilizar `astra_control_center.yaml` Como CR alternativo.

```
vim astra_control_center_min.yaml
```

> Si está utilizando un registro que no requiere autorización, debe eliminar `secret` línea dentro `imageRegistry` o se producirá un error en la instalación.

a. Cambiar `[your_registry_path]` a la ruta de acceso del registro en la que ha insertado las imágenes en el paso anterior.

b. Cambie el `accountName` cadena al nombre que desea asociar a la cuenta.

c. Cambie el `astraAddress` Cadena al FQDN que desea utilizar en su navegador para acceder a Astra. No utilizar `http://` o. `https://` en la dirección. Copie este FQDN para utilizarlo en un paso posterior.

d. Cambie el `email` cadena en la dirección inicial predeterminada del administrador. Copie esta dirección de correo electrónico para su uso en un paso posterior.

e. Cambiar `enrolled` Para AutoSupport a. `false` para sitios sin conexión a internet o retención `true` para sitios conectados.

f. Si utiliza un administrador de certificados externo, añada las siguientes líneas a. `spec`:

```
spec:
  crds:
    externalCertManager: true
```

g. (Opcional) Añada un nombre `firstName` y apellidos `lastName` del usuario asociado con la cuenta. Este paso se puede realizar ahora o una versión posterior dentro de la interfaz de usuario.

h. (Opcional) cambie el `storageClass` Valor en otro recurso de la clase de almacenamiento de Trident, si es necesario para su instalación.

i. (Opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación y ya lo tiene se ha creado el secreto que contiene el kubeconfig para este cluster, Proporcione el nombre del secreto agregando un nuevo campo a este archivo YLMA llamado `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

j. Realice uno de los siguientes pasos:

- **Otro controlador de entrada (ingressType:Generic)**: Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

  La instalación predeterminada de Astra Control Center configura su puerta de enlace (`service/traefik`) ser del tipo `ClusterIP`. Esta instalación predeterminada requiere que configure además un dispositivo de entrada/controlador de Kubernetes para enrutar el tráfico hacia él. Si desea utilizar una entrada, consulte "Configure la entrada para el equilibrio de carga".

- **Equilibrador de carga de servicio (ingressType:AccTraefik)**: Si no desea instalar un controlador IngressController o crear un recurso de entrada, establezca `ingressType` para `AccTraefik`.

  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 asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y 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 más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte "Requisitos".

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

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]
   ```

   Respuesta de ejemplo:

   ```
   namespace/netapp-acc created
   ```

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

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

   Respuesta de ejemplo:

   ```
   astracontrolcenter.astra.netapp.io/astra created
   ```

Comprobar el estado del sistema

> Si prefiere utilizar OpenShift, puede utilizar comandos de OC comparables para realizar los pasos de verificación.

1. 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.

Ejemplo de respuesta

```
NAME                                        READY   STATUS    RESTARTS
AGE
acc-helm-repo-6b44d68d94-d8m55              1/1     Running   0
13m
activity-78f99ddf8-hltct                    1/1     Running   0
10m
api-token-authentication-457nl              1/1     Running   0
9m28s
api-token-authentication-dgwsz              1/1     Running   0
9m28s
api-token-authentication-hmqqc              1/1     Running   0
9m28s
asup-75fd554dc6-m6qzh                       1/1     Running   0
9m38s
authentication-6779b4c85d-92gds             1/1     Running   0
8m11s
bucketservice-7cc767f8f8-lqwr8              1/1     Running   0
9m31s
certificates-549fd5d6cb-5kmd6               1/1     Running   0
9m56s
certificates-549fd5d6cb-bkjh9               1/1     Running   0
9m56s
cloud-extension-7bcb7948b-hn8h2             1/1     Running   0
10m
cloud-insights-service-56ccf86647-fgg69     1/1     Running   0
9m46s
composite-compute-677685b9bb-7vgsf          1/1     Running   0
10m
composite-volume-657d6c5585-dnq79           1/1     Running   0
9m49s
credentials-755fd867c8-vrlmt                1/1     Running   0
11m
entitlement-86495cdf5b-nwhh2                1/1     Running   2
10m
features-5684fb8b56-8d6s8                   1/1     Running   0
10m
fluent-bit-ds-rhx7v                         1/1     Running   0
7m48s
fluent-bit-ds-rjms4                         1/1     Running   0
7m48s
fluent-bit-ds-zf5ph                         1/1     Running   0
7m48s
graphql-server-66d895f544-w6hjd             1/1     Running   0
3m29s
```

```
identity-744df448d5-rlcmm                1/1     Running   0
10m
influxdb2-0                              1/1     Running   0
13m
keycloak-operator-75c965cc54-z7csw       1/1     Running   0
8m16s
krakend-798d6df96f-9z2sk                 1/1     Running   0
3m26s
license-5fb7d75765-f8mjg                 1/1     Running   0
9m50s
login-ui-7d5b7df85d-l2s7s                1/1     Running   0
3m20s
loki-0                                   1/1     Running   0
13m
metrics-facade-599b9d7fcc-gtmgl          1/1     Running   0
9m40s
monitoring-operator-67cc74f844-cdplp     2/2     Running   0
8m11s
nats-0                                   1/1     Running   0
13m
nats-1                                   1/1     Running   0
13m
nats-2                                   1/1     Running   0
12m
nautilus-769f5b74cd-k5jxm                1/1     Running   0
9m42s
nautilus-769f5b74cd-kd9gd                1/1     Running   0
8m59s
openapi-84f6ccd8ff-76kvp                 1/1     Running   0
9m34s
packages-6f59fc67dc-4g2f5                1/1     Running   0
9m52s
polaris-consul-consul-server-0           1/1     Running   0
13m
polaris-consul-consul-server-1           1/1     Running   0
13m
polaris-consul-consul-server-2           1/1     Running   0
13m
polaris-keycloak-0                       1/1     Running   0
8m7s
polaris-keycloak-1                       1/1     Running   0
5m49s
polaris-keycloak-2                       1/1     Running   0
5m15s
polaris-keycloak-db-0                    1/1     Running   0
8m6s
```

```
polaris-keycloak-db-1                     1/1     Running   0
5m49s
polaris-keycloak-db-2                     1/1     Running   0
4m57s
polaris-mongodb-0                         2/2     Running   0
13m
polaris-mongodb-1                         2/2     Running   0
12m
polaris-mongodb-2                         2/2     Running   0
12m
polaris-ui-565f56bf7b-zwr8b               1/1     Running   0
3m19s
polaris-vault-0                           1/1     Running   0
13m
polaris-vault-1                           1/1     Running   0
13m
polaris-vault-2                           1/1     Running   0
13m
public-metrics-6d86d66444-2wbzl           1/1     Running   0
9m30s
storage-backend-metrics-77c5d98dcd-dbhg5 1/1     Running   0
9m44s
storage-provider-78c885f57c-6zcv4         1/1     Running   0
9m36s
telegraf-ds-2l2m9                         1/1     Running   0
7m48s
telegraf-ds-qfzgh                         1/1     Running   0
7m48s
telegraf-ds-shrms                         1/1     Running   0
7m48s
telegraf-rs-bjpkt                         1/1     Running   0
7m48s
telemetry-service-6684696c64-qzfdf        1/1     Running   0
10m
tenancy-6596b6c54d-vmpsm                  1/1     Running   0
10m
traefik-7489dc59f9-6mnst                  1/1     Running   0
3m19s
traefik-7489dc59f9-xrkgg                  1/1     Running   0
3m4s
trident-svc-6c8dc458f5-jswcl              1/1     Running   0
10m
vault-controller-6b954f9b76-gz9nm         1/1     Running   0
11m
```

2. (Opcional) para asegurarse de que la instalación ha finalizado, puede ver el `acc-operator` registra utilizando el siguiente comando.

```
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 un error de registro del clúster que se indica en los registros, puede volver a intentar el registro a través del flujo de trabajo de add cluster "En la interfaz de usuario de" O API.

3. Cuando todos los pods estén en ejecución, verifique que la instalación se haya realizado correctamente (`READY` es `True`) Y obtenga la contraseña única que utilizará cuando inicie sesión en Astra Control Center:

```
kubectl get AstraControlCenter -n netapp-acc
```

Respuesta:

```
NAME    UUID                                        VERSION     ADDRESS
READY
astra   ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  22.08.1-26
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 una controladora de entrada de Kubernetes que gestione el acceso externo a los servicios, como el equilibrio de carga en un clúster.

Este procedimiento explica cómo configurar un controlador de entrada (`ingressType:Generic`). Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

> Si no desea configurar un controlador de entrada, puede configurarlo `ingressType:AccTraefik`). 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 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 más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte "Requisitos".

Los pasos varían en función del tipo de controlador de entrada que utilice:

- Entrada Istio
- Controlador de entrada nginx
- Controlador OpenShift Ingress

Lo que necesitará

- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.
- Se utilizan versiones de Kubernetes entre e incluidas v1.19 y v1.22.

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 uso del tipo de recurso v1beta1 (obsoleto en la versión de Kubernetes menor que o 1.22) o v1 para un esquema obsoleto o nuevo:

   Salida:

```yaml
apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          serviceName: traefik
          servicePort: 80
```

Para el nuevo esquema v1, siga este ejemplo:

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

Salida:

```
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: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Implementar Astra Control Center como es habitual.
6. Compruebe el estado de la entrada:

```
kubectl get ingress -n netapp-acc
```

Respuesta:

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

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` (o nombre personalizado) mediante el `v1beta1` (Obsoleto en la versión de Kubernetes inferior a o 1.22) o. `v1` tipo de recurso para un esquema obsoleto o nuevo:

   a. Para un `v1beta1` esquema obsoleto, siga este ejemplo:

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

   b. Para la `v1` nuevo esquema, siga este ejemplo:

```yaml
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 addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

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

Después de instalar Astra Control Center, cambiará la contraseña del administrador predeterminado e inicie sesión en el panel de interfaz de usuario de Astra Control Center.

Pasos

1. En un explorador, introduzca el FQDN que utilizó en `astraAddress` en la `astra_control_center_min.yaml` CR cuando Ha instalado Astra Control Center.
2. Acepte los certificados autofirmados cuando se le solicite.

> 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_min.yaml` CR cuando Ha instalado Astra Control Center, seguido de la contraseña única (`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 este es su primer inicio de sesión y olvida la contraseña y aún no se han creado otras cuentas de usuario administrativas, comuníquese con el servicio de 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.

Pasos

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

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n
netapp-acc-operator -o name) -c manager
```

El futuro

Complete la implementación llevando a cabo "tareas de configuración".

=
:allow-uri-read:

Comprender las restricciones de directivas de seguridad de POD

Astra Control Center admite la limitación de privilegios mediante directivas de seguridad de POD (PSP). Las políticas de seguridad de POD permiten limitar los usuarios o grupos que pueden ejecutar contenedores y los privilegios que dichos contenedores pueden tener.

Algunas distribuciones de Kubernetes, como RKE2, tienen una política de seguridad de POD predeterminada que es demasiado restrictiva y provoca problemas al instalar Astra Control Center.

Puede utilizar la información y los ejemplos que se incluyen aquí para comprender las directivas de seguridad de POD que Astra Control Center crea y configurar las directivas de seguridad de POD que proporcionan la protección necesaria sin interferir con las funciones de Astra Control Center.

PSP instalado por Astra Control Center

Astra Control Center crea varias directivas de seguridad de POD durante la instalación. Algunas de ellas son permanentes y algunas se crean durante ciertas operaciones y se eliminan una vez que se completa la operación.

Se crean PSP durante la instalación

Durante la instalación de Astra Control Center, el operador Astra Control Center instala una directiva de seguridad de POD personalizada, un objeto Role y un objeto RoleBinding para admitir la implementación de los servicios Astra Control Center en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp

NAME                            PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
avp-psp                         false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *
netapp-astra-deployment-psp     false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                     CREATED AT
netapp-astra-deployment-role             2022-06-27T19:34:58Z

kubectl get rolebinding

NAME                                     ROLE
AGE
netapp-astra-deployment-rb               Role/netapp-astra-deployment-role
32m
```

Se crean PSP durante las operaciones de backup

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

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                   CREATED AT
netapp-astra-backup    2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                   ROLE                        AGE
netapp-astra-backup    Role/netapp-astra-backup    62s
```

Se crean PSP durante la gestión del clúster

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

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo      true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                            CREATED AT
netapp-monitoring-role-privileged               2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                                                    ROLE
AGE
netapp-monitoring-role-binding-privileged               Role/netapp-
monitoring-role-privileged              2m5s
```

Active la comunicación de red entre espacios de nombres

Algunos entornos utilizan construcciones de NetworkPolicy para restringir el tráfico entre espacios de nombres. El operador Astra Control Center, Astra Control Center y el complemento Astra para VMware vSphere están todos en espacios de nombres diferentes. Los servicios de estos distintos espacios de nombres deben poder comunicarse entre sí. Para activar esta comunicación, siga estos pasos.

Pasos

1. Elimine los recursos de NetworkPolicy que existan en el espacio de nombres de Astra Control Center:

```
kubectl get networkpolicy -n netapp-acc
```

2. Para cada objeto NetworkPolicy devuelto por el comando anterior, utilice el siguiente comando para eliminarlo. Sustituya <OBJECT_NAME> por el nombre del objeto devuelto:

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Aplique el siguiente archivo de recursos para configurar el objeto de política de red ACC-avp con el fin de permitir que los servicios de Astra Plugin para VMware vSphere puedan realizar solicitudes a los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. Aplique el siguiente archivo de recursos para configurar el objeto de directiva de red-operador de ACC con el fin de permitir que el operador de Astra Control Center se comunique con los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME
```

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. Debe eliminarlos 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 el espacio de nombres ACC-netapp:

   ```
   kubectl get quota -n netapp-acc
   ```

   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
```

```
kubectl delete resourcequota  pods-low -n netapp-acc
```

```
kubectl delete resourcequota  pods-medium -n netapp-acc
```

3. Obtenga los rangos de límites en el espacio de nombres ACC-netapp:

```
kubectl get limits -n netapp-acc
```

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
```

=
:allow-uri-read:

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.

Lo que necesitará

- "Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center".
- En el clúster OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado (`available` es `true`):

```
oc get clusteroperators
```

- Desde su clúster OpenShift, asegúrese de que todos los servicios API se encuentran en buen estado (`available` es `true`):

```
oc get apiservices
```

- Cree una dirección FQDN para Astra Control Center en su centro de datos.
- Obtenga los permisos necesarios y acceda a Red Hat OpenShift Container Platform para realizar los pasos de instalación descritos.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos "requisitos previos" Por lo tanto, Astra Control Center no instala su propio cert-Manager.

Pasos

- Descargue y desembale el paquete Astra Control Center
- Instale el complemento Astra kubectl de NetApp
- Agregue las imágenes al registro local
- Busque la página de instalación del operador
- Instale el operador
- Instalar Astra Control Center

Descargue y desembale el paquete Astra Control Center

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del "Sitio de soporte de NetApp".
2. Descargue el archivo zip de los certificados y claves de Astra Control Center de "Sitio de soporte de NetApp".
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

4. Extraiga las imágenes:

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

Instale el complemento Astra kubectl de NetApp

La Astra de NetApp `kubectl` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux y Mac, puede utilizar `uname -a` comando para recopilar esta información.

Pasos

1. Enumere la Astra de NetApp disponible `kubectl` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubectl-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubectl` utilidad. En este ejemplo, la `kubectl` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

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

Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Inicie sesión en su registro:

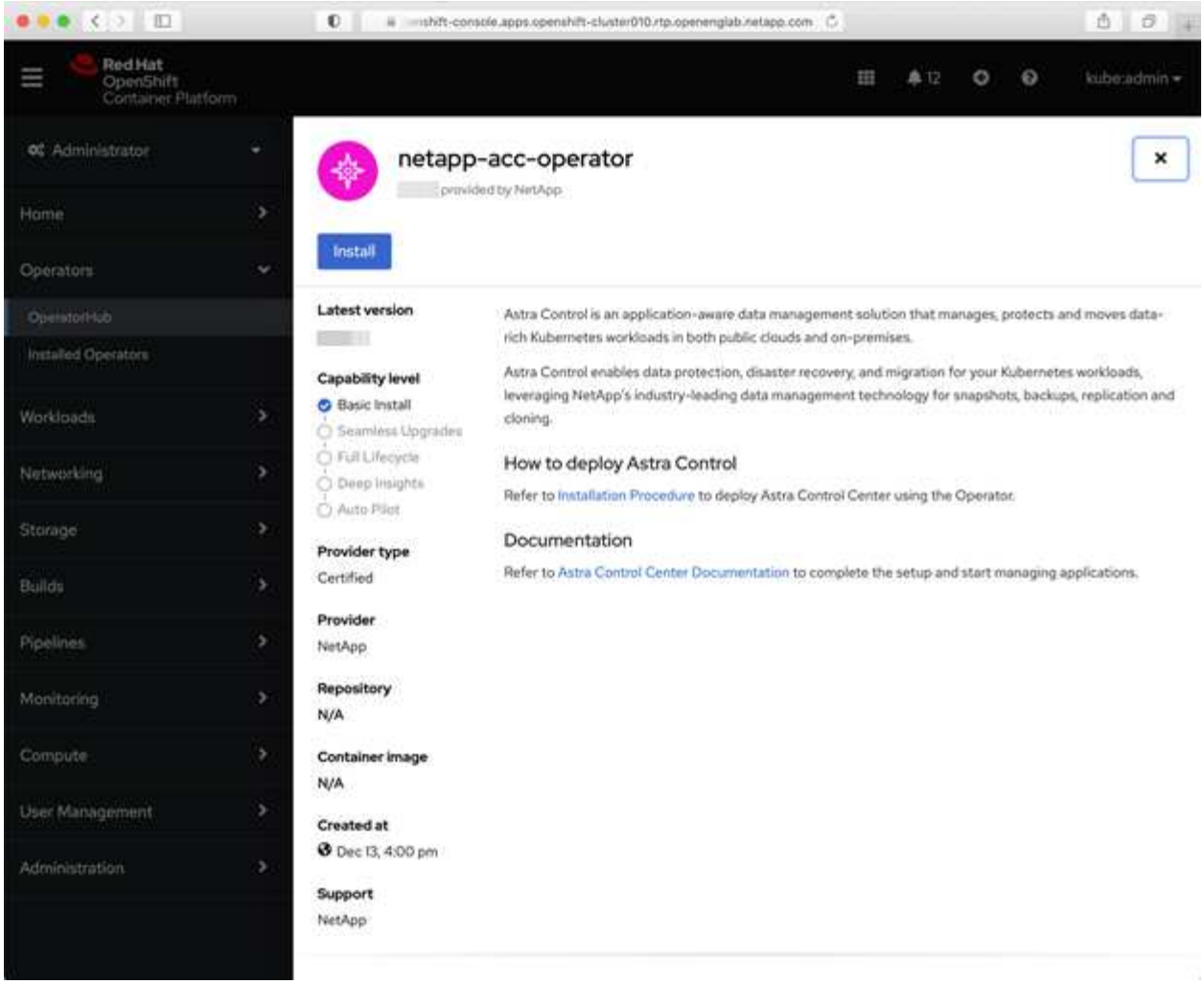
```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR_REGISTRY> como se indica en los comentarios:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Busque la página de instalación del operador

1. Realice uno de los siguientes procedimientos para acceder a la página de instalación del operador:
   - Desde la consola web de Red Hat OpenShift:



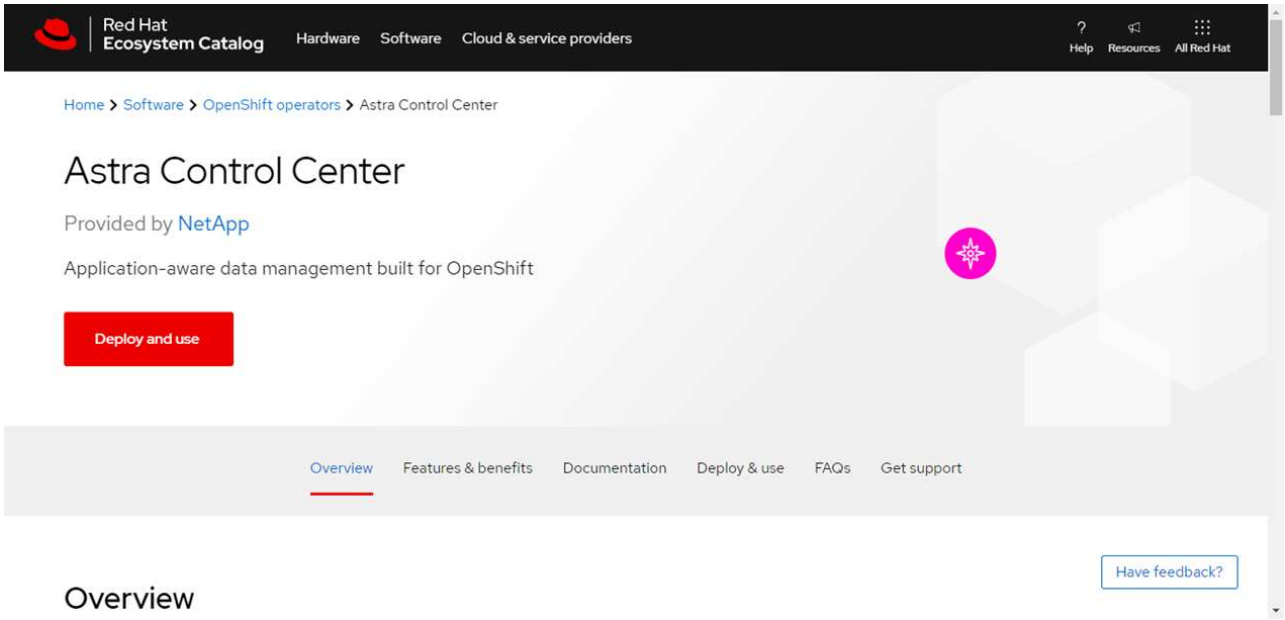
i. Inicie sesión en la IU de OpenShift Container Platform.

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

iii. Seleccione el operador NetApp Astra Control Center.

iv. Seleccione **instalar**.

- En el catálogo de ecosistemas de Red Hat:



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

ii. Seleccione **desplegar y utilizar**.

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. En la consola de la vista de detalles del operador del Centro de control de Astra, seleccione `Create instance` En la sección proporcionada API.

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

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

   b. (Opcional) Habilitar o deshabilitar AutoSupport. Se recomienda conservar la funcionalidad de AutoSupport.

c. Introduzca la dirección de Astra Control Center. No entre `http://` o. `https://` en la dirección.
d. Introduzca la versión de Astra Control Center; por ejemplo, 21.12.60.
e. Introduzca un nombre de cuenta, una dirección de correo electrónico y un apellido de administrador.
f. Conserve la política de reclamaciones de volumen predeterminada.
g. En **Registro de imágenes**, introduzca la ruta de registro de la imagen del contenedor local. No entre `http://` o. `https://` en la dirección.
h. Si utiliza un registro que requiere autenticación, introduzca el secreto.
i. Introduzca el nombre del administrador.
j. Configure el escalado de recursos.
k. Conserve la clase de almacenamiento predeterminada.
l. Defina las preferencias de manejo de CRD.

3. Seleccione `Create`.

El futuro

Compruebe que la instalación de Astra Control Center se ha realizado correctamente y complete el "pasos restantes" para iniciar sesión. Además, completará la implementación siguiendo este proceso "tareas de configuración".

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. Puede poner en marcha Astra Control Center en sus clústeres de Kubernetes en las instalaciones o en uno de los clústeres de Kubernetes autogestionados en el entorno de cloud.

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 poner en marcha Astra Control Center en AWS, necesitará 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 requieren entradas de zona alojada de AWS y ruta 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:

- OpenShift Container Platform de Red Hat 4.8

> 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 los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible
Nodos de trabajo (requisitos de AWS EC2)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento

Componente	Requisito
Registro de imágenes	Debe tener un registro privado existente, como AWS Elastic Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes. El clúster alojado de Astra Control Center y el clúster gestionado deben tener acceso al mismo registro de imágenes para poder realizar copias de seguridad y restaurar aplicaciones mediante la imagen basada en Restic.
Configuración de Astra Trident/ONTAP	Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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.

El token del registro de AWS caduca en 12 horas, después del cual deberá renovar el secreto del registro de imagen 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. Configure Cloud Manager de NetApp.
5. Instalar Astra Control Center.

Compruebe que dispone de suficientes permisos IAM

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

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 instancias de computación EC2, crear un bloque de AWS S3, crear un Elastic Container Register (ECR) para alojar las imágenes de Astra Control Center y empujar las imágenes a este registro.

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

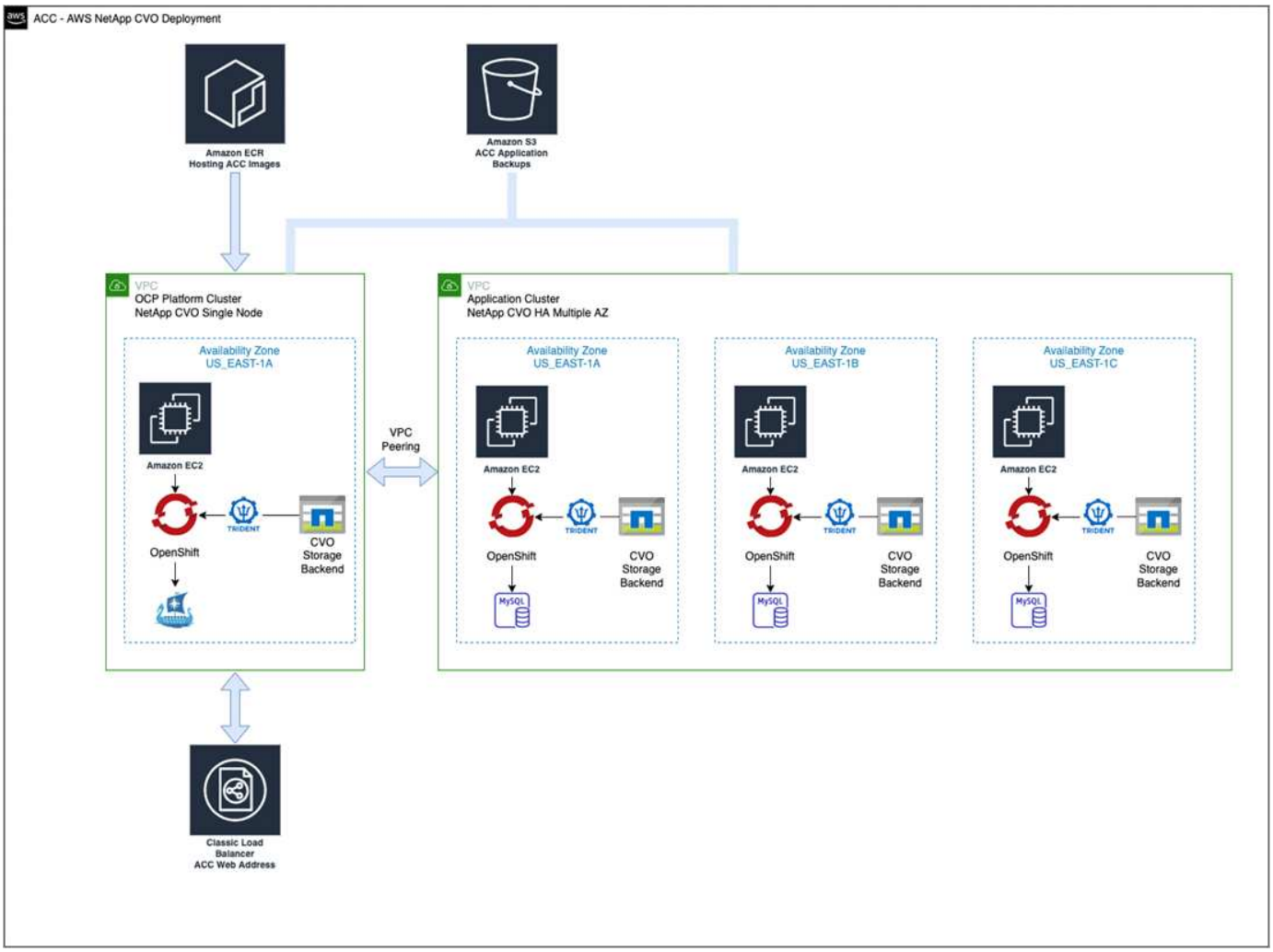
1. Cree una red virtual AWS.
2. Revise las instancias de computación EC2. Puede ser un servidor con configuración básica o máquinas virtuales en AWS.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia 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. Cree un AWS Elastic Container Registry (ECR) para alojar todas las imágenes ACC.

> 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.

6. Inserte las imágenes ACC en el 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:



Configure Cloud Manager de NetApp

Con 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 Cloud Manager para completar los siguientes pasos. Consulte lo siguiente:

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

Pasos

1. Añada sus credenciales a Cloud Manager.
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, tenga en cuenta la versión de Trident.

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. Trident 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.

Instalar Astra Control Center

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, necesitará 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 se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.10
- 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 los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible

Componente	Requisito
Nodos de trabajo (requisitos de computación de GCP)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN (ZONA DNS DE GCP)	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento
Registro de imágenes	Debe tener un registro privado existente, como Google Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes. Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.
Configuración de Astra Trident/ONTAP	Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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.

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. Configure Cloud Manager de NetApp.
6. Instalar y configurar Astra Control Center.

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 para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "Credenciales y permisos iniciales de GCP".

Configure GCP

A continuación, configure GCP para crear un VPC, configure instancias de computación, cree un almacenamiento de objetos de Google Cloud, cree un Registro de contenedor de Google para alojar las imágenes de Astra Control Center y empuje las imágenes a 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. Cree un registro de Google Container para alojar todas las imágenes de Astra Control Center.
7. 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 ACC se pueden insertar en este registro introduciendo la siguiente secuencia de comandos:

   ```
   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=astra-control-center-<version>.manifest
   GCP_CR_REGISTRY=<target image repository>
   ASTRA_REGISTRY=<source ACC image repository>

   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 < astra-control-center-22.04.41.manifest
   ```

8. Configure zonas DNS.

Configure Cloud Manager de NetApp

Con 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 Cloud Manager para completar los siguientes pasos. Consulte "Introducción a Cloud Volumes ONTAP en GCP".

Lo que necesitará

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

Pasos

1. Añada sus credenciales a Cloud Manager. 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 Cloud Manager".

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, tenga en cuenta la versión de Trident.

   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. Trident 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.

Instalar Astra Control Center

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 poner en marcha Astra Control Center en Azure, necesitará 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 se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.8
- 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 los siguientes recursos además de los requisitos de recursos del entorno:

Consulte "Requisitos del entorno operativo del Centro de control de Astra".

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible
Nodos de trabajo (requisitos de computación de Azure)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN (zona DNS de Azure)	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Como back-end de almacenamiento, se usará Astra Trident 21.04 o posterior instalado y configurado, y NetApp ONTAP versión 9.5 o posterior
Registro de imágenes	Debe disponer de un registro privado existente, como Azure Container Registry (ACR), al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes. Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.

Componente	Requisito
Configuración de Astra Trident/ONTAP	Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

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.

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. Configure Cloud Manager de NetApp.
6. Instalar y configurar Astra Control Center.

Instale un clúster RedHat OpenShift en Azure

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

Para obtener instrucciones de instalación, consulte la documentación de RedHat en "Instalación del clúster OpenShift en Azure" y.. "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 de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "Credenciales y permisos de Azure".

Configure Azure

A continuación, configure Azure para crear una red virtual, configurar instancias de computación, crear un contenedor de Azure Blob, crear un registro de contenedores de Azure (ACR) para alojar las imágenes de Astra Control Center y colocar 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. Necesitará una cuenta de almacenamiento para crear un contenedor que se utilizará como bloque en Astra Control Center.
6. Crear un secreto, que es necesario para el acceso a bloques.
7. Cree un Azure Container Registry (ACR) para alojar todas las imágenes de Astra Control Center.
8. Configure el acceso ACR para pulsar/extraer todas las imágenes del Centro de control de Astra.
9. Inserte las imágenes ACC en este registro introduciendo el siguiente script:

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

   Ejemplo:

```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

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 $AZ_ACR_REGISTRYY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Configure zonas DNS.

Configure Cloud Manager de NetApp

Con 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 Cloud Manager para completar los siguientes pasos. Consulte "Introducción a Cloud Manager en Azure".

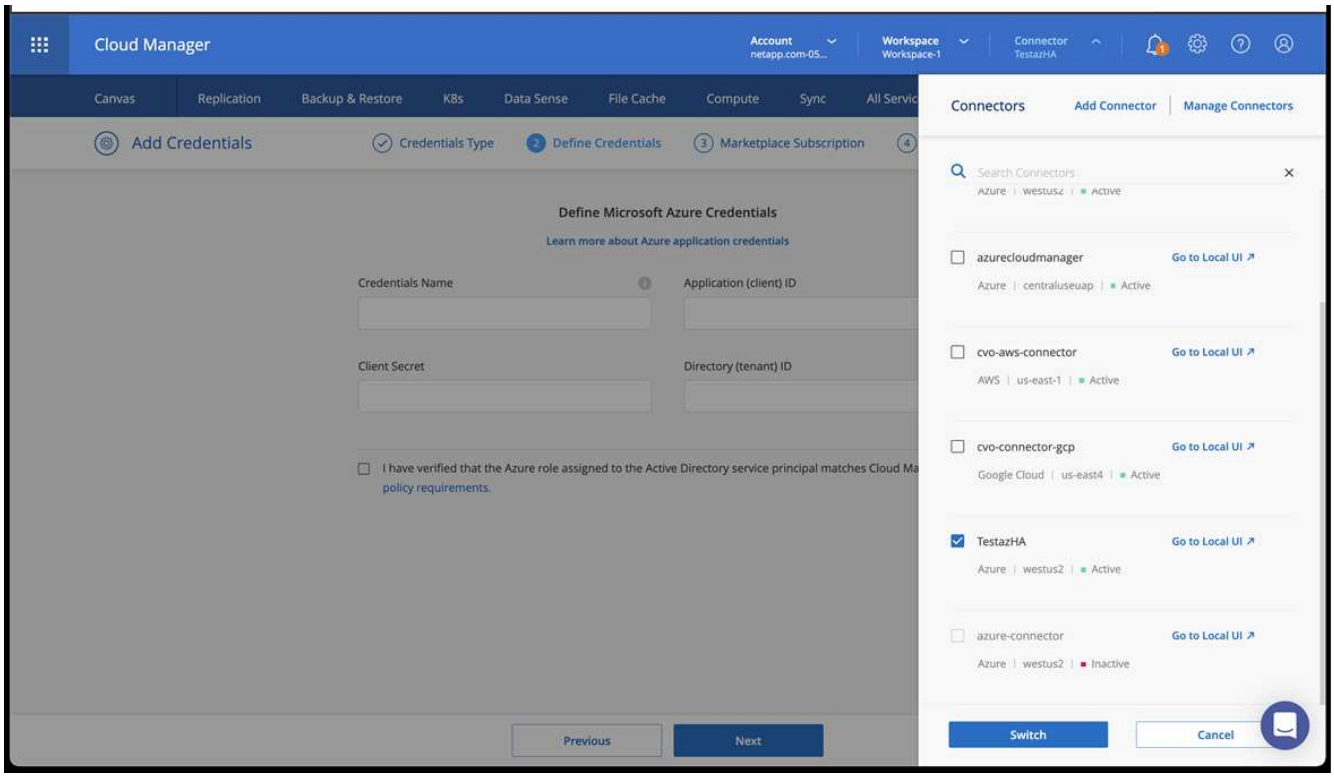
Lo que necesitará

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

Pasos

1. Añada sus credenciales a Cloud Manager.
2. Agregue un conector para Azure. Consulte "Políticas de Cloud Manager".
   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).

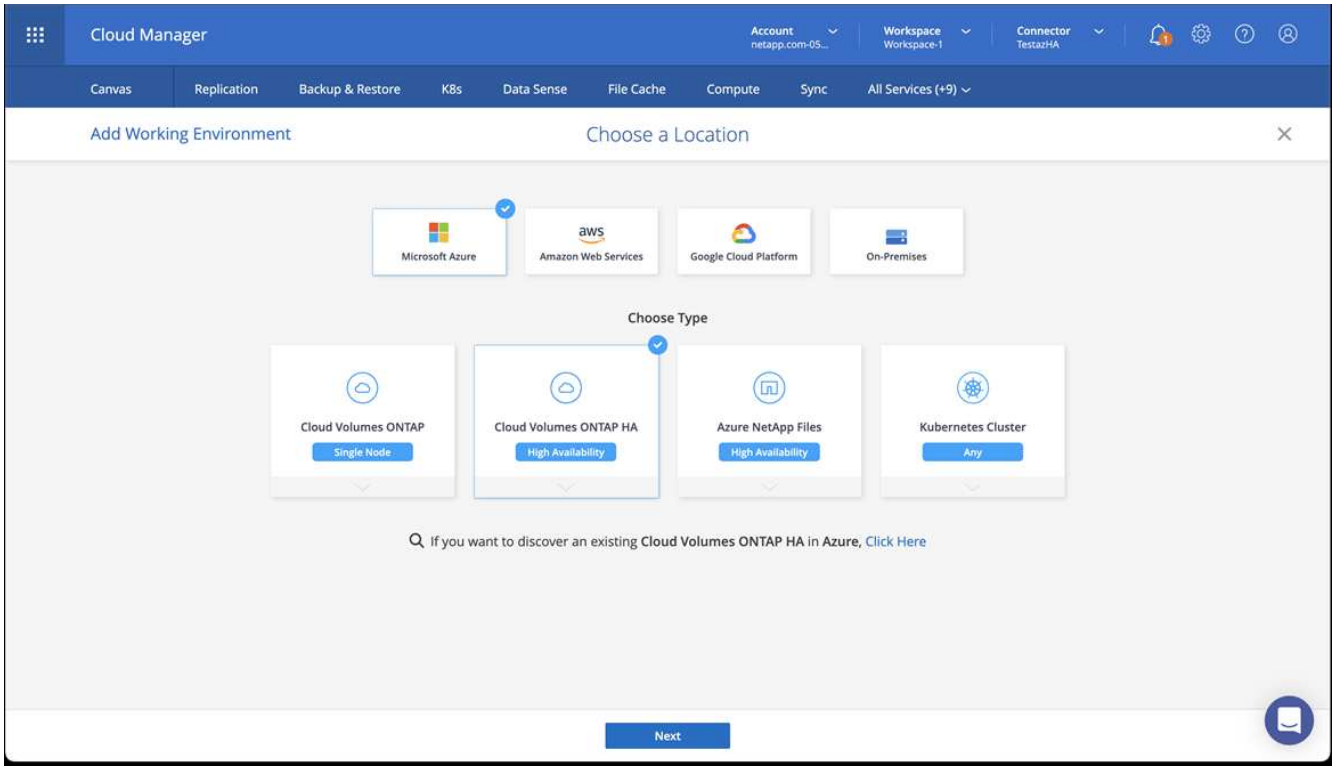
      Consulte "Crear un conector en Azure desde Cloud Manager".
3. Asegúrese de que el conector está en marcha y cambie a dicho conector.



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

   a. Ubicación: "Microsoft Azure".

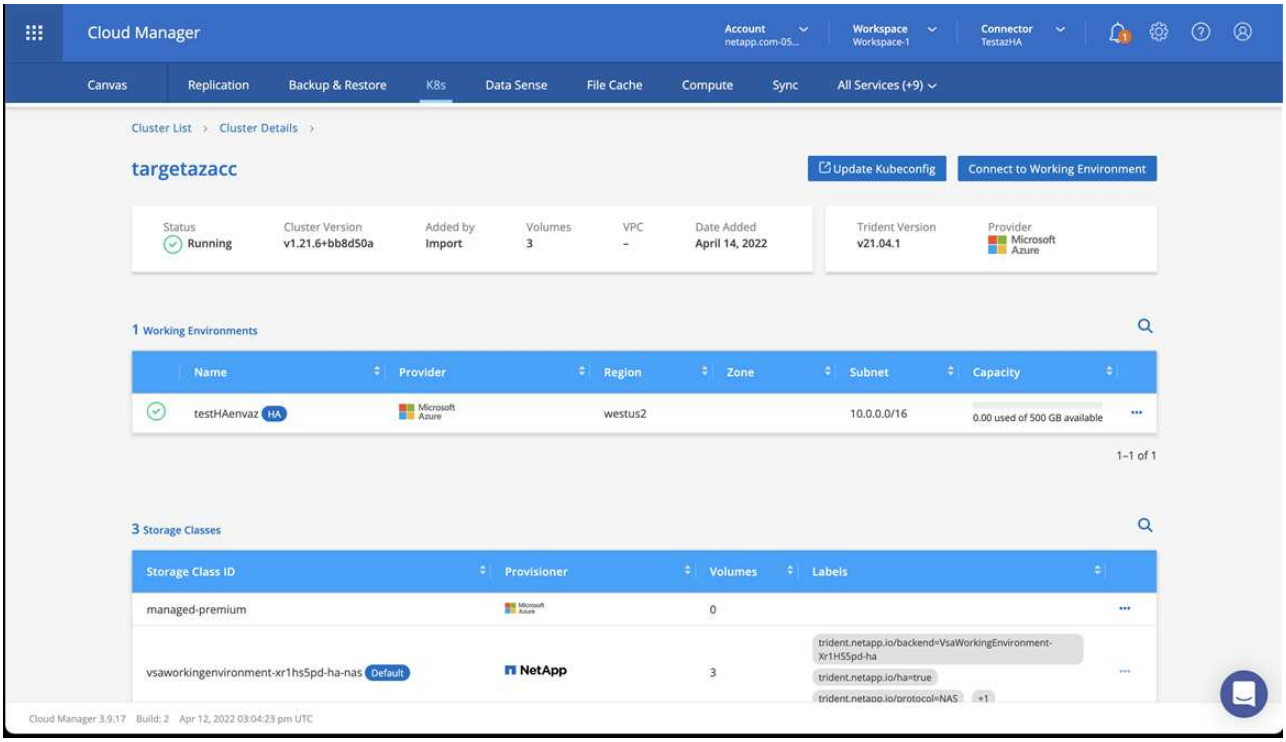
   b. Tipo: "Cloud Volumes ONTAP ha".



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, tenga en cuenta la versión de Trident.

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. Trident 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

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".

Configure Astra Control Center

Astra Control Center admite y supervisa ONTAP y Astra Data Store como back-end de almacenamiento. Después de instalar Astra Control Center, inicie sesión en la interfaz de usuario y cambie la contraseña, le interesa configurar una licencia, añadir clústeres, gestionar el almacenamiento y añadir bloques.

Tareas

- Agregue una licencia de Astra Control Center

- Añada el clúster
- Añada un back-end de almacenamiento
- Añadir un bucket

Agregue una licencia de Astra Control Center

Puede añadir una licencia nueva con la interfaz de usuario o. "API" Para obtener todas las funciones de Astra Control Center. Sin una licencia, el uso de Astra Control Center se limita a gestionar usuarios y agregar nuevos clústeres.

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

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

Las licencias de Astra Control Center miden los recursos de CPU mediante unidades de CPU de Kubernetes. La licencia debe tener en cuenta los recursos de CPU asignados a los nodos de trabajo de todos los clústeres de Kubernetes gestionados. Antes de agregar una licencia, debe obtener el archivo de licencia (NLF) de "Sitio de soporte de NetApp".

También puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Puede inscribirse para obtener una prueba gratuita registrándose "aquí".

> 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.

Lo que necesitará

Al descargar Astra Control Center desde "Sitio de soporte de NetApp"También puede descargar el archivo de licencia de NetApp (NLF). Asegúrese de tener acceso a este archivo de licencia.

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 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.

Añada el 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. Para Astra Data Store, queremos añadir el clúster de aplicaciones Kubernetes que contiene aplicaciones que utilizan volúmenes aprovisionados por Astra Data Store.

> 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. Puede utilizar la función **Agregar clúster** para administrar un clúster con Astra Control Center.

> Cuando Astra Control gestiona un clúster, realiza un seguimiento de la clase de almacenamiento predeterminada del clúster. Si cambia la clase de almacenamiento con `kubectl` Comandos, Control Astra revierte el cambio. Para cambiar la clase de almacenamiento predeterminada de un clúster gestionado por Astra Control, utilice uno de los siguientes métodos:
>
> - Utilice la API Astra Control `PUT /managedClusters` asimismo, asigne una clase de almacenamiento predeterminada diferente con el `DefaultStorageClass` parámetro.
> - Utilice la interfaz de usuario web de Astra Control para asignar una clase de almacenamiento predeterminada diferente. Consulte Cambie la clase de almacenamiento predeterminada.

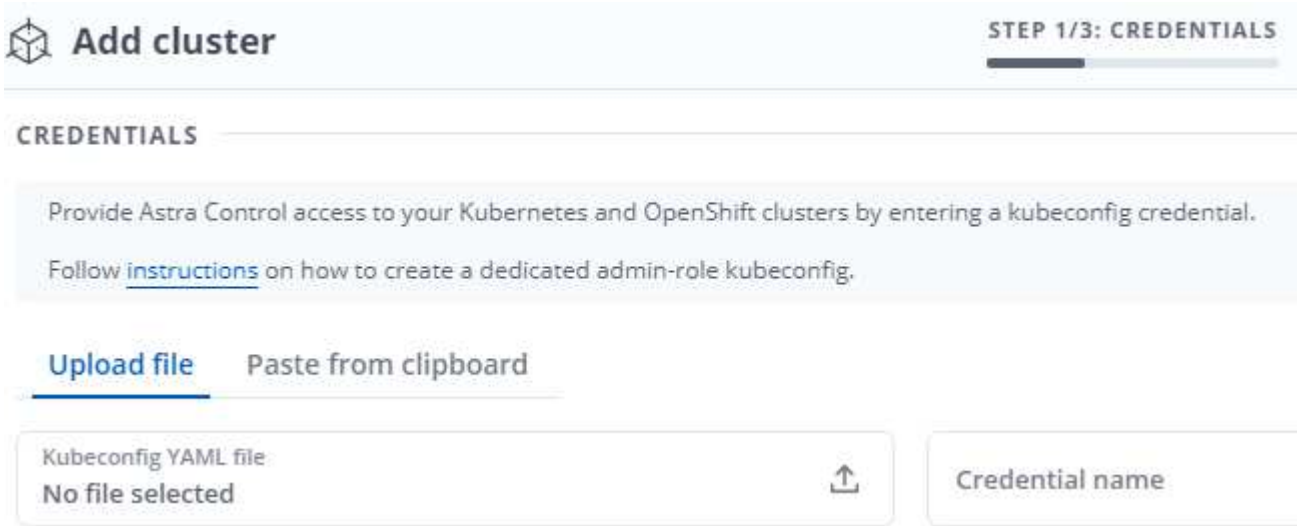
Lo que necesitará

- Antes de añadir un clúster, revise y realice la operación necesaria "requisitos previos".

Pasos

1. En **Dashboard** de la interfaz de usuario de Astra Control Center, seleccione **Agregar** en la sección Clusters.
2. En la ventana **Agregar clúster** que se abre, cargue un `kubeconfig.yaml` archivar o pegar el contenido de un `kubeconfig.yaml` archivo.

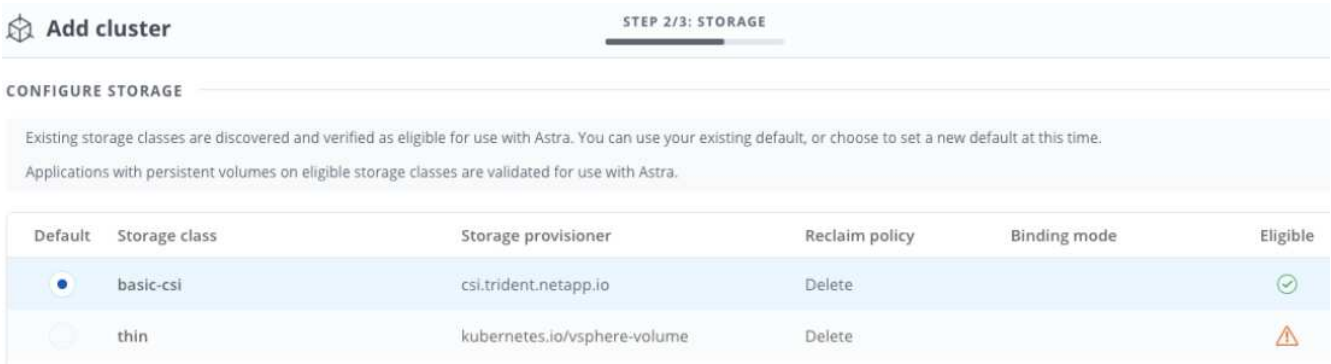
> La `kubeconfig.yaml` el archivo debe incluir **sólo la credencial de cluster para un cluster**.



> 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.

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

> Debe seleccionar una clase de almacenamiento de Trident con el respaldo del almacenamiento de ONTAP o el almacén de datos Astra.



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

Resultado

El clúster entra en el estado **detectando** y luego cambia a **ejecutando**. Ha añadido correctamente un clúster de Kubernetes y ahora lo gestiona en 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. Deberá consultar los registros del operador de supervisión para depurar el problema.

Añada un back-end de almacenamiento

Puede añadir un back-end de almacenamiento para que Astra Control pueda gestionar sus recursos. Es posible poner en marcha un back-end de almacenamiento en un clúster gestionado o utilizar un back-end de almacenamiento existente.

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.

Lo que necesitará para las puestas en marcha existentes de Astra Data Store

- Ha añadido el clúster de aplicaciones de Kubernetes y el clúster de computación subyacente.

> Después de añadir su clúster de aplicaciones Kubernetes para Astra Data Store y lo gestiona Astra Control, el clúster aparece como `unmanaged` en la lista de back-ends detectados. A continuación, debe añadir el clúster informático que contiene Astra Data Store y es la base para el clúster de aplicaciones de Kubernetes. Puede hacerlo desde **Backends** en la interfaz de usuario. Seleccione el menú Actions para el clúster, seleccione `Manage`, y. "añada el clúster". Tras el estado del clúster de `unmanaged` Los cambios en el nombre del clúster de Kubernetes, puede continuar con la adición de un back-end.

Lo que necesitará para las nuevas puestas en marcha de Astra Data Store

- Ya tienes "ha cargado la versión del paquete de instalación que pretende implementar" A una ubicación accesible a Astra Control.
- Añadió el clúster Kubernetes que pretende usar para la implementación.
- Ha cargado el Licencia de Astra Data Store Para su implementación en una ubicación a la que pueda acceder Astra Control.

Opciones

- Instale recursos de almacenamiento
- Utilice un back-end de almacenamiento existente

Instale recursos de almacenamiento

Puede poner en marcha un nuevo almacén de datos de Astra y gestionar el back-end de almacenamiento asociado.

Pasos

1. Navegue desde el panel o el menú backends (backends):
   - En **Dashboard**: En el Resumen de recursos, seleccione un enlace del panel Storage Backends y seleccione **Add** en la sección Backends.
   - Desde **Backends**:
     i. En el área de navegación de la izquierda, seleccione **Backends**.
     ii. Seleccione **Agregar**.
2. Seleccione la opción de implementación **Astra Data Store** en la ficha **despliegue**.
3. Seleccione el paquete Astra Data Store para implementar:
   a. Introduzca un nombre para la aplicación Astra Data Store.
   b. Elija la versión de Astra Data Store que desea implementar.

   > Si todavía no ha cargado la versión que pretende implementar, puede utilizar la opción **Agregar paquete** o salir del asistente y utilizar "gestión de paquetes" para cargar el paquete de instalación.

4. Seleccione una licencia de Astra Data Store que haya cargado previamente o utilice la opción **Agregar licencia** para cargar una licencia para usar con la aplicación.

> Las licencias de Astra Data Store con permisos completos están asociadas con el clúster de Kubernetes y estos clústeres asociados deben aparecer automáticamente. Si no hay un clúster gestionado, puede seleccionar la opción **Agregar un clúster** para agregar uno a la administración de Astra Control. Para las licencias de Astra Data Store, si no se ha establecido ninguna asociación entre la licencia y el clúster, puede definir esta asociación en la siguiente página del asistente.

5. Si no ha añadido un clúster Kubernetes a Astra Control Management, debe hacerlo desde la página **Kubernetes Cluster**. Seleccione un clúster existente de la lista o seleccione **agregue el clúster subyacente** para agregar un clúster a Astra Control Management.
6. Seleccione un tamaño de plantilla para el clúster de Kubernetes que proporcione recursos para el almacén de datos Astra. Puede elegir una de las siguientes opciones:
   - Si lo desea `Recommended Kubernetes worker node requirements`, seleccione una plantilla de grande a pequeña en función de lo que permita su licencia.
   - Si lo desea `Custom Kubernetes worker node requirements`, seleccione el número de núcleos y la memoria total que desea para cada nodo del clúster. También se puede mostrar el número de nodos elegibles del clúster que cumplen con los criterios de selección de los núcleos y la memoria.

> Al seleccionar una plantilla, seleccione nodos más grandes con más memoria y núcleos para cargas de trabajo más grandes o un mayor número de nodos para cargas de trabajo más pequeñas. Debe seleccionar una plantilla en función de lo que permita su licencia. Cada opción de plantilla recomendada sugiere el número de nodos elegibles que cumplen con el patrón de plantilla para la memoria y los núcleos y la capacidad de cada nodo.

7. Configure los nodos:
   a. Agregue una etiqueta de nodo para identificar el pool de nodos de trabajo que admiten este clúster de almacén de datos Astra.

> Debe añadirse la etiqueta a cada nodo individual del clúster que se utilizará para la puesta en marcha de Astra Data Store antes de que falle el inicio de la implementación o la implementación.

   b. Configure la capacidad (GIB) por nodo manualmente o seleccione la capacidad máxima permitida de nodo.
   c. Configure un número máximo de nodos permitidos en el clúster o permita el número máximo de nodos en el clúster.
8. (Sólo licencias completas del almacén de datos Astra) Introduzca la clave de la etiqueta que desea utilizar para los dominios de protección.

> Cree al menos tres etiquetas únicas para la clave de cada nodo. Por ejemplo, si la clave es `astra.datastore.protection.domain`, puede crear las siguientes etiquetas: `astra.datastore.protection.domain=domain1`,`astra.datastore.protection.domain=domain2`, y. `astra.datastore.protection.domain=domain3`.

9. Configure la red de administración:
   a. Introduzca una dirección IP de gestión para la gestión interna de Astra Data Store que se encuentra en la misma subred que las direcciones IP de nodos de trabajo.

b. Elija utilizar el mismo NIC tanto para la administración como para las redes de datos o configúrelo por separado.

c. Introduzca el pool de direcciones IP de red de datos, la máscara de subred y la puerta de enlace para acceder al almacenamiento.

10. Revise la configuración y seleccione **despliegue** para comenzar la instalación.

Resultado

Tras una instalación correcta, el back-end aparece en `available` estado en la lista de los back-ends, junto con información de rendimiento activa.

> Es posible que deba actualizar la página para que se muestre el back-end.

Utilice un back-end de almacenamiento existente

Puede traer un back-end de almacenamiento de ONTAP o Astra Data Store al centro de control de Astra.

Pasos

1. Navegue desde el panel o el menú backends (backends):
   - En **Dashboard**: En el Resumen de recursos, seleccione un enlace del panel Storage Backends y seleccione **Add** en la sección Backends.
   - Desde **Backends**:
     i. En el área de navegación de la izquierda, seleccione **Backends**.
     ii. Seleccione **gestionar** en un back-end detectado desde el clúster administrado o seleccione **Agregar** para administrar un back-end existente adicional.
2. Seleccione la ficha **utilizar existente**.
3. Realice una de las siguientes acciones según el tipo de backend:
   - **Almacén de datos Astra**:
     i. Seleccione **Astra Data Store**.
     ii. Seleccione el clúster de cálculo administrado y seleccione **Siguiente**.
     iii. Confirme los detalles del backend y seleccione **Agregar backend de almacenamiento**.
   - **ONTAP**:
     i. Seleccione **ONTAP** y seleccione **Siguiente**.
     ii. Introduzca la dirección IP de gestión del clúster de ONTAP y las credenciales de administrador.

     > 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, habilite los métodos de acceso `ontapi` y.. `http` Para el usuario en ambos clústeres de ONTAP. Consulte "Gestionar cuentas de usuario" si quiere más información.

     iii. Seleccione **Revisión**.
     iv. Confirme los detalles del backend y seleccione **Agregar backend de almacenamiento**.

Resultado

El back-end aparece en `available` estado en la lista con información resumida.

Es posible que deba actualizar la página para que se muestre el back-end.

Añadir un bucket

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.

Cuando se agrega un bloque, Astra Control Marca un bloque como el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado.

No necesita un bucket si va a clonar la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster.

Utilice cualquiera de los siguientes tipos de bloques:

- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp
- Genérico S3

  Amazon Web Services (AWS) y Google Cloud Platform (GCP) utilizan el tipo de bloque Generic S3.

- Microsoft Azure

  Aunque Astra Control Center es compatible con Amazon S3 como proveedor de cubos de S3 genérico, Astra Control Center podría no admitir todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

- Microsoft Azure

Para obtener instrucciones sobre cómo añadir cubos con la API Astra Control, consulte "Información sobre API y automatización de Astra".

Pasos

1. En el área de navegación de la izquierda, seleccione **Cuchos**.
   a. Seleccione **Agregar**.
   b. 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.

   c. Cree un nuevo nombre de bloque o introduzca un nombre de bloque existente y una descripción opcional.

> El nombre del bloque y la descripción aparecen como una ubicación de copia de seguridad que puede elegir más tarde al crear una copia de seguridad. El nombre también aparece durante la configuración de la política de protección.

d. Introduzca el nombre o la dirección IP del extremo de S3.

e. Si desea que este bloque sea el bloque predeterminado para todos los backups, compruebe la `Make this bucket the default bucket for this private cloud` opción.

> Esta opción no aparece para el primer bloque que cree.

f. Continúe añadiendo información sobre credenciales.

Añada credenciales de acceso de S3

Añada credenciales de acceso de S3 en cualquier momento.

Pasos

1. En el cuadro de diálogo Cuchos, seleccione la ficha **Agregar** o **utilizar existente**.
   a. Introduzca un nombre para la credencial que la distingue de otras credenciales en Astra Control.
   b. Escriba el identificador de acceso y la clave secreta pegando el contenido del portapapeles.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

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**.

El futuro

Ahora que ha iniciado sesión y agregado clústeres a Astra Control Center, está listo para empezar a utilizar las funciones de gestión de datos de aplicaciones de Astra Control Center.

- "Gestionar usuarios"
- "Inicie la gestión de aplicaciones"
- "Proteja sus aplicaciones"
- "Clone aplicaciones"
- "Gestionar notificaciones"
- "Conéctese a Cloud Insights"
- "Agregue un certificado TLS personalizado"

Obtenga más información

- "Utilice la API Astra Control"
- "Problemas conocidos"

Requisitos previos para añadir un clúster

Debe asegurarse de que se cumplan las condiciones previas antes de añadir un clúster. También debe ejecutar las comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

Qué necesitará antes de añadir un clúster

Asegúrese de que su clúster cumpla los requisitos descritos en "Requisitos del clúster de aplicaciones".

> Si tiene pensado añadir un segundo clúster OpenShift 4.6, 4.7 o 4.8 como un recurso informático gestionado, debe asegurarse de que la función de Snapshot de volumen de Astra Trident esté habilitada. Consulte la Astra Trident oficial "instrucciones" Para habilitar y probar Volume Snapshots con Astra Trident.

- Clases de almacenamiento de Astra Trident configuradas con un "back-end de almacenamiento admitido" (necesario para cualquier tipo de clúster)
- El superusuario y el ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center. Ejecute el siguiente comando en la línea de comandos de la ONTAP:
  `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Una Astra Trident `volumesnapshotclass` objeto definido por un administrador. Vea la Astra Trident "instrucciones" Para habilitar y probar Volume Snapshots con Astra Trident.
- Compruebe que solo tiene una única clase de almacenamiento predeterminada definida para el clúster de Kubernetes.

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. Compruebe la versión de Trident.

   ```
   kubectl get tridentversions -n trident
   ```

   Si Trident existe, se muestra una salida similar a la siguiente:

   ```
   NAME       VERSION
   trident    21.04.0
   ```

   Si Trident no existe, se muestra un resultado similar al siguiente:

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

> Si Trident no está instalado o la versión instalada no es la más reciente, debe instalar la versión más reciente de Trident antes de continuar. Consulte "Documentación de Trident" si desea obtener instrucciones.

2. Compruebe si las clases de almacenamiento están usando los controladores de Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get sc
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
thin                    kubernetes.io/vsphere-volume   Delete
Immediate           false                  6d
```

Cree una imagen de rol administrativo

Asegúrese de que dispone de lo siguiente en su máquina antes de realizar los pasos siguientes:

- `kubectl` v1.19 o posterior instalado
- Una imagen marcada activa con los derechos de administrador del clúster para el contexto activo

Pasos

1. Cree una cuenta de servicio del siguiente modo:

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

      Ajuste el nombre y el espacio de nombres según sea necesario. Si se realizan cambios aquí, debe aplicar los mismos cambios en los pasos siguientes.

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

+

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

   a. Aplicar la cuenta de servicio:

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

2. (Opcional) Si el clúster utiliza una directiva de seguridad de POD restrictiva que no permite la creación de POD privilegiadas o permite que los procesos dentro de los contenedores Pod se ejecuten como usuario raíz, cree una directiva de seguridad de POD personalizada para el clúster que permita a Astra Control crear y administrar POD. Para ver instrucciones, consulte "Cree una directiva de seguridad de POD personalizada".
3. Conceda permisos de administrador del clúster de la siguiente manera:

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

      Ajuste los nombres y espacios de nombres modificados al crear la cuenta de servicio según sea necesario.

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

+

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

   a. Aplique el enlace de roles del clúster:

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

4. 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-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-vhz87` sería 0 y el índice para `astracontrol-service-account-token-r59kr` sería 1. En la salida, anote el índice del nombre de la cuenta de servicio que contiene la palabra "token".

5. Genere la kubeconfig de la siguiente manera:

   a. Cree un `create-kubeconfig.sh` archivo. 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
```

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

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

6. (**opcional**) cambie el nombre de la kubeconfig por un nombre significativo para el clúster. Proteja las credenciales del clúster.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```

El futuro

Ahora que ha comprobado que se cumplen los requisitos previos, está listo "añadir un clúster".

Obtenga más información

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

Agregue un certificado TLS personalizado

Puede quitar el certificado TLS autofirmado existente y reemplazarlo con un certificado TLS firmado por una entidad de certificación (CA).

Lo que necesitará

- 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>
```

Añadir un nuevo certificado

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>
....

#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>
....

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:

```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #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>
....

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 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.containo.us -n <ACC-deployment-
namespace>
....

# tls:
#    options:
#      name: default
#    secretName: secure-testing-cert
#    store:
#      name: default

 tls:
    options:
      name: default
    secretName: <certificate-secret-name>
    store:
      name: default
```

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

Cree una directiva de seguridad de POD personalizada

Astra Control debe crear y gestionar pods de Kubernetes en los clústeres que gestiona. Si el clúster utiliza una directiva de seguridad de POD restrictiva que no permite la creación de POD con privilegios ni permite que los procesos dentro de los contenedores Pod se ejecuten como usuario raíz, debe crear una directiva de seguridad de POD menos restrictiva para permitir que Astra Control cree y administre estas POD.

Pasos

1. Cree una directiva de seguridad de POD para el clúster que sea menos restrictiva que la predeterminada y guárdela en un archivo. Por ejemplo:

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. Cree un nuevo rol para la política de seguridad del pod.

```bash
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. Vincule el nuevo rol a la cuenta de servicio.

```bash
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

Preguntas frecuentes para Astra Control Center

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

- ¿Cuál es la URL de Astra Control?*

Astra Control Center utiliza autenticación local y una dirección URL específica para cada entorno.

Para la dirección URL, en un explorador, introduzca el nombre de dominio completo (FQDN) establecido en el campo spec.astraAddress del archivo astra_control_Center_min.yaml custom resource definition (CRD) 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_min.ylma CRD.

Licencia

Estoy utilizando la licencia de Evaluación. ¿Cómo puedo cambiar a la licencia completa?

Si desea cambiar fácilmente a una licencia completa, obtenga el archivo de licencia de NetApp (NLF).

- Pasos*
- En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
- Seleccione **Agregar licencia**.
- Busque el archivo de licencia que ha descargado y seleccione **Agregar**.

Estoy utilizando la licencia de Evaluación. ¿Puedo seguir gestionando aplicaciones?

Sí, puede comprobar la funcionalidad de administración de aplicaciones con la licencia de evaluación.

Registrar clústeres de Kubernetes

Necesito añadir nodos de trabajo a mi clúster Kubernetes después de añadir 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 descontrolo 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 eliminar el clúster 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.

- ¿Trident de NetApp se desinstala automáticamente de un clúster cuando lo descontrolo?* cuando se desvincula un clúster de Astra Control Center, Trident no se desinstala automáticamente del clúster. Para desinstalar Trident, tendrá que hacerlo "Siga estos pasos en la documentación de Trident".

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 administrarlas 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 utiliza un almacenamiento que no sea de NetApp?

No Aunque Astra Control puede detectar aplicaciones que utilizan almacenamiento de terceros, no puede gestionar una aplicación que utilice almacenamiento de terceros.

¿Debo administrar Astra Control mismo? no, no debería gestionar Astra Control por sí mismo porque es una "app del sistema".

¿Afectan los POD que no son saludables a la gestión de aplicaciones? Si una aplicación gestionada tiene pods en estado incorrecto, Astra Control no puede crear nuevos backups y clones.

Operaciones de gestión de datos

- hay instantáneas en mi cuenta que no creé. ¿de dónde vienen?*

En algunas situaciones, Astra Control creará automáticamente una instantánea como parte de un proceso de backup, clonado o restauración.

Mi aplicación utiliza varios VP. ¿Tomará Astra Control instantáneas y copias de seguridad de todas estas EVs?

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 las instantáneas tomadas por Astra Control directamente a través de una interfaz o almacenamiento de objetos diferente?

No Las copias Snapshot y las copias de seguridad realizadas por Astra Control solo se pueden gestionar con

Astra Control.

Utilice Astra

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 empezar a gestionar las aplicaciones y sus recursos.

Para obtener más información, consulte "Requisitos de gestión de aplicaciones".

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. La gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. 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 diseñados con una arquitectura de "paso por valor" en lugar de "paso por referencia". Un operador y la aplicación que instale deben usar el mismo espacio de nombres; es posible que deba modificar el archivo .yaml de despliegue para que el operador se asegure de que así sea.

  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. Se puede gestionar cualquier aplicación que esté delimita a un espacio de nombres único.

Gestionar aplicaciones

Una vez que Astra Control detecta espacios de nombres en sus clústeres, puede definir las aplicaciones que desea administrar. Puede elegir "gestione un espacio de nombres completo como una única aplicación o gestione una o varias aplicaciones en el espacio de nombres de forma individual". Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Aunque Astra Control permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones de ese espacio de nombres), la mejor práctica 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.

Lo que necesitará

- 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.
- Uno o más pods activos.
- Espacios de nombres especificados en el clúster Kubernetes que se agregó a Astra Control.
- Etiqueta de Kubernetes (opcional) 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".

Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".

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

Opciones de gestión de aplicaciones adicionales

- Desgestionar aplicaciones

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. Obtenga más información acerca de las prácticas recomendadas.

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. Seleccione el espacio de nombres de la aplicación en la lista desplegable **espacio de nombres**.

   > Las aplicaciones solo se pueden definir dentro de un espacio de nombres especificado en un único clúster. Astra Control no admite la capacidad de que las aplicaciones abarquen varios espacios de nombres o clústeres.

5. Introduzca una etiqueta para la aplicación y el 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. Después de seleccionar **definir**, repita el proceso para otras aplicaciones, según sea necesario.

Cuando termine de definir una aplicación, ésta aparecerá 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.

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 gestionar varios espacios de nombres, seleccione los espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **gestionar**.

> 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. Show system namespaces "Leer más".

Una vez completado el proceso, las aplicaciones asociadas al espacio de nombres aparecen en la `Associated applications` columna.

Desgestionar aplicaciones

Cuando ya no desee realizar una copia de seguridad, una instantánea o clonar una aplicación, puede dejar de administrarla.

> Si desgestiona una aplicación, se perderán todos los backups o las instantáneas que se hayan creado anteriormente.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione la aplicación.
3. En el menú de la columna **acciones**, seleccione **Unmanage**.
4. Revise la información.
5. Escriba "desgestionar" para confirmar.
6. Seleccione **Sí, Desactivar aplicación**.

¿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** .

Show system namespaces

> Astra Control en sí no es una aplicación estándar; es una "aplicación del sistema". No debe intentar gestionar Astra Control por sí mismo. Astra Control no se muestra de forma predeterminada para la gestión.

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"

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 o. "La API de control Astra" para proteger aplicaciones.

Si utiliza Helm para implantar 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.

Al crear 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
```

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
- 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

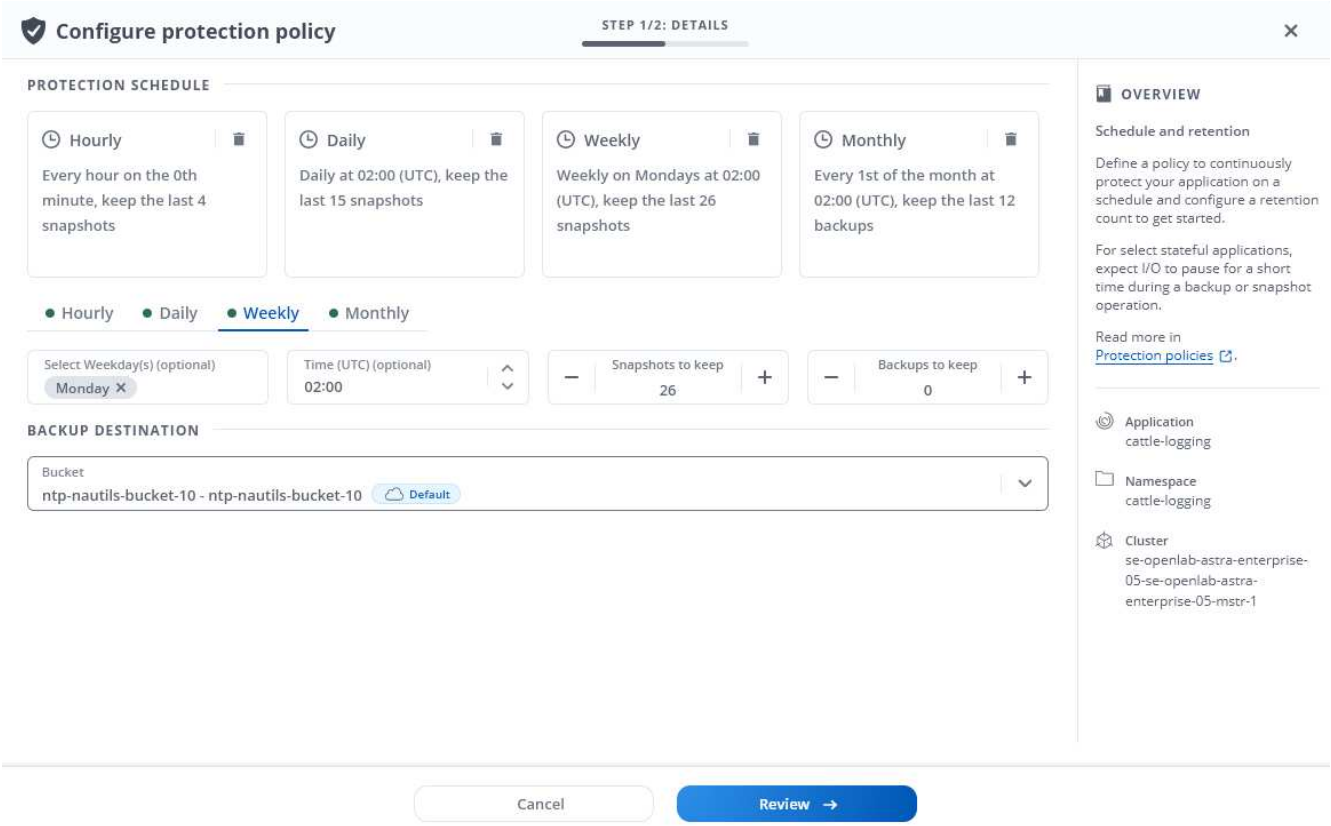
especificar la cantidad de copias que desea retener. A modo de ejemplo, una política de protección puede crear backups semanales y copias Snapshot diarias, y conservar los backups y las copias Snapshot por un mes. La frecuencia con la que se crean snapshots y backups y el tiempo que se retienen depende de las necesidades de la organización.

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.

   En el siguiente ejemplo, se establecen cuatro programaciones de protección: Por hora, día, semana y mes para las copias Snapshot y los backups.



5. Seleccione **Revisión**.
6. Seleccione **Configurar política de protección.**

Resultado

Astra Control Center implementa la normativa de protección de datos mediante la creación y retención de instantáneas y copias de seguridad con la programación y retención que ha definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

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 **Revisión**.
4. Revise el resumen de la instantánea y seleccione **Snapshot**.

Resultado

Se inicia el proceso Snapshot. Una instantánea se realiza correctamente cuando el estado es **disponible** en la columna **acciones** de la página **Protección de datos** > **instantáneas**.

Cree un backup

También puede realizar copias de seguridad de una aplicación en cualquier momento.

> 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.

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 destino para el backup seleccionando de la lista de bloques de almacenamiento.
6. Seleccione **Revisión**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control Center 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.

> No existe ninguna forma de detener un backup en ejecución. Si necesita eliminar el backup, espere hasta que se haya completado y, a continuación, utilice las instrucciones de Eliminar backups. Para eliminar una copia de seguridad fallida, "Utilice la API Astra Control".

> 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.

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 puede eliminar una copia Snapshot que se está replicando actualmente.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
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 Center 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 estado en ejecución. No es posible cancelar un backup que esté en estado Pending.

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 eliminación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

Eliminar backups

Elimine los backups programados o bajo demanda que ya no necesita.

No existe ninguna forma de detener un backup en ejecución. Si necesita eliminar el backup, espere hasta que se haya completado y, a continuación, utilice estas instrucciones. Para eliminar una copia de seguridad fallida, "Utilice la API Astra Control".

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 Center elimina la copia de seguridad.

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. "La API de control Astra" para restaurar aplicaciones.

Acerca de esta tarea

- Se recomienda tomar una instantánea o realizar una copia de seguridad de la aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup en el caso de que la restauración no se realice correctamente.
- Si utiliza Helm para implantar 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.
- Si restaura en un clúster diferente, asegúrese de que el clúster 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.
- 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 crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.
- Al crear 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** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Si desea restaurar desde una instantánea, mantenga seleccionado el icono **instantáneas**. De lo contrario, seleccione el icono **copias de seguridad** para restaurar desde una copia de seguridad.
4. En el menú Opciones de la columna **acciones** de la instantánea o copia de seguridad desde la que desea restaurar, seleccione **Restaurar aplicación**.
5. **Detalles de la restauración**: Especifique los detalles de la aplicación restaurada. De forma predeterminada, se muestran el clúster y el espacio de nombres actuales. Deje estos valores intactos para restaurar una aplicación in situ, que revierte la aplicación a una versión anterior de sí misma. Cambie estos valores si desea restaurar a un clúster o espacio de nombres diferentes.
   - Introduzca un nombre y un espacio de nombres para la aplicación.
   - Seleccione el clúster de destino de la aplicación.
   - Seleccione **Revisión**.

   > 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.

6. **Resumen de restauración**: Revise los detalles sobre la acción de restauración, escriba "restore" y seleccione **Restaurar**.

Resultado

Astra Control Center restaura la aplicación en función de la información proporcionada. Si restauró la aplicación en un lugar, el contenido de cualquier volumen persistente existente se reemplaza por el contenido de los volúmenes persistentes de la aplicación restaurada.

> Después de una operación de protección de datos (clonado, backup, restauración) y un posterior cambio de tamaño de volumen persistente, se producen retrasos de hasta veinte minutos antes de que se muestre el nuevo tamaño del 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.

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

Para ver la 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:

- En el sitio Local A al sitio local B
- Del entorno local al cloud con Cloud Volumes ONTAP
- Cloud con Cloud Volumes ONTAP para infraestructura en 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 (que se ejecute en el otro clúster o sitio) 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
- Conectar una aplicación replicada 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

Consulte "requisitos previos de replicación" antes de empezar.

Configurar una relación de replicación

La configuración de una relación de replicación implica los siguientes elementos que componen la directiva de replicación:

- Elegir la frecuencia con la que desea que Astra Control tome una Snapshot de aplicaciones (que incluye los recursos de Kubernetes de la aplicación, así como las copias Snapshot por volumen para 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 el tiempo para que se tome la instantánea

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, seleccione **Configurar directiva 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:
   - Clúster de destino
   - **Clase de almacenamiento de destino**: Seleccione o introduzca la clase de almacenamiento que utiliza la SVM emparejado en el clúster ONTAP de destino.
   - **Tipo de replicación**: "Asincrónica" es actualmente el único tipo de replicación disponible.
   - **Espacio de nombres de destino**: Introduzca un espacio de nombres de destino nuevo o existente para el clúster de destino.

     Se sobrescribirá cualquier recurso en conflicto en el espacio de nombres seleccionado.

   - **Frecuencia de replicación**: Establezca la frecuencia con la que desea que Astra Control tome una instantánea y la replique en su destino.
   - * Offset*: Establezca el número de minutos desde la parte superior de la hora que desea que Astra Control tome una instantánea. Es posible que desee utilizar un offset para no coincidir con otras operaciones programadas. Por ejemplo, si desea tomar la copia Snapshot cada 5 minutos a partir de las 10:02, introduzca "02" como el desplazamiento minutos. El resultado sería 10:02, 10:07, 10:12, etc.
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 instantánea de aplicación que se utiliza para la replicación.

6. Para ver el estado de la instantánea de la aplicación, seleccione la ficha **aplicaciones** > **instantáneas**.

   El nombre de Snapshot utiliza el formato "replication-schedule-<string>". Astra Control conserva la última snapshot utilizada para la replicación. Las snapshots de replicación más antiguas se eliminan 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.
- Toma una snapshot inicial coherente con las aplicaciones.
- Establece la relación SnapMirror para los volúmenes persistentes mediante la snapshot inicial.

En la página Data Protection, se muestra el estado y estado de la relación de replicación: <Health status> | <Relationship life cycle state>

Por ejemplo: Normal | establecido

Obtenga más información sobre los estados y el estado de la replicación a continuación.

Conectar una aplicación replicada en el clúster de destino (conmutación por error)

Con Astra Control, puede "conmutar por error" las aplicaciones replicadas a 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. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **failover**.
4. En la página de conmutación por error, revise la información y seleccione **failover**.

Resultado

Las siguientes acciones ocurren como resultado del procedimiento de conmutación por error:

- En el clúster de destino, la aplicación se inicia a partir de la snapshot replicada más reciente.
- 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 en función de los horarios presentes en la aplicación de origen en el momento de la conmutación por error.
- 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. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **Resync**.
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 clúster de destino y seguir replicando de nuevo 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.

En esta situación, está intercambiando el origen y el destino. El clúster de origen original se convierte en el nuevo clúster de destino, y el clúster de destino original se convierte en el nuevo clúster de origen.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, 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 realiza una copia Snapshot de los recursos de Kubernetes de las aplicaciones de origen originales.
- 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).
- Una vez apagados los pods, se realizan copias Snapshot de los volúmenes de la aplicación y se replican.
- 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 desde la copia Snapshot previa al apagado, utilizando los datos de volumen replicados después del apagado de 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 lograr una "recuperación tras fallos" tras una operación de "conmutación por error" mediante la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Astra Control replica (resyncs) cualquier aplicación vuelve a cambiar al clúster de origen original antes de revertir la dirección de replicación.

Este proceso comienza a partir de una relación que ha completado una conmutación por error 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. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **Resync**.
4. Para realizar una operación de recuperación tras fallos, elija la aplicación con error como origen de la operación de resincronización (cómo conservar los datos escritos en una post conmuta al nodo de respaldo).
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. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación , 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.
  - La relación está establecida (por lo que se ha replicado un snapshot correcto y es posible la recuperación tras fallos), pero la snapshot más reciente ha fallado o ha fallado para replicarse.

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 las RVP están disponibles, comprueba la relación de replicación, crea periódicamente instantáneas de la aplicación e identifica cualquier EVs de origen nuevo en la aplicación. Si es así, Astra Control crea los recursos para incluirlos en la replicación.
- **Recuperación tras fallos**: Astra Control rompe las relaciones de SnapMirror y restaura los recursos Kubernetes de la aplicación desde la última instantánea de aplicación replicada correctamente.
- * Fallo en*: Astra Control deja de replicar desde el clúster de origen, utiliza la instantánea de aplicación replicada más reciente (correcta) 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

Clone una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control Center 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 o. "La API de control Astra" para clonar y migrar aplicaciones.

Lo que necesitará

Para clonar aplicaciones en un clúster diferente, necesita un bloque predeterminado. Cuando se agrega su primer bloque, se convierte en el bloque predeterminado.

Acerca de esta tarea

- Si se implementa una aplicación con un StorageClass configurado explícitamente y se necesita clonar la aplicación, el clúster de destino debe tener el StorageClass especificado originalmente. Se producirá un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo de almacenamiento.
- Si clona una instancia de Jenkins CI que ha puesto en marcha un operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.
- 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.
- Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar 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.
- 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 crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.

Consideraciones sobre OpenShift

- 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.
- Al crear 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. **Detalles del clon**: Especifique los detalles del clon:
   - Introduzca un nombre.
   - Introduzca un espacio de nombres para el clon.
   - Elija un clúster de destino para el clon.
   - Elija si desea crear el clon a partir de una snapshot o un backup existente. Si no selecciona esta opción, Astra Control Center crea el clon a partir del estado actual de la aplicación.
5. **Fuente**: Si decide clonar desde una instantánea o copia de seguridad existente, elija la instantánea o copia de seguridad que desea utilizar.
6. Seleccione **Revisión**.
7. **Resumen de clones**: Revise los detalles sobre el clon y seleccione **clon**.

Resultado

Astra Control Center clona esa aplicación basándose en la información que nos ha proporcionado. La operación de clonado se realiza correctamente cuando el nuevo clon de la aplicación está en `Available` en la página **aplicaciones**.

> 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.

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 tiene una aplicación de base de datos, puede utilizar los enlaces de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez finalizada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Tipos de enlaces de ejecución

Astra Control admite los siguientes tipos de enlaces de ejecución, en función de cuándo se pueden ejecutar:

- Copia previa de Snapshot
- Possnapshot
- Previo al backup
- Después del backup
- Después de la restauración

Notas importantes sobre los enlaces de ejecución personalizados

Tenga en cuenta lo siguiente al planificar enlaces de ejecución para sus aplicaciones.

- 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 ad hoc, 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).

> Puesto 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 un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

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 los cinco tipos diferentes de

ganchos sería 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
1	Clonar	N	N	Nuevo	Igual	Y	N	Y

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
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	Y	Y
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y
7	Restaurar	Y	N	Existente	Igual	N	N	Y
8	Restaurar	N	Y	Existente	Igual	N	N	Y
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.
11	Backup	Y	N.A.	N.A.	N.A.	N	Y	N.A.

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, el origen y el momento en que se ejecuta un gancho (pre o post-operación). Para ver los registros de eventos que rodean los enlaces de ejecución, vaya a la página **actividad** en el área de navegación del lado izquierdo.

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

Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos enlaces de ejecución pueden hacer referencia a la misma secuencia de comandos; esto permite actualizar muchos enlaces de ejecución sólo cambiando una secuencia de comandos.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Seleccione **Agregar**.
4. 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.
5. 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

Puede crear un enlace de ejecución personalizado para una aplicación. 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. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione **Agregar**.
4. En el área **Detalles del gancho**, determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.
5. Introduzca un nombre único para el gancho.
6. (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.
7. En el área **Imágenes de contenedor**, si el gancho debe funcionar con todas las imágenes de contenedor contenidas en la aplicación, active la casilla de verificación **aplicar a todas las imágenes de contenedor**. Si en su lugar el gancho sólo debe actuar en una o más imágenes contenedoras especificadas, introduzca los nombres de imagen contenedora en el campo **nombres de imagen contenedora para que coincidan**.
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 **Agregar gancho**.

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.

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**.

Ejemplos de gancho de ejecución

Utilice los siguientes ejemplos para obtener una idea de cómo estructurar los enlaces de ejecución. Puede utilizar estos enlaces como plantillas o como scripts de prueba.

Ejemplo de éxito simple

Este es un ejemplo de un simple enlace que se realiza correctamente y escribe un mensaje en la salida estándar y en un error estándar.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
```

```
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo de éxito simple (versión de bash)

Este es un ejemplo de un simple enlace que funciona y escribe un mensaje en la salida estándar y en un error estándar, escrito para bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
```

```
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo sencillo de éxito (versión zsh)

Este es un ejemplo de un simple enlace que se realiza correctamente y escribe un mensaje en la salida estándar y en un error estándar, escrito para el shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
```

```
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Éxito con argumentos ejemplo

En el siguiente ejemplo se muestra cómo se pueden utilizar args en un gancho.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
```

```
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"
```

```
# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo de gancho de instantánea previa/posinstantánea

En el siguiente ejemplo se muestra cómo se puede utilizar el mismo script tanto para una instantánea previa como para un enlace posterior a una instantánea.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"
```

```
if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

Ejemplo de fallo

En el siguiente ejemplo se muestra cómo puede controlar los fallos en un gancho.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
```

```
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Ejemplo de fallo detallado

En el ejemplo siguiente se muestra cómo puede controlar los errores en un enlace, con un registro más detallado.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
```

```
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
```

```
exit 8
```

Fallo con un ejemplo de código de salida

En el siguiente ejemplo se muestra un error de enlace con un código de salida.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
```

```
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Ejemplo de éxito tras fallo

El siguiente ejemplo muestra un gancho que falla la primera vez que se ejecuta, pero que tiene éxito después de la segunda ejecución.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
```

```
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

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 y los detalles de los clústeres

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.

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.

Ver el estado y los detalles de una aplicación

Una vez que empiece a gestionar una aplicación, Astra ofrece detalles sobre la aplicación que permite identificar su estado (si está en buen estado), su estado de protección (si está totalmente protegida 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. Encuentre la información que busca:

Estado de la aplicación

Proporciona un estado que refleja el estado de la aplicación en Kubernetes. Por ejemplo, ¿los pods y los volúmenes persistentes están en línea? Si una aplicación no es saludable, deberá ir y solucionar el problema en el clúster mirando los registros de Kubernetes. Astra no proporciona información para ayudarle a arreglar una aplicación rota.

Estado de protección de aplicaciones

Proporciona el 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 asociados con la aplicación.

Protección de datos

Permite configurar una política de protección de datos y ver las Snapshot y los backups existentes.

Reducida

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 gestionando y haciendo backup.

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

Gestionar usuarios

Puede invitar, añadir, eliminar y editar a los 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. "La 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. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra correspondientes a las definiciones LDAP. Consulte "Autenticación LDAP" si quiere más información.

Invitar a los usuarios

Los propietarios y administradores de cuentas pueden invitar a nuevos usuarios a Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Invitar usuario**.
4. Introduzca el nombre y la dirección de correo electrónico del usuario.
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 "Gestionar roles".

7. Seleccione **Invitar usuarios**.

   El usuario recibe un correo electrónico informándole de que ha sido invitado a Astra Control Center. El correo electrónico incluye una contraseña temporal, que deberá cambiar en el primer inicio de sesión.

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 "Gestionar 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**.

Cambiar el rol de un usuario

Los usuarios con el rol propietario pueden cambiar el rol de todos los usuarios, mientras que los usuarios con el rol Admin pueden cambiar el rol de los usuarios que tienen el rol Admin, Member o Viewer.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la lista desplegable **acciones**.
3. Seleccione **Editar rol**.
4. Seleccione un rol nuevo.
5. Para aplicar restricciones a la función, active la casilla de verificación **restringir la función a restricciones** y seleccione una restricción de la lista.

   Si no hay restricciones, puede agregar una restricción. Para obtener más información, consulte "Gestionar roles".

6. Seleccione **Confirmar**.

Resultado

Astra Control Center actualiza los permisos del usuario en función de la nueva función que haya seleccionado.

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. "La API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Admin o Owner puede agregar restricciones de espacio de nombres.

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"

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 con un clúster nuevo, consulte "Añada un clúster de Kubernetes".

> 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.

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.

Si gestiona los clústeres de Kubernetes desde Astra Control y Astra Control se conecta a Cloud Insights, Astra Control envía registros de eventos a Cloud Insights. La información de registro, incluida la información sobre la implementación de POD y los archivos adjuntos de PVC, aparece en el registro de actividad de control de Astra. Utilice esta información para identificar cualquier problema en los clústeres de Kubernetes que está gestionando.

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 o. "La 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 conexiones de repositorios

Puede conectar repositorios a Astra Control para utilizarlos como referencia para imágenes y artefactos de instalación de paquetes de software. Al importar paquetes de software, Astra Control hace referencia a imágenes de instalación en el repositorio de imágenes y binarios y otros artefactos en el repositorio de artefactos.

Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Un repositorio de Docker en ejecución al que se puede acceder
- Un repositorio de artefactos en ejecución (como Artifactory) al que se puede acceder

Conecte un repositorio de imágenes Docker

Puede conectar un repositorio de imágenes Docker para almacenar imágenes de instalación del paquete, como las de Astra Data Store. Al instalar paquetes, Astra Control importa los archivos de imagen del paquete desde el repositorio de imágenes.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **Docker Image Repository**, seleccione el menú de la parte superior derecha.
4. Seleccione **conectar**.
5. Añada la URL y el puerto para el repositorio.
6. Introduzca las credenciales del repositorio.
7. Seleccione **conectar**.

Resultado

El repositorio está conectado. En la sección **Docker Image Repository**, el repositorio debe mostrar un estado conectado.

Desconecte un repositorio de imágenes Docker

Puede eliminar la conexión a un repositorio de imágenes Docker si ya no es necesario.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **Docker Image Repository**, seleccione el menú de la parte superior derecha.
4. Seleccione **desconectar**.
5. Seleccione **Sí, desconecte el repositorio de imágenes Docker**.

Resultado

El repositorio está desconectado. En la sección **Docker Image Repository**, el repositorio debe mostrar un estado desconectado.

Conecte un repositorio de artefactos

Puede conectar un repositorio de artefactos a artefactos host como los binarios de paquetes de software. Al instalar paquetes, Astra Control importa los artefactos para los paquetes de software desde el repositorio de imágenes.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **repositorio de artefactos**, seleccione el menú de la parte superior derecha.
4. Seleccione **conectar**.
5. Añada la URL y el puerto para el repositorio.
6. Si se requiere autenticación, active la casilla de verificación **usar autenticación** e introduzca las credenciales del repositorio.
7. Seleccione **conectar**.

Resultado

El repositorio está conectado. En la sección **repositorio de artefactos**, el repositorio debe mostrar un estado conectado.

Desconecte un repositorio de artefactos

Puede eliminar la conexión a un repositorio de artefactos si ya no es necesaria.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **repositorio de artefactos**, seleccione el menú de la parte superior derecha.
4. Seleccione **desconectar**.
5. Seleccione **Sí, desconectar el repositorio de artefactos**.

Resultado

El repositorio está desconectado. En la sección **repositorio de artefactos**, el repositorio debe mostrar un estado conectado.

Obtenga más información

- "Gestione los paquetes de software"

Gestione los paquetes de software

NetApp ofrece funcionalidades adicionales para Astra Control Center con paquetes de software que puede descargar en el sitio de soporte de NetApp. Después de conectar los repositorios de Docker y artefactos, puede cargar e importar paquetes para agregar esta funcionalidad a Astra Control Center. Puede utilizar la CLI o la interfaz de usuario web de Astra Control Center para gestionar los paquetes de software.

Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Un repositorio de imágenes Docker conectado para contener imágenes de paquetes de software. Para obtener más información, consulte "Gestionar conexiones de repositorios".
- Un repositorio de artefactos conectado para contener binarios y artefactos de paquetes de software. Para obtener más información, consulte "Gestionar conexiones de repositorios".
- Un paquete de software del sitio de soporte de NetApp

Cargue imágenes de paquetes de software en los repositorios

Astra Control Center hace referencia a imágenes de paquetes y artefactos en repositorios conectados. Puede cargar imágenes y artefactos en los repositorios con la CLI.

Pasos

1. Descargue el paquete de software del sitio de soporte de NetApp y guárdelo en un equipo que tenga el `kubectl` utilidad instalada.
2. Extraiga el archivo de paquete comprimido y cambie el directorio a la ubicación del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
3. Inserte las imágenes de los paquetes en el repositorio de Docker. Realice las siguientes sustituciones:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

   ```
   kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
   MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
   ```

4. Si el paquete tiene artefactos, copie los artefactos en el repositorio de artefactos. Sustituya BUNDLE_FILE por el nombre del archivo de paquete Astra Control y NETWORK_LOCATION por la ubicación de red para copiar los archivos de artefactos a:

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

Añada un paquete de software

Puede importar paquetes de software mediante un archivo de paquete Astra Control Center. De esta forma, se instala el paquete y se pone el software a disposición de Astra Control Center.

Agregue un paquete de software mediante la interfaz de usuario web de Astra Control

Puede utilizar la interfaz de usuario web de Astra Control Center para agregar un paquete de software que se ha cargado en los repositorios conectados.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **Paquetes**.
3. Seleccione el botón **Agregar**.
4. En el cuadro de diálogo de selección de archivos, seleccione el icono de carga.
5. Elija un archivo de paquete de Astra Control, en `.yaml` formato, para cargar.
6. Seleccione **Agregar**.

Resultado

Si el archivo de paquete es válido y las imágenes y artefactos del paquete se encuentran en los repositorios conectados, el paquete se agrega a Astra Control Center. Cuando el estado de la columna **Estado** cambia a **disponible**, puede utilizar el paquete. Puede pasar el ratón sobre el estado de un paquete para obtener más información.

> Si no se encuentran una o más imágenes o artefactos para un paquete en su repositorio, aparece un mensaje de error para ese paquete.

Añada un paquete de software mediante la CLI

Es posible usar la CLI para importar un paquete de software que haya cargado en los repositorios conectados. Para ello, primero debe registrar el ID de cuenta de Astra Control Center y un token de API.

Pasos

1. Con un navegador web, inicie sesión en la interfaz de usuario web de Astra Control Center.
2. En el panel de control, seleccione el icono de usuario en la parte superior derecha.
3. Seleccione **acceso API**.
4. Observe el ID de cuenta cerca de la parte superior de la pantalla.
5. Seleccione **generar símbolo de API**.
6. En el cuadro de diálogo resultante, seleccione **generar símbolo de API**.
7. Observe el token resultante y seleccione **Cerrar**. En la CLI, cambie los directorios a la ubicación de `.yaml` archivo de paquete en el contenido del paquete extraído.
8. Importe el paquete utilizando el archivo de paquete, realizando las siguientes sustituciones:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle.
   - Sustituya EL SERVIDOR por el nombre DNS de la instancia de Astra Control.
   - Reemplace ACCOUNT_ID y TOKEN con el ID de cuenta y el token de API que haya registrado anteriormente.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

Resultado

Si el archivo de paquete es válido y las imágenes y artefactos del paquete se encuentran en los repositorios conectados, el paquete se agrega a Astra Control Center.

Si no se encuentran una o más imágenes o artefactos para un paquete en su repositorio, aparece un mensaje de error para ese paquete.

Quite un paquete de software

Puede utilizar la interfaz de usuario web de Astra Control Center para eliminar un paquete de software importado previamente en Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **Paquetes**.

   En esta página puede ver la lista de paquetes instalados y sus Estados.

3. En la columna **acciones** del paquete, abra el menú acciones.
4. Seleccione **Eliminar**.

Resultado

El paquete se elimina de Astra Control Center, pero las imágenes y artefactos del paquete permanecen en sus repositorios.

Obtenga más información

- "Gestionar conexiones de repositorios"

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 la configuración de sus aplicaciones y el 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 cubos de S3 genérico, Astra Control Center podría no admitir 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.
- Removido: El cucharón no está accesible 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
- Gire o elimine las credenciales del cucharón
- Retirar un cucharón

> 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 Opciones 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**.

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.

Lo que necesitará

- 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 lo 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**.

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. Puede supervisar la capacidad del almacenamiento y los detalles del estado, incluido el rendimiento si el Centro de control Astra está conectado a Cloud Insights.

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
- Desgestione un back-end de almacenamiento
- Actualizar una licencia de back-end de almacenamiento de Astra Data Store
- Actualice un back-end de almacenamiento de Astra Data Store
- Quite un back-end de almacenamiento
- Añada nodos a un clúster de back-end de almacenamiento
- Quite nodos de un clúster de 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.

En la página Storage Backend Details, en Astra Data Store, puede consultar la siguiente información:

- Clúster de almacén de datos de Astra
  - Rendimiento, IOPS y latencia
  - Capacidad utilizada en comparación con la capacidad total
- Para cada volumen de clúster de Astra Data Store
  - Capacidad utilizada en comparación con la capacidad total
  - Rendimiento

Consulte los detalles del back-end de almacenamiento en la Consola

Pasos

1. En la navegación de la izquierda, seleccione **Tablero**.
2. Revise la sección Storage backend 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

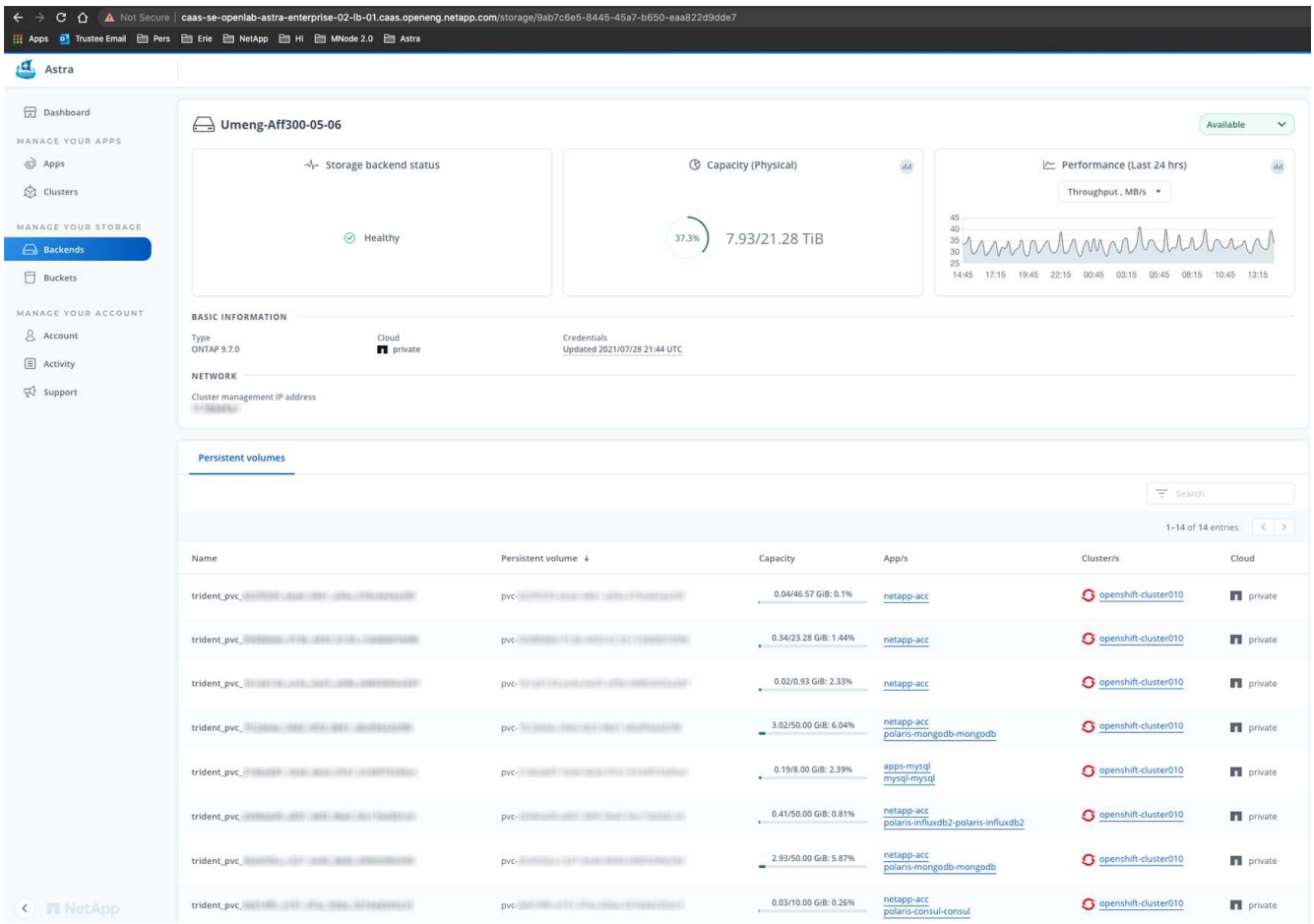
Vea información sobre el estado, la capacidad y el rendimiento del back-end (rendimiento de IOPS y/o latencia).

Puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado. Con Cloud Insights, puede ver información adicional. Consulte "Documentación de Cloud Insights".

Pasos

1. En el área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.

> Si conectas a Cloud Insights de NetApp, aparecerán extractos de datos de Cloud Insights en la página backends.



3. Para ir directamente a Cloud Insights, seleccione el icono **Cloud Insights** junto a la imagen de métricas.

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.

Si va a eliminar un back-end de Astra Data Store, vCenter no debe haberlo creado.

Lo que necesitará

- Asegúrese de que el back-end de almacenamiento no esté gestionado.
- Asegúrese de que el back-end de almacenamiento no tenga ningún volumen asociado con el clúster de almacén de datos de Astra.

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**.

Actualizar una licencia de back-end de almacenamiento de Astra Data Store

Puede actualizar la licencia de un back-end de almacenamiento de Astra Data Store para admitir una implementación mayor o funciones mejoradas.

Lo que necesitará

- Un back-end de almacenamiento de Astra Data Store implementado y gestionado
- Un archivo de licencia de Astra Data Store (póngase en contacto con su representante de ventas de NetApp para adquirir una licencia de Astra Data Store)

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.

2. Seleccione el nombre de un back-end de almacenamiento.
3. En **Información básica**, puede ver el tipo de licencia instalada.

   Si pasa el ratón por encima de la información de la licencia, aparece un cuadro emergente con más información, como información sobre la caducidad y los derechos.

4. En **Licencia**, seleccione el icono de edición junto al nombre de la licencia.
5. En la página **Actualizar licencia**, siga uno de estos procedimientos:

Estado de la licencia	Acción
Se ha añadido al menos una licencia a Astra Data Store.	Seleccione una licencia de la lista.
No se han añadido licencias a Astra Data Store.	a. Seleccione el botón **Agregar**. b. Seleccione un archivo de licencia para cargar. c. Seleccione **Agregar** para cargar el archivo de licencia.

6. Seleccione **Actualizar**.

Actualice un back-end de almacenamiento de Astra Data Store

Puede actualizar su entorno de administración de Astra Data Store desde Astra Control Center. Para ello, primero debe cargar un paquete de actualización; Astra Control Center utilizará este paquete de actualización para actualizar Astra Data Store.

Lo que necesitará

- Un back-end de almacenamiento gestionado de Astra Data Store
- Un paquete de actualización de Astra Data Store cargado (consulte "Gestione los paquetes de software")

Pasos

1. Seleccione **Backends**.
2. Elija un back-end de almacenamiento de Astra Data Store de la lista y seleccione el menú correspondiente en la columna **acciones**.
3. Seleccione **Actualizar**.
4. Seleccione una versión de actualización de la lista.

   Si tiene varios paquetes de actualización en el repositorio que son versiones diferentes, puede abrir la lista desplegable para seleccionar la versión que necesita.

5. Seleccione **Siguiente**.
6. Seleccione **Iniciar actualización**.

Resultado

La página **backends** muestra un estado **Upgrade** en la columna **Status** hasta que la actualización se haya completado.

Añada nodos a un clúster de back-end de almacenamiento

Puede agregar nodos a un clúster de almacén de datos de Astra, hasta el número de nodos admitidos por el tipo de licencia instalada para Astra Data Store.

Lo que necesitará

- Un back-end de almacenamiento de Astra Data Store con licencia y puesto en marcha
- Ha agregado el paquete de software Astra Data Store en Astra Control Center
- Uno o más nodos nuevos para añadir al clúster

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el nombre de un back-end de almacenamiento.
3. En Basic Information, puede ver el número de nodos en este clúster de back-end de almacenamiento.
4. En **Nodes**, seleccione el icono de edición junto al número de nodos.
5. En la página **Add Nodes**, introduzca información sobre el nuevo nodo o nodos:
   a. Asigne una etiqueta de nodo para cada nodo.
   b. Debe realizar una de las siguientes acciones:
      - Si desea que Astra Data Store utilice siempre el número máximo de nodos disponibles según su licencia, active la casilla de verificación * utilizar siempre hasta el número máximo de nodos permitidos*.
      - Si no desea que Astra Data Store utilice siempre el número máximo de nodos disponibles, seleccione el número deseado de nodos totales que desea utilizar.
   c. Si implementó Astra Data Store con Protection Domains habilitado, asigne el nodo o los nodos nuevos a Protection Domains.
6. Seleccione **Siguiente**.
7. Introduzca la dirección IP y la información de red para cada nodo nuevo. Introduzca una sola dirección IP para un solo nodo nuevo o un pool de direcciones IP para varios nodos nuevos.

   Si Astra Data Store puede utilizar las direcciones IP configuradas durante la implementación, no necesita introducir ninguna información de dirección IP.
8. Seleccione **Siguiente**.
9. Revise la configuración de los nodos nuevos.
10. Seleccione **Agregar nodos**.

Quite nodos de un clúster de back-end de almacenamiento

Puede eliminar nodos de un clúster de almacén de datos de Astra. Estos nodos pueden estar en buen estado o con errores.

Al quitar un nodo de un clúster Astra Data Store, se mueven sus datos a otros nodos del clúster y se quita el nodo de Astra Data Store.

El proceso requiere las siguientes condiciones:

- Debe haber suficiente espacio libre en los otros nodos para recibir los datos.

- Debe haber 4 o más nodos en el clúster.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el nombre de un back-end de almacenamiento.
3. Seleccione la ficha **Nodes**.
4. En el menú acciones, seleccione **Quitar**.
5. Confirme la eliminación introduciendo "eliminar".
6. Seleccione **Sí, eliminar nodo**.

Obtenga más información

- "Utilice la API Astra Control"

Supervise la infraestructura con conexiones Cloud Insights y Fluentd

Puede configurar varios ajustes opcionales para mejorar su experiencia con Astra Control Center. Para supervisar y obtener información sobre toda su infraestructura, cree una conexión con Cloud Insights de NetApp. Para recopilar eventos Kubernetes de sistemas supervisados por Astra Control Center, añada una conexión fluentd.

Si la red en la que ejecuta Astra Control Center requiere un proxy para conectarse a Internet (para cargar los paquetes de soporte en el sitio de soporte de NetApp o establecer una conexión con Cloud Insights), debe configurar un servidor proxy en Astra Control Center.

También puede supervisar el rendimiento del back-end de almacenamiento de Astra Data Store, las IOPS y la capacidad desde la página Astra Control Center Storage Backends. Consulte "Gestione los back-ends de almacenamiento".

Añada un servidor proxy para conexiones a Cloud Insight o 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 los paquetes de soporte en el sitio de soporte de NetApp o establecer una conexión con Cloud Insights), debe configurar un servidor proxy en Astra Control Center.

> 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** en 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 desactivar que se pueden producir posibles interrupciones en 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 Cloud Insights

Para supervisar y obtener información sobre toda su infraestructura, conecte Cloud Insights de NetApp con su instancia de Astra Control Center. Cloud Insights está incluido en su licencia de Astra Control Center.

Debe accederse a Cloud Insights desde la red que utiliza Astra Control Center, o indirectamente mediante un servidor proxy.

Cuando el Centro de control de Astra está conectado a Cloud Insights, se crea un POD de unidad de adquisición. Este pod recoge datos de los back-ends de almacenamiento gestionados por Astra Control Center y los empuja a Cloud Insights. Este pod requiere 8 GB de RAM y 2 núcleos de CPU.

Además, si gestiona los clústeres de Astra Data Store con Astra Control (que está conectado a Cloud Insights), se crea una unidad de adquisición en el almacén de datos Astra para cada clúster de Astra Data Store y las métricas se envían desde Astra Data Store al sistema Cloud Insights emparejado. Cada pod requiere 8 GB de RAM y 2 núcleos de CPU.

> Después de activar la conexión Cloud Insights, puede ver la información de rendimiento en la página **backends** así como conectarse a Cloud Insights desde aquí después de seleccionar un back-end de almacenamiento. También puede encontrar la información en **Panel** en la sección clúster, y también puede conectarse a Cloud Insights desde allí.

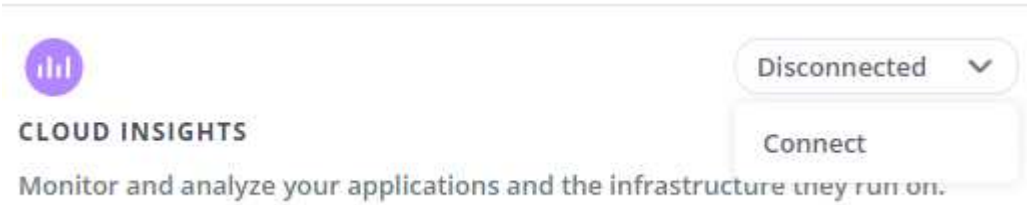
Lo que necesitará

- Una cuenta de Astra Control Center con privilegios **admin**/**owner**.
- Una licencia válida de Astra Control Center.
- Un servidor proxy si la red en la que se ejecuta Astra Control Center requiere un proxy para conectarse a Internet.

> Si no tiene experiencia en Cloud Insights, familiarícese con las funciones y las funcionalidades. Consulte "Documentación de Cloud Insights".

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** donde aparece **Desconectado** en la lista desplegable para agregar la conexión.



4. Introduzca los tokens de la API Cloud Insights y la URL del inquilino. La URL del inquilino tiene el siguiente formato, como ejemplo:

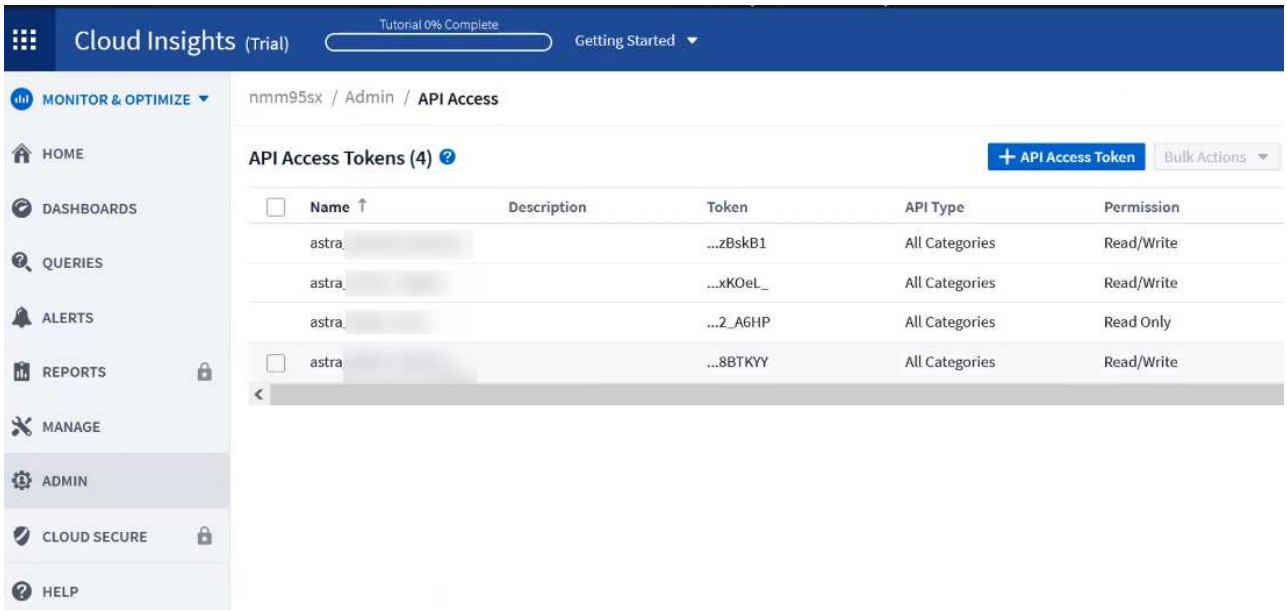
```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Obtiene la URL de inquilino al obtener la licencia de Cloud Insights. Si no tiene la URL de inquilino,

consulte "Documentación de Cloud Insights".

a. Para obtener la "Token de API", Inicie sesión en la dirección URL del inquilino de Cloud Insights.

b. En Cloud Insights, genere un token de acceso de **lectura/escritura** y un símbolo de acceso de API **sólo lectura** haciendo clic en **Admin** > **acceso de API**.



c. Copie la tecla **sólo lectura**. Deberá pegarlo en la ventana Centro de control de Astra para habilitar la conexión a Cloud Insights. Para los permisos de clave de token de acceso a la API de lectura, seleccione: Activos, Alertas, Unidad de adquisición y recolección de datos.

d. Copie la tecla **Read/Write**. Deberá pegarlo en la ventana Centro de control de Astra **Connect Cloud Insights**. Para los permisos de clave de acceso a la API de lectura/escritura, seleccione: Activos, ingestión de datos, ingestión de registros, unidad de adquisición, Y recopilación de datos.

> Le recomendamos que genere una tecla **sólo lectura** y una tecla **Leer/escribir**, y que no utilice la misma clave para ambos propósitos. De forma predeterminada, el período de caducidad del token se establece en un año. Le recomendamos que mantenga la selección predeterminada para dar al token la duración máxima antes de que caduque. Si el token caduca, la telemetría se detendrá.

e. Pegue las claves que ha copiado de Cloud Insights en Astra Control Center.

5. Seleccione **conectar**.

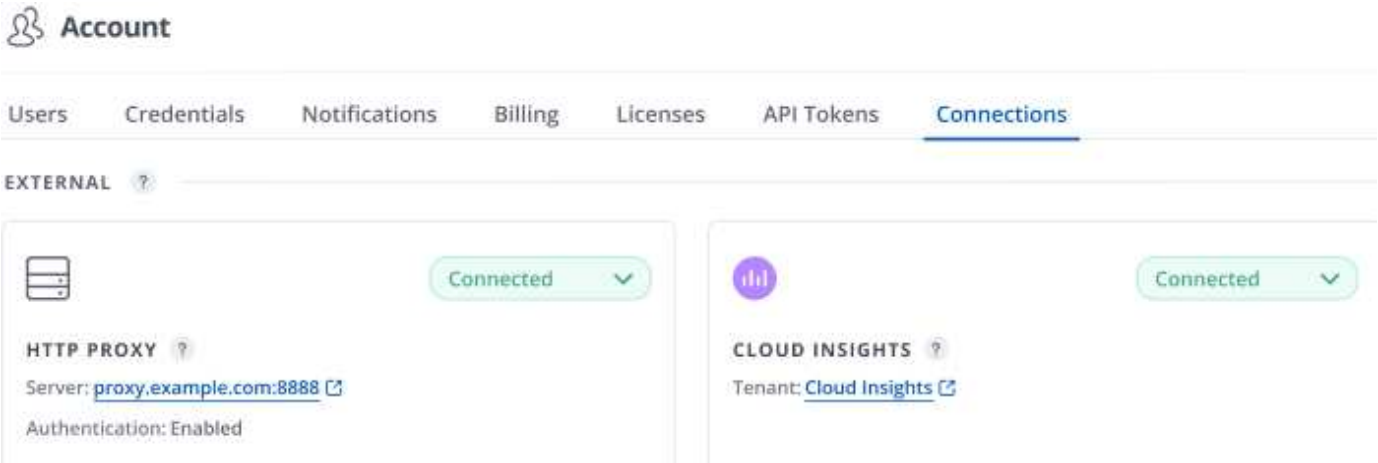
> Después de seleccionar **conectar,** el estado de la conexión cambia a **pendiente** en la sección **Cloud Insights** de la página **cuenta** > **conexiones**. Puede pasar unos minutos para que la conexión esté activada y el estado cambie a **conectado**.

> Para retroceder y avanzar fácilmente entre el Centro de control de Astra y las interfaces de usuario de Cloud Insights, asegúrese de que ha iniciado sesión en ambos.

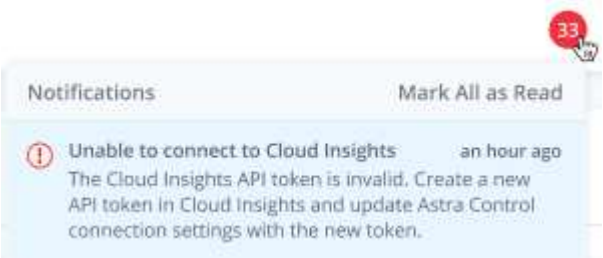
Ver datos en Cloud Insights

Si la conexión se realizó correctamente, la sección **Cloud Insights** de la página **cuenta** > **conexiones** indica que está conectada y muestra la dirección URL del inquilino. Puede visitar Cloud Insights para ver los datos

que se han recibido y mostrado correctamente.

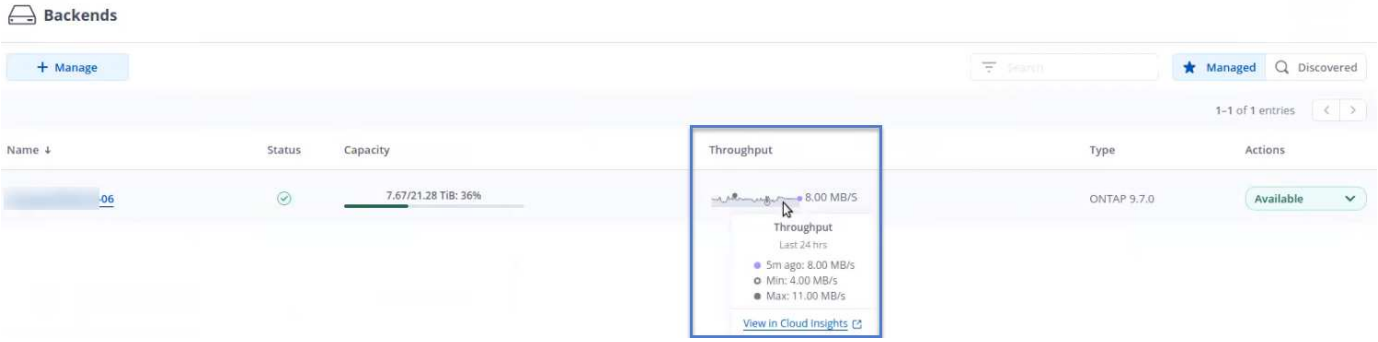


Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.



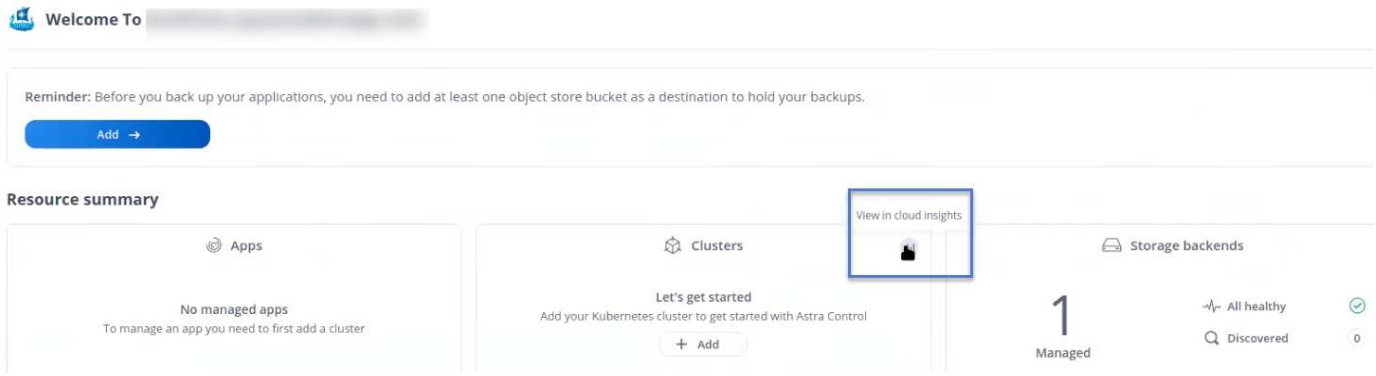
También puede encontrar la misma información en **cuenta** > **Notificaciones**.

Desde Astra Control Center, puede ver la información sobre el rendimiento en la página **backends**, así como conectarse a Cloud Insights desde aquí tras seleccionar un backend de almacenamiento.



Para ir directamente a Cloud Insights, seleccione el icono **Cloud Insights** junto a la imagen de métricas.

También puede encontrar la información en el **Panel**.



Después de habilitar la conexión Cloud Insights, si quita los back-ends que agregó en Astra Control Center, los back-ends dejan de informar a Cloud Insights.

Editar conexión Cloud Insights

Puede editar la conexión Cloud Insights.

Solo puede editar las claves de API. Para cambiar la URL de inquilino de Cloud Insights, le recomendamos que desconecte la conexión de Cloud Insights y se conecte con la nueva URL.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** en la lista desplegable para editar la conexión.
4. Edite la configuración de la conexión Cloud Insights.
5. Seleccione **Guardar**.

Deshabilite la conexión Cloud Insights

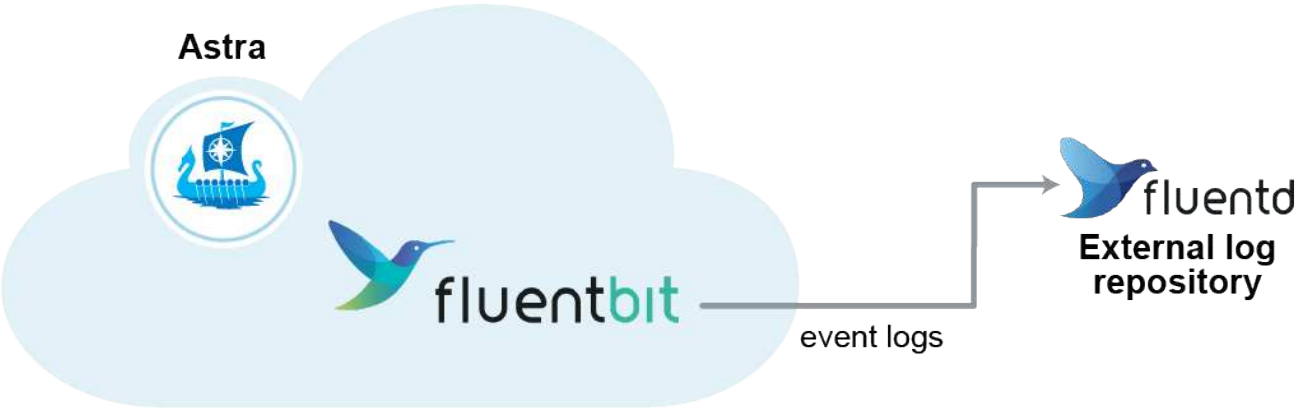
Puede deshabilitar la conexión Cloud Insights para un clúster de Kubernetes gestionado por Astra Control Center. Al deshabilitar la conexión Cloud Insights, no se eliminan los datos de telemetría ya cargados en Cloud Insights.

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. Después de confirmar la operación, en la página **cuenta** > **conexiones**, el estado de Cloud Insights cambia a **pendiente**. El estado tarda unos minutos en cambiar a **desconectado**.

Conectar a Fluentd

Puede enviar registros (eventos Kubernetes) desde Astra Control Center a su terminal Fluentd. La conexión fluentd está desactivada de forma predeterminada.



Sólo se reenvían a Fluentd los registros de eventos de los clusters gestionados.

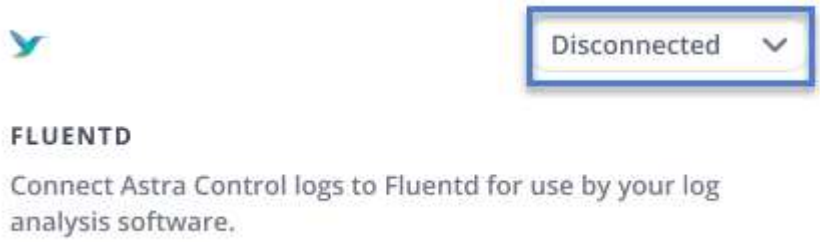
Lo que necesitará

- 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** en 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.

- 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 casilla de verificación de las aplicaciones que ya no desea administrar.
3. En el menú **Acción**, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar.
5. Confirme que desea anular la administración de las aplicaciones y, a continuación, seleccione **Sí, anular la administración de la aplicación**.

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

Anule la gestión del clúster que ya no desea administrar desde Astra Control Center.

- Con esta acción, Astra Control Center no gestiona su clúster. No realiza cambios en la configuración del clúster y no elimina el clúster.
- Trident no se desinstalará del clúster. "Descubra cómo desinstalar Trident".

> Antes de anular la administración del clúster, debe anular la administración de las aplicaciones asociadas al clúster.

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla de comprobación del clúster que ya no desea gestionar en Astra Control Center.
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** y después de que el clúster se eliminará de la página **Clusters** y Astra Control Center ya no lo gestiona.

> **Si el Centro de control de Astra y Cloud Insights no están conectados**, al anular la gestión del clúster se quitan todos los recursos que se instalaron para enviar datos de telemetría. **Si el Centro de control de Astra y Cloud Insights están conectados**, al anular la gestión del clúster sólo se elimina el `fluentbit` y.. `event-exporter` pods.

Actualice Astra Control Center

Para actualizar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y complete estas instrucciones para actualizar los componentes de Astra Control Center en su entorno. Puede utilizar este procedimiento para actualizar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Lo que necesitará

- "Antes de comenzar la actualización, asegúrese de que su entorno cumple los requisitos mínimos para la implementación de Astra Control Center".
- Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

```
kubectl get clusteroperators
```

- Asegúrese de que todos los servicios de API están en buen estado y disponibles.

```
kubectl get apiservices
```

- Cierre la sesión en 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:

- Descargue el paquete Astra Control Center
- Desembale el paquete y cambie el directorio
- Agregue las imágenes al registro local
- Instale el operador actualizado de Astra Control Center
- Actualice Astra Control Center
- Actualizar servicios de terceros (opcional)
- Comprobar el estado del sistema
- Configure la entrada para el equilibrio de carga

No ejecute el siguiente comando durante todo el proceso de actualización para evitar eliminar todas las POD de Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

Realice actualizaciones en una ventana de mantenimiento cuando no se estén ejecutando las programaciones, los backups y las snapshots.

Los comandos de Podman se pueden utilizar en lugar de los comandos de Docker si está utilizando Podman de Red Hat en lugar de Docker Engine.

Descargue el paquete Astra Control Center

1. Descargue el paquete de actualización de Astra Control Center (`astra-control-center-[version].tar.gz`) Del sitio de soporte https:mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp].
2. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

Desembale el paquete y cambie el directorio

1. Extraiga las imágenes:

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

Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR_REGISTRY> como se indica en los comentarios:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Instale el operador actualizado de Astra Control Center

1. Cambie el directorio:

```
cd manifests
```

2. Edite la implementación del operador de Astra Control Center yaml (`astra_control_center_operator_deploy.yaml`) para referirse a su registro local y secreto.

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

b. Cambiar `[your_registry_path]` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

c. Cambiar `[your_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

d. 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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. 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.astra.
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
```

4. Verifique que los pods se estén ejecutando:

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

Actualice Astra Control Center

1. Editar el recurso personalizado de Astra Control Center (CR) (`astra_control_center_min.yaml`) Y cambie la versión Astra (`astraVersion` dentro de `Spec`) número a la última:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> La ruta de acceso del Registro debe coincidir con la ruta de acceso del Registro en la que ha insertado las imágenes en un paso anterior.

2. 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
```

3. Debe realizar una de las siguientes acciones:
   a. Si no tiene su propio IngressController o Ingress y ha estado utilizando el Astra Control Center con su puerta de enlace Traefik como servicio de tipo LoadBalancer y desea continuar con esa configuración, especifique otro campo `ingressType` (si aún no está presente) y configúrelo en `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Si desea cambiar a la implementación de entrada genérica predeterminada de Astra Control Center, proporcione su propia configuración IngressController/Ingress (con terminación TLS, etc.), abra una ruta a Astra Control Center y establezca `ingressType` para `Generic`.

      ```
      ingressType: Generic
      ```

      Si omite el campo, el proceso se convierte en la implementación genérica. Si no desea la implementación genérica, asegúrese de agregar el campo.

4. (Opcional) Verifique que los POD terminan y estén disponibles de nuevo:

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

5. Espere a que las condiciones de estado de Astra indiquen que la actualización está completa y lista:

   ```
   kubectl get -o yaml -n [netapp-acc or custom namespace]
   astracontrolcenters.astra.netapp.io astra
   ```

   Respuesta:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

6. Vuelva a iniciar sesión y compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.
7. Si el operador no actualizó el gerente de cert, actualice los servicios de terceros, a continuación.

Actualizar servicios de terceros (opcional)

Los servicios de otros fabricantes Traefik y Cert-Manager no se actualizan durante los pasos de actualización anteriores. Opcionalmente, puede actualizarlos con el procedimiento descrito aquí o conservar versiones de servicio existentes si su sistema lo requiere.

- **Traefik**: Por defecto, Astra Control Center gestiona el ciclo de vida de la implementación de Traefik. Ajuste `externalTraefik` para `false` (Predeterminado) indica que no existe ninguna Traefik externa en el sistema y que Astra Control Center está instalando y gestionando Traefik. En este caso, `externalTraefik` se establece en `false`.

  Por otro lado, si usted tiene su propio despliegue de Traefik, set `externalTraefik` para `true`. En este caso, usted mantiene la implementación y Astra Control Center no actualizará los CRD, a menos que `shouldUpgrade` se establece en `true`.

- **Cert-Manager**: De forma predeterminada, Astra Control Center instala el cert-Manager (y CRD) a menos que usted establezca `externalCertManager` para `true`. Configurado `shouldUpgrade` para `true` Para que Astra Control Center actualice los CRD.

Traefik se actualiza si se cumple alguna de las siguientes condiciones:

- ExternalTraefik: Falso
- ExternalTraefik: Verdadero Y deberíldUpgrade: Verdadero.

Pasos

1. Edite el `acc` CR:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

2. Cambie el `externalTraefik` y la `shouldUpgrade` campo para uno de los dos `true` o. `false` según se necesite.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

Comprobar el estado del sistema

1. Inicie sesión en Astra Control Center.
2. Compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.

Configure la entrada para el equilibrio de carga

Puede configurar un objeto de entrada de Kubernetes que gestione el acceso externo a los servicios, como el equilibrio de carga en un clúster.

- La actualización predeterminada utiliza la implementación de ingreso genérico. En este caso, también deberá configurar un controlador de entrada o un recurso de entrada.
- Si no desea un controlador de entrada y desea conservar lo que ya tiene, configure `ingressType` para `AccTraefik`.

> Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte "Requisitos".

Los pasos varían en función del tipo de controlador de entrada que utilice:

- Controlador de entrada nginx
- Controlador OpenShift Ingress

Lo que necesitará

- En la especificación CR,
  - Si `crd.externalTraefik` está presente, debe estar configurado en `false` O.
  - Si `crd.externalTraefik` es `true`, `crd.shouldUpgrade` también debería ser `true`.
- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.
- Se utilizan versiones de Kubernetes entre e incluidas v1.19 y v1.21.

Pasos para el controlador de entrada Nginx

1. Utilice el secreto existente `secure-testing-cert` o 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) para un esquema obsoleto o nuevo:
   a. Para un esquema obsoleto, siga este ejemplo:

```
apiVersion: extensions/v1beta1
kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Para un nuevo esquema, siga 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
```

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
```

Compruebe la configuración de entrada

Puede verificar la configuración de entrada antes de continuar.

1. Asegúrese de que Traefik ha cambiado a. `clusterIP` Desde LoadBalancer:

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

2. Verificar rutas en Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

El resultado debe estar vacío.

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.

Lo que necesitará

- Utilice la interfaz de usuario de Astra Control Center para anular la gestión de todos "de clúster".

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_min.yaml -n netapp-acc
   ```

   Resultado:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utilice el siguiente comando para eliminar la `netapp-acc` espacio de nombres:

   ```
   kubectl delete ns netapp-acc
   ```

   Resultado:

   ```
   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"

Automatización con la API de REST

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 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"

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

- "**Knowledge base** (se requiere inicio de sesión)": Buscar artículos, preguntas frecuentes o romper información relacionada con Astra Control.
- **Centro de documentación**: Este es el sitio de documentación 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 de definición de recursos personalizados (CRD) de Astra Control Center (`astra_control_center_min.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 22.04"
- "Documentación de Astra Control Center 21.12"
- "Documentación de Astra Control Center 21.08"

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"
- "Aviso para Astra Data Store"

Licencia Astra Control API

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf