



Documentación de Astra Control Center 23,04

Astra Control Center

NetApp
November 21, 2023

Tabla de contenidos

- Documentación de Astra Control Center 23,04 1
- Notas de la versión. 2
 - Novedades de esta versión de Astra Control Center 2
 - Problemas conocidos 5
 - Limitaciones conocidas 9
- Manos a la obra 14
 - Más información sobre Astra Control 14
 - Requisitos del Centro de Control de Astra 17
 - Inicio rápido para Astra Control Center 22
 - Información general de la instalación 24
 - Configure Astra Control Center 90
 - Preguntas frecuentes para Astra Control Center 110
- Conceptos 113
 - Arquitectura y componentes 113
 - Protección de datos 114
 - Licencia 117
 - Gestión de aplicaciones 119
 - Clases de almacenamiento y tamaño de volumen persistente 121
 - Roles de usuario y espacios de nombres 121
 - Seguridad de POD 122
- Utilice Astra Control Center 125
 - Inicie la gestión de aplicaciones 125
 - Proteja sus aplicaciones 130
 - Supervise el estado de las aplicaciones y del clúster 159
 - Gestione su cuenta 162
 - Gestionar bloques 172
 - Gestione el entorno de administración del almacenamiento 175
 - Supervisar tareas en ejecución 178
 - Supervise la infraestructura con conexiones Cloud Insights, Prometheus o Fluentd 179
 - Desgestione aplicaciones y clústeres 188
 - Actualice Astra Control Center 189
 - Desinstale Astra Control Center 198
- Automatice con la API REST de Astra Control 202
 - Automatización mediante la API REST de Astra Control 202
- Conocimiento y apoyo 203
 - Resolución de problemas 203
 - Obtenga ayuda 203
- Versiones anteriores de la documentación de Astra Control Center 206
- Avisos legales 207
 - Derechos de autor 207
 - Marcas comerciales 207
 - Estadounidenses 207
 - Política de privacidad 207

Código abierto	207
Licencia Astra Control API	207

Documentación de Astra Control Center 23,04

Notas de la versión

Nos complace anunciar la última versión de Astra Control Center.

- ["¿Qué hay en esta versión de Astra Control Center"](#)
- ["Problemas conocidos"](#)
- ["Limitaciones conocidas"](#)

Síguenos 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.

18 de mayo de 2023 (23.04.2)

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

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

25 de abril de 2023 (23.04.0)

Nuevas funciones y soporte

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

Problemas y limitaciones conocidos

- ["Problemas conocidos de esta versión"](#)
- ["Limitaciones conocidas de esta versión"](#)

22 de noviembre de 2022 (22.11.0)

Detalles

Nuevas funciones y soporte

- ["Compatibilidad con aplicaciones que abarcan varios espacios de nombres"](#)
- ["Soporte para incluir recursos de clúster en una definición de aplicación"](#)
- ["Autenticación LDAP mejorada con integración de control de acceso basado en roles \(RBAC\)"](#)
- ["Compatibilidad añadida para Kubernetes 1.25 y admisión de seguridad en Pod \(PSA\)"](#)
- ["Generación de informes de progreso mejorado para sus operaciones de backup, restauración y clonado"](#)

Problemas y limitaciones conocidos

- ["Problemas conocidos de esta versión"](#)
- ["Limitaciones conocidas de esta versión"](#)

8 de septiembre de 2022 (22.08.1)

Detalles

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)

Detalles

Nuevas funciones y soporte

- ["Replicación de aplicaciones con la tecnología SnapMirror de NetApp"](#)
- ["Flujo de trabajo de gestión de aplicaciones mejorado"](#)
- ["Mejora la funcionalidad de enlaces de ejecución propios"](#)



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

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

Problemas y limitaciones conocidos

- ["Problemas conocidos de esta versión"](#)
- ["Limitaciones conocidas de esta versión"](#)

26 de abril de 2022 (22.04.0)

Detalles

Nuevas funciones y soporte

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

Problemas y limitaciones conocidos

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

14 de diciembre de 2021 (21.12)

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"
- "Actualizaciones de Astra Control Center"
- "Opción Red Hat OperatorHub para la instalación"

Problemas resueltos

- "Se han resuelto problemas para esta versión"

Problemas y limitaciones conocidos

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

5 de agosto de 2021 (21.08)

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"](#)
- ["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](#)
- [04](#)
- [04 a 23.04.2](#)
- [Un pod de supervisión puede fallar en entornos Istio](#)

Otros temas

- [Los clústeres gestionados no aparecen en Cloud Insights de NetApp cuando se conectan a través de un proxy](#)
- [Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio \(500\) cuando Astra Trident está sin conexión](#)

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.

Algunos pods no se inician después de actualizar a Astra Control Center 23,04

Después de actualizar a Astra Control Center 23,04, es posible que algunos pods no se inicien. Como solución alternativa, reinicie manualmente los pods afectados mediante los siguientes pasos:

1. Busque los pods afectados y sustituya a <namespace> por el espacio de nombres actual:

```
kubectl get pods -n <namespace> | grep au-pod
```

Los pods afectados tendrán resultados similares a los siguientes:

```
pcloud-astra-control-center-au-pod-0 0/1 CreateContainerConfigError 0  
13s
```

2. Reinicie cada pod afectado, sustituyendo <namespace> por el espacio de nombres actual:

```
kubectl delete pod pcloud-astra-control-center-au-pod-0 -n <namespace>
```

Algunos pods muestran un estado de error después de la etapa de depuración de la actualización de 23,04 a 23.04.2

Después de actualizar a Astra Control Center 23.04.2, es posible que algunos pods muestren un error en registros relacionados con task-service-task-purge:

```
kubectl get all -n netapp-acc -o wide|grep purge  
  
pod/task-service-task-purge-28282828-ab1cd      0/1      Error      0  
48m      10.111.0.111      openshift-clstr-ol-07-zwlj8-worker-jhp2b      <none>  
<none>
```

Este estado de error significa que un paso de limpieza no se ejecutó correctamente. La actualización general a 23.04.2 se realiza correctamente. Ejecute el siguiente comando para limpiar la tarea y eliminar el estado de error:

```
kubectl delete job task-service-task-purge-[system-generated task ID] -n  
<netapp-acc or custom namespace>
```

Un pod de supervisión puede fallar en entornos Istio

Si emparejas Astra Control Center con Cloud Insights en un entorno de Istio, el telegraf-rs el pod puede bloquearse. Para solucionar esta solución, siga estos pasos:

1. Busque el pod averiado:

```
kubectl -n netapp-monitoring get pod | grep Error
```

Debería ver una salida similar a la siguiente:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
```

2. Reinicie el pod averiado, sustituyéndolo <pod_name_from_output> con el nombre del pod afectado:

```
kubectl -n netapp-monitoring delete pod <pod_name_from_output>
```

Debería ver una salida similar a la siguiente:

```
pod "telegraf-rs-fhhrh" deleted
```

3. Compruebe que el pod se ha reiniciado y que no está en un estado de error:

```
kubectl -n netapp-monitoring get pod
```

Debería ver una salida similar a la siguiente:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-rrnsb 2/2 Running 0 11s
```

Los clústeres gestionados no aparecen en Cloud Insights de NetApp cuando se conectan a través de un proxy

Cuando Astra Control Center se conecta a Cloud Insights de NetApp mediante un proxy, es posible que los clústeres gestionados no aparezcan en Cloud Insights. Para solucionar esta solución, ejecute los siguientes comandos en cada clúster gestionado:

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\ \[\[outputs.http\]\]n \ use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\ \[\[outputs.http\]\]n \ use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-  
ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-  
monitoring pod
```

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.

Obtenga más información

- ["Limitaciones conocidas"](#)

Limitaciones conocidas

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

Limitaciones de gestión de clústeres

- [Dos instancias de Astra Control Center no pueden gestionar el mismo clúster](#)
- [Astra Control Center no puede gestionar dos clústeres con el mismo nombre](#)

Limitaciones de control de acceso basado en roles (RBAC)

- [Un usuario con restricciones de RBAC de espacio de nombres puede añadir y anular la gestión de un clúster](#)
- [Un miembro con restricciones de espacio de nombres no puede acceder a las aplicaciones clonadas o restauradas hasta que el administrador agregue el espacio de nombres a la restricción](#)

Limitaciones en la gestión de aplicaciones

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

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](#)
- [Limitaciones de usuarios y grupos LDAP](#)
- [La página Actividad muestra hasta 100000 eventos](#)
- [25 o posteriores con ciertas versiones de controladoras Snapshot](#)

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

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

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

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

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

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

Para solucionar este problema, haga lo siguiente:

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

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

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

```
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
  ExAmPLERb2tCcJZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
  server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
  cluster: xyz-cluster
  namespace: default
  user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

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

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

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

Cualquiera `member` El usuario con limitaciones de RBAC por nombre/ID de espacio de nombres puede clonar o restaurar una aplicación en un espacio de nombres nuevo en el mismo clúster o en cualquier otro clúster de la cuenta de la organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. 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.

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

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

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

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

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

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

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

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

- ["Apache K8ssandra"](#)



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

- ["Jenkins CI"](#)
- ["Clúster Percona XtraDB"](#)

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



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

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

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

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

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

Las aplicaciones implementadas con Helm 2 no son compatibles

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

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.

Limitaciones de usuarios y grupos LDAP

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

La página Actividad muestra hasta 100000 eventos

La página Actividad de Astra Control puede mostrar hasta 100.000 eventos. Para ver todos los eventos registrados, recupere los eventos mediante ["API REST de Astra Control"](#).

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

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

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

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

Obtenga más información

- ["Problemas conocidos"](#)

Manos a la obra

Más información sobre Astra Control

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

Funciones

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

- Gestione automáticamente el almacenamiento persistente
- Crear copias Snapshot y backups bajo demanda que se tienen en cuenta las aplicaciones
- Automatice las operaciones de backup y Snapshot condicionadas por políticas
- Migre aplicaciones y datos de un clúster de Kubernetes a otro
- Replicar aplicaciones en un sistema remoto mediante la tecnología SnapMirror de NetApp (Astra Control Center)
- Clone aplicaciones de almacenamiento provisional a producción
- Visualizar el estado de la protección y el estado de la aplicación
- Trabaje con una interfaz de usuario web o una API para implementar sus flujos de trabajo de backup y migración

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de implementación:

- **Astra Control Service:** Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.
- **Astra Control Center:** Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local. Astra Control Center también se puede instalar en varios entornos de proveedores de cloud con un back-end de almacenamiento de NetApp Cloud Volumes ONTAP.

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

	Servicio de control Astra	Astra Control Center
¿Cuáles son los back-ends de almacenamiento compatibles?	<ul style="list-style-type: none"> • Servicios web de Amazon: <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Amazon FSX para ONTAP de NetApp ◦ "Cloud Volumes ONTAP" • Google Cloud: <ul style="list-style-type: none"> ◦ Disco persistente de Google ◦ Cloud Volumes Service de NetApp ◦ "Cloud Volumes ONTAP" • Azure de Microsoft: <ul style="list-style-type: none"> ◦ Discos gestionados de Azure ◦ Azure NetApp Files ◦ "Cloud Volumes ONTAP" • Clústeres autogestionados: <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Disco persistente de Google ◦ Discos gestionados de Azure ◦ "Cloud Volumes ONTAP" 	<ul style="list-style-type: none"> • Sistemas ONTAP AFF y FAS de NetApp • "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 Azure gestionó discos como back-end de almacenamiento para sus volúmenes persistentes.
 - Para clústeres de Amazon EKS, utiliza Astra Control Service ["Amazon Elastic Block Store"](#) o ["Amazon FSX para ONTAP de NetApp"](#) como back-end de almacenamiento para sus volúmenes persistentes.
- Agregue su primera tecnología Kubernetes al servicio Astra Control. A continuación, el servicio de control de Astra realiza lo siguiente:
 - Crea un almacén de objetos en su cuenta de proveedor de cloud, que es donde se almacenan las copias de backup.

En Azure, Astra Control Service también crea un grupo de recursos, una cuenta de almacenamiento y

claves para el contenedor Blob.

- Crea un nuevo rol de administrador y una cuenta de servicio de Kubernetes en el clúster.
- Utiliza la nueva función de administración para instalar ["Astra Trident"](#) en el clúster y para crear una o varias clases de almacenamiento.
- Si utiliza una oferta de almacenamiento de servicios cloud de NetApp como back-end de almacenamiento, Astra Control Service utiliza Astra Trident para aprovisionar volúmenes persistentes para sus aplicaciones. Si utiliza discos administrados de Amazon EBS o Azure como back-end de almacenamiento, deberá instalar un controlador CSI específico del proveedor. Se proporcionan instrucciones de instalación en ["Configure Amazon Web Services"](#) y.. ["Configure Microsoft Azure con discos gestionados de Azure"](#).
- En este momento, puede añadir aplicaciones al clúster. Se aprovisionan volúmenes persistentes en la nueva clase de almacenamiento predeterminada.
- A continuación, utilice Astra Control Service para gestionar estas aplicaciones y empiece a crear copias Snapshot, copias de seguridad y clones.

El plan gratuito de Astra Control le permite gestionar hasta 10 espacios de nombres en su cuenta. Si desea gestionar más de 10, deberá configurar la facturación actualizando del plan gratuito al plan Premium.

Cómo funciona Astra Control Center

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

Astra Control Center admite clústeres de Kubernetes con un tipo de almacenamiento basado en Astra Trident con un back-end de almacenamiento ONTAP 9,5 y superior.

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.

Puedes probar Astra Control Center con una licencia de evaluación integrada de 90 días. Mientras estás evaluando Astra Control Center, puedes obtener soporte a través del correo electrónico y las opciones de la comunidad. Además, tendrá acceso a los artículos de la base de conocimientos y a la documentación desde la consola de soporte del producto.

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

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

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

- Agregue un bloque de almacenamiento de objetos que almacenará las copias de seguridad de la aplicación.

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

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

Si quiere más información

- ["Documentación de Astra Control Service"](#)
- ["Documentación de Astra Control Center"](#)
- ["Documentación de Astra Trident"](#)
- ["Utilice la API Astra Control"](#)
- ["Documentación de Cloud Insights"](#)
- ["Documentación de ONTAP"](#)

Requisitos del Centro de Control de Astra

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

- [Entornos de Kubernetes de clústeres host admitidos](#)
- [Requisitos de recursos del clúster de hosts](#)
- [Requisitos de Astra Trident](#)
- [Back-ends de almacenamiento](#)
- [Registro de imágenes](#)
- [Licencia de Astra Control Center](#)
- [Licencias ONTAP](#)
- [Requisitos de red](#)
- [Entrada para clústeres de Kubernetes en las instalaciones](#)
- [Exploradores web compatibles](#)
- [Requisitos adicionales para clusters de aplicaciones](#)

Entornos de Kubernetes de clústeres host admitidos

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



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

Distribución de Kubernetes en clúster de hosts	Versiones compatibles
Azure Kubernetes Service en HCI de pila de Azure	Azure Stack HCI 21H2 y 22H2 con AKS 1,23 y 1,24
Anthos de Google	1,12 a 1,14 (consulte Requisitos de incorporación de Google Anthos)
Kubernetes (ascendente)	1,24 a 1,26 (se requiere Astra Trident 22,10 o posterior para Kubernetes 1,25 o posterior)
Motor Kubernetes de rancher (RKE)	RKE 1,3 con Rancher 2,6 RKE 1,4 con Rancher 2,7 RKE 2 (v1,23.x) con Rancher 2,6 RKE 2 (v1,24.x) con Rancher 2,7
OpenShift Container Platform de Red Hat	4,10 hasta 4,12
Grid de Kubernetes de VMware Tanzania	1,6 (consulte Requisitos de recursos del clúster de hosts)
VMware Tanzu Kubernetes Grid Integrated Edition	1,14 y 1,15 (consulte Requisitos de recursos del clúster de hosts)

Requisitos de recursos del clúster de hosts

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



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

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

Requisitos de Astra Trident

Asegúrese de cumplir los siguientes requisitos de Astra Trident específicos para las necesidades de su entorno:

- **Versión mínima para usar con Astra Control Center:** Astra Trident 22,04 o posterior instalado y configurado.
- **Replicación de SnapMirror:** Astra Trident 22,07 o posterior instalado para la replicación de aplicaciones basada en SnapMirror.
- **Para compatibilidad con Kubernetes 1,25 o posterior:** Astra Trident 22,10 o posterior instalado para Kubernetes 1,25 o clústeres más recientes (debe actualizar a Astra Trident 22,10 antes de actualizar a Kubernetes 1,25 o más reciente)
- **Configuración ONTAP con Astra Trident:**
 - *** Clase de almacenamiento*:** Configure al menos una clase de almacenamiento Astra Trident en el clúster. Si se configura una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento con la designación predeterminada.
 - **Controladores de almacenamiento y nodos de trabajo:** Asegúrese de que los nodos de trabajo en su clúster estén configurados con los controladores de almacenamiento adecuados para que los pods puedan interactuar con el almacenamiento de backend. Astra Control Center es compatible con los siguientes controladores de ONTAP proporcionados por Astra Trident:
 - `ontap-nas`
 - `ontap-san`
 - `ontap-san-economy` (la replicación de aplicaciones no está disponible con este tipo de clase de almacenamiento)
 - `ontap-nas-economy` (las copias snapshot, políticas de replicación y políticas de protección no están disponibles con este tipo de clase de almacenamiento)

Back-ends de almacenamiento

Asegúrese de tener un backend soportado con capacidad suficiente.

- **Backends soportados:** Astra Control Center soporta los siguientes backends de almacenamiento:
 - NetApp ONTAP 9,8 o sistemas AFF, FAS y ASA posteriores
 - NetApp ONTAP Select 9,8 o posterior
 - NetApp Cloud Volumes ONTAP 9,8 o posterior
- *** Capacidad de almacenamiento de backend requerida*:** Al menos 500GB disponibles

Licencias ONTAP

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

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

Para comprobar si su sistema ONTAP tiene las licencias necesarias, consulte ["Gestione licencias de ONTAP"](#).

Registro de imágenes

Debe tener un registro de imágenes de Docker privado existente en el que pueda transferir las imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.

Licencia de Astra Control Center

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

Para probar Astra Control Center, regístrate para obtener una prueba gratuita. Puede registrarse registrándose ["aquí"](#).

Para configurar la licencia, consulte ["utilice una licencia de evaluación de 90 días"](#).

Para obtener más información sobre cómo funcionan las licencias, consulte ["Licencia"](#).

Requisitos de red

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

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



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

Origen	Destino	Puerto	Protocolo	Específico
PC cliente	Astra Control Center	443	HTTPS	Acceso 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 (https://www.netapp.com/cloud-services/cloud-insights/)	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 (https://support.netapp.com)	443	HTTPS	Comunicación AutoSupport de NetApp

Entrada para clústeres de Kubernetes en las instalaciones

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



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

Para obtener más información, consulte ["Configure la entrada para el equilibrio de carga"](#).

Requisitos de incorporación de Google Anthos

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

Exploradores web compatibles

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

Requisitos adicionales para clusters de aplicaciones

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

- **Requisitos del clúster de aplicaciones:** ["Requisitos de gestión de clústeres"](#)
 - **Requisitos de aplicación gestionada:** ["Y gestión de aplicaciones"](#)
 - **Requisitos adicionales para la replicación de aplicaciones:** ["Requisitos previos de replicación"](#)

El futuro

Vea la ["inicio rápido"](#) descripción general.

Inicio rápido para Astra Control Center

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

1

Revise los requisitos del clúster de Kubernetes

Asegúrese de que su entorno cumple estos requisitos:

Clúster de Kubernetes

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

Integración de almacenamiento

- ["Compruebe que su entorno incluye la versión compatible con Astra Trident"](#)
- ["Prepare los nodos de trabajo"](#)
- ["Configure el back-end de almacenamiento de Astra Trident"](#)
- ["Configure las clases de almacenamiento de Astra Trident"](#)
- ["Instale la controladora Snapshot de volumen Astra Trident"](#)

- ["Cree una clase de snapshot de volumen"](#)

Credenciales de ONTAP

- ["Configure las credenciales de ONTAP"](#)

2

Descargue e instale Astra Control Center

Complete estas tareas de instalación:

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

3

Complete algunas tareas de configuración inicial

Complete algunas tareas básicas para comenzar:

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

4

Utilice Astra Control Center

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

- ["Gestionar aplicaciones"](#): Definir recursos para gestionar.
- ["Proteja sus aplicaciones"](#): Configurar directivas de protección y replicar, clonar y migrar aplicaciones.
- ["Gestionar cuentas"](#): Usuarios, roles, LDAP, credenciales y más.
- ["Opcionalmente, conéctese a Cloud Insights"](#): Vea las métricas sobre el estado del sistema.

Si quiere más información

- ["API de control Astra"](#)
- ["Actualice Astra Control Center"](#)
- ["Obtenga ayuda con Astra Control"](#)

Información general de la instalación

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

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

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

- ["Configurar Astra Control Center después de la instalación"](#)

Instale Astra Control Center mediante el proceso estándar

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

Otros procedimientos de instalación

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

Para ver una demostración del proceso de instalación de Astra Control Center, consulte ["este vídeo"](#).

Antes de empezar

- ["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"](#).
- 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 intenta instalar su propio administrador de certificados. De forma predeterminada, Astra Control Center instala su propio administrador de certificados durante la instalación.



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

Acerca de esta tarea

El proceso de instalación de Astra Control Center le ayuda a hacer lo siguiente:

- Instale los componentes de Astra en la `netapp-acc` (o nombre personalizado).
- Cree una cuenta predeterminada de administrador de propietario de Astra Control.
- Establecer una dirección de correo electrónico de usuario administrativo y una contraseña de configuración inicial predeterminada. A este usuario se le asigna el rol de propietario que se necesita para iniciar sesión por primera vez en la interfaz de usuario.
- Determine que se están ejecutando todas las pods de Astra Control Center.
- Instale la interfaz de usuario de Astra Control Center.



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

Pasos

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

- [Descargue y extraiga 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 extraiga Astra Control Center

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

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

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

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

4. Extraiga las imágenes del paquete Astra Control Center:

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

Instale el complemento Astra kubectl de NetApp

Puede utilizar el complemento de línea de comandos kubectl de Astra de NetApp para insertar imágenes en un repositorio de Docker local.

Antes de empezar

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

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

Pasos

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



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

```
ls kubectl-astra/
```

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

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

Agregue las imágenes al registro local

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

Docker

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:
 - Sustituya `<BUNDLE_FILE>` por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
 - Sustituya `<MY_FULL_REGISTRY_PATH>` por la URL del repositorio de Docker; por ejemplo, "`<a href="https://<docker-registry>" class="bare">https://<docker-registry>"`".
 - Reemplace `<MY_REGISTRY_USER>` por el nombre de usuario.
 - Sustituya `<MY_REGISTRY_TOKEN>` por un token autorizado para el registro.

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

Podman

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

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]
```



Antes de completar la instalación, asegúrese de que KUBECONFIG apunta al clúster en el que desea instalar Astra Control Center. El KUBECONFIG sólo puede contener un contexto.

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/23.04.2-7`).

```
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, vuelva a crear el espacio de nombres y, a continuación, vuelva a generar el secreto para el espacio de nombres.

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

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

Respuesta de ejemplo:

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

- d. Cree un secreto para netapp-acc (o nombre 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
```

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](#).

```
<strong>astra_control_center_operator_deploy.yaml</strong>
```

```
apiVersion: apps/v1
```

```

kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: [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
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_INSTALLTIMEOUT
              value: 5m
          image: [your_registry_path]/acc-operator:23.04.36
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
              port: 8081
            initialDelaySeconds: 15
            periodSeconds: 20

```

```

name: manager
readinessProbe:
  httpGet:
    path: /readyz
    port: 8081
  initialDelaySeconds: 5
  periodSeconds: 10
resources:
  limits:
    cpu: 300m
    memory: 750Mi
  requests:
    cpu: 100m
    memory: 75Mi
securityContext:
  allowPrivilegeEscalation: false
imagePullSecrets: []
securityContext:
  runAsUser: 65532
terminationGracePeriodSeconds: 10

```

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.yaml`) para realizar las configuraciones de cuenta, soporte, registro y otras necesarias:

```
vim astra_control_center.yaml
```



Una muestra anotada de AYLMA sigue estos pasos.

2. Modifique o confirme los siguientes ajustes:

`<code>accountName</code>`

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

`<code>astraVersion</code>`

Ajuste	Orientación	Tipo	Ejemplo
astraVersion	La versión de Astra Control Center para implementar. No se necesita ninguna acción para este ajuste, ya que el valor se rellenará previamente.	cadena	23.04.2-7

`<code>astraAddress</code>`

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

<code>autoSupport</code>

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

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

`<code>email</code>`

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

`<code>firstName</code>`

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

`<code>LastName</code>`

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

`<code>imageRegistry</code>`

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

Ajuste	Uso	Orientación	Tipo	Ejemplo
<code>imageRegistry.name</code>	Obligatorio	El nombre del registro de imágenes en el que se insertó las imágenes en el paso anterior . No utilizar <code>http://</code> o <code>https://</code> en el nombre del registro.	cadena	<code>example.registry.com/astra</code>
<code>imageRegistry.secret</code>	Obligatorio si la cadena introducida para <code>imageRegistry.name</code> requiere a <code>secret</code> . IMPORTANT: If you are using a registry that does not require authorization, you must delete this <code>secret</code> línea dentro <code>imageRegistry</code> o se producirá un error en la instalación.	El nombre del secreto Kubernetes utilizado para autenticarse con el registro de imágenes.	cadena	<code>astra-registry-cred</code>

`<code>storageClass</code>`

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

`<code>volumeReclaimPolicy</code>`

Ajuste	Orientación	Tipo	Opciones
volumeReclaimPolicy	De esta forma se establece la política de reclamaciones para los vehículos de Astra. Configuración de esta directiva como Retain Conserva los volúmenes persistentes una vez que Astra se elimina. Configuración de esta directiva como Delete elimina los volúmenes persistentes después de eliminar astra. Si no se establece este valor, se conservan los VP.	cadena	<ul style="list-style-type: none">• Retain (Este es el valor predeterminado)• Delete

`<code>ingressType</code>`





Ajuste	Orientación	Tipo	Opciones
ingressType	<p>Utilice uno de los siguientes tipos de entrada:</p> <p>Generic (ingressType: "Generic") (Predeterminado) Utilice esta opción cuando tenga otro controlador de entrada en uso o prefiera utilizar su propio controlador de entrada. Después de implementar Astra Control Center, deberá configurar el "controlador de entrada" Para exponer Astra Control Center con una URL.</p> <p>AccTraefik (ingressType: "AccTraefik") Utilice esta opción cuando prefiera no configurar un controlador de entrada. Esto despliega el Astra Control Center traefik Puerta de enlace como servicio de tipo Kubernetes LoadBalancer.</p> <p>Astra Control Center utiliza un servicio del tipo "LoadBalancer" (svc/traefik En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y aún no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En</p>	cadena	<ul style="list-style-type: none"> • Generic (este es el valor predeterminado) • AccTraefik

`<code>scaleSize</code>`

Ajuste	Orientación	Tipo	Opciones
scaleSize	<p>De forma predeterminada, Astra utilizará la alta disponibilidad (HA) <code>scaleSize</code> de <code>Medium</code>, Que despliega la mayoría de los servicios en HA y despliega múltiples réplicas para redundancia. Con <code>scaleSize</code> como <code>Small</code>, Astra reducirá el número de réplicas para todos los servicios excepto los servicios esenciales para reducir el consumo.</p> <p>CONSEJO: <code>Medium</code> las puestas en marcha constan de unos 100 pods (sin incluir cargas de trabajo transitorias. 100 pod se basa en la configuración de tres nodos principales y tres nodos de trabajador). Tenga en cuenta las limitaciones de límites de red por pod que pueden ser un problema en su entorno, sobre todo cuando tenga en cuenta situaciones de recuperación ante desastres.</p>	cadena	<ul style="list-style-type: none">• <code>Small</code>• <code>Medium</code> (Este es el valor predeterminado)

`<code>astraResourcesScaler</code>`

Ajuste	Orientación	Tipo	Opciones
<code>astraResourcesScaler</code>	<p>Opciones de escalado para los límites de recursos de <code>AstraControlCenter</code>. De forma predeterminada, <code>Astra Control Center</code> se despliega con solicitudes de recursos establecidas para la mayoría de los componentes de <code>Astra</code>. Esta configuración permite que la pila de software de <code>Astra Control Center</code> tenga un mejor rendimiento en entornos con un mayor nivel de carga y escalabilidad de las aplicaciones.</p> <p>Sin embargo, en situaciones que utilizan grupos de desarrollo o pruebas más pequeños, el campo <code>CR astraResourcesScaler</code> se puede establecer en <code>Off</code>. De este modo se deshabilitan las solicitudes de recursos y se puede implementar en clústeres más pequeños.</p>	cadena	<ul style="list-style-type: none">• <code>Default</code> (Este es el valor predeterminado)• <code>Off</code>

<code>additionalValues</code>

- Para el Centro de control astral y la comunicación Cloud Insights, la verificación de certificados TLS está desactivada de forma predeterminada. Puede habilitar la verificación de la certificación TLS para la comunicación entre Cloud Insights y el clúster de host del Centro de control de Astra y el clúster gestionado, añadiendo la siguiente sección en la `additionalValues`.

```
additionalValues:
  netapp-monitoring-operator:
    config:
      ciSkipTlsVerify: false
  cloud-insights-service:
    config:
      ciSkipTlsVerify: false
  telemetry-service:
    config:
      ciSkipTlsVerify: false
```

`<code>crds</code>`

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

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



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

```
<strong>astra_control_center.yaml</strong>
```

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

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

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

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

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.yaml -n [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

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



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

Comprobar el estado del sistema

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

Pasos

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

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



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

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



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

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

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

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

Ejemplo de respuesta

NAME	READY	STATUS	
RESTARTS	AGE		
acc-helm-repo-6cc7696d8f-pmhm8	1/1	Running	0
9h			
activity-597fb656dc-5rd4l	1/1	Running	0
9h			
activity-597fb656dc-mqmcw	1/1	Running	0
9h			
api-token-authentication-62f84	1/1	Running	0
9h			
api-token-authentication-68nlf	1/1	Running	0
9h			
api-token-authentication-ztgrm	1/1	Running	0
9h			
asup-669d4ddbc4-fnmwp	1/1	Running	1
(9h ago) 9h			
authentication-78789d7549-lk686	1/1	Running	0
9h			
bucket-service-65c7d95496-24x7l	1/1	Running	3
(9h ago) 9h			
cert-manager-c9f9fbf9f-k8zq2	1/1	Running	0
9h			
cert-manager-c9f9fbf9f-qj1zm	1/1	Running	0
9h			
cert-manager-cainjector-dbbbd8447-b5q1l	1/1	Running	0
9h			
cert-manager-cainjector-dbbbd8447-p5whs	1/1	Running	0
9h			
cert-manager-webhook-6f97bb7d84-4722b	1/1	Running	0
9h			
cert-manager-webhook-6f97bb7d84-86kv5	1/1	Running	0
9h			
certificates-59d9f6f4bd-2j899	1/1	Running	0
9h			
certificates-59d9f6f4bd-9d9k6	1/1	Running	0
9h			
certificates-expiry-check-28011180--1-81kxz	0/1	Completed	0
9h			
cloud-extension-5c9c9958f8-jdhrp	1/1	Running	0
9h			
cloud-insights-service-5cdd5f7f-pp8r5	1/1	Running	0
9h			
composite-compute-66585789f4-hxn5w	1/1	Running	0
9h			

composite-volume-68649f68fd-tb7p4	1/1	Running	0
9h			
credentials-dfc844c57-jsx92	1/1	Running	0
9h			
credentials-dfc844c57-xw26s	1/1	Running	0
9h			
entitlement-7b47769b87-4jb6c	1/1	Running	0
9h			
features-854d8444cc-c24b7	1/1	Running	0
9h			
features-854d8444cc-dv6sm	1/1	Running	0
9h			
fluent-bit-ds-9tlv4	1/1	Running	0
9h			
fluent-bit-ds-bpkcb	1/1	Running	0
9h			
fluent-bit-ds-cxmwX	1/1	Running	0
9h			
fluent-bit-ds-jgnhc	1/1	Running	0
9h			
fluent-bit-ds-vtr6k	1/1	Running	0
9h			
fluent-bit-ds-vxqd5	1/1	Running	0
9h			
graphql-server-7d4b9d44d5-zdbf5	1/1	Running	0
9h			
identity-6655c48769-4pwk8	1/1	Running	0
9h			
influxdb2-0	1/1	Running	0
9h			
keycloak-operator-55479d6fc6-slvmt	1/1	Running	0
9h			
krakend-f487cb465-78679	1/1	Running	0
9h			
krakend-f487cb465-rjsxx	1/1	Running	0
9h			
license-64cbc7cd9c-qxsr8	1/1	Running	0
9h			
login-ui-5db89b5589-ndb96	1/1	Running	0
9h			
loki-0	1/1	Running	0
9h			
metrics-facade-8446f64c94-x8h7b	1/1	Running	0
9h			
monitoring-operator-6b44586965-pvcl4	2/2	Running	0
9h			

nats-0	1/1	Running	0
9h			
nats-1	1/1	Running	0
9h			
nats-2	1/1	Running	0
9h			
nautilus-85754d87d7-756qb	1/1	Running	0
9h			
nautilus-85754d87d7-q8j7d	1/1	Running	0
9h			
openapi-5f9cc76544-7fnjm	1/1	Running	0
9h			
openapi-5f9cc76544-vzr7b	1/1	Running	0
9h			
packages-5db49f8b5-lrzhd	1/1	Running	0
9h			
polaris-consul-consul-server-0	1/1	Running	0
9h			
polaris-consul-consul-server-1	1/1	Running	0
9h			
polaris-consul-consul-server-2	1/1	Running	0
9h			
polaris-keycloak-0	1/1	Running	2
(9h ago) 9h			
polaris-keycloak-1	1/1	Running	0
9h			
polaris-keycloak-2	1/1	Running	0
9h			
polaris-keycloak-db-0	1/1	Running	0
9h			
polaris-keycloak-db-1	1/1	Running	0
9h			
polaris-keycloak-db-2	1/1	Running	0
9h			
polaris-mongodb-0	1/1	Running	0
9h			
polaris-mongodb-1	1/1	Running	0
9h			
polaris-mongodb-2	1/1	Running	0
9h			
polaris-ui-66fb99479-qp9gq	1/1	Running	0
9h			
polaris-vault-0	1/1	Running	0
9h			
polaris-vault-1	1/1	Running	0
9h			

polaris-vault-2 9h	1/1	Running	0
public-metrics-76fbf9594d-zmxzw 9h	1/1	Running	0
storage-backend-metrics-7d7fbc9cb9-lmd25 9h	1/1	Running	0
storage-provider-5bdd456c4b-2fftc 9h	1/1	Running	0
task-service-87575df85-dnn2q (9h ago) 9h	1/1	Running	3
task-service-task-purge-28011720--1-q6w4r 28m	0/1	Completed	0
task-service-task-purge-28011735--1-vk6pd 13m	1/1	Running	0
telegraf-ds-2r2kw 9h	1/1	Running	0
telegraf-ds-6s9d5 9h	1/1	Running	0
telegraf-ds-96jl7 9h	1/1	Running	0
telegraf-ds-hbp84 9h	1/1	Running	0
telegraf-ds-plwzv 9h	1/1	Running	0
telegraf-ds-sr22c 9h	1/1	Running	0
telegraf-rs-4sbg8 9h	1/1	Running	0
telemetry-service-fb9559f7b-mk917 (9h ago) 9h	1/1	Running	3
tenancy-559bbc6b48-5msgg 9h	1/1	Running	0
traefik-d997b8877-7xpf4 9h	1/1	Running	0
traefik-d997b8877-9xv96 9h	1/1	Running	0
trident-svc-585c97548c-d25z5 9h	1/1	Running	0
vault-controller-88484b454-2d6sr 9h	1/1	Running	0
vault-controller-88484b454-fc5cz 9h	1/1	Running	0
vault-controller-88484b454-jktld 9h	1/1	Running	0

4. (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 que se produzca un error de registro del clúster que se indica en los registros, puede volver a intentar realizar el registro a través de la ["Añada el flujo de trabajo del clúster en la interfaz de usuario de" O API](#).

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

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

Respuesta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.04.2-7	10.111.111.111
True			



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

Configure la entrada para el equilibrio de carga

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

Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

Los pasos de configuración varían en función del tipo de controlador de entrada que utilice. Astra Control Center admite muchos tipos de controladores Ingress. Estos procedimientos de configuración ofrecen ejemplos de los siguientes tipos de controladores de entrada:

- Entrada Istio
- Controlador de entrada nginx

- Controlador OpenShift Ingress

Antes de empezar

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

Pasos para la entrada de Istio

1. Configurar la entrada de Istio.



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

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

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

Comando de ejemplo:

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

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

Comando de ejemplo:

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



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

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

```

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

```

5. Aplicar los cambios:

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

6. Compruebe el estado de la entrada:

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

Respuesta:

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

7. Finalice la instalación de Astra Control Center.

Pasos para el controlador de entrada Nginx

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

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

3. Aplicar los cambios:

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



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

Pasos para el controlador de entrada de OpenShift

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

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

Inicie sesión en la interfaz de usuario de Astra Control Center

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



Se puede crear un certificado personalizado después de iniciar sesión.

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



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

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



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

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

Solucione los problemas de instalación

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

Opciones

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

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

- Para comprobar el resultado de Astra Control Center CR:

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

El futuro

- (Opcional) en función de su entorno, post-instalación completa "[pasos de configuración](#)".
- Complete la implementación llevando a cabo "[tareas de configuración](#)".

Configure un administrador de certificados externo

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

Pasos

1. Confirme que tiene instalado un administrador de certificados:

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

Respuesta de ejemplo:

```
cert-manager   essential-cert-manager-84446f49d5-sf2zd   1/1
Running       0      6d5h
cert-manager   essential-cert-manager-cainjector-66dc99cc56-91dmt   1/1
Running       0      6d5h
cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq   1/1
Running       0      6d5h
```

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

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

Respuesta de ejemplo:

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

3. Crear un secreto con archivos generados previamente:

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

Respuesta de ejemplo:

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

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

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

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

Respuesta de ejemplo:

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

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

```
kubectl get ClusterIssuer
```

Respuesta de ejemplo:

NAME	READY	AGE
astra-ca-clusterissuer	True	9s

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

Instale Astra Control Center utilizando OpenShift OperatorHub

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

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

Antes de empezar

- **Requisitos ambientales cumplidos:** ["Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center"](#).
- **Operadores de cluster sanos y servicios API:**
 - En el clúster de OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado:

```
oc get clusteroperators
```

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

```
oc get apiservices
```

- **Dirección FQDN:** Obtenga una dirección FQDN para Astra Control Center en su centro de datos.
- **Permisos de OpenShift:** Obtenga los permisos necesarios y acceda a Red Hat OpenShift Container Platform para realizar los pasos de instalación descritos.
- **Administrador de certificados configurado:** Si ya existe un administrador de certificados en el clúster, deberá realizar algunas ["requisitos previos"](#) Por lo tanto, Astra Control Center no instala su propio administrador de certificados. De forma predeterminada, Astra Control Center instala su propio administrador de certificados durante la instalación.
- **Controlador de entrada de Kubernetes:** Si tiene un controlador de entrada de Kubernetes que gestiona el acceso externo a servicios, como el equilibrio de carga en un clúster, debe configurarlo para su uso con Astra Control Center:
 - a. Crear el espacio de nombres del operador:

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

- b. ["Completar la configuración"](#) para el tipo de controlador de entrada.

Pasos

- [Descargue y extraiga 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 extraiga Astra Control Center

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

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

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

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

4. Extraiga las imágenes del paquete Astra Control Center:

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

Instale el complemento Astra kubectl de NetApp

Puede utilizar el complemento de línea de comandos kubectl de Astra de NetApp para insertar imágenes en un repositorio de Docker local.

Antes de empezar

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

Pasos

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



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

```
ls kubectl-astra/
```

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

```
cp kubect1-astra/<binary-name> /usr/local/bin/kubect1-astra
```

Agregue las imágenes al registro local

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

Docker

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

```
acc.manifest.bundle.yaml
acc/
```

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

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

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

Podman

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

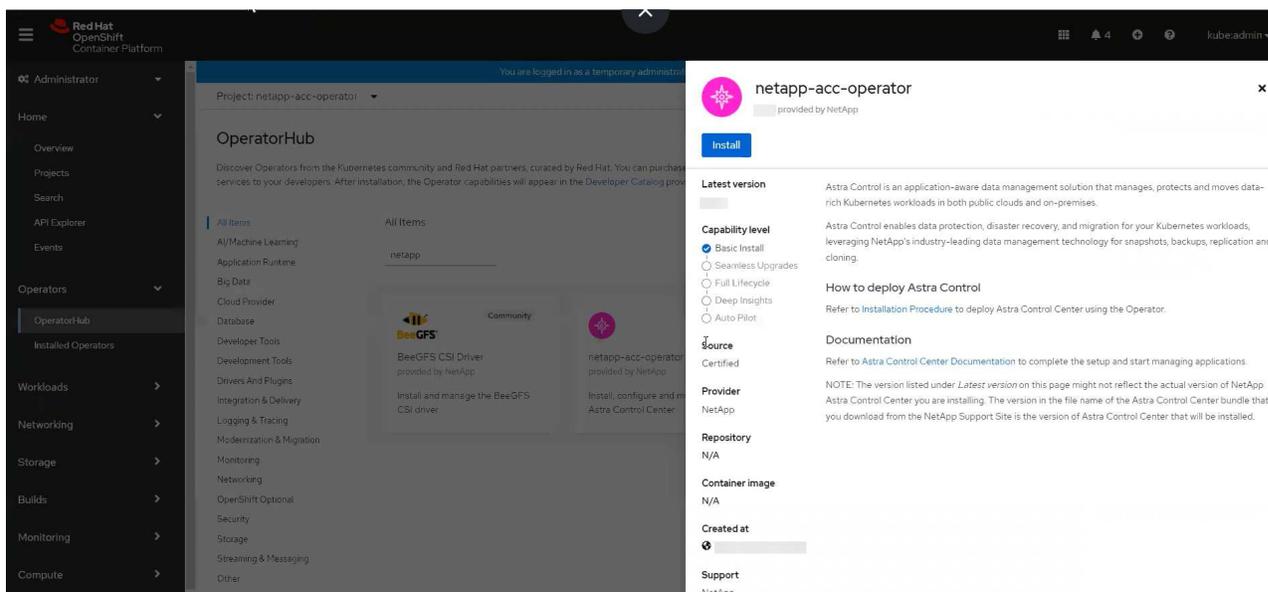
https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

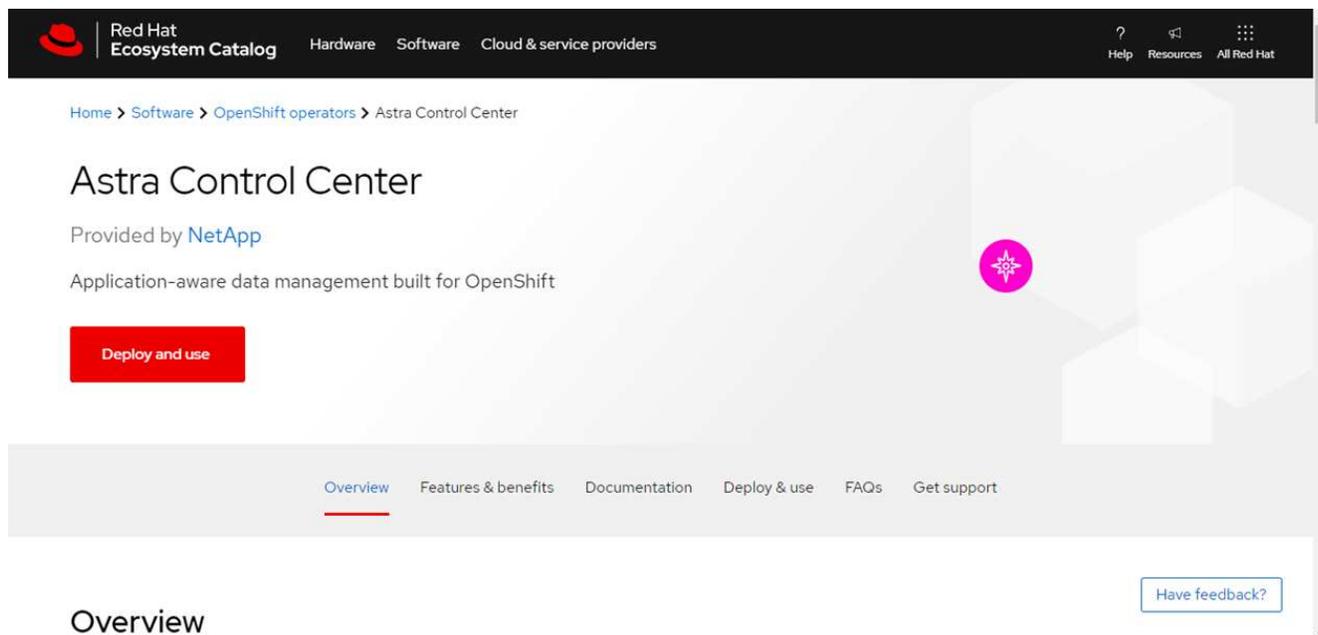
Busque la página de instalación del operador

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. Busque y seleccione el operador Centro de control Astra de NetApp.



- 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**.

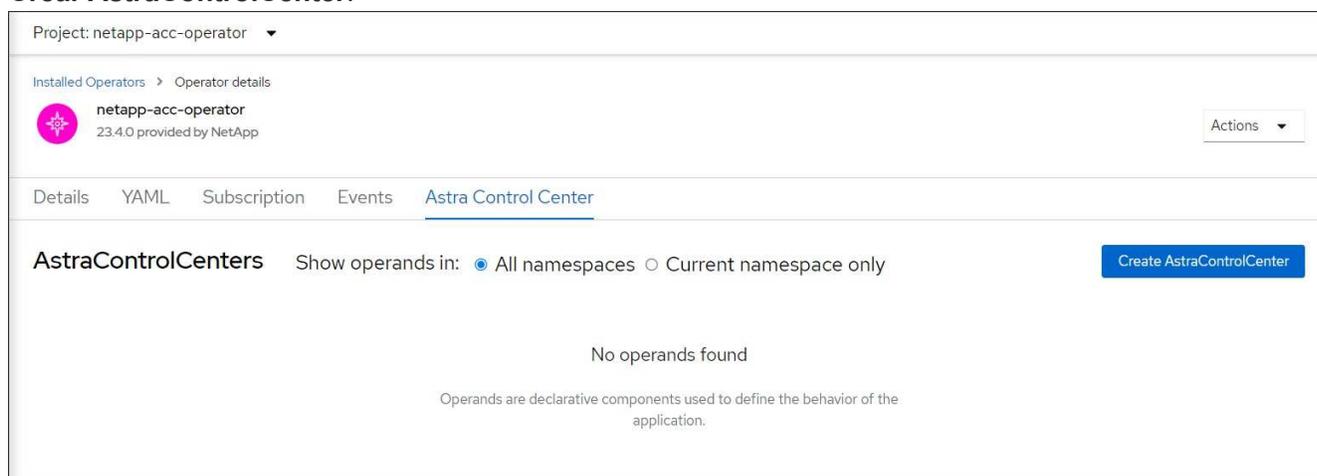


Si ha seleccionado una estrategia de aprobación manual, se le pedirá que apruebe el plan de instalación manual para este operador.

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

Instalar Astra Control Center

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



2. Complete el `Create AstraControlCenter` campo de formulario:
 - a. Mantenga o ajuste el nombre del Centro de control de Astra.
 - b. Agregue etiquetas para Astra Control Center.
 - c. Habilitar o deshabilitar AutoSupport. Se recomienda conservar la funcionalidad de AutoSupport.
 - d. Introduzca el FQDN o la dirección IP de Astra Control Center. No entre `http://` o `https://` en el campo de dirección.
 - e. Introduce la versión de Astra Control Center; por ejemplo, `23.04.2-7`.
 - f. Introduzca un nombre de cuenta, una dirección de correo electrónico y un apellido de administrador.
 - g. Seleccione una política de reclamaciones de volumen de `Retain`, `Recycle`, o `Delete`. El valor predeterminado es `Retain`.
 - h. Seleccione el `scaleSize` de la instalación.



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

i. Seleccione el tipo de entrada:

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

Utilice esta opción cuando tenga otro controlador de entrada en uso o prefiera utilizar su propio controlador de entrada. Después de implementar Astra Control Center, deberá configurar el ["controlador de entrada"](#) Para exponer Astra Control Center con una URL.

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

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

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



Para obtener detalles sobre el tipo de servicio de "LoadBalancer" e Ingress, consulte ["Requisitos"](#).

- a. En **Registro de imágenes**, introduzca la ruta de registro de la imagen del contenedor local. No entre `http://` o `https://` en el campo de dirección.
- b. Si utiliza un registro de imágenes que requiere autenticación, introduzca el secreto de imagen.



Si utiliza un registro que requiere autenticación, [cree un secreto en el clúster](#).

- c. Introduzca el nombre del administrador.
- d. Configure el escalado de recursos.
- e. Proporcione la clase de almacenamiento predeterminada.



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

f. Defina las preferencias de manejo de CRD.

3. Seleccione la vista YAML para revisar los ajustes seleccionados.
4. Seleccione `Create`.

Cree un secreto de registro

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

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

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

2. Cree un secreto en este espacio de nombres:

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



Astra Control sólo admite secretos de registro Docker.

3. Complete los campos restantes en [El campo de formulario Create AstraControlCenter](#).

El futuro

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

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

Con Astra Control Center, puede gestionar sus aplicaciones en un entorno de cloud híbrido con clústeres de Kubernetes e instancias de Cloud Volumes ONTAP autogestionados. 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 BlueXP, anteriormente 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	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>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.</p> </div>
Configuración de Astra Trident/ONTAP	<p>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 de Kubernetes a NetApp BlueXP (anteriormente Cloud Manager). Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san csi.trident.netapp.io</code>



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. [Configuración de BlueXP de NetApp para AWS.](#)

5. [Instale Astra Control Center para AWS.](#)

Compruebe que dispone de suficientes permisos IAM

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

Consulte "[Credenciales iniciales de AWS](#)".

Instale un clúster RedHat OpenShift en AWS

Instale un clúster RedHat OpenShift Container Platform en AWS.

Para obtener instrucciones de instalación, consulte "[Instalación de un clúster en AWS en OpenShift Container Platform](#)".

Configure AWS

A continuación, configure AWS para crear una red virtual, configurar 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.



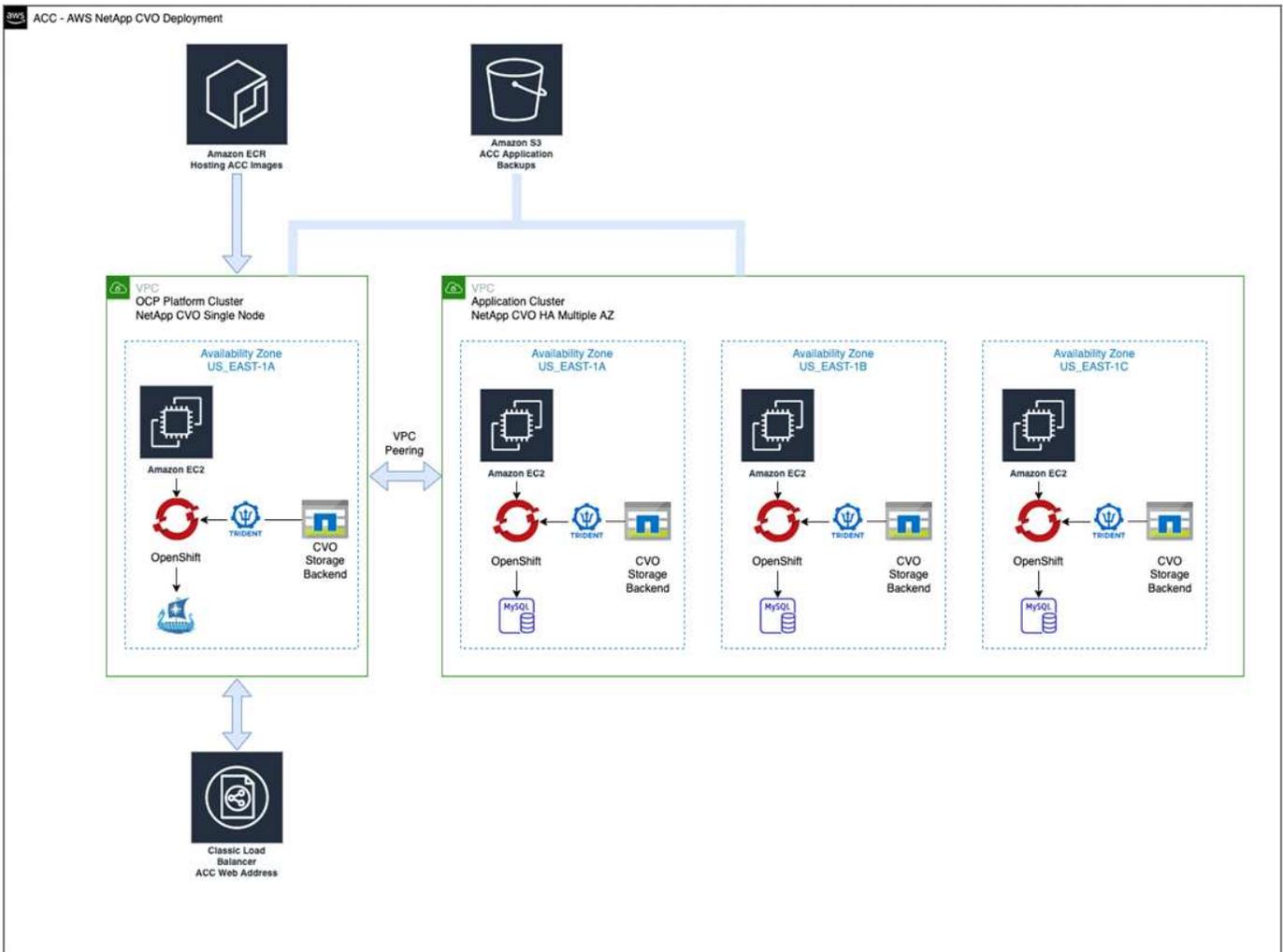
Si no crea la ECR, Astra Control Center no puede acceder a los datos de supervisión de un clúster que contenga Cloud Volumes ONTAP con un back-end de AWS. El problema se produce cuando el clúster que intenta detectar y gestionar mediante Astra Control Center no tiene acceso a AWS ECR.

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:



Configuración de BlueXP de NetApp para AWS

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

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

- ["Introducción a Cloud Volumes ONTAP en AWS"](#).
- ["Cree un conector en AWS mediante BlueXP"](#)

Pasos

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

- b. En la esquina superior derecha, observa la versión de Astra Trident.
- c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el proveedor.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento.

Astra 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.

Instale Astra Control Center para AWS

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



AWS utiliza el tipo de bloque Generic S3.

Ponga en marcha Astra Control Center en Google Cloud Platform

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

Qué necesitará para GCP

Antes de implementar Astra Control Center en GCP, 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 BlueXP, anteriormente 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	<p>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.</p> <div style="display: flex; align-items: center;">  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>
Configuración de Astra Trident/ONTAP	<p>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 BlueXP de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san csi.trident.netapp.io</code>



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. [Instalar 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. [Configurar GCP.](#)
5. [Configuración de NetApp BlueXP para GCP.](#)
6. [Instala Astra Control Center para GCP.](#)

Instalar un clúster RedHat OpenShift en GCP

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

Para obtener instrucciones de instalación, consulte lo siguiente:

- ["Instalar un clúster OpenShift en GCP"](#)
- ["Creación de una cuenta de servicio de GCP"](#)

Cree un proyecto de GCP y una nube privada virtual

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



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

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

Compruebe que dispone de suficientes permisos IAM

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

Consulte ["Credenciales y permisos iniciales de GCP"](#).

Configurar 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.

Configuración de NetApp BlueXP para GCP

Utilizando NetApp BlueXP (anteriormente Cloud Manager), crear un espacio de trabajo, añadir un conector a GCP, crear un entorno de trabajo e importar el clúster.

Siga la documentación de BlueXP para completar los siguientes pasos. Consulte "[Primeros pasos con Cloud Volumes ONTAP en GCP](#)".

Antes de empezar

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

Pasos

1. Agregue sus credenciales a BlueXP. Consulte "[Adición de cuentas de GCP](#)".
2. Añade un conector para GCP.

- a. Elija "GCP" como el proveedor.
 - b. Introduzca las credenciales de GCP. Consulte ["Creación de un conector en GCP desde BlueXP"](#).
 - c. Asegúrese de que el conector está en marcha y cambie a dicho conector.
3. Cree un entorno de trabajo para su entorno de cloud.
 - a. Ubicación: «GCP»
 - b. Tipo: "Cloud Volumes ONTAP ha"
 4. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
 - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del clúster**.
 - b. En la esquina superior derecha, 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 proveedor.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Astra 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.

Instala Astra Control Center para GCP

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



GCP utiliza el tipo de bucket 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 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 BlueXP)	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	<p>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.</p> <div style="display: flex; align-items: center;">  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>

Componente	Requisito
Configuración de Astra Trident/ONTAP	<p>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 BlueXP de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



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. [Configuración de NetApp BlueXP \(anteriormente Cloud Manager\) para Azure.](#)
6. [Instalar y configurar Astra Control Center para Azure.](#)

Instale un clúster RedHat OpenShift en Azure

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

Para obtener instrucciones de instalación, consulte lo siguiente:

- ["Instalando el clúster de OpenShift en Azure"](#).
- ["Instalar una cuenta de Azure"](#).

Cree grupos de recursos de Azure

Cree al menos un grupo de recursos de Azure.



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

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

Compruebe que dispone de suficientes permisos IAM

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

Consulte "[Credenciales y permisos de Azure](#)".

Configure Azure

A continuación, configure Azure para crear una red virtual, configurar instancias de computación, 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 $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Configure zonas DNS.

Configuración de NetApp BlueXP (anteriormente Cloud Manager) para Azure

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

Siga la documentación de BlueXP para completar los siguientes pasos. Consulte ["Introducción a BlueXP en Azure"](#).

Antes de empezar

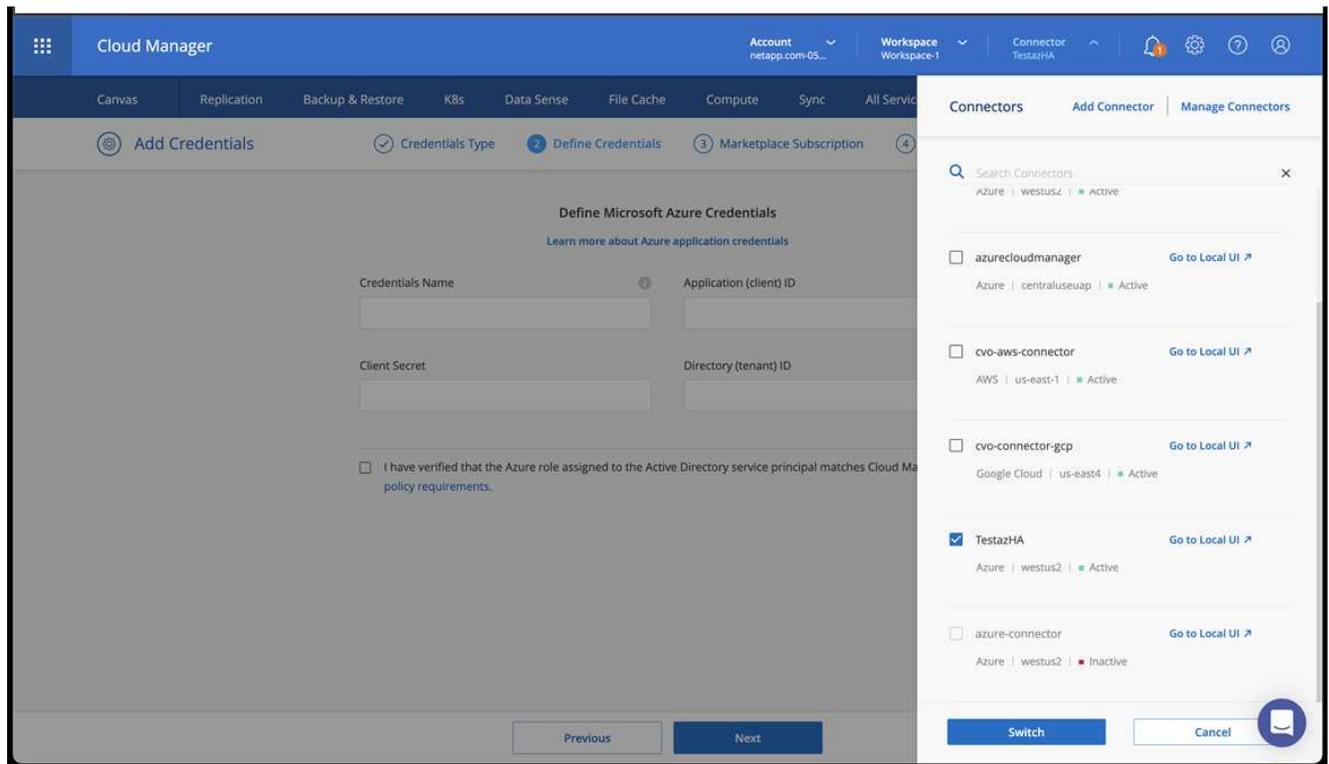
Acceso a la cuenta de Azure con los permisos y roles de IAM necesarios

Pasos

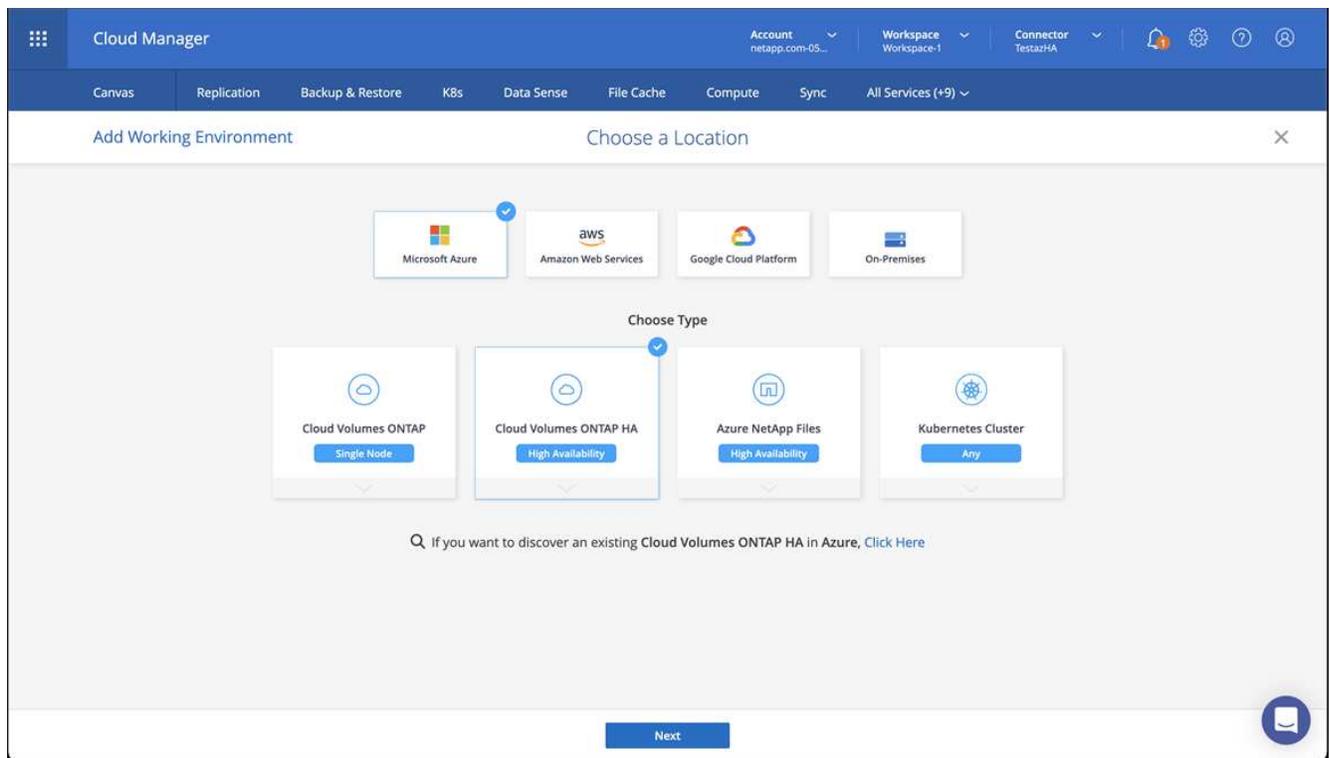
1. Agregue sus credenciales a BlueXP.
2. Agregue un conector para Azure. Consulte ["Políticas de BlueXP"](#).
 - a. Elija **Azure** como proveedor.
 - b. Introduzca las credenciales de Azure, incluidos el ID de aplicación, el secreto de cliente y el ID del directorio (inquilino).

Consulte ["Creación de un conector en Azure desde BlueXP"](#).

3. Asegúrese de que el conector está en marcha y cambie a dicho conector.

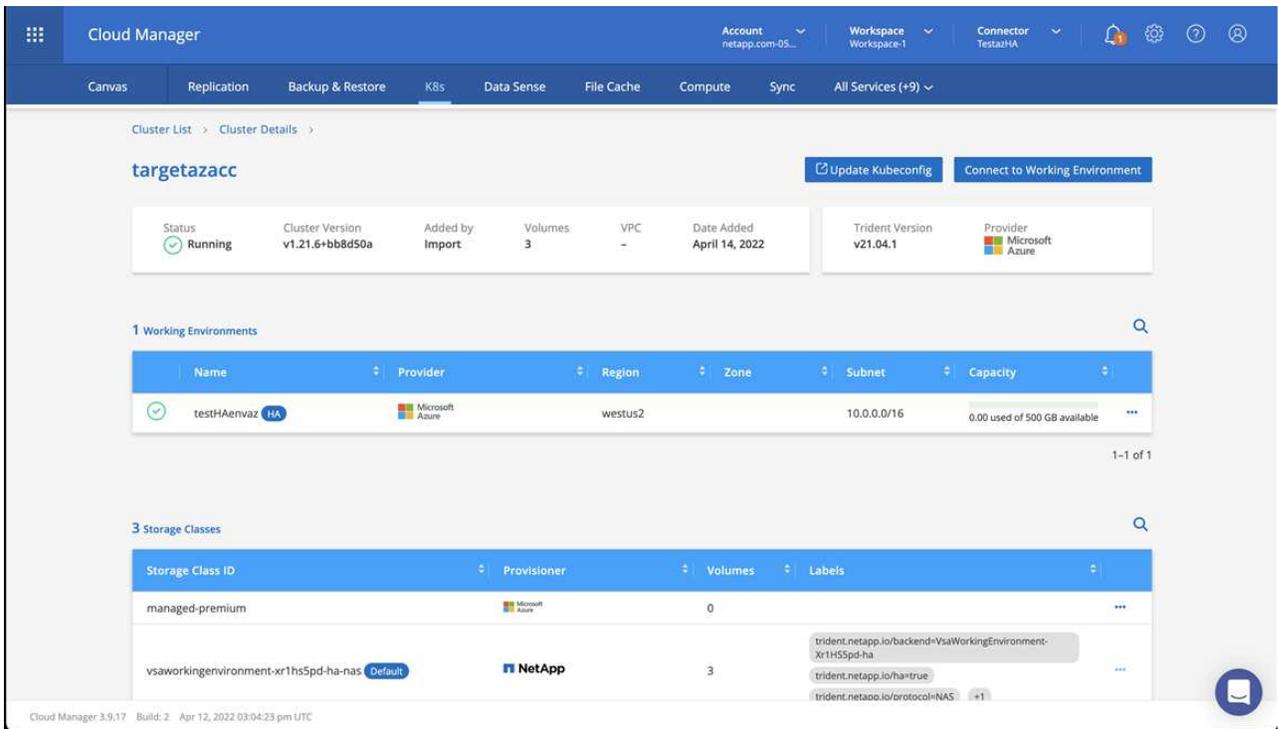


4. Cree un entorno de trabajo para su entorno de cloud.
 - a. Ubicación: "Microsoft Azure".
 - b. Tipo: "Cloud Volumes ONTAP ha".



5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
 - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del**

clúster.



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

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

Esto importa su clúster de Red Hat OpenShift y asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento.

Astra 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 para Azure

Instale Astra Control Center con el estándar "[instrucciones de instalación](#)".

Con Astra Control Center, añada un bucket de Azure. Consulte "[Configure Astra Control Center y añada cucharones](#)".

Configurar Astra Control Center después de la instalación

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

Quite las limitaciones de recursos

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

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

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

Pasos

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

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

Respuesta:

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

2. Elimine todas las cuotas de recursos por nombre:

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

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

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

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

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

Respuesta:

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

4. Eliminar los rangos de límites por nombre:

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

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 y Astra Control Center se encuentran en diferentes espacios de nombres. 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 or custom namespace]
```

2. Para cada objeto NetworkPolicy devuelto por el comando anterior, utilice el siguiente comando para eliminarlo. Reemplace [OBJECT_NAME] por el nombre del objeto devuelto:

```
kubectl delete networkpolicy [OBJECT_NAME] -n [netapp-acc or custom namespace]
```

3. Aplique el siguiente archivo de recursos para configurar el `acc-avp-network-policy` Objetos para permitir que los servicios de complemento de Astra hagan 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 NAMESPACE NAME
```

4. Aplique el siguiente archivo de recursos para configurar el `acc-operator-network-policy` Objeto para permitir que el operador de Astra Control Center se comunice 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
```

Agregue un certificado TLS personalizado

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

El certificado autofirmado predeterminado se utiliza para dos tipos de conexiones:

- Conexiones HTTPS a la interfaz de usuario web de Astra Control Center
- Tráfico del controlador de entrada (sólo si el `ingressType: "AccTraefik"` la propiedad se estableció en `astra_control_center.yaml` Archivo durante la instalación de Astra Control Center)



Al reemplazar el certificado TLS predeterminado, se reemplaza el certificado utilizado para la autenticación de estas conexiones.

Antes de empezar

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

Quite el certificado autofirmado

Quite el certificado TLS autofirmado existente.

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

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

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

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

Añada un nuevo certificado mediante la línea de comandos

Añada un nuevo certificado TLS firmado por una CA.

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

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

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

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

#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:

```
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.

Configure Astra Control Center

Después de instalar Astra Control Center, iniciar sesión en la interfaz de usuario y cambiar la contraseña, querrá configurar una licencia, añadir clústeres, habilitar la autenticación, gestionar el almacenamiento y añadir buckets.

Tareas

- [Agregue una licencia de Astra Control Center](#)
- [Prepare su entorno para la gestión de clústeres con Astra Control](#)
- [Añada el clúster](#)
- [Habilite la autenticación en el back-end de almacenamiento de ONTAP](#)
- [Añada un back-end de almacenamiento](#)
- [Añadir un bucket](#)

Agregue una licencia de Astra Control Center

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

Puede añadir una nueva licencia con la interfaz de usuario de Astra Control o ["API"](#).

Las licencias de Astra Control Center miden los recursos de CPU mediante unidades de CPU de Kubernetes y representan los recursos de CPU asignados a los nodos de trabajo de todos los clústeres de Kubernetes

gestionados. Las licencias se basan en el uso de vCPU. Para obtener más información sobre cómo se calculan las licencias, consulte ["Licencia"](#).



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



Para actualizar una evaluación existente o una licencia completa, consulte ["Actualizar una licencia existente"](#).

Antes de empezar

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

Pasos

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

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



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

Prepare su entorno para la gestión de clústeres con Astra Control

Antes de añadir un clúster, debe asegurarse de que se cumplen las siguientes condiciones previas. También debe realizar comprobaciones de cumplimiento de las condiciones para asegurarse de que su clúster esté listo para añadirse a Astra Control Center y crear funciones para la gestión de clústeres.

Antes de empezar

- Asegúrese de que los nodos de trabajo del clúster estén configurados con los controladores de almacenamiento adecuados para que los pods puedan interactuar con el almacenamiento de back-end.
- Su entorno cumple con el ["requisitos del entorno operativo"](#) Para Astra Trident y Astra Control Center.
- Una versión de Astra Trident que es ["Compatible con Astra Control Center"](#) está instalado:



Puede hacerlo ["Ponga en marcha Astra Trident"](#) Usar el operador Astra Trident (manualmente o mediante un gráfico Helm) o. `tridentctl`. Antes de instalar o actualizar Astra Trident, revise ["compatibles con front-ends, back-ends y configuraciones de host"](#).

- **El backend de almacenamiento Astra Trident configurado:** Debe haber al menos un backend de almacenamiento Astra Trident ["configurado"](#) en el clúster.
- **Clases de almacenamiento Astra Trident configuradas:** Al menos una clase de almacenamiento

Astra Trident debe ser "configurado" en el clúster. Si se configura una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento que tiene la anotación predeterminada.

- **Astra Trident volume snapshot Controller y volume snapshot class instalado y configurado:** La controladora de instantáneas de volumen debe ser "instalado" Para poder crear instantáneas en Astra Control. Al menos un Astra Trident VolumeSnapshotClass ha sido "configuración" por un administrador.
- **Kubeonfig accesible:** Usted tiene acceso al "imagen de agrupación" esto incluye sólo un elemento de contexto.
- **Credenciales de ONTAP:** Necesita credenciales de ONTAP y un superusuario e ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center.

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

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

- **Sólo rancher:** Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.

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 Astra Trident.

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

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

```
NAME          VERSION
trident       22.10.0
```

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

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



Si Astra Trident no está instalado o la versión instalada no es la más reciente, debe instalar la versión más reciente de Astra Trident antes de continuar. Consulte la "[Documentación de Astra Trident](#)" si desea obtener instrucciones.

2. Asegúrese de que los pods estén ejecutando:

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

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

```
kubectl get sc
```

Respuesta de ejemplo:

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

Cree una imagen de rol de clúster limitada

Opcionalmente, puede crear una función de administrador limitada para Astra Control Center. Este procedimiento no es obligatorio para la configuración de Astra Control Center. Este procedimiento ayuda a crear una imagen de kubeconfig independiente que limita los permisos de control de Astra en los clústeres que gestiona.

Antes de empezar

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

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



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

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

Pasos

1. Cree una cuenta de servicio:

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

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>
```

+

```
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. Cree una función de clúster limitada con los permisos mínimos necesarios para que un clúster sea gestionado por Astra Control:

- a. Cree un `ClusterRole` archivo llamado `astra-admin-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>astra-admin-account.yaml</strong>
```

+

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

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
```

```

- '*'
resources:
- '*'
verbs:
- get
- list
- create
- patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
- ""
- apps
- autoscaling
- batch
- crd.projectcalico.org
- extensions
- networking.k8s.io
- policy
- rbac.authorization.k8s.io
- snapshot.storage.k8s.io
- trident.netapp.io
resources:
- configmaps
- cronjobs
- daemonsets
- deployments
- horizontalpodautoscalers
- ingresses
- jobs
- namespaces
- networkpolicies
- persistentvolumeclaims
- poddisruptionbudgets
- pods
- podtemplates
- podsecuritypolicies
- replicaset
- replicationcontrollers
- replicationcontrollers/scale
- rolebindings
- roles
- secrets
- serviceaccounts
- services

```

```

- statefulsets
- tridentmirrorrelationships
- tridentnapshotinfos
- volumesnapshots
- volumesnapshotcontents
verbs:
- delete

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

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagedtags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use

```

a. Aplique el rol de clúster:

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

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

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

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: astra-admin-account
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:

- 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 Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

El futuro

Ahora que ha comprobado que se cumplen los requisitos previos, está listo [añadir un clúster](#).

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.



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

Antes de empezar

- Antes de añadir un clúster, revise y realice la operación necesaria [requisitos previos](#).

Pasos

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



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



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

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



Debe seleccionar una clase de almacenamiento de Astra Trident respaldada por almacenamiento de ONTAP.

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

Resultado

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



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

Habilite la autenticación en el back-end de almacenamiento de ONTAP

El Centro de control de Astra ofrece dos modos de autenticación de un back-end de ONTAP:

- **Autenticación basada en credenciales:** El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos requeridos. Debe utilizar un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin`, para garantizar la máxima compatibilidad con las versiones de ONTAP.
- **Autenticación basada en certificados:** Astra Control Center también puede comunicarse con un clúster de ONTAP utilizando un certificado instalado en el backend. Debe usar el certificado de cliente, la clave y el certificado de CA de confianza si se utilizan (recomendado).

Más adelante, puede actualizar los back-ends existentes para pasar de un tipo de autenticación a otro método. Solo se admite un método de autenticación a la vez.

Habilite la autenticación basada en credenciales

Astra Control Center requiere las credenciales para un ámbito del clúster `admin` Para comunicarse con el backend de ONTAP. Debe utilizar roles estándar predefinidos como `admin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones para que las utilicen en futuras versiones del Centro de control de Astra.



Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Astra Control Center, pero no es recomendable.

Una definición de backend de ejemplo tiene el siguiente aspecto:

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

La definición de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. De este modo, se trata de una operación exclusiva para administrador que realiza el administrador de Kubernetes o de almacenamiento.

Habilite la autenticación basada en certificados

Astra Control Center puede utilizar certificados para comunicarse con back-ends de ONTAP nuevos y existentes. Debe introducir la siguiente información en la definición de backend.

- `clientCertificate`: Certificado de cliente.
- `clientPrivateKey`: Clave privada asociada.
- `trustedCACertificate`: Certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Es posible usar uno de los siguientes tipos de certificados:

- Certificado autofirmado
- Certificado de terceros

Habilite la autenticación con un certificado autofirmado

Un flujo de trabajo típico implica los pasos siguientes.

Pasos

1. Genere una clave y un certificado de cliente. Al generar, defina el nombre común (CN) en el usuario ONTAP para autenticarse como.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
```

2. Instale el certificado de cliente de tipo `client-ca` Y el clúster de ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-  
name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Confirme que el rol de inicio de sesión de seguridad de ONTAP admite el método de autenticación de certificado.

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

4. Pruebe la autenticación mediante el certificado generado. Sustituya <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre SVM. Debe asegurarse de que la LIF tiene su política de servicio establecida en `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key --cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>
```

5. Con los valores obtenidos del paso anterior, añada el back-end del almacenamiento en la interfaz de usuario de Astra Control Center.

Active la autenticación con un certificado de terceros

Si tiene un certificado de terceros, puede configurar la autenticación basada en certificados con estos pasos.

Pasos

1. Genere la clave privada y CSR:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem -out ontap_cert_request.csr -keyout ontap_cert_request.key -addext "subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>"
```

2. Transfiera la CSR a la CA de Windows (CA de terceros) y emita el certificado firmado.
3. Descargue el certificado firmado y asígnele el nombre `ontap_signed_cert.crt`
4. Exporte el certificado raíz de Windows CA (CA de terceros).
5. Asigne un nombre a este archivo `ca_root.crt`

Ahora tiene los siguientes tres archivos:

- **Clave privada:** `ontap_signed_request.key` (Esta es la clave correspondiente para el certificado de servidor en ONTAP. Se necesita al instalar el certificado de servidor.)
 - **Certificado firmado:** `ontap_signed_cert.crt` (Esto también se denomina *server certificate* en ONTAP.)
 - **Certificado de CA raíz:** `ca_root.crt` (Esto también se denomina *server-ca certificate* en ONTAP.)
6. Instale estos certificados en ONTAP. Generar e instalar `server` y.. `server-ca` Certificados en ONTAP.

Detalles en `sample.yaml`

```
# Copy the contents of ca_root.crt and use it here.
```

```
security certificate install -type server-ca
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificate details>
```

```
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

===

```
# Copy the contents of ontap_signed_cert.crt and use it here. For key, use the contents of ontap_cert_request.key file.
```

```
security certificate install -type server
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificate details>
```

```
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
```

```
-----BEGIN PRIVATE KEY-----
```

```
<private key details>
```

```
-----END PRIVATE KEY-----
```

Enter certificates of certification authorities (CA) which form the certificate chain of the server certificate. This starts with the issuing CA certificate of the server certificate and can range up to the root CA certificate.

Do you want to continue entering root and/or intermediate certificates {y|n}: n

The provided certificate does not have a common name in the subject field.

Enter a valid common name to continue installation of the certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

==

```
# Modify the vservers settings to enable SSL for the installed certificate
```

```
ssl modify -vservers <vservers_name> -ca <CA> -server-enabled true  
-serial <serial number> (security ssl modify)
```

==

```
# Verify if the certificate works fine:
```

```
openssl s_client -CAfile ca_root.crt -showcerts -servername server  
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
```

```
CONNECTED(00000005)
```

```
depth=1 DC = local, DC = umca, CN = <CA>
```

```
verify return:1
```

```
depth=0
```

```
verify return:1
```

```
write W BLOCK
```

```
---
```

```
Certificate chain
```

```
0 s:
```

```
  i:/DC=local/DC=umca/<CA>
```

```
-----BEGIN CERTIFICATE-----
```

```
<Certificate details>
```

7. Cree el certificado de cliente para el mismo host para la comunicación sin contraseña. Astra Control Center utiliza este proceso para comunicarse con ONTAP.
8. Genere e instale los certificados de cliente en ONTAP:

Detalles en sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"
```

Copy the content of ontap_test_client.pem file and use it in the below command:

```
security certificate install -type client-ca -vserver <vserver_name>
```

Please enter Certificate: Press <Enter> when done

```
-----BEGIN CERTIFICATE-----
```

```
<Certificate details>
```

```
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

```
==
```

```
ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)
```

```
# Setting permissions for certificates
```

```
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>
```

```
security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>
```

```
==
```

```
#Verify passwordless communication works fine with the use of only
certificates:
```

```
curl --cacert ontap_signed_cert.crt --key ontap_test_client.key
--cert ontap_test_client.pem
```

```
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
```

```
{
```

```
"records": [
```

```

{
  "uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
  "name": "<aggr_name>",
  "node": {
    "uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
    "name": "<node_name>",
    "_links": {
      "self": {
        "href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
      }
    },
  },
  "_links": {
    "self": {
      "href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-4bf5378b41bd"
    }
  },
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/storage/aggregates"
  }
}
}%

```

9. Añada el back-end de almacenamiento en la interfaz de usuario de Astra Control Center y proporcione los siguientes valores:

- **Certificado de cliente:** ontap_test_client.pem
- **Clave privada:** ontap_test_client.key
- **Certificado de CA de confianza:** ontap_signed_cert.crt

Añada un back-end de almacenamiento

Puede añadir un back-end de almacenamiento de ONTAP existente a Astra Control Center para gestionar sus recursos.

Gestionar los clústeres de almacenamiento en Astra Control como back-end de almacenamiento le permite obtener vínculos entre los volúmenes persistentes (VP) y el back-end de almacenamiento, así como mediciones de almacenamiento adicionales.

Después de configurar las credenciales o la información de autenticación de certificados, puede añadir un back-end de almacenamiento de ONTAP existente a Astra Control Center para gestionar sus recursos.

Pasos

1. En el panel de control del área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione **Agregar**.
3. En la sección Usar existente de la página Agregar backend de almacenamiento, seleccione **ONTAP**.
4. Seleccione una de las siguientes opciones:
 - **Usar credenciales de administrador:** Ingrese la dirección IP de administración del clúster de ONTAP y las credenciales de administración. Las credenciales deben ser credenciales para todo el clúster.



El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, aplique las credenciales de usuario con el rol "admin", que tiene los métodos de acceso `ontapi` y `http`. En clústeres ONTAP de origen y destino. Consulte ["Gestionar cuentas de usuario en la documentación de ONTAP"](#) si quiere más información.

- **Utilice un certificado:** Cargue el certificado `.pem` archivo, la clave de certificado `.key` archivo y, opcionalmente, el archivo de entidad de certificación.

5. Seleccione **Siguiente**.
6. Confirme los detalles del backend y seleccione **Administrar**.

Resultado

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



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

Añadir un bucket

Puede añadir un bloque con la interfaz de usuario de Astra Control o **"API"**. Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina.

No necesita un bloque de Astra Control si clona la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster. La funcionalidad de snapshots de aplicaciones no requiere un bloque.

Antes de empezar

- Un cubo al que se puede acceder desde sus clusters gestionados por Astra Control Center.
- Credenciales para el bloque.
- Un bloque de los siguientes tipos:
 - NetApp ONTAP S3
 - StorageGRID S3 de NetApp
 - Microsoft Azure
 - Genérico S3



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



Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Pasos

1. En el área de navegación de la izquierda, seleccione **Cuchos**.
2. Seleccione **Agregar**.
3. Seleccione el tipo de bloque.



Cuando agregue un bloque, seleccione el proveedor de segmento correcto y proporcione las credenciales correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como tipo y acepta credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los futuros backups de aplicaciones y restauraciones usando este bucket.

4. Introduzca un nombre de bloque existente y una descripción opcional.



El nombre y la descripción del bloque aparecen como una ubicación de backup que se puede elegir más adelante al crear un backup. El nombre también aparece durante la configuración de la política de protección.

5. Introduzca el nombre o la dirección IP del extremo de S3.
6. En **Seleccionar credenciales**, elija la ficha **Agregar** o **utilizar existente**.
 - Si ha elegido **Agregar**:
 - i. Introduzca un nombre para la credencial que la distingue de otras credenciales en Astra Control.
 - ii. Escriba el identificador de acceso y la clave secreta pegando el contenido del portapapeles.
 - Si ha elegido **utilizar existente**:
 - i. Seleccione las credenciales existentes que desea utilizar con el bloque.
7. Seleccione **Add**.



Cuando se agrega un bloque, Astra Control Marca un bloque con el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado. A medida que se añaden bloques, más adelante se puede decidir a. "[establecer otro bloque predeterminado](#)".

El futuro

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

- "[Gestione usuarios locales y roles](#)"
- "[Inicie la gestión de aplicaciones](#)"
- "[Proteja sus aplicaciones](#)"
- "[Gestionar notificaciones](#)"
- "[Conéctese a Cloud Insights](#)"

- "Agregue un certificado TLS personalizado"
- "Cambie la clase de almacenamiento predeterminada"

Obtenga más información

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

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 URL, en un explorador, introduzca el nombre de dominio completo (FQDN) que haya establecido en el campo `spec.astraAddress` del archivo `astra_control_Center.yaml` custom resource (CR) cuando instaló Astra Control Center. El mensaje de correo electrónico es el valor que se ha establecido en el campo `SPEC.Email` del `astra_control_Center.ylma` CR.

Licencia

Estoy usando una licencia de evaluación. ¿Cómo cambio a la licencia completa?

Puede cambiar fácilmente a una licencia completa si obtiene el archivo de licencia de NetApp (NLF) de NetApp.

- Pasos*
 1. En la navegación de la izquierda, seleccione **cuenta > Licencia**.
 2. En la descripción general de la licencia, a la derecha de la información de la licencia, seleccione el menú Opciones.
 3. Seleccione **Reemplazar**.
 4. Busque el archivo de licencia que ha descargado y seleccione **Agregar**.

Estoy usando una licencia de evaluación. ¿Puedo seguir gestionando aplicaciones?

Sí, puede probar la funcionalidad de administración de aplicaciones con una licencia de evaluación (incluida la licencia de evaluación integrada que se instala de forma predeterminada). No hay diferencia en las capacidades o características entre una licencia de evaluación y una licencia completa; la licencia de evaluación simplemente tiene una vida útil más corta. Consulte "[Licencia](#)" si quiere más información.

Registrar clústeres de Kubernetes

Necesito añadir nodos de 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.

- ¿NetApp Astra Trident se desinstala automáticamente de un clúster cuando lo desgestiono?*
- Cuando se desgestiona un clúster de Astra Control Center, Astra Trident no se desinstala automáticamente del clúster. Para desinstalar Astra Trident, debes hacerlo ["Siga estos pasos en la documentación de Astra 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.

Debería gestionar Astra Control en sí?

No, no deberías gestionar Astra Control en sí mismo porque es una «aplicación del sistema».

¿Las vainas poco saludables afectan a la gestión de la aplicación?

No, el estado de los pods no afecta a la gestión de la aplicación.

Operaciones de gestión de datos

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

Sí. Una operación de instantánea en una aplicación de Astra Control incluye una instantánea de todos los VP vinculados a las RVP de la aplicación.

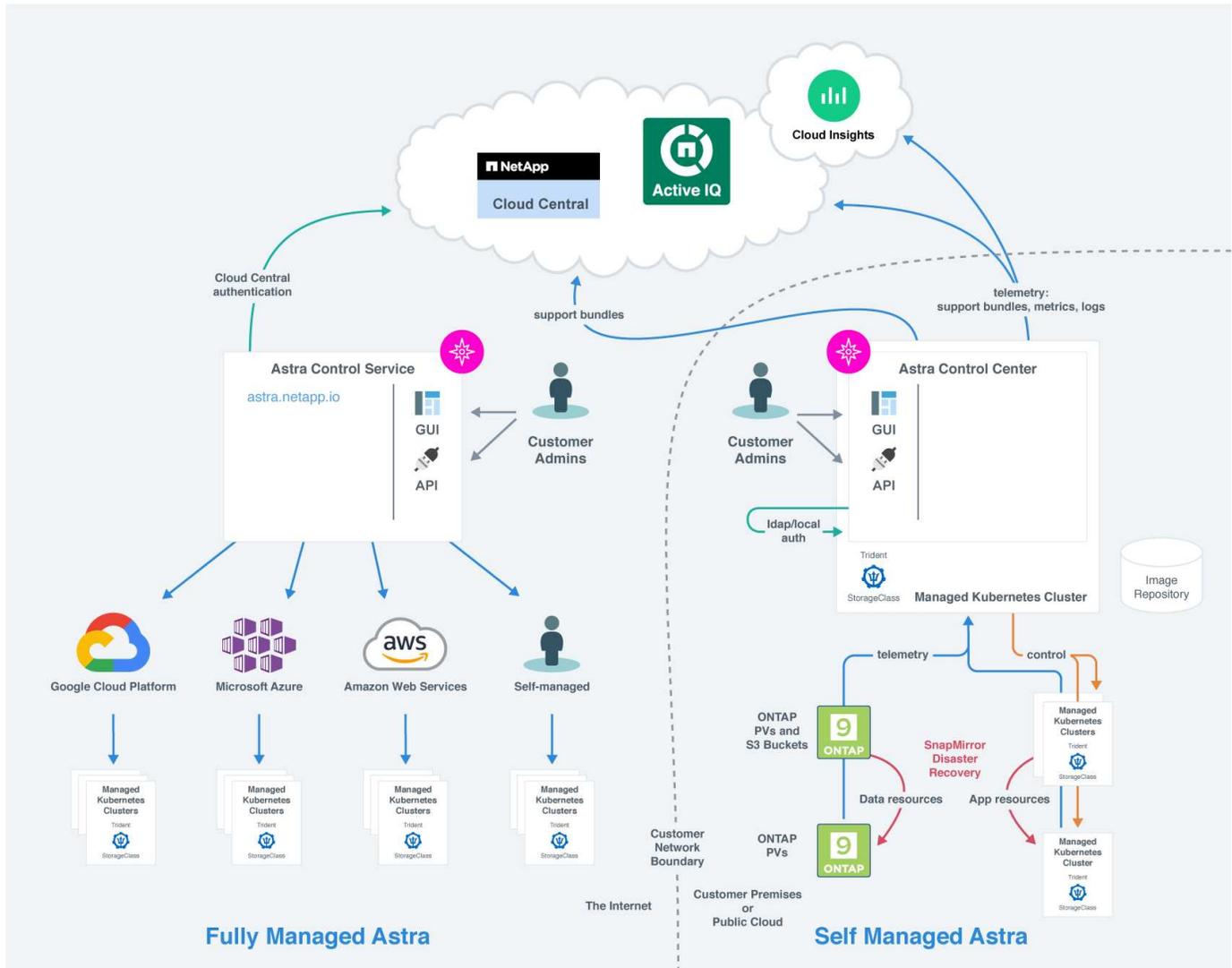
¿Puedo gestionar las instantáneas tomadas por Astra Control directamente a través de una interfaz o almacenamiento de objetos diferente?

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

Conceptos

Arquitectura y componentes

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



Componentes de Astra Control

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

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

Interfaces Astra Control

Puede completar tareas utilizando diferentes interfaces:

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

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

Si quiere más información

- ["Documentación de Astra Control Service"](#)
- ["Documentación de Astra Control Center"](#)
- ["Documentación de Astra Trident"](#)
- ["Utilice la API Astra Control"](#)
- ["Documentación de Cloud Insights"](#)
- ["Documentación de ONTAP"](#)

Protección de datos

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

Snapshot, backups y políticas de protección

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

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

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

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

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



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

Clones

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

La replicación en un clúster remoto

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

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

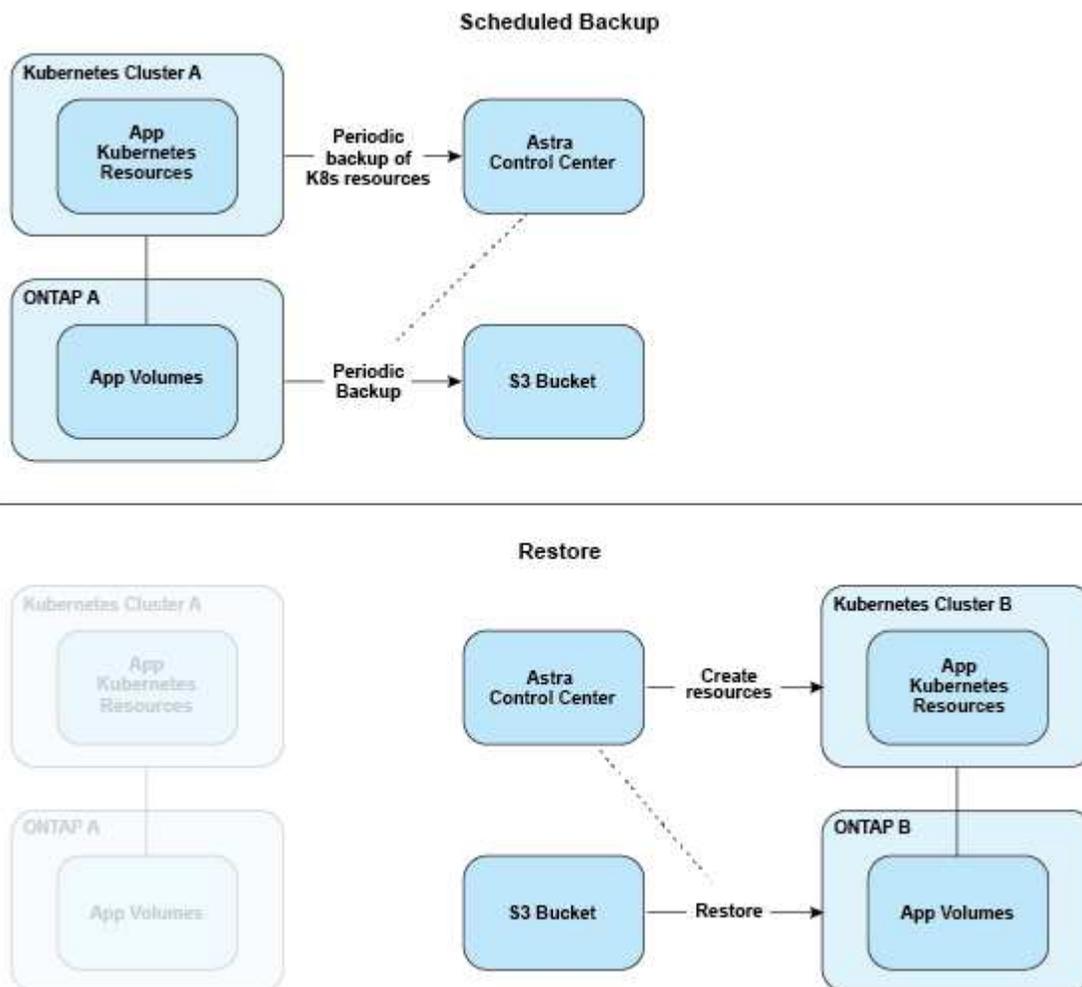
La replicación de aplicaciones es diferente de la copia de seguridad y la restauración de aplicaciones de las siguientes formas:

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

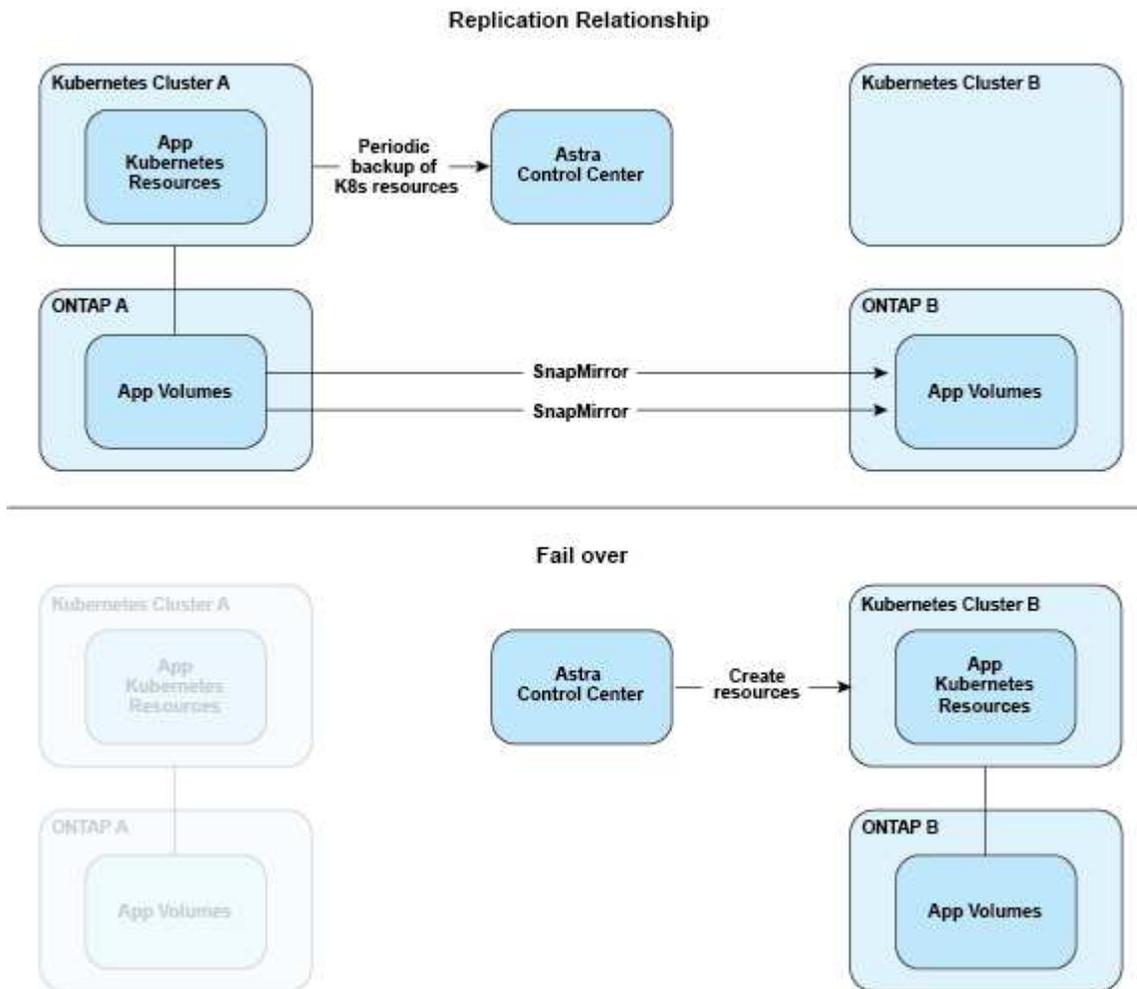
Para obtener más información sobre cómo replicar aplicaciones, consulte ["Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror"](#).

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

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



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



Backups, snapshots y clones con una licencia caducada

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

Licencia

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

Usted obtiene una licencia de una de las siguientes maneras:

- Si va a evaluar Astra Control Center y necesita términos de evaluación distintos a los incluidos en la licencia de evaluación integrada, póngase en contacto con NetApp para solicitar un archivo de licencia de evaluación diferente.

- ["Si ya ha adquirido Astra Control Center, genere su archivo de licencia de NetApp \(NLF\)"](#) Al iniciar sesión en el sitio de soporte de NetApp y navegar a sus licencias de software en el menú Sistemas.

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



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

Licencias de evaluación y licencias completas

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

Caducidad de la licencia

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

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

Cómo se calcula el consumo de licencias

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

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



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

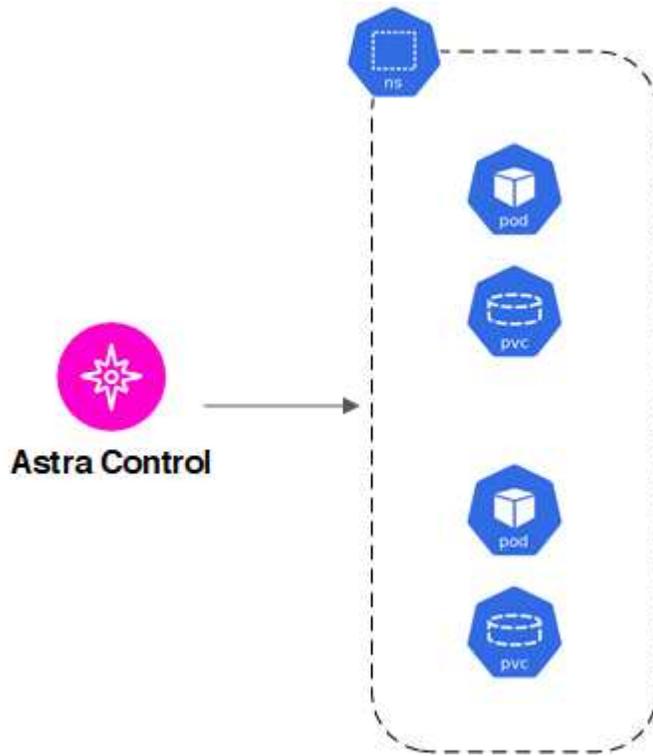
Obtenga más información

- ["Agregue una licencia cuando configure por primera vez Astra Control Center"](#)
- ["Actualizar una licencia existente"](#)

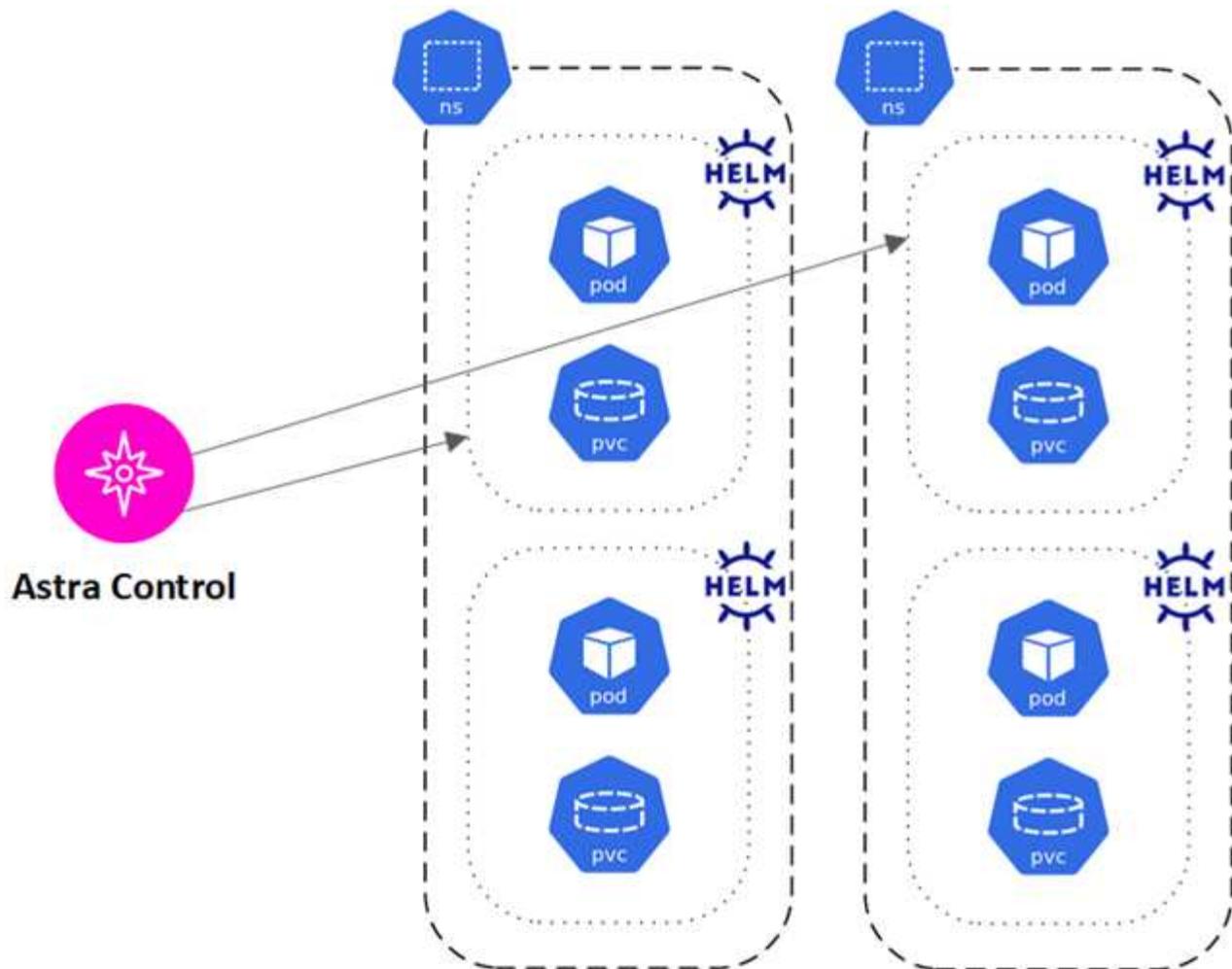
Gestión de aplicaciones

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

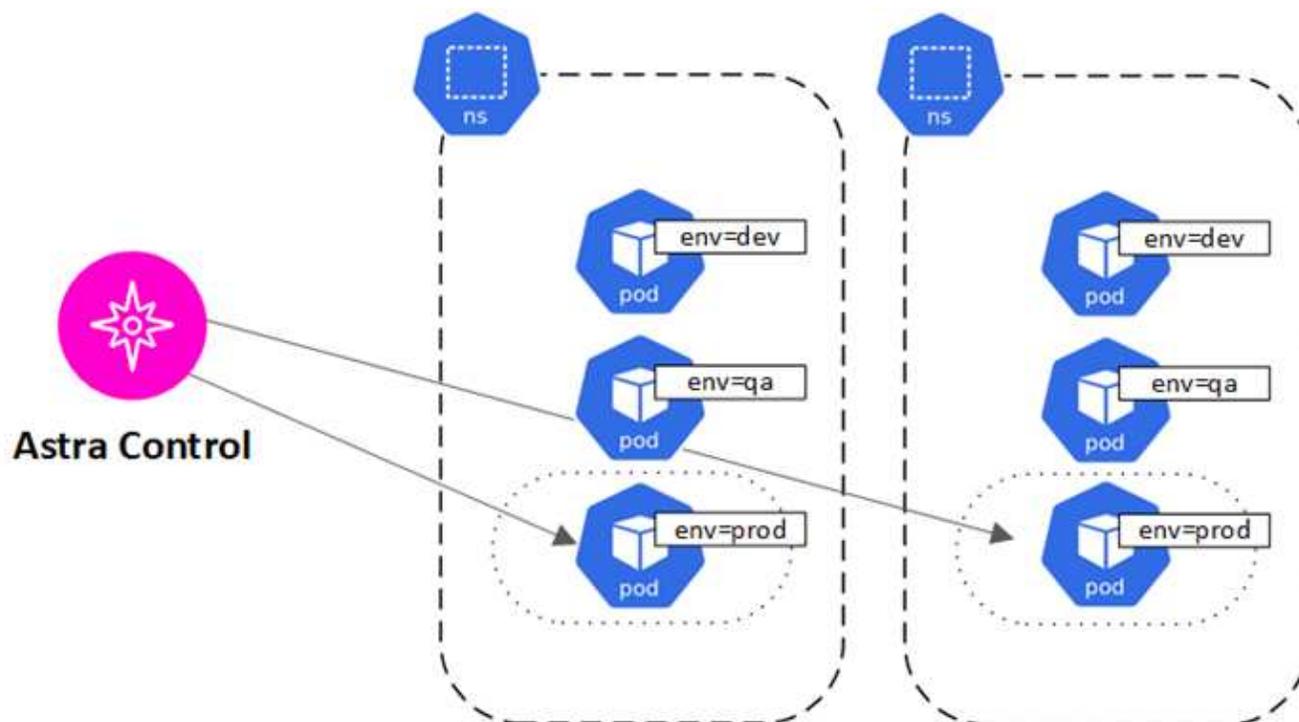
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



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



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



Clases de almacenamiento y tamaño de volumen persistente

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

Descripción general

Astra Control Center admite lo siguiente:

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



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

Clases de almacenamiento

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

Si quiere más información

- ["Documentación de Astra Trident"](#)

Roles de usuario y espacios de nombres

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

Roles de usuario

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

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

Puede agregar restricciones a un usuario Miembro o Visor para restringir el usuario a uno o más [Espacios de nombres](#).

Espacios de nombres

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

Obtenga más información

["Gestione usuarios locales y roles"](#)

Seguridad de POD

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

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

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

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

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

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

PSP instalado por Astra Control Center

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

Se crean PSP durante la instalación

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

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

Se crean PSP durante las operaciones de backup

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

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

Se crean PSP durante la gestión del clúster

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

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

Utilice Astra Control Center

Inicie la gestión de aplicaciones

Usted primero "[Añada un clúster a la gestión de Astra Control](#)", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para definir las aplicaciones y sus recursos.

Y gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencias:** Para administrar aplicaciones con Astra Control Center, necesitas la licencia de evaluación integrada de Astra Control Center o una licencia completa.
- **Namespaces:** Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.
- **Clase de almacenamiento:** Si instala una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Recursos de Kubernetes:** Las aplicaciones que usan recursos de Kubernetes no recopilados por Astra Control podrían no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

ClusterRole	ClusterRoleBinding	ConfigMap
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

Métodos de instalación de aplicaciones compatibles

Astra Control es compatible con los siguientes métodos de instalación de aplicaciones:

- **Fichero manifiesto:** Astra Control admite aplicaciones instaladas desde un archivo manifiesto mediante kubectl. Por ejemplo:

```
kubectl apply -f myapp.yaml
```

- **Helm 3:** Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. Es totalmente compatible con la gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3). No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador:** Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres que, en general, están diseñadas con una arquitectura "pass-by-value" en lugar de "pass-by-reference". Un operador y la aplicación que instala deben usar el mismo espacio de nombres; es posible que deba modificar el archivo YAML de implementación para que el operador se asegure de que este es el caso.

Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

- ["Apache K8ssandra"](#)



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

- ["Jenkins CI"](#)
- ["Clúster Percona XtraDB"](#)

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

Instale las aplicaciones en el clúster

La tienes ["ha agregado el clúster"](#) A Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Cualquier aplicación que se limita a uno o más espacios de nombres se puede gestionar.

Defina las aplicaciones

Una vez que Astra Control detecta espacios de nombres en sus clústeres, puede definir las aplicaciones que desea administrar. Puede elegir [administrar una aplicación que abarque uno o más espacios de nombres](#) o [gestione un espacio de nombres completo como una única aplicación](#). Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Aunque Astra Control le permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones en ese espacio de nombres o espacio de nombres expansivo), la práctica recomendada es elegir uno u otro. Las acciones que realice en Astra Control pueden fallar si las acciones se llevan a cabo al mismo tiempo tanto en el espacio de nombres como en el nivel de la aplicación.



A modo de ejemplo, puede que desee establecer una normativa de backup para «maria» con una cadencia semanal, pero es posible que deba realizar backups de «mariadb» (que se encuentra en el mismo espacio de nombres) con mayor frecuencia que esta. Según estas necesidades, debería gestionar las aplicaciones por separado, no como una aplicación de espacio de nombres único.

Antes de empezar

- Se añadió un clúster de Kubernetes a Astra Control.
- Una o más aplicaciones instaladas en el clúster. [Obtenga más información sobre los métodos de instalación de aplicaciones compatibles](#).
- Espacios de nombres existentes en el clúster Kubernetes que se añadió a Astra Control.
- (Opcional) una etiqueta de Kubernetes en cualquiera ["Recursos de Kubernetes compatibles"](#).



Una etiqueta es una pareja clave/valor que se puede asignar a objetos de Kubernetes para su identificación. Las etiquetas facilitan la ordenación, la organización y la búsqueda de los objetos de Kubernetes. Para obtener más información acerca de las etiquetas de Kubernetes, ["Consulte la documentación oficial de Kubernetes"](#).

Acerca de esta tarea

- Antes de empezar, también debe entender ["gestión de espacios de nombres estándar y del sistema"](#).
- Si planea utilizar varios espacios de nombres con sus aplicaciones en Astra Control, ["modificar los roles de usuario con restricciones de espacio de nombres"](#) Tras actualizar a una versión de Astra Control Center compatible con varios espacios de nombres.
- Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte ["Información sobre API y automatización de Astra"](#).

Opciones de gestión de aplicaciones

- [Defina los recursos que se van a administrar como una aplicación](#)
- [Defina un espacio de nombres para administrar como una aplicación](#)

Defina los recursos que se van a administrar como una aplicación

Puede especificar el ["Los recursos de Kubernetes forman una aplicación"](#) Que desea gestionar con Astra Control. Definir una aplicación le permite agrupar elementos de su clúster de Kubernetes en una única aplicación. Esta colección de recursos de Kubernetes está organizada por criterios de espacio de nombres y selector de etiquetas.

Definir una aplicación le proporciona un control más granular de lo que se debe incluir en una operación Astra Control, que incluye clonado, copias Snapshot y backups.



Al definir aplicaciones, asegúrese de no incluir un recurso de Kubernetes en varias aplicaciones con políticas de protección. La superposición de políticas de protección en recursos de Kubernetes puede provocar conflictos de datos. [Más información en un ejemplo](#).

Obtenga más información sobre la adición de recursos con ámbito de clúster a los espacios de nombres de la aplicación.

Puede importar recursos de clúster asociados a los recursos de espacio de nombres además de los que se incluyen automáticamente Astra Control. Puede agregar una regla que incluirá recursos de un grupo específico, tipo, versión y, opcionalmente, etiqueta. Es posible que desee hacer esto si hay recursos que Astra Control no incluye automáticamente.

No puede excluir ninguno de los recursos con ámbito de clúster que Astra Control incluya automáticamente.

Puede agregar lo siguiente `apiVersions` (Que son los grupos combinados con la versión API):

Tipo de recursos	ApiVersions (grupo + versión)
ClusterRole	rbac.authorization.k8s.io/v1
ClusterRoleBinding	rbac.authorization.k8s.io/v1
CustomResource	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
CustomResourceDefinition	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
MutatingWebhookConfiguration	admission registration.k8s.io/v1
ValidatingWebhookConfiguration	admission registration.k8s.io/v1

Pasos

1. En la página aplicaciones, seleccione **definir**.
2. En la ventana **definir aplicación**, introduzca el nombre de la aplicación.
3. Seleccione el clúster en el que se ejecuta la aplicación en la lista desplegable **Cluster**.
4. Elija un espacio de nombres para su aplicación en la lista desplegable **espacio de nombres**.



Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.

5. (Opcional) Introduzca una etiqueta para los recursos de Kubernetes en cada espacio de nombres. Puede especificar una sola etiqueta o un criterio de selector de etiquetas (consulta).



Para obtener más información acerca de las etiquetas de Kubernetes, "[Consulte la documentación oficial de Kubernetes](#)".

6. (Opcional) Añada espacios de nombres adicionales para la aplicación seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
7. (Opcional) Introduzca los criterios de etiqueta única o selector de etiquetas para los espacios de nombres adicionales que añada.
8. (Opcional) para incluir recursos de ámbito de clúster además de los que Astra Control incluye

automáticamente, marque **incluir recursos adicionales de ámbito de clúster** y complete lo siguiente:

- a. Seleccione **Agregar regla de inclusión**.
- b. **Grupo**: En la lista desplegable, seleccione el grupo API de recursos.
- c. **Kind**: En la lista desplegable, seleccione el nombre del esquema de objetos.
- d. **Versión**: Introduzca la versión API.
- e. **Selector de etiquetas**: Opcionalmente, incluya una etiqueta que se agregará a la regla. Esta etiqueta se utiliza para recuperar solo los recursos que coincidan con esta etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster.
- f. Revise la regla que se crea en función de las entradas.
- g. Seleccione **Agregar**.



Puede crear tantas reglas de recursos con ámbito de clúster como desee. Las reglas aparecen en definir resumen de la aplicación.

9. Seleccione **definir**.

10. Después de seleccionar **definir**, repita el proceso para otras aplicaciones, según sea necesario.

Cuando termine de definir una aplicación, la aplicación aparecerá en `Healthy` estado en la lista de aplicaciones de la página aplicaciones. Ahora puede clonarla y crear backups y copias Snapshot.



Es posible que la aplicación que acaba de agregar tenga un icono de advertencia en la columna protegido, lo que indica que no se ha realizado una copia de seguridad y que aún no está programada para las copias de seguridad.



Para ver los detalles de una aplicación en particular, seleccione el nombre de la aplicación.

Para ver los recursos agregados a esta aplicación, seleccione la ficha **Recursos**. Seleccione el número después del nombre del recurso en la columna Resource o introduzca el nombre del recurso en la búsqueda para ver los recursos adicionales con ámbito del clúster incluidos.

Defina un espacio de nombres para administrar como una aplicación

Puede añadir todos los recursos de Kubernetes en un espacio de nombres a la gestión de Astra Control al definir los recursos de ese espacio de nombres como una aplicación. Este método es preferible a definir las aplicaciones individualmente si piensa administrar y proteger todos los recursos de un espacio de nombres determinado de una manera similar y en intervalos comunes.

Pasos

1. En la página Clusters, seleccione un clúster.
2. Seleccione la ficha **Namespaces**.
3. Seleccione el menú acciones del espacio de nombres que contiene los recursos de aplicación que desea administrar y seleccione **definir como aplicación**.



Si desea definir varias aplicaciones, seleccione en la lista de espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **definir como aplicación**. Esto definirá varias aplicaciones individuales en sus espacios de nombres individuales. Para aplicaciones con varios espacios de nombres, consulte [Defina los recursos que se van a administrar como una aplicación](#).



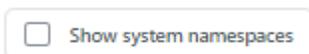
Active la casilla de verificación **Mostrar espacios de nombres del sistema** para mostrar los espacios de nombres del sistema que normalmente no se usan en la administración de aplicaciones de forma predeterminada. Show system namespaces ["Leer más"](#).

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

¿Qué ocurre con los espacios de nombres del sistema?

Astra Control también detecta espacios de nombres de sistemas en un clúster de Kubernetes. No le mostramos estos espacios de nombres del sistema de forma predeterminada porque es raro que necesite realizar backups de los recursos de la aplicación del sistema.

Puede visualizar los espacios de nombres del sistema desde la ficha espacios de nombres de un clúster seleccionado activando la casilla de verificación **Mostrar espacios de nombres del sistema**.



Astra Control 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"](#)
- ["Desgestionar una aplicación"](#)

Proteja sus aplicaciones

Información general sobre la protección

Puede crear backups, clones, snapshots y políticas de protección para sus aplicaciones con Astra Control Center. El backup de sus aplicaciones ayuda a que los servicios y los datos asociados estén disponibles lo más posible; durante un desastre, la restauración a partir de una copia de seguridad puede garantizar la recuperación completa de una aplicación y sus datos asociados con una interrupción mínima. Los backups, clones y copias Snapshot pueden ayudar a protegerse frente a amenazas comunes como el ransomware, la pérdida accidental de datos y los desastres medioambientales. ["Conozca los tipos disponibles de protección de datos en Astra Control Center y cuándo utilizarlas"](#).

Además, puede replicar aplicaciones en un clúster remoto como preparación para la recuperación ante desastres.

Flujo de trabajo de protección de aplicaciones

Puede utilizar el siguiente ejemplo de flujo de trabajo para empezar a proteger las aplicaciones.

[Uno] Proteja todas las aplicaciones

Para asegurarse de que sus aplicaciones están protegidas inmediatamente, [" Cree una copia de seguridad manual de todas las aplicaciones "](#).

[Dos] Configure una política de protección para cada aplicación

Para automatizar futuros backups y copias Snapshot, [" configure una política de protección para cada aplicación "](#). A modo de ejemplo, puede comenzar con backups semanales y snapshots diarias, con una retención de un mes para ambos. La automatización de backups y snapshots con una política de protección es muy recomendada con respecto a copias de Snapshot y backups manuales.

[Tres] Ajuste las políticas de protección

A medida que cambian las aplicaciones y sus patrones de uso, ajuste las políticas de protección según sea necesario para proporcionar la mejor protección.

[Cuatro] Replicar aplicaciones en un clúster remoto

[" Replicar aplicaciones "](#) A un clúster remoto mediante la tecnología SnapMirror de NetApp. Astra Control replica las instantáneas en un clúster remoto, lo que proporciona una función asíncrona y de recuperación ante desastres.

[Cinco] En caso de desastre, restaure sus aplicaciones con la última copia de seguridad o replicación en el sistema remoto

Si se produce la pérdida de datos, puede recuperarlo [" restaurar la copia de seguridad más reciente "](#) la primera para cada aplicación. Luego puede restaurar la snapshot más reciente (si está disponible). O bien, puede utilizar la replicación en un sistema remoto.

Proteja las aplicaciones con snapshots y backups

Proteger todas las aplicaciones mediante la toma de snapshots y backups a través de una política de protección automatizada o de manera ad hoc. Puede utilizar la interfaz de

usuario de Astra Control Center o ["La API de control Astra"](#) para proteger aplicaciones.

Acerca de esta tarea

- **Helm implementó aplicaciones:** Si utiliza Helm para implementar aplicaciones, Astra Control Center requiere Helm versión 3. Se admite por completo la gestión y clonación de las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Las aplicaciones implementadas con Helm 2 no son compatibles.
- **(sólo clústeres de OpenShift) Agregar directivas:** Cuando se crea un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

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.

Si necesita que backups o snapshots se ejecuten con más frecuencia de una vez por hora, puede hacerlo ["Utilice la API REST de Astra Control para crear copias Snapshot y copias de seguridad"](#).



Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.



Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, las políticas de protección no se pueden utilizar. Migra a un tipo de almacenamiento compatible con Astra Control si quieres programar backups y copias Snapshot.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.

2. Seleccione **Protección de datos**.
3. Seleccione **Configurar política de protección**.
4. Defina una programación de protección eligiendo la cantidad de snapshots y backups que se mantendrán por hora, día, semana y mes.

Puede definir las programaciones por hora, por día, por semana y por mes de forma simultánea. Una programación no se activa hasta que se establece un nivel de retención.

Al establecer un nivel de retención para backups, puede elegir el bloque en el que desea almacenar los backups.

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

The screenshot shows the 'Configure protection policy' interface with the following details:

- PROTECTION SCHEDULE:** Four options are shown:
 - Hourly:** Every hour on the 0th minute, keep the last 4 snapshots.
 - Daily:** Daily at 02:00 (UTC), keep the last 15 snapshots.
 - Weekly:** Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots.
 - Monthly:** Every 1st of the month at 02:00 (UTC), keep the last 12 backups.
- Selection:** Radio buttons for Hourly, Daily, Weekly (selected), and Monthly.
- Configuration:**
 - Select Weekday(s) (optional): Monday X
 - Time (UTC) (optional): 02:00
 - Snapshots to keep: 26
 - Backups to keep: 0
- BACKUP DESTINATION:** A dropdown menu for Bucket, currently showing 'ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10' with a 'Default' tag.
- OVERVIEW:** A sidebar on the right with the title 'OVERVIEW' and sub-section 'Schedule and retention'. It contains instructions on how to define a policy and a link to 'Protection policies'.
- Buttons:** 'Cancel' and 'Review →' buttons at the bottom.

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

Resultado

Astra Control implementa la política de protección de datos mediante la creación y retención de copias Snapshot y copias de seguridad con la política de programación y retención que haya definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.



Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, no se pueden crear instantáneas. Utilice una clase de almacenamiento alternativa para las instantáneas.

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **Snapshot**.
3. Personalice el nombre de la instantánea y, a continuación, seleccione **Siguiente**.
4. Revise el resumen de la instantánea y seleccione **Snapshot**.

Resultado

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

Cree un backup

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.



Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, asegúrese de que ha definido un `backendType` parámetro en la "[Objeto de almacenamiento de Kubernetes](#)" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección. Copias de seguridad para aplicaciones respaldadas por el `ontap-nas-economy` son disruptivos y la aplicación no estará disponible hasta que se complete la operación de backup.

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. Seleccione un bucket de destino para el backup en la lista de bloques de almacenamiento.
6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control crea una copia de seguridad de la aplicación.



Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.



Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de [Cancelar backups](#). Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice las instrucciones de [Eliminar backups](#).



Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

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 es posible eliminar una copia de Snapshot que se está replicando actualmente.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione **Protección de datos**.
3. En el menú Opciones de la columna **acciones** de la instantánea deseada, seleccione **Eliminar instantánea**.
4. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete snapshot**.

Resultado

Astra Control elimina la instantánea.

Cancelar backups

Es posible cancelar una copia de seguridad que esté en curso.



Para cancelar una copia de seguridad, la copia de seguridad debe estar en **Running** estado. No puede cancelar una copia de seguridad que esté en **Pending** estado.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.

3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** para la copia de seguridad deseada, seleccione **Cancelar**.
5. Escriba la palabra "cancelar" para confirmar la operación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

Eliminar backups

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



Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de [Cancelar backups](#). Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice estas instrucciones.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** de la copia de seguridad deseada, seleccione **Eliminar copia de seguridad**.
5. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete backup**.

Resultado

Astra Control elimina la copia de seguridad.

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.



Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Acerca de esta tarea

- **Proteja sus aplicaciones primero:** Se recomienda encarecidamente que tome una instantánea o una copia de seguridad de su aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup en el caso de que la restauración no se realice correctamente.
- **Comprobar volúmenes de destino:** Si restaura a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de restauración si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o `ontap-san`, hará que falle la operación de restauración. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la ["Kubernetes"](#) documentación.

- **Planificar necesidades de espacio:** Cuando se realiza una restauración in situ de una aplicación que utiliza almacenamiento ONTAP de NetApp, el espacio utilizado por la aplicación restaurada puede duplicarse. Después de realizar una restauración sin movimiento, elimine las instantáneas no deseadas de la aplicación restaurada para liberar espacio de almacenamiento.
- **(sólo clústeres de OpenShift) Agregar directivas:** Cuando se crea un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- *** Aplicaciones implementadas de Helm*:** Las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. Las aplicaciones implementadas con Helm 2 no son compatibles.



La ejecución de una operación de restauración sin movimiento en una aplicación que comparte recursos con otra aplicación puede tener resultados no intencionados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones. Para obtener más información, consulte [este ejemplo](#).

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.
3. Elija el tipo de restauración:
 - **Restaurar en espacios de nombres originales:** Utilice este procedimiento para restaurar la aplicación en su sitio al cluster original.



Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy driver`, debe restaurar la aplicación utilizando las clases de almacenamiento originales. No puede especificar una clase de almacenamiento diferente si va a restaurar la aplicación en el mismo espacio de nombres.

- i. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación en el lugar, lo que revierte la aplicación a una versión anterior de sí misma.
- ii. Seleccione **Siguiente**.



Si se restaura en un espacio de nombres que se eliminó previamente, se crea un espacio de nombres nuevo con el mismo nombre como parte del proceso de restauración. Cualquier usuario que tenga derechos para administrar aplicaciones en el espacio de nombres previamente eliminado debe restaurar manualmente los derechos en el espacio de nombres recién creado.

- **Restaurar en nuevos espacios de nombres:** Utilice este procedimiento para restaurar la aplicación en otro clúster o con diferentes espacios de nombres desde el origen.



Puede utilizar este procedimiento para cualquiera de los dos a una clase de almacenamiento respaldada por `ontap-nas`. En el mismo clúster **O** copie la aplicación en otro clúster con una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador.

- i. Especifique el nombre de la aplicación restaurada.
- ii. Elija el clúster de destino de la aplicación que desea restaurar.
- iii. Introduzca un espacio de nombres de destino para cada espacio de nombres de origen asociado a la aplicación.



Astra Control crea nuevos espacios de nombres de destino como parte de esta opción de restauración. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

- iv. Seleccione **Siguiente**.
- v. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación.
- vi. Seleccione **Siguiente**.
- vii. Elija una de las siguientes opciones:
 - **Restaurar usando clases de almacenamiento originales:** La aplicación utiliza la clase de almacenamiento asociada originalmente a menos que no exista en el clúster de destino. En este caso, se utilizará la clase de almacenamiento predeterminada para el clúster.
 - **Restaurar usando una clase de almacenamiento diferente:** Seleccione una clase de almacenamiento que exista en el clúster de destino. Todos los volúmenes de aplicaciones, independientemente de sus tipos de almacenamiento asociados originalmente, se migrarán a esta clase de almacenamiento diferente como parte de la restauración.

viii. Seleccione **Siguiente**.

4. Elija cualquier recurso para filtrar:

- **Restaurar todos los recursos:** Restaurar todos los recursos asociados con la aplicación original.
- **Filtrar recursos:** Especificar reglas para restaurar un subconjunto de los recursos originales de la aplicación:
 - i. Seleccione incluir o excluir recursos de la aplicación restaurada.
 - ii. Seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión** y configure la regla para filtrar los recursos correctos durante la restauración de la aplicación. Puede editar una regla o eliminarla y volver a crear una regla hasta que la configuración sea correcta.



Para obtener más información sobre la configuración de reglas de inclusión y exclusión, consulte [Filtre recursos durante una restauración de aplicación](#).

5. Seleccione **Siguiente**.

6. Revise los detalles sobre la acción de restauración cuidadosamente, escriba “restaurar” (si se le solicita) y seleccione **Restaurar**.

Resultado

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



Después de una operación de protección de datos (clonado, backup o restauración) y un posterior tamaño de volumen persistente, se produce un retraso de hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario web. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.



Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de 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.

Filtre recursos durante una restauración de aplicación

Puede agregar una regla de filtro a un "restaurar" operación que especificará los recursos de aplicación existentes que se incluirán o excluirán de la aplicación restaurada. Puede incluir o excluir recursos basados en un espacio de nombres, etiqueta o GVK (GroupVersionKind) especificado.

Lea más sobre Incluir y excluir escenarios

- **Selecciona una regla de inclusión con espacios de nombres originales (restauración in situ):** Los recursos de aplicación existentes que definas en la regla se eliminarán y reemplazarán por aquellos de la instantánea o copia de seguridad seleccionada que estés utilizando para la restauración. Cualquier recurso que no especifique en la regla Incluir permanecerá sin cambios.
- **Selecciona una regla de inclusión con nuevos espacios de nombres:** Usa la regla para seleccionar los recursos específicos que deseas en la aplicación restaurada. Los recursos que no especifique en la regla Incluir no se incluirán en la aplicación restaurada.
- **Selecciona una regla de exclusión con espacios de nombres originales (restauración in situ):** Los recursos que especifiques para ser excluidos no se restaurarán y permanecerán sin cambios. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup. Todos los datos de los volúmenes persistentes se eliminarán y volverán a crear si el StatefulSet correspondiente forma parte de los recursos filtrados.
- **Selecciona una regla de exclusión con nuevos espacios de nombres:** Usa la regla para seleccionar los recursos específicos que deseas eliminar de la aplicación restaurada. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup.

Las reglas son tipos de inclusión o exclusión. Las reglas que combinan la inclusión y exclusión de recursos no están disponibles.

Pasos

1. Una vez que haya elegido filtrar recursos y seleccionado una opción Incluir o Excluir en el asistente Restaurar aplicación, seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión**.



No puede excluir ningún recurso en el ámbito del clúster que Astra Control incluya automáticamente.

2. Configure la regla de filtro:



Debe especificar al menos un espacio de nombres, una etiqueta o un GVK. Asegúrese de que los recursos que retenga después de aplicar las reglas de filtro sean suficientes para mantener la aplicación restaurada en buen estado.

- a. Seleccione un espacio de nombres específico para la regla. Si no hace una selección, se usarán todos los espacios de nombres en el filtro.



Si la aplicación contenía originalmente varios espacios de nombres y la restauraba en nuevos espacios de nombres, todos los espacios de nombres se crearán incluso si no contienen recursos.

- b. (Opcional) Introduzca un nombre de recurso.
- c. (Opcional) **Selector de etiquetas:** Incluye a. "[selector de etiquetas](#)" para agregar a la regla. El selector de etiquetas se utiliza para filtrar sólo los recursos que coincidan con la etiqueta seleccionada.
- d. (Opcional) Seleccione **Usar GVK (GroupVersionKind) configurado para filtrar recursos** para opciones de filtrado adicionales.



Si utiliza un filtro GVK, debe especificar Versión y Tipo.

- i. (Opcional) **Grupo:** En la lista desplegable, seleccione el grupo API de Kubernetes.
- ii. **Kind:** En la lista desplegable, seleccione el esquema de objeto para el tipo de recurso de Kubernetes a utilizar en el filtro.
- iii. **Versión:** Seleccione la versión de la API de Kubernetes.

3. Revise la regla que se crea en función de las entradas.

4. Seleccione **Agregar**.



Puede crear tantas reglas de inclusión y exclusión de recursos como desee. Las reglas aparecen en el resumen de la aplicación de restauración antes de iniciar la operación.

Migre del almacenamiento económico de `ontap-nas` al almacenamiento `ontap-nas`

Puedes utilizar un Astra Control "[restauración de aplicaciones](#)" o "[clon de aplicación](#)" operación para migrar volúmenes de aplicaciones desde un tipo de almacenamiento respaldado por `ontap-nas-economy`, que permite opciones limitadas de protección de aplicaciones, a una clase de almacenamiento respaldada por `ontap-nas` Con toda su gama de opciones de protección Astra Control. La operación de clonado o restauración migra los volúmenes basados en `qtree` que usan una `ontap-nas-economy` back-end a volúmenes estándar respaldados por `ontap-nas`. Volúmenes, independientemente de si lo sean `ontap-nas-economy` con un respaldo exclusivo o mixto, se migrará a la clase de almacenamiento de destino. Una vez finalizada la migración, las opciones de protección dejan de limitarse.

Complicaciones de restauración in situ para una aplicación que comparte recursos con otra aplicación

Puede realizar una operación de restauración in situ en una aplicación que comparta recursos con otra aplicación y produzca resultados no deseados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones.

A continuación se muestra un ejemplo que crea una situación no deseable cuando se usa la replicación

SnapMirror de NetApp para una restauración:

1. Defina la aplicación `app1` uso del espacio de nombres `ns1`.
2. Puede configurar una relación de replicación para `app1`.
3. Defina la aplicación `app2` (en el mismo clúster) mediante los espacios de nombres `ns1` y `ns2`.
4. Puede configurar una relación de replicación para `app2`.
5. La replicación se invierte para `app2`. Esto provoca la `app1` en el clúster de origen que se va a desactivar.

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.

Si quiere ver una comparación entre backups/restauraciones y replicación, consulte ["Conceptos de protección de datos"](#).

Puede replicar aplicaciones en diferentes situaciones, como las siguientes situaciones de solo en las instalaciones, de cloud híbrido y multicloud:

- 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, Z se pueden replicar del centro de datos 2 al centro de datos 1.

Con Astra Control, puede realizar las siguientes tareas relacionadas con la replicación de aplicaciones:

- [Configurar una relación de replicación](#)
- [Ponga una aplicación replicada en línea en el clúster de destino \(conmutación por error\)](#)
- [Se ha producido un error al sincronizar una replicación](#)
- [Replicación de aplicaciones inversa](#)
- [Conmutación tras error de las aplicaciones al clúster de origen original](#)
- [Eliminar una relación de replicación de aplicaciones](#)

Requisitos previos de replicación

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

- **ONTAP clusters:**
 - **Trident:** Astra Trident versión 22,07 o posterior debe existir en los clústeres de Kubernetes de origen y destino que utilizan ONTAP como backend.
 - **Licencias:** Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte ["Información general sobre las licencias de SnapMirror en ONTAP"](#) si quiere más información.
- **Emparejamiento:**
 - **Cluster y SVM:** Los clústeres de ONTAP y la SVM host deben estar emparejados. Consulte ["Información general sobre relaciones entre iguales de clústeres y SVM"](#) si quiere más información.
 - **Trident y SVM:** La SVM remota emparejada debe estar disponible para Astra Trident en el clúster de destino.
- **Astra Control Center:**



["Pon en marcha Astra Control Center"](#) en un tercer dominio de fallo o centro secundario para proporcionar una recuperación ante desastres sin problemas.

- **Clusters administrados:** Los siguientes clusters deben ser agregados y administrados por Astra Control, idealmente en diferentes dominios o sitios de falla:
 - Clúster de Kubernetes de origen
 - Clúster de Kubernetes de destino
 - Clústeres de ONTAP asociados
- **Cuentas de usuario:** Cuando añades un backend de almacenamiento de ONTAP al Centro de control de Astra, aplica las credenciales de usuario con el rol "admin". Este rol tiene métodos de acceso `http` y `ontapi`. Se habilitó en los clústeres de origen y destino de ONTAP. Consulte ["Gestionar cuentas de usuario en la documentación de ONTAP"](#) si quiere más información.
- **Configuración de Astra Trident / ONTAP:** Astra Control Center requiere que configure al menos una clase de almacenamiento que admita la replicación tanto para los clústeres de origen como de destino.



La replicación de Astra Control admite aplicaciones que utilicen una única clase de almacenamiento. Al agregar una aplicación a un espacio de nombres, asegúrese de que la aplicación tenga la misma clase de almacenamiento que otras aplicaciones del espacio de nombres. Cuando agregue una RVP a una aplicación replicada, asegúrese de que la nueva RVP tenga la misma clase de almacenamiento que otras RVP del espacio de nombres.

Configurar una relación de replicación

La configuración de una relación de replicación implica lo siguiente:

- 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**: Introduzca un clúster de destino que sea diferente del origen.
 - **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 espacios de nombres de destino nuevos o existentes para el clúster de destino.
 - (Opcional) Añada espacios de nombres adicionales seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
 - **Frecuencia de replicación**: 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.



Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

5. Seleccione **Siguiente**, revise el resumen y seleccione **Guardar**.



Al principio, el estado muestra "app-mirror" antes de que se produzca la primera programación.

Astra Control crea una 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 Snapshot utiliza el formato de `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.

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

Por ejemplo:
Normal | Establecido

Obtenga más información acerca de los estados y el estado de replicación al final de este tema.

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

Mediante Astra Control, puede conmutar al respaldo las aplicaciones replicadas en un clúster de destino. Este procedimiento detiene la relación de replicación y conecta la aplicación en el clúster de destino. Este procedimiento no detiene la aplicación en el clúster de origen si estaba operativa.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. 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 se producen como resultado del procedimiento de failover:

- En el clúster de destino, la aplicación se inicia según la última instantánea replicada.
- El clúster de origen y la aplicación (si están operativas) no se han detenido y se seguirá ejecutando.
- El estado de replicación cambia a "recuperación tras fallos" y luego a "recuperación tras fallos" cuando ha finalizado.
- La política de protección de la aplicación de origen se copia en la aplicación de destino según los horarios presentes en la aplicación de origen en el momento de la conmutación por error.
- Si la aplicación de origen tiene uno o más ganchos de ejecución posteriores a la restauración habilitados, esos ganchos de ejecución se ejecutan para la aplicación de destino.
- Astra Control muestra la aplicación tanto en los clústeres de origen como de destino y su estado respectivo.

Se ha producido un error al sincronizar una replicación

La operación de resincronización vuelve a establecer la relación de replicación. Puede elegir el origen de la relación para conservar los datos en el clúster de origen o de destino. Esta operación vuelve a establecer las relaciones de SnapMirror para iniciar la replicación de volúmenes en la dirección que se desee.

El proceso detiene la aplicación en el nuevo clúster de destino antes de volver a establecer la replicación.



Durante el proceso de resincronización, el estado del ciclo de vida muestra como "establecer".

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. 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 conseguir un «retorno tras la recuperación» después de una operación de conmutación por error utilizando la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Astra Control replica (resyncs) cualquier aplicación vuelve a cambiar al clúster de origen original antes de revertir la dirección de replicación.

Este proceso se inicia desde una relación que ha completado una conmutación al nodo de respaldo a un destino e implica los siguientes pasos:

- Comience con un estado de conmutación al respaldo.
- Volver a sincronizar la relación.
- Invierta la replicación.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. 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 una operación de conmutación por error, seleccione la aplicación con error como origen de la operación de resincronización (conservando los datos escritos después de la conmutación por error).
5. Escriba "Resync" para confirmar.
6. Seleccione **Sí, resincronización** para finalizar.
7. Una vez finalizada la resincronización, en la ficha Protección de datos > replicación, en el menú acciones, seleccione **replicación inversa**.
8. En la página replicación inversa, revise la información y seleccione **replicación inversa**.

Resultado

Esto combina los resultados de las operaciones de "resincronización" y "relación inversa" para conectar la aplicación en el clúster de origen original con la reanudación de la replicación al clúster de destino original.

Eliminar una relación de replicación de aplicaciones

La eliminación de la relación da como resultado dos aplicaciones independientes sin relación entre ellas.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. 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

Puede clonar una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control clona una aplicación, crea un clon de la configuración de la aplicación y del almacenamiento persistente.

El clonado puede ayudarle si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro. Por ejemplo, es posible que desee mover cargas de trabajo mediante una canalización de CI/CD y entre espacios de nombres Kubernetes. Puede utilizar la interfaz de usuario de Astra Control Center o "[La API de control Astra](#)" para clonar y migrar aplicaciones.



Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Antes de empezar

- **Comprobar volúmenes de destino:** Si clona a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de clonado si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que se produzca un error en la operación de clonado. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "[Kubernetes](#)" documentación.
- Para clonar aplicaciones en un clúster diferente, debe asegurarse de que las instancias de cloud que contienen los clústeres de origen y destino (si no son iguales) tienen un bloque predeterminado. Deberá asignar un bloque predeterminado para cada instancia de cloud.
- Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.



Durante la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Por este motivo, es necesario configurar una política de exportación de volúmenes ONTAP para permitir estas operaciones. Puede hacerlo con los siguientes comandos:

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

Limitaciones de clones

- **Clases de almacenamiento explícitas:** Si implementa una aplicación con una clase de almacenamiento

definida explícitamente y necesita clonar la aplicación, el clúster de destino debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.

- **Clase de almacenamiento respaldada por la economía de ontap-nas:** Si su aplicación utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, la parte de backup de una operación de clonado causa interrupciones. La aplicación de origen no está disponible hasta que se complete el backup. La porción de restauración de la operación de clonado no es disruptiva.
- **Clones y restricciones de usuario:** Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación a un nuevo espacio de nombres en el mismo clúster o a cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de 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.
- **Los clones utilizan cubos predeterminados:** Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar opcionalmente un ID de bloque. Sin embargo, en una operación de clonado de aplicaciones, siempre se utiliza el bloque predeterminado que se ha definido. No existe ninguna opción para cambiar bloques para un clon. Si desea controlar qué segmento se utiliza, puede hacer lo mismo "[cambiar el valor predeterminado del segmento](#)" o haga un "[Backup](#)" seguido de un "[restaurar](#)" por separado.
- **Con Jenkins CI:** Si clona una instancia de Jenkins CI desplegada por el operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.
- **Con bloques S3:** Los bloques S3 de Astra Control Center no informan de la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Consideraciones sobre OpenShift

- **Clusters y OpenShift versiones:** Si clona una aplicación entre clústeres, los clústeres de origen y destino deben ser la misma distribución de OpenShift. Por ejemplo, si clona una aplicación de un clúster de OpenShift 4.7, utilice un clúster de destino que también sea OpenShift 4.7.
- **Proyectos y UID:** Cuando se crea un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Pasos

1. Seleccione **aplicaciones**.
2. Debe realizar una de las siguientes acciones:
 - Seleccione el menú Opciones de la columna **acciones** de la aplicación deseada.
 - Seleccione el nombre de la aplicación deseada y seleccione la lista desplegable de estado en la parte superior derecha de la página.

3. Seleccione **Clonar**.

4. Especifique los detalles del clon:

- Introduzca un nombre.
- Elija un clúster de destino para el clon.
- Introduzca los espacios de nombres de destino para el clon. Cada espacio de nombres de origen asociado a la aplicación se asigna al espacio de nombres de destino que defina.



Astra Control crea nuevos espacios de nombres de destino como parte de la operación de clonación. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

- Seleccione **Siguiente**.
- Elija 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.
 - Si decide clonar desde una snapshot o un backup existente, elija la snapshot o el backup que desee utilizar.
- Seleccione **Siguiente**.
- Elija mantener la clase de almacenamiento original asociada a la aplicación o seleccionar una clase de almacenamiento diferente.



Puede migrar una clase de almacenamiento de una aplicación a un tipo de almacenamiento de proveedor de nube nativo u otra clase de almacenamiento compatible, a una clase de almacenamiento respaldada por `ontap-nas` en el mismo clúster o copie la aplicación en otro clúster con una clase de almacenamiento respaldada por `ontap-nas-economy` controlador.



Si selecciona otra clase de almacenamiento y esta clase de almacenamiento no existe en el momento de la restauración, se devolverá un error.

5. Seleccione **Siguiente**.

6. Revise la información sobre el clon y seleccione **Clonar**.

Resultado

Astra Control clona la aplicación en función de la información proporcionada. La operación de clonado se realiza correctamente cuando se encuentra el nuevo clon de la aplicación `Healthy` en la página **aplicaciones**.

Después de 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.



Después de una operación de protección de datos (clonado, backup o restauración) y un posterior cambio de tamaño de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Gestione los enlaces de ejecución de aplicaciones

Un enlace de ejecución es una acción personalizada que puede configurar para que se ejecute junto con una operación de protección de datos de una aplicación gestionada. Por ejemplo, si dispone de una aplicación de base de datos, puede utilizar un enlace de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez completada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Tipos de enlaces de ejecución

Astra Control 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

Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución a una aplicación, puede agregar filtros a un enlace de ejecución para gestionar qué contenedores coincidirán el gancho. Los filtros son útiles para aplicaciones que usan la misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito diferente (como Elasticsearch). Los filtros permiten crear escenarios en los que los enlaces de ejecución se ejecutarán en algunos de esos contenedores idénticos, pero no necesariamente en todos ellos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agregue a un enlace de ejecución utiliza una expresión regular para hacer coincidir los contenedores del clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor.



Las expresiones regulares para los filtros utilizan la sintaxis expresión regular 2 (RE2), que no admite la creación de un filtro que excluye contenedores de la lista de coincidencias.

Para obtener información sobre la sintaxis que admite Astra Control para las expresiones regulares en los filtros de enlace de ejecución, consulte ["Soporte de sintaxis de expresión regular 2 \(RE2\)"](#).

Notas importantes sobre los enlaces de ejecución personalizados

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



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 la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

- 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).
- Si Astra Control Center conmuta por error una aplicación de origen replicada a la aplicación de destino, todos los ganchos de ejecución posteriores a la restauración que estén habilitados para la aplicación de origen se ejecutan para la aplicación de destino una vez completada la conmutación por error.
- Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

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	Funcionamiento en los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos
1	Clonar	N	N	Nuevo	Igual	Y	N	Y
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	N	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	N	N.A.

Ejemplos de gancho de ejecución

Visite la "[Proyecto Verda GitHub de NetApp](#)" Para descargar enlaces de ejecución real para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios enlaces de ejecución personalizados.

Ver los enlaces de ejecución existentes

Puede ver los enlaces de ejecución personalizados existentes para una aplicación.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.

Puede ver todos los enlaces de ejecución habilitados o desactivados en la lista resultante. Puede ver el estado de un gancho, cuántos contenedores coinciden, la hora de creación y cuándo se ejecuta (antes o después de la operación). Puede seleccionar la + icono junto al nombre del gancho para expandir la lista de contenedores en los que se ejecutará. Para ver los registros de eventos que rodean los enlaces de ejecución de esta aplicación, vaya a la ficha **actividad**.

Ver los scripts existentes

Puede ver los scripts cargados existentes. También puede ver qué scripts están en uso, y qué enlaces los están utilizando, en esta página.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.

En esta página puede ver una lista de los scripts cargados existentes. La columna **Used by** muestra los enlaces de ejecución que utilizan cada script.

Agregar un script

Cada enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos 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 asíelos 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**:
 - a. Determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.
 - b. Introduzca un nombre único para el gancho.
 - c. (Opcional) Introduzca cualquier argumento para pasar al gancho durante la ejecución, pulsando la tecla Intro después de cada argumento que introduzca para grabar cada uno.
5. (Opcional) en el área **Detalles de filtro de gancho**, puede añadir filtros para controlar en qué contenedores se ejecuta el gancho de ejecución:
 - a. Seleccione **Agregar filtro**.
 - b. En la columna **Tipo de filtro Hook**, elija un atributo en el que filtrar en el menú desplegable.
 - c. En la columna **Regex**, introduzca una expresión regular que se utilizará como filtro. Astra Control utiliza "[Sintaxis de regex de expresión regular 2 \(RE2\)](#)".



Si filtra el nombre exacto de un atributo (como un nombre de pod) sin ningún otro texto en el campo de expresión regular, se realiza una coincidencia de subcadena. Para que coincida con un nombre exacto y sólo con ese nombre, utilice la sintaxis de coincidencia de cadena exacta (por ejemplo, `^exact_podname$`).

- d. Para añadir más filtros, seleccione **Agregar filtro**.



Se combinan varios filtros para un enlace de ejecución con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

6. Cuando termine, seleccione **Siguiente**.
7. 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.

8. Seleccione **Siguiente**.
9. Revise la configuración del gancho de ejecución.
10. Seleccione **Agregar**.

Compruebe el estado de un enlace de ejecución

Después de que una operación de instantánea, backup o restauración finalice la ejecución, puede comprobar el estado de los enlaces de ejecución que se ejecutan como parte de la operación. Puede utilizar esta información de estado para determinar si desea mantener el enlace de ejecución, modificarlo o eliminarlo.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **Protección de datos**.
3. Seleccione **instantáneas** para ver las instantáneas en ejecución, o **copias de seguridad** para ver las copias de seguridad en ejecución.

El estado * gancho* muestra el estado de la ejecución del gancho de ejecución una vez completada la operación. Puede pasar el ratón sobre el estado para obtener más detalles. Por ejemplo, si hay fallos de enlace de ejecución durante una instantánea, pasar el ratón sobre el estado de enlace de esa instantánea proporciona una lista de los enlaces de ejecución fallidos. Para ver las razones de cada fallo, puede consultar la página **actividad** en el área de navegación del lado izquierdo.

Ver el uso de las secuencias de comandos

Puede ver qué enlaces de ejecución utilizan una secuencia de comandos determinada en la interfaz de usuario web de Astra Control.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **Scripts**.

La columna **usado por** de la lista de scripts contiene detalles sobre qué ganchos están utilizando cada script de la lista.

3. Seleccione la información de la columna **utilizado por** para un script que le interese.

Aparece una lista más detallada, con los nombres de los ganchos que utilizan la secuencia de comandos y el tipo de operación con la que están configurados para ejecutarse.

Edite un gancho de ejecución

Puede editar un enlace de ejecución si desea cambiar sus atributos, filtros o la secuencia de comandos que utiliza. Necesita tener permisos de propietario, administrador o miembro para editar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para un gancho que desee editar.
4. Seleccione **Editar**.
5. Haga los cambios necesarios, seleccione **Siguiente** después de completar cada sección.
6. Seleccione **Guardar**.

Desactivar un gancho de ejecución

Puede desactivar un gancho de ejecución si desea impedir temporalmente que se ejecute antes o después de una instantánea de una aplicación. Necesita tener permisos de propietario, administrador o miembro para desactivar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea desactivar.
4. Seleccione **Desactivar**.

Eliminar un gancho de ejecución

Puede eliminar un enlace de ejecución por completo si ya no lo necesita. Necesita tener permisos de propietario, administrador o miembro para eliminar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea eliminar.
4. Seleccione **Eliminar**.

5. En el cuadro de diálogo que aparece, escriba "delete" para confirmar.
6. Seleccione **Sí, elimine el enlace de ejecución**.

Si quiere más información

- ["Proyecto Verda GitHub de NetApp"](#)

Supervise el estado de las aplicaciones y del clúster

Ver un resumen del estado de las aplicaciones y el clúster

Seleccione * Dashboard* para ver una vista de alto nivel de sus aplicaciones, clusters, back-ends de almacenamiento y su estado.

No se trata sólo de números o Estados estáticos, sino que se puede profundizar en cada uno de ellos. Por ejemplo, si las aplicaciones no están completamente protegidas, puede pasar el ratón sobre el icono para identificar qué aplicaciones no están completamente protegidas, lo que incluye un motivo.

Aplicaciones

El mosaico **aplicaciones** le ayuda a identificar lo siguiente:

- Cuántas aplicaciones gestiona actualmente con Astra.
- Si esas aplicaciones gestionadas están en buen estado.
- Si las aplicaciones están totalmente protegidas (están protegidas si hay backups recientes disponibles).
- El número de aplicaciones que se han detectado, pero que aún no se han administrado.

Lo ideal sería que este número fuera cero porque gestionaría o ignoraría aplicaciones después de que se descubrieran. Y, a continuación, supervisaría el número de aplicaciones detectadas en el Panel de control para identificar cuándo los desarrolladores añaden nuevas aplicaciones a un clúster.

Icono de clústeres

El mosaico **Clusters** proporciona detalles similares sobre el estado de los clústeres que está administrando utilizando Astra Control Center, y puede profundizar para obtener más detalles como usted puede con una app.

Icono de los back-ends de almacenamiento

El mosaico **back-ends** de almacenamiento proporciona información para ayudarle a identificar el estado de los back-ends de almacenamiento, incluidos:

- Cuántos back-ends de almacenamiento se gestionan
- Si estos back-ends administrados son en buen estado
- Si los back-ends están totalmente protegidos
- La cantidad de back-ends que se detectan, pero todavía no se gestionan.

Consulte el estado del clúster y gestione las clases de almacenamiento

Después de añadir clústeres que debe gestionar Astra Control Center, puede ver detalles sobre el clúster, como su ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento. También es posible cambiar la clase de almacenamiento predeterminada para los clústeres gestionados.

Ver el estado y los detalles del clúster

Puede ver detalles sobre el clúster, como la ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento.

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster cuyos detalles desea ver.



Si hay un clúster en `removed` estado aunque la conectividad del clúster y de la red parece correcta (los intentos externos de acceder al clúster mediante las API de Kubernetes se han realizado correctamente), es posible que la imagen que proporcionó a Astra Control ya no sea válida. Esto puede deberse a la rotación o a la caducidad del certificado en el clúster. Para corregir este problema, actualice las credenciales asociadas con el clúster en Astra Control mediante "[API de control Astra](#)".

3. Consulte la información en las pestañas **Descripción general**, **almacenamiento** y **actividad** para encontrar la información que busca.
 - **Descripción general**: Detalles sobre los nodos de trabajo, incluido su estado.
 - **almacenamiento**: Los volúmenes persistentes asociados con el cálculo, incluyendo la clase de almacenamiento y el estado.
 - **Actividad**: Muestra las actividades relacionadas con el cluster.



También puede ver la información del clúster a partir de Astra Control Center **Dashboard**. En la ficha **Clusters** de **Resumen de recursos**, puede seleccionar los clústeres administrados, que le llevará a la página **Clusters**. Después de llegar a la página **Clusters**, siga los pasos descritos anteriormente.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de. Cuando Astra Control gestiona un clúster, realiza un seguimiento de la clase de almacenamiento predeterminada del clúster.



No cambie la clase de almacenamiento con comandos `kubectl`. Utilice este procedimiento en su lugar. Astra Control revertirá los cambios si se realizan con `kubectl`.

Pasos

1. En la interfaz de usuario web de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.

5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Ver el estado y los detalles de una aplicación

Una vez que empiece a gestionar una aplicación, Astra Control proporciona información detallada 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. Revise la información.

- **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.
- **App Protection Status:** Proporciona un estado de la protección de la aplicación:
 - **totalmente protegido:** La aplicación tiene una programación de copia de seguridad activa y una copia de seguridad exitosa que tiene menos de una semana de antigüedad
 - **parcialmente protegido:** La aplicación tiene una programación de copia de seguridad activa, una programación de instantáneas activa o una copia de seguridad o instantánea correcta
 - **desprotegido:** Aplicaciones que no están completamente protegidas o parcialmente protegidas.

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

- **Descripción general:** Información sobre el estado de los pods que están asociados con la aplicación.
- **Protección de datos:** Permite configurar una directiva de protección de datos y ver las instantáneas y copias de seguridad existentes.
- **Almacenamiento:** Muestra los volúmenes persistentes a nivel de aplicación. El estado de un volumen persistente es desde el punto de vista del clúster de Kubernetes.
- **Recursos:** Permite verificar qué recursos se están haciendo copias de seguridad y gestionando.
- **Actividad:** Muestra las actividades relacionadas con la aplicación.



También puede ver la información de la aplicación, empezando por Astra Control Center **Dashboard**. En la ficha **aplicaciones de Resumen de recursos**, puede seleccionar las aplicaciones administradas, que le llevará a la página **aplicaciones**. Después de llegar a la página **aplicaciones**, siga los pasos descritos anteriormente.

Gestione su cuenta

Gestione usuarios locales y roles

Puede añadir, eliminar y editar usuarios de la instalación de Astra Control Center mediante la interfaz de usuario de Astra Control. Puede utilizar la interfaz de usuario de Astra Control o ["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 Control. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP. En la siguiente documentación, se ofrece más información:

- ["Utilice la API Astra Control para gestionar la autenticación y los usuarios remotos"](#)
- ["Utilice la interfaz de usuario de Astra Control para gestionar grupos y usuarios remotos"](#)
- ["Utilice la interfaz de usuario de Astra Control para gestionar la autenticación remota"](#)

Añadir usuarios

Los propietarios y administradores de cuentas pueden agregar más usuarios a la instalación de Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Agregar usuario**.
4. Introduzca el nombre del usuario, la dirección de correo electrónico y una contraseña temporal.

El usuario deberá cambiar la contraseña en el primer inicio de sesión.

5. Seleccione una función de usuario con los permisos de sistema adecuados.

Cada rol proporciona los siguientes permisos:

- Un **Visor** puede ver los recursos.
 - Un **Miembro** tiene permisos de función de Viewer y puede administrar aplicaciones y clústeres, anular la administración de aplicaciones y eliminar instantáneas y copias de seguridad.
 - Un **Admin** tiene permisos de rol de miembro y puede agregar y quitar cualquier otro usuario excepto el propietario.
 - **Owner** tiene permisos de función de administrador y puede agregar y eliminar cualquier cuenta de usuario.
6. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones**.

Para obtener más información sobre cómo agregar restricciones, consulte "[Gestione usuarios locales y roles](#)".

7. Seleccione **Agregar**.

Gestionar contraseñas

Puede gestionar las contraseñas de las cuentas de usuario en Astra Control Center.

Cambie la contraseña

Puede cambiar la contraseña de su cuenta de usuario en cualquier momento.

Pasos

1. Seleccione el icono Usuario situado en la parte superior derecha de la pantalla.
2. Seleccione **Perfil**.
3. En el menú Opciones de la columna **acciones** y seleccione **Cambiar contraseña**.
4. Introduzca una contraseña que se ajuste a los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.
6. Seleccione **Cambiar contraseña**.

Restablecer la contraseña de otro usuario

Si su cuenta tiene permisos de rol de administrador o propietario, puede restablecer las contraseñas de otras cuentas de usuario así como las suyas propias. Al restablecer una contraseña, asigna una contraseña temporal que el usuario tendrá que cambiar al iniciar sesión.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la lista desplegable **acciones**.
3. Seleccione **Restablecer contraseña**.
4. Introduzca una contraseña temporal que cumpla los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.



La próxima vez que el usuario inicie sesión, se le pedirá que cambie la contraseña.

6. Seleccione **Restablecer contraseña**.

Quitar usuarios

Los usuarios con el rol propietario o administrador pueden eliminar otros usuarios de la cuenta en cualquier momento.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios**, active la casilla de verificación en la fila de cada usuario que desee quitar.
3. En el menú Opciones de la columna **acciones**, seleccione **Eliminar usuario/s**.
4. Cuando se le solicite, confirme la eliminación escribiendo la palabra "eliminar" y, a continuación,

seleccione **Sí, Eliminar usuario**.

Resultado

Astra Control Center elimina al usuario de la cuenta.

Gestionar roles

Es posible gestionar roles si se añaden restricciones de espacio de nombres y se restringen los roles del usuario a dichas restricciones. Esto le permite controlar el acceso a los recursos de su organización. Puede utilizar la interfaz de usuario de Astra Control o "[La API de control Astra](#)" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Administrador o propietario puede agregar restricciones de espacio de nombres a las funciones de miembro o de visor.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor.
4. Seleccione **Editar rol**.
5. Active la casilla de verificación **restringir rol a restricciones**.

La casilla de verificación sólo está disponible para funciones de miembro o de visor. Puede seleccionar un rol diferente de la lista desplegable **rol**.

6. Seleccione **Agregar restricción**.

Se puede ver la lista de restricciones disponibles por espacio de nombres o por etiqueta de espacio de nombres.

7. En la lista desplegable **Tipo de restricción**, seleccione **espacio de nombres Kubernetes** o **etiqueta de espacio de nombres Kubernetes** dependiendo de cómo estén configurados los espacios de nombres.
8. Seleccione uno o más espacios de nombres o etiquetas de la lista para redactar una restricción que restrinja las funciones a esos espacios de nombres.
9. Seleccione **Confirmar**.

La página **Editar función** muestra la lista de restricciones que ha elegido para esta función.

10. Seleccione **Confirmar**.

En la página **cuenta**, puede ver las restricciones de cualquier rol de miembro o de visor en la columna **rol**.



Si habilita restricciones para una función y selecciona **Confirmar** sin agregar restricciones, se considera que la función tiene restricciones completas (se deniega el acceso a cualquier recurso asignado a espacios de nombres).

Quitar una restricción de espacio de nombres de una función

Un usuario Admin o Owner puede eliminar una restricción de espacio de nombres de una función.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor que tiene restricciones activas.
4. Seleccione **Editar rol**.

El cuadro de diálogo **Editar función** muestra las restricciones activas para la función.

5. Seleccione **X** a la derecha de la restricción que debe eliminar.
6. Seleccione **Confirmar**.

Si quiere más información

- ["Roles de usuario y espacios de nombres"](#)

Administrar la autenticación remota

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra Control.

En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP.



Astra Control Center utiliza la dirección de correo electrónico en el atributo "mail" LDAP para buscar y realizar un seguimiento de los usuarios remotos. Este atributo puede ser un campo opcional o vacío en su directorio. Debe existir una dirección de correo electrónico en este campo para los usuarios remotos que desee que aparezcan en Astra Control Center. Esta dirección de correo electrónico se utiliza como nombre de usuario en Astra Control Center para la autenticación.

Añada un certificado para la autenticación LDAPS

Agregue el certificado TLS privado del servidor LDAP para que Astra Control Center pueda autenticarse con el servidor LDAP cuando utilice una conexión LDAPS. Sólo tiene que hacerlo una vez o cuando caduque el certificado que ha instalado.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **certificados**.
3. Seleccione **Agregar**.
4. Cargue el `.pem` archivo o pega el contenido del archivo desde el portapapeles.
5. Seleccione la casilla de verificación **Trusted**.
6. Seleccione **Agregar certificado**.

Habilite la autenticación remota

Puede habilitar la autenticación LDAP y configurar la conexión entre Astra Control y el servidor LDAP remoto.

Antes de empezar

Si planea utilizar LDAPS, asegúrese de que el certificado TLS privado del servidor LDAP está instalado en Astra Control Center para que Astra Control Center pueda autenticarse con el servidor LDAP. Consulte [Añada un certificado para la autenticación LDAPS](#) si desea obtener instrucciones.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **conectar**.
4. Introduzca la dirección IP del servidor, el puerto y el protocolo de conexión preferido (LDAP o LDAPS).



Como práctica recomendada, use LDAPS al conectarse con el servidor LDAP. Debe instalar el certificado TLS privado del servidor LDAP en Astra Control Center antes de conectarse con LDAPS.

5. Introduzca las credenciales de la cuenta de servicio en formato de correo electrónico ([administrator@example.com](#)). Astra Control utilizará estas credenciales al conectar con el servidor LDAP.
6. En la sección **coincidencia de usuario**, introduzca el DN base y un filtro de búsqueda de usuario apropiado que se utilizará al recuperar información de usuario del servidor LDAP.
7. En la sección **coincidencia de grupo**, introduzca el DN base de búsqueda de grupo y un filtro de búsqueda de grupo personalizado adecuado.



Asegúrese de utilizar el nombre completo (DN) de base correcto y un filtro de búsqueda apropiado para **coincidencia de usuario** y **coincidencia de grupo**. El DN base indica a Astra Control en qué nivel del árbol de directorios iniciar la búsqueda, y el filtro de búsqueda limita las partes del árbol de directorios de las búsquedas de Astra Control.

8. Seleccione **Enviar**.

Resultado

El estado del panel **autenticación remota** pasa a **pendiente** y a **conectado** cuando se establece la conexión con el servidor LDAP.

Desactivar la autenticación remota

Puede deshabilitar temporalmente una conexión activa con el servidor LDAP.



Cuando se deshabilita una conexión a un servidor LDAP, se guardan todas las opciones y se conservan todos los usuarios y grupos remotos que se agregaron a Astra Control desde ese servidor LDAP. Puede volver a conectarse a este servidor LDAP en cualquier momento.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Desactivar**.

Resultado

El estado del panel **autenticación remota** pasa a **Desactivada**. Se conservan todos los ajustes de autenticación remota, usuarios remotos y grupos remotos, y se puede volver a habilitar la conexión en cualquier momento.

Edite la configuración de autenticación remota

Si ha desactivado la conexión al servidor LDAP o el panel **autenticación remota** se encuentra en el estado "error de conexión", puede editar los valores de configuración.



No puede editar la dirección IP o la dirección URL del servidor LDAP cuando el panel **autenticación remota** está en estado "Desactivada". Necesita hacerlo [Desconecte la autenticación remota](#) primero.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Editar**.
4. Realice los cambios necesarios y seleccione **Editar**.

Desconecte la autenticación remota

Puede desconectarse de un servidor LDAP y eliminar los ajustes de configuración de Astra Control.



Cuando se desconecta del servidor LDAP, todas las opciones de configuración de ese servidor LDAP se eliminan de Astra Control, así como todos los usuarios y grupos remotos que se hayan agregado de ese servidor LDAP.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **desconectar**.

Resultado

El estado del panel **autenticación remota** pasa a **desconectado**. La configuración de autenticación remota, los usuarios remotos y los grupos remotos se eliminan de Astra Control.

Administrar grupos y usuarios remotos

Si ha activado la autenticación LDAP en el sistema Astra Control, puede buscar usuarios y grupos LDAP e incluirlos en los usuarios aprobados del sistema.

Agregar un usuario remoto

Los propietarios y administradores de cuentas pueden agregar usuarios remotos a Astra Control.



No puede agregar un usuario remoto si ya existe en el sistema un usuario local con la misma dirección de correo electrónico. Para agregar el usuario como usuario remoto, elimine primero el usuario local del sistema.



Astra Control Center utiliza la dirección de correo electrónico en el atributo "mail" LDAP para buscar y realizar un seguimiento de los usuarios remotos. Este atributo puede ser un campo opcional o vacío en su directorio. Debe existir una dirección de correo electrónico en este campo para los usuarios remotos que desee que aparezcan en Astra Control Center. Esta dirección de correo electrónico se utiliza como nombre de usuario en Astra Control Center para la autenticación.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **usuarios remotos**.
4. Seleccione **Agregar**.
5. Opcionalmente, busque un usuario LDAP introduciendo la dirección de correo electrónico del usuario en el campo **Filtrar por correo electrónico**.
6. Seleccione uno o varios usuarios de la lista.
7. Asigne un rol al usuario.



Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este usuario y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.



Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo usuario aparece en la lista de usuarios remotos. En esta lista, puede ver restricciones activas en el usuario, así como administrar el usuario desde el menú **acciones**.

Agregar un grupo remoto

Para agregar muchos usuarios remotos a la vez, los propietarios de cuentas y los administradores pueden agregar grupos remotos a Astra Control. Cuando agrega un grupo remoto, todos los usuarios remotos de ese grupo se agregan a Astra Control y heredan la misma función.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **grupos remotos**.
4. Seleccione **Agregar**.

En esta ventana, puede ver una lista de los nombres comunes y nombres distintivos de los grupos LDAP que Astra Control ha recuperado del directorio.

5. Opcionalmente, busque un grupo LDAP introduciendo el nombre común del grupo en el campo **filtro por nombre común**.
6. Seleccione uno o varios grupos de la lista.
7. Asigne un rol a los grupos.



El rol que seleccione se asigna a todos los usuarios de este grupo. Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este grupo y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.



Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo grupo aparece en la lista de grupos remotos y todos los usuarios remotos de este grupo aparecen en la lista de usuarios remotos. En esta lista, puede ver detalles sobre el grupo, así como administrar el grupo desde el menú **acciones**.

Ver y gestionar notificaciones

Astra le notifica cuando las acciones se han completado o han fallado. Por ejemplo, verá una notificación si una copia de seguridad de una aplicación se ha completado correctamente.

Puede gestionar estas notificaciones desde la parte superior derecha de la interfaz:



Pasos

1. Seleccione el número de notificaciones sin leer en la parte superior derecha.
2. Revise las notificaciones y seleccione **Marcar como leído** o **Mostrar todas las notificaciones**.

Si ha seleccionado **Mostrar todas las notificaciones**, se cargará la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, seleccione **Acción** y seleccione **Marcar como leído**.

Añada y elimine credenciales

Añada y elimine credenciales de proveedores de cloud privado local como ONTAP S3, clústeres de Kubernetes gestionados con OpenShift o clústeres de Kubernetes no gestionados de su cuenta en cualquier momento. Astra Control Center utiliza estas credenciales para descubrir los clústeres y las aplicaciones de Kubernetes en los clústeres, y para aprovisionar recursos en su nombre.

Tenga en cuenta que todos los usuarios de Astra Control Center comparten los mismos conjuntos de credenciales.

Añada credenciales

Puede agregar credenciales a Astra Control Center cuando gestiona los clústeres. Para añadir credenciales al añadir un clúster nuevo, consulte ["Añada un clúster de Kubernetes"](#).



Si 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 Control Center 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 bloques

Un proveedor de bloques de almacenamiento de objetos es esencial si desea realizar backups de las aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Con Astra Control Center, agregue un proveedor de almacenes de objetos como destino de copia de seguridad fuera del clúster para sus aplicaciones.

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

Use uno de los siguientes proveedores de bloques de Amazon simple Storage Service (S3):

- NetApp ONTAP S3
- StorageGRID S3 de NetApp
- Microsoft Azure
- Genérico S3



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



Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Un cubo puede estar en uno de estos estados:

- Pending: Se ha programado la detección del bloque.
- Disponible: El cucharón está disponible para su uso.
- Eliminado: No se puede acceder al depósito actualmente.

Para obtener instrucciones sobre cómo gestionar los cubos con la API Astra Control, consulte ["Información sobre API y automatización de Astra"](#).

Puede realizar estas tareas relacionadas con la gestión de bloques:

- ["Añadir un bucket"](#)
- [Editar un bloque](#)
- [Establecer el bloque predeterminado](#)

- [Gire o elimine las credenciales del cucharón](#)
- [Retirar un cucharón](#)



Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Editar un bloque

Puede cambiar la información de credenciales de acceso de un bloque y cambiar si un bloque seleccionado es el bloque predeterminado.



Cuando agregue un bloque, seleccione el proveedor de segmento correcto y proporcione las credenciales correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como tipo y acepta credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los futuros backups de aplicaciones y restauraciones usando este bucket. Consulte "[Notas de la versión](#)".

Pasos

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú de la columna **acciones**, seleccione **Editar**.
3. Cambie cualquier información que no sea el tipo de segmento.



No puede modificar el tipo de segmento.

4. Seleccione **Actualizar**.

Establecer el bloque predeterminado

Cuando se realiza un clon entre clústeres, Astra Control requiere un bloque predeterminado. Siga estos pasos para establecer un bloque predeterminado para todos los clústeres.

Pasos

1. Vaya a **instancias de cloud**.
2. Seleccione el menú en la columna **acciones** para la instancia de nube de la lista.
3. Seleccione **Editar**.
4. En la lista **bloque**, seleccione el segmento que desea que sea el predeterminado.
5. Seleccione **Guardar**.

Gire o elimine las credenciales del cucharón

Astra Control utiliza las credenciales de bloque para obtener acceso y proporcionar claves secretas para un bloque de S3, de forma que Astra Control Center pueda comunicarse con el cucharón.

Rotar las credenciales del cucharón

Si gira las credenciales, gírelos durante una ventana de mantenimiento cuando no haya copias de seguridad en curso (programadas o bajo demanda).

Pasos para editar y girar credenciales

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú Opciones de la columna **acciones**, seleccione **Editar**.
3. Cree la nueva credencial.
4. Seleccione **Actualizar**.

Quitar las credenciales del bloque

Debe eliminar las credenciales de bloque solo si se han aplicado credenciales nuevas a un bloque o si ya no se utiliza el bloque de forma activa.



El primer conjunto de credenciales que agregue a Astra Control siempre está en uso porque Astra Control utiliza las credenciales para autenticar el bloque de copia de seguridad. No elimine estas credenciales si el bloque está en uso activo, ya que esto dará lugar a fallos de copia de seguridad y a falta de disponibilidad de copia de seguridad.



Si elimina las credenciales de bloque activas, consulte ["solución de problemas de eliminación de credenciales del bloque"](#).

Para obtener instrucciones sobre cómo eliminar credenciales de S3 mediante la API Astra Control, consulte ["Información sobre API y automatización de Astra"](#).

Retirar un cucharón

Puede eliminar un cubo que ya no esté en uso o que no esté sano. Se recomienda hacer esto para mantener la configuración del almacén de objetos sencilla y actualizada.



No se puede eliminar un bloque predeterminado. Si desea eliminar ese bloque, seleccione primero otro bloque como predeterminado.

Antes de empezar

- Antes de empezar, debe comprobar que no hay copias de seguridad en ejecución o completadas para este bloque.
- Debe comprobar que el bloque no se esté utilizando en ninguna política de protección activa.

Si 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](#)
- [Editar los detalles de autenticación del back-end de almacenamiento](#)
- [Gestionar un back-end de almacenamiento detectado](#)
- [Desgestione un back-end de almacenamiento](#)
- [Quite un back-end de almacenamiento](#)

Ver detalles del back-end de almacenamiento

Puede ver la información del back-end de almacenamiento desde Dashboard o desde la opción Backends.

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

Pasos

1. En la navegación de la izquierda, seleccione **Tablero**.
2. Revise el panel del back-end de almacenamiento de Dashboard que muestra el estado:
 - **Insalubre**: El almacenamiento no está en un estado óptimo. Esto puede deberse a un problema de latencia o a que una aplicación está degradada debido a un problema de contenedor, por ejemplo.
 - **Todo sano**: El almacenamiento ha sido gestionado y se encuentra en un estado óptimo.
 - **Descubierto**: El almacenamiento ha sido descubierto, pero no gestionado por Astra Control.

Consulte los detalles del backends de almacenamiento en la opción Backends

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

Puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado. 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.

Name	Persistent volume	Capacity	App/s	Cluster/s	Cloud
trident_pvc_...	pvc_...	0.04/46.57 GiB: 0.1%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	0.34/23.28 GiB: 1.44%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	0.02/0.93 GiB: 2.33%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	3.02/50.00 GiB: 6.04%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc_...	0.19/8.00 GiB: 2.39%	apps-mysql mysql-mysql	openshift-cluster010	private
trident_pvc_...	pvc_...	0.41/50.00 GiB: 0.81%	netapp-acc polaris-influxdb2-polaris-influxdb2	openshift-cluster010	private
trident_pvc_...	pvc_...	2.93/50.00 GiB: 5.87%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc_...	0.03/10.00 GiB: 0.26%	netapp-acc polaris-consul-consul	openshift-cluster010	private

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

Editar los detalles de autenticación del back-end de almacenamiento

El Centro de control de Astra ofrece dos modos de autenticación de un back-end de ONTAP.

- **Autenticación basada en credenciales:** El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos requeridos. Debe utilizar un rol de inicio de sesión de seguridad predefinido, como admin, para garantizar la máxima compatibilidad con las versiones de ONTAP.
- **Autenticación basada en certificados:** Astra Control Center también puede comunicarse con un clúster de ONTAP utilizando un certificado instalado en el backend. Debe usar el certificado de cliente, la clave y el certificado de CA de confianza si se utilizan (recomendado).

Puede actualizar los back-ends existentes para pasar de un tipo de autenticación a otro método. Solo se admite un método de autenticación a la vez.

Para obtener más información sobre la activación de la autenticación basada en certificados, consulte "[Habilite la autenticación en el back-end de almacenamiento de ONTAP](#)".

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el campo Credenciales, seleccione el icono **Editar**.
4. En la página Editar, seleccione una de las siguientes opciones.
 - **Usar credenciales de administrador:** Ingrese la dirección IP de administración del clúster de ONTAP y las credenciales de administración. Las credenciales deben ser credenciales para todo el clúster.



El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, aplique las credenciales de usuario con el rol "admin", que tiene los métodos de acceso `ontapi` y `http`. En clústeres ONTAP de origen y destino. Consulte ["Gestionar cuentas de usuario en la documentación de ONTAP"](#) si quiere más información.

- **Utilice un certificado:** Cargue el certificado `.pem` archivo, la clave de certificado `.key` archivo y, opcionalmente, el archivo de entidad de certificación.
5. Seleccione **Guardar**.

Gestionar un back-end de almacenamiento detectado

Puede seleccionar gestionar un back-end de almacenamiento no gestionado pero detectado. Cuando gestionas un back-end de almacenamiento, Astra Control indica si ha caducado un certificado para la autenticación.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione la opción **Descubrido**.
3. Seleccione el back-end de almacenamiento.
4. En el menú Opciones de la columna **Acciones**, selecciona **Administrar**.
5. Realice los cambios.
6. Seleccione **Guardar**.

Desgestione un back-end de almacenamiento

Puede anular la gestión del back-end.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el menú Opciones de la columna **acciones**, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar la acción.
5. Seleccione **Sí, anular la administración del backend de almacenamiento**.

Quite un back-end de almacenamiento

Puede eliminar un back-end de almacenamiento que ya no se esté utilizando. Se recomienda hacer esto para mantener su configuración sencilla y actualizada.

Antes de empezar

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

Pasos

1. En la navegación izquierda, seleccione **Backends**.
2. Si se gestiona el back-end, desgestione.
 - a. Seleccione **gestionado**.
 - b. Seleccione el back-end de almacenamiento.
 - c. Desde la opción **Acciones**, selecciona **Desgestionar**.
 - 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**, selecciona **Eliminar**.
 - c. Escriba "eliminar" para confirmar la acción.
 - d. Seleccione **Sí, quite el backend de almacenamiento**.

Obtenga más información

- ["Utilice la API Astra Control"](#)

Supervisar tareas en ejecución

Puede ver detalles sobre las tareas en ejecución y las tareas que se han completado, han fallado o han sido canceladas en las últimas 24 horas en Astra Control. Por ejemplo, puede ver el estado de una operación de backup, restauración o clonado en ejecución, y ver detalles como un porcentaje completado y el tiempo restante estimado. Es posible ver el estado de una operación programada que se haya ejecutado o una operación que se inició manualmente.

Mientras ve una tarea en ejecución o completada, puede expandir los detalles de la tarea para ver el estado de cada una de las subtareas. La barra de progreso de la tarea es verde para las tareas en curso o completadas, azul para las tareas canceladas y rojo para las tareas que han fallado debido a un error.



Para las operaciones de clonado, las subtareas consisten en una operación de restauración de Snapshot y de Snapshot.

Para ver más información sobre las tareas fallidas, consulte ["Controlar la actividad de la cuenta"](#).

Pasos

1. Mientras se está ejecutando una tarea, vaya a **aplicaciones**.
2. Seleccione el nombre de una aplicación de la lista.
3. En los detalles de la aplicación, seleccione la ficha **tareas**.

Puede ver detalles de tareas actuales o pasadas y filtrar por estado de tarea.



Las tareas se conservan en la lista **tareas** durante un máximo de 24 horas. Puede configurar este límite y otros ajustes del monitor de tareas mediante "[API de control Astra](#)".

Supervise la infraestructura con conexiones Cloud Insights, Prometheus o Fluentd

Puede configurar varios ajustes opcionales para mejorar su experiencia con Astra Control Center. Para supervisar y obtener información sobre toda su infraestructura, cree una conexión con Cloud Insights de NetApp, configure Prometheus o 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.

- [Conéctese a Cloud Insights](#)
- [Conéctese a Prometheus](#)
- [Conectar a Fluentd](#)

Añada un servidor proxy para las conexiones a Cloud Insights 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.



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected ▼

Connect

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.



Connected



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Edite la configuración del servidor proxy

Puede editar la configuración del servidor proxy.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin/owner**.
2. Seleccione **cuenta > conexiones**.
3. Seleccione **Editar** de la lista desplegable para editar la conexión.
4. Edite los detalles del servidor y la información de autenticación.
5. Seleccione **Guardar**.

Desactive la conexión del servidor proxy

Puede desactivar la conexión del servidor proxy. Se le advertirá antes de 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.



Cuando Astra Control Center se empareja con Cloud Insights, no debes usar la opción **Modificar implementación** en Cloud Insights.



Después de habilitar la conexión Cloud Insights, puede ver la información de rendimiento en la página **Backends**, así como conectarse a Cloud Insights después de seleccionar un backend de almacenamiento. También puede encontrar la información en el **Tablero** en la sección **Clúster** y conectarse a Cloud Insights desde allí.

Antes de empezar

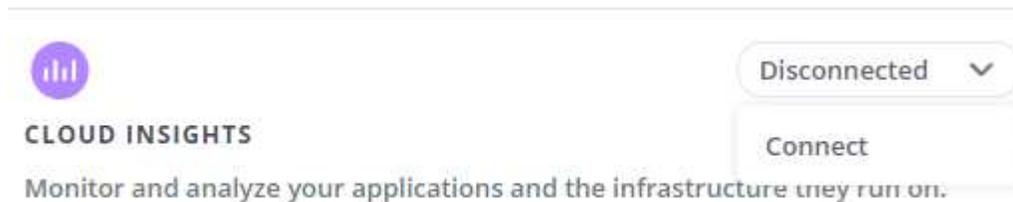
- Una cuenta de Astra Control Center con privilegios **admin/owner**.
- Una licencia válida de Astra Control Center.
- Un servidor proxy si la red en la que se ejecuta Astra Control Center requiere un proxy para conectarse a Internet.



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**.

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission
<input type="checkbox"/>	astra_...		...zBskB1	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...xKOeL_	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...2_A6HP	All Categories	Read Only
<input type="checkbox"/>	astra_...		...8BTKYY	All Categories	Read/Write

- 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: Ingesta de datos, ingestión de registros, unidad de adquisición y recopilación de datos.



Le recomendamos que genere una tecla **sólo lectura** y una tecla **Leer/escibir**, 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.

EXTERNAL ?

The screenshot shows two connection cards. The first is for 'HTTP PROXY' with a server address of 'proxy.example.com:8888' and authentication enabled. The second is for 'CLOUD INSIGHTS' with a tenant of 'Cloud Insights'. Both cards have a 'Connected' status and a dropdown arrow.

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.

The notification panel shows a red notification icon with the number '33'. The notification message reads: 'Unable to connect to Cloud Insights an hour ago. The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.'

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.

The screenshot shows the 'Backends' page with a table of storage backends. The table has columns for Name, Status, Capacity, Throughput, Type, and Actions. A tooltip for the 'Throughput' column is shown, displaying a line graph and statistics: 'Throughput Last 24 hrs', '5m ago: 8.00 MB/s', 'Min: 4.00 MB/s', and 'Max: 11.00 MB/s'. A link to 'View in Cloud Insights' is also present.

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**.

Reminder: Before you back up your applications, you need to add at least one object store bucket as a destination to hold your backups.

Add →

Resource summary

The screenshot shows the 'Resource summary' section of the Astra Control Center dashboard. It is divided into three main panels: 'Apps', 'Clusters', and 'Storage backends'. The 'Apps' panel shows 'No managed apps'. The 'Clusters' panel has a 'Let's get started' message and an 'Add' button. The 'Storage backends' panel shows '1 Managed' and '0 Discovered'. A blue box highlights the 'View in cloud insights' link above the Clusters 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** de 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**.

Conéctese a Prometheus

Puede supervisar los datos del Centro de control de Astra con Prometheus. Puede configurar Prometheus para recopilar métricas desde el extremo de métricas del clúster de Kubernetes, y también puede utilizar Prometheus para visualizar los datos de métricas.

Para obtener más información sobre el uso de Prometheus, consulte su documentación en ["Introducción a Prometheus"](#).

Lo que necesitará

Asegúrese de que ha descargado e instalado el paquete Prometheus en el clúster Astra Control Center o en un clúster diferente que pueda comunicarse con el clúster Astra Control Center.

Siga las instrucciones de la documentación oficial para ["Instale Prometheus"](#).

Prometheus debe poder comunicarse con el clúster Kubernetes de Astra Control Center. Si Prometheus no está instalado en el clúster de Astra Control Center, debe asegurarse de que puede comunicarse con el servicio de métricas que se ejecuta en el clúster de Astra Control Center.

Configure Prometheus

Astra Control Center expone un servicio de mediciones en el puerto TCP 9090 del clúster de Kubernetes. Debe configurar Prometheus para recopilar métricas de este servicio.

Pasos

1. Inicie sesión en el servidor Prometheus.
2. Añada la entrada del clúster en el `prometheus.yml` archivo. En la `yml` file, añada una entrada similar a la siguiente para su clúster en el `scrape_configs` section:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
metrics_path: /accounts/<replace with your account ID>/metrics
authorization:
  credentials: <replace with your API token>
tls_config:
  insecure_skip_verify: true
static_configs:
  - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```



Si establece la `tls_config insecure_skip_verify` para `true`, El protocolo de cifrado TLS no es necesario.

3. Reinicie el servicio Prometheus:

```
sudo systemctl restart prometheus
```

Prometheus de acceso

Acceda a la URL de Prometheus.

Pasos

1. En un explorador, introduzca la URL Prometheus con el puerto 9090.

2. Compruebe su conexión seleccionando **Estado > objetivos**.

Ver datos en Prometheus

Puede utilizar Prometheus para ver los datos de Astra Control Center.

Pasos

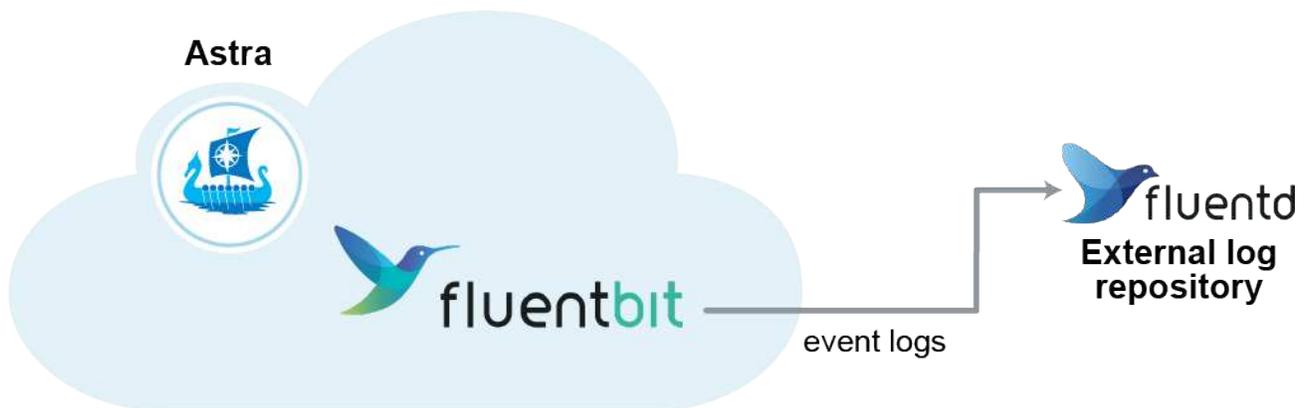
1. En un navegador, introduzca la URL de Prometheus.
2. En el menú Prometheus, seleccione **Gráfico**.
3. Para utilizar el Explorador de métricas, seleccione el icono situado junto a **Ejecutar**.
4. Seleccione `scrape_samples_scraped` Y seleccione **Ejecutar**.
5. Para ver el raspado de muestras a lo largo del tiempo, seleccione **Gráfico**.



Si se recopilaron varios datos de clúster, las métricas de cada clúster aparecen en un color diferente.

Conectar a Fluentd

Puede enviar registros (eventos de Kubernetes) desde un sistema supervisado por Astra Control Center a su extremo de Fluentd. La conexión fluentd está desactivada de forma predeterminada.



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

Antes de empezar

- Una cuenta de Astra Control Center con privilegios **admin/owner**.
- Astra Control Center se ha instalado y se ejecuta en un clúster de Kubernetes.

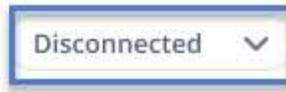


Astra Control Center no valida los detalles que introduzca para su servidor Fluentd. Asegúrese de introducir los valores correctos.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin/owner**.
2. Seleccione **cuenta > conexiones**.

3. Seleccione **conectar** en la lista desplegable en la que aparece **Desconectado** para agregar la conexión.



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

4. Introduzca la dirección IP del host, el número de puerto y la clave compartida para el servidor Fluentd.
5. Seleccione **conectar**.

Resultado

Si se guardaron los datos introducidos para el servidor Fluentd, la sección **Fluentd** de la página **cuenta > conexiones** indica que está conectado. Ahora puede visitar el servidor Fluentd que ha conectado y ver los registros de eventos.

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

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



Si tiene problemas con la recopilación de registros, debe iniciar sesión en el nodo de trabajo y asegurarse de que los registros están disponibles en `/var/log/containers/`.

Edite la conexión fluentd

Puede editar la conexión Fluentd a su instancia de Astra Control Center.

Pasos

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

Desactive la conexión fluentd

Puede desactivar la conexión Fluentd a la instancia de Astra Control Center.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin/owner**.
2. Seleccione **cuenta > conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación.

Desgestione aplicaciones y clústeres

Elimine las aplicaciones o clústeres que ya no desee gestionar desde Astra Control Center.

Desgestionar una aplicación

Detenga la gestión de las aplicaciones de las que ya no desee realizar copias de seguridad, copias Snapshot o clones de Astra Control Center.

Al anular la gestión de una aplicación:

- Se eliminarán todos los backups y las snapshots existentes.
- Las aplicaciones y los datos siguen estando disponibles.

Pasos

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

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

Deje de gestionar el clúster que ya no desea gestionar desde Astra Control Center.



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

Cuando se desadministra un clúster:

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

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla de comprobación del clúster que ya no desee administrar.
3. En el menú Opciones de la columna **acciones**, seleccione **Unmanage**.
4. Confirme que desea anular la administración del clúster y, a continuación, seleccione **Sí, anular la administración del clúster**.

Resultado

El estado del clúster cambia a **Extracción**. Después de eso, el clúster se eliminará de la página **Clusters** y ya no será gestionado por Astra Control Center.



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. Puede utilizar este procedimiento para actualizar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Antes de empezar

- Antes de realizar la actualización, consulte ["requisitos del entorno operativo"](#) Para garantizar que su entorno cumple los requisitos mínimos para la implantación de Astra Control Center. Su entorno debe tener lo siguiente:
 - Una versión de Astra Trident compatible
Para determinar la versión que estás ejecutando, ejecuta el siguiente comando en tu Astra Control Center existente:

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

Consulte ["Documentación de Astra Trident"](#) para actualizar desde una versión anterior.



Debe actualizar a Astra Trident 22.10 **ANTERIOR** a la actualización a Kubernetes 1.25.

- Una distribución de Kubernetes compatible
Para determinar la versión que estás ejecutando, ejecuta el siguiente comando en tu Astra Control Center existente: `kubectl get nodes -o wide`
- Suficientes recursos de clúster
Para determinar los recursos del clúster, ejecute el siguiente comando en su clúster de Astra Control Center existente: `kubectl describe node <node name>`
- Registro que puede utilizar para insertar y cargar imágenes de Astra Control Center
- Clase de almacenamiento predeterminada
Para determinar tu clase de almacenamiento predeterminada, ejecuta el siguiente comando en tu Astra Control Center actual: `kubectl get storageclass`
- (Sólo OpenShift) Asegúrese de que todos los operadores de clúster están en buen estado y disponibles.

```
kubectl get clusteroperators
```

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

```
kubectl get apiservices
```

- Cierre la sesión de la interfaz de usuario de Astra Control Center antes de comenzar la actualización.

Acerca de esta tarea

El proceso de actualización del Centro de control de Astra le guiará por los siguientes pasos de alto nivel:

- [Descargue y extraiga Astra Control Center](#)
- [Elimine el complemento Astra kubectl de NetApp y vuelva a instalarlo](#)
- [Agregue las imágenes al registro local](#)
- [Instale el operador actualizado de Astra Control Center](#)
- [Actualice Astra Control Center](#)
- [Comprobar el estado del sistema](#)



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



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

Descargue y extraiga Astra Control Center

1. Vaya a la "[Página de descargas de productos de Astra Control Center](#)" En el sitio de soporte de NetApp. Puede seleccionar la última versión u otra que desee en el menú desplegable.
2. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete:

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

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

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

4. Extraiga las imágenes del paquete Astra Control Center:

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

Elimine el complemento Astra kubectl de NetApp y vuelva a instalarlo

Puede utilizar el complemento de línea de comandos kubectl de Astra de NetApp para insertar imágenes en un repositorio de Docker local.

1. Determine si tiene instalado el plugin:

```
kubectl astra
```

2. Realice una de estas acciones:

- Si el complemento está instalado, el comando debería devolver la ayuda del complemento kubectl. Para eliminar una versión existente de kubectl-astra, ejecute este comando: `delete /usr/local/bin/kubectl-astra`.
- Si el comando devuelve un error, el plugin no está instalado y puede continuar con el siguiente paso para instalarlo.

3. Instale el complemento:

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



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

```
ls kubectl-astra/
```

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

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

Agregue las imágenes al registro local

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

Docker

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

```
acc.manifest.bundle.yaml  
acc/
```

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

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

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

Podman

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

```
acc.manifest.bundle.yaml  
acc/
```

2. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

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 o edite 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 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_UPGRADE_TIMEOUT  
  value: 300m
```

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

```

- args:
  - --secure-listen-address=0.0.0.0:8443
  - --upstream=http://127.0.0.1:8080/
  - --logtostderr=true
  - --v=10
  image: [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
  env:
    - name: ACCOP_LOG_LEVEL
      value: "2"
    - name: ACCOP_HELM_UPGRADE_TIMEOUT
      value: 300m
  image: [your_registry_path]/acc-operator:23.04.36
  imagePullPolicy: IfNotPresent
  livenessProbe:
    httpGet:
      path: /healthz
      port: 8081
      initialDelaySeconds: 15
      periodSeconds: 20
  name: manager
  readinessProbe:
    httpGet:
      path: /readyz
      port: 8081
      initialDelaySeconds: 5
      periodSeconds: 10
  resources:
    limits:
      cpu: 300m
      memory: 750Mi
    requests:
      cpu: 100m
      memory: 75Mi
  securityContext:
    allowPrivilegeEscalation: false
  imagePullSecrets: []
  securityContext:
    runAsUser: 65532

```

```
terminationGracePeriodSeconds: 10
```

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. Edite el recurso personalizado de Astra Control Center (CR):

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

2. Cambie el número de versión de Astra (astraVersion dentro de spec) a la versión que está actualizando a:

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Compruebe que la ruta del Registro de imágenes coincide con la ruta del Registro a la que ha insertado las imágenes en [paso anterior](#). Actualizar `imageRegistry` dentro de `spec` si el registro ha cambiado desde la última instalación.

```
imageRegistry:
  name: "[your_registry_path]"
```

4. Añada lo siguiente a su `crds` configuración dentro de `spec`:

```
crds:
  shouldUpgrade: true
```

5. Añada las siguientes líneas dentro de `additionalValues` dentro de `spec` En el Centro de control de Astra CR:

```
additionalValues:
  nautilus:
    startupProbe:
      periodSeconds: 30
      failureThreshold: 600
```

6. Guarde y salga del editor de archivos. Se aplicarán los cambios y comenzará la actualización.
7. (Opcional) Verifique que los POD terminan y estén disponibles de nuevo:

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

8. Espere a que las condiciones de estado de Astra Control indiquen que la actualización está completa y lista (True):

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

Respuesta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.04.2-7	
10.111.111.111	True		



Para supervisar el estado de actualización durante la operación, ejecute el siguiente comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`



Para inspeccionar los registros del operador de Astra Control Center, ejecute el siguiente comando:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Comprobar el estado del sistema

1. Inicie sesión en Astra Control Center.
2. Compruebe que la versión se ha actualizado. Consulte la página **Soporte** de la interfaz de usuario.
3. Compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.

Desinstale Astra Control Center

Es posible que necesite eliminar los componentes de Astra Control Center si va a actualizar de una versión de prueba a una versión completa del producto. Para retirar el Centro de control Astra y el operador del Centro de control Astra, ejecute las instrucciones descritas en este procedimiento en secuencia.

Si tiene algún problema con la desinstalación, consulte [Solución de problemas de desinstalación](#).

Antes de empezar

1. ["Anular la gestión de todas las aplicaciones"](#) en los clústeres.
2. ["Anule la gestión de todos los clústeres"](#).

Pasos

1. Eliminar Astra Control Center. El comando de ejemplo siguiente se basa en una instalación predeterminada. Modifique el comando si ha realizado configuraciones personalizadas.

```
kubectl delete -f astra_control_center.yaml -n netapp-acc
```

Resultado:

```
astracontrolcenter.astra.netapp.io "astra" deleted
```

2. Utilice el siguiente comando para eliminar la `netapp-acc` espacio de nombres (o con nombre personalizado):

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

Resultado de ejemplo:

```
namespace "netapp-acc" deleted
```

3. Utilice el siguiente comando para eliminar los componentes del sistema del operador de Astra Control Center:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Resultado:

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

Solución de problemas de desinstalación

Utilice las siguientes soluciones alternativas para solucionar cualquier problema que tenga al desinstalar Astra Control Center.

La desinstalación de Astra Control Center no puede limpiar el módulo de control del operador de supervisión en el clúster gestionado

Si no ha desgestionado 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"](#)

Automatice con la API REST de Astra Control

Automatización mediante la API REST de Astra Control

Astra Control dispone de una API REST que le permite acceder directamente a la funcionalidad Astra Control mediante un lenguaje de programación o una utilidad como Curl. También puede gestionar las puestas en marcha de Astra Control con Ansible y otras tecnologías de automatización.

Para configurar y gestionar sus aplicaciones Kubernetes, puede utilizar la interfaz de usuario de Astra Control Center o la API de Astra Control.

Para obtener más información, visite la "[Documentos de automatización de Astra](#)".

Conocimiento y apoyo

Resolución de problemas

Aprenda a solucionar algunos problemas comunes que puede encontrar.

["Base de conocimientos de NetApp para Astra"](#)

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 Astra Control Center Custom Resource (CR) (`astra_control_center.yaml`), los paquetes de soporte diario se cargan automáticamente en el "[Sitio de soporte de NetApp](#)".

Genere el paquete de soporte para suministrar soporte de NetApp

Astra Control Center permite al usuario administrador generar paquetes, que incluyen información útil para el soporte de NetApp, incluidos registros, eventos para todos los componentes de la implementación, métricas e información de topología sobre los clústeres y las aplicaciones que se están gestionando. Si está conectado a Internet, puede cargar los paquetes de soporte en el sitio de soporte de NetApp (NSS) directamente desde la interfaz de usuario de Astra Control Center.



El tiempo que tarda Astra Control Center en generar el paquete depende del tamaño de la instalación de Astra Control Center, así como de los parámetros del paquete de soporte solicitado. La duración especificada al solicitar un bundle de soporte determina el tiempo que se tarda en generar el paquete (por ejemplo, un periodo de tiempo más corto provoca una generación más rápida de los paquetes).

Antes de empezar

Determine si se necesitará una conexión proxy para cargar paquetes en NSS. Si se necesita una conexión proxy, compruebe que Astra Control Center se ha configurado para utilizar un servidor proxy.

1. Seleccione **Cuentas > conexiones**.
2. Compruebe la configuración del proxy en **Ajustes de conexión**.

Pasos

1. Cree un caso en el portal NSS utilizando el número de serie de la licencia que aparece en la página **Soporte** de la interfaz de usuario de Astra Control Center.
2. Realice los siguientes pasos para generar el paquete de soporte con la interfaz de usuario de Astra Control Center:
 - a. En la página **Soporte**, en el icono paquete de soporte, seleccione **generar**.
 - b. En la ventana **generar un paquete de soporte**, seleccione el periodo de tiempo.

Puede elegir entre períodos de tiempo rápidos o personalizados.



Puede elegir un intervalo de fechas personalizado, así como especificar un período de tiempo personalizado durante el intervalo de fechas.

- c. Después de realizar las selecciones, seleccione **Confirmar**.
- d. Active la casilla de comprobación **Upload el paquete en el sitio de soporte de NetApp cuando se genere**.
- e. Seleccione **generar paquete**.

Cuando el paquete de soporte esté listo, aparecerá una notificación en la página **Cuentas > notificación** del área Alertas, en la página **actividad** y también en la lista de notificaciones (accesible seleccionando el icono en la parte superior derecha de la interfaz de usuario).

Si la generación ha fallado, aparecerá un icono en la página generar paquete. Seleccione el icono para ver

el mensaje.



El icono de notificaciones en el lado superior derecho de la interfaz de usuario proporciona información sobre los eventos relacionados con el paquete de soporte, como cuando se crea correctamente el paquete, cuando se produce un error en la creación del paquete, cuando no se pudo cargar el paquete, cuando no se pudo descargar el paquete, etc.

Si tiene una instalación con problemas de aire

Si tiene una instalación con problemas de aire, realice los siguientes pasos después de que se genere el paquete de soporte.

Cuando el paquete está disponible para descarga, el icono Descargar aparece junto a **generar** en la sección **Paquetes de soporte** de la página **Soporte**.

Pasos

1. Seleccione el icono Descargar para descargar el paquete localmente.
2. Cargue manualmente el paquete en NSS.

Puede utilizar uno de los siguientes métodos para ello:

- Uso "[Carga de archivos autenticados de NetApp \(se requiere inicio de sesión\)](#)".
- Adjunte el paquete al caso directamente en NSS.
- Utilice Active IQ de NetApp.

Obtenga más información

- "[Cómo cargar un archivo en NetApp \(se requiere inicio de sesión\)](#)"
- "[Cómo cargar manualmente un archivo en NetApp \(se requiere inicio de sesión\)](#)"

Versiones anteriores de la documentación de Astra Control Center

Hay documentación disponible sobre versiones anteriores.

- ["Documentación de Astra Control Center 22,11"](#)
- ["Documentación de Astra Control Center 22,08"](#)
- ["Documentación de Astra Control Center 22,04"](#)
- ["Documentación de Astra Control Center 21,12"](#)
- ["Documentación de Astra Control Center 21,08"](#)

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/"](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/"](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/"](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 23.04.2"](#)
- ["Aviso para Astra Control Center 23.04.0"](#)

Licencia Astra Control API

<https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf>

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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