



## **Notas de la versión**

### **Astra Control Center**

NetApp  
August 11, 2025

# Tabla de contenidos

Notas de la versión	1
Novedades de esta versión de Astra Control Center	1
7 de noviembre de 2023 (23.10.0)	1
31 de julio de 2023 (23.07.0)	2
18 de mayo de 2023 (23.04.2)	2
25 de abril de 2023 (23.04.0)	3
22 de noviembre de 2022 (22.11.0)	3
8 de septiembre de 2022 (22.08.1)	4
10 de agosto de 2022 (22.08.0)	4
26 de abril de 2022 (22.04.0)	4
14 de diciembre de 2021 (21.12)	5
5 de agosto de 2021 (21.08)	5
Obtenga más información	5
Problemas conocidos	5
Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster	6
Se produce un error en la gestión de un clúster con Astra Control Center cuando el archivo kubeconfig contiene más de un contexto	6
Un pod de supervisión puede fallar en entornos Istio	6
Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión	7
Las operaciones de restauración sin movimiento a las clases de almacenamiento económico ontap-nas fallan	7
Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos	7
Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida	8
Obtenga más información	8
Limitaciones conocidas	8
Dos instancias de Astra Control Center no pueden gestionar el mismo clúster	9
Astra Control Center no puede gestionar dos clústeres con el mismo nombre	9
Un usuario con restricciones de RBAC de espacio de nombres puede añadir y anular la gestión de un clúster	10
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	10
No es posible restaurar varias aplicaciones en un espacio de nombres único de forma colectiva en un espacio de nombres diferente	10
Astra Control no es compatible con aplicaciones que usan varias clases de almacenamiento por espacio de nombres	10
Astra Control no asigna automáticamente bloques predeterminados para las instancias de la nube	11
Se pueden producir errores en los clones de aplicaciones instaladas con operadores de paso a referencia	11
No se admiten las operaciones de restauración in situ de las aplicaciones que utilizan un	

administrador de certificados .....	11
No se admiten aplicaciones puestas en marcha de operadores con OLM y ámbito de clúster .....	11
Las aplicaciones implementadas con Helm 2 no son compatibles .....	11
Es posible que las copias de Snapshot fallen en clústeres de Kubernetes 1,25 o posteriores con ciertas versiones de controladoras Snapshot .....	12
Es posible que no se conserven las copias de Snapshot durante la eliminación de una instancia de Astra Control Center .....	12
Limitaciones de usuarios y grupos LDAP .....	12
Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible .....	12
Astra Control Center no valida los detalles introducidos para su servidor proxy .....	12
Las conexiones existentes a un pod Postgres provocan fallos .....	12
La página Actividad muestra hasta 100000 eventos .....	12
SnapMirror no admite aplicaciones que utilizan NVMe over TCP para back-ends de almacenamiento ..	13
Obtenga más información .....	13

# Notas de la versión

Nos complace anunciar la última versión de Astra Control Center.

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

Envíe sus comentarios sobre la documentación convirtiéndose en una ["Colaborador de GitHub"](#) o enviar un correo electrónico a [doccomments@netapp.com](mailto:doccomments@netapp.com).

## Novedades de esta versión de Astra Control Center

Nos complace anunciar la última versión de Astra Control Center.

### 7 de noviembre de 2023 (23.10.0)

#### Nuevas funciones y soporte

- \* Capacidades de copia de seguridad y restauración para aplicaciones con backends de almacenamiento respaldados por controladores de economía ontap-nas\*: Permite operaciones de copia de seguridad y restauración para ontap-nas-economy con algunos ["sencillos pasos"](#).
- **Copias de seguridad inmutables:** Astra Control ahora es compatible ["backups de solo lectura que se pueden modificar"](#) como capa de seguridad adicional contra el malware y otras amenazas.
- **Presentamos Astra Control Provisionador**

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

- **Empieza con Astra Control Provisioner**

Puede hacerlo ["Habilita el aprovisionador de Astra Control"](#) Si ha instalado y configurado su entorno de modo que utilice Astra Trident 23,10.

- **La funcionalidad de Astra Control Provisionador**

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

- \* Seguridad de backend de almacenamiento mejorada con cifrado Kerberos 5\*: Puede mejorar la seguridad del almacenamiento ["habilitar cifrado"](#) para el tráfico entre el clúster gestionado y el back-end de almacenamiento. El aprovisionador de control de Astra admite el cifrado Kerberos 5 a través de conexiones NFSv4,1 GbE desde clústeres de Red Hat OpenShift a Azure NetApp Files y volúmenes ONTAP en las instalaciones
- **Recuperar datos usando una instantánea:** Astra Control Provisioner proporciona una restauración de volumen rápida y en el lugar desde una instantánea usando el `TridentActionSnapshotRestore (TASR)` CR.
- **Mejoras de SnapMirror:** Utilice la función de replicación de aplicaciones en entornos en los que Astra Control no tenga conectividad directa a un clúster de ONTAP ni acceso a credenciales de ONTAP. Esta función le permite utilizar la replicación sin tener que gestionar un back-end de

almacenamiento ni sus credenciales en Astra Control.

- \* Capacidades de copia de seguridad y restauración para aplicaciones con `ontap-nas-economy` Back-ends de almacenamiento respaldados por el conductor\*: Como se describe [anterior](#).

- **Soporte para la gestión de aplicaciones que utilizan almacenamiento NVMe/TCP**

Astra Control ahora puede gestionar aplicaciones respaldadas por volúmenes persistentes que están conectados mediante NVMe/TCP.

- \* Ganchos de ejecución desactivados por defecto\*: A partir de esta versión, la funcionalidad de los ganchos de ejecución puede ser "[activado](#)" o desactivado para seguridad adicional (está desactivado de forma predeterminada). Si todavía no has creado enlaces de ejecución para usarlos con Astra Control, debes hacerlo "[active la función de enlaces de ejecución](#)" para empezar a crear ganchos. Si ha creado enlaces de ejecución antes de esta versión, la funcionalidad de enlaces de ejecución permanece activada y puede utilizar los enlaces como lo haría normalmente.

### Problemas y limitaciones conocidos

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

## 31 de julio de 2023 (23.07.0)

### Detalles

#### Nuevas funciones y soporte

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

#### Problemas y limitaciones conocidos

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

## 18 de mayo de 2023 (23.04.2)

## Detalles

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)

### Detalles

#### 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:

- Los backups de aplicaciones y las snapshots producen errores si la clase `volumesnapshotse` añade después de gestionar un clúster
- Se produce un error en la gestión de un clúster con Astra Control Center cuando el archivo `kubeconfig` contiene más de un contexto
- Un pod de supervisión puede fallar en entornos Istio
- Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión
- Las operaciones de restauración sin movimiento a las clases de almacenamiento económico `ontap-nas` fallan
- Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos
- Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida

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

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

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

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

## 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
```

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

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

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

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

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

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



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

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

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

### Obtenga más información

- ["Limitaciones conocidas"](#)

## Limitaciones conocidas

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

### Limitaciones de gestión de clústeres

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

### Limitaciones de control de acceso basado en roles (RBAC)

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

### Limitaciones en la gestión de aplicaciones

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

### Limitaciones generales

- [Limitaciones de usuarios y grupos LDAP](#)
- [Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible](#)
- [Astra Control Center no valida los detalles introducidos para su servidor proxy](#)

- Las conexiones existentes a un pod Postgres provocan fallos
- La página Actividad muestra hasta 100000 eventos
- SnapMirror no admite aplicaciones que utilizan NVMe over TCP para back-ends de almacenamiento

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

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

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

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

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

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

Para solucionar este problema, haga lo siguiente:

1. Edite su kubeadm-config Mapa de ConfigMap:

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

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

```

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

```

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

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

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

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

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

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

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

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

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

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

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

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

- ["Apache K8ssandra"](#)



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

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

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



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

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

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

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

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

## Las aplicaciones implementadas con Helm 2 no son compatibles

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

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

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

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

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

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

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

## Limitaciones de usuarios y grupos LDAP

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

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

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

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

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

Asegúrese de que usted ["introduzca los valores correctos"](#) al establecer una conexión.

## Las conexiones existentes a un pod Postgres provocan fallos

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

## La página Actividad muestra hasta 100000 eventos

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

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

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

### **Obtenga más información**

- ["Problemas conocidos"](#)



## Información de copyright

Copyright © 2025 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.