Notas de la versión

Astra Control Center

NetApp
November 21, 2023

Tabla de contenidos

Notas de la versión . . . 1
Novedades de esta versión de Astra Control Center . . . 1
Problemas resueltos . . . 2
Problemas conocidos con la vista previa de Astra Data Store y esta versión de Astra Control Center . . . 3
Problemas conocidos . . . 5
Limitaciones conocidas . . . 11

Notas de la versión

Nos complace anunciar la versión 21.12 de Astra Control Center.

- "¿Qué hay en esta versión de Astra Control Center"
- "Problemas resueltos"
- "Problemas conocidos"
- "Problemas conocidos con la vista previa de Astra Data Store y esta versión de Astra Control Center"
- "Limitaciones conocidas"

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

Novedades de esta versión de Astra Control Center

Nos complace anunciar la última versión 21.12 de Astra Control Center.

14 de diciembre de 2021 (21.12)

Versión actualizada de Astra Control Center.

Nuevas funciones y soporte

- "Restauración de aplicaciones"
- "Ganchos de ejecución"
- "Soporte para aplicaciones implementadas con operadores con ámbito de espacio de nombres"
- "Compatibilidad adicional para upstream Kubernetes y Rancher"
- "Astra Data Store vista previa de la gestión y supervisión del entorno de administración"
- "Actualizaciones de Astra Control Center"
- "Opción Red Hat OperatorHub para la instalación"

Problemas resueltos

- "Se han resuelto problemas para esta versión"

Problemas y limitaciones conocidos

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

5 de agosto de 2021 (21.08)

Lanzamiento inicial de Astra Control Center.

- "Qué es"
- "Comprensión de la arquitectura y los componentes"
- "Qué se necesita para empezar"

- "Instale" y.. "configuración"
- "Gestione" y.. "proteger" aplicaciones
- "Gestionar bloques" y.. "back-ends de almacenamiento"
- "Gestionar cuentas"
- "Automatización con API"

Obtenga más información

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

Problemas resueltos

Estos problemas se han corregido en esta versión del producto.

Los backups adicionales se retienen como parte del backup programado

A veces, uno o varios backups de Astra Control Center se retienen más allá del número especificado para retener en el programa de copia de seguridad. Estos backups adicionales deben eliminarse como parte de un backup programado, pero no se eliminan y quedan bloqueados en un `pending` estado.

La copia de seguridad o la clonación fallan en las aplicaciones que utilizan PVC con unidades decimales en Astra Control Center

Los volúmenes creados con unidades decimales fallan con el proceso de copia de seguridad o clonación de Astra Control Center.

La interfaz de usuario de Astra Control Center se ralentiza para mostrar los cambios en los recursos de las aplicaciones, como los cambios de volúmenes persistentes

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. Este retraso en la interfaz de usuario también puede producirse cuando se agregan o modifican recursos de la aplicación. En este caso, una operación de protección de datos se realiza correctamente en minutos y se puede usar el software de gestión del back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Enlace incorrecto de la función de clúster creado por la definición de recursos personalizados de Astra Control Center durante la instalación

En esta versión, la revisión para corregir el enlace de rol de clúster durante la instalación ya no es necesario.

La recogida de ASUP se ha atascado en un estado de generación o carga

Si se detiene o se reinicia un pod de ASUP, es posible que una recogida de ASUP se atasque en un estado de generación o carga.

Aplicaciones y espacios de nombres implementados por el operador

El operador y la aplicación que ponga en marcha deben utilizar el mismo espacio de nombres. Astra Control solo admite una aplicación implementada por un operador por espacio de nombres.

Obtenga más información

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

Problemas conocidos con la vista previa de Astra Data Store y esta versión de Astra Control Center

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

Los siguientes problemas conocidos afectan a la gestión de Astra Data Store con esta versión actual de Astra Control Center:

La vista previa de Astra Data Store no se puede utilizar como clase de almacenamiento para Astra Control Center debido a un fallo en la sonda de nivel de presencia de POD de MongoDB

Cuando intenta utilizar una vista previa de Astra Data Store como el aprovisionador de clase de almacenamiento durante una puesta en marcha de Astra Control Center, la sonda de nivel livismo MongoDB falla, lo que provoca una implementación que no finalice.

Para corregir este problema, realice los siguientes cambios además de los cambios estándar de la AYM al completar la "Proceso de instalación de Astra Control Center":

1. Edite el "Astra Control Center Operator Deployment YAML (astra_control_Center_Operator_Deploy.ylma)" Para cambiar el tiempo de espera de instalación de Helm:

   ```
   - name: ACCOP_HELM_INSTALLTIMEOUT
     value: 20m
   ```

2. Edite el "Archivo de recursos personalizados (CR) del Centro de control de Astra (astra_control_Center_min.ylma)" e incluya los valores adicionales resaltados en `spec`:

```
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"
  additionalValues:
    polaris-mongodb:
      mongodb:
        livenessProbe:
          initialDelaySeconds: 400
      metrics:
        livenessProbe:
          initialDelaySeconds: 400
```

Astra Control Center muestra una vista previa del back-end de almacenamiento de Astra Data Store en `Unknown` estado

Astra Control Center muestra el fondo de almacenamiento de vista previa de Astra Data Store en una `Unknown` estado de la página backends de la interfaz de usuario. En esta condición, el back-end de almacenamiento está realmente disponible y se puede comunicar con. Es probable que un componente del back-end de almacenamiento esté en estado incorrecto y deba regresar a un estado correcto para que el back-end de almacenamiento se muestre como `available`.

Obtenga más información

- "Problemas resueltos"
- "Problemas conocidos"
- "Limitaciones conocidas"
- "Documentación de Astra Data Store"

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:

- La aplicación con etiqueta definida por el usuario pasa al estado "eliminado"
- No se puede detener la ejecución de la copia de seguridad de la aplicación
- Trident crea un VP mayor que el VP original
- Rendimiento de clonado afectado por volúmenes persistentes de gran tamaño
- 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)
- La reutilización de cubos entre instancias de Astra Control Center provoca fallos
- se producen fallos de protección de datos
- Es posible que no se conserven las copias de Snapshot durante la eliminación de una instancia de Astra Control Center
- "La operación de clonado no puede utilizar otros bloques además del valor predeterminado"
- La administración de un clúster con Astra Control Center falla cuando el archivo kubeconfig predeterminado contiene más de un contexto
- 500 error interno del servicio al intentar la gestión de datos de la aplicación Trident
- Ejecución de aplicaciones personalizadas: Se agota el tiempo de espera de las secuencias de comandos de enlace y se hace que no se ejecuten las secuencias de comandos posteriores a la instantánea
- "No se puede determinar el estado del paquete ASUP tar en un entorno a escala"
- las snapshots comienzan a fallar cuando se utiliza una copia de Snapshot externa versión 4.2.0
- Se puede producir un error en las operaciones simultáneas de restauración de aplicaciones en el mismo espacio de nombres
- La actualización genera errores si la versión de origen utiliza un registro de imagen contenedor que no requiere autenticación y la versión de destino utiliza un registro de imagen contenedor que requiere autenticación
- La desinstalación de Astra Control Center no puede limpiar el módulo de control del operador de supervisión en el clúster gestionado
- La desinstalación de Astra Control Center no limpia los CRD de Traefik

La aplicación con etiqueta definida por el usuario pasa al estado "eliminado"

Si define una aplicación con una etiqueta k8s no existente, Astra Control Center creará, gestionará y eliminará inmediatamente la aplicación. Para evitarlo, añada la etiqueta k8s a pods y recursos después de que Astra Control Center gestione la aplicación.

No se puede detener la ejecución de la copia de seguridad de la aplicación

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

de seguridad fallida, utilice "API de control Astra".

Durante la restauración de aplicaciones a partir del backup, Trident crea un VP mayor que el 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.

Rendimiento de clonado afectado por volúmenes persistentes de gran tamaño

Los clones de volúmenes grandes y consumidos pueden ser intermitentemente lentos, dependiendo del acceso del clúster al almacén de objetos. Si el clon se bloquea y no se han copiado datos durante más de 30 minutos, Astra Control finaliza la acción clonada.

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 OCP. 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.

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 reutilización de cubos entre instancias de Astra Control Center provoca fallos

Si intenta reutilizar un bloque utilizado por otra instalación o anterior de Astra Control Center, las operaciones de copia de seguridad y restauración fallarán. Debe utilizar un cucharón diferente o limpiar completamente el cucharón usado anteriormente. No se pueden compartir bloques entre instancias de Astra Control Center.

Al seleccionar un tipo de proveedor de cubos con credenciales para otro tipo, se producen fallos de protección de datos

Cuando agregue un bloque, seleccione el proveedor de segmento correcto e introduzca las credenciales adecuadas 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.

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.

La operación de clonado no puede utilizar otros bloques además del valor predeterminado

Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar un ID de bloque. Sin embargo, en una operación de clonado de aplicaciones, siempre se utiliza el bloque predeterminado que se ha definido. No existe ninguna opción para cambiar bloques para un clon. Si desea controlar qué segmento se utiliza, puede hacer lo mismo "cambiar el valor predeterminado del segmento" o haga un "Backup" seguido de un "restaurar" por separado.

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.

500 error interno del servicio al intentar la gestión de datos de la aplicación Trident

Si Trident on un clúster de aplicaciones se desconecta (y vuelve a estar en línea) y se producen 500 errores internos de servicio al intentar gestionar datos de la aplicación, reinicie todos los nodos de Kubernetes del clúster de aplicaciones para restaurar la funcionalidad.

Ejecución de aplicaciones personalizadas: Se agota el tiempo de espera de las secuencias de comandos de enlace y se hace que no se ejecuten las secuencias de comandos posteriores a la instantánea

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.

Debido a que los enlaces de ejecución a menudo reducen o desactivan por completo la funcionalidad de la aplicación con la que se ejecutan, siempre debe intentar minimizar el tiempo que tardan los enlaces de ejecución personalizados.

No se puede determinar el estado del paquete ASUP tar en un entorno a escala

Durante la recogida de ASUP, el estado del paquete en la interfaz de usuario se informa como o. `collecting` o. `done`. La recopilación puede tardar hasta una hora en entornos grandes. Durante la descarga de ASUP, es posible que la velocidad de transferencia del archivo de red del paquete sea insuficiente y es posible que el tiempo de espera de la descarga se agote después de 15 minutos sin indicación en la interfaz de usuario. Los problemas de descarga dependen del tamaño de ASUP, el tamaño del clúster escalado y si el tiempo de recogida supera el límite de siete días.

Al final, las snapshots comienzan a fallar cuando se utiliza una copia de Snapshot externa versión 4.2.0

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

Se puede producir un error en las operaciones simultáneas de restauración de aplicaciones en el mismo espacio de nombres

Si intenta restaurar una o varias aplicaciones gestionadas individualmente dentro de un espacio de nombres simultáneamente, las operaciones de restauración pueden fallar luego de un largo periodo de tiempo. Como solución alternativa, restaure cada aplicación de una en una.

La actualización genera errores si la versión de origen utiliza un registro de imagen contenedor que no requiere autenticación y la versión de destino utiliza un registro de imagen contenedor que requiere autenticación

Si actualiza un sistema Astra Control Center que utiliza un registro que no requiere autenticación a una versión más reciente que utilice un registro que requiere autenticación, la actualización falla. Para solucionar esta solución, siga estos pasos:

1. Inicie sesión en un host que tenga acceso de red al clúster de Astra Control Center.
2. Asegúrese de que el host tenga la siguiente configuración:
   - `kubectl` se instala la versión 1.19 o posterior
   - La variable de entorno KUBECONFIG se establece en el archivo kubeconfig para el clúster Astra Control Center
3. Ejecute el siguiente script:

```
namespace="<netapp-acc>"
statefulsets=("polaris-vault" "polaris-mongodb" "influxdb2" "nats"
"loki")
for ss in ${statefulsets[@]}; do
    existing=$(kubectl get -n ${namespace} statefulsets.apps ${ss} -o
jsonpath='{.spec.template.spec.imagePullSecrets}')
    if [ "${existing}" = "[{}]" ] || [ "${existing}" = "[{},{},{}]" ];
then
        kubectl patch -n ${namespace} statefulsets.apps ${ss} --type
merge --patch '{"spec": {"template": {"spec": {"imagePullSecrets":
[]}}}}'
    else
        echo "${ss} not patched"
    fi
done
```

   Debería ver una salida similar a la siguiente:

```
statefulset.apps/polaris-vault patched
statefulset.apps/polaris-mongodb patched
statefulset.apps/influxdb2 patched
statefulset.apps/nats patched
statefulset.apps/loki patched
```

4. Continúe con la actualización mediante el "Instrucciones de actualización de Astra Control Center".

La desinstalación de Astra Control Center no puede limpiar el módulo de control del operador de supervisión en el clúster gestionado

Si no ha desgestionar los clústeres antes de desinstalar Astra Control Center, puede eliminar manualmente los POD del espacio de nombres para la supervisión de netapp y el espacio de nombres con los siguientes comandos:

Pasos

1. Eliminar `acc-monitoring` agente:

   ```
   oc delete agents acc-monitoring -n netapp-monitoring
   ```

   Resultado:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Elimine el espacio de nombres:

   ```
   oc delete ns netapp-monitoring
   ```

   Resultado:

   ```
   namespace "netapp-monitoring" deleted
   ```

3. Confirme los recursos eliminados:

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

   Resultado:

   ```
   No resources found in netapp-monitoring namespace.
   ```

4. Confirme que se ha eliminado el agente de supervisión:

```
oc 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):

```
oc 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 resueltos"
- "Problemas conocidos con la revisión de Astra Data Store y esta versión de Astra Control Center"
- "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.

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 idéntico en la misma nube

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

Para solucionar este problema, haga lo siguiente:

1. Edite su Config Map de kubeadm-config:

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

2. Cambie el `clusterName` valor de campo desde `kubernetes` (El nombre predeterminado de Kubernetes) a un nombre personalizado único.
3. Editar imagen de kubeconfig (`.kube/config`).

4. Actualice el nombre del clúster desde `kubernetes` a un nombre personalizado único (`xyz-cluster` se utiliza en los siguientes ejemplos). Realice la actualización en ambos `clusters` y.. `contexts` secciones como se muestra en este ejemplo:

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

Se puede producir un error en los clones de aplicaciones instaladas con operadores de referencia de paso

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"
- "Jenkins CI"
- "Clúster Percona XtraDB"

Tenga en cuenta que Astra Control podría no ser capaz de clonar a un operador diseñado con una arquitectura de "paso 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.

El clúster está en `removed` estado aunque el clúster y la red funcionan de otro modo como se esperaba

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":

1. Ejecute una llamada POSTERIOR para agregar un archivo kubeconfig actualizado al `/credentials` endpoint y recupere el asignado `id` del cuerpo de respuesta.

2. Ejecute una llamada PUT desde el `/clusters` Extremo que utiliza el ID de clúster adecuado y establece el `credentialID` para la `id` valor del paso anterior.

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

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

El Centro de control de Astra no admite aplicaciones que se implementen con operadores habilitados para Operator Lifecycle Manager (OLM) o operadores con ámbito de clúster.

Las aplicaciones de clonado solo se pueden realizar con la misma distribución K8s

Si clona una aplicación entre clústeres, los clústeres de origen y destino deben ser la misma distribución de Kubernetes. Por ejemplo, si clona una aplicación de un clúster de OpenShift 4.7, utilice un clúster de destino que también sea OpenShift 4.7.

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.

No se admite metalLB 0.11.0

MetalLB 0.11.0 no es un equilibrador de carga admitido para Astra Control Center. Para obtener más información sobre balanceadores de carga admitidos, consulte "Requisitos del Centro de Control de Astra".

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".

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

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

La protección de datos para Astra Control Center ya que la aplicación no está disponible todavía

Esta versión no permite gestionar Astra como aplicación mediante las opciones de Snapshot, backup o restauración.

Los POD que no son saludables afectan a la gestión de aplicaciones

Si una aplicación gestionada tiene pods en estado incorrecto, Astra Control no puede crear nuevos backups y clones.

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.

Trident no se desinstala de un clúster

Cuando desvincula un clúster de Astra Control Center, Trident no se desinstala automáticamente del clúster. Para desinstalar Trident, tendrá que hacerlo "Siga estos pasos en la documentación de Trident".

Obtenga más información

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