Notas de la versión

Astra Control Center

NetApp
November 21, 2023

This PDF was generated from https://docs.netapp.com/es-es/astra-control-center-2204/release-notes/whats-new.html on November 21, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

Notas de la versión 1
Novedades de esta versión de Astra Control Center 1
Problemas conocidos 2
Limitaciones conocidas 4

Notas de la versión

Nos complace anunciar la versión 22.04.0 de Astra Control Center.

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

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

Novedades de esta versión de Astra Control Center

Nos complace anunciar la última versión 22.04.0 de Astra Control Center.

26 de abril de 2022 (22.04.0)

Nuevas funciones y soporte

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

Problemas y limitaciones conocidos

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

14 de diciembre de 2021 (21.12)

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 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

De clúster

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

Otros temas

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

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

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

Los clones de aplicaciones producen un error al utilizar una versión específica de PostgreSQL

Los clones de aplicaciones dentro del mismo clúster fallan constantemente con el gráfico BitNami PostgreSQL 11.5.0. Para clonar correctamente, utilice una versión anterior o posterior del gráfico.

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

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

Se produce un error en los clones de aplicaciones después de poner en marcha una aplicación con una clase de almacenamiento establecida

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

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

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

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

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

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

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

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

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

Obtenga más información

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

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

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

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

Obtenga más información

- "Problemas conocidos"
- "Limitaciones conocidas"

Limitaciones conocidas

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

Limitaciones de gestión de clústeres

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

Limitaciones de control de acceso basado en roles (RBAC)

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

Limitaciones en la gestión de aplicaciones

- No se pueden detener las copias de seguridad de aplicaciones en curso
- Se pueden producir errores en los clones de aplicaciones instaladas con operadores de paso a referencia
- No se admiten las operaciones de restauración in situ de las aplicaciones que utilizan un administrador de certificados
- No se admiten aplicaciones puestas en marcha de operadores con OLM y ámbito de clúster
- Las aplicaciones implementadas con Helm 2 no son compatibles

Limitaciones generales

- Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible
- Astra Control Center no valida los detalles introducidos para su servidor proxy
- Las conexiones existentes a un pod Postgres provocan fallos
- Es posible que no se conserven las copias de Snapshot durante la eliminación de una instancia de Astra Control Center

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

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

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

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

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

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

Para solucionar este problema, haga lo siguiente:

1. Edite su Config Map de kubeadm-config:

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

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

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

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

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

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

Cualquiera `member` Los usuarios con limitaciones de RBAC por nombre/ID de espacio de nombres o por las etiquetas de espacio de nombres pueden clonar o restaurar una aplicación en un nuevo espacio de nombres 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 se pueden detener las copias de seguridad de aplicaciones en curso

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".

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"

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.

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

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

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

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

Las aplicaciones implementadas con Helm 2 no son compatibles

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

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

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

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

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

Las conexiones existentes a un pod Postgres provocan fallos

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

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

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

Obtenga más información

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

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.