Notas de la versión

Astra Control Center

NetApp
November 20, 2023

Tabla de contenidos

Notas de la versión

Nos complace anunciar el lanzamiento inicial de Astra Control Center.

- "¿Qué hay en esta versión de Astra Control Center"
- "Problemas conocidos"
- "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.

¿Qué hay en esta versión de Astra Control Center

Nos complace anunciar el lanzamiento de Astra Control Center.

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"

Problemas conocidos con esta versión

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:

- ClusterRoleBinding incorrecto creado por Astra Control Center CRD durante la instalación
- 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
- La copia de seguridad o la clonación fallan en las aplicaciones que utilizan PVC con unidades decimales en Astra Control Center

- como los cambios de volúmenes persistentes
- 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)
- Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible
- 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
- Los backups adicionales se retienen como parte del backup programado
- "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
- "No se puede determinar el estado del paquete ASUP tar en un entorno a escala"
- 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 recogida de ASUP se ha atascado en un estado de generación o carga

ClusterRoleBinding incorrecto creado por Astra Control Center CRD durante la instalación

Aplique el siguiente parche a todos los clústeres de Kubernetes en los que se haya implementado la versión 21.08.65 del operador ACC. También debe aplicarse si el operador ACC se vuelve a desplegar.

Para resolver este problema:

1. Sustituya `ACC_NAMESPACE` en la secuencia de comandos siguiente con el espacio de nombres al que se utilizó "Ponga en marcha Astra Control Center".

```
cat <<EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: acc-operator-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: acc-operator-manager-role
subjects:
- kind: ServiceAccount
  name: default
  namespace: netapp-acc-operator
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts:ACC_NAMESPACE
EOF
```

2. Ejecute el script.

El parche elimina los dos temas siguientes `ClusterRoleBinding: "acc-operator-manager-rolebinding"`

```
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
- apiGroup: ""
  kind: Group
  name: system:serviceaccounts
```

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 Astra".

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. Consulte "artículo de base de conocimientos" si quiere más información.

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.

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 coincide 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.

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.

La reutilización de cubos entre instancias de Astra Control Center provoca fallos

Si intenta reutilizar un cucharón utilizado por otra instalación o anterior de Astra Control Center, la copia de seguridad y la 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 cubo, seleccione el tipo de proveedor de cucharón correcto con las credenciales que sean correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como el tipo con credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los backups y las restauraciones futuras de aplicaciones que utilizan este bloque.

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.

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. Para resolver el problema: "forzar eliminación" los backups adicionales.

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.

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.

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:

Pasos

1. Confirme qué CRD no se han eliminado mediante el proceso de desinstalación:

   ```
   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
   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
   ```

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

Si se mata o reinicia un pod de ASUP, es posible que una recogida de ASUP se atasque en un estado de generación o carga. Realice lo siguiente "API REST de Astra Control" llamar para iniciar de nuevo la recopilación manual:

Método HTTP	Ruta
PUBLICAR	/Accounts/{accountID}/core/v1/asups

Esta solución de API solo funciona si se realiza más de 10 minutos después del inicio de ASUP.

Obtenga más información

- "Limitaciones conocidas de esta versión"

Limitaciones conocidas de esta versión

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.

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.

OpenShift 4.8 no es compatible

OpenShift 4.8 no es compatible con la versión de julio de Astra Control Center. Para obtener más información, 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. Se admite por completo la gestión y clonación de las 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 conocidos de esta versión"