



Gestione Astra Trident

Astra Trident

NetApp
September 04, 2024

Tabla de contenidos

- Gestione Astra Trident 1
- Actualice Astra Trident 1
- Desinstale Astra Trident 14
- Degradar Astra Trident 16

Gestione Astra Trident

Actualice Astra Trident

Actualice Astra Trident

Astra Trident sigue una cadencia de lanzamientos trimestrales y ofrece cuatro lanzamientos principales cada año. Cada versión nueva se basa en las versiones anteriores, y ofrece nuevas funciones y mejoras de rendimiento, así como correcciones de errores y mejoras. Le animamos a que realice una actualización al menos una vez al año para aprovechar las nuevas funciones de Astra Trident.

Consideraciones antes de la actualización

Cuando actualice a la versión más reciente de Astra Trident, tenga en cuenta lo siguiente:

- Solo debe haber una instancia de Astra Trident instalada en todos los espacios de nombres en un clúster de Kubernetes determinado.
- A partir de Trident 20.01, solo la versión en beta de ["copias de snapshot de volumen"](#) compatible. Los administradores de Kubernetes deben tener cuidado de realizar un backup o convertir de forma segura los objetos Snapshot alfa en beta para conservar las snapshots alfa heredadas.
 - Las instantáneas de volumen CSI son ahora una función de GA que comienza con Kubernetes 1.20. Antes de actualizar, debe eliminar los CRD de instantánea alfa utilizando `tridentctl obliviate alpha-snapshot-crd` Para eliminar los CRD de la especificación de instantánea alfa.
 - La versión beta de instantáneas de volumen introduce un conjunto modificado de CRD y un controlador de instantáneas, que deben configurarse antes de actualizar Astra Trident.
 - Para obtener más información, consulte ["Qué necesita saber antes de actualizar su clúster de Kubernetes"](#).
- Todas las actualizaciones de las versiones 19.04 y anteriores requieren la migración de metadatos de Astra Trident desde él mismo `etcd` Para crear objetos. Asegúrese de comprobar el ["Documentación específica para la versión de Astra Trident"](#) para entender cómo funciona la actualización.
- Al actualizar, es importante que proporcione `parameter.fsType` `pulg` `StorageClasses` Utilizado por Astra Trident. Puede eliminar y volver a crear `StorageClasses` sin interrumpir los volúmenes preexistentes.
 - Este es un **requisito** para hacer cumplir ["contextos de seguridad"](#) Para volúmenes SAN.
 - El directorio [sample input](#) contiene ejemplos, como `storage-class-basic.yaml` `templ` y `storage-class-bronze-default.yaml` `#`. Para obtener más información, consulte ["Problemas conocidos"](#).

Paso 1: Seleccione una versión

Las versiones de Astra Trident siguen una fecha basada `YY.MM` Convención de nomenclatura, donde "YY" es los dos últimos dígitos del año y "MM" es el mes. Las versiones de puntos siguen a `YY.MM.X` convención, donde "X" es el nivel de parche. Deberá seleccionar la versión a la que se actualizará en función de la versión desde la que se actualice.

- Puede realizar una actualización directa a cualquier versión de destino que esté dentro de una ventana de

cuatro versiones de la versión instalada. Por ejemplo, puede actualizar a 23,04 desde 22,04 (incluidas las versiones de puntos, como 22.04.1) directamente.

- Si dispone de una versión anterior, debe realizar una actualización en varios pasos con la documentación de la versión correspondiente para obtener instrucciones específicas. Esto requiere que primero actualice a la versión más reciente que se ajuste a su ventana de cuatro lanzamientos. Por ejemplo, si ejecuta 18.07 y desea actualizar a la versión 20.07, siga el proceso de actualización de varios pasos como se indica a continuación:
 - a. Primera actualización de 18.07 a 19.07.
 - b. A continuación, actualice de 19.07 a 20.07.



Cuando se actualice con el operador Trident en OpenShift Container Platform, debe actualizar a Trident 21.01.1 o una versión posterior. El operador Trident publicado con 21.01.0 contiene un problema conocido que se ha solucionado en 21.01.1. Si quiere más detalles, consulte "[Detalles del problema en GitHub](#)".

Paso 2: Determine el método de instalación original

Por lo general, debe actualizar utilizando el mismo método que utilizó para la instalación inicial, sin embargo, puede hacerlo "[desplazarse entre los métodos de instalación](#)".

Para determinar qué versión solías instalar originalmente Astra Trident:

1. Uso `kubectl get pods - trident` para examinar los pods.
 - Si no existe ningún pod de operador, Astra Trident se instaló mediante `tridentctl`.
 - Si hay un pod de operador, se instaló Astra Trident mediante el operador Trident manualmente o mediante Helm.
2. Si hay un pod del operador, utilice `kubectl describe tproc trident` Para determinar si Astra Trident se instaló mediante Helm.
 - Si hay una etiqueta Helm, Astra Trident se instaló usando Helm.
 - Si no hay ninguna etiqueta Helm, Astra Trident se instaló manualmente mediante el operador Trident.

Paso 3: Seleccione un método de actualización

Existen dos métodos para actualizar Astra Trident.

Cuándo actualizar con el operador

Puede hacerlo "[Actualice con el operador Trident](#)" si:

- Originalmente instaló Astra Trident con el operador o con el uso `tridentctl`.
- Desinstaló CSI Trident y los metadatos de la instalación persisten.
- Tiene una instalación de Astra Trident basada en CSI. Todas las versiones de 19.07 en adelante se basan en CSI. Puede examinar los pods en el espacio de nombres de Trident para verificar su versión.
 - Nombres de POD en versiones anteriores a 23,01 Usos: `trident-csi-*`
 - La nomenclatura de POD en 23.01 y versiones posteriores utiliza:
 - `trident-controller-<generated id>` para el pod del controlador
 - `trident-node-<operating system>-<generated id>` para los pods de nodo

- `trident-operator-<generated id>` para el pod del operador



Si utiliza una, no utilice el operador para actualizar Trident `etcd` Versión de Trident basada en (19.04 o anterior).

Cuándo actualizar mediante `tridentctl`

Puede hacerlo Si originalmente instaló Astra Trident usando ``tridentctl``.

`tridentctl` Es el método convencional de instalación de Astra Trident y proporciona la mayor cantidad de opciones para aquellos que requieren complejas personalizaciones. Para obtener información detallada, consulte "[Elija el método de instalación](#)".

Cambios en el operador

La versión 21,01 de Astra Trident introdujo cambios de arquitectura para el operador:

- El operador ahora está **ámbito de clúster**. Las instancias anteriores del operador Trident (versiones 20.04 a 20.10) eran **espacio de nombres**. Un operador con ámbito de clúster puede ser ventajoso por los siguientes motivos:
 - Responsabilidad de recursos: Ahora el operador gestiona los recursos asociados con una instalación de Astra Trident a nivel de clúster. Como parte de la instalación de Astra Trident, el operador crea y mantiene varios recursos mediante el uso `ownerReferences`. Mantenimiento `ownerReferences` En los recursos de ámbito de clúster pueden generar errores en determinados distribuidores de Kubernetes como OpenShift. Esto se mitiga con un operador con ámbito de clúster. Para la reparación automática y parches de recursos de Trident, este es un requisito esencial.
 - Limpieza durante la desinstalación: Una eliminación completa de Astra Trident requeriría que se eliminen todos los recursos asociados. Un operador con ámbito de espacio de nombres puede experimentar problemas con la eliminación de recursos con ámbito de clúster (como `clusterRole`, `ClusterRoleBinding` y `PodSecurityPolicy`) y dar lugar a una limpieza incompleta. Un operador con ámbito de clúster elimina este problema. Los usuarios pueden desinstalar por completo Astra Trident e instalar de nuevo si es necesario.
- `TridentProvisioner` se sustituye ahora por `TridentOrchestrator` Como recurso personalizado utilizado para instalar y gestionar Astra Trident. Además, se introduce un nuevo campo en el `TridentOrchestrator` `spec`. Los usuarios pueden especificar que el espacio de nombres Trident debe instalarse o actualizarse desde mediante el `spec.namespace` campo. Puede echar un vistazo a un ejemplo "[aquí](#)".

Actualizar con el operador

Puede actualizar fácilmente una instalación existente de Astra Trident con el operador, ya sea manualmente o mediante Helm.

Actualice con el operador Trident

Normalmente, debe actualizar Astra Trident mediante el mismo método que se utilizaba para instalarlo originalmente. Revisar "[Seleccione un método de actualización](#)" Antes de intentar actualizar con el operador Trident.

Al actualizar desde una instancia de Astra Trident instalada con el operador que cuenta con el ámbito de espacio de nombres (de las versiones 20,07 a la 20,10), el operador Trident realiza automáticamente lo siguiente:



- Migra `tridentProvisioner` a `tridentOrchestrator` objeto con el mismo nombre,
- Eliminaciones `TridentProvisioner` los objetos y la `tridentprovisioner` CRD
- Actualiza Astra Trident a la versión del operador en el ámbito del clúster que se usa
- Instale Astra Trident en el mismo espacio de nombres donde estaba instalado originalmente

Actualice una instalación de operador de Trident de ámbito de clúster

Puede actualizar una instalación del operador Trident en el ámbito del clúster. Todas las versiones 21.01 y posteriores de Astra Trident utilizan un operador con ámbito de clúster.

Antes de empezar

Asegúrese de que está utilizando un clúster de Kubernetes en ejecución "[Una versión de Kubernetes compatible](#)".

Pasos

1. Compruebe su versión de Astra Trident:

```
./tridentctl -n trident version
```

2. Elimine el operador Trident que se ha utilizado para instalar la instancia actual de Astra Trident. Por ejemplo, si va a actualizar desde 22,01, ejecute el siguiente comando:

```
kubectl delete -f 22.01/trident-installer/deploy/bundle.yaml -n trident
```

3. Si ha personalizado la instalación inicial mediante `TridentOrchestrator` atributos, puede editar `TridentOrchestrator` objeto para modificar los parámetros de instalación. Esto podría incluir cambios realizados para especificar registros de imágenes de Trident y CSI reflejados para el modo sin conexión, habilitar registros de depuración o especificar secretos de extracción de imágenes.
4. Instale Astra Trident con el archivo YAML de paquete correcto para su entorno y la versión Astra Trident. Por ejemplo, si va a instalar Astra Trident 23,04 para Kubernetes 1,27, ejecute el siguiente comando:

```
kubectl create -f 23.04.0/trident-installer/deploy/bundle_post_1_25.yaml -n trident
```

Trident proporciona un archivo de paquete que se puede usar para instalar el operador y crear objetos asociados para la versión de Kubernetes.



- Para los clústeres que ejecutan Kubernetes 1,24 o una versión anterior, utilice "[bundle_pre_1_25.yaml](#)".
- Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice "[bundle_post_1_25.yaml](#)".

Resultados

El operador de Trident identifica una instalación existente de Astra Trident y la actualiza a la misma versión que el operador.

Actualice la instalación de un operador de ámbito de espacio de nombres

Puede actualizar desde una instancia de Astra Trident instalada mediante el operador con ámbito de espacio de nombres (versiones 20,07 a 20,10) a una instalación de operadores en el ámbito del clúster.

Antes de empezar

Necesita el archivo YAML del paquete utilizado para desplegar el operador de ámbito de espacio de nombres desde <https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/BUNDLE.YAML> donde *vXX.XX* es el número de versión y *BUNDLE.YAML* Es el nombre del archivo YAML del grupo.

Pasos

1. Compruebe el `TridentProvisioner` El estado de la instalación existente de Trident es `Installed`.

```
kubectl describe tprov trident -n trident | grep Message: -A 3

Message:  Trident installed
Status:   Installed
Version:  v20.10.1
```



Si el estado muestra `Updating`, asegúrese de resolverlo antes de continuar. Para obtener una lista de los posibles valores de estado, consulte ["aquí"](#).

2. Cree el `TridentOrchestrator` CRD mediante el manifiesto proporcionado con el instalador de Trident.

```
# Download the release required [23.04.0]
mkdir 23.04.0
cd 23.04.0
wget
https://github.com/NetApp/trident/releases/download/v23.04.0/trident-
installer-23.04.0.tar.gz
tar -xf trident-installer-23.04.0.tar.gz
cd trident-installer
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. Elimine el operador de ámbito del espacio de nombres mediante su manifiesto.
 - a. Asegúrese de que está en el directorio correcto.

```
pwd
/root/20.10.1/trident-installer
```

b. Suprime el operador de ámbito de espacio de nombres.

```
kubectl delete -f deploy/<BUNDLE.YAML> -n trident

serviceaccount "trident-operator" deleted
clusterrole.rbac.authorization.k8s.io "trident-operator" deleted
clusterrolebinding.rbac.authorization.k8s.io "trident-operator"
deleted
deployment.apps "trident-operator" deleted
podsecuritypolicy.policy "tridentoperatorpods" deleted
```

c. Confirme que se ha eliminado el operador Trident.

```
kubectl get all -n trident
```

NAME	READY	STATUS	RESTARTS	AGE
pod/trident-csi-68d979fb85-dsrmn	6/6	Running	12	99d
pod/trident-csi-8jfhf	2/2	Running	6	105d
pod/trident-csi-jtnjz	2/2	Running	6	105d
pod/trident-csi-lcxvh	2/2	Running	8	105d

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP
service/trident-csi	ClusterIP	10.108.174.125	<none>
34571/TCP,9220/TCP	105d		

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AGE
daemonset.apps/trident-csi	3	3	3	3	105d
3					kubernetes.io/arch=amd64,kubernetes.io/os=linux

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/trident-csi	1/1	1	1	105d

NAME	DESIRED	CURRENT	READY
replicaset.apps/trident-csi-68d979fb85	1	1	1
105d			

4. (Opcional) Si es necesario modificar los parámetros de instalación, actualice `TridentProvisioner` espec. Esto puede incluir cambios como cambiar: Los valores de `tridentImage`, `autosupportImage`, repositorio privado de imágenes y provisión (`imagePullSecrets`) después de eliminar el operador de ámbito de espacio de nombres y antes de instalar el operador de ámbito de clúster. Para obtener una lista completa de los parámetros que se pueden actualizar, consulte la ["opciones de configuración"](#).


```
kubectl patch tprov <trident-provisioner-name> -n <trident-namespace>
--type=merge -p '{"spec":{"debug":true}}'
```

5. Instale el operador del ámbito del clúster Trident.

a. Asegúrese de que está en el directorio correcto.

```
pwd
/root/23.04.0/trident-installer
```

b. Instale el operador de ámbito de cluster en el mismo espacio de nombres.

Trident proporciona un archivo de paquete que se puede usar para instalar el operador y crear objetos asociados para la versión de Kubernetes.



- Para los clústeres que ejecutan Kubernetes 1,24 o una versión anterior, utilice ["bundle_pre_1_25.yaml"](#).
- Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice ["bundle_post_1_25.yaml"](#).

```
kubectl create -f deploy/<BUNDLE.YAML>

serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#All tridentProvisioners will be removed, including the CRD itself
kubectl get tprov -n trident
Error from server (NotFound): Unable to list "trident.netapp.io/v1,
Resource=tridentprovisioners": the server could not find the
requested resource (get tridentprovisioners.trident.netapp.io)

#tridentProvisioners are replaced by tridentOrchestrator
kubectl get torc
NAME          AGE
trident      13s
```

c. Examine los pods de Trident en el espacio de nombres. La `trident-controller` y los nombres de pod reflejan la convención de nomenclatura introducida en 23.01.

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

NAME	READY	STATUS	RESTARTS
AGE			
trident-controller-79df798bdc-m79dc	6/6	Running	0
1m41s			
trident-node-linux-xrst8	2/2	Running	0
1m41s			
trident-operator-5574dbbc68-nthjv	1/1	Running	0
1m52s			

d. Confirme que Trident se ha actualizado a la versión prevista.

```
kubectl describe torc trident | grep Message -A 3
Message:          Trident installed
Namespace:        trident
Status:           Installed
Version:          v23.04.0
```

Actualice la instalación de un operador basado en Helm

Realice los pasos siguientes para actualizar la instalación de un operador basado en Helm.



Cuando actualice un clúster de Kubernetes de 1.24 a 1.25 o posterior que tenga instalado Astra Trident, debe actualizar Values.yaml para establecer `excludePodSecurityPolicy` para `true` o agregar `--set excludePodSecurityPolicy=true` para la `helm upgrade` comando antes de poder actualizar el clúster.

Pasos

1. Descargue la última versión de Astra Trident.
2. Utilice la `helm upgrade` comando donde `trident-operator-23.04.0.tgz` refleja la versión a la que desea actualizar.

```
helm upgrade <name> trident-operator-23.04.0.tgz
```

Si establece cualquier opción no predeterminada durante la instalación inicial (como especificar registros privados reflejados para imágenes Trident y CSI), utilice `--set` para asegurarse de que estas opciones están incluidas en el comando `upgrade`, de lo contrario, los valores se restablecerán a los valores predeterminados.



Por ejemplo, para cambiar el valor predeterminado de `tridentDebug`, ejecute el siguiente comando:

```
helm upgrade <name> trident-operator-23.04.0-custom.tgz --set
tridentDebug=true
```

3. Ejecución `helm list` para comprobar que la versión de la gráfica y de la aplicación se han actualizado. Ejecución `tridentctl logs` para revisar cualquier mensaje de depuración.

Resultados

El operador de Trident identifica una instalación existente de Astra Trident y la actualiza a la misma versión que el operador.

Actualizar desde una instalación que no sea del operador

Puede actualizarlo a la versión más reciente del operador de Trident desde un `tridentctl` instalación.

Pasos

1. Descargue la última versión de Astra Trident.

```
# Download the release required [23.04.0]
mkdir 23.04.0
cd 23.04.0
wget
https://github.com/NetApp/trident/releases/download/v22.01.1/trident-
installer-23.04.0.tar.gz
tar -xf trident-installer-23.04.0.tar.gz
cd trident-installer
```

2. Cree el `tridentorchestrator` CRD del manifiesto.

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. Despliegue el operador de ámbito de cluster en el mismo espacio de nombres.

```
kubectl create -f deploy/<BUNDLE.YAML>

serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#Examine the pods in the Trident namespace
```

NAME	READY	STATUS	RESTARTS	AGE
trident-controller-79df798bdc-m79dc	6/6	Running	0	150d
trident-node-linux-xrst8	2/2	Running	0	150d
trident-operator-5574dbbc68-nthjv	1/1	Running	0	1m30s

4. Cree un TridentOrchestrator CR para instalar Astra Trident.

```
cat deploy/crds/tridentorchestrator_cr.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident

kubectl create -f deploy/crds/tridentorchestrator_cr.yaml

#Examine the pods in the Trident namespace
```

NAME	READY	STATUS	RESTARTS	AGE
trident-csi-79df798bdc-m79dc	6/6	Running	0	1m
trident-csi-xrst8	2/2	Running	0	1m
trident-operator-5574dbbc68-nthjv	1/1	Running	0	5m41s

5. Confirmar que Trident se ha actualizado a la versión prevista.

```
kubectl describe torc trident | grep Message -A 3

Message:          Trident installed
Namespace:        trident
Status:           Installed
Version:          v23.04.0
```

Resultados

Los back-ends y las CVP existentes están disponibles automáticamente.

Actualice con `tridentctl`

Puede actualizar fácilmente una instalación de Astra Trident existente mediante `tridentctl`.

Actualiza Astra Trident con `tridentctl`

La desinstalación y reinstalación de Astra Trident actúa como una actualización. Cuando desinstala Trident, la reclamación de volumen persistente (PVC) y el volumen persistente (PV) que utiliza la puesta en marcha de Astra Trident no se eliminan. Las RVP que ya se han aprovisionado seguirán disponibles mientras Astra Trident está offline y Astra Trident aprovisiona volúmenes para cualquier RVP que se crean interanualmente una vez que vuelve a estar online.

Antes de empezar

Revisar "[Seleccione un método de actualización](#)" antes de actualizar mediante `tridentctl`.

Pasos

1. Ejecute el comando `uninstall` en `tridentctl` Para quitar todos los recursos asociados con Astra Trident, excepto los CRD y los objetos relacionados.

```
./tridentctl uninstall -n <namespace>
```

2. Vuelva a instalar Astra Trident. Consulte "[Instalar Astra Trident mediante tridentctl](#)".



No interrumpa el proceso de actualización. Asegúrese de que el instalador se ejecuta hasta su finalización.

Actualizar volúmenes mediante `tridentctl`

Después de la actualización, puede utilizar el completo conjunto de funciones que están disponibles en las versiones más recientes de Trident (como, las Snapshots de volumen bajo demanda), puede actualizar los volúmenes con el `tridentctl upgrade` comando.

Si hay volúmenes heredados, debe actualizar desde un tipo NFS o iSCSI al tipo CSI para utilizar el conjunto completo de funciones nuevas en Astra Trident. Un VP heredado que ha sido aprovisionado por Trident admite el conjunto tradicional de funciones.

Antes de empezar

Tenga en cuenta lo siguiente antes de decidir actualizar los volúmenes al tipo CSI:

- Es posible que no sea necesario actualizar todos los volúmenes. Los volúmenes creados previamente seguirán siendo accesibles y funcionarán normalmente.
- Un PV se puede montar como parte de un despliegue/Statilusionados al actualizar. No es necesario que los ilusionados traigan el despliegue/StatSet.
- **No puede** conectar un PV a un pod independiente al realizar la actualización. Debe apagar el pod antes de actualizar el volumen.
- Solo puede actualizar un volumen vinculado a una RVP. Los volúmenes que no están enlazados a PVC

deben eliminarse e importarse antes de actualizar.

Pasos

1. Ejecución `kubectl get pv` Para enumerar los VP.

```
kubectl get pv
NAME                                CAPACITY   ACCESS MODES   RECLAIM POLICY
STATUS   CLAIM                STORAGECLASS   REASON   AGE
default-pvc-1-a8475                 1073741824   RWO                               Delete
Bound   default/pvc-1        standard                               19h
default-pvc-2-a8486                 1073741824   RWO                               Delete
Bound   default/pvc-2        standard                               19h
default-pvc-3-a849e                 1073741824   RWO                               Delete
Bound   default/pvc-3        standard                               19h
default-pvc-4-a84de                 1073741824   RWO                               Delete
Bound   default/pvc-4        standard                               19h
trident                              2Gi         RWO                               Retain
Bound   trident/trident      standard                               19h
```

Actualmente hay cuatro VP creados por Trident 20.07 con la `netapp.io/trident` aprovisionador.

2. Ejecución `kubectl describe pv` Para obtener los detalles del PV.

```
kubectl describe pv default-pvc-2-a8486

Name:          default-pvc-2-a8486
Labels:        <none>
Annotations:   pv.kubernetes.io/provisioned-by: netapp.io/trident
               volume.beta.kubernetes.io/storage-class: standard
Finalizers:    [kubernetes.io/pv-protection]
StorageClass:  standard
Status:        Bound
Claim:         default/pvc-2
Reclaim Policy: Delete
Access Modes:  RWO
VolumeMode:    Filesystem
Capacity:      1073741824
Node Affinity: <none>
Message:
Source:
  Type:        NFS (an NFS mount that lasts the lifetime of a pod)
  Server:      10.xx.xx.xx
  Path:        /trid_1907_alpha_default_pvc_2_a8486
  ReadOnly:    false
```

El VP se creó mediante la `netapp.io/trident` provisioner y es del tipo NFS. Para admitir todas las nuevas funciones proporcionadas por Astra Trident, este PV debe actualizarse al tipo CSI.

3. Ejecute el `tridentctl upgrade volume <name-of-trident-volume>` Comando para actualizar un volumen heredado de Astra Trident a la especificación CSI.

```
./tridentctl get volumes -n trident
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS | PROTOCOL |
BACKEND UUID           | STATE  | MANAGED      |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| default-pvc-2-a8486 | 1.0 GiB | standard      | file     | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true         |          |
| default-pvc-3-a849e | 1.0 GiB | standard      | file     | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true         |          |
| default-pvc-1-a8475 | 1.0 GiB | standard      | file     | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true         |          |
| default-pvc-4-a84de | 1.0 GiB | standard      | file     | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true         |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

./tridentctl upgrade volume default-pvc-2-a8486 -n trident
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS | PROTOCOL |
BACKEND UUID           | STATE  | MANAGED      |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| default-pvc-2-a8486 | 1.0 GiB | standard      | file     | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true         |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

4. Ejecute un `kubectl describe pv` Para verificar que el volumen es un volumen CSI.

```
kubectl describe pv default-pvc-2-a8486
Name:                default-pvc-2-a8486
Labels:              <none>
Annotations:         pv.kubernetes.io/provisioned-by: csi.trident.netapp.io
                    volume.beta.kubernetes.io/storage-class: standard
Finalizers:          [kubernetes.io/pv-protection]
StorageClass:        standard
Status:              Bound
Claim:               default/pvc-2
Reclaim Policy:      Delete
Access Modes:        RWO
VolumeMode:          Filesystem
Capacity:            1073741824
Node Affinity:       <none>
Message:
Source:
  Type:               CSI (a Container Storage Interface (CSI) volume
source)
  Driver:             csi.trident.netapp.io
  VolumeHandle:       default-pvc-2-a8486
  ReadOnly:           false
  VolumeAttributes:   backendUUID=c5a6f6a4-b052-423b-80d4-
8fb491a14a22
internalName=trid_1907_alpha_default_pvc_2_a8486
                    name=default-pvc-2-a8486
                    protocol=file
Events:              <none>
```

Desinstale Astra Trident

En función de la instalación de Astra Trident, hay varias opciones para desinstalarla.

Desinstalar utilizando Helm

Si ha instalado Astra Trident mediante Helm, puede desinstalarlo mediante `helm uninstall`.


```
#List the Helm release corresponding to the Astra Trident install.
helm ls -n trident
NAME                NAMESPACE          REVISION          UPDATED
STATUS              CHART               APP VERSION
trident             trident             1                 2021-04-20
00:26:42.417764794 +0000 UTC deployed      trident-operator-21.07.1
21.07.1

#Uninstall Helm release to remove Trident
helm uninstall trident -n trident
release "trident" uninstalled
```

Desinstale mediante el operador Trident

Si ha instalado Astra Trident mediante el operador, puede desinstalarlo realizando una de las siguientes acciones:

- **Edición `TridentOrchestrator` Para establecer el indicador de desinstalación:** puede editar `TridentOrchestrator` y ajustar `spec.uninstall=true`. Edite el `TridentOrchestrator` CR y ajuste la `uninstall` marcar como se muestra a continuación:

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"uninstall":true}}'
```

Cuando la `uninstall` el indicador se establece en `true`, El operador Trident desinstala Trident, pero no quita el propio `TridentOrchestrator`. Debe limpiar el `TridentOrchestrator` y crear uno nuevo si lo desea. Vuelva a instalar Trident.

- **Eliminar `TridentOrchestrator`:** extrayendo el `TridentOrchestrator` CR utilizado para implementar Astra Trident, indica al operador que desinstale Trident. El operador procesa la eliminación de `TridentOrchestrator` Y procede a eliminar la implementación y el demonset de Astra Trident, con la eliminación de los pods de Trident que ha creado como parte de la instalación. Para eliminar completamente Astra Trident (incluidos los CRD que crea) y borrar la pizarra de forma efectiva, puede editar `TridentOrchestrator` para pasar la `wipeout` opción. Consulte el siguiente ejemplo:

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

Esto desinstala Astra Trident por completo y borra todos los metadatos relacionados con los back-ends y los volúmenes que gestiona. Las instalaciones posteriores se tratan como instalaciones frescas.



Sólo debe considerar borrar los CRD al realizar una desinstalación completa. Esta acción no se puede deshacer. **No limpie los CRD a menos que esté buscando empezar y crear una nueva instalación de Astra Trident.**

Desinstale mediante `tridentctl`

Ejecute el `uninstall` comando en `tridentctl`. A continuación, se eliminan todos los recursos asociados con Astra Trident, excepto los CRD y los objetos relacionados, lo que facilita la ejecución del instalador de nuevo para actualizar a una versión más reciente.

```
./tridentctl uninstall -n <namespace>
```

Para realizar una eliminación completa de Astra Trident, debe eliminar los finalizadores de los CRD creados por Astra Trident y eliminar los CRD.

Degradar Astra Trident

Conozca los pasos que se deben seguir para cambiar a una versión anterior de Astra Trident.

Cuándo degradar

Es posible que tenga en cuenta la degradación por varios motivos, como los siguientes:

- Planificación de contingencia
- Solución inmediata de errores observados como resultado de una actualización
- Problemas de dependencia, actualizaciones incorrectas e incompletas

Debe considerar una degradación al cambiar a una versión de Astra Trident que utiliza CRD. Como Astra Trident utiliza CRD para el mantenimiento del estado, todas las entidades de almacenamiento creadas (back-ends, clases de almacenamiento, VP y snapshots de volúmenes) tienen objetos CRD asociados en lugar de los datos escritos en la `trident PV` (utilizado por la versión anterior de Astra Trident). Las clases de almacenamiento, los back-ends y los VP recién creados se mantienen como objetos CRD.

Solo intente realizar una degradación a una versión de Astra Trident que se ejecute con CRD (19.07 y posterior). Esto garantiza que las operaciones realizadas en la versión actual de Astra Trident sean visibles una vez que se produce la degradación.

Cuando no se debe degradar

No debe degradar a una versión de Trident que utilice `etcd` mantener el estado (19.04 y anteriores). Todas las operaciones realizadas con la versión actual de Astra Trident no se reflejan después de la degradación. Los VP recién creados no se pueden utilizar al volver a una versión anterior. Los cambios que se realizan en objetos como los back-ends, VP, las clases de almacenamiento y las snapshots de volúmenes (creadas, actualizadas o eliminadas) no son visibles para Astra Trident al volver a una versión anterior. Volver a una versión anterior no interrumpe el acceso a los VP que ya se habían creado con la versión anterior, a menos que se hayan actualizado.

Proceso de degradación cuando se instala Astra Trident mediante el operador

En el caso de las instalaciones realizadas mediante el operador Trident, el proceso de degradación es diferente y no requiere el uso de `tridentctl`.

En el caso de las instalaciones realizadas mediante el operador Trident, es posible reclasificar Astra Trident a

uno de los siguientes:

- Versión que se instala mediante el operador namespace-scoped (20.07 - 20.10).
- Versión que se instala mediante el operador de ámbito del clúster (21.01 y posteriores).

Degradar al operador de ámbito del clúster

Para degradar Astra Trident a una versión que utilice el operador de ámbito del clúster, siga los pasos que se mencionan a continuación.

Pasos

1. **"Desinstale Astra Trident". No elimine los CRD a menos que desee eliminar completamente una instalación existente.**
2. El operador de Trident puede eliminarse mediante el manifiesto de operador asociado con su versión de Trident. Por ejemplo: <https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/bundle.yaml> donde *vXX.XX* es el número de versión (por ejemplo v22.10) y *bundle.yaml* Es el nombre del archivo YAML del grupo.
3. Continúe con la degradación instalando la versión deseada de Astra Trident. Siga la documentación para la versión deseada.

Degradar al operador de ámbito de espacio de nombres

En esta sección se resumen los pasos necesarios para la degradación a una versión de Astra Trident que está dentro del intervalo comprendido entre el 20.07 y el 20.10, que se instalará utilizando el operador de ámbito del espacio de nombres.

Pasos

1. **"Desinstale Astra Trident". No extraiga los CRD a menos que desee eliminar completamente una instalación existente.**
Asegúrese de que el `tridentorchestrator` se ha eliminado.

```
#Check to see if there are any tridentorchestrators present
kubectl get torc
NAME          AGE
trident      20h

#Looks like there is a tridentorchestrator that needs deleting
kubectl delete torc trident
tridentorchestrator.trident.netapp.io "trident" deleted
```

2. El operador de Trident puede eliminarse mediante el manifiesto de operador asociado con su versión de Trident. Por ejemplo: <https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/bundle.yaml> donde *vXX.XX* es el número de versión (por ejemplo v22.10) y *bundle.yaml* Es el nombre del archivo YAML del grupo.
3. Elimine el `tridentorchestrator` CRD.

```
#Check to see if ``tridentorchestrators.trident.netapp.io`` CRD is present and delete it.
```

```
kubectl get crd tridentorchestrators.trident.netapp.io
```

```
NAME                                CREATED AT
tridentorchestrators.trident.netapp.io 2021-01-21T21:11:37Z
```

```
kubectl delete crd tridentorchestrators.trident.netapp.io
```

```
customresourcedefinition.apiextensions.k8s.io
"tridentorchestrators.trident.netapp.io" deleted
```

Astra Trident se ha desinstalado.

4. Continúe con la degradación instalando la versión deseada. Siga la documentación para la versión deseada.

Bajar utilizando Helm

Para degradar, utilice `helm rollback` comando. Consulte el siguiente ejemplo:

```
helm rollback trident [revision #]
```

Proceso de degradación cuando Astra Trident se instala mediante `tridentctl`

Si instaló Astra Trident mediante `tridentctl`, el proceso de degradación implica los siguientes pasos. Esta secuencia le guiará por el proceso de degradación para pasar de Astra Trident 21.07 a 20.07.



Antes de iniciar la degradación, debe tomar una instantánea del clúster de Kubernetes `etcd`. Esto le permite realizar una copia de seguridad del estado actual de los CRD de Astra Trident.

Pasos

1. Compruebe que Trident se instala mediante `tridentctl`. Si no está seguro de cómo está instalado Astra Trident, ejecute esta sencilla prueba:
 - a. Enumere los pods presentes en el espacio de nombres de Trident.
 - b. Identifique la versión de Astra Trident que se ejecuta en su clúster. Puede utilizar cualquiera de estos dos usos `tridentctl`. También puede ver la imagen utilizada en los pods de Trident.
 - c. Si **no ve** a `tridentOrchestrator`, (o) un `tridentprovisioner`, (o) un pod llamado `trident-operator-xxxxxxxx-xxxxx`, Astra Trident **está instalado** con `tridentctl`.
2. Desinstale Astra Trident con el existente `tridentctl` binario. En este caso, se desinstalará con el binario 21.07.

```

tridentctl version -n trident
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 21.07.0        | 21.07.0        |
+-----+-----+

tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted Trident daemonset.
INFO Deleted Trident service.
INFO Deleted Trident secret.
INFO Deleted Trident cluster role binding.
INFO Deleted Trident cluster role.
INFO Deleted Trident service account.
INFO Deleted Trident pod security policy.
podSecurityPolicy=tridentpods
INFO The uninstaller did not delete Trident's namespace in case it is
going to be reused.
INFO Trident uninstallation succeeded.

```

3. Una vez finalizado este proceso, obtenga el binario de Trident correspondiente a la versión deseada (en este ejemplo, 20.07) y utilícelo para instalar Astra Trident. Puede generar YAML personalizados para un ["instalación personalizada"](#) si es necesario.

```

cd 20.07/trident-installer/
./tridentctl install -n trident-ns
INFO Created installer service account.
serviceaccount=trident-installer
INFO Created installer cluster role.                clusterrole=trident-
installer
INFO Created installer cluster role binding.
clusterrolebinding=trident-installer
INFO Created installer configmap.                  configmap=trident-
installer
...
...
INFO Deleted installer cluster role binding.
INFO Deleted installer cluster role.
INFO Deleted installer service account.

```

Se completó el proceso de degradación.

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.