



# Documentación de Trident 24,10

Trident

NetApp  
November 22, 2024

# Tabla de contenidos

Documentación de Trident 24,10	1
Notas de la versión	2
Lo nuevo	2
Versiones anteriores de la documentación	15
Manos a la obra	17
Obtenga más información sobre Trident	17
Inicio rápido para Trident	25
Requisitos	26
Instale Trident	30
Obtenga información acerca de la instalación de Trident	30
Realice la instalación mediante el operador Trident	34
Instale utilizando trimentctl	64
Utilizar Trident	70
Prepare el nodo de trabajo	70
Configurar y gestionar back-ends	80
Crear y gestionar clases de almacenamiento	236
Aprovisione y gestione volúmenes	241
Gestione y supervise Trident	283
Actualice Trident	283
Gestione Trident con tridentctl	290
Supervisar Trident	298
Desinstale Trident	301
Trident para Docker	304
Requisitos previos para la implementación	304
Ponga en marcha Trident	307
Actualice o desinstale Trident	312
Trabaje con volúmenes	313
Recopilar registros	322
Gestione múltiples instancias de Trident	323
Opciones de configuración de almacenamiento	324
Problemas y limitaciones conocidos	334
Prácticas recomendadas y recomendaciones	336
Puesta en marcha	336
Configuración del almacenamiento	336
Integre Trident	343
Protección de datos y recuperación ante desastres	354
Seguridad	356
Protege aplicaciones con Trident Protect	364
Más información sobre Trident Protect	364
Instale Trident Protect	364
Gestione Trident Protect	375
Gestione y proteja aplicaciones	383
Desinstale Trident Protect	427

Conocimiento y apoyo .....	428
Preguntas frecuentes .....	428
Resolución de problemas .....	435
Soporte técnico .....	441
Referencia .....	443
Puertos Trident .....	443
API de REST de Trident .....	443
Opciones de línea de comandos .....	444
Objetos de Kubernetes y Trident .....	445
Pod Security Standards (PSS) y las restricciones de contexto de seguridad (SCC) .....	457
Avisos legales .....	463
Derechos de autor .....	463
Marcas comerciales .....	463
Estadounidenses .....	463
Política de privacidad .....	463
Código abierto .....	463

# Documentación de Trident 24,10

# Notas de la versión

## Lo nuevo

Las notas de la versión proporcionan información sobre las nuevas funciones, las mejoras y las correcciones de errores en la última versión de Trident.



La `tridentctl` Binario para Linux que se proporciona en el archivo zip del instalador es la versión probada y compatible. Tenga en cuenta que `macos` binario proporcionado en la `/extras` parte del archivo zip no se ha probado ni es compatible.

## ¿Cuáles son las novedades de 24,10

### Mejoras

- El controlador de volúmenes de Google Cloud NetApp ahora está disponible de forma general para los volúmenes de NFS y es compatible con el aprovisionamiento que tiene en cuenta las zonas.
- La identidad de carga de trabajo de GCP se usará como identidad de cloud para NetApp Volumes de Google Cloud con GKE.
- Se ha añadido `formatOptions` el parámetro de configuración a los controladores ONTAP-SAN y ONTAP-SAN-Economy para permitir a los usuarios especificar las opciones de formato de LUN.
- Se redujo el tamaño mínimo de volumen mínimo de Azure NetApp Files a 50 GiB. Se espera que el nuevo tamaño mínimo de Azure esté disponible de forma general en noviembre.
- Se ha añadido `denyNewVolumePools` el parámetro de configuración para restringir los controladores ONTAP-NAS-Economy y ONTAP-SAN-Economy a pools FlexVol preexistentes.
- Detección añadida para la adición, eliminación o cambio de nombre de agregados desde la SVM en todos los controladores de ONTAP.
- Se ha agregado una sobrecarga de 18MiB a los LUN LUKS para garantizar que el tamaño de PVC informado sea utilizable.
- Mejora de la etapa de nodos ONTAP-SAN y ONTAP-SAN-Economy y eliminación de errores en la etapa de almacenamiento para permitir la eliminación de dispositivos después de una etapa fallida.
- Se ha añadido un generador de roles personalizado que permite a los clientes crear un rol minimalista para Trident en ONTAP.
- Se ha añadido un registro adicional para la solución de problemas `lsscsi` ("[Problema n.o 792](#)").

### Kubernetes

- Se han agregado nuevas funciones Trident para flujos de trabajo nativos de Kubernetes:
  - Protección de datos
  - Migración de datos
  - Recuperación tras siniestros
  - Movilidad de aplicaciones

["Obtenga más información sobre Trident Protect"](#).

- Se ha agregado un nuevo indicador `--k8s_api_qps` a los instaladores para establecer el valor QPS utilizado por Trident para comunicarse con el servidor API de Kubernetes.
- Se ha agregado `--node-prep` un indicador a los instaladores para la gestión automática de las dependencias del protocolo de almacenamiento en los nodos del clúster de Kubernetes. Compatibilidad probada y verificada con el protocolo de almacenamiento iSCSI Amazon Linux 2023
- Se ha añadido compatibilidad con la desconexión forzada para volúmenes ONTAP-NAS-Economy durante los escenarios de apagado de nodos sin gracia.
- Los nuevos volúmenes de NFS de ONTAP-NAS-Economy utilizan políticas de exportación por `qtree` cuando se utiliza `autoExportPolicy` la opción `back-end`. `Qtrees` solo se asignarán a políticas de exportación restrictivas de nodos en el momento de la publicación para mejorar el control de acceso y la seguridad. Los `qtrees` existentes se cambiarán al nuevo modelo de políticas de exportación cuando Trident cancelará el volumen de todos los nodos para hacerlo sin afectar a las cargas de trabajo activas.
- Añadido soporte para Kubernetes 1,31.

### Mejoras experimentales

- Se ha agregado una vista previa técnica para el soporte de Fibre Channel en el controlador ONTAP-SAN. Consulte ["Compatibilidad con Fibre Channel"](#).

### Soluciones

- **Kubernetes:**
  - Webhook de admisión de ranchero fijo que impide las instalaciones de Trident Helm (["Problema n.o 839"](#)).
  - Clave de afinidad fija en valores del gráfico de timón (["Problema n.o 898"](#)).
  - Fijo `tridentControllerPluginNodeSelector/tridentNodePluginNodeSelector` no funcionará con el valor verdadero (["Problema n.o 899"](#)).
  - Se han eliminado las snapshots efímeras creadas durante la clonación (["Problema n.o 901"](#)).
- Se ha añadido soporte para Windows Server 2019.
- Arreglado ``go mod tidy`` en Trident repo (["Problema n.o 767"](#)).

### Amortización

- **Kubernetes:**
  - Se actualizó el mínimo admitido de Kubernetes a 1,25.
  - Se ha eliminado el soporte para la política de seguridad de POD.

### Cambio de marca de productos

A partir del lanzamiento de la versión 24,10, Astra Trident cambia la marca a Trident (NetApp Trident). Esta nueva marca no afecta a ninguna función, plataforma compatible ni interoperabilidad de Trident.

## Cambios en 24,06

### Mejoras

- **IMPORTANTE:** El `limitVolumeSize` parámetro ahora limita el tamaño de `qtree/LUN` en los controladores económicos de ONTAP. Utilice el parámetro `new limitVolumePoolSize` para controlar

los tamaños de FlexVol en esos controladores. ("[Problema n.o 341](#)").

- Se ha añadido la capacidad de reparación automática de iSCSI para iniciar análisis de SCSI con un ID de LUN exacto si se están utilizando iGroups obsoletos ("[Problema n.o 883](#)").
- Se ha añadido compatibilidad con operaciones de clones de volúmenes y cambio de tamaño que se permite incluso cuando el back-end está en modo suspendido.
- Se ha agregado la capacidad de los ajustes de registro configurados por el usuario para que la controladora Trident se propague a los pods de nodos de Trident.
- Se ha agregado soporte en Trident para usar REST DE forma predeterminada, en lugar de ZAPI para las versiones 9.15.1 y posteriores de ONTAP.
- Se ha añadido soporte para nombres de volúmenes y metadatos personalizados en los back-ends de almacenamiento de ONTAP para los nuevos volúmenes persistentes.
- Se ha mejorado `azure-netapp-files` el controlador (ANF) para habilitar automáticamente el directorio Snapshot de forma predeterminada cuando las opciones de montaje de NFS se establecen para utilizar NFS versión 4.x.
- Se ha añadido soporte para Bottlerocket para volúmenes NFS.
- Se ha añadido soporte de previsualización técnica para Google Cloud NetApp Volumes.

### Kubernetes

- Añadido soporte para Kubernetes 1,30.
- Se ha añadido la capacidad de Trident DaemonSet para limpiar montajes zombis y archivos de seguimiento residual al inicio ("[Problema n.o 883](#)").
- Se ha agregado una anotación de PVC `trident.netapp.io/luksEncryption` para importar dinámicamente volúmenes LUKS ("[Problema n.o 849](#)").
- Se añadió el reconocimiento de topología al controlador de ANF.
- Se ha agregado compatibilidad con nodos de Windows Server 2022.

### Soluciones

- Se han corregido los fallos de instalación de Trident debido a transacciones obsoletas.
- Se ha corregido el `tridentctl` para ignorar los mensajes de advertencia de Kubernetes ("[Problema n.o 892](#)").
- Se ha cambiado la prioridad de la controladora Trident `SecurityContextConstraint` a 0 ("[Problema n.o 887](#)").
- Los controladores ONTAP ahora aceptan tamaños de volumen inferiores a 20MiB ("[Problema\[#885\]](#)").
- Se corrigió Trident para evitar la reducción de FlexVols durante la operación de cambio de tamaño para el controlador ONTAP-SAN.
- Se corrigió un error de importación de volúmenes de ANF con NFS v4,1.

### Amortización

- Se ha eliminado el soporte para EOL Windows Server 2019.

## Cambios en 24,02

## Mejoras

- Se ha añadido soporte para Cloud Identity.
  - AKS con ANF: La identidad de carga de trabajo de Azure se utilizará como identidad de nube.
  - EKS con FSxN - El rol AWS IAM se utilizará como identidad en la nube.
- Se ha añadido soporte para instalar Trident como complemento en el clúster EKS desde la consola EKS.
- Se ha añadido la capacidad para configurar y deshabilitar la reparación automática de iSCSI ("[Problema n.o 864](#)").
- Se ha añadido la personalidad de FSx a los controladores de ONTAP para permitir la integración con AWS IAM y SecretsManager, y para permitir que Trident elimine volúmenes FSx con backups ("[Problema n.o 453](#)").

## Kubernetes

- Añadido soporte para Kubernetes 1,29.

## Soluciones

- Se corrigieron los mensajes de advertencia ACP, cuando ACP no está habilitado ("[Problema n.o 866](#)").
- Se añadió un retraso de 10 segundos antes de ejecutar una división de clones durante la eliminación de copias de Snapshot para controladores ONTAP cuando se asocia un clon a la copia de Snapshot.

## Amortización

- Se ha eliminado el marco de atestaciones in-toto de los manifiestos de imágenes multiplataforma.

## Cambios en 23,10

### Soluciones

- Expansión de volumen fija si un tamaño nuevo solicitado es menor que el tamaño de volumen total de los controladores de almacenamiento ontap-nas y ontap-nas-flexgroup ("[Problema n.o 834](#)").
- Tamaño de volumen fijo para mostrar solo el tamaño utilizable del volumen durante la importación para los controladores de almacenamiento ontap-nas y ontap-nas-flexgroup ("[Problema n.o 722](#)").
- Conversión de nombres FlexVol fija para ONTAP-NAS-Economy.
- Se ha solucionado el problema de inicialización de Trident en un nodo de Windows cuando se reinicia el nodo.

## Mejoras

### Kubernetes

Añadido soporte para Kubernetes 1,28.

### Trident

- Soporte añadido para el uso de Azure Managed Identity (AMI) con controlador de almacenamiento de archivos de azure-netapp.
- Se añadió compatibilidad con NVMe over TCP para el controlador ONTAP-SAN.



- Se ha añadido la capacidad para pausar el aprovisionamiento de un volumen cuando el backend está establecido en estado suspendido por el usuario ("[Problema n.o 558](#)").

## Cambios en 23.07.1

**Kubernetes:** Eliminación de inicio de datos fija para admitir actualizaciones de cero tiempo de inactividad ("[Problema n.o 740](#)").

## Cambios en 23,07

### Soluciones

#### Kubernetes

- Se ha corregido la actualización de Trident para ignorar los pods antiguos atascados en estado de finalización ("[Problema n.o 740](#)").
- Se ha agregado tolerancia a la definición de «transient-trident-version-pod» ("[Problema n.o 795](#)").

#### Trident

- Se han corregido las solicitudes de ZAPI de ONTAP para garantizar que se consulten los números de serie de LUN al obtener atributos de LUN para identificar y corregir dispositivos iSCSI fantasma durante las operaciones de almacenamiento en caché de nodos.
- Arreglado el manejo de errores en el código del controlador de almacenamiento ("[Problema n.o 816](#)").
- Se corrigió el cambio de tamaño de la cuota al utilizar controladores ONTAP con use-rest=true.
- Creación de clones LUN fijos en ontap-san-economy.
- Revertir el campo de información de publicación desde `rawDevicePath` para `devicePath`; se ha añadido lógica para rellenar y recuperar (en algunos casos) `devicePath` campo.

### Mejoras

#### Kubernetes

- Se añadió compatibilidad para importar snapshots aprovisionadas previamente.
- Minimización de la implementación y el inicio de los permisos de linux ("[Problema n.o 817](#)").

#### Trident

- Ya no se notifica el campo de estado para volúmenes y copias Snapshot «en línea».
- Actualiza el estado del backend si el backend de ONTAP está fuera de línea ("[Problemas #801](#)", "[N.o 543](#)").
- El número de serie de LUN siempre se recupera y se publica durante el flujo de trabajo `ControllerVolumePublish`.
- Se ha agregado lógica adicional para verificar el tamaño y el número de serie del dispositivo multivía iSCSI.
- Verificación adicional de los volúmenes iSCSI para garantizar que se deja sin almacenar el dispositivo multivía correcto.

## Mejora experimental

Se ha añadido soporte de vista previa técnica para NVMe over TCP para el controlador ONTAP-SAN.

## Documentación

Se han realizado muchas mejoras organizativas y de formato.

## Amortización

### Kubernetes

- Se ha eliminado el soporte para las instantáneas v1beta1.
- Se ha eliminado la compatibilidad con los volúmenes previos a CSI y las clases de almacenamiento.
- Se actualizó el mínimo admitido de Kubernetes a 1,22.

## Cambios en 23,04



La fuerza de desconexión de volúmenes para volúmenes ONTAP-SAN-\* solo es compatible con las versiones de Kubernetes con la puerta de la función de apagado de nodos no agraciados habilitada. La desconexión forzada debe estar habilitada en el momento de la instalación mediante `--enable-force-detach` Indicador del instalador de Trident.

## Soluciones

- Se ha corregido el operador Trident para usar IPv6 localhost para la instalación cuando se especifica en SPEC.
- Se corrigieron los permisos de rol de clúster de operador de Trident que estaban sincronizados con los permisos del paquete ("[Número 799](#)").
- Se ha solucionado el problema al conectar un volumen de bloques sin configurar en varios nodos en el modo RWX.
- Compatibilidad con clonado de FlexGroup fijo e importación de volúmenes para volúmenes de SMB.
- Se corrigió el problema por el que la controladora Trident no podía apagarse inmediatamente ("[Problema n.o 811](#)").
- Se agregó una corrección para mostrar todos los nombres de igroup asociados con un LUN especificado aprovisionado con controladores ontap-san-\*.
- Se ha agregado una corrección para permitir que los procesos externos se ejecuten hasta su finalización.
- Corregido error de compilación para la arquitectura s390 ("[Problema n.o 537](#)").
- Se solucionó un nivel de registro incorrecto durante las operaciones de montaje de volúmenes ("[Problema n.o 781](#)").
- Se ha corregido el error de afirmación de tipo potencial ("[Problema n.o 802](#)").

## Mejoras

- Kubernetes:
  - Añadido soporte para Kubernetes 1,27.
  - Se ha añadido soporte para importar volúmenes LUKS.

- Se ha añadido soporte para el modo de acceso de PVC ReadWriteOncePod.
- Se añadió compatibilidad con la desconexión forzada para volúmenes ONTAP-SAN-\* durante los escenarios de apagado de nodos sin gracia.
- Todos los volúmenes de ONTAP-SAN-\* ahora utilizarán iGroups por nodo. Las LUN solo se asignarán a iGroups, mientras que se publicarán de forma activa en esos nodos para mejorar nuestra política de seguridad. Los volúmenes existentes se cambiarán de forma oportunista al nuevo esquema de igroup cuando Trident determina que es seguro hacerlo sin afectar a las cargas de trabajo activas ("[Problema n.o 758](#)").
- Mejora en la seguridad de Trident mediante la limpieza de los iGroups gestionados por Trident sin utilizar de los back-ends ONTAP-SAN-\*.
- Se ha añadido soporte para volúmenes SMB con Amazon FSx para la economía de ontap-nas y los controladores de almacenamiento de ontap-nas-flexgroup.
- Se añadió compatibilidad con recursos compartidos SMB con los controladores de almacenamiento ONTAP-nas, ontap-nas y ontap-nas-flexgroup.
- Se ha añadido compatibilidad con los nodos arm64 ("[Problema n.o 732](#)").
- Ha mejorado el procedimiento de apagado de Trident desactivando los servidores API en primer lugar ("[Problema n.o 811](#)").
- Agregado soporte de compilación multiplataforma para hosts Windows y arm64 a Makefile; consulte BUILD.md.

## Amortización

**Kubernetes:** Ya no se crearán iGroups en el ámbito del back-end al configurar controladores ontap-san y ontap-san-economy ("[Problema n.o 758](#)").

## Cambios en 23.01.1

### Soluciones

- Se ha corregido el operador Trident para usar IPv6 localhost para la instalación cuando se especifica en SPEC.
- Se han corregido los permisos de rol de clúster del operador de Trident para que estén sincronizados con los permisos del paquete "[Número 799](#)".
- Se ha agregado una corrección para permitir que los procesos externos se ejecuten hasta su finalización.
- Se ha solucionado el problema al conectar un volumen de bloques sin configurar en varios nodos en el modo RWX.
- Compatibilidad con clonado de FlexGroup fijo e importación de volúmenes para volúmenes de SMB.

## Cambios en 23.01



Kubernetes 1,27 ahora es compatible con Trident. Actualice Trident antes de actualizar Kubernetes.

### Soluciones

- Kubernetes: Se han añadido opciones para excluir la creación de políticas de seguridad de Pod para corregir las instalaciones de Trident mediante Helm ("[Cuestiones #783, #794](#)").

## Mejoras

### Kubernetes

- Se ha añadido la compatibilidad con Kubernetes 1.26.
- Mejora de la utilización general de recursos de RBAC de Trident ("[Número 757](#)").
- Se agregó la automatización para detectar y corregir sesiones iSCSI rotas o obsoletas en los nodos de host.
- Compatibilidad añadida para ampliar volúmenes cifrados de LUKS.
- Kubernetes: Compatibilidad con rotación de credenciales añadida para volúmenes cifrados de LUKS.

### Trident

- Se ha agregado compatibilidad para volúmenes SMB con Amazon FSX para ONTAP al controlador de almacenamiento ontap-nas.
- Se añadió soporte para permisos NTFS cuando se utilizan volúmenes SMB.
- Se ha agregado soporte para pools de almacenamiento para volúmenes de GCP con el nivel de servicio CVS.
- Se ha añadido compatibilidad para el uso opcional de flexgroupagregarList al crear FlexGroups con el controlador de almacenamiento ontap-nas-flexgroup.
- Rendimiento mejorado para el controlador de almacenamiento ONTAP-nas-Economy al gestionar múltiples FlexVols.
- Actualizaciones de datLIF activadas para todas las controladoras de almacenamiento NAS de ONTAP.
- Se han actualizado la convención de nomenclatura Trident Deployment y DemonSet para reflejar el sistema operativo del nodo del host.

### Amortización

- Kubernetes: Se ha actualizado el mínimo admitido de Kubernetes a 1.21.
- Ya no se deben especificar LIF de datos al realizar la configuración `ontap-san 0. ontap-san-economy` de windows

## Cambios en 22.10

Debe leer la siguiente información crítica antes de actualizar a Trident 22,10.

### **Información crítica sobre Trident 22.10**

- Kubernetes 1,25 ahora es compatible con Trident. Debe actualizar Trident a 22,10 antes de actualizar a Kubernetes 1,25.
- Ahora, Trident aplica estrictamente el uso de la configuración de rutas múltiples en entornos SAN, con un valor recomendado de `find_multipaths: no` en el archivo `multipath.conf`.



Uso de la configuración sin multivía o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Soluciones

- Se ha solucionado un problema específico del back-end de ONTAP creado mediante `credentials` el campo no se puede conectar durante la actualización 22.07.0 ("[Número 759](#)").
- **Docker:** se ha solucionado un problema que provocaba que el complemento para volúmenes de Docker no empezara en algunos entornos ("[Número 548](#)" y.. "[Número 760](#)").
- Se ha solucionado el problema de SLM específico de los back-ends DE SAN de ONTAP para garantizar que solo se publicara un subconjunto de LIF de datos que pertenecen a nodos de generación de informes.
- Se ha solucionado un problema de rendimiento por el que se realizaron análisis innecesarios de LUN iSCSI al conectar un volumen.
- Se han eliminado reintentos granulares dentro del flujo de trabajo de iSCSI de Trident para producir fallos rápidamente y reducir los intervalos de reintentos externos.
- Se solucionó un problema cuando se devolvió un error al vaciar un dispositivo iSCSI cuando ya se había vaciado el dispositivo multivía correspondiente.

## Mejoras

- Kubernetes:
  - Añadido soporte para Kubernetes 1,25. Debe actualizar Trident a 22,10 antes de actualizar a Kubernetes 1,25.
  - Se ha agregado una cuenta de servicio, ClusterRole y ClusterRoleBinding aparte para la implementación de Trident y DemonSet para permitir futuras mejoras de permisos.
  - Se ha agregado compatibilidad con "[uso compartido de volúmenes entre espacios de nombres](#)".
- Todos los Trident `ontap-*` Los controladores de almacenamiento ahora funcionan con la API DE REST de ONTAP.
- Se ha añadido un nuevo operador yaml (`bundle_post_1_25.yaml`) sin `a.PodSecurityPolicy` Para admitir Kubernetes 1.25.
- Añadido "[Compatibilidad con volúmenes cifrados LUKS](#)" para `ontap-san` y.. `ontap-san-economy` impulsores del almacenamiento.
- Se ha agregado compatibilidad con nodos de Windows Server 2019.
- Añadido "[Compatibilidad con volúmenes SMB en nodos de Windows](#)" a través de la `azure-netapp-files` controlador de almacenamiento.
- La detección de conmutación automática de MetroCluster para controladores ONTAP está disponible por lo general.

## Amortización

- **Kubernetes:** Actualizado el mínimo admitido de Kubernetes a 1.20.
- Se ha eliminado el controlador Astra Data Store (ADS).
- Se ha quitado el soporte de `yes` y.. `smart` opciones para `find_multipaths` Al configurar accesos múltiples de nodos de trabajo para iSCSI.

## Cambios en 22.07

## Soluciones

### Kubernetes

- Se ha solucionado el problema para manejar los valores booleanos and Number para el selector de nodos cuando se configura Trident con Helm o el operador de Trident. ("[GitHub número 700](#)")
- Se ha solucionado el problema al gestionar errores de ruta no CHAP, de modo que kubelet lo volverá a intentar si falla. ("[GitHub número 736](#)")

### Mejoras

- Pasar de k8s.gcr.io a registry.k8s.io como registro predeterminado para las imágenes CSI
- Los volúmenes de ONTAP-SAN ahora utilizan iGroups por nodo y solo asignan LUN a iGroups, mientras se publican de forma activa en esos nodos para mejorar nuestra política de seguridad. Los volúmenes existentes se conmutarán de manera oportunista al nuevo esquema de igroup, cuando Trident determina que es seguro hacerlo sin afectar a las cargas de trabajo activas.
- Se incluye un ResourceQuota con las instalaciones de Trident para garantizar que Trident DemonSet se programe cuando el consumo de PriorityClass esté limitado de forma predeterminada.
- Se ha añadido compatibilidad con las funciones de red al controlador Azure NetApp Files. ("[GitHub número 717](#)")
- Se ha añadido una vista previa tecnológica con detección automática de conmutación de MetroCluster a los controladores de ONTAP. ("[GitHub número 228](#)")

### Amortización

- **Kubernetes:** Actualizado el mínimo admitido de Kubernetes a 1.19.
- La configuración de back-end ya no permite múltiples tipos de autenticación en una única configuración.

### Absorciones

- Se ha eliminado el controlador CVS de AWS (obsoleto desde 22.04).
- Kubernetes
  - Se eliminó la capacidad SYS\_ADMIN innecesaria de los POD de nodos.
  - Reduce la preparación de nodos a una información de host sencilla y la detección de servicios activos para confirmar que los servicios NFS/iSCSI están disponibles en los nodos de trabajo.

### Documentación

Se ha agregado una nueva "[Estándares de seguridad de POD](#)" sección (PSS) que detalla los permisos habilitados por Trident en la instalación.

## Cambios en 22.04

NetApp mejora y mejora continuamente sus productos y servicios. Estas son algunas de las últimas características en Trident. Para versiones anteriores, consulte "[Versiones anteriores de la documentación](#)".



Si actualiza desde cualquier versión de Trident anterior y utiliza Azure NetApp Files, el `location` el parámetro `config` es ahora un campo obligatorio singleton.

## Soluciones

- Análisis mejorado de nombres de iniciadores iSCSI. (["GitHub número 681"](#))
- Se ha solucionado un problema en el que no se permitían los parámetros de clase de almacenamiento CSI. (["GitHub número 598"](#))
- Se ha corregido la declaración de clave duplicada en Trident CRD. (["GitHub número 671"](#))
- Se han corregido registros de instantánea CSI imprecisos. (["GitHub número 629"](#))
- Se ha solucionado el problema con la anulación de la publicación de volúmenes en nodos eliminados. (["GitHub número 691"](#))
- Se ha añadido el tratamiento de incoherencias del sistema de archivos en dispositivos de bloque. (["GitHub número 656"](#))
- Se ha solucionado el problema al extraer imágenes de soporte automático al configurar el `imageRegistry` indicador durante la instalación. (["GitHub número 715"](#))
- Se solucionó el problema en el que el controlador Azure NetApp Files no pudo clonar un volumen con varias reglas de exportación.

## Mejoras

- Las conexiones entrantes con los extremos seguros de Trident ahora requieren un mínimo de TLS 1.3. (["GitHub número 698"](#))
- Trident ahora añade encabezados HSTS a las respuestas desde sus extremos seguros.
- Trident ahora intenta habilitar automáticamente la función de permisos de unix de Azure NetApp Files.
- **Kubernetes:** El demonset de Trident ahora se ejecuta en la clase prioritaria del nodo-sistema. (["GitHub número 694"](#))

## Absorciones

Se ha quitado el controlador E-Series (desactivado desde 20.07).

## Cambios en 22.01.1

### Soluciones

- Se ha solucionado el problema con la anulación de la publicación de volúmenes en nodos eliminados. (["GitHub número 691"](#))
- Alerta fija al acceder a campos nulos para añadir espacio en respuestas de la API de ONTAP.

## Cambios en 22.01.0

### Soluciones

- **Kubernetes:** aumente el tiempo de reintento de retroceso de registro de nodos para clústeres grandes.
- Problema fijo donde el controlador Azure-netapp-files podría confundirse con varios recursos con el mismo nombre.
- Los LIF de datos IPv6 DE SAN de ONTAP ahora funcionan si se especifican con paréntesis.
- Un problema fijo en el que intentar importar un volumen ya importado devuelve EOF dejando PVC en estado pendiente. (["GitHub número 489"](#))

- Se solucionó el problema cuando el rendimiento de Trident se ralentiza al crear más de 32 snapshots en un volumen de SolidFire.
- Se reemplazó SHA-1 por SHA-256 en la creación de certificados SSL.
- Se corrigió el controlador Azure NetApp Files para permitir nombres de recursos duplicados y limitar operaciones a una sola ubicación.
- Se corrigió el controlador Azure NetApp Files para permitir nombres de recursos duplicados y limitar operaciones a una sola ubicación.

## Mejoras

- Mejoras de Kubernetes:
  - Se ha añadido la compatibilidad con Kubernetes 1.23.
  - Añada opciones de programación para los pods de Trident cuando se instalen mediante Trident Operator o Helm. (["GitHub número 651"](#))
- Permitir volúmenes entre regiones en el controlador GCP. (["GitHub número 633"](#))
- Se añadió compatibilidad con la opción 'unixPermissions' para volúmenes Azure NetApp Files. (["GitHub número 666"](#))

## Amortización

La interfaz DE REST de Trident solo puede escuchar y servir en 127.0.0.1 o direcciones [::1]

## Cambios en 21.10.1



La versión v21.10.0 tiene un problema que puede poner a la controladora Trident en estado CrashLoopBackOff cuando se elimina un nodo y, a continuación, volver a añadirse al clúster de Kubernetes. Este problema se soluciona en v21.10.1 ([GitHub número 669](#)).

## Soluciones

- Se ha corregido una condición de carrera potencial al importar un volumen en un back-end CVS de GCP, lo que provoca un error al importar.
- Se ha solucionado un problema que puede poner la controladora Trident en estado CrashLoopBackOff cuando se quita un nodo y, a continuación, se vuelve a añadir al clúster de Kubernetes ([GitHub número 669](#)).
- Problema fijo donde ya no se detectaron SVM si no se especificó ningún nombre de SVM ([GitHub, número 612](#)).

## Cambios en 21.10.0

### Soluciones

- Se ha solucionado el problema por el que no se podían montar clones de volúmenes XFS en el mismo nodo que el volumen de origen (problema 514 de [GitHub](#)).
- Se ha solucionado el problema por el que Trident registraba un error fatal al cerrar ([GitHub problema 597](#)).
- Correcciones relacionadas con Kubernetes:
  - Devuelva el espacio usado de un volumen como el tamaño mínimo de restoreSize a la hora de crear



snapshots con `ontap-nas` y.. `ontap-nas-flexgroup` Controladores (GitHub, número 645).

- Se ha solucionado el problema `Failed to expand filesystem` Se registró el error después de cambiar el tamaño del volumen (problema 560 de GitHub).
- Se ha solucionado un problema por el que se podría atascar un pod `Terminating` estado (GitHub número 572).
- Se ha fijado la caja donde un `ontap-san-economy` Es posible que FlexVol esté lleno de LUN de snapshot (GitHub, número 533).
- Se ha solucionado el problema del instalador de YAML personalizado con una imagen diferente (GitHub, número 613).
- Se ha corregido el cálculo del tamaño de la instantánea (GitHub, número 611).
- Se solucionó un problema por el que todos los instaladores de Trident podían identificar Kubernetes sin formato como OpenShift (GitHub número 639).
- Se ha solucionado el operador Trident para detener la reconciliación si no se puede acceder al servidor API de Kubernetes (GitHub, número 599).

## Mejoras

- Se ha agregado compatibilidad con `unixPermissions` Opción para los volúmenes de rendimiento GCP-CVS.
- Se ha agregado compatibilidad con volúmenes CVS optimizados para el escalado en GCP en el intervalo de 600 GiB a 1 TiB.
- Mejoras relacionadas con Kubernetes:
  - Se ha añadido la compatibilidad con Kubernetes 1.22.
  - Se ha habilitado el operador de Trident y el gráfico Helm para que funcionen con Kubernetes 1.22 (GitHub, número 628).
  - Se ha añadido la imagen del operador a. `tridentctl` Comando `images` (GitHub, número 570).

## Mejoras experimentales

- Se añadió la compatibilidad con la replicación de volúmenes en `ontap-san` controlador.
- Se ha añadido el soporte DE DESCANSO **vista previa tecnológica** para el `ontap-nas-flexgroup`, `ontap-san`, y. `ontap-nas-economy` de `windows`

## Problemas conocidos

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

- Cuando actualice un clúster de Kubernetes de 1,24 a 1,25 o una versión posterior que tiene Trident instalado, debe actualizar los valores.yaml para establecer `excludePodSecurityPolicy true` o agregar `--set excludePodSecurityPolicy=true` al `helm upgrade` comando antes de poder actualizar el clúster.
- Trident ahora aplica un espacio en blanco `fsType` (`fsType=""`) para volúmenes que no tienen el `fsType` especificado en su clase de almacenamiento. Al trabajar con Kubernetes 1,17 o una versión posterior, Trident admite proporcionar un espacio vacío `fsType` para volúmenes NFS. Para los volúmenes iSCSI, debe establecer `fsType` en su clase de almacenamiento al aplicar un `fsGroup` contexto de uso de seguridad.

- Cuando se utiliza un backend en varias instancias de Trident, cada archivo de configuración de backend debe tener un valor diferente `storagePrefix` para los back-ends de ONTAP o utilizar otro `TenantName` para los back-ends de SolidFire. Trident no puede detectar volúmenes que han creado otras instancias de Trident. Si se intenta crear un volumen existente en back-ends ONTAP o SolidFire se completa correctamente, porque Trident trata la creación de volúmenes como una operación idempotente. Si `storagePrefix` se diferencian o `TenantName` no, es posible que existan colisiones de nombres para los volúmenes creados en el mismo back-end.
- Al instalar Trident (utilizando `tridentctl` o el Operador Trident) y utilizar `tridentctl` para administrar Trident, debe asegurarse de que la `KUBECONFIG` variable de entorno está definida. Esto es necesario para indicar el clúster de Kubernetes en `tridentctl` el que debería funcionar. Cuando trabaje con varios entornos de Kubernetes, debe asegurarse de que el `KUBECONFIG` archivo se obtenga con precisión.
- Para realizar una reclamación de espacio en línea para VP iSCSI, el sistema operativo subyacente del nodo de trabajo puede requerir que se pasen las opciones de montaje al volumen. Esto es así para las instancias de RHEL/RedHat CoreOS, que requieren el `discard` "opción de montaje"; Asegúrese de que la opción de montaje de descarte esté incluida en su `StorageClass` para admitir descarte de bloques en línea.
- Si hay más de una instancia de Trident por clúster de Kubernetes, Trident no puede comunicarse con otras instancias y no puede detectar otros volúmenes que hayan creado, lo que provoca un comportamiento inesperado e incorrecto si más de una instancia se ejecuta en un clúster. Solo debería haber una instancia de Trident por clúster de Kubernetes.
- Si los objetos basados en Trident `StorageClass` se eliminan de Kubernetes mientras Trident está desconectado, Trident no elimina las clases de almacenamiento correspondientes de su base de datos cuando vuelve a estar online. Debe eliminar estas clases de almacenamiento mediante `tridentctl` o la API de REST.
- Si un usuario elimina un volumen persistente provisionado por Trident antes de eliminar la RVP correspondiente, Trident no elimina automáticamente el volumen de respaldo. Debe quitar el volumen a través de `tridentctl` o la API DE REST.
- ONTAP no puede provisionar simultáneamente más de un FlexGroup a menos que el conjunto de agregados sea único para cada solicitud de aprovisionamiento.
- Cuando se usa Trident a través de IPv6, debe especificar `managementLIF` y `dataLIF` en la definición de back-end dentro de corchetes. Por ejemplo, `[fd20:8b1e:b258:2000:f816:3eff:feec:0]`.



No se puede especificar `dataLIF` en un back-end de SAN de ONTAP. Trident descubre todos los LIF iSCSI disponibles y los usa para establecer la sesión multivía.

- Si utiliza `solidfire-san` Controlador con OpenShift 4.5, asegúrese de que los nodos de trabajo subyacentes utilizan MD5 como algoritmo de autenticación CHAP. Los algoritmos CHAP SHA1, SHA-256 y SHA3-256 compatibles con FIPS están disponibles con Element 12.7.

## Obtenga más información

- ["Trident GitHub"](#)
- ["Blogs de Trident"](#)

## Versiones anteriores de la documentación

Si no está ejecutando Trident 24,10, la documentación de versiones anteriores está disponible en función de la ["Ciclo de vida del soporte de Trident"](#).

- "Trident 24,06"
- "Trident 24,02"
- "Trident 23,10"
- "Trident 23,07"
- "Trident 23,04"
- "Trident 23,01"
- "Trident 22,10"
- "Trident 22,07"
- "Trident 22,04"
- "Trident 22,01"

# Manos a la obra

## Obtenga más información sobre Trident

### Obtenga más información sobre Trident

Trident es un proyecto de código abierto totalmente compatible y mantenido por NetApp. Se ha diseñado para ayudarle a cumplir las demandas de persistencia de sus aplicaciones en contenedores mediante interfaces estándar del sector, como la Container Storage Interface (CSI).

#### ¿Qué es Trident?

NetApp Trident permite el consumo y la gestión de recursos de almacenamiento en todas las plataformas de almacenamiento más conocidas de NetApp, ya sea en el cloud público o en las instalaciones, incluidos ONTAP (AFF, FAS, Select, Cloud, Amazon FSx para NetApp ONTAP), el software Element (NetApp HCI, SolidFire), el servicio Azure NetApp Files y Cloud Volumes Service en Google Cloud.

Trident es una interfaz de almacenamiento de contenedores (CSI) que ordena el almacenamiento dinámico conforme a la normativa que se integra de forma nativa con ["Kubernetes"](#). Trident se ejecuta como un pod de controladora más un pod de nodo en cada nodo trabajador del clúster. Consulte ["Arquitectura de Trident"](#) para obtener más información.

Trident también proporciona integración directa con el ecosistema de Docker para las plataformas de almacenamiento de NetApp. El complemento para volúmenes de Docker de NetApp (nDVP) admite el aprovisionamiento y la gestión de recursos de almacenamiento desde la plataforma de almacenamiento a los hosts de Docker. Consulte ["Ponga en marcha Trident para Docker"](#) para obtener más información.



Si es la primera vez que usa Kubernetes, deberá familiarizarse con el ["Conceptos y herramientas de Kubernetes"](#).

### Realice la prueba de Trident

Para realizar una prueba, solicite acceso a «Puesta en marcha y clonación sencilla de almacenamiento persistente para cargas de trabajo en contenedores» ["Versión de prueba de NetApp"](#) mediante una imagen de laboratorio lista para usar. La unidad de prueba proporciona un entorno de pruebas con un clúster de Kubernetes de tres nodos y Trident instalado y configurado. Esta es una excelente manera de familiarizarse con Trident y explorar sus características.

Otra opción es la ["Guía de instalación de Kubeadm"](#) Proporcionado por Kubernetes.



No utilice un clúster de Kubernetes creado con estas instrucciones en un entorno de producción. Use las guías de puesta en marcha de producción proporcionadas por su distribución para clústeres listos para la producción.

### Integración de Kubernetes con productos de NetApp

La cartera de productos de almacenamiento de NetApp se integra con muchos aspectos de un clúster de Kubernetes, lo que ofrece capacidades de gestión de datos avanzadas que mejoran la funcionalidad, la capacidad, el rendimiento y la disponibilidad de la puesta en marcha de Kubernetes.

## Amazon FSX para ONTAP de NetApp

"[Amazon FSX para ONTAP de NetApp](#)" Es un servicio AWS totalmente gestionado que le permite iniciar y ejecutar sistemas de archivos con tecnología del sistema operativo de almacenamiento NetApp ONTAP.

## Azure NetApp Files

"[Azure NetApp Files](#)" Es un servicio de recursos compartidos de archivos de Azure de clase empresarial con la tecnología de NetApp. Puede ejecutar sus cargas de trabajo basadas en archivos más exigentes de forma nativa en Azure, con el rendimiento y la gestión de datos enriquecidos que espera de NetApp.

## Cloud Volumes ONTAP

"[Cloud Volumes ONTAP](#)" Es un dispositivo de almacenamiento exclusivamente de software que ejecuta el software para la gestión de datos ONTAP en el cloud.

## NetApp Volumes para Google Cloud

"[NetApp Volumes para Google Cloud](#)" Es un servicio de almacenamiento de archivos completamente gestionado en Google Cloud que ofrece un almacenamiento de archivos de alto rendimiento y clase empresarial.

## Software Element

"[Elemento](#)" permite al administrador de almacenamiento consolidar cargas de trabajo garantizando el rendimiento y haciendo posible un espacio de almacenamiento simplificado y optimizado.

## NetApp HCI

"[NetApp HCI](#)" simplifica la gestión y el escalado del centro de datos mediante la automatización de las tareas rutinarias y permite que los administradores de la infraestructura se centren en funciones más importantes.

Trident puede aprovisionar y gestionar dispositivos de almacenamiento para aplicaciones en contenedores directamente en la plataforma de almacenamiento subyacente de NetApp HCI.

## ONTAP de NetApp

"[ONTAP de NetApp](#)" Es el sistema operativo de almacenamiento unificado multiprotocolo de NetApp que proporciona capacidades avanzadas de gestión de datos para cualquier aplicación.

Los sistemas ONTAP tienen configuraciones all-flash, híbridas o all-HDD y ofrecen muchos modelos de puesta en marcha diferentes, como hardware a medida (FAS y AFF), unidad genérica (ONTAP Select) y solo cloud (Cloud Volumes ONTAP). Trident admite estos modelos de puesta en marcha de ONTAP.

## Arquitectura de Trident

Trident se ejecuta como un pod de controladora más un pod de nodo en cada nodo trabajador del clúster. El pod de nodo debe ejecutarse en cualquier host en el que desee potencialmente montar un volumen de Trident.

### Descripción de los pods de la controladora y los pods de nodo

Trident se pone en marcha como [Pod de controladora de Trident](#) uno o más [Pods de nodos de Trident](#) en el clúster de Kubernetes y utiliza contenedores Sidecar Containers\_ estándar de Kubernetes \_CSI para simplificar la implementación de los complementos CSI. "[Contenedores Sidecar de Kubernetes CSI](#)" Los mantiene la comunidad de Kubernetes Storage.

Kubernetes "[selectores de nodos](#)" y "[toleraciones y tints](#)" se utilizan para restringir que un pod se ejecute en un nodo específico o preferido. Durante la instalación de Trident, se pueden configurar selectores de nodos y toleraciones para pods de nodos y controladoras.

- El complemento de la controladora se ocupa del aprovisionamiento y la gestión de volúmenes, como snapshots y redimensionamiento.
- El complemento de nodo se encarga de conectar el almacenamiento al nodo.

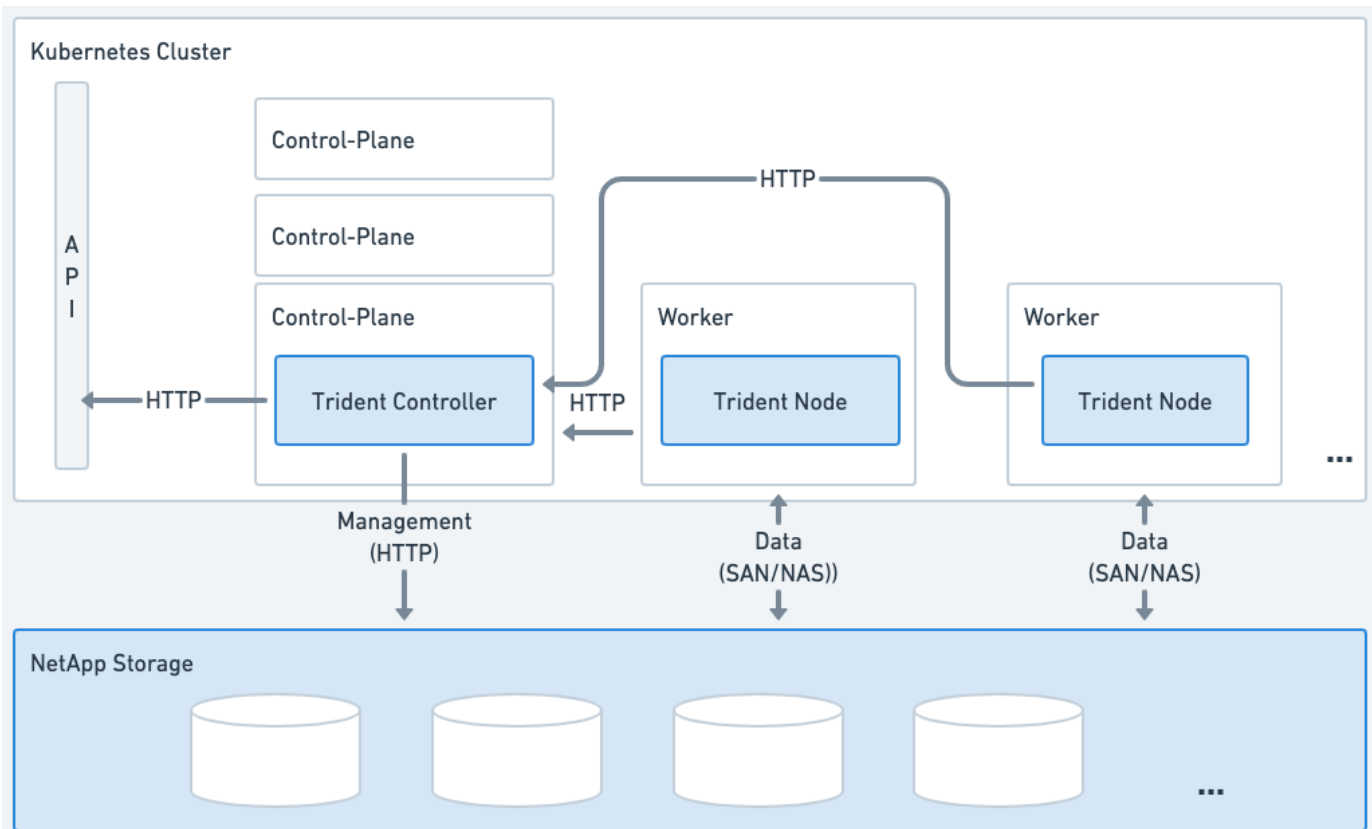


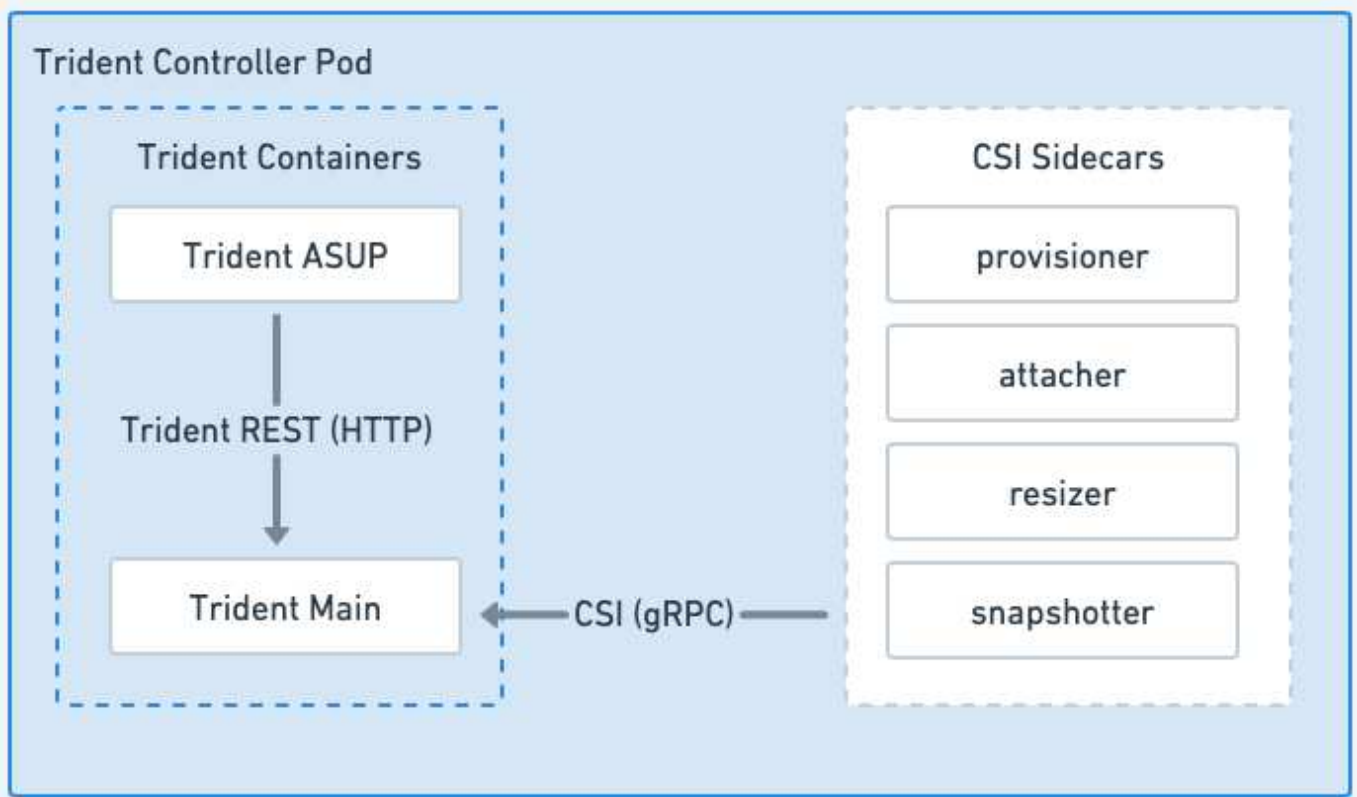
Figura 1. Trident puesto en marcha en el clúster de Kubernetes

### Pod de controladora de Trident

Trident Controller Pod es un pod único que ejecuta el complemento CSI Controller.

- Responsable de aprovisionar y gestionar volúmenes en el almacenamiento de NetApp

- Gestionado por una puesta en marcha de Kubernetes
- Se puede ejecutar en el plano de control o en los nodos de trabajo, según los parámetros de instalación.



**Figura 2. Diagrama de Trident Controller Pod**

#### **Pods de nodos de Trident**

Los pods de nodos Trident son pods con privilegios que ejecutan el plugin de nodo CSI.

- Responsable del montaje y desmontaje del almacenamiento de los pods que se ejecutan en el host
- Gestionado por un DaemonSet de Kubernetes
- Debe ejecutarse en cualquier nodo que monte el almacenamiento de NetApp

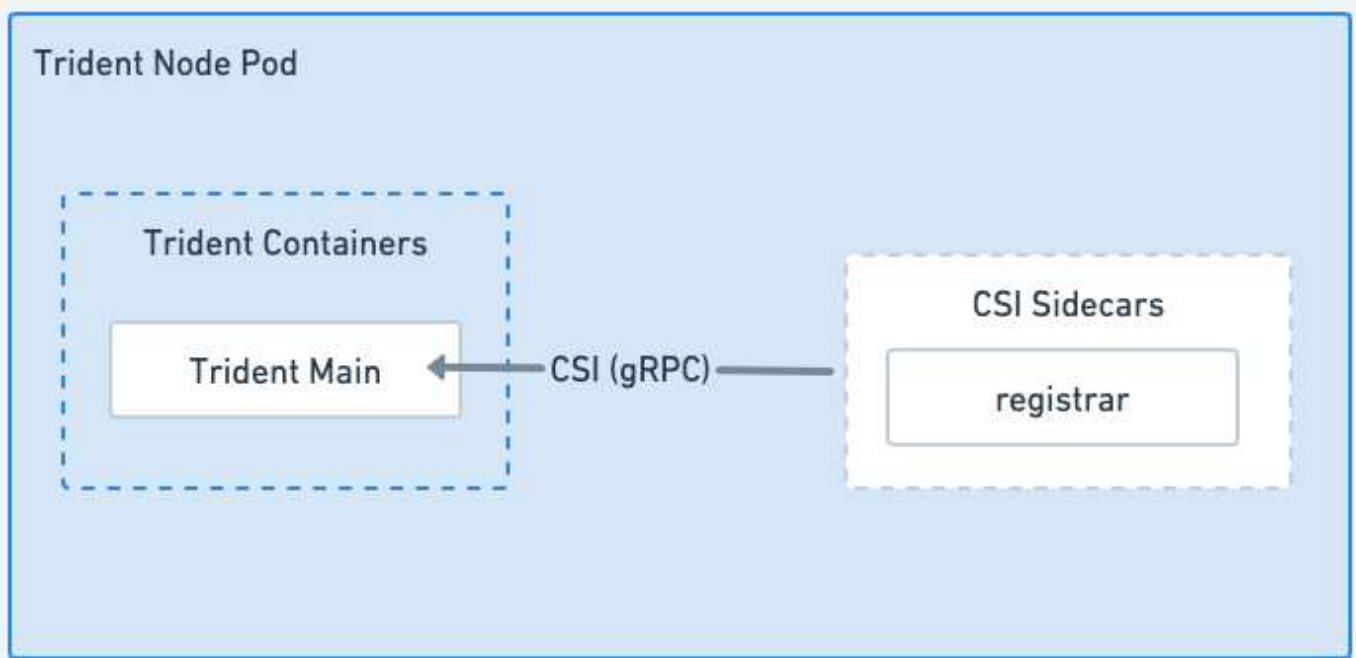


Figura 3. Diagrama de Trident Node Pod

### Arquitecturas de clúster de Kubernetes compatibles

Trident es compatible con las siguientes arquitecturas de Kubernetes:

Arquitecturas de clústeres de Kubernetes	Compatible	Instalación predeterminada
Un único maestro, informática	Sí	Sí
Varios maestros, informáticos	Sí	Sí
Maestro, etcd, cálculo	Sí	Sí
Maestro, infraestructura y computación	Sí	Sí

## Conceptos

### El provisionamiento

El aprovisionamiento en Trident tiene dos fases principales. La primera fase asocia una clase de almacenamiento con el conjunto de agrupaciones de almacenamiento back-end adecuadas y tiene lugar como preparación necesaria antes del aprovisionamiento. La segunda fase incluye la creación misma del volumen y requiere la selección de un pool de almacenamiento entre los asociados con la clase de almacenamiento del volumen pendiente.

#### Asociación de clase de almacenamiento

La asociación de pools de almacenamiento de backend con una clase de almacenamiento depende tanto de los atributos solicitados de la clase de almacenamiento como de sus `storagePools` listas ,



`additionalStoragePools` y `excludeStoragePools` Al crear una clase de almacenamiento, Trident compara los atributos y pools que ofrecen cada uno de sus back-ends con los solicitados por la clase de almacenamiento. Si los atributos y el nombre de un pool de almacenamiento coinciden con todos los atributos y nombres de pools solicitados, Trident agrega ese pool de almacenamiento al conjunto de pools de almacenamiento adecuados para esa clase de almacenamiento. Además, Trident añade a ese conjunto todos los pools de almacenamiento mostrados en `additionalStoragePools` la lista, aunque sus atributos no cumplan todos o ninguno de los atributos solicitados de la clase de almacenamiento. Debe usar la `excludeStoragePools` lista para anular y quitar pools de almacenamiento del uso para una clase de almacenamiento. Trident realiza un proceso similar cada vez que agrega un nuevo back-end, comprobando si sus pools de almacenamiento satisfacen las de las clases de almacenamiento existentes y eliminando las que se hayan marcado como excluidas.

### Creación del volumen

A continuación, Trident utiliza las asociaciones entre las clases de almacenamiento y los pools de almacenamiento para determinar dónde aprovisionar volúmenes. Al crear un volumen, Trident obtiene primero el conjunto de pools de almacenamiento para la clase de almacenamiento de ese volumen y, si especifica un protocolo para el volumen, Trident quita los pools de almacenamiento que no pueden proporcionar el protocolo solicitado (por ejemplo, un back-end NetApp HCI/SolidFire no puede proporcionar un volumen basado en archivos, mientras que un back-end NAS de ONTAP no puede ofrecer un volumen basado en bloques). Trident aleatoriza el orden de este conjunto resultante para facilitar una distribución uniforme de los volúmenes y, luego, repite a través del mismo, intentando aprovisionar el volumen en cada pool de almacenamiento. Si se produce correctamente en una, vuelve con éxito y registra los fallos encontrados en el proceso. Trident devuelve un fallo **solo si** no proporciona en **all** los pools de almacenamiento disponibles para la clase de almacenamiento y el protocolo solicitados.

### Copias de Snapshot de volumen

Obtenga más información sobre cómo Trident maneja la creación de snapshots de volúmenes para sus controladores.

#### Obtenga información acerca de la creación de snapshots de volúmenes

- Para la `ontap-nas`, `ontap-san`, `gcp-cvs`, y `azure-netapp-files` Controladores, cada volumen persistente (PV) se asigna a una FlexVol. Como resultado, las copias de Snapshot de volumen se crean como copias de Snapshot de NetApp. La tecnología Snapshot de NetApp ofrece una mayor estabilidad, escalabilidad, capacidad de recuperación y rendimiento que la tecnología snapshot de la competencia. Estas copias Snapshot son extremadamente eficientes, tanto en el tiempo necesario para crearlas como en el espacio de almacenamiento.
- Para la `ontap-nas-flexgroup` Cada controlador, cada volumen persistente (PV) se asigna a una FlexGroup. Como resultado, las copias de Snapshot de volumen se crean como copias de Snapshot de FlexGroup de NetApp. La tecnología Snapshot de NetApp ofrece una mayor estabilidad, escalabilidad, capacidad de recuperación y rendimiento que la tecnología snapshot de la competencia. Estas copias Snapshot son extremadamente eficientes, tanto en el tiempo necesario para crearlas como en el espacio de almacenamiento.
- Para la `ontap-san-economy` Controlador, VP se asigna a las LUN creadas en los FlexVols compartidos. Las copias Snapshot Volumede VP realizan FlexClones del LUN asociado. La tecnología FlexClone de ONTAP permite crear copias de incluso los conjuntos de datos más grandes casi al instante. Las copias comparten bloques de datos con sus padres, sin consumir almacenamiento, excepto lo que se necesita para los metadatos.
- Para la `solidfire-san` Cada controlador, cada VP asigna una LUN creada en el software NetApp Element/clúster HCI de NetApp. Las copias Snapshot de volumen están representadas por copias

Snapshot de Element de la LUN subyacente. Estas copias Snapshot son copias puntuales y solo ocupan una pequeña cantidad de recursos y espacio del sistema.

- Cuando trabajan con los `ontap-nas` controladores y `ontap-san`, las copias Snapshot de ONTAP son copias puntuales de la FlexVol y consumen espacio en la propia FlexVol. Esto puede dar como resultado la cantidad de espacio editable en el volumen para reducirlo con el tiempo a medida que se crean y se programan las copias Snapshot. Una forma sencilla de abordar esto es aumentar el volumen mediante el cambio de tamaño a través de Kubernetes. Otra opción es eliminar las snapshots que ya no son necesarias. Cuando se elimina una snapshot de volumen creada mediante Kubernetes, Trident elimina la snapshot de ONTAP asociada. También se pueden eliminar las copias de Snapshot de ONTAP que no se crearon con Kubernetes.

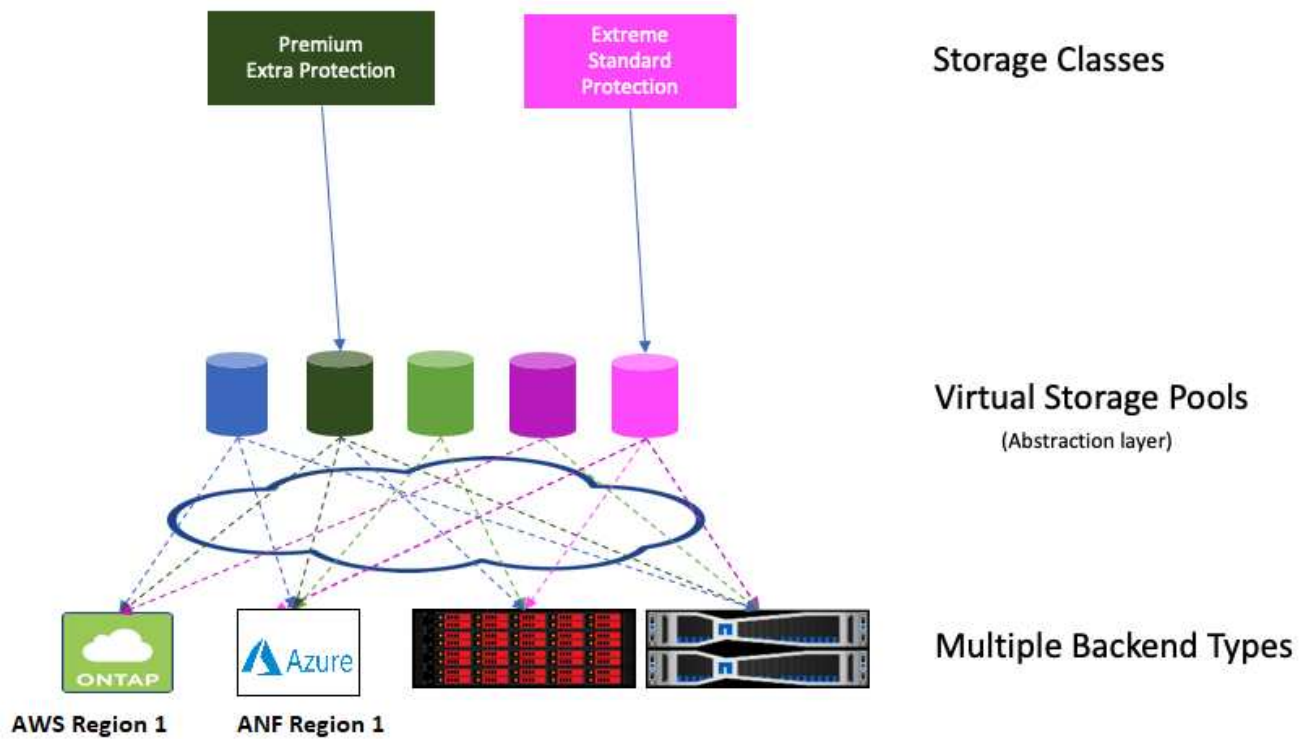
Con Trident, puede usar VolumeSnapshots para crear nuevos VP a partir de ellos. La creación de VP a partir de estas snapshots se realiza usando la tecnología FlexClone para los back-ends de ONTAP y CVS compatibles. Cuando se crea un volumen persistente a partir de una copia Snapshot, el volumen de backup es FlexClone del volumen principal de la copia Snapshot. `solidfire-san`` El controlador usa clones de volúmenes del software Element para crear VP a partir de snapshots. Aquí se crea un clon a partir de la copia de Snapshot de Element.

## **Pools virtuales**

Los pools virtuales proporcionan una capa de abstracción entre los back-ends de almacenamiento de Trident y Kubernetes `StorageClasses`. Permiten a un administrador definir aspectos, como la ubicación, el rendimiento y la protección para cada backend de una manera común e independiente del backend sin `StorageClass` especificar qué backend físico, pool de backend o tipo de backend utilizar para cumplir con los criterios deseados.

### **Más información sobre los pools virtuales**

El administrador de almacenamiento puede definir pools virtuales en cualquiera de los back-ends de Trident en un archivo de definición JSON o YAML.



Cualquier aspecto especificado fuera de la lista de pools virtuales es global para el back-end y se aplicará a todos los pools virtuales, mientras que cada pool virtual puede especificar uno o más aspectos individualmente (reemplazar cualquier aspecto back-end-global).



- Al definir los pools virtuales, no intente reorganizar el orden de los pools virtuales existentes en una definición de back-end.
- Se aconseja modificar los atributos de un pool virtual existente. Debe definir un nuevo pool virtual para realizar cambios.

La mayoría de los aspectos se especifican en términos específicos del back-end. Lo más importante es que los valores de aspecto no se exponen fuera del controlador del backend y no están disponibles para coincidir en `StorageClasses`. En su lugar, el administrador define una o varias etiquetas para cada pool virtual. Cada etiqueta es una pareja clave:valor y las etiquetas pueden ser comunes en los back-ends únicos. Al igual que en los aspectos, las etiquetas se pueden especificar por grupo o globalmente en el backend. A diferencia de los aspectos, que tienen nombres y valores predefinidos, el administrador tiene la total discreción de definir claves y valores de etiqueta según sea necesario. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

1. `StorageClass` identifica el pool virtual que se debe utilizar haciendo referencia a las etiquetas dentro de un parámetro de selector. Los selectores de pools virtuales admiten los siguientes operadores:

Operador	Ejemplo	El valor de etiqueta de un pool debe:
=	rendimiento=premium	Coincidencia
!=	rendimiento!=extremo	No coincide
in	ubicación en (este, oeste)	Esté en el conjunto de valores

Operador	Ejemplo	El valor de etiqueta de un pool debe:
<code>notin</code>	rendimiento de la muesca (plata, bronce)	No esté en el conjunto de valores
<code>&lt;key&gt;</code>	protección	Existe con cualquier valor
<code>!&lt;key&gt;</code>	!protección	No existe

## Los grupos de acceso de volúmenes

Obtenga más información sobre cómo utiliza Trident ["los grupos de acceso de volúmenes"](#) .



Ignore esta sección si está utilizando CHAP, que se recomienda para simplificar la gestión y evitar el límite de escalado descrito a continuación. Además, si utiliza Trident en modo CSI, puede ignorar esta sección. Trident utiliza CHAP cuando se instala como un proveedor de CSI mejorado.

### Obtenga información acerca de los grupos de acceso de volúmenes

Trident puede usar grupos de acceso de volúmenes para controlar el acceso a los volúmenes que aprovisiona. Si CHAP está deshabilitado, espera encontrar un grupo de acceso llamado `trident` a menos que especifique uno o más ID de grupo de acceso en la configuración.

Mientras que Trident asocia nuevos volúmenes con los grupos de acceso configurados, no crea ni gestiona ellos mismos grupos de acceso. Los grupos de acceso deben existir antes de que el back-end de almacenamiento se añada a Trident y deben contener los IQN iSCSI de cada nodo en el clúster de Kubernetes, que podrían montar los volúmenes aprovisionados por ese back-end. En la mayoría de las instalaciones, esto incluye todos los nodos de trabajo del clúster.

Para los clústeres de Kubernetes con más de 64 nodos, se deben usar varios grupos de acceso. Cada grupo de acceso puede contener hasta 64 IQN, y cada volumen puede pertenecer a cuatro grupos de acceso. Con un máximo de cuatro grupos de acceso configurados, cualquier nodo de un clúster con un tamaño de hasta 256 nodos podrá acceder a cualquier volumen. Para conocer los límites más recientes sobre los grupos de acceso de volúmenes, consulte ["aquí"](#).

Si está modificando la configuración desde una que esté utilizando el valor predeterminado `trident` Incluya el ID de para uno que utilice también otros `trident` grupo de acceso de la lista.

## Inicio rápido para Trident

Puede instalar Trident y empezar a gestionar los recursos de almacenamiento en unos pocos pasos. Antes de empezar, revise ["Requisitos de Trident"](#).



Para Docker, consulte ["Trident para Docker"](#).



### 1 Instale Trident

Trident ofrece varios métodos de instalación y modos optimizados para una variedad de entornos y organizaciones.

["Instale Trident"](#)

2

### Prepare el nodo de trabajo

Todos los nodos de trabajadores del clúster de Kubernetes deben poder montar los volúmenes que haya aprovisionado para los pods.

["Prepare el nodo de trabajo"](#)

3

### Cree un back-end

Un back-end define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él.

["Configurar un backend"](#) de su sistema de almacenamiento

4

### Cree una clase de almacenamiento de Kubernetes

El objeto Kubernetes StorageClass especifica Trident como el aprovisionador y le permite crear una clase de almacenamiento para aprovisionar volúmenes con atributos personalizables. Trident crea una clase de almacenamiento correspondiente para los objetos de Kubernetes que especifica el aprovisionador de Trident.

["Cree una clase de almacenamiento"](#)

5

### Aprovisione un volumen

Un *PersistentVolume* (PV) es un recurso de almacenamiento físico aprovisionado por el administrador del clúster en un clúster de Kubernetes. *PersistentVolumeClaim* (RVP) es una solicitud para acceder al volumen persistente en el clúster.

Cree un volumen persistente (VP) y una reclamación de volumen persistente (RVP) que utilice el tipo de almacenamiento de Kubernetes configurado para solicitar acceso al VP. A continuación, puede montar el VP en un pod.

["Aprovisione un volumen"](#)

## El futuro

Ahora puede añadir back-ends adicionales, gestionar clases de almacenamiento, gestionar back-ends y realizar operaciones de volumen.

## Requisitos

Antes de instalar Trident, debe revisar estos requisitos generales del sistema. Es posible que los back-ends específicos tengan requisitos adicionales.

## Información crítica sobre Trident

Debe leer la siguiente información crítica sobre Trident.

## <strong>Información crítica sobre Trident </strong>

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin `multivía` o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Front-ends compatibles (orquestadores)

Trident admite varios motores de contenedor y orquestadores, entre los que se incluyen los siguientes:

- Anthos on-premises (VMware) y Anthos en 1,16 básico
- Kubernetes 1,25 - 1,31
- OpenShift 4,10 - 4,17
- Rancher Kubernetes Engine 2 (RKE2) v1.28.5+rke2r1

El operador Trident es compatible con las siguientes versiones:

- Anthos on-premises (VMware) y Anthos en 1,16 básico
- Kubernetes 1,25 - 1,31
- OpenShift 4,10 - 4,17
- Rancher Kubernetes Engine 2 (RKE2) v1.28.5+rke2r1

Trident también funciona con una gran cantidad de ofertas de Kubernetes totalmente gestionadas y autogestionadas, como Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Services (EKS), Azure Kubernetes Service (AKS), Mirantis Kubernetes Engine (MKE) y la cartera de VMware Tanzu.

Trident y ONTAP se pueden utilizar como proveedor de almacenamiento para ["Virt de KubeVirt"](#).



Antes de actualizar un clúster de Kubernetes de la versión 1,24 a la versión 1,25 o una versión posterior que tenga instalado Trident, consulte ["Actualizar una instalación Helm"](#).

## Back-ends compatibles (almacenamiento)

Para utilizar Trident, se necesitan uno o varios de los siguientes back-ends admitidos:

- Amazon FSX para ONTAP de NetApp
- Azure NetApp Files
- Cloud Volumes ONTAP
- NetApp Volumes para Google Cloud
- FAS/AFF/Seleccione 9.5 o posterior

- Cabina All SAN de NetApp (ASA)
- Software HCI/Element de NetApp 11 o posterior

## Requisitos de funciones

En la tabla siguiente se resumen las funciones disponibles con este lanzamiento de Trident y las versiones de Kubernetes compatibles.

Función	La versión de Kubernetes	¿Se requieren puertos de funciones?
Trident	1,25 - 1,31	No
Snapshots de volumen	1,25 - 1,31	No
RVP desde snapshots de volumen	1,25 - 1,31	No
Cambio de tamaño del VP de iSCSI	1,25 - 1,31	No
CHAP bidireccional de ONTAP	1,25 - 1,31	No
Políticas de exportación dinámicas	1,25 - 1,31	No
Operador de Trident	1,25 - 1,31	No
Topología CSI	1,25 - 1,31	No

## Se probaron sistemas operativos host

Aunque Trident no admite oficialmente sistemas operativos específicos, se sabe que los siguientes funcionan:

- Versiones de RedHat CoreOS (RHCOS) compatibles con OpenShift Container Platform (AMD64 y ARM64)
- RHEL 8+ (AMD64 Y ARM64)



NVMe/TCP requiere RHEL 9 o posterior.

- Ubuntu 22,04 o posterior (AMD64 y ARM64)
- Windows Server 2022

De forma predeterminada, Trident se ejecuta en un contenedor y, por lo tanto, se ejecuta en cualquier trabajador Linux. Sin embargo, estos trabajadores deben poder montar los volúmenes que proporciona Trident con el cliente NFS estándar o el iniciador de iSCSI, en función de los back-ends que utilice.

La `tridentctl` Utility también se ejecuta en cualquiera de estas distribuciones de Linux.

## Configuración de hosts

Todos los nodos de trabajadores del clúster de Kubernetes deben poder montar los volúmenes que haya

aprovisionado para los pods. Para preparar los nodos de trabajo, debe instalar las herramientas NFS, iSCSI o NVMe según la selección de controladores.

["Prepare el nodo de trabajo"](#)

## Configuración del sistema de almacenamiento

Es posible que Trident requiera cambios en un sistema de almacenamiento antes de que la configuración de back-end pueda utilizarlo.

["Configurar los back-ends"](#)

## Puertos Trident

Trident requiere acceso a puertos específicos para la comunicación.

["Puertos Trident"](#)

## Imágenes de contenedor y las versiones de Kubernetes correspondientes

En el caso de instalaciones de aire acondicionado, la siguiente lista es una referencia de las imágenes de contenedores necesarias para instalar Trident. Utilice `tridentctl images` el comando para verificar la lista de imágenes de contenedor necesarias.

Versiones de Kubernetes	Imagen de contenedor
v1.25.0, v1.26.0, v1.27.0, v1.28.0, v1.29.0, v1.30.0 y v1.31.0	<ul style="list-style-type: none"><li>• <code>docker.io/netapp/trident:24.10.0</code></li><li>• <code>docker.io/netapp/trident-autosupport:24,10</code></li><li>• <code>registry.k8s.io/sig-storage/csi-provisioner:v5,1.0</code></li><li>• <code>registry.k8s.io/sig-storage/csi-attacher:v4,7.0</code></li><li>• <code>registry.k8s.io/sig-storage/csi-resizer:v1.12.0</code></li><li>• <code>registry.k8s.io/sig-storage/csi-snapshotter:v8,1.0</code></li><li>• <code>registry.k8s.io/sig-storage/csi-node-driver-registrador:v2.12.0</code></li><li>• <code>docker.io/netapp/trident-operator:24.10.0</code> (opcional)</li></ul>



# Instale Trident

## Obtenga información acerca de la instalación de Trident

Para garantizar que Trident se puede instalar en una amplia variedad de entornos y organizaciones, NetApp ofrece varias opciones de instalación. Puede instalar Trident usando el operador Trident (manualmente o usando Helm) o con `tridentctl`. En este tema se proporciona información importante para seleccionar el proceso de instalación adecuado.

### Información crítica sobre Trident 24,06

Debe leer la siguiente información crítica sobre Trident.

#### **Información crítica sobre Trident**

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin `multivía` o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

### Antes de empezar

Independientemente de la ruta de instalación, debe tener:

- Privilegios completos en un clúster de Kubernetes compatible que ejecuta una versión compatible de Kubernetes y requisitos de funciones habilitados. Revise la "[requisitos](#)" para obtener más detalles.
- Acceso a un sistema de almacenamiento de NetApp compatible.
- Capacidad para montar volúmenes de todos los nodos de trabajo de Kubernetes.
- Un host Linux con `kubect1` (o. `oc`, Si está utilizando OpenShift) instalado y configurado para administrar el clúster de Kubernetes que desea utilizar.
- La `KUBECONFIG` Variable de entorno establecida en el clúster de Kubernetes.
- Si utiliza Kubernetes con Docker Enterprise, "[Siga sus pasos para habilitar el acceso a la CLI](#)".



Si usted no se ha familiarizado con el "[conceptos básicos](#)", ahora es un gran momento para hacerlo.

## Elija el método de instalación

Seleccione el método de instalación adecuado. También debe revisar las consideraciones de ["moverse entre métodos"](#) antes de tomar su decisión.

### Utilice el operador Trident

Tanto si se implementa manualmente como si se utiliza Helm, el operador Trident es una excelente manera de simplificar la instalación y administrar dinámicamente los recursos de Trident. Incluso puede ["Personalice la implementación del operador de Trident"](#) utilizar los atributos en el `TridentOrchestrator` recurso personalizado (CR).

Algunas de las ventajas de usar el operador Trident son:

#### Creación de objetos de **Trident.**

El operador Trident crea automáticamente los siguientes objetos para la versión de Kubernetes.

- ServiceAccount para el operador
- ClusterRole y ClusterRoleBinding a la cuenta de servicio
- Dedicated PodSecurityPolicy (para Kubernetes 1.25 y versiones anteriores)
- El propio operador

#### **Contabilidad de recursos**

El operador Trident en el ámbito del clúster gestiona los recursos asociados con una instalación de Trident en el nivel del clúster. Esto mitiga los errores que pueden producirse al mantener los recursos de ámbito de cluster mediante un operador de ámbito de espacio de nombres. Esto es esencial para la reparación automática y la aplicación de parches.

#### **de capeel de curación de las Ouna**

El operador supervisa la instalación de Trident y toma medidas activas para solucionar problemas, como cuando se elimina el despliegue o se modifica accidentalmente. Se crea un `trident-operator-  
<generated-id>` pod que asocia un `TridentOrchestrator` CR a una instalación de Trident. Esto garantiza que solo haya una instancia de Trident en el clúster y controla su configuración, asegurándose de que la instalación sea idempotente. Cuando se realizan cambios en la instalación (como eliminar el despliegue o el conjunto de nodos), el operador los identifica y los corrige individualmente.

## <strong>® actualizaciones en la </strong> existente

Puede actualizar fácilmente una implementación existente con el operador. Sólo tiene que editar el `TridentOrchestrator` CR para realizar actualizaciones de una instalación.

Por ejemplo, considere un escenario en el que debe activar Trident para generar registros de depuración. Para ello, aplique un parche `TridentOrchestrator` a para establecer `spec.debug` en `true`:

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

Después `TridentOrchestrator` se actualiza, el operador procesa las actualizaciones y parches de la instalación existente. Esto podría desencadenar la creación de nuevos pods para modificar la instalación en consecuencia.

## <strong>Clean reinstallation</strong>

El operador Trident en el ámbito del clúster permite eliminar sin problemas los recursos del ámbito del clúster. Los usuarios pueden desinstalar completamente Trident y reinstalar fácilmente.

## Mejora a <strong> de Kubernetes a mano </strong>

Cuando se actualiza la versión de Kubernetes del clúster a una versión compatible, el operador actualiza una instalación existente de Trident automáticamente y la cambia para garantizar que cumple con los requisitos de la versión de Kubernetes.



Si el clúster se actualiza a una versión no compatible, el operador impide la instalación de Trident. Si Trident ya se ha instalado con el operador, se muestra una advertencia para indicar que Trident está instalado en una versión de Kubernetes no compatible.

## Uso `tridentctl`

Si tiene un despliegue existente que debe actualizarse o si está buscando personalizar altamente su despliegue, debe considerar `tridentctl`. Este es el método convencional de poner en marcha Trident.

Puede generar los manifiestos para los recursos de Trident. Esto incluye la puesta en marcha, el inicio de datos, la cuenta de servicio y la función de clúster que crea Trident como parte de su instalación.



A partir de la versión 22,04, las claves AES ya no se regenerarán cada vez que se instale Trident. Con esta versión, Trident instalará un nuevo objeto secreto que persiste en todas las instalaciones. Esto significa que `tridentctl` en 22,04 se pueden desinstalar versiones anteriores de Trident, pero las versiones anteriores no pueden desinstalar instalaciones de 22,04. Seleccione la instalación *method* adecuada.

## Elija el modo de instalación

Determine el proceso de implementación según el *installation mode* (Standard, Offline o Remote) requerido por su organización.

### Instalación estándar

Esta es la forma más fácil de instalar Trident y funciona en la mayoría de entornos que no imponen restricciones de red. El modo de instalación estándar utiliza registros predeterminados para almacenar (registry.k8s.io`las imágenes Trident (`docker.io) y CSI ) necesarias.

Cuando utilice el modo estándar, el instalador de Trident:

- Obtiene las imágenes del contenedor por Internet
- Crea un inicio de nodo o una implementación, lo que aumenta la velocidad de giro de los pods de Trident en todos los nodos elegibles del clúster de Kubernetes

### Instalación sin conexión

Es posible que se requiera el modo de instalación sin conexión en una ubicación segura o con un sistema de activación por aire. En este escenario, puede crear un único registro privado duplicado o dos registros reflejados para almacenar las imágenes Trident y CSI necesarias.



Independientemente de la configuración del registro, las imágenes CSI deben residir en un registro.

### Instalación remota

A continuación se ofrece una descripción general de alto nivel del proceso de instalación remota:

- Implemente la versión adecuada de `kubectl` en el equipo remoto desde donde desea implementar Trident.
- Copie los archivos de configuración del clúster de Kubernetes y establezca el `KUBECONFIG` variable de entorno en el equipo remoto.
- Inicie un `kubectl get nodes` Comando para verificar que puede conectarse al clúster de Kubernetes necesario.
- Complete la implementación desde la máquina remota mediante los pasos de instalación estándar.

## Seleccione el proceso según el método y el modo

Después de tomar sus decisiones, seleccione el proceso apropiado.

Método	Modo de instalación
Operador de Trident (manualmente)	"Instalación estándar" "Instalación sin conexión"
Operador Trident (Helm)	"Instalación estándar" "Instalación sin conexión"
<code>tridentctl</code>	"Instalación estándar o sin conexión"

## Moverse entre los métodos de instalación

Puede decidir cambiar el método de instalación. Antes de hacerlo, tenga en cuenta lo siguiente:

- Utilice siempre el mismo método para instalar y desinstalar Trident. Si ha desplegado con `tridentctl`, debe utilizar la versión apropiada del `tridentctl` binario para desinstalar Trident. Del mismo modo, si está desplegando con el operador, debe editar el `TridentOrchestrator` CR y configurar `spec.uninstall=true` la desinstalación de Trident.
- Si tiene un despliegue basado en el operador que desea eliminar y utilizar en su lugar `tridentctl` para implementar Trident, primero debe editar `TridentOrchestrator` y establecer `spec.uninstall=true` para desinstalar Trident. A continuación, suprima `TridentOrchestrator` y despliegue del operador. A continuación, puede instalar utilizando `tridentctl`.
- Si tiene una puesta en marcha manual basada en el operador y desea utilizar la puesta en marcha del operador de Trident basado en Helm, primero debe desinstalar manualmente al operador y, a continuación, llevar a cabo la instalación de Helm. De este modo, Helm puede poner en marcha el operador Trident con las etiquetas y anotaciones necesarias. Si no lo hace, la puesta en marcha del operador de Trident basado en Helm generará un error de validación de la etiqueta y un error de validación de la anotación. Si usted tiene un `'tridentctl'`La implementación basada en , puede utilizar la puesta en marcha basada en Helm sin que se produzcan problemas.

## Otras opciones de configuración conocidas

Al instalar Trident en productos de la cartera de VMware Tanzu:

- El clúster debe admitir cargas de trabajo con privilegios.
- La `--kubelet-dir` el indicador se debe establecer en la ubicación del directorio kubelet. De forma predeterminada, esta es `/var/vcap/data/kubelet`.

Especificación de la ubicación del kubelet mediante `--kubelet-dir` Sabe que funciona para el operador, Helm y `tridentctl` implementaciones.

## Realice la instalación mediante el operador Trident

### Implemente manualmente el operador de Trident (modo estándar)

Puede implementar manualmente el operador Trident para instalar Trident. Este proceso se aplica a instalaciones en las que las imágenes de contenedor requeridas por Trident no se almacenan en un registro privado. Si tiene un registro de imágenes privado, utilice el ["proceso de puesta en marcha sin conexión"](#).

### Información crítica sobre Trident 24,10

Debe leer la siguiente información crítica sobre Trident.

## <strong>Información crítica sobre Trident </strong>

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin `multivía` o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Implemente manualmente el operador de Trident e instale Trident

Revisar "[descripción general de la instalación](#)" para asegurarse de cumplir con los requisitos previos de instalación y seleccionar la opción de instalación correcta para el entorno.

### Antes de empezar

Antes de iniciar la instalación, inicie sesión en el host Linux y compruebe que esté gestionando un trabajo, "[Clúster de Kubernetes compatible](#)" y que tenga los privilegios necesarios.



Con OpenShift, utilícelo `oc` en lugar de `kubectl` en todos los ejemplos que siguen, e inicie sesión como **system:admin** primero ejecutando `oc login -u system:admin` o `oc login -u kube-admin`.

1. Compruebe su versión de Kubernetes:

```
kubectl version
```

2. Comprobar los privilegios de administrador de clúster:

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. Compruebe que puede iniciar un pod que utilice una imagen de Docker Hub para llegar al sistema de almacenamiento a través de la red de pod:

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### Paso 1: Descargue el paquete de instalación de Trident

El paquete de instalación de Trident contiene todo lo necesario para implementar el operador Trident e instalar Trident. Descargue y extraiga la última versión del instalador de Trident de "[La sección Assets de GitHub](#)".

```
wget https://github.com/NetApp/trident/releases/download/v24.10.0/trident-
installer-24.10.0.tar.gz
tar -xf trident-installer-24.10.0.tar.gz
cd trident-installer
```

### Paso 2: Cree la TridentOrchestrator CRD

Cree la TridentOrchestrator definición de recursos personalizados (CRD). Posteriormente, creará TridentOrchestrator recursos personalizados. Utilice la versión YAML de CRD adecuada en `deploy/crds` para crear la TridentOrchestrator CRD.

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

### Paso 3: Ponga en marcha el operador de Trident

El instalador de Trident proporciona un archivo de paquete que se puede utilizar para instalar el operador y crear objetos asociados. El archivo `bundle` es una manera fácil de implementar el operador e instalar Trident usando una configuración predeterminada.

- Para los clústeres que ejecutan Kubernetes 1,24, utilice `bundle_pre_1_25.yaml`.
- Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice `bundle_post_1_25.yaml`.

### Antes de empezar

- De forma predeterminada, el instalador de Trident implementa el operador en la `trident` espacio de nombres. Si la `trident` el espacio de nombres no existe, créelo con:

```
kubectl apply -f deploy/namespace.yaml
```

- Para implementar el operador en un espacio de nombres distinto del `trident` espacio de nombres, actualización `serviceaccount.yaml`, `clusterrolebinding.yaml` y `operator.yaml` y genere el archivo del paquete con el `kustomization.yaml`.

- a. Cree el `kustomization.yaml` con el siguiente comando donde está `<bundle.yaml>`  
`bundle_pre_1_25.yaml` o `bundle_post_1_25.yaml` Según su versión de Kubernetes.

```
cp deploy/kustomization_<bundle.yaml> deploy/kustomization.yaml
```

- b. Compile el paquete con el siguiente comando donde está `<bundle.yaml>` `bundle_pre_1_25.yaml` o `bundle_post_1_25.yaml` Según su versión de Kubernetes.

```
kubectl kustomize deploy/ > deploy/<bundle.yaml>
```

## Pasos

1. Crear los recursos e implementar el operador:

```
kubectl create -f deploy/<bundle.yaml>
```

2. Compruebe que se han creado el operador, el despliegue y los replicaset.

```
kubectl get all -n <operator-namespace>
```



Solo debe haber **una instancia** del operador en un clúster de Kubernetes. No cree varias implementaciones del operador Trident.

### Paso 4: Cree el `TridentOrchestrator` E instale Trident

Ahora puede crear `TridentOrchestrator` e instalar Trident. Opcionalmente, puede ["Personalice su instalación de Trident"](#) utilizar los atributos de la `TridentOrchestrator` especificación.



```

kubect1 create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubect1 describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Spec:
  Debug:       true
  Namespace:   trident
  nodePrep:
    - iscsi
Status:
  Current Installation Params:
    IPv6:                false
    Autosupport Hostname:
    Autosupport Image:   netapp/trident-autosupport:24.10
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:               true
    Image Pull Secrets:
    Image Registry:
    k8sTimeout:         30
    Kubelet Dir:        /var/lib/kubelet
    Log Format:          text
    Silence Autosupport: false
    Trident Image:      netapp/trident:24.10.0
  Message:              Trident installed Namespace:
trident
  Status:               Installed
  Version:              v24.10.0
Events:
  Type Reason Age From Message ---- -
  Installing 74s trident-operator.netapp.io Installing Trident Normal
  Installed 67s trident-operator.netapp.io Trident installed

```

## Compruebe la instalación

Existen varias formas de verificar su instalación.

## Uso `TridentOrchestrator` estado

El estado de `TridentOrchestrator` indica si la instalación se realizó correctamente y muestra la versión de Trident instalada. Durante la instalación, el estado de `TridentOrchestrator` cambia de `Installing` para `Installed`. Si observa la `Failed` y el operador no puede recuperarse por sí solo, "[compruebe los registros](#)".

Estado	Descripción
Instalación	El operador está instalando Trident con este <code>TridentOrchestrator</code> CR.
Instalado	Trident se ha instalado correctamente.
Desinstalando	El operador está desinstalando Trident, porque <code>spec.uninstall=true</code> .
Desinstalado	Trident se ha desinstalado.
Error	El operador no ha podido instalar, aplicar parches, actualizar o desinstalar Trident; el operador intentará automáticamente recuperarse de este estado. Si este estado continúa, necesitará solucionar problemas.
Actualizando	El operador está actualizando una instalación existente.
Error	La <code>TridentOrchestrator</code> no se utiliza. Otro ya existe.

## Uso del estado de creación de pod

Puede confirmar si la instalación de Trident ha finalizado revisando el estado de los pods creados:

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

NAME	READY	STATUS	RESTARTS
trident-controller-7d466bf5c7-v4cpw 1m	6/6	Running	0
trident-node-linux-mr6zc 1m	2/2	Running	0
trident-node-linux-xrp7w 1m	2/2	Running	0
trident-node-linux-zh2jt 1m	2/2	Running	0
trident-operator-766f7b8658-ldzsv 3m	1/1	Running	0

## Uso `tridentctl`

Puede utilizar `tridentctl` para comprobar la versión de Trident instalada.

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

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 24.10.0        | 24.10.0        |
+-----+-----+
```

## Implemente manualmente el operador Trident (modo sin conexión).

Puede implementar manualmente el operador Trident para instalar Trident. Este proceso se aplica a instalaciones en las que las imágenes de contenedor requeridas por Trident se almacenan en un registro privado. Si no dispone de un registro de imágenes privado, utilice el ["proceso de implementación estándar"](#).

### Información crítica sobre Trident 24,10

Debe leer la siguiente información crítica sobre Trident.

#### **Información crítica sobre Trident**

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin multivía o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Implemente manualmente el operador de Trident e instale Trident

Revisar ["descripción general de la instalación"](#) para asegurarse de cumplir con los requisitos previos de instalación y seleccionar la opción de instalación correcta para el entorno.

### Antes de empezar

Inicie sesión en el host Linux y compruebe que está gestionando un funcionamiento y ["Clúster de Kubernetes compatible"](#) y que tenga los privilegios necesarios.



Con OpenShift, utilícelo `oc` en lugar de `kubectl` en todos los ejemplos que siguen, e inicie sesión como **system:admin** primero ejecutando `oc login -u system:admin o. oc login -u kube-admin`.

1. Compruebe su versión de Kubernetes:

```
kubectl version
```

2. Comprobar los privilegios de administrador de clúster:

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. Compruebe que puede iniciar un pod que utilice una imagen de Docker Hub para llegar al sistema de almacenamiento a través de la red de pod:

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### Paso 1: Descargue el paquete de instalación de Trident

El paquete de instalación de Trident contiene todo lo necesario para implementar el operador Trident e instalar Trident. Descargue y extraiga la última versión del instalador de Trident de "[La sección Assets de GitHub](#)".

```
wget https://github.com/NetApp/trident/releases/download/v24.10.0/trident-
installer-24.10.0.tar.gz
tar -xf trident-installer-24.10.0.tar.gz
cd trident-installer
```

### Paso 2: Cree la TridentOrchestrator CRD

Cree la TridentOrchestrator definición de recursos personalizados (CRD). Posteriormente, creará TridentOrchestrator recursos personalizados. Utilice la versión YAML de CRD adecuada en `deploy/crds` para crear el TridentOrchestrator CRD:

```
kubectl create -f deploy/crds/<VERSION>.yaml
```

### Paso 3: Actualice la ubicación del registro en el operador

En `/deploy/operator.yaml`, actualice `image: docker.io/netapp/trident-operator:24.10.0` para reflejar la ubicación del registro de imágenes. "[Imágenes Trident y CSI](#)" Puede estar ubicado en un registro o registros diferentes, pero todas las imágenes CSI deben estar ubicadas en el mismo registro. Por ejemplo:

- `image: <your-registry>/trident-operator:24.10.0` si todas sus imágenes están ubicadas en un registro.
- `image: <your-registry>/netapp/trident-operator:24.10.0` Si su imagen Trident se

encuentra en un registro diferente de sus imágenes CSI.

#### Paso 4: Ponga en marcha el operador de Trident

El instalador de Trident proporciona un archivo de paquete que se puede utilizar para instalar el operador y crear objetos asociados. El archivo `bundle` es una manera fácil de implementar el operador e instalar Trident usando una configuración predeterminada.

- Para los clústeres que ejecutan Kubernetes 1,24, utilice `bundle_pre_1_25.yaml`.
- Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice `bundle_post_1_25.yaml`.

#### Antes de empezar

- De forma predeterminada, el instalador de Trident implementa el operador en la `trident` espacio de nombres. Si la `trident` el espacio de nombres no existe, créelo con:

```
kubectl apply -f deploy/namespace.yaml
```

- Para implementar el operador en un espacio de nombres distinto del `trident` espacio de nombres, actualización `serviceaccount.yaml`, `clusterrolebinding.yaml` y `operator.yaml` y genere el archivo del paquete con el `kustomization.yaml`.

- a. Cree el `kustomization.yaml` con el siguiente comando donde está `<bundle.yaml>` `bundle_pre_1_25.yaml` o `bundle_post_1_25.yaml` Según su versión de Kubernetes.

```
cp deploy/kustomization_<bundle.yaml> deploy/kustomization.yaml
```

- b. Compile el paquete con el siguiente comando donde está `<bundle.yaml>` `bundle_pre_1_25.yaml` o `bundle_post_1_25.yaml` Según su versión de Kubernetes.

```
kubectl kustomize deploy/ > deploy/<bundle.yaml>
```

#### Pasos

1. Crear los recursos e implementar el operador:

```
kubectl create -f deploy/<bundle.yaml>
```

2. Compruebe que se han creado el operador, el despliegue y los replicaset.

```
kubectl get all -n <operator-namespace>
```



Solo debe haber **una instancia** del operador en un clúster de Kubernetes. No cree varias implementaciones del operador Trident.

### Paso 5: Actualice la ubicación del registro de imágenes en el `TridentOrchestrator`

Su "Imágenes Trident y CSI" Se pueden ubicar en un registro o en diferentes registros, pero todas las imágenes CSI deben estar ubicadas en el mismo registro. Actualizar `deploy/crds/tridentorchestrator_cr.yaml` para agregar las especificaciones de ubicación adicionales basadas en la configuración de su registro.

#### Imágenes en un registro

```
imageRegistry: "<your-registry>"
autosupportImage: "<your-registry>/trident-autosupport:24.10"
tridentImage: "<your-registry>/trident:24.10.0"
```

#### Imágenes en diferentes registros

```
imageRegistry: "<your-registry>"
autosupportImage: "<your-registry>/trident-autosupport:24.10"
tridentImage: "<your-registry>/trident:24.10.0"
```

### Paso 6: Cree el `TridentOrchestrator` E instale Trident

Ahora puede crear `TridentOrchestrator` e instalar Trident. Si lo desea, puede "[Personalice su instalación de Trident](#)" utilizar los atributos de la `TridentOrchestrator` especificación. En el siguiente ejemplo se muestra una instalación donde las imágenes Trident y CSI se encuentran en diferentes registros.

```

kubect1 create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubect1 describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:  <none>
API Version:  trident.netapp.io/v1
Kind:         TridentOrchestrator
...
Spec:
  Autosupport Image: <your-registry>/trident-autosupport:24.10
  Debug:             true
  Image Registry:   <your-registry>
  Namespace:       trident
  Trident Image:    <your-registry>/trident:24.10.0
Status:
  Current Installation Params:
    IPv6:           false
    Autosupport Hostname:
    Autosupport Image: <your-registry>/trident-autosupport:24.10
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:          true
    Http Request Timeout: 90s
    Image Pull Secrets:
    Image Registry: <your-registry>
    k8sTimeout:     30
    Kubelet Dir:    /var/lib/kubelet
    Log Format:     text
    Probe Port:    17546
    Silence Autosupport: false
    Trident Image: <your-registry>/trident:24.10.0
  Message:         Trident installed
  Namespace:       trident
  Status:          Installed
  Version:         v24.10.0
Events:
  Type Reason Age From Message -----Normal
  Installing 74s trident-operator.netapp.io Installing Trident Normal
  Installed 67s trident-operator.netapp.io Trident installed

```

## Compruebe la instalación

Existen varias formas de verificar su instalación.

### Uso `TridentOrchestrator` estado

El estado de `TridentOrchestrator` Indica si la instalación se realizó correctamente y muestra la versión de Trident instalada. Durante la instalación, el estado de `TridentOrchestrator` cambia de `Installing` para `Installed`. Si observa la `Failed` y el operador no puede recuperarse por sí solo, "[compruebe los registros](#)".

Estado	Descripción
Instalación	El operador está instalando Trident con este <code>TridentOrchestrator CR</code> .
Instalado	Trident se ha instalado correctamente.
Desinstalando	El operador está desinstalando Trident, porque <code>spec.uninstall=true</code> .
Desinstalado	Trident se ha desinstalado.
Error	El operador no ha podido instalar, aplicar parches, actualizar o desinstalar Trident; el operador intentará automáticamente recuperarse de este estado. Si este estado continúa, necesitará solucionar problemas.
Actualizando	El operador está actualizando una instalación existente.
Error	La <code>TridentOrchestrator</code> no se utiliza. Otro ya existe.

### Uso del estado de creación de pod

Puede confirmar si la instalación de Trident ha finalizado revisando el estado de los pods creados:

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

NAME	READY	STATUS	RESTARTS
trident-controller-7d466bf5c7-v4cpw 1m	6/6	Running	0
trident-node-linux-mr6zc 1m	2/2	Running	0
trident-node-linux-xrp7w 1m	2/2	Running	0
trident-node-linux-zh2jt 1m	2/2	Running	0
trident-operator-766f7b8658-ldzsv 3m	1/1	Running	0



## Uso tridentctl

Puede utilizar `tridentctl` para comprobar la versión de Trident instalada.

```
./tridentctl -n trident version

+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 24.10.0       | 24.10.0       |
+-----+-----+
```

## Puesta en marcha del operador de Trident con Helm (modo estándar)

Puede desplegar el operador Trident e instalar Trident con Helm. Este proceso se aplica a instalaciones en las que las imágenes de contenedor requeridas por Trident no se almacenan en un registro privado. Si tiene un registro de imágenes privado, utilice el ["proceso de puesta en marcha sin conexión"](#).

### Información crítica sobre Trident 24,10

Debe leer la siguiente información crítica sobre Trident.

#### **Información crítica sobre Trident**

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin multivía o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Despliegue el operador Trident e instale Trident usando Helm

Usar Trident ["Carta del timón"](#) Es posible poner en marcha el operador de Trident e instalar Trident en un paso.

Revisar ["descripción general de la instalación"](#) para asegurarse de cumplir con los requisitos previos de instalación y seleccionar la opción de instalación correcta para el entorno.

### Antes de empezar

Además de la ["requisitos previos a la implementación"](#) que necesita ["Versión timón 3"](#).

### Pasos

## 1. Añada el repositorio Helm de Trident:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

## 2. Utilice `helm install` y especifique un nombre para la implementación como en el siguiente ejemplo, donde `100.2404.0` se encuentra la versión de Trident que está instalando.

```
helm install <name> netapp-trident/trident-operator --version 100.2410.0 --create-namespace --namespace <trident-namespace>
```



Si ya creó un espacio de nombres para Trident, el `--create-namespace` el parámetro no creará un espacio de nombres adicional.

Puede utilizar `helm list` para revisar detalles de la instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación, y el número de revisión.

## Pasar los datos de configuración durante la instalación

Existen dos formas de pasar los datos de configuración durante la instalación:

Opción	Descripción
<code>--values (o. -f)</code>	Especifique un archivo YAML con anulaciones. Esto se puede especificar varias veces y el archivo de la derecha tendrá prioridad.
<code>--set</code>	Especifique anulaciones en la línea de comandos.


Por ejemplo, para cambiar el valor predeterminado de `debug`, ejecute el siguiente comando donde `100.2410.0` es la versión de Trident que está instalando:

```
helm install <name> netapp-trident/trident-operator --version 100.2410.0 --create-namespace --namespace trident --set tridentDebug=true
```

## Opciones de configuración

Esta tabla y la `values.yaml` File, que forma parte del gráfico Helm, proporciona la lista de claves y sus valores predeterminados.

Opción	Descripción	Predeterminado
<code>nodeSelector</code>	Etiquetas de nodo para la asignación de pod	
<code>podAnnotations</code>	Anotaciones del pod	

Opción	Descripción	Predeterminado
deploymentAnnotations	Anotaciones de despliegue	
tolerations	Toleraciones para la asignación de POD	
affinity	Afinidad para la asignación de pod	<pre> affinity:   nodeAffinity:  requiredDuringSchedulingIgnoredDuringExecution:   nodeSelectorTerms:     - matchExpressions:       - key: kubernetes.io/arch         operator: In         values:           - arm64           - amd64       - key: kubernetes.io/os         operator: In         values:           - linux </pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>No elimine la afinidad predeterminada del archivo values.yaml. Cuando desee proporcionar una afinidad personalizada, amplíe la afinidad predeterminada.</p> </div>
tridentControllerPluginNodeSelector	Selectores de nodos adicionales para POD. Consulte <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> para obtener más detalles.	
tridentControllerPluginTolerations	Anula la toleración de Kubernetes en pods. Consulte <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> para obtener más detalles.	
tridentNodePluginNodeSelector	Selectores de nodos adicionales para POD. Consulte <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> para obtener más detalles.	

Opción	Descripción	Predeterminado
tridentNodePluginTolerations	Anula la toleración de Kubernetes en pods. Consulte <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> para obtener más detalles.	
imageRegistry	Identifica el registro de <code>trident-operator</code> , <code>trident</code> y otras imágenes. Déjelo vacío para aceptar el valor predeterminado. <b>IMPORTANTE:</b> Al instalar Trident en un repositorio privado, si está utilizando el <code>imageRegistry</code> conmutador para especificar la ubicación del repositorio, no lo utilice <code>/netapp/</code> en la ruta de acceso del repositorio.	""
imagePullPolicy	Establece la política de extracción de imágenes para el <code>trident-operator</code> .	IfNotPresent
imagePullSecrets	Establece los secretos de extracción de imágenes para el <code>trident-operator</code> , <code>trident</code> , y otras imágenes.	
kubeletDir	Permite anular la ubicación del host del estado interno de kubelet.	"/var/lib/kubelet"
operatorLogLevel	Permite establecer el nivel de registro del operador Trident en: <code>trace</code> , <code>debug</code> , <code>info</code> , <code>warn</code> , <code>error</code> , o <code>fatal</code> .	"info"
operatorDebug	Permite configurar en debug el nivel de registro del operador Trident.	true
operatorImage	Permite la sustitución completa de la imagen durante <code>trident-operator</code> .	""
operatorImageTag	Permite sobrescribir la etiqueta del <code>trident-operator</code> imagen.	""
tridentIPv6	Permite permitir que Trident funcione en clústeres de IPv6.	false
tridentK8sTimeout	Anula el tiempo de espera predeterminado de 30 segundos para la mayoría de las operaciones de la API de Kubernetes (si no es cero, en segundos).	0

Opción	Descripción	Predeterminado
tridentHttpRequestTimeout	Sustituye el timeout por defecto de 90 segundos para las solicitudes HTTP, con 0s ser una duración infinita para el timeout. No se permiten valores negativos.	"90s"
tridentSilenceAutoSupport	Permite deshabilitar la generación de informes periódicos de AutoSupport de Trident.	false
tridentAutoSupportImageTag	Permite sobrescribir la etiqueta de la imagen para el contenedor Trident AutoSupport.	<version>
tridentAutoSupportProxy	Permite al contenedor Trident AutoSupport llamar a casa a través de un proxy HTTP.	""
tridentLogFormat	Define el formato de registro de Trident (text `o `json).	"text"
tridentDisableAuditLog	Deshabilita el registrador de auditorías de Trident.	true
tridentLogLevel	Permite definir el nivel de log de Trident en: trace, , , , debug, info warn error O fatal.	"info"
tridentDebug	Permite establecer el nivel de registro de Trident en debug.	false
tridentLogWorkflows	Permite habilitar flujos de trabajo de Trident específicos para el registro de seguimiento o la supresión de registros.	""
tridentLogLayers	Permite activar capas de Trident específicas para el registro de rastreo o la supresión de registros.	""
tridentImage	Permite la sustitución completa de la imagen para Trident.	""
tridentImageTag	Permite sobrescribir la etiqueta de la imagen para Trident.	""
tridentProbePort	Permite sobrescribir el puerto predeterminado utilizado para las sondas de vida/preparación de Kubernetes.	""
windows	Permite instalar Trident en el nodo de trabajo de Windows.	false
enableForceDetach	Permite habilitar la función Forzar separación.	false

Opción	Descripción	Predeterminado
excludePodSecurityPolicy	Excluye la política de seguridad del pod del operador de la creación.	false
cloudProvider	Establezca en "Azure" Cuando se utilizan identidades gestionadas o una identidad de nube en un clúster de AKS. Establecer en «AWS» cuando se utiliza una identidad de nube en un clúster de EKS.	""
cloudIdentity	Defina la identidad de carga de trabajo («azure.workload.identity/client-id: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX») cuando utilice la identidad de cloud en un clúster de AKS. Establezca el rol de AWS IAM ('eks.amazonaws.com/role-arn: arn:aws:iam::123456:ROLE/Trident-ROLE') cuando utilice la identidad de cloud en un clúster de EKS.	""
iscsiSelfHealingInterval	El intervalo en el que se invoca la reparación automática de iSCSI.	5m0s
iscsiSelfHealingWaitTime	La duración después del cual la reparación automática de iSCSI inicia un intento de resolver una sesión obsoleta realizando un cierre de sesión y un inicio de sesión posterior.	7m0s
nodePrep	Permite a Trident preparar los nodos del clúster de Kubernetes para gestionar volúmenes mediante el protocolo de almacenamiento de datos especificado. <b>Actualmente, iscsi es el único valor soportado.</b>	

### Descripción de los pods de la controladora y los pods de nodo

Trident se ejecuta como un pod de controladora único, más un pod de nodo en cada nodo trabajador del clúster. El pod de nodo debe ejecutarse en cualquier host en el que desee potencialmente montar un volumen de Trident.

Kubernetes "[selectores de nodos](#)" y.. "[toleraciones y tintes](#)" se utilizan para restringir un pod para ejecutarse en un nodo concreto o preferido. Uso del "ControllerPlugin" y. NodePlugin, puede especificar restricciones y anulaciones.

- El complemento de la controladora se ocupa del aprovisionamiento y la gestión de volúmenes, como snapshots y redimensionamiento.

- El complemento de nodo se encarga de conectar el almacenamiento al nodo.

## Implementar el operador de Trident con Helm (modo sin conexión)

Puede desplegar el operador Trident e instalar Trident con Helm. Este proceso se aplica a instalaciones en las que las imágenes de contenedor requeridas por Trident se almacenan en un registro privado. Si no dispone de un registro de imágenes privado, utilice el ["proceso de implementación estándar"](#).

### Información crítica sobre Trident 24,10

Debe leer la siguiente información crítica sobre Trident.

#### **Información crítica sobre Trident**

- Kubernetes 1,31 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin `multivía` o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Despliegue el operador Trident e instale Trident usando Helm

Usar Trident ["Carta del timón"](#) Es posible poner en marcha el operador de Trident e instalar Trident en un paso.

Revisar ["descripción general de la instalación"](#) para asegurarse de cumplir con los requisitos previos de instalación y seleccionar la opción de instalación correcta para el entorno.

### Antes de empezar

Además de la ["requisitos previos a la implementación"](#) que necesita ["Versión timón 3"](#).



Al instalar Trident en un repositorio privado, si está utilizando el `imageRegistry` conmutador para especificar la ubicación del repositorio, no lo utilice `/netapp/` en la ruta de acceso del repositorio.

### Pasos

1. Añada el repositorio Helm de Trident:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Utilice `helm install` y especifique un nombre para el despliegue y la ubicación del registro de imágenes. ["Imágenes Trident y CSI"](#) Puede estar ubicado en un registro o registros diferentes, pero todas

las imágenes CSI deben estar ubicadas en el mismo registro. En los ejemplos, 100.2410.0 es la versión de Trident que está instalando.

### Imágenes en un registro

```
helm install <name> netapp-trident/trident-operator --version
100.2410.0 --set imageRegistry=<your-registry> --create-namespace
--namespace <trident-namespace> --set nodePrep={iscsi}
```

### Imágenes en diferentes registros

```
helm install <name> netapp-trident/trident-operator --version
100.2410.0 --set imageRegistry=<your-registry> --set
operatorImage=<your-registry>/trident-operator:24.10.0 --set
tridentAutosupportImage=<your-registry>/trident-autosupport:24.06
--set tridentImage=<your-registry>/trident:24.10.0 --create
-namespace --namespace <trident-namespace> --set nodePrep={iscsi}
```



Si ya creó un espacio de nombres para Trident, el `--create-namespace` el parámetro no creará un espacio de nombres adicional.

Puede utilizar `helm list` para revisar detalles de la instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación, y el número de revisión.

### Pasar los datos de configuración durante la instalación

Existen dos formas de pasar los datos de configuración durante la instalación:

Opción	Descripción
<code>--values (o. -f)</code>	Especifique un archivo YAML con anulaciones. Esto se puede especificar varias veces y el archivo de la derecha tendrá prioridad.
<code>--set</code>	Especifique anulaciones en la línea de comandos.

Por ejemplo, para cambiar el valor predeterminado de `debug`, ejecute el siguiente comando donde 100.2410.0 es la versión de Trident que está instalando:

```
helm install <name> netapp-trident/trident-operator --version 100.2410.0
--create-namespace --namespace trident --set tridentDebug=true
```

Para agregar el valor `nodePrep`, ejecute el siguiente comando:



```
helm install <name> netapp-trident/trident-operator --version 100.2406.0
--create-namespace --namespace trident --set nodePrep={iscsi}
```


## Opciones de configuración

Esta tabla y la `values.yaml` File, que forma parte del gráfico Helm, proporciona la lista de claves y sus valores predeterminados.



No elimine la afinidad predeterminada del archivo `values.yaml`. Cuando desee proporcionar una afinidad personalizada, amplíe la afinidad predeterminada.

Opción	Descripción	Predeterminado
<code>nodeSelector</code>	Etiquetas de nodo para la asignación de pod	
<code>podAnnotations</code>	Anotaciones del pod	
<code>deploymentAnnotations</code>	Anotaciones de despliegue	
<code>tolerations</code>	Toleraciones para la asignación de POD	

Opción	Descripción	Predeterminado
affinity	Afinidad para la asignación de pod	<pre> affinity:   nodeAffinity:      requiredDuringSchedulingIgnoredDuringExecution:        nodeSelectorTerms:         -           matchExpressions:             - key:               kubernetes.io/arch            operator: In             values:               - arm64               - amd64             - key:               kubernetes.io/os            operator: In             values:               - linux </pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>No elimine la afinidad predeterminada del archivo values.yaml. Cuando desee proporcionar una afinidad personalizada, amplíe la afinidad predeterminada.</p> </div>
tridentControllerPluginNodeSelector	Selectores de nodos adicionales para POD. Consulte <a href="#">"Descripción de los pods de la controladora y los pods de nodo"</a> para obtener más detalles.	
tridentControllerPluginTolerations	Anula la toleración de Kubernetes en pods. Consulte <a href="#">"Descripción de los pods de la controladora y los pods de nodo"</a> para obtener más detalles.	

Opción	Descripción	Predeterminado
<code>tridentNodePluginNodeSelector</code>	Selectores de nodos adicionales para POD. Consulte " <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> " para obtener más detalles.	
<code>tridentNodePluginTolerations</code>	Anula la toleración de Kubernetes en pods. Consulte " <a href="#">Descripción de los pods de la controladora y los pods de nodo</a> " para obtener más detalles.	
<code>imageRegistry</code>	Identifica el registro de <code>trident-operator</code> , <code>trident</code> y otras imágenes. Déjelo vacío para aceptar el valor predeterminado. <b>IMPORTANTE:</b> Al instalar Trident en un repositorio privado, si está utilizando el <code>imageRegistry</code> conmutador para especificar la ubicación del repositorio, no lo utilice <code>/netapp/</code> en la ruta de acceso del repositorio.	""
<code>imagePullPolicy</code>	Establece la política de extracción de imágenes para el <code>trident-operator</code> .	IfNotPresent
<code>imagePullSecrets</code>	Establece los secretos de extracción de imágenes para el <code>trident-operator</code> , <code>trident</code> , y otras imágenes.	
<code>kubeletDir</code>	Permite anular la ubicación del host del estado interno de kubelet.	<code>"/var/lib/kubelet"</code>
<code>operatorLogLevel</code>	Permite establecer el nivel de registro del operador Trident en: <code>trace</code> , <code>debug</code> , <code>info</code> , <code>warn</code> , <code>error</code> , o <code>fatal</code> .	<code>"info"</code>
<code>operatorDebug</code>	Permite configurar en debug el nivel de registro del operador Trident.	<code>true</code>
<code>operatorImage</code>	Permite la sustitución completa de la imagen durante <code>trident-operator</code> .	""
<code>operatorImageTag</code>	Permite sobrescribir la etiqueta del <code>trident-operator</code> imagen.	""
<code>tridentIPv6</code>	Permite permitir que Trident funcione en clústeres de IPv6.	<code>false</code>

Opción	Descripción	Predeterminado
<code>tridentK8sTimeout</code>	Anula el tiempo de espera predeterminado de 30 segundos para la mayoría de las operaciones de la API de Kubernetes (si no es cero, en segundos).	0
<code>tridentHttpRequestTimeout</code>	Sustituye el timeout por defecto de 90 segundos para las solicitudes HTTP, con 0s ser una duración infinita para el timeout. No se permiten valores negativos.	"90s"
<code>tridentSilenceAutosupport</code>	Permite deshabilitar la generación de informes periódicos de AutoSupport de Trident.	false
<code>tridentAutosupportImageTag</code>	Permite sobrescribir la etiqueta de la imagen para el contenedor Trident AutoSupport.	<version>
<code>tridentAutosupportProxy</code>	Permite al contenedor Trident AutoSupport llamar a casa a través de un proxy HTTP.	""
<code>tridentLogFormat</code>	Define el formato de registro de Trident (text`o`json).	"text"
<code>tridentDisableAuditLog</code>	Deshabilita el registrador de auditorías de Trident.	true
<code>tridentLogLevel</code>	Permite definir el nivel de log de Trident en: trace, , , , debug, info warn error O fatal.	"info"
<code>tridentDebug</code>	Permite establecer el nivel de registro de Trident en debug.	false
<code>tridentLogWorkflows</code>	Permite habilitar flujos de trabajo de Trident específicos para el registro de seguimiento o la supresión de registros.	""
<code>tridentLogLayers</code>	Permite activar capas de Trident específicas para el registro de rastreo o la supresión de registros.	""
<code>tridentImage</code>	Permite la sustitución completa de la imagen para Trident.	""
<code>tridentImageTag</code>	Permite sobrescribir la etiqueta de la imagen para Trident.	""
<code>tridentProbePort</code>	Permite sobrescribir el puerto predeterminado utilizado para las sondas de vida/preparación de Kubernetes.	""

Opción	Descripción	Predeterminado
windows	Permite instalar Trident en el nodo de trabajo de Windows.	false
enableForceDetach	Permite habilitar la función Forzar separación.	false
excludePodSecurityPolicy	Excluye la política de seguridad del pod del operador de la creación.	false
nodePrep	Permite a Trident preparar los nodos del clúster de Kubernetes para gestionar volúmenes mediante el protocolo de almacenamiento de datos especificado. <b>Actualmente, <code>iscsi</code> es el único valor soportado.</b>	

## Personalice la instalación del operador de Trident

El operador Trident le permite personalizar la instalación de Trident utilizando los atributos de la `TridentOrchestrator` especificación. Si desea personalizar la instalación más allá de lo que `TridentOrchestrator` permiten los argumentos, considere utilizar `tridentctl` para generar manifiestos YAML personalizados para modificarlos según sea necesario.

### Descripción de los pods de la controladora y los pods de nodo

Trident se ejecuta como un pod de controladora único, más un pod de nodo en cada nodo trabajador del clúster. El pod de nodo debe ejecutarse en cualquier host en el que desee potencialmente montar un volumen de Trident.

Kubernetes "[selectores de nodos](#)" y.. "[toleraciones y tintes](#)" se utilizan para restringir un pod para ejecutarse en un nodo concreto o preferido. Uso del "ControllerPlugin" y. `NodePlugin`, puede especificar restricciones y anulaciones.

- El complemento de la controladora se ocupa del aprovisionamiento y la gestión de volúmenes, como snapshots y redimensionamiento.
- El complemento de nodo se encarga de conectar el almacenamiento al nodo.

### Opciones de configuración



`spec.namespace` Se especifica en `TridentOrchestrator` para indicar el espacio de nombres donde se instala Trident. Este parámetro **no se puede actualizar después de instalar Trident**. Si lo intenta, el `TridentOrchestrator` estado cambia a `Failed`. La intención de Trident no es migrar entre espacios de nombres.

Esta tabla detalla `TridentOrchestrator` atributos.

Parámetro	Descripción	Predeterminado
namespace	Espacio de nombres para instalar Trident en	"default"
debug	Active la depuración para Trident	false
enableForceDetach	ontap-san, ontap-san-economy y ontap-nas-economy sólo. Funciona con cierre de nodos no controlado (NGN) de Kubernetes para conceder a los administradores de clústeres la capacidad de migrar de forma segura cargas de trabajo con volúmenes montados a nodos nuevos en caso de que un nodo se vuelva en mal estado.	false
windows	Ajuste a. true Permite la instalación en nodos de trabajo de Windows.	false
cloudProvider	Establezca en "Azure" Cuando se utilizan identidades gestionadas o una identidad de nube en un clúster de AKS. Establecer en «AWS» cuando se utiliza una identidad de nube en un clúster de EKS.	" "
cloudIdentity	Defina la identidad de carga de trabajo («azure.workload.identity/client-id: Xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx») cuando utilice la identidad de cloud en un clúster de AKS. Establezca el rol de AWS IAM ('eks.amazonaws.com/role-arn: arn:aws:iam::123456:ROLE/Trident-ROLE) cuando utilice la identidad de cloud en un clúster de EKS.	" "
IPv6	Instale Trident sobre IPv6	falso
k8sTimeout	Tiempo de espera para las operaciones de Kubernetes	30sec
silenceAutosupport	No envíe paquetes AutoSupport a NetApp automáticamente	false
autosupportImage	La imagen contenedora para telemetría AutoSupport	"netapp/trident-autosupport:24.10"
autosupportProxy	La dirección/puerto de un proxy para enviar AutoSupport Telemetría	"http://proxy.example.com:8888"
uninstall	Indicador utilizado para desinstalar Trident	false
logFormat	Formato de registro Trident que se va a utilizar [text,json]	"text"
tridentImage	Imagen Trident para instalar	"netapp/trident:24.10"
imageRegistry	Ruta de acceso al registro interno, del formato <registry FQDN>[:port][ /subpath]	"k8s.gcr.io" (Kubernetes 1,19 o posterior) o "quay.io/k8scsi"
kubeletDir	Ruta al directorio kubelet del host	"/var/lib/kubelet"

Parámetro	Descripción	Predeterminado
wipeout	Una lista de recursos que se deben eliminar para realizar una eliminación completa de Trident	
imagePullSecrets	Secretos para extraer imágenes de un registro interno	
imagePullPolicy	Establece la política de extracción de imágenes para el operador Trident. Valores válidos: Always para tirar siempre de la imagen. IfNotPresent para extraer la imagen solo si aún no existe en el nodo. Never para no tirar nunca de la imagen.	IfNotPresent
controllerPluginNodeSelector	Selectores de nodos adicionales para POD. Sigue el mismo formato que <code>pod.spec.nodeSelector</code> .	Sin valores predeterminados; opcional
controllerPluginTolerations	Anula la toleración de Kubernetes en pods. Sigue el mismo formato que <code>pod.spec.Tolerations</code> .	Sin valores predeterminados; opcional
nodePluginNodeSelector	Selectores de nodos adicionales para POD. Sigue el mismo formato que <code>pod.spec.nodeSelector</code> .	Sin valores predeterminados; opcional
nodePluginTolerations	Anula la toleración de Kubernetes en pods. Sigue el mismo formato que <code>pod.spec.Tolerations</code> .	Sin valores predeterminados; opcional
nodePrep	Permite a Trident preparar los nodos del clúster de Kubernetes para gestionar volúmenes mediante el protocolo de almacenamiento de datos especificado. <b>Actualmente, <code>iscsi</code> es el único valor soportado.</b>	



Para obtener más información sobre el formato de los parámetros del pod, consulte ["Asignación de pods a nodos"](#).

### Detalles acerca de forzar separación

Forzar separación está disponible sólo para `ontap-san`, `ontap-san-economy` y `onatap-nas-economy`. Antes de habilitar la desconexión forzada, se debe habilitar el cierre de nodos (NGN) no controlado en el clúster de Kubernetes. Para obtener más información, consulte ["Kubernetes: Cierre de nodo sin gracia"](#).



Cuando se utiliza `ontap-nas-economy` el controlador, es necesario establecer el `autoExportPolicy` parámetro en la configuración de backend para `true` que Trident pueda restringir el acceso desde el nodo de Kubernetes con la contaminación aplicada mediante políticas de exportación gestionadas.



Dado que Trident se basa en LAS NGN de Kubernetes, no elimine `out-of-service` los daños de un nodo en mal estado hasta que se reprogramen todas las cargas de trabajo no tolerables. La aplicación o eliminación imprudente de la contaminación puede poner en peligro la protección de datos de back-end.

Cuando el administrador del clúster de Kubernetes haya aplicado la `node.kubernetes.io/out-of-service=nodeshutdown:NoExecute` tinte al nodo y `enableForceDetach` se establezca en `true`, Trident determinará el estado del nodo y:

1. Cese el acceso de I/O back-end para los volúmenes montados en ese nodo.

2. Marque el objeto de nodo Trident como `dirty` (no es seguro para las nuevas publicaciones).



El controlador Trident rechazará nuevas solicitudes de volumen de publicación hasta que el nodo se vuelva a calificar (después de haberse marcado como `dirty`) por el pod del nodo Trident. No se aceptarán todas las cargas de trabajo programadas con una RVP montada (incluso después de que el nodo del clúster esté en buen estado y listo) hasta que Trident pueda verificar el nodo `clean` (seguro para las nuevas publicaciones).

Cuando se restaure el estado del nodo y se elimine el tinte, Trident:

1. Identifique y limpie las rutas publicadas obsoletas en el nodo.
2. Si el nodo está en un `cleanable` estado (se ha quitado el taint de fuera de servicio y el nodo está en `Ready` estado) y todas las rutas obsoletas publicadas están limpias, Trident readmitirá el nodo como `clean` y permitirá que los nuevos volúmenes publicados al nodo.

### Configuraciones de ejemplo

Puede utilizar los atributos en [Opciones de configuración](#) al definir `TridentOrchestrator` para personalizar la instalación.

### Configuración personalizada básica

Este es un ejemplo de una instalación personalizada básica.

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



## Selectores de nodos

En este ejemplo se instala Trident con selectores de nodos.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  controllerPluginNodeSelector:
    nodetype: master
  nodePluginNodeSelector:
    storage: netapp
```

## Nodos de trabajo de Windows

En este ejemplo se instala Trident en un nodo de trabajo de Windows.

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

## Identidades administradas en un cluster AKS

En este ejemplo se instala Trident para activar identidades gestionadas en un cluster AKS.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "Azure"
```

## Identidad de nube en un clúster AKS

En este ejemplo se instala Trident para utilizarlo con una identidad de nube en un clúster AKS.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "Azure"
  cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxxx'
```

## Identidad de nube en un clúster de EKS

En este ejemplo se instala Trident para utilizarlo con una identidad de nube en un clúster AKS.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "AWS"
  cloudIdentity: "'eks.amazonaws.com/role-arn:
arn:aws:iam::123456:role/trident-role'"
```

## Identidad de nube para GKE

En este ejemplo se instala Trident para su uso con una identidad de nube en un clúster de GKE.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcp-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '012345678901'
  network: gcnv-network
  location: us-west2
  serviceLevel: Premium
  storagePool: pool-premium1
```

# Instale utilizando trimentctl

## Instale utilizando trimentctl

Puede instalar Trident mediante `tridentctl`. Este proceso se aplica a instalaciones en las que las imágenes de contenedor requeridas por Trident se almacenan en un registro privado o no. Para personalizar `tridentctl` el despliegue, consulte ["Personalice la implementación trimentctl"](#).

## Información crítica sobre Trident 24,10

Debe leer la siguiente información crítica sobre Trident.

### **Información crítica sobre Trident**

- Kubernetes 1,27 ahora es compatible con Trident. Actualizar Trident antes de actualizar Kubernetes.
- Trident aplica estrictamente el uso de la configuración de múltiples rutas en entornos SAN, con un valor recomendado de `find_multipaths: no` en archivo `multipath.conf`.

Uso de la configuración sin multivía o el uso de `find_multipaths: yes` o `find_multipaths: smart` el valor del archivo `multipath.conf` provocará fallos de montaje. Trident ha recomendado el uso de `find_multipaths: no` desde la versión 21.07.

## Instalar Trident mediante `tridentctl`

Revisar "[descripción general de la instalación](#)" para asegurarse de cumplir con los requisitos previos de instalación y seleccionar la opción de instalación correcta para el entorno.

### Antes de empezar

Antes de iniciar la instalación, inicie sesión en el host Linux y compruebe que esté gestionando un trabajo, "[Clúster de Kubernetes compatible](#)" y que tenga los privilegios necesarios.



Con OpenShift, utilícelo `oc` en lugar de `kubectl` en todos los ejemplos que siguen, e inicie sesión como **system:admin** primero ejecutando `oc login -u system:admin` o `oc login -u kube-admin`.

1. Compruebe su versión de Kubernetes:

```
kubectl version
```

2. Comprobar los privilegios de administrador de clúster:

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. Compruebe que puede iniciar un pod que utilice una imagen de Docker Hub para llegar al sistema de almacenamiento a través de la red de pod:

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

## Paso 1: Descargue el paquete de instalación de Trident

El paquete del instalador de Trident crea un pod Trident, configura los objetos CRD que se utilizan para mantener su estado e inicializa los sidecars CSI para realizar acciones como el aprovisionamiento y la conexión de volúmenes a los hosts del clúster. Descargue y extraiga la última versión del instalador de Trident de "[La sección Assets de GitHub](#)". Actualice `<Trident-installer-XX.XX.X.tar.gz>` en el ejemplo con la versión de Trident seleccionada.

```
wget https://github.com/NetApp/trident/releases/download/v24.10.0/trident-
installer-24.10.0.tar.gz
tar -xf trident-installer-24.10.0.tar.gz
cd trident-installer
```

## Paso 2: Instale Trident

Instale Trident en el espacio de nombres deseado ejecutando `tridentctl install` el comando. Puede agregar argumentos adicionales para especificar la ubicación del registro de imágenes.

### Modo estándar

```
./tridentctl install -n trident
```

### Imágenes en un registro

```
./tridentctl install -n trident --image-registry <your-registry>
--autosupport-image <your-registry>/trident-autosupport:24.10 --trident
-image <your-registry>/trident:24.10.0
```

### Imágenes en diferentes registros

```
./tridentctl install -n trident --image-registry <your-registry>
--autosupport-image <your-registry>/trident-autosupport:24.10 --trident
-image <your-registry>/trident:24.10.0
```

El estado de su instalación debería tener un aspecto parecido a este.

```

.....
INFO Starting Trident installation.                namespace=trident
INFO Created service account.
INFO Created cluster role.
INFO Created cluster role binding.
INFO Added finalizers to custom resource definitions.
INFO Created Trident service.
INFO Created Trident secret.
INFO Created Trident deployment.
INFO Created Trident daemonset.
INFO Waiting for Trident pod to start.
INFO Trident pod started.                        namespace=trident
pod=trident-controller-679648bd45-cv2mx
INFO Waiting for Trident REST interface.
INFO Trident REST interface is up.                version=24.10.0
INFO Trident installation succeeded.
.....

```

## Compruebe la instalación

Puede verificar la instalación con el estado de creación de un pod o. `tridentctl`.

### Uso del estado de creación de pod

Puede confirmar si la instalación de Trident ha finalizado revisando el estado de los pods creados:

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

NAME	READY	STATUS	RESTARTS	AGE
trident-controller-679648bd45-cv2mx	6/6	Running	0	5m29s
trident-node-linux-vgc8n	2/2	Running	0	5m29s



Si el instalador no se completa correctamente o. `trident-controller-<generated id>` (`trident-csi-<generated id>` En versiones anteriores a 23.01) no tiene un estado **en ejecución**, la plataforma no estaba instalada. Uso `-d` para "[activa el modo de depuración](#)" y solucionar el problema.

### Uso `tridentctl`

Puede utilizar `tridentctl` para comprobar la versión de Trident instalada.

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

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 24.10.0        | 24.10.0        |
+-----+-----+
```

## Configuraciones de ejemplo

Los siguientes ejemplos proporcionan configuraciones de ejemplo para instalar Trident utilizando `tridentctl`.

### Nodos de Windows

Para habilitar Trident para que se ejecute en los nodos de Windows:

```
tridentctl install --windows -n trident
```

### Forzar separación

Para obtener más información acerca de forzar separación, consulte ["Personalice la instalación del operador de Trident"](#).

```
tridentctl install --enable-force-detach=true -n trident
```

## Personalice la instalación trimentctl

Puede usar el instalador de Trident para personalizar la instalación.

### Obtenga más información sobre el instalador

El instalador de Trident le permite personalizar atributos. Por ejemplo, si ha copiado la imagen Trident en un repositorio privado, puede especificar el nombre de la imagen mediante `--trident-image`. Si ha copiado la imagen Trident, así como las imágenes de sidecar CSI necesarias en un repositorio privado, es preferible especificar la ubicación de ese repositorio mediante el `--image-registry` switch, que toma el formulario `<registry FQDN>[:port]`.



Al instalar Trident en un repositorio privado, si está utilizando el `--image-registry` conmutador para especificar la ubicación del repositorio, no lo utilice `/netapp/` en la ruta de acceso del repositorio. Por ejemplo: `./tridentctl install --image-registry <image-registry> -n <namespace>`

Si utiliza una distribución de Kubernetes, donde `kubelet` mantiene los datos en una ruta distinta de la

habitual `/var/lib/kubelet`, puede especificar la ruta alternativa mediante `--kubelet-dir`.

Si necesita personalizar la instalación más allá de lo que permiten los argumentos del instalador, también puede personalizar los archivos de implementación. Con el `--generate-custom-yaml` El parámetro crea los siguientes archivos YAML en el instalador `setup` directorio:

- `trident-clusterrolebinding.yaml`
- `trident-deployment.yaml`
- `trident-crds.yaml`
- `trident-clusterrole.yaml`
- `trident-daemonset.yaml`
- `trident-service.yaml`
- `trident-namespace.yaml`
- `trident-serviceaccount.yaml`
- `trident-resourcequota.yaml`

Después de haber generado estos archivos, puede modificarlos según sus necesidades y luego usarlos `--use-custom-yaml` para instalar su implementación personalizada.

```
./tridentctl install -n trident --use-custom-yaml
```



# Utilizar Trident

## Prepare el nodo de trabajo

Todos los nodos de trabajadores del clúster de Kubernetes deben poder montar los volúmenes que haya aprovisionado para los pods. Para preparar los nodos de trabajo, debe instalar herramientas NFS, iSCSI, NVMe/TCP o FC según haya seleccionado los controladores.

### Seleccionar las herramientas adecuadas

Si está utilizando una combinación de controladores, debe instalar todas las herramientas necesarias para sus controladores. Las versiones recientes de RedHat CoreOS tienen las herramientas instaladas de forma predeterminada.

#### Herramientas de NFS

"[Instale las herramientas NFS](#)" si está utilizando: `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`.

#### Herramientas iSCSI

"[Instale las herramientas iSCSI](#)" si está utilizando: `ontap-san`, `ontap-san-economy`, `solidfire-san`.

#### Herramientas de NVMe

"[Instale las herramientas NVMe](#)" si está utilizando `ontap-san` Para el protocolo de memoria no volátil rápida (NVMe) sobre TCP (NVMe/TCP).



Recomendamos ONTAP 9,12 o posterior para NVMe/TCP.

#### Herramientas de SCSI sobre FC

**SCSI sobre canal de fibra (FC) es una función de vista previa técnica en la versión Trident 24,10.**

"[Instale las herramientas iSCSI](#)" Si utiliza `ontap-san` con `sanType fcp` (SCSI sobre FC).

Consulte "[Formas de configurar hosts de SAN FC FC-NVMe](#)" si desea obtener más información.

### Detección del servicio de nodos

Trident intenta detectar automáticamente si el nodo puede ejecutar servicios iSCSI o NFS.



La detección de servicios de nodo identifica los servicios detectados, pero no garantiza que los servicios se configuren correctamente. Por el contrario, la ausencia de un servicio detectado no garantiza que se produzca un error en el montaje del volumen.

#### Revisar los eventos

Trident crea eventos para que el nodo identifique los servicios detectados. Para revisar estos eventos, ejecute:

```
kubectl get event -A --field-selector involvedObject.name=<Kubernetes node name>
```

### Revisar los servicios detectados

Trident identifica los servicios habilitados para cada nodo del CR de nodo Trident. Para ver los servicios detectados, ejecute:

```
tridentctl get node -o wide -n <Trident namespace>
```

## Volúmenes de NFS

Instale las herramientas de NFS mediante los comandos del sistema operativo. Asegúrese de que el servicio NFS se haya iniciado durante el arranque.

### RHEL 8 O POSTERIOR

```
sudo yum install -y nfs-utils
```

### Ubuntu

```
sudo apt-get install -y nfs-common
```



Reinicie los nodos de trabajo después de instalar las herramientas NFS para evitar que se produzcan fallos cuando conecte volúmenes a los contenedores.

## Volúmenes iSCSI

Trident puede establecer automáticamente una sesión iSCSI, escanear LUN y detectar dispositivos multivía, formatearlos y montarlos en un pod.

### Funcionalidades de reparación automática de iSCSI

En el caso de los sistemas ONTAP, Trident ejecuta la reparación automática de iSCSI cada cinco minutos para:

1. **Identifique** el estado de sesión iSCSI deseado y el estado actual de la sesión iSCSI.
2. **Compare** el estado deseado al estado actual para identificar las reparaciones necesarias. Trident determina las prioridades de reparación y cuándo se deben adelantar a las reparaciones.
3. **Realice las reparaciones** necesarias para devolver el estado actual de la sesión iSCSI al estado deseado de la sesión iSCSI.



Los registros de la actividad de autorrecuperación se encuentran en `trident-main` el contenedor del pod `Daemonset` correspondiente. Para ver los registros, debe haberse establecido `debug` en «true» durante la instalación de Trident.

Las funcionalidades de reparación automática de iSCSI de Trident pueden ayudar a evitar lo siguiente:

- Sesiones iSCSI obsoletas o poco saludables que podrían producirse después de un problema de conectividad de red. En el caso de una sesión obsoleta, Trident espera siete minutos antes de cerrar la sesión para restablecer la conexión con un portal.



Por ejemplo, si los secretos CHAP se rotaban en la controladora de almacenamiento y la red pierde la conectividad, podrían persistir los secretos CHAP antiguos (*obsoleta*). La reparación automática puede reconocer esto y restablecer automáticamente la sesión para aplicar los secretos CHAP actualizados.

- Faltan sesiones iSCSI
- Faltan LUN

### Puntos a tener en cuenta antes de actualizar Trident

- Si solo se utilizan iGroups por nodo (introducidos en 23,04+), la reparación automática de iSCSI iniciará los análisis de SCSI para todos los dispositivos del bus SCSI.
- Si solo se utilizan iGroups de ámbito back-end (obsoletos a partir de 23,04), la reparación automática de iSCSI iniciará los nuevos análisis SCSI de los ID exactos de LUN en el bus SCSI.
- Si se utiliza una combinación de iGroups por nodo y iGroups de ámbito back-end, la reparación automática de iSCSI iniciará los análisis SCSI de los ID exactos de LUN en el bus SCSI.

### Instale las herramientas iSCSI

Instale las herramientas iSCSI mediante los comandos del sistema operativo.

#### Antes de empezar

- Cada nodo del clúster de Kubernetes debe tener un IQN único. **Este es un requisito previo necesario.**
- Si utiliza RHCOS versión 4.5 o posterior, u otra distribución Linux compatible con RHEL, con `solidfire-san` Controlador y Element OS 12.5 o anterior, asegúrese de que el algoritmo de autenticación CHAP esté establecido en MD5 in `/etc/iscsi/iscsid.conf`. Los algoritmos CHAP SHA1, SHA-256 y SHA3-256 compatibles con FIPS están disponibles con Element 12.7.

```
sudo sed -i 's/^\(node.session.auth.chap_algs\).*\/\1 = MD5/'  
/etc/iscsi/iscsid.conf
```

- Cuando utilice nodos de trabajo que ejecutan RHEL/RedHat CoreOS con VP iSCSI, especifique el `discard` MountOption en StorageClass para realizar un reclamación de espacio en línea. Consulte ["Documentación de redhat"](#).

## RHEL 8 O POSTERIOR

1. Instale los siguientes paquetes del sistema:

```
sudo yum install -y lsscsi iscsi-initiator-utils device-mapper-  
multipath
```

2. Compruebe que la versión de iscsi-initiator-utils sea 6.2.0.874-2.el7 o posterior:

```
rpm -q iscsi-initiator-utils
```

3. Activar accesos múltiples:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



Asegúrese etc/multipath.conf contiene find\_multipaths no inferior defaults.

4. Asegúrese de que así sea iscsid y.. multipathd están en ejecución:

```
sudo systemctl enable --now iscsid multipathd
```

5. Activar e iniciar iscsi:

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. Instale los siguientes paquetes del sistema:

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools  
scsitools
```

2. Compruebe que la versión Open-iscsi sea 2.0.874-5ubuntu2.10 o posterior (para bionic) o 2.0.874-7.1ubuntu6.1 o posterior (para focal):

```
dpkg -l open-iscsi
```

3. Configure el escaneo en manual:

```
sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'
/etc/iscsi/iscsid.conf
```

#### 4. Activar accesos múltiples:

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```



Asegúrese `etc/multipath.conf` contiene `find_multipaths no` inferior `defaults`.

#### 5. Asegúrese de que así sea `open-iscsi` y. `multipath-tools` están habilitadas y en ejecución:

```
sudo systemctl status multipath-tools
sudo systemctl enable --now open-iscsi.service
sudo systemctl status open-iscsi
```



Para Ubuntu 18.04, debe descubrir los puertos de destino con `iscsiadm` antes de comenzar `open-iscsi` Para que se inicie el daemon iSCSI. También puede modificar el `iscsi` servicio para empezar `iscsid` automáticamente.

## Configure o deshabilite la reparación automática de iSCSI

Es posible configurar los siguientes ajustes de reparación automática de iSCSI de Trident para corregir las sesiones obsoletas:

- **Intervalo de autorrecuperación iSCSI:** Determina la frecuencia a la que se invoca la autorrecuperación iSCSI (valor predeterminado: 5 minutos). Puede configurarlo para que se ejecute con más frecuencia estableciendo un número menor o con menos frecuencia estableciendo un número mayor.



Si se configura el intervalo de reparación automática de iSCSI en 0, se detiene por completo la reparación automática de iSCSI. No recomendamos deshabilitar la reparación automática de iSCSI; solo debe deshabilitarse en ciertos casos cuando la reparación automática de iSCSI no funciona como se esperaba o con fines de depuración.

- **Tiempo de espera de autorrecuperación iSCSI:** Determina la duración de las esperas de autorrecuperación iSCSI antes de cerrar sesión en una sesión en mal estado e intentar iniciar sesión de nuevo (por defecto: 7 minutos). Puede configurarlo a un número mayor para que las sesiones identificadas

como en mal estado tengan que esperar más tiempo antes de cerrar la sesión y, a continuación, se intente volver a iniciar sesión, o un número menor para cerrar la sesión e iniciar sesión anteriormente.

### Timón

Para configurar o cambiar los ajustes de reparación automática de iSCSI, pase el `iscsiSelfHealingInterval` y `iscsiSelfHealingWaitTime` parámetros durante la instalación del timón o actualización del timón.

En el siguiente ejemplo, se establece el intervalo de reparación automática de iSCSI en 3 minutos y el tiempo de espera de reparación automática en 6 minutos:

```
helm install trident trident-operator-100.2410.0.tgz --set
iscsiSelfHealingInterval=3m0s --set iscsiSelfHealingWaitTime=6m0s -n
trident
```

### tridentctl

Para configurar o cambiar los ajustes de reparación automática de iSCSI, pase el `iscsi-self-healing-interval` y `iscsi-self-healing-wait-time` parámetros durante la instalación o actualización de `tridentctl`.

En el siguiente ejemplo, se establece el intervalo de reparación automática de iSCSI en 3 minutos y el tiempo de espera de reparación automática en 6 minutos:

```
tridentctl install --iscsi-self-healing-interval=3m0s --iscsi-self
-healing-wait-time=6m0s -n trident
```

## Volúmenes NVMe/TCP

Instale las herramientas NVMe mediante los comandos de su sistema operativo.



- NVMe requiere RHEL 9 o posterior.
- Si la versión del kernel de su nodo de Kubernetes es demasiado antigua o si el paquete NVMe no está disponible para la versión de kernel, es posible que deba actualizar la versión del kernel del nodo a una con el paquete NVMe.

## RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Verifique la instalación

Después de la instalación, compruebe que cada nodo del clúster de Kubernetes tenga un NQN único mediante el comando:

```
cat /etc/nvme/hostnqn
```



Trident modifica `ctrl_device_tmo` el valor para garantizar que NVMe no se rinde en la ruta si deja de funcionar. No cambie esta configuración.

## Compatibilidad con Fibre Channel (FC)

Ahora se puede utilizar el protocolo Fibre Channel (FC) con Trident para aprovisionar y gestionar recursos de almacenamiento en el sistema ONTAP.

**SCSI sobre canal de fibra (FC) es una función de vista previa técnica en la versión Trident 24,10.**

Fibre Channel es un protocolo adoptado de forma generalizada en entornos de almacenamiento empresarial debido a su alto rendimiento, fiabilidad y escalabilidad. Proporciona un canal de comunicación robusto y eficiente para dispositivos de almacenamiento, lo que permite transferencias de datos rápidas y seguras. Al utilizar SCSI sobre Fibre Channel, puede aprovechar su infraestructura de almacenamiento basada en SCSI existente y beneficiarse de las funcionalidades de alto rendimiento y larga distancia de Fibre Channel. Permite consolidar los recursos de almacenamiento y crear redes de área de almacenamiento (SAN) eficaces y escalables que pueden gestionar grandes cantidades de datos con una baja latencia.

Use la función FC con Trident, es posible hacer lo siguiente:

- Aprovisionar RVP de forma dinámica mediante las especificaciones de la puesta en marcha.
- Tome las snapshots de volumen y cree un volumen nuevo a partir de la copia de Snapshot.
- Clone un FC-PVC existente.
- Cambie el tamaño de un volumen ya implementado.

## Requisitos previos

Configure los ajustes de nodo y red necesarios para FC.

### Ajustes de red

1. Obtenga el WWPN de las interfaces de destino. Consulte ["se muestra la interfaz de red"](#) si desea obtener más información.
2. Obtenga el WWPN de las interfaces del iniciador (host).

Consulte las utilidades del sistema operativo host correspondientes.

3. Configure la división en zonas en el switch de FC mediante WWPN del host y el destino.

Consulte la documentación nueva del proveedor de switches para obtener más información.

Consulte la siguiente documentación de ONTAP para obtener más detalles:

- ["Información general sobre la división en zonas de Fibre Channel y FCoE"](#)
- ["Formas de configurar hosts de SAN FC FC-NVMe"](#)

### Prepare el nodo de trabajo

Todos los nodos de trabajadores del clúster de Kubernetes deben poder montar los volúmenes que haya provisionado para los pods. Para preparar los nodos de trabajo para FC, debe instalar las herramientas necesarias.

### Instale las herramientas FC

Instale las herramientas de FC mediante los comandos del sistema operativo.

- Cuando utilice nodos de trabajo que ejecutan RHEL/RedHat CoreOS con VP iSCSI, especifique el `discard` MountOption en StorageClass para realizar un reclamación de espacio en línea. Consulte ["Documentación de redhat"](#).



## RHEL 8 O POSTERIOR

1. Instale los siguientes paquetes del sistema:

```
sudo yum install -y lsscsi iscsi-initiator-utils device-mapper-  
multipath
```

2. Compruebe que la versión de iscsi-initiator-utils sea 6.2.0.874-2.el7 o posterior:

```
rpm -q iscsi-initiator-utils
```

3. Activar accesos múltiples:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



Asegúrese etc/multipath.conf contiene find\_multipaths no inferior defaults.

4. Asegúrese de que así sea iscsid y.. multipathd están en ejecución:

```
sudo systemctl enable --now iscsid multipathd
```

5. Activar e iniciar iscsi:

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. Instale los siguientes paquetes del sistema:

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools  
scsitools
```

2. Compruebe que la versión Open-iscsi sea 2.0.874-5ubuntu2.10 o posterior (para bionic) o 2.0.874-7.1ubuntu6.1 o posterior (para focal):

```
dpkg -l open-iscsi
```

3. Configure el escaneo en manual:

```
sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'
/etc/iscsi/iscsid.conf
```

#### 4. Activar accesos múltiples:

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```



Asegúrese `etc/multipath.conf` contiene `find_multipaths no` inferior `defaults`.

#### 5. Asegúrese de que así sea `open-iscsi` y. `multipath-tools` están habilitadas y en ejecución:

```
sudo systemctl status multipath-tools
sudo systemctl enable --now open-iscsi.service
sudo systemctl status open-iscsi
```



Para Ubuntu 18.04, debe descubrir los puertos de destino con `iscsiadm` antes de comenzar `open-iscsi` Para que se inicie el daemon iSCSI. También puede modificar el `iscsi` servicio para empezar `iscsid` automáticamente.

## Cree una configuración de backend

Cree un backend Trident para `ontap-san` el controlador y `fc` como `sanType`.

Consulte:

- ["Prepárese para configurar el back-end con los controladores SAN de ONTAP"](#)
- ["Opciones y ejemplos de configuración DE SAN ONTAP"](#)

## Ejemplo de configuración de back-end con FC

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  sanType: fcp
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

## Cree una clase de almacenamiento

Para obtener más información, consulte:

- ["Opciones de configuración de almacenamiento"](#)

## Ejemplo de clase de almacenamiento

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: fcp-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  protocol: "fcp"
  storagePool: "aggr1"
allowVolumeExpansion: True
```

# Configurar y gestionar back-ends

## Configurar los back-ends

Un back-end define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él.

Trident ofrece automáticamente pools de almacenamiento de back-ends que coincidan con los requisitos definidos por una clase de almacenamiento. Aprenda a configurar el back-end para el sistema de almacenamiento.

- ["Configure un back-end de Azure NetApp Files"](#)
- ["Configure un back-end de Cloud Volumes Service para Google Cloud Platform"](#)
- ["Configure un back-end de NetApp HCI o SolidFire"](#)
- ["Configure un back-end con controladores NAS ONTAP o Cloud Volumes ONTAP"](#)
- ["Configurar un back-end con controladores SAN ONTAP o Cloud Volumes ONTAP"](#)
- ["Utiliza Trident con Amazon FSx para NetApp ONTAP"](#)

## Azure NetApp Files

### Configure un back-end de Azure NetApp Files

Puede configurar Azure NetApp Files como backend de Trident. Puede asociar volúmenes NFS y SMB con un back-end de Azure NetApp Files. Trident también admite la gestión de credenciales mediante identidades administradas para clústeres de Azure Kubernetes Services (AKS).

#### Información del controlador de Azure NetApp Files

Trident proporciona los siguientes controladores de almacenamiento de Azure NetApp Files para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
azure-netapp-files	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	nfs, smb

### Consideraciones

- El servicio Azure NetApp Files no admite volúmenes de menos de 50 GiB. Trident crea automáticamente volúmenes de 50 GiB si se solicita un volumen más pequeño.
- Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.

#### Identidades administradas para AKS

Trident es compatible con ["identidades administradas"](#) clústeres de Azure Kubernetes Services. Para aprovechar la gestión de credenciales optimizada que ofrecen las identidades gestionadas, debe tener:

- Un clúster de Kubernetes puesto en marcha mediante AKS
- Identidades gestionadas configuradas en el clúster de kubernetes de AKS
- Trident instalado que incluye el `cloudProvider` para especificar "Azure".

## Operador de Trident

Para instalar Trident con el operador Trident, edite `tridentorchestrator_cr.yaml` en `cloudProvider "Azure"` . Por ejemplo:

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
```

## Timón

En el siguiente ejemplo se instalan conjuntos de Trident `cloudProvider` en Azure mediante la variable de entorno `$CP` :

```
helm install trident trident-operator-100.2410.0.tgz --create
--namespace --namespace <trident-namespace> --set cloudProvider=$CP
```

## `tridentctl`

En el siguiente ejemplo se instala Trident y se establece el `cloudProvider` indicador en Azure:

```
tridentctl install --cloud-provider="Azure" -n trident
```

## Identidad de nube para AKS

La identidad en la nube permite que los pods de Kubernetes accedan a los recursos de Azure autenticándose como identidad de carga de trabajo, en lugar de proporcionar credenciales explícitas de Azure.

Para aprovechar la identidad de la nube en Azure, debes tener:

- Un clúster de Kubernetes puesto en marcha mediante AKS
- Identidad de carga de trabajo y emisor de oidc configurados en el clúster de Kubernetes de AKS
- Trident instalado que incluye `cloudProvider` para "Azure" especificar y `cloudIdentity` especificar la identidad de la carga de trabajo

## Operador de Trident

Para instalar Trident mediante el operador Trident, edite `tridentorchestrator_cr.yaml` en Establecer `cloudProvider` en "Azure" y establezca `cloudIdentity` en `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.

Por ejemplo:

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
  *cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx' *
```

## Timón

Establezca los valores para los indicadores **cloud-provider (CP)** y **cloud-identity (CI)** utilizando las siguientes variables de entorno:

```
export CP="Azure"
export CI="'azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx' "
```

En el siguiente ejemplo, se instala Trident y se establece `cloudProvider` en Azure mediante la variable de entorno `$CP` y se establece el `cloudIdentity` uso de la variable de entorno `$CI` :

```
helm install trident trident-operator-100.2410.0.tgz --set
cloudProvider=$CP --set cloudIdentity="$CI"
```

## `tridentctl`

Establezca los valores para los indicadores **cloud provider** y **cloud identity** utilizando las siguientes variables de entorno:

```
export CP="Azure"
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx"
```

En el siguiente ejemplo se instala Trident y se establece el `cloud-provider` indicador en `$CP`, y `cloud-identity` en `$CI`:

```
tridentctl install --cloud-provider=$CP --cloud-identity="$CI" -n
trident
```

## Prepárese para configurar un back-end de Azure NetApp Files

Antes de configurar el back-end de Azure NetApp Files, debe asegurarse de que se cumplan los siguientes requisitos.

### Requisitos previos para volúmenes NFS y SMB

Si utiliza Azure NetApp Files por primera vez o en una ubicación nueva, es necesario realizar alguna configuración inicial para configurar Azure NetApp Files y crear un volumen NFS. Consulte ["Azure: Configure Azure NetApp Files y cree un volumen NFS"](#).

Para configurar y utilizar un ["Azure NetApp Files"](#) back-end, necesita lo siguiente:



- `subscriptionID`, `tenantID`, `clientID`, `location`, y `clientSecret` Son opcionales cuando se utilizan identidades administradas en un clúster AKS.
- `tenantID`, `clientID`, y `clientSecret` Son opcionales cuando se utiliza una identidad de nube en un clúster de AKS.

- Un pool de capacidad. Consulte ["Microsoft: Cree un pool de capacidad para Azure NetApp Files"](#).
- Una subred delegada en Azure NetApp Files. Consulte ["Microsoft: Delege una subred en Azure NetApp Files"](#).
- `subscriptionID` Desde una suscripción de Azure con Azure NetApp Files habilitado.
- `tenantID`, `clientID`, y `clientSecret` desde una ["Registro de aplicaciones"](#) En Azure Active Directory con permisos suficientes para el servicio Azure NetApp Files. El registro de aplicaciones debe usar:
  - El rol propietario o Colaborador ["Predefinidos por Azure"](#).
  - A ["Rol Colaborador personalizado"](#) en el nivel de suscripción (`assignableScopes`) con los siguientes permisos que están limitados solo a lo que Trident requiere. Después de crear el rol personalizado, ["Asigne el rol mediante el portal de Azure"](#).

## Rol de contribuyente personalizado

```
{
  "id": "/subscriptions/<subscription-
id>/providers/Microsoft.Authorization/roleDefinitions/<role-
definition-id>",
  "properties": {
    "roleName": "custom-role-with-limited-perms",
    "description": "custom role providing limited
permissions",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.NetApp/netAppAccounts/capacityPools/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/
read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/
write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/
delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTarge
ts/read",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/read",
          "Microsoft.Features/featureProviders/subscriptionFeatureRegistrat
ions/read",
          "Microsoft.Features/featureProviders/subscriptionFeatureRegistrat
```



```

ions/write",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrat
ions/delete",
        "Microsoft.Features/features/read",
        "Microsoft.Features/operations/read",
        "Microsoft.Features/providers/features/read",

"Microsoft.Features/providers/features/register/action",

"Microsoft.Features/providers/features/unregister/action",

"Microsoft.Features/subscriptionFeatureRegistrations/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
}
}

```

- Azure location que contiene al menos uno ["subred delegada"](#). A partir de Trident 22.01, la location parámetro es un campo obligatorio en el nivel superior del archivo de configuración del back-end. Los valores de ubicación especificados en los pools virtuales se ignoran.
- Para usar Cloud Identity, obtén el client ID desde a ["identidad gestionada asignada por el usuario"](#) Y especifique ese ID en `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.

### Requisitos adicionales para volúmenes SMB

Para crear un volumen de SMB, debe tener lo siguiente:

- Active Directory configurado y conectado a Azure NetApp Files. Consulte ["Microsoft: Cree y gestione conexiones de Active Directory para Azure NetApp Files"](#).
- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2022. Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Trident que contiene sus credenciales de Active Directory para que Azure NetApp Files pueda autenticarse en Active Directory. Para generar secreto `smbcreds`:

```

kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'

```

- Proxy CSI configurado como servicio de Windows. Para configurar un `csi-proxy`, consulte ["GitHub:](#)

[Proxy CSI](#) o. ["GitHub: Proxy CSI para Windows"](#) Para nodos Kubernetes que se ejecutan en Windows.

## Opciones y ejemplos de configuración del back-end de Azure NetApp Files

Obtenga más información sobre las opciones de configuración de back-end NFS y SMB para Azure NetApp Files y revise los ejemplos de configuración.

### Opciones de configuración del back-end

Trident utiliza la configuración de back-end (subred, red virtual, nivel de servicio y ubicación) para crear volúmenes de Azure NetApp Files en los pools de capacidad que están disponibles en la ubicación solicitada y coincidir con el nivel de servicio y la subred solicitados.



Trident no admite pools de capacidad de calidad de servicio manual.

Los back-ends de Azure NetApp Files proporcionan estas opciones de configuración.

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	"azure-netapp-files"
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre del controlador + "_" + caracteres aleatorios
subscriptionID	El ID de suscripción de su suscripción de Azure  Opcional cuando se activan identidades gestionadas en un clúster de AKS.	
tenantID	El ID de inquilino de un registro de aplicación  Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	
clientID	El ID de cliente de un registro de aplicación  Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	

Parámetro	Descripción	Predeterminado
clientSecret	El secreto de cliente de un registro de aplicaciones  Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	
serviceLevel	Uno de Standard, Premium, o. Ultra	"" (aleatorio)
location	Nombre de la ubicación de Azure donde se crearán los nuevos volúmenes  Opcional cuando se activan identidades gestionadas en un clúster de AKS.	
resourceGroups	Lista de grupos de recursos para filtrar los recursos detectados	[] (sin filtro)
netappAccounts	Lista de cuentas de NetApp para filtrar los recursos detectados	[] (sin filtro)
capacityPools	Lista de pools de capacidad para filtrar los recursos detectados	[] (sin filtro, aleatorio)
virtualNetwork	Nombre de una red virtual con una subred delegada	""
subnet	Nombre de una subred delegada a. Microsoft.Netapp/volumes	""
networkFeatures	Puede que el conjunto de funciones de vnet para un volumen sea Basic o. Standard. Las funciones de red no están disponibles en todas las regiones y es posible que tengan que activarse en una suscripción. Especificando networkFeatures cuando la funcionalidad no está habilitada, hace que no se pueda realizar el aprovisionamiento del volumen.	""

Parámetro	Descripción	Predeterminado
nfsMountOptions	Control preciso de las opciones de montaje NFS. Ignorada para volúmenes de SMB. Para montar volúmenes con NFS versión 4.1, incluya <code>nfsvers=4</code> En la lista de opciones de montaje delimitadas por comas para elegir NFS v4.1. Las opciones de montaje establecidas en una definición de clase de almacenamiento anulan las opciones de montaje establecidas en la configuración de back-end.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo: <code>\{"api": false, "method": true, "discovery": true\}</code> . No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o nulo. El valor predeterminado es nulo en volúmenes de NFS.	nfs
supportedTopologies	Representa una lista de regiones y zonas soportadas por este backend. Para obtener más información, consulte <a href="#">"Utilice Topología CSI"</a> .	



Para obtener más información sobre las funciones de red, consulte ["Configure las funciones de red para un volumen de Azure NetApp Files"](#).

### Permisos y recursos necesarios

Si recibes un error "No se han encontrado pools de capacidad" al crear una RVP, es probable que el registro de tu aplicación no tenga los permisos y recursos necesarios (subred, red virtual, pool de capacidad) asociados. Si DEBUG está habilitado, Trident registrará los recursos de Azure detectados al crear el backend. Compruebe que se está utilizando un rol adecuado.

Los valores para `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork`, y `subnet` puede especificarse utilizando nombres cortos o completos. En la mayoría de las situaciones, se recomiendan nombres completos, ya que los nombres cortos pueden coincidir con varios recursos con el mismo nombre.

La `resourceGroups`, `netappAccounts`, y `capacityPools` los valores son filtros que restringen el conjunto de recursos detectados a los disponibles en este back-end de almacenamiento y pueden especificarse en cualquier combinación de estos. Los nombres completos siguen este formato:

Tipo	Formato
Grupo de recursos	<resource group>
Cuenta de NetApp	<resource group>/<netapp account>
Pool de capacidad	<resource group>/<netapp account>/<capacity pool>
Red virtual	<resource group>/<virtual network>
Subred	<resource group>/<virtual network>/<subnet>

### Aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento de volúmenes predeterminado especificando las siguientes opciones en una sección especial del archivo de configuración. Consulte [Configuraciones de ejemplo](#) para obtener más detalles.

Parámetro	Descripción	Predeterminado
<code>exportRule</code>	Reglas de exportación de volúmenes nuevos. <code>exportRule</code> Debe ser una lista separada por comas con cualquier combinación de direcciones IPv4 o subredes IPv4 en notación CIDR. Ignorada para volúmenes de SMB.	"0.0.0.0/0"
<code>snapshotDir</code>	Controla la visibilidad del directorio <code>.snapshot</code>	"True" para NFSv4 "false" para NFSv3
<code>size</code>	El tamaño predeterminado de los volúmenes nuevos	"100 G"
<code>unixPermissions</code>	Los permisos unix de nuevos volúmenes (4 dígitos octal). Ignorada para volúmenes de SMB.	"" (función de vista previa, requiere incluir en la lista blanca de suscripciones)

### Configuraciones de ejemplo

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.

## Configuración mínima

Ésta es la configuración mínima absoluta del back-end. Con esta configuración, Trident detecta todas sus cuentas de NetApp, pools de capacidad y subredes delegadas en Azure NetApp Files en la ubicación configurada, y coloca volúmenes nuevos en uno de esos pools y subredes de forma aleatoria. Dado que `nasType` se omite, `nfs` se aplica el valor predeterminado y el back-end se aprovisionará para los volúmenes de NFS.

Esta configuración es ideal cuando solo se está empezando a usar Azure NetApp Files y probando cosas, pero en la práctica va a querer proporcionar un ámbito adicional para los volúmenes que aprovisiona.

```
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
  tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
  clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
  clientSecret: SECRET
  location: eastus
```

## Identidades administradas para AKS

Esta configuración de backend omite `subscriptionID`, `tenantID`, `clientID`, y `clientSecret`, que son opcionales cuando se utilizan identidades gestionadas.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
```

## Identidad de nube para AKS

Esta configuración de backend omite `tenantID`, `clientID`, y `clientSecret`, que son opcionales cuando se utiliza una identidad de nube.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
  location: eastus
  subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
```

## Configuración de niveles de servicio específica con filtros de pools de capacidad

Esta configuración de backend coloca los volúmenes en la ubicación de Azure `eastus` en un `Ultra` pool de capacidad. Trident detecta automáticamente todas las subredes delegadas en Azure NetApp Files en esa ubicación y coloca un volumen nuevo en una de ellas de forma aleatoria.

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
```



## Configuración avanzada

Esta configuración de back-end reduce aún más el alcance de la ubicación de volúmenes en una única subred y también modifica algunos valores predeterminados de aprovisionamiento de volúmenes.

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
virtualNetwork: my-virtual-network
subnet: my-subnet
networkFeatures: Standard
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 500Gi
defaults:
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  snapshotDir: 'true'
  size: 200Gi
  unixPermissions: '0777'
```

## Configuración de pool virtual

Esta configuración back-end define varios pools de almacenamiento en un único archivo. Esto resulta útil cuando hay varios pools de capacidad que admiten diferentes niveles de servicio y desea crear clases de almacenamiento en Kubernetes que representan estos. Se utilizaron etiquetas de pools virtuales para diferenciar los pools según *performance*.

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
resourceGroups:
- application-group-1
networkFeatures: Basic
nfsMountOptions: vers=3,proto=tcp,timeo=600
labels:
  cloud: azure
storage:
- labels:
  performance: gold
  serviceLevel: Ultra
  capacityPools:
  - ultra-1
  - ultra-2
  networkFeatures: Standard
- labels:
  performance: silver
  serviceLevel: Premium
  capacityPools:
  - premium-1
- labels:
  performance: bronze
  serviceLevel: Standard
  capacityPools:
  - standard-1
  - standard-2
```

## Configuración de topologías admitidas

Trident facilita el aprovisionamiento de volúmenes para cargas de trabajo según regiones y zonas de disponibilidad. El `supportedTopologies` bloque en esta configuración de backend se utiliza para proporcionar una lista de regiones y zonas por backend. Los valores de región y zona especificados aquí deben coincidir con los valores de región y zona de las etiquetas de cada nodo de clúster de Kubernetes. Estas regiones y zonas representan la lista de valores permitidos que se pueden proporcionar en una clase de almacenamiento. Para las clases de almacenamiento que contienen un subconjunto de las regiones y zonas proporcionadas en un backend, Trident crea volúmenes en la región y zona mencionadas. Para obtener más información, consulte "[Utilice Topología CSI](#)".

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
supportedTopologies:
- topology.kubernetes.io/region: eastus
  topology.kubernetes.io/zone: eastus-1
- topology.kubernetes.io/region: eastus
  topology.kubernetes.io/zone: eastus-2
```

### Definiciones de clases de almacenamiento

Lo siguiente `StorageClass` las definiciones hacen referencia a los pools de almacenamiento anteriores.

### Definiciones de ejemplo mediante `parameter.selector` campo

Uso `parameter.selector` puede especificar para cada una de ellas `StorageClass` el pool virtual que se utiliza para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze"
allowVolumeExpansion: true

```

### Definiciones de ejemplo de volúmenes SMB

Uso `nasType`, `node-stage-secret-name`, y `node-stage-secret-namespace`, Puede especificar un volumen SMB y proporcionar las credenciales necesarias de Active Directory.

## Configuración básica en el espacio de nombres predeterminado

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## Uso de diferentes secretos por espacio de nombres

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

## Uso de diferentes secretos por volumen

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```



`nasType: smb` Filtra los pools que admiten volúmenes SMB. `nasType: nfs` o `nasType: null` Filtros para pools NFS.

### Cree el back-end

Después de crear el archivo de configuración del back-end, ejecute el siguiente comando:

```
tridentctl create backend -f <backend-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando `create`.

## NetApp Volumes para Google Cloud

### Configura un back-end de Google Cloud NetApp Volumes

Ahora puede configurar Google Cloud NetApp Volumes como back-end para Trident. Puede adjuntar volúmenes de NFS con un back-end de Google Cloud NetApp Volumes.

#### Detalles del controlador de Google Cloud NetApp Volumes

Trident proporciona `google-cloud-netapp-volumes` el controlador para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
<code>google-cloud-netapp-volumes</code>	NFS	Sistema de archivos	RWO, ROX, RWX, RWOP	<code>nfs</code>

### Identidad de nube para GKE

La identidad de cloud permite a los pods de Kubernetes acceder a los recursos de Google Cloud autenticándose como identidad de carga de trabajo en lugar de proporcionando credenciales explícitas de Google Cloud.

Para aprovechar la identidad de la nube en Google Cloud, debes tener:

- Un clúster de Kubernetes puesto en marcha mediante GKE.
- Identidad de carga de trabajo y emisor de oidc configurados en el cluster de GKE.
- Trident instalado que incluye `cloudProvider` para "GCP" especificar y `cloudIdentity` especificar la identidad de la carga de trabajo.

## Operador de Trident

Para instalar Trident mediante el operador Trident, edite `tridentorchestrator_cr.yaml` en Establecer `cloudProvider` en "GCP" y establezca `cloudIdentity` en `iam.gke.io/gcp-service-account: cloudvolumes-admin-sa@mygcpproject.iam.gserviceaccount.com`.

Por ejemplo:

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "GCP"
  cloudIdentity: 'iam.gke.io/gcp-service-account: cloudvolumes-
admin-sa@mygcpproject.iam.gserviceaccount.com'
```

## Timón

Establezca los valores para los indicadores **cloud-provider (CP)** y **cloud-identity (CI)** utilizando las siguientes variables de entorno:

```
export CP="GCP"
export ANNOTATION="iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com"
```

En el siguiente ejemplo se instala Trident y se establece `cloudProvider` en GCP mediante la variable de entorno `$CP` y se establece el `cloudIdentity` uso de la variable de entorno `$ANNOTATION`:

```
helm install trident trident-operator-100.2406.0.tgz --set
cloudProvider=$CP --set cloudIdentity="$ANNOTATION"
```

## <code>tridentctl</code>

Establezca los valores para los indicadores **cloud provider** y **cloud identity** utilizando las siguientes variables de entorno:

```
export CP="GCP"
export ANNOTATION="iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com"
```

En el siguiente ejemplo se instala Trident y se establece el `cloud-provider` indicador en `$CP`, y `cloud-identity` en `$ANNOTATION`:

```
tridentctl install --cloud-provider=$CP --cloud
-identity="$ANNOTATION" -n trident
```

## Prepárate para configurar un back-end de Google Cloud NetApp Volumes

Para poder configurar el back-end de Google Cloud NetApp Volumes, debe asegurarse de que se cumplan los siguientes requisitos.

### Requisitos previos para volúmenes de NFS

Si utiliza Google Cloud NetApp Volumes por primera vez o en una ubicación nueva, es necesario tener alguna configuración inicial para configurar volúmenes de Google Cloud NetApp y crear un volumen NFS. Consulte ["Antes de empezar"](#).

Asegúrate de disponer de lo siguiente antes de configurar el back-end de Google Cloud NetApp Volumes:

- Una cuenta de Google Cloud configurada con el servicio NetApp Volumes de Google Cloud. Consulte ["NetApp Volumes para Google Cloud"](#).
- Número de proyecto de tu cuenta de Google Cloud. Consulte ["Identificación de proyectos"](#).
- Una cuenta de servicio de Google Cloud con el rol Administrador de volúmenes de NetApp (`netappcloudvolumes.admin`). Consulte ["Funciones y permisos de Identity and Access Management"](#).
- Archivo de claves de API para tu cuenta de GCNV. Consulte ["Cree una clave de cuenta de servicio"](#)
- Un pool de almacenamiento. Consulte ["Información general sobre pools de almacenamiento"](#).

Para obtener más información acerca de cómo configurar el acceso a volúmenes de Google Cloud NetApp, consulte ["Configure el acceso a Google Cloud NetApp Volumes"](#).

## Opciones de configuración y ejemplos de back-end de Google Cloud NetApp Volumes

Obtén más información sobre las opciones de configuración del back-end de NFS para Google Cloud NetApp Volumes y revisa los ejemplos de configuración.

### Opciones de configuración del back-end

Cada back-end aprovisiona volúmenes en una única región de Google Cloud. Para crear volúmenes en otras regiones, se pueden definir back-ends adicionales.

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	El valor de <code>storageDriverName</code> debe especificarse como «google-cloud-netapp-Volumes».



Parámetro	Descripción	Predeterminado
backendName	(Opcional) Nombre personalizado del back-end de almacenamiento	Nombre de controlador + "_ " + parte de la clave de API
storagePools	Parámetro opcional que se utiliza para especificar pools de almacenamiento para la creación del volumen.	
projectNumber	Número de proyecto de cuenta de Google Cloud. El valor está disponible en la página de inicio del portal de Google Cloud.	
location	La ubicación de Google Cloud donde Trident crea volúmenes de GCNV. Al crear clústeres de Kubernetes entre regiones, los volúmenes creados en un location se pueden usar en cargas de trabajo programadas en nodos de varias regiones de Google Cloud. El tráfico entre regiones conlleva un coste adicional.	
apiKey	La clave de la API para la cuenta de servicio de Google Cloud con netappcloudvolumes.admin el rol. Incluye el contenido en formato JSON del archivo de clave privada de una cuenta de servicio de Google Cloud (copiado literal en el archivo de configuración de back-end). apiKey`Debe incluir pares clave-valor para las siguientes claves` `type:,,,project_idclient_email` `client_id,,auth_uri token_uri` `auth_provider_x509_cert_url,y` `client_x509_cert_url.`	
nfsMountOptions	Control preciso de las opciones de montaje NFS.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica de forma predeterminada)
serviceLevel	El nivel de servicio de un pool de almacenamiento y sus volúmenes. Los valores son flex, standard, premium, o extreme.	
network	La red de Google Cloud utilizada para los volúmenes GCNV.	
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}. No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo

Parámetro	Descripción	Predeterminado
supportedTopologies	Representa una lista de regiones y zonas soportadas por este backend. Para obtener más información, consulte <a href="#">"Utilice Topología CSI"</a> . Por ejemplo: supportedTopologies: - topology.kubernetes.io/region: asia-east1 topology.kubernetes.io/zone: asia-east1-a	

### Opciones de aprovisionamiento de volúmenes

Es posible controlar el aprovisionamiento de volúmenes predeterminado en la `defaults` sección del archivo de configuración.

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación de nuevos volúmenes. Debe ser una lista separada por comas de cualquier combinación de direcciones IPv4.	"0.0.0.0/0"
snapshotDir	Acceso a la <code>.snapshot</code> directorio	"True" para NFSv4 "false" para NFSv3
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	" (aceptar valor por defecto de 0)
unixPermissions	Los permisos unix de nuevos volúmenes (4 dígitos octal).	""

### Configuraciones de ejemplo

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.



```
XsYg6gyxy4zq7OlwWgLwGa==\n
-----END PRIVATE KEY-----\n
```

```
---
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '123455380079'
  location: europe-west6
  serviceLevel: premium
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-
project.iam.gserviceaccount.com
    client_id: '103346282737811234567'
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
```



```
version: 1
storageDriverName: google-cloud-netapp-volumes
projectNumber: '123455380079'
location: europe-west6
serviceLevel: premium
storagePools:
- premium-pool1-europe-west6
- premium-pool2-europe-west6
apiKey:
  type: service_account
  project_id: my-gcnv-project
  client_email: myproject-prod@my-gcnv-
project.iam.gserviceaccount.com
  client_id: '103346282737811234567'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
```



```
znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
XsYg6gyxy4zq70lwWgLwGa==
-----END PRIVATE KEY-----
```

---

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '123455380079'
  location: europe-west6
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-
project.iam.gserviceaccount.com
    client_id: '103346282737811234567'
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
  defaults:
    snapshotReserve: '10'
    exportRule: 10.0.0.0/24
  storage:
    - labels:
        performance: extreme
        serviceLevel: extreme
      defaults:
        snapshotReserve: '5'
        exportRule: 0.0.0.0/0
    - labels:
        performance: premium
        serviceLevel: premium
```



```
- labels:  
  performance: standard  
  serviceLevel: standard
```

## Identidad de nube para GKE

```
apiVersion: trident.netapp.io/v1  
kind: TridentBackendConfig  
metadata:  
  name: backend-tbc-gcp-gcnv  
spec:  
  version: 1  
  storageDriverName: google-cloud-netapp-volumes  
  projectNumber: '012345678901'  
  network: gcnv-network  
  location: us-west2  
  serviceLevel: Premium  
  storagePool: pool-premium1
```

## Configuración de topologías admitidas

Trident facilita el aprovisionamiento de volúmenes para cargas de trabajo según regiones y zonas de disponibilidad. El `supportedTopologies` bloque en esta configuración de backend se utiliza para proporcionar una lista de regiones y zonas por backend. Los valores de región y zona especificados aquí deben coincidir con los valores de región y zona de las etiquetas de cada nodo de clúster de Kubernetes. Estas regiones y zonas representan la lista de valores permitidos que se pueden proporcionar en una clase de almacenamiento. Para las clases de almacenamiento que contienen un subconjunto de las regiones y zonas proporcionadas en un backend, Trident crea volúmenes en la región y zona mencionadas. Para obtener más información, consulte "[Utilice Topología CSI](#)".

```
---
version: 1
storageDriverName: google-cloud-netapp-volumes
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: asia-east1
serviceLevel: flex
supportedTopologies:
- topology.kubernetes.io/region: asia-east1
  topology.kubernetes.io/zone: asia-east1-a
- topology.kubernetes.io/region: asia-east1
  topology.kubernetes.io/zone: asia-east1-b
```

### El futuro

Después de crear el archivo de configuración del back-end, ejecute el siguiente comando:

```
kubectl create -f <backend-file>
```

Para verificar que el backend se ha creado correctamente, ejecute el siguiente comando:

```
kubectl get tridentbackendconfig
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-gcnv	backend-tbc-gcnv	b2fd1ff9-b234-477e-88fd-713913294f65
Bound	Success	

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede describir el backend con el `kubectl get tridentbackendconfig <backend-name>` comando o ver los logs para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede suprimir el backend y ejecutar el comando `create` de nuevo.

### Más ejemplos

#### Ejemplos de definición de la clase de almacenamiento

La siguiente es una definición básica `StorageClass` que hace referencia al backend anterior.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-nfs-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
```

#### Ejemplo de definiciones usando el `parameter.selector` campo:

Mediante el uso `parameter.selector` de puede especificar para cada uno `StorageClass` de los "pool virtual" que se utiliza para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: extreme-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=extreme"
  backendType: "google-cloud-netapp-volumes"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: premium-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium"
  backendType: "google-cloud-netapp-volumes"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: standard-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=standard"
  backendType: "google-cloud-netapp-volumes"

```

Para obtener más información sobre las clases de almacenamiento, consulte ["Cree una clase de almacenamiento"](#).

### Ejemplo de definición de PVC

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: gcnv-nfs-pvc
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-nfs-sc

```

Para verificar si la RVP está vinculada, ejecute el siguiente comando:

```
kubectl get pvc gcnv-nfs-pvc
```

NAME	STATUS	VOLUME	CAPACITY
gcnv-nfs-pvc	Bound	pvc-b00f2414-e229-40e6-9b16-ee03eb79a213	100Gi
ACCESS MODES	STORAGECLASS	AGE	
RWX	gcnv-nfs-sc	1m	

## Configure un back-end de Cloud Volumes Service para Google Cloud

Aprenda a configurar NetApp Cloud Volumes Service para Google Cloud como el back-end para su instalación de Trident con las configuraciones de ejemplo proporcionadas.

### Detalles del controlador de Google Cloud

Trident proporciona `gcp-cvs` el controlador para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMode	Modos de acceso compatibles	Sistemas de archivos compatibles
<code>gcp-cvs</code>	NFS	Sistema de archivos	RWO, ROX, RWX, RWOP	<code>nfs</code>

### Obtén más información sobre el soporte de Trident para Cloud Volumes Service para Google Cloud

Trident puede crear volúmenes de Cloud Volumes Service en uno de estos dos "tipos de servicio":

- **CVS-Performance:** El tipo de servicio Trident predeterminado. Este tipo de servicio optimizado para el rendimiento es más adecuado para cargas de trabajo de producción que valoran el rendimiento. El tipo de servicio CVS-Performance es una opción de hardware que admite volúmenes con un tamaño mínimo de 100 GiB. Puede elegir una de "tres niveles de servicio" las opciones:
  - `standard`
  - `premium`
  - `extreme`
- **CVS:** El tipo de servicio CVS proporciona una alta disponibilidad zonal con niveles de rendimiento limitados a moderados. El tipo de servicio CVS es una opción de software que usa pools de almacenamiento para admitir volúmenes de solo 1 GiB. El pool de almacenamiento puede contener hasta 50 volúmenes en los que todos los volúmenes comparten la capacidad y el rendimiento del pool. Puede elegir uno de "dos niveles de servicio":
  - `standardsw`
  - `zoneredundantstandardsw`

### Lo que necesitará

Para configurar y usar el "Cloud Volumes Service para Google Cloud" back-end, necesita lo siguiente:

- Una cuenta de Google Cloud configurada con Cloud Volumes Service de NetApp
- Número de proyecto de su cuenta de Google Cloud
- Cuenta de servicio de Google Cloud con el `netappcloudvolumes.admin` función
- Archivo de claves API para la cuenta de Cloud Volumes Service

## Opciones de configuración del back-end

Cada back-end aprovisiona volúmenes en una única región de Google Cloud. Para crear volúmenes en otras regiones, se pueden definir back-ends adicionales.

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	"gcp-cvs"
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + "_ " + parte de la clave de API
<code>storageClass</code>	Parámetro opcional utilizado para especificar el tipo de servicio CVS. Se utiliza <code>software</code> para seleccionar el tipo de servicio CVS. De lo contrario, Trident asume el tipo de servicio CVS-Performance ( <code>hardware</code> ).	
<code>storagePools</code>	Solo tipo de servicio CVS. Parámetro opcional que se utiliza para especificar pools de almacenamiento para la creación del volumen.	
<code>projectNumber</code>	Número de proyecto de cuenta de Google Cloud. El valor está disponible en la página de inicio del portal de Google Cloud.	
<code>hostProjectNumber</code>	Se requiere si se utiliza una red VPC compartida. En este escenario, <code>projectNumber</code> es el proyecto de servicio, y <code>hostProjectNumber</code> es el proyecto anfitrión.	
<code>apiRegion</code>	La región de Google Cloud donde Trident crea Cloud Volumes Service Volumes. Al crear clústeres de Kubernetes entre regiones, los volúmenes creados en un <code>apiRegion</code> se pueden usar en cargas de trabajo programadas en nodos de varias regiones de Google Cloud. El tráfico entre regiones conlleva un coste adicional.	
<code>apiKey</code>	Clave de API para la cuenta de servicio de Google Cloud con el <code>netappcloudvolumes.admin</code> función. Incluye el contenido en formato JSON del archivo de clave privada de una cuenta de servicio de Google Cloud (copiado literal en el archivo de configuración de back-end).	

Parámetro	Descripción	Predeterminado
proxyURL	URL de proxy si se requiere servidor proxy para conectarse a la cuenta CVS. El servidor proxy puede ser un proxy HTTP o HTTPS. En el caso de un proxy HTTPS, se omite la validación de certificados para permitir el uso de certificados autofirmados en el servidor proxy. No se admiten los servidores proxy con autenticación habilitada.	
nfsMountOptions	Control preciso de las opciones de montaje NFS.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica de forma predeterminada)
serviceLevel	El nivel de servicio CVS-Performance o CVS para nuevos volúmenes. Los valores de CVS-Performance son <code>standard</code> , <code>premium</code> , o <code>extreme</code> . Los valores CVS son <code>standardsw</code> o <code>zoneredundantstandardsw</code> .	El valor predeterminado de CVS-Performance es "estándar". El valor predeterminado de CVS es "standardsw".
network	Se utiliza la red de Google Cloud para Cloud Volumes Service Volumes.	"predeterminado"
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo: <code>\{"api":false,"method":true\}</code> . No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
allowedTopologies	Para habilitar el acceso a varias regiones, se debe definir <code>StorageClass</code> para <code>allowedTopologies</code> debe incluir todas las regiones. Por ejemplo: <ul style="list-style-type: none"> <li>- <code>key: topology.kubernetes.io/region</code></li> <li><code>values:</code></li> <li>- <code>us-east1</code></li> <li>- <code>europa-west1</code></li> </ul>	

## Opciones de aprovisionamiento de volúmenes

Es posible controlar el aprovisionamiento de volúmenes predeterminado en la `defaults` sección del archivo de configuración.

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación de nuevos volúmenes. Debe ser una lista separada por comas con cualquier combinación de direcciones IPv4 o subredes IPv4 en notación CIDR.	"0.0.0.0/0"
snapshotDir	Acceso a la <code>.snapshot</code> directorio	"falso"
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	"" (Aceptar CVS por defecto de 0)

Parámetro	Descripción	Predeterminado
size	El tamaño de los volúmenes nuevos. CVS-Performance mínimo es 100 GIB. El mínimo de CVS es 1 GIB.	El tipo de servicio CVS-Performance se establece de manera predeterminada en "100GIB". El tipo de servicio CVS no establece un valor predeterminado, pero requiere un mínimo de 1 GIB.

## Ejemplos de tipo de servicio CVS-Performance

Los siguientes ejemplos proporcionan ejemplos de configuraciones para el tipo de servicio CVS-Performance.

### Ejemplo 1: Configuración mínima

Esta es la configuración de back-end mínima usando el tipo de servicio CVS-Performance predeterminado con el nivel de servicio "estándar" predeterminado.

```

---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com

```



## Ejemplo 2: Configuración de nivel de servicio

Este ejemplo muestra las opciones de configuración del back-end, incluidos el nivel de servicio y los valores predeterminados de volumen.

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
proxyURL: http://proxy-server-hostname/
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 10Ti
serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '5'
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  size: 5Ti
```

### Ejemplo 3: Configuración de pool virtual

Este ejemplo utiliza `storage` para configurar los pools virtuales y el `StorageClasses` eso se refiere a ellos. Consulte [Definiciones de clases de almacenamiento](#) para ver cómo se definieron las clases de almacenamiento.

Aquí, se establecen valores predeterminados específicos para todos los pools virtuales, con los que se establece el `snapshotReserve` con el 5% y la `exportRule` a 0.0.0.0/0. Los pools virtuales se definen en la `storage` sección. Cada pool virtual individual define el suyo propio `serviceLevel`, y algunos pools sobrescriben los valores predeterminados. Se utilizaron etiquetas de pools virtuales para diferenciar los pools según `performance` y `protection`.

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
nfsMountOptions: vers=3,proto=tcp,timeo=600
defaults:
  snapshotReserve: '5'
  exportRule: 0.0.0.0/0
labels:
  cloud: gcp
region: us-west2
storage:
- labels:
  performance: extreme
  protection: extra
  serviceLevel: extreme
```

```

defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
  exportRule: 10.0.0.0/24
- labels:
  performance: extreme
  protection: standard
  serviceLevel: extreme
- labels:
  performance: premium
  protection: extra
  serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
- labels:
  performance: premium
  protection: standard
  serviceLevel: premium
- labels:
  performance: standard
  serviceLevel: standard

```

### Definiciones de clases de almacenamiento

Las siguientes definiciones de StorageClass se aplican al ejemplo de configuración de pool virtual. Uso `parameters.selector`, Puede especificar para cada clase de almacenamiento el pool virtual utilizado para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

## Ejemplo de clase de almacenamiento

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=standard"
allowVolumeExpansion: true
```

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=extra"
allowVolumeExpansion: true
```

- El primer tipo de almacenamiento (`cvs-extreme-extra-protection`) se asigna al primer grupo virtual. Se trata del único pool que ofrece un rendimiento extremo con una reserva Snapshot del 10%.
- The Last StorageClass (`cvs-extra-protection`) llama a cualquier pool de almacenamiento que proporciona una reserva de instantáneas del 10%. Trident decide qué pool virtual se selecciona y garantiza que se cumpla el requisito de reserva de snapshots.

### Ejemplos de tipo de servicio CVS

Los siguientes ejemplos proporcionan configuraciones de ejemplo para el tipo de servicio CVS.

## Ejemplo 1: Configuración mínima

Esta es la configuración mínima del back-end mediante `storageClass` Para especificar el tipo de servicio CVS y el valor predeterminado `standardsw` nivel de servicio.

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
storageClass: software
apiRegion: us-east4
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
serviceLevel: standardsw
```

## Ejemplo 2: Configuración del pool de almacenamiento

Esta configuración de entorno de administración de ejemplo utiliza `storagePools` para configurar un pool de almacenamiento.

```
---
version: 1
storageDriverName: gcp-cvs
backendName: gcp-std-so-with-pool
projectNumber: '531265380079'
apiRegion: europe-west1
apiKey:
  type: service_account
  project_id: cloud-native-data
  private_key_id: "<id_value>"
  private_key: |-
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@cloud-native-
data.iam.gserviceaccount.com
  client_id: '107071413297115343396'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40cloud-native-data.iam.gserviceaccount.com
storageClass: software
zone: europe-west1-b
network: default
storagePools:
- 1bc7f380-3314-6005-45e9-c7dc8c2d7509
serviceLevel: Standardsw
```

## El futuro

Después de crear el archivo de configuración del back-end, ejecute el siguiente comando:

```
tridentctl create backend -f <backend-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando create.

## Configure un back-end de NetApp HCI o SolidFire

Aprende a crear y usar un back-end de Element con tu instalación de Trident.

### Detalles del controlador de elementos

Trident proporciona `solidfire-san` el controlador de almacenamiento para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

```
`solidfire-san`El controlador de almacenamiento admite los modos de volumen _FILE_ y _BLOCK_. Para el `Filesystem` volumeMode, Trident crea un volumen y crea un sistema de archivos. El tipo de sistema de archivos se especifica mediante StorageClass.
```

Controlador	Protocolo	Modo VolumeMode	Modos de acceso compatibles	Sistemas de archivos compatibles
solidfire-san	ISCSI	Bloque	RWO, ROX, RWX, RWOP	No hay sistema de archivos. Dispositivo de bloque RAW.
solidfire-san	ISCSI	Sistema de archivos	RWO, RWOP	xfv, ext3, ext4

### Antes de empezar

Necesitarás lo siguiente antes de crear un backend de elemento.

- Es un sistema de almacenamiento compatible que ejecuta el software Element.
- Credenciales a un usuario administrador del clúster o inquilino de HCI de NetApp/SolidFire que puede gestionar volúmenes.
- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulte ["información de preparación del nodo de trabajo"](#).

### Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
version		Siempre 1



Parámetro	Descripción	Predeterminado
storageDriverName	Nombre del controlador de almacenamiento	Siempre "solidfire-san"
backendName	Nombre personalizado o el back-end de almacenamiento	Dirección IP "SolidFire_" + almacenamiento (iSCSI)
Endpoint	MVIP para el clúster de SolidFire con credenciales de inquilino	
SVIP	La dirección IP y el puerto de almacenamiento (iSCSI)	
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes.	""
TenantName	Nombre de inquilino que se va a usar (creado si no se encuentra)	
InitiatorIFace	Restringir el tráfico de iSCSI a una interfaz de host específica	"predeterminado"
UseCHAP	Utilice CHAP para autenticar iSCSI. Trident utiliza CHAP.	verdadero
AccessGroups	Lista de ID de grupos de acceso que se van a usar	Busca el código de un grupo de acceso denominado "trident".
Types	Especificaciones de calidad de servicio	
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}	nulo



No utilizar `debugTraceFlags` a menos que esté solucionando problemas y necesite un volcado de registro detallado.

### Ejemplo 1: Configuración de back-end para `solidfire-san` controlador con tres tipos de volumen

Este ejemplo muestra un archivo de back-end mediante autenticación CHAP y modelado de tres tipos de volúmenes con garantías de calidad de servicio específicas. Lo más probable es que, a continuación, defina clases de almacenamiento para consumir cada una de ellas mediante el `IOPS` parámetro de clase de almacenamiento.

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000

```

## Ejemplo 2: Configuración de clase de almacenamiento y de entorno de administración para solidfire-san controlador con pools virtuales

En este ejemplo, se muestra el archivo de definición del back-end configurado con pools virtuales junto con StorageClasses que les devuelve referencia.

Las etiquetas de copias de Trident están presentes en un pool de almacenamiento en el LUN de almacenamiento back-end en el momento del aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En el archivo de definición de backend de ejemplo que se muestra a continuación, se establecen valores predeterminados específicos para todos los grupos de almacenamiento, que establecen el `type` En Silver. Los pools virtuales se definen en la `storage` sección. En este ejemplo, algunos pools de almacenamiento establecen su propio tipo, y algunos pools anulan los valores predeterminados definidos anteriormente.

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0

```

```

SVIP: "<svip>:3260"
TenantName: "<tenant>"
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver
labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
  performance: gold
  cost: '4'
  zone: us-east-1a
  type: Gold
- labels:
  performance: silver
  cost: '3'
  zone: us-east-1b
  type: Silver
- labels:
  performance: bronze
  cost: '2'
  zone: us-east-1c
  type: Bronze
- labels:
  performance: silver
  cost: '1'
  zone: us-east-1d

```

Las siguientes definiciones de StorageClass se refieren a los pools virtuales anteriores. Con el

`parameters.selector` Field, cada clase de almacenamiento llama a qué pools virtuales se pueden utilizar para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

El primer StorageClass (`solidfire-gold-four`) se asignará al primer pool virtual. Este es el único pool que ofrece rendimiento de oro con `Volume Type QoS` de Oro. The Last StorageClass (`solidfire-silver`) llama a cualquier pool de almacenamiento que ofrece un rendimiento óptimo. Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"
```

## Obtenga más información

- ["Los grupos de acceso de volúmenes"](#)

## Unidades SAN de ONTAP

### Información general del controlador de SAN de ONTAP

Obtenga información sobre la configuración de un back-end de ONTAP con controladores SAN de ONTAP y Cloud Volumes ONTAP.

### Información sobre el controlador de SAN de ONTAP

Trident proporciona los siguientes controladores de almacenamiento SAN para comunicarse con el clúster de ONTAP. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-san	ISCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
ontap-san	ISCSI	Sistema de archivos	RWO, RWOP  ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfis, ext3, ext4
ontap-san	NVMe/TCP  Consulte <a href="#">Consideraciones adicionales para NVMe/TCP.</a>	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
ontap-san	NVMe/TCP  Consulte <a href="#">Consideraciones adicionales para NVMe/TCP.</a>	Sistema de archivos	RWO, RWOP  ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfis, ext3, ext4
ontap-san-economy	ISCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar

Controlador	Protocolo	VolumenMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-san-economy	ISCSI	Sistema de archivos	RWO, RWOP  ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfs, ext3, ext4



- Uso `ontap-san-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)".
- Uso `ontap-nas-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)" y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.

### Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el usuario del clúster o `vsadmin` un usuario de SVM, `admin` o bien como usuario con un nombre distinto que tenga el mismo rol. Para puestas en marcha de Amazon FSx para NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, utilizando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o como un usuario con un nombre distinto que tenga el mismo rol. `fsxadmin` El usuario es un sustituto limitado para el usuario administrador del clúster.



Si se usa `limitAggregateUsage` el parámetro, se requieren permisos de administrador del clúster. Cuando se usa Amazon FSx para NetApp ONTAP con Trident, el `limitAggregateUsage` parámetro no funcionará con `vsadmin` las cuentas de usuario y `fsxadmin` La operación de configuración generará un error si se especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que puede utilizar un controlador Trident, no lo recomendamos. La mayoría de las nuevas versiones de Trident denominan API adicionales que se tendrían que tener en cuenta, por lo que las actualizaciones son complejas y propensas a errores.

### Consideraciones adicionales para NVMe/TCP

Trident admite el protocolo exprés de memoria no volátil (NVMe) mediante `ontap-san` el controlador que se incluye:

- IPv6
- Snapshots y clones de volúmenes NVMe
- Cambiar el tamaño de un volumen NVMe
- Se importa un volumen NVMe que se creó fuera de Trident para que su ciclo de vida se pueda gestionar mediante Trident
- Multivía nativa de NVMe
- Cierre correcto o sin complicaciones de los K8s nodos (24,06)

Trident no admite:

- DH-HMAC-CHAP que es compatible con NVMe de forma nativa
- Rutas múltiples del asignador de dispositivos (DM)
- Cifrado LUKS

## Prepárese para configurar el back-end con los controladores SAN de ONTAP

Conozca los requisitos y las opciones de autenticación para configurar un back-end de ONTAP con controladores SAN de ONTAP.

### Requisitos

Para todos los back-ends de ONTAP, Trident requiere al menos un agregado asignado a la SVM.

Recuerde que también puede ejecutar más de un controlador y crear clases de almacenamiento que señalen a uno o a otro. Por ejemplo, puede configurar un `san-dev` clase que utiliza `ontap-san` controlador y a `san-default` clase que utiliza `ontap-san-economy` uno.

Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulte "[Prepare el nodo de trabajo](#)" para obtener más detalles.

### Autentique el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP.

- Basado en credenciales: El nombre de usuario y la contraseña de un usuario ONTAP con los permisos requeridos. Se recomienda utilizar un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin`. Garantizar la máxima compatibilidad con versiones de ONTAP.
- Basado en certificado: Trident también puede comunicarse con un clúster de ONTAP mediante un certificado instalado en el back-end. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puede actualizar los back-ends existentes para moverse entre métodos basados en credenciales y basados en certificados. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a un método de autenticación diferente, debe eliminar el método existente de la configuración del back-end.



Si intenta proporcionar **tanto credenciales como certificados**, la creación de backend fallará y se producirá un error en el que se haya proporcionado más de un método de autenticación en el archivo de configuración.

### Habilite la autenticación basada en credenciales

Trident requiere que las credenciales se comuniquen con un administrador de SVM o con el ámbito del clúster para que se comunique con el back-end de ONTAP. Se recomienda hacer uso de roles estándar, predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones que podrán utilizarse en futuras versiones de Trident. Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Una definición de backend de ejemplo tendrá este aspecto:



## YAML

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

## JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

Tenga en cuenta que la definición de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. Una vez creado el back-end, los nombres de usuario y las contraseñas se codifican con Base64 y se almacenan como secretos de Kubernetes. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. Por tanto, es una operación de solo administración que deberá realizar el administrador de Kubernetes o almacenamiento.

### Habilite la autenticación basada en certificados

Los back-ends nuevos y existentes pueden utilizar un certificado y comunicarse con el back-end de ONTAP. Se necesitan tres parámetros en la definición de backend.

- **ClientCertificate:** Valor codificado en base64 del certificado de cliente.
- **ClientPrivateKey:** Valor codificado en base64 de la clave privada asociada.
- **TrustedCACertificate:** Valor codificado en base64 del certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico implica los pasos siguientes.

### Pasos

1. Genere una clave y un certificado de cliente. Al generar, establezca el nombre común (CN) en el usuario de ONTAP para autenticarse como.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
```

2. Añada un certificado de CA de confianza al clúster ONTAP. Es posible que ya sea gestionado por el administrador de almacenamiento. Ignore si no se utiliza ninguna CA de confianza.

```
security certificate install -type server -cert-name <trusted-ca-cert-
name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca
<cert-authority>
```

3. Instale el certificado y la clave de cliente (desde el paso 1) en el clúster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Confirme los compatibilidad con el rol de inicio de sesión de seguridad ONTAP cert método de autenticación.

```
security login create -user-or-group-name admin -application ontapi
-authentication-method cert
security login create -user-or-group-name admin -application http
-authentication-method cert
```

5. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de SVM.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Codifique certificados, claves y certificados de CA de confianza con Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Cree un backend utilizando los valores obtenidos del paso anterior.

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "trustedCACertificate": "QNFinfO...SiqOyN",
  "storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |           UUID           |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |         0 |
+-----+-----+-----+-----+
+-----+-----+
```

### Actualice los métodos de autenticación o gire las credenciales

Puede actualizar un back-end existente para utilizar un método de autenticación diferente o para rotar sus credenciales. Esto funciona de las dos maneras: Los back-ends que utilizan nombre de usuario/contraseña se pueden actualizar para usar certificados. Los back-ends que utilizan certificados pueden actualizarse a nombre de usuario/contraseña. Para ello, debe eliminar el método de autenticación existente y agregar el nuevo método de autenticación. A continuación, utilice el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutarse `tridentctl backend update`.

```

cat cert-backend-updated.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |          UUID          |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |      9 |
+-----+-----+-----+
+-----+-----+

```



Quando gira contraseñas, el administrador de almacenamiento debe actualizar primero la contraseña del usuario en ONTAP. A esto le sigue una actualización de back-end. Al rotar certificados, se pueden agregar varios certificados al usuario. A continuación, el back-end se actualiza para usar el nuevo certificado, siguiendo el cual se puede eliminar el certificado antiguo del clúster de ONTAP.

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que Trident puede comunicarse con el back-end de ONTAP y manejar operaciones de volumen futuras.

### Crear rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privileges mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "[Generador de roles personalizados de Trident](#)" para obtener más información sobre la creación de roles personalizados de Trident.

## Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

2. Cree un nombre de usuario para el usuario de Trident:

```
security login create -username <user_name\> -application ontapi  
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver  
<svm_name\> -comment "user_description"
```

3. Asignar el rol al usuario:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

## Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado:**

- a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

(O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > required svm > Settings > Users and Roles**.

- b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.

- c. Seleccione **+Agregar** en **Roles**.

- d. Defina las reglas para el rol y haga clic en **Guardar**.

2. **Asignar el rol al usuario de Trident:** + Realizar los siguientes pasos en la página **Usuarios y Roles**:

- a. Seleccione Agregar icono **+** en **Usuarios**.

- b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.

- c. Haga clic en **Guardar**.

Consulte las siguientes páginas si quiere más información:

- ["Roles personalizados para la administración de ONTAP"](#) o ["Definir funciones personalizadas"](#)
- ["Trabajar con roles y usuarios"](#)

## Autentica conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para `ontap-san` los controladores y `ontap-san-economy`. Esto requiere la activación de `useCHAP` la opción en la definición de backend. Cuando se establece en `true`, Trident configura la seguridad del iniciador predeterminado de la SVM como CHAP bidireccional y establece el nombre de usuario y los secretos del archivo back-end. NetApp recomienda utilizar CHAP bidireccional para autenticar las conexiones. Consulte la siguiente configuración de ejemplo:

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
```



La `useCHAP` Parameter es una opción booleana que solo se puede configurar una vez. De forma predeterminada, se establece en `FALSE`. Después de configurarlo en `true`, no puede establecerlo en `false`.

Además de `useCHAP=true`, la `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername`, y `chapUsername` los campos deben incluirse en la definición del backend. Los secretos se pueden cambiar después de crear un back-end ejecutando `tridentctl update`.

### Cómo funciona

Al configurarse `useCHAP` en `true`, el administrador de almacenamiento le ordena a Trident que configure CHAP en el back-end de almacenamiento. Esto incluye lo siguiente:

- Configuración de CHAP en la SVM:
  - Si el tipo de seguridad de iniciador predeterminado de la SVM es `none` (establecido de forma predeterminada) y no hay LUN preexistentes ya presentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en `CHAP` y continuará configurando el iniciador CHAP y el nombre de usuario y los secretos de destino.
  - Si la SVM contiene LUN, Trident no habilitará CHAP en la SVM. De este modo se garantiza que no se restrinja el acceso a las LUN que ya están presentes en la SVM.
- Configurar el iniciador de CHAP, el nombre de usuario y los secretos de destino; estas opciones deben especificarse en la configuración del back-end (como se muestra más arriba).

Después de crear el backend, Trident crea un CRD correspondiente `tridentbackend` y almacena los secretos CHAP y nombres de usuario como secretos de Kubernetes. Todos los VP que crea Trident en este back-end se montarán y conectarán mediante CHAP.

### Rotar las credenciales y actualizar los back-ends

Para actualizar las credenciales de CHAP, se deben actualizar los parámetros de CHAP en `backend.json` archivo. Para ello, será necesario actualizar los secretos CHAP y utilizar el `tridentctl update` comando para reflejar estos cambios.



Al actualizar los secretos CHAP para un backend, debe utilizar `tridentctl` para actualizar el backend. No actualice las credenciales en el clúster de almacenamiento a través de la interfaz de usuario de CLI/ONTAP, ya que Trident no podrá recoger estos cambios.

```
cat backend-san.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "password",
  "chapInitiatorSecret": "cl9qxUpDaTeD",
  "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|  NAME          | STORAGE DRIVER |          UUID                               |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online |       7 |
+-----+-----+-----+-----+
+-----+-----+
```

Las conexiones existentes no se verán afectadas; seguirán activas si las credenciales se actualizan mediante Trident en la SVM. Las nuevas conexiones utilizan las credenciales actualizadas y las conexiones existentes siguen activas. Al desconectar y volver a conectar los VP antiguos, se utilizarán las credenciales actualizadas.

## Opciones y ejemplos de configuración DE SAN ONTAP


Aprenda a crear y utilizar controladores SAN de ONTAP con su instalación de Trident. Esta sección proporciona ejemplos de configuración de backend y detalles para la asignación de back-ends a StorageClasses.

### Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDrive rName	Nombre del controlador de almacenamiento	ontap-nas, ontap-nas- economy, ontap-nas- flexgroup, ontap-san, ontap- san-economy
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos
managementLIF	La dirección IP de un clúster o una LIF de gestión de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555] como . Para una conmutación de sitios MetroCluster fluida, consulte <a href="#">[mcc-best]</a> .	“10.0.0.1”, “[2001:1234:abcd::fefe]”
dataLIF	Dirección IP de LIF de protocolo. <b>No especifique para iSCSI.</b> Trident utiliza <a href="#">"Asignación de LUN selectiva de ONTAP"</a> para descubrir las LIF iSCSI necesarias para establecer una sesión de rutas múltiples. Se genera una advertencia si dataLIF se define explícitamente. <b>Omitir para MetroCluster.</b> Consulte la <a href="#">[mcc-best]</a> .	Derivado del SVM
svm	Máquina virtual de almacenamiento que usar  <b>Omitir para MetroCluster.</b> Ver <a href="#">[mcc-best]</a> .	Derivado si una SVM managementLIF está especificado
useCHAP	Use CHAP para autenticar iSCSI para los controladores SAN de ONTAP [Boolean]. Establezca como true para que Trident configure y utilice CHAP bidireccional como la autenticación predeterminada para la SVM especificada en el back-end. Consulte <a href="#">"Prepárese para configurar el back-end con los controladores SAN de ONTAP"</a> para obtener más información.	false
chapInitiatorSecret	Secreto CHAP del iniciador. Obligatorio si useCHAP=true	""
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
chapTargetInitiatorSecret	Secreto CHAP del iniciador de destino. Obligatorio si useCHAP=true	""
chapUsername	Nombre de usuario entrante. Obligatorio si useCHAP=true	""
chapTargetUsername	Nombre de usuario de destino. Obligatorio si useCHAP=true	""



Parámetro	Descripción	Predeterminado
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	El nombre de usuario necesario para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
password	La contraseña necesaria para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
svm	Máquina virtual de almacenamiento que usar	Derivado si una SVM managementLIF está especificado
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede modificar más adelante. Para actualizar este parámetro, deberá crear un nuevo backend.	trident
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el <code>ontap-nas-flexgroup</code> controlador, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles puede usarse para aprovisionar un volumen FlexGroup.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Quando el agregado se actualiza en SVM, se actualiza automáticamente en Trident sondeando SVM sin tener que reiniciar la controladora Trident. Cuando se haya configurado un agregado específico en Trident para aprovisionar volúmenes, si se cambia el nombre de este agregado o se saca de la SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar el agregado por uno presente en la SVM o quitarlo por completo para que el back-end vuelva a estar en línea.</p> </div>	""

Parámetro	Descripción	Predeterminado
limitAggregateUsage	Error al aprovisionar si el uso supera este porcentaje. Si estás usando un backend de Amazon FSx for NetApp ONTAP, no especifiques <code>limitAggregateUsage</code> . El proporcionado <code>fsxadmin</code> y <code>vsadmin</code> no contiene los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Trident.	"" (no se aplica de forma predeterminada)
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. Además, restringe el tamaño máximo de los volúmenes que gestiona para las LUN.	" (no se aplica por defecto)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	100
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true}  No lo utilice a menos que esté solucionando problemas y necesite un volcado de log detallado.	null
useREST	Parámetro booleano para usar las API DE REST de ONTAP. <code>useREST</code> Cuando se define en <code>true</code> , Trident utiliza las API REST DE ONTAP para comunicarse con el backend; cuando se define en <code>false</code> , Trident utiliza llamadas de ONTAP ZAPI para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> la aplicación. Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code> . A partir de la versión Trident 24,06 y ONTAP 9.15,1 o posterior, <code>useREST</code> se establece en <code>true</code> de forma predeterminada; cambie <code>useREST</code> a <code>false</code> Usar llamadas ZAPI de ONTAP. <code>useREST</code> Está totalmente cualificado para NVMe/TCP.	<code>true</code> Para ONTAP 9.15.1 o posterior, de lo contrario <code>false</code> .
sanType	Utilice para seleccionar <code>iscsi</code> para iSCSI, <code>nvme</code> para NVMe/TCP o <code>fcp</code> para SCSI over Fibre Channel (FC). <b>'fcp' (SCSI sobre FC) es una función de previsualización técnica en la versión Trident 24,10.</b>	<code>iscsi</code> si está en blanco

Parámetro	Descripción	Predeterminado
formatOptions	Puede <code>formatOptions</code> usarse para especificar argumentos de línea de comandos para <code>mkfs</code> el comando, que se aplicará cada vez que se formatee un volumen. Esto permite formatear el volumen según sus preferencias. Asegúrese de especificar las opciones <code>formatOptions</code> similares a las de los comandos <code>mkfs</code> , excluyendo la ruta del dispositivo. Ejemplo: «-E nodiscard»  <b>Compatible <code>ontap-san</code> <code>ontap-san-economy</code> solo para conductores y.</b>	
limitVolumePoolSize	Tamaño máximo de FlexVol solicitable al usar LUN en back-end económico de ONTAP-san.	"" (no se aplica de forma predeterminada)
denyNewVolumePools	Restringe <code>ontap-san-economy</code> los back-ends para que no creen nuevos volúmenes de FlexVol para contener sus LUN. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	

## Recomendaciones para utilizar `formatOptions`

Trident recomienda la siguiente opción para acelerar el proceso de formato:

### -E nodiscard:

- Keep, no intente descartar bloques en `mkfs time` (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento ligero/Thin-Provisioning). Esto reemplaza la opción anticuada “-K” y es aplicable a todos los sistemas de archivos (xfs, ext3 y ext4).

## Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para las LUN	verdadero
spaceReserve	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	ninguno
snapshotPolicy	Política de Snapshot que se debe usar	ninguno

Parámetro	Descripción	Predeterminado
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento. Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	«0» si snapshotPolicy no es "ninguno", de lo contrario
splitOnClone	Divida un clon de su elemento principal al crearlo	"falso"
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE. Para obtener más información, consulte: <a href="#">"Cómo funciona Trident con NVE y NAE"</a> .	"falso"
luksEncryption	Active el cifrado LUKS. Consulte <a href="#">"Usar la configuración de clave unificada de Linux (LUKS)"</a> .  El cifrado LUKS no es compatible con NVMe/TCP.	""
securityStyle	Estilo de seguridad para nuevos volúmenes	unix
tieringPolicy	Política de organización en niveles para utilizar ninguna	«Solo Snapshot» para la configuración SVM-DR anterior a ONTAP 9,5
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""

## Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados definidos:

```

---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'

```



Para todos los volúmenes creados con `ontap-san` el controlador, Trident añade un 10 % de capacidad adicional al FlexVol para acomodar los metadatos del LUN. La LUN se aprovisionará con el tamaño exacto que el usuario solicite en la RVP. Trident agrega un 10 % a FlexVol (se muestra como tamaño disponible en ONTAP). Los usuarios obtienen ahora la cantidad de capacidad utilizable que soliciten. Este cambio también impide que las LUN se conviertan en de solo lectura a menos que se utilice completamente el espacio disponible. Esto no se aplica a `ontap-san-economy`.

Para los back-ends que definen `snapshotReserve`, Trident calcula el tamaño de los volúmenes de la siguiente manera:

```

Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1

```

El 1,1 es el 10 % adicional que Trident agrega a la FlexVol para acomodar los metadatos de la LUN. Para `snapshotReserve = 5%`, y solicitud de PVC = 5GiB, el tamaño total del volumen es 5,79GiB y el tamaño disponible es 5,5GiB. El `volume show` comando debería mostrar resultados similares a este ejemplo:

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

En la actualidad, el cambio de tamaño es la única manera de utilizar el nuevo cálculo para un volumen existente.

### Ejemplos de configuración mínima

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.



Si utiliza Amazon FSx en NetApp ONTAP con Trident, le recomendamos que especifique nombres de DNS para las LIF en lugar de direcciones IP.

### Ejemplo de SAN ONTAP

Se trata de una configuración básica que utiliza el `ontap-san` controlador.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

### Ejemplo de economía de SAN ONTAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
username: vsadmin
password: <password>
```

## 1. ejemplo

Puede configurar el backend para evitar tener que actualizar manualmente la definición de backend después del switchover y el switchover durante "[Replicación y recuperación de SVM](#)".

Para obtener una conmutación de sitios y una conmutación de estado sin problemas, especifique la SVM con `managementLIF` y omita la `dataLIF` y.. `svm` parámetros. Por ejemplo:

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

### Ejemplo de autenticación basada en certificados

En este ejemplo de configuración básica `clientCertificate`, `clientPrivateKey`, y `trustedCACertificate` (Opcional, si se utiliza una CA de confianza) se completan en `backend.json` Y tome los valores codificados base64 del certificado de cliente, la clave privada y el certificado de CA de confianza, respectivamente.

```
---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

## Ejemplos de CHAP bidireccional

Estos ejemplos crean un backend con `useCHAP` establezca en `true`.

### Ejemplo de CHAP de SAN de ONTAP

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
```

### Ejemplo de CHAP de economía de SAN ONTAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
```



## Ejemplo de NVMe/TCP

Debe tener una SVM configurada con NVMe en el back-end de ONTAP. Esta es una configuración de back-end básica para NVMe/TCP.

```
---
version: 1
backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true
```

## Ejemplo de configuración de backend con nameTemplate

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap-san-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults: {
  "nameTemplate":
    "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.volume.RequestName}}"
},
"labels": {"cluster": "ClusterA", "PVC":
  "{{.volume.Namespace}}_{{.volume.RequestName}}"}
}
```

## Ejemplo de formatOptions para el controlador `ONTAP-san-economy`

```
version: 1
storageDriverName: ontap-san-economy
managementLIF: ''
svm: svm1
username: ''
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: "-E nodiscard"
```

### Ejemplos de back-ends con pools virtuales

En estos archivos de definición de backend de ejemplo, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo de comentarios. Los comentarios se establecen en la FlexVol. Trident copia todas las etiquetas presentes en un pool virtual en el volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los pools de almacenamiento establecen sus propios `spaceReserve`, `spaceAllocation`, y `encryption` y algunos pools sustituyen los valores predeterminados.

**Ejemplo de SAN ONTAP**



```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '40000'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
    adaptiveQosPolicy: adaptive-extreme
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
    qosPolicy: premium
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
```

## Ejemplo de economía de SAN ONTAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
labels:
  store: san_economy_store
region: us_east_1
storage:
- labels:
  app: oracledb
  cost: '30'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
- labels:
  app: postgresdb
  cost: '20'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
- labels:
  app: mysqldb
  cost: '10'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
- labels:
  department: legal
  creditpoints: '5000'
  zone: us_east_1c
```

```
defaults:
  spaceAllocation: 'true'
  encryption: 'false'
```

## Ejemplo de NVMe/TCP

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: 'false'
  encryption: 'true'
storage:
- labels:
  app: testApp
  cost: '20'
  defaults:
    spaceAllocation: 'false'
    encryption: 'false'
```

## Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass hacen referencia a la [Ejemplos de back-ends con pools virtuales](#). Con el `parameters.selector` Cada StorageClass llama la atención sobre qué pools virtuales pueden usarse para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- La `protection-gold` StorageClass se asignará al primer pool virtual del `ontap-san` back-end. Este es el único pool que ofrece protección de nivel Gold.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- La `protection-not-gold` StorageClass se asignará al segundo y tercer pool virtual en `ontap-san` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto del oro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- La `app-mysqldb` StorageClass se asignará al tercer pool virtual en `ontap-san-economy` back-end. Este es el único pool que ofrece configuración de pool de almacenamiento para la aplicación de tipo `mysqldb`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- La `protection-silver-creditpoints-20k` StorageClass se asignará al segundo pool virtual de `ontap-san` back-end. Este es el único pool que ofrece protección de nivel plata y 20000 puntos de crédito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
```

- La `creditpoints-5k` StorageClass se asignará al tercer pool virtual en `ontap-san` backend y cuarto pool virtual en `ontap-san-economy` back-end. Estas son las únicas ofertas de grupo con 5000 puntos de crédito.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

- La `my-test-app-sc` StorageClass se asignará al `testAPP` pool virtual en el `ontap-san` conductor con `sanType: nvme`. Esta es la única oferta de pool `testApp`.

```

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: my-test-app-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=testApp"
  fsType: "ext4"

```

Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

## Unidades NAS de ONTAP

### Información general del controlador NAS de ONTAP

Obtenga información sobre la configuración de un back-end de ONTAP con controladores NAS de ONTAP y Cloud Volumes ONTAP.

### Información del controlador NAS de ONTAP

Trident proporciona los siguientes controladores de almacenamiento NAS para comunicarse con el clúster de ONTAP. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-nas	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb
ontap-nas-economy	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb



Controlador	Protocolo	VolumenMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-nas-flexgroup	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb



- Uso `ontap-san-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)".
- Uso `ontap-nas-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)" y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.

### Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el usuario del clúster o `vsadmin` un usuario de SVM, `admin` o bien como usuario con un nombre distinto que tenga el mismo rol.

Para puestas en marcha de Amazon FSx para NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, utilizando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o como un usuario con un nombre distinto que tenga el mismo rol. `fsxadmin` El usuario es un sustituto limitado para el usuario administrador del clúster.



Si se usa `limitAggregateUsage` el parámetro, se requieren permisos de administrador del clúster. Cuando se usa Amazon FSx para NetApp ONTAP con Trident, el `limitAggregateUsage` parámetro no funcionará con `vsadmin` las cuentas de usuario y `fsxadmin` La operación de configuración generará un error si se especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que puede utilizar un controlador Trident, no lo recomendamos. La mayoría de las nuevas versiones de Trident denominan API adicionales que se tendrían que tener en cuenta, por lo que las actualizaciones son complejas y propensas a errores.

### Prepárese para configurar un back-end con controladores NAS de ONTAP

Conozca los requisitos, las opciones de autenticación y las políticas de exportación para configurar un backend de ONTAP con controladores NAS de ONTAP.

#### Requisitos

- Para todos los back-ends de ONTAP, Trident requiere al menos un agregado asignado a la SVM.
- Puede ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, puede configurar una clase Gold que utilice `ontap-nas` Controlador y clase Bronze que utiliza `ontap-nas-economy` uno.
- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulte "[aquí](#)" para obtener más detalles.
- Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte [Prepárese para aprovisionar los volúmenes de SMB](#) para obtener más información.

## Autentique el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP.

- **Basado en Credenciales:** Este modo requiere permisos suficientes para el backend de ONTAP. Se recomienda utilizar una cuenta asociada con un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin`. Garantizar la máxima compatibilidad con versiones de ONTAP.
- **Basado en certificado:** Este modo requiere un certificado instalado en el back-end para que Trident se comunique con un clúster de ONTAP. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puede actualizar los back-ends existentes para moverse entre métodos basados en credenciales y basados en certificados. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a un método de autenticación diferente, debe eliminar el método existente de la configuración del back-end.



Si intenta proporcionar **tanto credenciales como certificados**, la creación de backend fallará y se producirá un error en el que se haya proporcionado más de un método de autenticación en el archivo de configuración.

## Habilite la autenticación basada en credenciales

Trident requiere que las credenciales se comuniquen con un administrador de SVM o con el ámbito del clúster para que se comunique con el back-end de ONTAP. Se recomienda hacer uso de roles estándar, predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones que podrán utilizarse en futuras versiones de Trident. Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Una definición de backend de ejemplo tendrá este aspecto:

## YAML

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

## JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

Tenga en cuenta que la definición de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. Una vez creado el back-end, los nombres de usuario y las contraseñas se codifican con Base64 y se almacenan como secretos de Kubernetes. La creación/mejora de un backend es el único paso que requiere conocimiento de las credenciales. Por tanto, es una operación de solo administración que deberá realizar el administrador de Kubernetes o almacenamiento.

### Habilite la autenticación basada en certificados

Los back-ends nuevos y existentes pueden utilizar un certificado y comunicarse con el back-end de ONTAP. Se necesitan tres parámetros en la definición de backend.

- `ClientCertificate`: Valor codificado en base64 del certificado de cliente.
- `ClientPrivateKey`: Valor codificado en base64 de la clave privada asociada.
- `TrustedCACertificate`: Valor codificado en base64 del certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico implica los pasos siguientes.

### Pasos

1. Genere una clave y un certificado de cliente. Al generar, establezca el nombre común (CN) en el usuario

de ONTAP para autenticarse como.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. Añada un certificado de CA de confianza al clúster ONTAP. Es posible que ya sea gestionado por el administrador de almacenamiento. Ignore si no se utiliza ninguna CA de confianza.

```
security certificate install -type server -cert-name <trusted-ca-cert-  
name> -vserver <vserver-name>  
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled  
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca  
<cert-authority>
```

3. Instale el certificado y la clave de cliente (desde el paso 1) en el clúster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-  
name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Confirme los compatibilidad con el rol de inicio de sesión de seguridad ONTAP `cert` método de autenticación.

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

5. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de SVM. Debe asegurarse de que la LIF tiene su política de servicio establecida en `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-  
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key  
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp  
xmlns="http://www.netapp.com/filer/admin" version="1.21"  
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Codifique certificados, claves y certificados de CA de confianza con Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

## 7. Cree un backend utilizando los valores obtenidos del paso anterior.

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |           UUID           |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |         9 |
+-----+-----+-----+
+-----+-----+

```

### Actualice los métodos de autenticación o gire las credenciales

Puede actualizar un back-end existente para utilizar un método de autenticación diferente o para rotar sus credenciales. Esto funciona de las dos maneras: Los back-ends que utilizan nombre de usuario/contraseña se pueden actualizar para usar certificados. Los back-ends que utilizan certificados pueden actualizarse a nombre de usuario/contraseña. Para ello, debe eliminar el método de autenticación existente y agregar el nuevo método de autenticación. A continuación, utilice el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutarse `tridentctl update backend`.

```

cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |           UUID           |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+

```



Quando gira contraseñas, el administrador de almacenamiento debe actualizar primero la contraseña del usuario en ONTAP. A esto le sigue una actualización de back-end. Al rotar certificados, se pueden agregar varios certificados al usuario. A continuación, el back-end se actualiza para usar el nuevo certificado, siguiendo el cual se puede eliminar el certificado antiguo del clúster de ONTAP.

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que Trident puede comunicarse con el back-end de ONTAP y manejar operaciones de volumen futuras.

### Crear rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privileges mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "[Generador de roles personalizados de Trident](#)" para obtener más información sobre la creación de roles personalizados de Trident.

## Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

2. Cree un nombre de usuario para el usuario de Trident:

```
security login create -username <user_name\> -application ontapi  
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver  
<svm_name\> -comment "user_description"
```

3. Asignar el rol al usuario:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

## Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado:**

- a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

(O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > required svm > Settings > Users and Roles**.

- b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.

- c. Seleccione **+Agregar** en **Roles**.

- d. Defina las reglas para el rol y haga clic en **Guardar**.

2. **Asignar el rol al usuario de Trident:** + Realizar los siguientes pasos en la página **Usuarios y Roles**:

- a. Seleccione Agregar icono **+** en **Usuarios**.

- b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.

- c. Haga clic en **Guardar**.

Consulte las siguientes páginas si quiere más información:

- ["Roles personalizados para la administración de ONTAP"](#) o. ["Definir funciones personalizadas"](#)
- ["Trabajar con roles y usuarios"](#)

## Gestione las políticas de exportación de NFS

Trident utiliza políticas de exportación de NFS para controlar el acceso a los volúmenes que aprovisiona.

Trident proporciona dos opciones al trabajar con políticas de exportación:

- Trident puede gestionar de manera dinámica la política de exportación; en este modo de funcionamiento,

el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Trident agrega IP de nodo aplicables que se encuentran en estos rangos a la política de exportación de forma automática en el momento de la publicación. Como alternativa, cuando no se especifica ningún CIDR, todas las IP de unidifusión de ámbito global que se encuentran en el nodo en el que se publica el volumen se agregarán a la política de exportación.

- Los administradores de almacenamiento pueden crear una normativa de exportación y añadir reglas manualmente. Trident utiliza la política de exportación predeterminada a menos que se especifique otro nombre de política de exportación en la configuración.

## Gestione de forma dinámica políticas de exportación

Trident proporciona la capacidad de gestionar dinámicamente políticas de exportación para back-ends de ONTAP. De este modo, el administrador de almacenamiento puede especificar un espacio de direcciones permitido para las IP de nodos de trabajo, en lugar de definir reglas explícitas de forma manual. Simplifica en gran medida la gestión de políticas de exportación; las modificaciones de la política de exportación ya no requieren intervención manual en el clúster de almacenamiento. Además, esto ayuda a restringir el acceso al clúster de almacenamiento solo a los nodos de trabajador que se montan volúmenes y que tienen IP en el rango especificado, lo que permite una gestión automatizada y precisa.



No utilice la traducción de direcciones de red (NAT) cuando utilice políticas de exportación dinámicas. Con NAT, el controlador de almacenamiento ve la dirección NAT de frontend y no la dirección de host IP real, por lo que el acceso se denegará cuando no se encuentre ninguna coincidencia en las reglas de exportación.



En Trident 24,10, `ontap-nas` el controlador de almacenamiento seguirá funcionando como en las versiones anteriores; no se ha realizado ningún cambio en el controlador ONTAP-nas. Solo `ontap-nas-economy` el controlador de almacenamiento tendrá control de acceso granular basado en el volumen en Trident 24,10.

## Ejemplo

Hay dos opciones de configuración que deben utilizarse. He aquí un ejemplo de definición de backend:

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
- 192.168.0.0/24
autoExportPolicy: true
```



Al usar esta función, debe asegurarse de que la unión raíz de la SVM tenga una política de exportación creada previamente con una regla de exportación que permite el bloque CIDR de nodo (como la política de exportación predeterminada). Siga siempre las prácticas recomendadas por NetApp para dedicar una SVM para Trident.



A continuación se ofrece una explicación del funcionamiento de esta función utilizando el ejemplo anterior:

- `autoExportPolicy` se establece en `true`. Esto indica que Trident crea una política de exportación para cada volumen provisionado con este back-end para `svm1` la SVM y administra la adición y eliminación de reglas mediante `autoexportCIDRs` bloques de direcciones. Hasta que un volumen se conecta a un nodo, el volumen usa una política de exportación vacía sin reglas para evitar el acceso no deseado a ese volumen. Cuando se publica un volumen en un nodo, Trident crea una política de exportación con el mismo nombre que el `qtree` subyacente que contiene la IP de nodo en el bloque CIDR especificado. Estas IP también se agregarán a la política de exportación utilizada por la FlexVol principal.
  - Por ejemplo:
    - UUID de backend `403b5326-8482-40dB-96d0-d83fb3f4daec`
    - `autoExportPolicy` establezca en `true`
    - prefijo de almacenamiento `trident`
    - PVC UUID `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
    - el `qtree` denominado `Trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` crea una política de exportación para la FlexVol llamada `trident-403b5326-8482-40db96d0-d83fb3f4daec`, una política de exportación para el `qtree` llamado `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` y una política de exportación vacía denominada `trident_empty` en la SVM. Las reglas de la política de exportación de FlexVol serán un superconjunto de reglas contenidas en las políticas de exportación de `qtree`. La política de exportación vacía será reutilizada por cualquier volumen que no esté asociado.
- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y se establece de forma predeterminada en `["0.0.0.0/0", "*/0"]`. Si no se define, Trident agrega todas las direcciones unicast de ámbito global que se encuentran en los nodos de trabajo con publicaciones.

En este ejemplo, `192.168.0.0/24` se proporciona el espacio de la dirección. Esto indica que las IP de nodo de Kubernetes que se encuentran dentro de este rango de direcciones con publicaciones se agregarán a la política de exportación que crea Trident. Cuando Trident registra un nodo en el que se ejecuta, recupera las direcciones IP del nodo y las comprueba con respecto a los bloques de direcciones proporcionados en `autoExportCIDRs`. En el momento de la publicación, después de filtrar las IP, Trident crea las reglas de política de exportación para las IP del cliente para el nodo en el que está publicando.

Puede actualizar `autoExportPolicy` y `autoExportCIDRs` para los back-ends después de crearlos. Puede añadir CIDR nuevos para un back-end que se gestiona o elimina automáticamente CIDR existentes. Tenga cuidado al eliminar CIDR para asegurarse de que las conexiones existentes no se hayan caído. También puede optar por desactivar `autoExportPolicy` para un back-end y caer en una política de exportación creada manualmente. Esto requerirá establecer la `exportPolicy` parámetro en la configuración del back-end.

Después de que Trident cree o actualice un backend, puede comprobar el backend utilizando `tridentctl` o el CRD correspondiente `tridentbackend`:

```

./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileType: ext4

```

Cuando se elimina un nodo, Trident comprueba todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar esta IP de nodo de las políticas de exportación de los back-ends gestionados, Trident evita los montajes no autorizados, a menos que un nuevo nodo del clúster reutilice esta IP.

Para los back-ends existentes anteriormente, al actualizar el backend con `tridentctl update backend` se garantiza que Trident administre las políticas de exportación automáticamente. Esto crea dos nuevas políticas de exportación llamadas después del UUID del back-end y el nombre de `qtree` cuando son necesarias. Los volúmenes presentes en el back-end utilizarán las políticas de exportación recién creadas después de desmontarlas y montarlas de nuevo.



Si se elimina un back-end con políticas de exportación gestionadas automáticamente, se eliminará la política de exportación creada de forma dinámica. Si se vuelve a crear el back-end, se trata como un nuevo back-end y dará lugar a la creación de una nueva política de exportación.

Si se actualiza la dirección IP de un nodo activo, debe reiniciar el pod de Trident en el nodo. A continuación, Trident actualizará la política de exportación de los back-ends que gestiona para reflejar este cambio de IP.

### Prepárese para aprovisionar los volúmenes de SMB

Con un poco de preparación adicional, puede aprovisionar volúmenes SMB con `ontap-nas` de `windows`



Debe configurar tanto los protocolos NFS como SMB/CIFS en la SVM para crear un `ontap-nas-economy` Volumen SMB para ONTAP en las instalaciones. Si no se configura ninguno de estos protocolos, se producirá un error en la creación del volumen de SMB.



autoExportPolicy No es compatible con los volúmenes de SMB.

## Antes de empezar

Para poder aprovisionar volúmenes de SMB, debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2022. Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Trident que contiene sus credenciales de Active Directory. Para generar secreto smbcreds:

```
kubectl create secret generic smbcreds --from-literal username=user  
--from-literal password='password'
```

- Proxy CSI configurado como servicio de Windows. Para configurar un `csi-proxy`, consulte ["GitHub: Proxy CSI"](#) o ["GitHub: Proxy CSI para Windows"](#) Para nodos Kubernetes que se ejecutan en Windows.

## Pasos

1. Para la ONTAP en las instalaciones, puede crear un recurso compartido de SMB, o bien Trident puede crearlo para usted.



Los recursos compartidos de SMB se requieren para Amazon FSx para ONTAP.

Puede crear recursos compartidos de administrador de SMB de una de dos formas mediante el ["Consola de administración de Microsoft"](#) Complemento carpetas compartidas o uso de la CLI de ONTAP. Para crear los recursos compartidos de SMB mediante la CLI de ONTAP:

- a. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

La `vserver cifs share create` comando comprueba la ruta especificada en la opción `-path` durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

- b. Cree un recurso compartido de SMB asociado con la SVM especificada:

```
vserver cifs share create -vserver vserver_name -share-name  
share_name -path path [-share-properties share_properties,...]  
[other_attributes] [-comment text]
```

- c. Compruebe que se ha creado el recurso compartido:

```
vserver cifs share show -share-name share_name
```



Consulte ["Cree un recurso compartido de SMB"](#) para obtener todos los detalles.

2. Al crear el back-end, debe configurar lo siguiente para especificar volúmenes de SMB. Para obtener información sobre todas las opciones de configuración del entorno de administración de ONTAP, consulte

## "Opciones y ejemplos de configuración de FSX para ONTAP".

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	smb-share
nasType	<b>Debe establecer en smb.</b> Si es nulo, el valor predeterminado es <code>nfs</code> .	smb
securityStyle	Estilo de seguridad para nuevos volúmenes. <b>Debe estar configurado en <code>ntfs</code> o <code>mixed</code> Para volúmenes SMB.</b>	<code>ntfs</code> o <code>mixed</code> Para volúmenes de SMB
unixPermissions	Modo para volúmenes nuevos. <b>Se debe dejar vacío para volúmenes SMB.</b>	""

### Opciones y ejemplos de configuración NAS de ONTAP



Aprenda a crear y utilizar controladores NAS de ONTAP con su instalación de Trident. Esta sección proporciona ejemplos de configuración de backend y detalles para la asignación de back-ends a StorageClasses.


#### Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDrive rName	Nombre del controlador de almacenamiento	«ontap-nas», «ontap-nas-economy», «ontap-nas-flexgroup», «ontap-san», «ontap-san-economy»
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos

Parámetro	Descripción	Predeterminado
managementLIF	Dirección IP de un clúster o una LIF de gestión de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555] como . Para una conmutación de sitios MetroCluster fluida, consulte <a href="#">[mcc-best]</a> .	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	Dirección IP de LIF de protocolo. Recomendamos especificar dataLIF. Si no se encuentra, Trident recupera los LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos. Se puede cambiar después del ajuste inicial. Consulte . Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555] como . <b>Omitir para MetroCluster.</b> Consulte la <a href="#">[mcc-best]</a> .	Dirección especificada o derivada de la SVM, si no se especifica (no recomendada)
svm	Máquina virtual de almacenamiento que usar  <b>Omitir para MetroCluster.</b> Ver <a href="#">[mcc-best]</a> .	Derivado si una SVM managementLIF está especificado
autoExportPolicy	Habilite la creación y actualización automática de la política de exportación [Boolean]. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	falso
autoExportCIDRs	Lista de CIDRs para filtrar las IP del nodo de Kubernetes contra cuando autoExportPolicy se habilita. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	[«0,0,0/0», «:/0»]
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados	""

Parámetro	Descripción	Predeterminado
username	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
password	Contraseña para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
storagePrefix	<p>El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede actualizar después de configurarlo</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Al utilizar ONTAP-nas-economy y un prefijo de almacenamiento con 24 caracteres o más, los qtrees no tendrán el prefijo de almacenamiento incrustado, pero estarán en el nombre del volumen.</p> </div>	«trident»
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el <code>ontap-nas-flexgroup</code> controlador, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles puede usarse para aprovisionar un volumen FlexGroup.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Cuando el agregado se actualiza en SVM, se actualiza automáticamente en Trident sondeando SVM sin tener que reiniciar la controladora Trident. Cuando se haya configurado un agregado específico en Trident para aprovisionar volúmenes, si se cambia el nombre de este agregado o se saca de la SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar el agregado por uno presente en la SVM o quitarlo por completo para que el back-end vuelva a estar en línea.</p> </div>	""
limitAggregateUsage	<p>Error al aprovisionar si el uso supera este porcentaje.  <b>No se aplica a Amazon FSX para ONTAP</b></p>	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
Lista de Agregados de Flexgroup	<p>Lista de agregados para el aprovisionamiento (opcional; si se ha definido, debe asignarse a la SVM). Todos los agregados asignados a la SVM se usan para aprovisionar un volumen FlexGroup. Compatible con el controlador de almacenamiento <b>ONTAP-nas-FlexGroup</b>.</p> <p> Cuando la lista de agregados se actualiza en SVM, la lista se actualiza automáticamente en Trident sondeando la SVM sin tener que reiniciar la controladora Trident. Cuando se configuró una lista de agregado específica en Trident para aprovisionar volúmenes, si se cambia el nombre de la lista de agregados o se sale de SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar la lista de agregados por una que esté presente en la SVM o quitarla por completo para que el back-end vuelva a estar en línea.</p>	""
limitVolumeSize	<p>Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. Además restringe el tamaño máximo de los volúmenes que gestiona para qtrees y la qtreesPerFlexvol opción permite personalizar el número máximo de qtrees por FlexVol.</p>	" (no se aplica por defecto)
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true}</p> <p>No utilizar debugTraceFlags a menos que esté solucionando problemas y necesite un volcado de registro detallado.</p>	nulo
nasType	<p>Configure la creación de volúmenes NFS o SMB. Las opciones son nfs, smb o nulo. El valor predeterminado es nulo en volúmenes de NFS.</p>	nfs

Parámetro	Descripción	Predeterminado
nfsMountOptions	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident volverá a utilizar las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento. Si no se especifican opciones de montaje en la clase almacenamiento o el archivo de configuración, Trident no definirá ninguna opción de montaje en un volumen persistente asociado.	""
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	«200»
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	smb-share
useREST	Parámetro booleano para usar las API DE REST de ONTAP. <code>useREST</code> Cuando se define en <code>true</code> , Trident utiliza las API REST DE ONTAP para comunicarse con el backend; cuando se define en <code>false</code> , Trident utiliza llamadas de ONTAP ZAPI para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> la aplicación. Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code> . A partir de la versión Trident 24,06 y ONTAP 9.15,1 o posterior, <code>useREST</code> se establece en <code>true</code> de forma predeterminada; cambie <code>useREST</code> a <code>false</code> Usar llamadas ZAPI de ONTAP.	<code>true</code> Para ONTAP 9.15.1 o posterior, de lo contrario <code>false</code> .
limitVolumePoolSize	Tamaño máximo de FlexVol que se puede solicitar cuando se utilizan qtrees en el back-end económico de ONTAP-nas.	"" (no se aplica de forma predeterminada)
denyNewVolumePools	Restringe <code>ontap-nas-economy</code> los back-ends de la creación de nuevos volúmenes de FlexVol para contener sus Qtrees. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	



## Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
<code>spaceAllocation</code>	Asignación de espacio para Qtrees	verdadero
<code>spaceReserve</code>	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	ninguno
<code>snapshotPolicy</code>	Política de Snapshot que se debe usar	ninguno
<code>qosPolicy</code>	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> por pool/back-end de almacenamiento	""
<code>adaptiveQosPolicy</code>	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> por pool/back-end de almacenamiento. no admitido por ontap-nas-Economy.	""
<code>snapshotReserve</code>	Porcentaje de volumen reservado para las Snapshot	«0» si <code>snapshotPolicy</code> no es "ninguno", de lo contrario
<code>splitOnClone</code>	Divida un clon de su elemento principal al crearlo	"falso"
<code>encryption</code>	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son <code>false</code> . Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE. Para obtener más información, consulte: <a href="#">"Cómo funciona Trident con NVE y NAE"</a> .	"falso"
<code>tieringPolicy</code>	Política de organización en niveles para utilizar ninguna	«Solo Snapshot» para la configuración SVM-DR anterior a ONTAP 9,5
<code>unixPermissions</code>	Modo para volúmenes nuevos	«777» para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
<code>snapshotDir</code>	Controla el acceso al <code>.snapshot</code> directorio	"True" para NFSv4 "false" para NFSv3
<code>exportPolicy</code>	Política de exportación que se va a utilizar	"predeterminado"
<code>securityStyle</code>	Estilo de seguridad para nuevos volúmenes. Compatibilidad con NFS <code>mixed y.</code> <code>unix</code> estilos de seguridad. SMB admite <code>mixed y.</code> <code>ntfs</code> estilos de seguridad.	El valor predeterminado de NFS es <code>unix</code> . La opción predeterminada de SMB es <code>ntfs</code> .

Parámetro	Descripción	Predeterminado
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""



Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.

## Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados definidos:

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: '10'
```

For `ontap-nas` and `ontap-nas-flexgroups`, Trident ahora utiliza un nuevo cálculo para garantizar que el tamaño del FlexVol se ajusta correctamente con el porcentaje de reserva de instantáneas y la RVP. Cuando el usuario solicita una RVP, Trident crea la FlexVol original con más espacio mediante el nuevo cálculo. Este cálculo garantiza que el usuario recibe el espacio de escritura que solicitó en el PVC y no menos espacio que el que solicitó. Antes de v21.07, cuando el usuario solicita una RVP (por ejemplo, 5GIB) con el 50 por ciento de `snapshotReserve`, solo obtiene 2,5 GIB de espacio editable. Esto se debe a que lo que el usuario solicitó es todo el volumen y `snapshotReserve` es un porcentaje de ello. Con Trident 21,07, lo que el usuario solicita es el espacio de escritura y Trident define `snapshotReserve` la cantidad como el porcentaje de todo el

volumen. Esto no se aplica a `ontap-nas-economy`. Vea el siguiente ejemplo para ver cómo funciona:

El cálculo es el siguiente:

```
Total volume size = (PVC requested size) / (1 - (snapshotReserve
percentage) / 100)
```

Para `snapshotReserve = 50 %` y la solicitud de RVP = 5 GIB, el tamaño total del volumen es  $2/5 = 10$  GIB y el tamaño disponible es de 5 GIB, lo que es lo que solicitó el usuario en la solicitud de RVP. La `volume show` el comando debería mostrar resultados similares a los de este ejemplo:

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
	<code>_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4</code>		online	RW	10GB	5.00GB	0%
	<code>_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba</code>		online	RW	1GB	511.8MB	0%

2 entries were displayed.

Los back-ends existentes de instalaciones anteriores aprovisionarán los volúmenes tal y como se explicó anteriormente al actualizar Trident. En el caso de los volúmenes que creó antes de actualizar, debe cambiar el tamaño de sus volúmenes para que se observe el cambio. Por ejemplo, una RVP de 2GiB GB con `snapshotReserve=50` versiones anteriores dio como resultado un volumen que proporciona 1GiB GB de espacio editable. Cambiar el tamaño del volumen a 3 GIB, por ejemplo, proporciona a la aplicación 3 GIB de espacio editable en un volumen de 6 GIB.

### Ejemplos de configuración mínima

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.



Si utiliza Amazon FSX en ONTAP de NetApp con Trident, la recomendación es especificar nombres DNS para las LIF en lugar de direcciones IP.

### Ejemplo de economía NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

## Ejemplo de FlexGroup NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

## Ejemplo de MetroCluster

Puede configurar el backend para evitar tener que actualizar manualmente la definición de backend después del switchover y el switchover durante ["Replicación y recuperación de SVM"](#).

Para obtener una conmutación de sitios y una conmutación de estado sin problemas, especifique la SVM con managementLIF y omita la dataLIF y.. svm parámetros. Por ejemplo:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

## Ejemplo de volúmenes de SMB

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

## Ejemplo de autenticación basada en certificados

Este es un ejemplo de configuración de backend mínima. `clientCertificate`, `clientPrivateKey`, y `trustedCACertificate` (Opcional, si se utiliza una CA de confianza) se completan en `backend.json` Y tome los valores codificados base64 del certificado de cliente, la clave privada y el certificado de CA de confianza, respectivamente.

```
---
version: 1
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

## Ejemplo de política de exportación automática

En este ejemplo, se muestra cómo puede indicar a Trident que utilice políticas de exportación dinámicas para crear y gestionar la política de exportación automáticamente. Esto funciona igual para `ontap-nas-economy` los controladores y `ontap-nas-flexgroup`

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

## Ejemplo de direcciones IPv6

Este ejemplo muestra managementLIF Uso de una dirección IPv6.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

## Ejemplo de Amazon FSx para ONTAP mediante volúmenes de bloque de mensajes del servidor

La smbShare El parámetro es obligatorio para FSx para ONTAP mediante volúmenes de bloque de mensajes del servidor.

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

## Ejemplo de configuración de backend con nameTemplate

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults: {
  "nameTemplate":
  "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.volume.R
  equestName}}"
},
"labels": {"cluster": "ClusterA", "PVC":
  "{{.volume.Namespace}}_{{.volume.RequestName}}"}
}
```

### Ejemplos de back-ends con pools virtuales

En los archivos de definición de backend de ejemplo que se muestran a continuación, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo de comentarios. Los comentarios se establecen en FlexVol for `ontap-nas` o FlexGroup para `ontap-nas-flexgroup`. Trident copia todas las etiquetas presentes en un pool virtual en el volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los pools de almacenamiento establecen sus propios `spaceReserve`, `spaceAllocation`, y `encryption` y algunos pools sustituyen los valores predeterminados.

## Ejemplo de NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: 'false'
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  app: msoffice
  cost: '100'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
    adaptiveQosPolicy: adaptive-premium
- labels:
  app: slack
  cost: '75'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: legal
  creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  app: wordpress
```



```
    cost: '50'  
    zone: us_east_1c  
    defaults:  
      spaceReserve: none  
      encryption: 'true'  
      unixPermissions: '0775'  
- labels:  
  app: mysqldb  
  cost: '25'  
  zone: us_east_1d  
  defaults:  
    spaceReserve: volume  
    encryption: 'false'  
    unixPermissions: '0775'
```

## Ejemplo de FlexGroup NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '50000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: gold
  creditpoints: '30000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  protection: bronze
  creditpoints: '10000'
  zone: us_east_1d
  defaults:
```

```
spaceReserve: volume  
encryption: 'false'  
unixPermissions: '0775'
```

## Ejemplo de economía NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: nas_economy_store
  region: us_east_1
storage:
- labels:
  department: finance
  creditpoints: '6000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: engineering
  creditpoints: '3000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  department: humanresource
  creditpoints: '2000'
  zone: us_east_1d
  defaults:
    spaceReserve: volume
```

```
encryption: 'false'  
unixPermissions: '0775'
```

### Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass se refieren a [Ejemplos de back-ends con pools virtuales](#). Con el `parameters.selector` Cada StorageClass llama la atención sobre qué pools virtuales pueden usarse para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- La `protection-gold` StorageClass se asignará al primer y segundo pool virtual del `ontap-nas-flexgroup` back-end. Estos son los únicos pools que ofrecen protección de nivel Gold.

```
apiVersion: storage.k8s.io/v1  
kind: StorageClass  
metadata:  
  name: protection-gold  
provisioner: csi.trident.netapp.io  
parameters:  
  selector: "protection=gold"  
  fsType: "ext4"
```

- La `protection-not-gold` StorageClass se asignará al tercer y cuarto pool virtual del `ontap-nas-flexgroup` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto al Gold.

```
apiVersion: storage.k8s.io/v1  
kind: StorageClass  
metadata:  
  name: protection-not-gold  
provisioner: csi.trident.netapp.io  
parameters:  
  selector: "protection!=gold"  
  fsType: "ext4"
```

- La `app-mysqldb` StorageClass se asignará al cuarto pool virtual del `ontap-nas` back-end. Este es el único pool que ofrece configuración de pool de almacenamiento para la aplicación de tipo `mysqldb`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- T. protection-silver-creditpoints-20k StorageClass se asignará al tercer pool virtual del ontap-nas-flexgroup back-end. Este es el único pool que ofrece protección de nivel plata y 20000 puntos de crédito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
```

- La creditpoints-5k StorageClass se asignará al tercer pool virtual del ontap-nas backend y segundo pool virtual en ontap-nas-economy back-end. Estas son las únicas ofertas de grupo con 5000 puntos de crédito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

#### **Actualizar dataLIF tras la configuración inicial**

Puede cambiar la LIF de datos tras la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON back-end con LIF de datos actualizadas.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-with-updated-dataLIF>
```



Si los RVP están conectados a uno o varios pods, deben recuperar todos los pods correspondientes y, a continuación, traerlos para que surta efecto el nuevo LIF de datos.

## Amazon FSX para ONTAP de NetApp

### Utiliza Trident con Amazon FSx para NetApp ONTAP

"[Amazon FSX para ONTAP de NetApp](#)" Es un servicio AWS totalmente gestionado que permite a los clientes iniciar y ejecutar sistemas de archivos con tecnología del sistema operativo de almacenamiento ONTAP de NetApp. FSX para ONTAP le permite aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp con las que ya está familiarizado, a la vez que aprovecha la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX para ONTAP es compatible con las funciones del sistema de archivos ONTAP y las API de administración.

Puede integrar su sistema de archivos de Amazon FSx para NetApp ONTAP con Trident para garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Un sistema de archivos es el recurso principal de Amazon FSX, similar a un clúster de ONTAP en las instalaciones. En cada SVM, se pueden crear uno o varios volúmenes, que son contenedores de datos que almacenan los archivos y las carpetas en el sistema de archivos. Con Amazon FSX para ONTAP de NetApp, Data ONTAP se proporcionará como un sistema de archivos gestionado en el cloud. El nuevo tipo de sistema de archivos se llama **ONTAP** de NetApp.

Al usar Trident con Amazon FSx para NetApp ONTAP, puedes garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

### Requisitos

Además "[Requisitos de Trident](#)" de , para integrar FSx para ONTAP con Trident, necesita:

- Un clúster de Amazon EKS existente o un clúster de Kubernetes autogestionado con `kubect1` instalado.
- Un sistema de archivos Amazon FSx para NetApp ONTAP y una máquina virtual de almacenamiento (SVM) a la que se puede acceder desde los nodos de trabajo del clúster.
- Nodos de trabajo preparados para "[NFS o iSCSI](#)".



Asegúrese de seguir los pasos de preparación de nodos necesarios para Amazon Linux y Ubuntu "[Imágenes de máquina de Amazon](#)" (AMI) en función del tipo de IAM EKS.

## Consideraciones

- Volúmenes SMB:
  - Se admiten los volúmenes de SMB mediante el `ontap-nas` sólo conductor.
  - Los volúmenes SMB no son compatibles con el complemento Trident EKS.
  - Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte ["Prepárese para aprovisionar los volúmenes de SMB"](#) para obtener más información.
- Antes de Trident 24,02, Trident no podía eliminar los volúmenes creados en el sistema de archivos Amazon FSx que tenían habilitados los backups automáticos. Para evitar este problema en Trident 24,02 o posterior, especifique `fsxFileSystemID`, `aws`, `apiKey` `aws` `apiRegion` y `aws secretKey` en el archivo de configuración de backend para AWS FSx for ONTAP.



Si especifica un rol de IAM en Trident, puede omitir la especificación de los `apiRegion` campos, `apiKey` y `secretKey` en Trident de forma explícita. Para obtener más información, consulte ["Opciones y ejemplos de configuración de FSX para ONTAP"](#).

## Autenticación

Trident ofrece dos modos de autenticación.

- Basado en credenciales (recomendado): Almacena las credenciales de forma segura en AWS Secrets Manager. Puede usar el `fsxadmin` usuario del sistema de archivos o del `vsadmin` usuario configurado para la SVM.



Trident espera ejecutarse como `vsadmin` usuario de SVM o como usuario con un nombre distinto que tenga el mismo rol. Amazon FSx para NetApp ONTAP tiene un `fsxadmin` usuario que sustituye de forma limitada al usuario del clúster de ONTAP `admin`. Recomendamos encarecidamente utilizar `vsadmin` con Trident.

- Basado en certificado: Trident se comunicará con la SVM en su sistema de archivos FSx a través de un certificado instalado en su SVM.

Para obtener más información sobre cómo habilitar la autenticación, consulte la autenticación del tipo de controlador:

- ["Autenticación NAS de ONTAP"](#)
- ["Autenticación SAN ONTAP"](#)

## Obtenga más información

- ["Documentación de Amazon FSX para ONTAP de NetApp"](#)
- ["Publicación del blog en Amazon FSX para ONTAP de NetApp"](#)

## Cree un rol de IAM y AWS Secret

Puede configurar los pods de Kubernetes para acceder a los recursos de AWS mediante la autenticación como un rol de AWS IAM en lugar de proporcionar credenciales de AWS explícitas.





Para autenticarse mediante un rol de AWS IAM, debe tener un clúster de Kubernetes implementado mediante EKS.

### Crear secreto de AWS Secret Manager

En este ejemplo, se crea un secreto de AWS Secret Manager para almacenar las credenciales de Trident CSI:

```
aws secretsmanager create-secret --name trident-secret --description "Trident CSI credentials" --secret-string "{\"user\":\"vsadmin\",\"password\":\"<svmpassword>\"}"
```

### Crear política de IAM

Los siguientes ejemplos crean una política de IAM mediante la CLI de AWS:

```
aws iam create-policy --policy-name AmazonFSxNCSIDriverPolicy --policy-document file://policy.json --description "This policy grants access to Trident CSI to FSxN and Secret manager"
```

### Policy JSON archivo:

```
policy.json:
{
  "Statement": [
    {
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:CreateVolume",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:UntagResource",
        "fsx:UpdateVolume",
        "fsx:TagResource",
        "fsx>DeleteVolume"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Resource": "arn:aws:secretsmanager:<aws-region>:<aws-account-id>:secret:<aws-secret-manager-name>"
    }
  ],
  "Version": "2012-10-17"
}
```

## Rol Crear e IAM para la cuenta de servicio

En el siguiente ejemplo, se crea un rol de IAM para la cuenta de servicio en EKS:

```
eksctl create iamserviceaccount --name trident-controller --namespace trident
--cluster <my-cluster> --role-name <AmazonEKS_FSxN_CSI_DriverRole> --role-only
--attach-policy-arn arn:aws:iam::aws:policy/service-
role/AmazonFSxNCSIDriverPolicy --approve
```

## Instale Astra Trident

Astra Trident optimiza la gestión del almacenamiento de Amazon FSx para NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores se centren en la puesta en marcha de aplicaciones.

Puedes instalar Astra Trident mediante uno de los siguientes métodos:

- Timón
- Complemento EKS

```
If you want to make use of the snapshot functionality, install the CSI
snapshot controller add-on. Refer to
https://docs.aws.amazon.com/eks/latest/userguide/csi-snapshot-
controller.html.
```

## Instala Astra Trident mediante helm

### 1. Descargue el paquete de instalador de Astra Trident

El paquete de instalación de Astra Trident incluye todo lo necesario para poner en marcha al operador de Trident e instalar Astra Trident. Descargue y extraiga la última versión del instalador de Astra Trident de la sección Activos de GitHub.

```
wget https://github.com/NetApp/trident/releases/download/v24.10.0/trident-
installer-24.10.0.tar.gz
tar -xf trident-installer-24.10.0.tar.gz
cd trident-installer
```

### 2. Establezca los valores para los indicadores **cloud provider** y **cloud identity** utilizando las siguientes variables de entorno:

```
export CP="AWS"
export CI="'eks.amazonaws.com/role-arn:
arn:aws:iam::<accountID>:role/<AmazonEKS_FSxN_CSI_DriverRole>'"
```

En el siguiente ejemplo, se instala Astra Trident y se establece `cloud-provider` la marca en `$CP`, y `cloud-identity` en `$CI`:

```
helm install trident trident-operator-100.2410.0.tgz --set
cloudProvider=$CP --set cloudIdentity=$CI --namespace trident
```

Puede utilizar `helm list` el comando para revisar detalles de instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación y número de revisión.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14 14:31:22.463122
+0300 IDT	deployed	trident-operator-100.2410.0	24.10.0

### Instala Astra Trident a través del complemento EKS

El complemento Astra Trident EKS incluye las últimas revisiones de seguridad, correcciones de errores y AWS lo valida para que funcione con Amazon EKS. El complemento EKS le permite garantizar de forma constante que sus clústeres de Amazon EKS sean seguros y estables y reducir la cantidad de trabajo que necesita para instalar, configurar y actualizar complementos.

### Requisitos previos

Asegúrate de disponer de lo siguiente antes de configurar el complemento Astra Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con suscripción complementaria
- Permisos de AWS para AWS Marketplace:  
"aws-marketplace:ViewSubscriptions",  
"aws-marketplace:Subscribe",  
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2\_x86\_64) o Amazon Linux 2 Arm (AL2\_ARM\_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx para NetApp ONTAP existente

### Habilita el complemento Astra Trident para AWS

## Clúster EKS

Los siguientes comandos de ejemplo instalan el complemento Astra Trident EKS:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v24.6.1-eksbuild  
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v24.6.1-eksbuild.1 (con una versión dedicada)
```



Al configurar el parámetro opcional `cloudIdentity`, asegúrese de especificar `cloudProvider` al instalar Trident mediante el complemento EKS.

## Consola de gestión

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, haga clic en **Clusters**.
3. Haga clic en el nombre del cluster para el que desea configurar el complemento CSI de NetApp Trident.
4. Haga clic en **Complementos** y luego haga clic en **Obtener más complementos**.
5. En la página **Select add-ons**, haz lo siguiente:
  - a. En la sección eks-addons de AWS Marketplace, selecciona la casilla de verificación **Astra Trident by NetApp**.
  - b. Haga clic en **Siguiente**.
6. En la página de configuración **Configure Selected add-ons**, haga lo siguiente:
  - a. Seleccione la **Versión** que desea usar.
  - b. Para **Seleccione el rol de IAM**, déjelo en **No establecido**.
  - c. Expanda la configuración **Opcional**, siga el esquema de configuración **Add-on** y establezca el parámetro `configurationValues` en la sección **Valores de configuración** en el rol-arn que creó en el paso anterior (el valor debe tener el siguiente formato `eks.amazonaws.com/role-arn:arn:aws:iam::464262061435:role/AmazonEKS_FSXN_CSI_DriverRole:`). Si selecciona **Sustituir** para el método de resolución de conflictos, una o más de las configuraciones del complemento existente se pueden sobrescribir con la configuración del complemento Amazon EKS. Si no habilita esta opción y existe un conflicto con la configuración existente, se producirá un error en la operación. Puede utilizar el mensaje de error resultante para solucionar el conflicto. Antes de seleccionar esta opción, asegúrese de que el complemento de Amazon EKS no gestiona la configuración que necesita para autogestionar.



Al configurar el parámetro opcional `cloudIdentity`, asegúrese de especificar `cloudProvider` al instalar Trident mediante el complemento EKS.

7. Elija **Siguiente**.
8. En la página **Revisar y agregar**, selecciona **Crear**.

Una vez finalizada la instalación del complemento, verá el complemento instalado.

## CLI DE AWS

1. Cree el `add-on.json` archivo:

```
add-on.json
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v24.6.1-eksbuild.1",
  "serviceAccountRoleArn": "arn:aws:iam::123456:role/astratrident-
role",
  "configurationValues": "{\"cloudIdentity\":
'eks.amazonaws.com/role-arn: arn:aws:iam::123456:role/astratrident-
role'"},
  "cloudProvider": "AWS"}
}
```



Al configurar el parámetro opcional `cloudIdentity`, asegúrese de especificar `AWS` como `cloudProvider` al instalar Trident mediante el complemento EKS.

## 2. Instala el complemento de Astra Trident EKS»

```
aws eks create-addon --cli-input-json file://add-on.json
```

## Actualiza el complemento EKS de Astra Trident

## Clúster EKS

- Compruebe la versión actual de su complemento FSxN Trident CSI. Sustituya `my-cluster` por el nombre del clúster.

```
eksctl get addon --name netapp_trident-operator --cluster my-cluster
```

### Ejemplo de salida:

```
NAME                                VERSION                                STATUS  ISSUES
IAMROLE  UPDATE AVAILABLE  CONFIGURATION VALUES
netapp_trident-operator  v24.6.1-eksbuild.1  ACTIVE  0
{"cloudIdentity":"'eks.amazonaws.com/role-arn:
arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole'"}

```

- Actualice el complemento a la versión devuelta bajo **ACTUALIZACIÓN DISPONIBLE** en la salida del paso anterior.

```
eksctl update addon --name netapp_trident-operator --version v24.6.1-
eksbuild.1 --cluster my-cluster --force
```

Si elimina la `--force` opción y cualquiera de las configuraciones del complemento de Amazon EKS entra en conflicto con la configuración existente, la actualización del complemento de Amazon EKS falla; recibirá un mensaje de error que le ayudará a resolver el conflicto. Antes de especificar esta opción, asegúrese de que el complemento de Amazon EKS no gestiona la configuración que debe administrar, ya que dicha configuración se sobrescribe con esta opción. Para obtener más información acerca de otras opciones para esta configuración, consulte "[Complementos](#)". Para obtener más información sobre la gestión de campos de Amazon EKS Kubernetes, consulte "[Gestión del campo de Kubernetes](#)".

## Consola de gestión

1. Abra la consola de Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, haga clic en **Clusters**.
3. Haga clic en el nombre del cluster para el que desea actualizar el complemento CSI de NetApp Trident.
4. Haga clic en la pestaña **Add-ons**.
5. Haz clic en **Astra Trident by NetApp** y luego haz clic en **Editar**.
6. En la página **Configure Astra Trident by NetApp**, haga lo siguiente:
  - a. Seleccione la **Versión** que desea usar.
  - b. (Opcional) Puede ampliar la **Configuración opcional** y modificarla según sea necesario.
  - c. Haga clic en **Guardar cambios**.

## CLI DE AWS

El siguiente ejemplo actualiza el complemento EKS:

```
aws eks update-addon --cluster-name my-cluster netapp_trident-operator vpc-cni
--addon-version v24.6.1-eksbuild.1 \
--service-account-role-arn arn:aws:iam::111122223333:role/role-name
```

```
--configuration-values '{} ' --resolve-conflicts --preserve
```

## Desinstale/quite el complemento de Astra Trident EKS

Tienes dos opciones para eliminar un complemento de Amazon EKS:

- **Preserve el software complementario en su clúster** – Esta opción elimina la administración de Amazon EKS de cualquier configuración. También elimina la posibilidad de que Amazon EKS le notifique las actualizaciones y actualice automáticamente el complemento de Amazon EKS después de iniciar una actualización. Sin embargo, conserva el software complementario en el clúster. Esta opción convierte el complemento en una instalación autogestionada, en lugar de un complemento de Amazon EKS. Con esta opción, no se produce tiempo de inactividad en el complemento. Conserve `--preserve` la opción en el comando para conservar el complemento.
- **\* Elimine el software complementario completamente de su clúster \***: Le recomendamos que elimine el complemento Amazon EKS de su clúster solo si no hay recursos en su clúster que dependan de él. Elimine `--preserve` la opción del `delete` comando para eliminar el complemento.



Si el complemento tiene una cuenta de IAM asociada, la cuenta de IAM no se elimina.

### Clúster EKS

El siguiente comando desinstala el complemento EKS de Astra Trident:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

### Consola de gestión

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, haga clic en **Clusters**.
3. Haga clic en el nombre del cluster del que desea quitar el complemento CSI de NetApp Trident.
4. Haz clic en la pestaña **Complementos** y luego haz clic en **Astra Trident by NetApp**.\*
5. Haga clic en **Quitar**.
6. En el cuadro de diálogo **Remove netapp\_trident-operator confirmation**, haga lo siguiente:
  - a. Si desea que Amazon EKS deje de administrar la configuración del complemento, seleccione **Conservar en clúster**. Haga esto si desea conservar el software complementario en su clúster para que pueda gestionar todos los ajustes del complemento por su cuenta.
  - b. Introduzca **netapp\_trident-operator**.
  - c. Haga clic en **Quitar**.

### CLI DE AWS

Reemplace `my-cluster` por el nombre del clúster y, a continuación, ejecute el siguiente comando.

```
aws eks delete-addon --cluster-name my-cluster --addon-name netapp_trident-operator --preserve
```

## Configure el backend de almacenamiento

## Integración de controladores ONTAP SAN y NAS

Puede crear un archivo backend con las credenciales de SVM (nombre de usuario y contraseña) almacenadas en AWS Secret Manager, como se muestra en este ejemplo:



## YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFileSystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn
```

## JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFileSystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}
```

Para obtener más información sobre la creación de back-ends, consulte estas páginas:

- ["Configurar un back-end con controladores NAS de ONTAP"](#)
- ["Configuración de un back-end con controladores SAN de ONTAP"](#)

### FSX para ONTAP detalles del controlador

Puedes integrar Trident con Amazon FSx for NetApp ONTAP mediante los siguientes controladores:

- `ontap-san`: Cada VP aprovisionado es un LUN dentro de su propio volumen de Amazon FSx para NetApp ONTAP. Recomendado para almacenamiento en bloques.
- `ontap-nas`: Cada VP aprovisionado es un volumen completo de Amazon FSx para NetApp ONTAP. Recomendado para NFS y SMB.
- `ontap-san-economy`: Cada VP aprovisionado es un LUN con un número configurable de LUN por Amazon FSX para el volumen ONTAP de NetApp.
- `ontap-nas-economy`: Cada VP aprovisionado es un qtree, con un número configurable de qtrees por Amazon FSX para el volumen ONTAP de NetApp.
- `ontap-nas-flexgroup`: Cada VP aprovisionado es un Amazon FSX completo para el volumen ONTAP FlexGroup de NetApp.

Para obtener información detallada sobre el conductor, consulte ["Controladores de NAS"](#) y.. ["Controladores de SAN"](#).

### Configuraciones de ejemplo

#### Configuración para AWS FSx para ONTAP con administrador secreto

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFilesystemID: fs-xxxxxxxxxx
  managementLIF:
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn
```

## Configuración de la clase de almacenamiento para volúmenes SMB

Uso `nasType`, `node-stage-secret-name`, y `node-stage-secret-namespace`, Puede especificar un volumen SMB y proporcionar las credenciales necesarias de Active Directory. Se admiten los volúmenes de SMB mediante el `ontap-nas` sólo conductor.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nas-smb-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## Configuración avanzada de backend y ejemplos

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Ejemplo
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	<code>ontap-nas</code> , <code>ontap-nas-economy</code> , <code>ontap-nas-flexgroup</code> , <code>ontap-san</code> , <code>ontap-san-economy</code>
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre del conductor + “_” + <code>dataLIF</code>

Parámetro	Descripción	Ejemplo
managementLIF	<p>Dirección IP de un clúster o una LIF de gestión de SVM Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si proporciona el fsxFilesystemID en aws el campo, no necesita proporcionar el managementLIF porque Trident recupera la información de la SVM managementLIF de AWS. Por lo tanto, debe proporcionar credenciales para un usuario en la SVM (por ejemplo: Vsadmin) y el usuario debe tener vsadmin el rol.</p>	<p>“10.0.0.1”, “[2001:1234:abcd::fefe]”</p>
dataLIF	<p>Dirección IP de LIF de protocolo.</p> <p><b>Controladores NAS de ONTAP:</b> Recomendamos especificar dataLIF. Si no se encuentra, Trident recupera los LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos. Se puede cambiar después del ajuste inicial. Consulte .</p> <p><b>Controladores SAN ONTAP:</b> No se especifica para iSCSI. Trident utiliza asignación de LUN selectiva de ONTAP para descubrir las LIF iSCSI necesarias para establecer una sesión multivía. Se genera una advertencia si dataLIF se define explícitamente. Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p>	

Parámetro	Descripción	Ejemplo
autoExportPolicy	Habilite la creación y actualización automática de la política de exportación [Boolean]. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	false
autoExportCIDRs	Lista de CIDRs para filtrar las IP del nodo de Kubernetes contra cuando autoExportPolicy se habilita. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	"["0.0.0.0/0", "*/0"]"
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	El nombre de usuario para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales. Por ejemplo, vsadmin.	
password	La contraseña para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales.	
svm	Máquina virtual de almacenamiento que usar	Derivado si se especifica una LIF de gestión de SVM.

Parámetro	Descripción	Ejemplo
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede modificar una vez creada. Para actualizar este parámetro, deberá crear un nuevo backend.	trident
limitAggregateUsage	<b>No especifique para Amazon FSx para NetApp ONTAP.</b> El proporcionado fsxadmin y vsadmin no contiene los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Trident.	No utilizar.
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. También restringe el tamaño máximo de los volúmenes que gestiona para qtrees y LUN, y la qtreesPerFlexvol Permite personalizar el número máximo de qtrees por FlexVol.	"" (no se aplica de forma predeterminada)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]. Solo SAN.	«100»
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Por ejemplo, {"api":false, "method":true} no se utiliza debugTraceFlags a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo

Parámetro	Descripción	Ejemplo
nfsMountOptions	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident volverá a utilizar las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento. Si no se especifican opciones de montaje en la clase almacenamiento o el archivo de configuración, Trident no definirá ninguna opción de montaje en un volumen persistente asociado.	""
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> , o nulo. <b>Debe establecer en <code>smb</code> Para volúmenes SMB.</b> el valor predeterminado es <code>null</code> en volúmenes NFS.	<code>nfs</code>
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	"200"
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado con la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP, o bien un nombre para permitir que Trident cree el recurso compartido de SMB. Este parámetro es obligatorio para los back-ends de Amazon FSx para ONTAP.	<code>smb-share</code>

Parámetro	Descripción	Ejemplo
useREST	<p>Parámetro booleano para usar las API DE REST de ONTAP. <b>Vista previa tecnológica</b></p> <p>useREST se proporciona como <b>vista previa tecnológica</b> que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en <code>true</code>, Trident utilizará las API REST DE ONTAP para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> la aplicación. Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code>.</p>	<code>false</code>
aws	<p>Puedes especificar lo siguiente en el archivo de configuración de AWS FSx para ONTAP:</p> <ul style="list-style-type: none"> <li>- <code>fsxFileSystemID</code>: Especifique el ID del sistema de archivos AWS FSx.</li> <li>- <code>apiRegion</code>: Nombre de la región de la API de AWS.</li> <li>- <code>apikey</code>: AWS API key.</li> <li>- <code>secretKey</code>: AWS clave secreta.</li> </ul>	<pre>"" "" ""</pre>
credentials	<p>Especifique las credenciales de FSx SVM que se van a almacenar en AWS Secret Manager.</p> <ul style="list-style-type: none"> <li>- <code>name</code>: Nombre de recurso de Amazon (ARN) del secreto, que contiene las credenciales de SVM.</li> <li>- <code>type</code>: Establecer en <code>awsarn</code>.</li> </ul> <p>Consulte <a href="#">"Cree un secreto de AWS Secrets Manager"</a> si quiere más información.</p>	

#### Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
<code>spaceAllocation</code>	Asignación de espacio para las LUN	<code>true</code>
<code>spaceReserve</code>	Modo de reserva de espacio; "none" (thin) o "VOLUME" (grueso)	<code>none</code>



Parámetro	Descripción	Predeterminado
snapshotPolicy	Política de Snapshot que se debe usar	none
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end. Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end. no admitido por ontap-nas-Economy.	""
snapshotReserve	Porcentaje del volumen reservado para instantáneas "0"	Si snapshotPolicy es none, else ""
splitOnClone	Divida un clon de su elemento principal al crearlo	false
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen provisionado en Trident será habilitado NAE. Para obtener más información, consulte: <a href="#">"Cómo funciona Trident con NVE y NAE"</a> .	false
luksEncryption	Active el cifrado LUKS. Consulte <a href="#">"Usar la configuración de clave unificada de Linux (LUKS)"</a> . Solo SAN.	""

Parámetro	Descripción	Predeterminado
tieringPolicy	Política de organización en niveles para utilizar <code>none</code>	<code>snapshot-only</code> Para configuraciones anteriores a ONTAP 9,5 SVM-DR
unixPermissions	Modo para volúmenes nuevos. <b>Dejar vacío para volúmenes SMB.</b>	""
securityStyle	Estilo de seguridad para nuevos volúmenes. Compatibilidad con NFS <code>mixed</code> y.. <code>unix</code> estilos de seguridad. SMB admite <code>mixed</code> y.. <code>ntfs</code> estilos de seguridad.	El valor predeterminado de NFS es <code>unix</code> . La opción predeterminada de SMB es <code>ntfs</code> .

### Prepárese para aprovisionar los volúmenes de SMB

Puede aprovisionar volúmenes SMB mediante el `ontap-nas` controlador. Antes de completar la tarea [Integración de controladores ONTAP SAN y NAS](#) complete los siguientes pasos.

#### Antes de empezar

Para poder aprovisionar volúmenes de SMB con el `ontap-nas` conductor, debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2019. Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Trident que contiene sus credenciales de Active Directory. Para generar secreto `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- Proxy CSI configurado como servicio de Windows. Para configurar un `csi-proxy`, consulte "[GitHub: Proxy CSI](#)" o "[GitHub: Proxy CSI para Windows](#)" Para nodos Kubernetes que se ejecutan en Windows.

#### Pasos

1. Cree recursos compartidos de SMB. Puede crear recursos compartidos de administrador de SMB de una de dos formas mediante el "[Consola de administración de Microsoft](#)" Complemento carpetas compartidas o uso de la CLI de ONTAP. Para crear los recursos compartidos de SMB mediante la CLI de ONTAP:
  - a. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

La `vserver cifs share create` comando comprueba la ruta especificada en la opción `-path` durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

- b. Cree un recurso compartido de SMB asociado con la SVM especificada:

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

c. Compruebe que se ha creado el recurso compartido:

```
vserver cifs share show -share-name share_name
```



Consulte "[Cree un recurso compartido de SMB](#)" para obtener todos los detalles.

2. Al crear el back-end, debe configurar lo siguiente para especificar volúmenes de SMB. Para obtener información sobre todas las opciones de configuración del entorno de administración de ONTAP, consulte "[Opciones y ejemplos de configuración de FSX para ONTAP](#)".

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado con la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP, o bien un nombre para permitir que Trident cree el recurso compartido de SMB. Este parámetro es obligatorio para los back-ends de Amazon FSx para ONTAP.	smb-share
nasType	<b>Debe establecer en smb.</b> Si es nulo, el valor predeterminado es nfs.	smb
securityStyle	Estilo de seguridad para nuevos volúmenes. <b>Debe estar configurado en ntfs o. mixed Para volúmenes SMB.</b>	ntfs o. mixed Para volúmenes de SMB
unixPermissions	Modo para volúmenes nuevos. <b>Se debe dejar vacío para volúmenes SMB.</b>	""

### Configure una clase de almacenamiento y la RVP

Configure un objeto StorageClass de Kubernetes y cree la clase de almacenamiento para indicar a Trident cómo se aprovisionan los volúmenes. Cree un volumen persistente (VP) y una reclamación de volumen persistente (RVP) que utilice el tipo de almacenamiento de Kubernetes configurado para solicitar acceso al VP. A continuación, puede montar el VP en un pod.

## Cree una clase de almacenamiento

### Configurar un objeto de Kubernetes StorageClass

El "[Objeto de Kubernetes StorageClass](#)" identifica a los Trident como el proveedor que se usa para esa clase indica a Trident cómo aprovisionar un volumen. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
```

Consulte el "[Objetos de Kubernetes y Trident](#)" para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los `PersistentVolumeClaim` parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

## Cree una clase de almacenamiento

### Pasos

1. Este es un objeto de Kubernetes, así que use `kubectl` Para crear en Kubernetes.

```
kubectl create -f storage-class-ontapnas.yaml
```

2. Ahora deberías ver una clase de almacenamiento **basic-csi** tanto en Kubernetes como en Trident, y Trident debería haber descubierto los pools en el back-end.

```
kubectl get sc basic-csi
NAME          PROVISIONER          AGE
basic-csi     csi.trident.netapp.io 15h
```

## Cree el VP y la RVP

1. "[Volumen persistente](#)" (PV) es un recurso de almacenamiento físico proporcionado por el administrador del clúster en un clúster de Kubernetes. La "[Claim de volumen persistente](#)" (RVP) es una solicitud para acceder al volumen persistente en el clúster.

La RVP se puede configurar para solicitar almacenamiento de un determinado tamaño o modo de acceso. Mediante el StorageClass asociado, el administrador del clúster puede controlar mucho más que el tamaño de los volúmenes persistentes y el modo de acceso, como el rendimiento o el nivel de servicio.

Después de crear el VP y la RVP, puede montar el volumen en un pod.

## Manifiestos de muestra

### Manifiesto de muestra de volumen persistente

Este manifiesto de ejemplo muestra un PV básico de 10Gi que está asociado con StorageClass `basic-csi`.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-storage
  labels:
    type: local
spec:
  storageClassName: basic-csi
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteMany
  hostPath:
    path: "/my/host/path"
```

## Manifiestos de muestra de PersistentVolumeClaim

Estos ejemplos muestran opciones básicas de configuración de PVC.

### PVC con acceso RWO

Este ejemplo muestra una PVC básica con acceso RWX que está asociada con una clase de almacenamiento llamada `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

### PVC con NVMe/TCP

En este ejemplo, se muestra una PVC básica para NVMe/TCP con acceso RWO asociado con una clase de almacenamiento denominada `protection-gold`.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san-nvme
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: protection-gold
```

## Cree el VP y la RVP

### Pasos

1. Cree el VP.

```
kubectl create -f pv.yaml
```

## 2. Compruebe el estado de PV.

```
kubectl get pv
NAME          CAPACITY  ACCESS MODES  RECLAIM POLICY  STATUS  CLAIM
STORAGECLASS REASON    AGE
pv-storage   4Gi      RWO           Retain          Available
7s
```

## 3. Cree la RVP.

```
kubectl create -f pvc.yaml
```

## 4. Verifique el estado de la RVP.

```
kubectl get pvc
NAME          STATUS  VOLUME          CAPACITY  ACCESS MODES  STORAGECLASS  AGE
pvc-storage  Bound  pv-name         2Gi      RWO           storageclass  5m
```

Consulte el ["Objetos de Kubernetes y Trident"](#) para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los PersistentVolumeClaim parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

### Atributos de la Trident

Estos parámetros determinan qué pools de almacenamiento gestionados por Trident se deben utilizar para aprovisionar volúmenes de un determinado tipo.

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
media 1	cadena	hdd, híbrido, ssd	Pool contiene medios de este tipo; híbrido significa ambos	Tipo de medios especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san y solidfire-san
AprovisionaciónTipo	cadena	delgado, grueso	El pool admite este método de aprovisionamiento	Método de aprovisionamiento o especificado	grueso: all ONTAP; thin: all ONTAP y solidfire-san

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
Tipo de backendType	cadena	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool pertenece a este tipo de backend	Backend especificado	Todos los conductores
snapshot	bool	verdadero, falso	El pool admite volúmenes con Snapshot	Volumen con snapshots habilitadas	ontap-nas, ontap-san, solidfire-san y gcp-cvs
clones	bool	verdadero, falso	Pool admite el clonado de volúmenes	Volumen con clones habilitados	ontap-nas, ontap-san, solidfire-san y gcp-cvs
cifrado	bool	verdadero, falso	El pool admite volúmenes cifrados	Volumen con cifrado habilitado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	int	entero positivo	El pool es capaz de garantizar IOPS en este rango	El volumen garantizado de estas IOPS	solidfire-san

Esta versión 1: No es compatible con sistemas ONTAP Select

### Despliegue la aplicación de muestra

Despliegue la aplicación de muestra.

#### Pasos

1. Monte el volumen en un pod.

```
kubectl create -f pv-pod.yaml
```

Estos ejemplos muestran configuraciones básicas para conectar el PVC a un pod: **Configuración básica:**



```

kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/my/mount/path"
          name: pv-storage

```



Puede supervisar el progreso con `kubectl get pod --watch`.

2. Compruebe que el volumen está montado en `/my/mount/path`.

```
kubectl exec -it task-pv-pod -- df -h /my/mount/path
```

```

Filesystem                                                    Size
Used Avail Use% Mounted on
192.168.188.78:/trident_pvc_ae45ed05_3ace_4e7c_9080_d2a83ae03d06 1.1G
320K 1.0G 1% /my/mount/path

```

1. Ahora puede eliminar el Pod. La aplicación Pod ya no existirá, pero el volumen permanecerá.

```
kubectl delete pod task-pv-pod
```

## Configura el complemento EKS de Astra Trident en un clúster de EKS

Astra Trident optimiza la gestión del almacenamiento de Amazon FSx para NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores se centren en la puesta en marcha de aplicaciones. El complemento Astra Trident EKS incluye las últimas revisiones de seguridad, correcciones de errores y AWS lo valida para que funcione con Amazon EKS. El complemento EKS le permite garantizar de forma constante que sus

clústeres de Amazon EKS sean seguros y estables y reducir la cantidad de trabajo que necesita para instalar, configurar y actualizar complementos.

### Requisitos previos

Asegúrate de disponer de lo siguiente antes de configurar el complemento Astra Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con suscripción complementaria
- Permisos de AWS para AWS Marketplace:  
"aws-marketplace:ViewSubscriptions",  
"aws-marketplace:Subscribe",  
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2\_x86\_64) o Amazon Linux 2 Arm (AL2\_ARM\_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx para NetApp ONTAP existente

### Pasos

1. En tu clúster de EKS Kubernetes, navega a la pestaña **Add-ons**.

The screenshot shows the AWS EKS console interface for a cluster named 'tri-env-eks'. At the top right, there are buttons for 'Delete cluster' and 'Upgrade version'. Below this is a notification banner about the end of standard support for Kubernetes version 1.30 on July 28, 2025, with an 'Upgrade now' button. The main section is titled 'Cluster info' and contains a table with the following data:

Status	Kubernetes version	Support period	Provider
Active	1.30	Standard support until July 28, 2025	EKS

Below the table is a navigation bar with tabs: Overview, Resources, Compute, Networking, **Add-ons** (with a notification icon), Access, Observability, Upgrade insights, Update history, and Tags. A notification banner below the tabs states 'New versions are available for 3 add-ons.' The 'Add-ons' section is active, showing a search bar with the text 'Find add-on', filters for 'Any category' and 'Any status', and a '3 matches' indicator. There are buttons for 'View details', 'Edit', 'Remove', and 'Get more add-ons'.

2. Vaya a **AWS Marketplace add-ons** y elija la categoría *storage*.

### AWS Marketplace add-ons (1) ↻

Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters.

Filtering options

Any category ▼
NetApp, Inc. ▼
Any pricing model ▼
Clear filters

NetApp, Inc. ✕

< 1 >

#### NetApp Trident

NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

**Standard Contract**

Category	Listed by	Supported versions	Pricing starting at
storage	<a href="#">NetApp, Inc.</a>	1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23	<a href="#">View pricing details</a>

Cancel
Next

3. Localiza **NetApp Trident** y selecciona la casilla de verificación para el complemento Astra Trident.
4. Elija la versión deseada del complemento.

216

**NetApp Trident** Remove add-on

Listed by <b>NetApp</b>	Category storage	Status ✔ Ready to install
----------------------------	---------------------	------------------------------

**You're subscribed to this software**  
You can view the terms and pricing details for this product or choose another offer if one is available.

View subscription ×

**Version**  
Select the version for this add-on.

v24.6.1-eksbuild.1

**Select IAM role**  
Select an IAM role to use with this add-on. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#).

Not set ↻

▶ **Optional configuration settings**

Cancel Previous Next

5. Seleccione la opción Rol IAM que desea heredar del nodo.

## Review and add

### Step 1: Select add-ons

Edit

Selected add-ons (1)

Find add-on

< 1 >

Add-on name



Type



Status

netapp\_trident-operator

storage

Ready to install

### Step 2: Configure selected add-ons settings

Edit

Selected add-ons version (1)

< 1 >

Add-on name



Version



IAM role for service account (IRSA)

netapp\_trident-operator

v24.6.1-eksbuild.1

Not set

Cancel

Previous

Create

6. (Opcional) Configure cualquier configuración opcional según sea necesario y seleccione **Siguiente**.

Siga el esquema de configuración **Add-On** y establezca el parámetro `configurationValues` en la sección **Valores de configuración** en el Role-arn que creó en el paso anterior (el valor debe tener el siguiente formato `eks.amazonaws.com/role-arn:arn:aws:iam::464262061435:role/AmazonEKS_FSXN_CSI_DriverRole:`). Si selecciona Sustituir para el método de resolución de conflictos, una o más de las configuraciones del complemento existente se pueden sobrescribir con la configuración del complemento Amazon EKS. Si no habilita esta opción y existe un conflicto con la configuración existente, se producirá un error en la operación. Puede utilizar el mensaje de error resultante para solucionar el conflicto. Antes de seleccionar esta opción, asegúrese de que el complemento de Amazon EKS no gestiona la configuración que necesita para autogestionar.



Al configurar el parámetro opcional `cloudIdentity`, asegúrese de especificar `AWS` como `cloudProvider` al instalar Trident mediante el complemento EKS.

**Select IAM role**  
 Select an IAM role to use with this add-on. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#).

Not set ▼ ↻

**Optional configuration settings**

**Add-on configuration schema**  
 Refer to the JSON schema below. The configuration values entered in the code editor will be validated against this schema.

```
{
  "$id": "http://example.com/example.json",
  "$schema": "https://json-schema.org/draft/2019-09/schema",
  "default": {},
  "examples": [
    {
      "cloudIdentity": ""
    }
  ],
  "properties": {
    "cloudIdentity": {
      "default": "",
      "examples": [

```

**Configuration values** [Info](#)  
 Specify any additional JSON or YAML configurations that should be applied to the add-on.

```
1 {
2   "cloudIdentity": "'eks.amazonaws.com/role-arn: arn:aws
3     :iam::139763910815:role
4     /AmazonEKS_FSXN_CSI_DriverRole'",
5   "cloudProvider": "AWS"
6 }
```

7. Seleccione **Crear**.
8. Compruebe que el estado del complemento es *Active*.

**Add-ons (1)** [Info](#) View details Edit Remove Get more add-ons

netapp × Any category Any status 1 match < 1 >

**NetApp** **Astra Trident by NetApp** ○

Astra Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Category	Status	Version	IAM role for service account (IRSA)	Listed by
storage	<span>✔ Active</span>	v24.6.1-eksbuild.1	Not set	<a href="#">NetApp, Inc.</a>

View subscription

### Instalar/desinstalar el complemento Astra Trident EKS mediante la CLI

#### Instale el complemento Astra Trident EKS mediante la CLI:

El siguiente comando de ejemplo instala el complemento EKS de Astra Trident:

```
eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v24.6.1-eksbuild
```

```
eksctl create addon --cluster clusterName --name netapp_trident-operator
--version v24.6.1-eksbuild.1 (Con una versión dedicada)
```



Al configurar el parámetro opcional `cloudIdentity`, asegúrese de especificar `cloudProvider` al instalar Trident mediante el complemento EKS.

### Desinstale el complemento Astra Trident EKS mediante la CLI:

El siguiente comando desinstala el complemento EKS de Astra Trident:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

## Cree back-ends con kubectl

Un back-end define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él. Después de instalar Trident, el siguiente paso es crear un backend. La `TridentBackendConfig` definición de recursos personalizados (CRD) le permite crear y administrar backends de Trident directamente a través de la interfaz de Kubernetes. Para ello, puede utilizar `kubectl` o la herramienta CLI equivalente para su distribución de Kubernetes.

`TridentBackendConfig`

`TridentBackendConfig (tbc, , tbconfig tbackendconfig)` Es una interfaz CRD con nombre que permite gestionar los backend de Trident mediante `kubectl`. Los administradores de Kubernetes y de almacenamiento ahora pueden crear y gestionar back-ends directamente mediante la CLI de Kubernetes sin necesidad de una utilidad de línea de comandos dedicada (`tridentctl`).

Sobre la creación de un `TridentBackendConfig` objeto, sucede lo siguiente:

- Trident crea automáticamente un backend basado en la configuración que proporcione. Esto se representa internamente como un `TridentBackend (tbe, tridentbackend)` CR.
- El `TridentBackendConfig` está vinculado exclusivamente a una `TridentBackend` que fue creada por Trident.

Cada uno `TridentBackendConfig` mantiene una asignación de uno a uno con un `TridentBackend`. El primero es la interfaz que se ofrece al usuario para diseñar y configurar los back-ends. El segundo es cómo Trident representa el objeto back-end real.



`TridentBackend` Trident crea los CRS automáticamente. Usted **no debe** modificarlos. Si desea realizar actualizaciones en los back-ends, haga esto modificando el `TridentBackendConfig` objeto.

Consulte el siguiente ejemplo para ver el formato del `TridentBackendConfig` CR:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

También puede echar un vistazo a los ejemplos de la ["instalador de trident"](#) directorio para configuraciones de ejemplo para la plataforma o servicio de almacenamiento que desee.

La `spec` toma parámetros de configuración específicos del back-end. En este ejemplo, el back-end utiliza el `ontap-san` controlador de almacenamiento y utiliza los parámetros de configuración que se tabulan aquí. Para obtener la lista de opciones de configuración para el controlador de almacenamiento deseado, consulte la ["información de configuración del back-end para el controlador de almacenamiento"](#).

La `spec` la sección también incluye `credentials` y `deletionPolicy` campos, que se introducen recientemente en `TridentBackendConfig` CR:

- `credentials`: Este parámetro es un campo obligatorio y contiene las credenciales utilizadas para autenticarse con el sistema/servicio de almacenamiento. Este juego debe ser un secreto de Kubernetes creado por el usuario. Las credenciales no se pueden pasar en texto sin formato y se producirá un error.
- `deletionPolicy`: Este campo define lo que debe suceder cuando `TridentBackendConfig` se ha eliminado. Puede ser necesario uno de los dos valores posibles:
  - `delete`: Esto resulta en la eliminación de ambos `TridentBackendConfig` CR y el back-end asociado. Este es el valor predeterminado.
  - `retain`: Cuando un `TridentBackendConfig` Se elimina la CR, la definición de backend seguirá estando presente y se puede gestionar con `tridentctl`. Establecimiento de la política de eliminación como `retain` permite a los usuarios degradar a una versión anterior (anterior a 21.04) y conservar los back-ends creados. El valor de este campo se puede actualizar después de un `TridentBackendConfig` se ha creado.



El nombre de un back-end se define mediante `spec.backendName`. Si no se especifica, el nombre del backend se establece en el nombre del `TridentBackendConfig` objeto (`metadata.name`). Se recomienda establecer explícitamente nombres de backend mediante `spec.backendName`.





Los back-ends que se crearon con `tridentctl` no tienen un objeto asociado `TridentBackendConfig`. Puede optar por gestionar dichos back-ends con `kubectl` creando una `TridentBackendConfig` CR. Se debe tener cuidado de especificar parámetros de configuración idénticos (`spec.backendName` como `, , , `spec.storagePrefix` spec.storageDriverName etc.). Trident enlazará automáticamente los recién creados TridentBackendConfig con el backend preexistente.`

## Descripción general de los pasos

Para crear un nuevo back-end mediante `kubectl`, debe hacer lo siguiente:

1. Cree a "**Secreto Kubernetes**". El secreto contiene las credenciales que Trident necesita para comunicarse con el clúster/servicio de almacenamiento.
2. Cree un `TridentBackendConfig` objeto. Este contiene detalles sobre el servicio/clúster de almacenamiento y hace referencia al secreto creado en el paso anterior.

Después de crear un backend, puede observar su estado utilizando `kubectl get tbc <tbc-name> -n <trident-namespace>` y recopile detalles adicionales.

### Paso 1: Cree un secreto de Kubernetes

Cree un secreto que contenga las credenciales de acceso para el back-end. Esto es único para cada servicio/plataforma de almacenamiento. Veamos un ejemplo:

```
kubectl -n trident create -f backend-tbc-ontap-san-secret.yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: cluster-admin
  password: t@Ax@7q(>
```

Esta tabla resume los campos que deben incluirse en el secreto para cada plataforma de almacenamiento:

Descripción de campos secretos de la plataforma de almacenamiento	Secreto	Descripción de los campos
Azure NetApp Files	ID del Cliente	El ID de cliente de un registro de aplicación
Cloud Volumes Service para GCP	id_clave_privada	ID de la clave privada. Parte de la clave API de la cuenta de servicio de GCP con el rol de administrador CVS

Descripción de campos secretos de la plataforma de almacenamiento	Secreto	Descripción de los campos
Cloud Volumes Service para GCP	clave_privada	Clave privada. Parte de la clave API de la cuenta de servicio de GCP con el rol de administrador CVS
Element (HCI/SolidFire de NetApp)	Extremo	MVIP para el clúster de SolidFire con credenciales de inquilino
ONTAP	nombre de usuario	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales
ONTAP	contraseña	Contraseña para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales
ONTAP	ClientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados
ONTAP	ChapUsername	Nombre de usuario entrante. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy
ONTAP	InitichapatorSecret	Secreto CHAP del iniciador. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy
ONTAP	ChapTargetUsername	Nombre de usuario de destino. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy
ONTAP	ChapTargetInitiatorSecret	Secreto CHAP del iniciador de destino. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy

El secreto creado en este paso será referenciado en el `spec.credentials` del `TridentBackendConfig` objeto creado en el paso siguiente.

## Paso 2: Cree la `TridentBackendConfig` CR

Ya está listo para crear su `TridentBackendConfig` CR. En este ejemplo, un back-end que utiliza `ontap-san` el controlador se crea mediante `TridentBackendConfig` objeto mostrado a continuación:

```
kubectl -n trident create -f backend-tbc-ontap-san.yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

## Paso 3: Compruebe el estado del `TridentBackendConfig` CR

Ahora que creó la `TridentBackendConfig` CR, puede comprobar el estado. Consulte el siguiente ejemplo:

```
kubectl -n trident get tbc backend-tbc-ontap-san
```

NAME	PHASE	STATUS	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san		Bound	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
			Success	

Se ha creado un backend correctamente y se ha enlazado a `TridentBackendConfig` CR.

La fase puede tomar uno de los siguientes valores:

- **Bound:** La `TridentBackendConfig` CR está asociado con un backend, y ese backend contiene `configRef` establezca en la `TridentBackendConfig` UID de CR.
- **Unbound:** Representado usando `""`. La `TridentBackendConfig` el objeto no está enlazado a un back-end. Creadas recientemente `TridentBackendConfig` CRS se encuentra en esta fase de forma predeterminada. Tras cambiar la fase, no puede volver a «sin límites».
- **Deleting:** La `TridentBackendConfig` CR `deletionPolicy` se ha configurado para eliminar. Cuando la `TridentBackendConfig` La CR se elimina y pasa al estado de supresión.
  - Si no existen reclamaciones de volumen persistentes (RVP) en el back-end, si se elimina el Trident, tanto el `TridentBackendConfig` back-end como la `TridentBackendConfig` CR.

- Si uno o más EVs están presentes en el backend, pasa a un estado de supresión. La `TridentBackendConfig` Posteriormente, CR también entra en fase de eliminación. El back-end y. `TridentBackendConfig` Se eliminan sólo después de que se hayan eliminado todas las EVs.
- **Lost:** El backend asociado con `TridentBackendConfig` La CR se eliminó accidental o deliberadamente y la `TridentBackendConfig` CR todavía tiene una referencia al backend eliminado. La `TridentBackendConfig` La CR puede ser eliminada independientemente de la `deletionPolicy` valor.
- **Unknown:** Trident no puede determinar el estado o la existencia del backend asociado al `TridentBackendConfig` CR. Por ejemplo, si el servidor API no responde o si falta el `tridentbackends.trident.netapp.io` CRD. Esto puede requerir intervención.

En esta fase, se ha creado un backend. Hay varias operaciones que se pueden realizar además, como ["actualizaciones back-end y eliminaciones backend"](#).

#### (Opcional) Paso 4: Obtener más detalles

Puede ejecutar el siguiente comando para obtener más información acerca de su entorno de administración:

```
kubectl -n trident get tbc backend-tbc-ontap-san -o wide
```

NAME	PHASE	STATUS	STORAGE DRIVER	BACKEND NAME	DELETION POLICY	BACKEND UUID
backend-tbc-ontap-san		Bound	Success	ontap-san-backend	ontap-san	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8

Además, también puede obtener un volcado YLMA/JSON de `TridentBackendConfig`.

```
kubectl -n trident get tbc backend-tbc-ontap-san -o yaml
```

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: "2021-04-21T20:45:11Z"
  finalizers:
  - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
  uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
    backendName: ontap-san-backend
    backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
  deletionPolicy: delete
  lastOperationStatus: Success
  message: Backend 'ontap-san-backend' created
  phase: Bound

```

`backendInfo` Contiene los `backendName` y el `backendUUID` del backend que se creó en respuesta a la `TridentBackendConfig` CR. El `lastOperationStatus` campo representa el estado de la última operación `TridentBackendConfig` del CR, que puede ser activada por el usuario (por ejemplo, el usuario cambió algo en `spec`) o activada por Trident (por ejemplo, durante los reinicios de Trident). Puede ser `Success` o `Failed`. `phase` Representa el estado de la relación entre `TridentBackendConfig` el CR y el backend. En el ejemplo anterior, `phase` tiene el valor `bound`, lo que significa que `TridentBackendConfig` el CR está asociado al backend.

Puede ejecutar el `kubectl -n trident describe tbc <tbc-cr-name>` comando para obtener detalles de los registros de eventos.



No puede actualizar ni eliminar un backend que contenga un archivo asociado `TridentBackendConfig` objeto con `tridentctl`. Comprender los pasos que implica cambiar entre `tridentctl` y `TridentBackendConfig`, ["ver aquí"](#).

## Gestionar back-ends

### Realice la gestión del entorno de administración con kubectl

Obtenga información sobre cómo realizar operaciones de administración de back-end mediante `kubectl`.

#### Eliminar un back-end

Al suprimir un `TridentBackendConfig`, indica a Trident que suprima/conserva los back-ends (según `deletionPolicy`). Para suprimir un backend, asegúrese de que `deletionPolicy` está definido como `DELETE`. Para suprimir sólo el `TridentBackendConfig`, asegúrese de que `deletionPolicy` está definido en `Retener`. Esto asegura que el backend todavía está presente y se puede gestionar mediante el uso `tridentctl`.

Ejecute el siguiente comando:

```
kubectl delete tbc <tbc-name> -n trident
```

Trident no elimina los secretos de Kubernetes que estaban en uso por `TridentBackendConfig`. El usuario de Kubernetes es responsable de limpiar los secretos. Hay que tener cuidado a la hora de eliminar secretos. Solo debe eliminar secretos si no los están utilizando los back-ends.

#### Ver los back-ends existentes

Ejecute el siguiente comando:

```
kubectl get tbc -n trident
```

También puede ejecutar `tridentctl get backend -n trident` o `tridentctl get backend -o yaml -n trident` obtener una lista de todos los back-ends que existen. Esta lista también incluirá los back-ends que se crearon con `tridentctl`.

#### Actualizar un back-end

Puede haber varias razones para actualizar un back-end:

- Las credenciales del sistema de almacenamiento han cambiado. Para actualizar las credenciales, se debe actualizar el secreto de Kubernetes utilizado en el `TridentBackendConfig` objeto. Trident actualizará automáticamente el backend con las últimas credenciales proporcionadas. Ejecute el siguiente comando para actualizar Kubernetes Secret:

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- Es necesario actualizar los parámetros (como el nombre de la SVM de ONTAP que se está utilizando).
  - Puede actualizar `TridentBackendConfig` Objetos directamente a través de Kubernetes usando el siguiente comando:

```
kubectl apply -f <updated-backend-file.yaml>
```

- Como alternativa, puede realizar cambios en los existentes `TridentBackendConfig` CR con el siguiente comando:

```
kubectl edit tbc <tbc-name> -n trident
```



- Si falla una actualización de back-end, el back-end continúa en su última configuración conocida. Puede ver los registros para determinar la causa ejecutando `kubectl get tbc <tbc-name> -o yaml -n trident` o `kubectl describe tbc <tbc-name> -n trident`.
- Después de identificar y corregir el problema con el archivo de configuración, puede volver a ejecutar el comando `update`.

## Realizar la administración de back-end con `tridentctl`

Obtenga información sobre cómo realizar operaciones de administración de back-end mediante `tridentctl`.

### Cree un back-end

Después de crear un ["archivo de configuración del back-end"](#), ejecute el siguiente comando:

```
tridentctl create backend -f <backend-file> -n trident
```

Si se produce un error en la creación del back-end, algo estaba mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs -n trident
```

Después de identificar y corregir el problema con el archivo de configuración, simplemente puede ejecutar el `create` comando de nuevo.

### Eliminar un back-end

Para suprimir un backend de Trident, haga lo siguiente:

1. Recupere el nombre del backend:

```
tridentctl get backend -n trident
```

2. Eliminar el back-end:

```
tridentctl delete backend <backend-name> -n trident
```



Si Trident ha provisionado volúmenes y snapshots a partir de este back-end que aún existen, al eliminar el back-end se evita que se provisionen nuevos volúmenes. El back-end continuará existiendo en un estado de “eliminación” y Trident seguirá gestionando esos volúmenes y instantáneas hasta que se eliminen.

### Ver los back-ends existentes

Para ver los back-ends que Trident conoce, haga lo siguiente:

- Para obtener un resumen, ejecute el siguiente comando:

```
tridentctl get backend -n trident
```

- Para obtener todos los detalles, ejecute el siguiente comando:

```
tridentctl get backend -o json -n trident
```

### Actualizar un back-end

Después de crear un nuevo archivo de configuración de back-end, ejecute el siguiente comando:

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

Si falla la actualización del back-end, algo estaba mal con la configuración del back-end o intentó una actualización no válida. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs -n trident
```

Después de identificar y corregir el problema con el archivo de configuración, simplemente puede ejecutar el update comando de nuevo.

### Identifique las clases de almacenamiento que utilizan un back-end

Este es un ejemplo del tipo de preguntas que puede responder con el JSON que `tridentctl` salidas para objetos backend. Utiliza la `jq` utilidad, que debe instalar.

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name, storageClasses: [.storage[].storageClasses]|unique}]'
```

Esto también se aplica a los back-ends que se crearon con el uso `TridentBackendConfig`.



## Pasar entre las opciones de administración del back-end

Obtén información sobre las diferentes formas de administrar back-ends en Trident.

### Opciones para gestionar back-ends

Con la introducción de `TridentBackendConfig`, los administradores ahora tienen dos formas únicas de administrar los back-ends. Esto plantea las siguientes preguntas:

- Pueden crearse back-ends con `tridentctl` administrarse con `TridentBackendConfig`?
- Pueden crearse back-ends con `TridentBackendConfig` se gestionan mediante `tridentctl`?

### Gestione `tridentctl` con los back-ends `TridentBackendConfig`

En esta sección se describen los pasos necesarios para gestionar los back-ends creados con `tridentctl` directamente mediante la interfaz de Kubernetes creando `TridentBackendConfig` objetos.

Esto se aplica a las siguientes situaciones:

- Back-ends preexistentes, que no tienen un `TridentBackendConfig` porque fueron creados con `tridentctl`.
- Nuevos back-ends que se crearon con `tridentctl`, mientras que otros `TridentBackendConfig` existen objetos.

En ambos escenarios, los back-ends seguirán presentes, con Trident programando volúmenes y operando en ellos. A continuación, los administradores tienen una de estas dos opciones:

- Siga utilizando `tridentctl` para gestionar los back-ends que se crearon con él.
- Enlazar los back-ends creados con `tridentctl` a un nuevo `TridentBackendConfig` objeto. Hacerlo significaría que se gestionarán los back-ends `kubectl` y no `tridentctl`.

Para administrar un back-end preexistente mediante `kubectl`, tendrá que crear un `TridentBackendConfig` que enlaza con el backend existente. A continuación se ofrece una descripción general de cómo funciona:

1. Cree un secreto de Kubernetes. El secreto contiene las credenciales que Trident necesita para comunicarse con el clúster/servicio de almacenamiento.
2. Cree un `TridentBackendConfig` objeto. Este contiene detalles sobre el servicio/clúster de almacenamiento y hace referencia al secreto creado en el paso anterior. Se debe tener cuidado para especificar parámetros de configuración idénticos (como `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName`, y así sucesivamente). `spec.backendName` se debe establecer el nombre del backend existente.

### Paso 0: Identificar el back-end

Para crear un `TridentBackendConfig` que se enlaza a un backend existente, necesitará obtener la configuración de backend. En este ejemplo, supongamos que se ha creado un back-end mediante la siguiente definición JSON:

```
tridentctl get backend ontap-nas-backend -n trident
```

```

+-----+-----+
+-----+-----+-----+-----+
|           NAME           | STORAGE DRIVER |           UUID
| STATE | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |      25 |
+-----+-----+
+-----+-----+-----+-----+

```

```
cat ontap-nas-backend.json
```

```

{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.10.10.1",
  "dataLIF": "10.10.10.2",
  "backendName": "ontap-nas-backend",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "admin-password",

  "defaults": {
    "spaceReserve": "none",
    "encryption": "false"
  },
  "labels": {"store": "nas_store"},
  "region": "us_east_1",
  "storage": [
    {
      "labels": {"app": "msoffice", "cost": "100"},
      "zone": "us_east_1a",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "true",
        "unixPermissions": "0755"
      }
    },
    {
      "labels": {"app": "mysqldb", "cost": "25"},
      "zone": "us_east_1d",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "false",
        "unixPermissions": "0775"
      }
    }
  ]
}

```

```
    }  
  }  
]  
}
```

### Paso 1: Cree un secreto de Kubernetes

Cree un secreto que contenga las credenciales del back-end, como se muestra en este ejemplo:

```
cat tbc-ontap-nas-backend-secret.yaml  
  
apiVersion: v1  
kind: Secret  
metadata:  
  name: ontap-nas-backend-secret  
type: Opaque  
stringData:  
  username: cluster-admin  
  password: admin-password  
  
kubectl create -f tbc-ontap-nas-backend-secret.yaml -n trident  
secret/backend-tbc-ontap-san-secret created
```

### Paso 2: Cree un TridentBackendConfig CR

El paso siguiente es crear un `TridentBackendConfig` CR que se enlazará automáticamente a la preexistente `ontap-nas-backend` (como en este ejemplo). Asegurarse de que se cumplen los siguientes requisitos:

- El mismo nombre de fondo se define en `spec.backendName`.
- Los parámetros de configuración son idénticos al backend original.
- Los pools virtuales (si están presentes) deben conservar el mismo orden que en el back-end original.
- Las credenciales se proporcionan a través de un secreto de Kubernetes, pero no en texto sin formato.

En este caso, el `TridentBackendConfig` tendrá este aspecto:

```

cat backend-tbc-ontap-nas.yaml
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: tbc-ontap-nas-backend
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.10.10.1
  dataLIF: 10.10.10.2
  backendName: ontap-nas-backend
  svm: trident_svm
  credentials:
    name: mysecret
  defaults:
    spaceReserve: none
    encryption: 'false'
  labels:
    store: nas_store
  region: us_east_1
  storage:
  - labels:
    app: msoffice
    cost: '100'
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: 'true'
      unixPermissions: '0755'
  - labels:
    app: mysqldb
    cost: '25'
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: 'false'
      unixPermissions: '0775'

kubect1 create -f backend-tbc-ontap-nas.yaml -n trident
tridentbackendconfig.trident.netapp.io/tbc-ontap-nas-backend created

```

### Paso 3: Compruebe el estado del TridentBackendConfig CR

Después del TridentBackendConfig se ha creado, su fase debe ser Bound. También debería reflejar el mismo nombre de fondo y UUID que el del back-end existente.

```

kubect1 get tbc tbc-ontap-nas-backend -n trident
NAME                                BACKEND NAME                BACKEND UUID
PHASE    STATUS
tbc-ontap-nas-backend  ontap-nas-backend          52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7    Bound    Success

#confirm that no new backends were created (i.e., TridentBackendConfig did
not end up creating a new backend)
tridentctl get backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID
| STATE  | VOLUMES |
+-----+-----+-----+-----+
| ontap-nas-backend     | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |          25 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

El back-end se gestionará completamente mediante el tbc-ontap-nas-backend TridentBackendConfig objeto.

**Gestione TridentBackendConfig con los back-ends tridentctl**

`tridentctl` se puede utilizar para enumerar los back-ends que se crearon con `TridentBackendConfig`. Además, los administradores también pueden optar por gestionar completamente estos back-ends `tridentctl` eliminando `TridentBackendConfig` y eso seguro `spec.deletionPolicy` se establece en `retain`.

**Paso 0: Identificar el back-end**

Por ejemplo, supongamos que se ha creado el siguiente back-end mediante TridentBackendConfig:

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                BACKEND UUID
PHASE  STATUS  STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound  Success  ontap-san  delete

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|      NAME      | STORAGE DRIVER |                               UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |      33 |
+-----+-----+
+-----+-----+-----+-----+
```

Desde la salida, se ve eso TridentBackendConfig Se ha creado correctamente y está enlazado a un backend [observe el UUID del backend].

**Paso 1: Confirmar** deletionPolicy **se establece en** retain

Echemos un vistazo al valor de deletionPolicy. Se debe establecer en retain. Esto garantiza que cuando se elimina un TridentBackendConfig CR, la definición de backend seguirá presente y se puede gestionar con tridentctl.

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                BACKEND UUID
PHASE  STATUS  STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound  Success  ontap-san  delete

# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                BACKEND UUID
PHASE  STATUS  STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound  Success  ontap-san  retain
```



No continúe con el siguiente paso a menos que `deletionPolicy` se establezca en `retain`.

## Paso 2: Elimine la `TridentBackendConfig` CR

El paso final es eliminar la `TridentBackendConfig` CR. Tras confirmar la `deletionPolicy` se establece en `retain`, puede utilizar `Adelante` con la eliminación:

```
kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                UUID
| STATE  | VOLUMES |
+-----+-----+-----+
+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |          33 |
+-----+-----+-----+
+-----+-----+-----+
```

Tras la eliminación del `TridentBackendConfig` objeto, Trident simplemente lo elimina sin eliminar realmente el backend.

# Crear y gestionar clases de almacenamiento

## Cree una clase de almacenamiento

Configure un objeto `StorageClass` de Kubernetes y cree la clase de almacenamiento para indicar a Trident cómo se aprovisionan los volúmenes.

### Configurar un objeto de Kubernetes `StorageClass`

El "[Objeto de Kubernetes `StorageClass`](#)" identifica el Trident como el aprovisionador que se usa para esa clase y le indica a Trident cómo aprovisionar un volumen. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters:
  <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate
```

Consulte el ["Objetos de Kubernetes y Trident"](#) para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los `PersistentVolumeClaim` parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

### Cree una clase de almacenamiento

Después de crear el objeto `StorageClass`, puede crear la clase de almacenamiento. [Muestras de clase de almacenamiento](#) proporciona algunas muestras básicas que puede utilizar o modificar.

#### Pasos

1. Este es un objeto de Kubernetes, así que use `kubectl` Para crear en Kubernetes.

```
kubectl create -f sample-input/storage-class-basic-csi.yaml
```

2. Ahora deberías ver una clase de almacenamiento **basic-csi** tanto en Kubernetes como en Trident, y Trident debería haber descubierto los pools en el back-end.



```

kubect1 get sc basic-csi
NAME          PROVISIONER          AGE
basic-csi    csi.trident.netapp.io  15h

./tridentctl -n trident get storageclass basic-csi -o json
{
  "items": [
    {
      "Config": {
        "version": "1",
        "name": "basic-csi",
        "attributes": {
          "backendType": "ontap-nas"
        },
        "storagePools": null,
        "additionalStoragePools": null
      },
      "storage": {
        "ontapnas_10.0.0.1": [
          "aggr1",
          "aggr2",
          "aggr3",
          "aggr4"
        ]
      }
    }
  ]
}

```

### Muestras de clase de almacenamiento

Trident ofrece ["definiciones simples de clase de almacenamiento para back-ends específicos"](#).

Como alternativa, puede editar `sample-input/storage-class-csi.yaml.template` archivo que viene con el instalador y reemplácelo `BACKEND_TYPE` con el nombre del controlador de almacenamiento.

```

./tridentctl -n trident get backend
+-----+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |           UUID           |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| nas-backend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |         0 |
+-----+-----+-----+-----+
+-----+-----+

cp sample-input/storage-class-csi.yaml.templ sample-input/storage-class-
basic-csi.yaml

# Modify __BACKEND_TYPE__ with the storage driver field above (e.g.,
ontap-nas)
vi sample-input/storage-class-basic-csi.yaml

```

## Gestione las clases de almacenamiento

Puede ver las clases de almacenamiento existentes, definir una clase de almacenamiento predeterminada, identificar el back-end de la clase de almacenamiento y eliminar clases de almacenamiento.

### Consulte las clases de almacenamiento existentes

- Para ver las clases de almacenamiento Kubernetes existentes, ejecute el siguiente comando:

```
kubectl get storageclass
```

- Para ver la información sobre la clase de almacenamiento Kubernetes, ejecute el siguiente comando:

```
kubectl get storageclass <storage-class> -o json
```

- Para ver las clases de almacenamiento sincronizado de Trident, ejecute el siguiente comando:

```
tridentctl get storageclass
```

- Para ver los detalles de la clase de almacenamiento sincronizado de Trident, ejecute el siguiente comando:

```
tridentctl get storageclass <storage-class> -o json
```

## Establecer una clase de almacenamiento predeterminada

Kubernetes 1.6 añadió la capacidad de establecer un tipo de almacenamiento predeterminado. Esta es la clase de almacenamiento que se usará para aprovisionar un volumen persistente si un usuario no especifica una en una solicitud de volumen persistente (PVC).

- Defina una clase de almacenamiento predeterminada configurando la anotación `storageclass.kubernetes.io/is-default-class` a `true` en la definición de la clase de almacenamiento. Según la especificación, cualquier otro valor o ausencia de la anotación se interpreta como falso.
- Puede configurar una clase de almacenamiento existente para que sea la clase de almacenamiento predeterminada mediante el siguiente comando:

```
kubectl patch storageclass <storage-class-name> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

- De forma similar, puede eliminar la anotación predeterminada de la clase de almacenamiento mediante el siguiente comando:

```
kubectl patch storageclass <storage-class-name> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

También hay ejemplos en el paquete del instalador de Trident que incluyen esta anotación.



Solo debe haber una clase de almacenamiento predeterminada en el clúster a la vez. Si no dispone de más de una, técnicamente, Kubernetes no le impide ofrecer más de una, pero funcionará como si no hubiera una clase de almacenamiento predeterminada en absoluto.

## Identifique el back-end para una clase de almacenamiento

Este es un ejemplo del tipo de preguntas que puede responder con el JSON que `tridentctl` genera los objetos de backend Trident. Esto utiliza la `jq` utilidad, que es posible que tenga que instalar primero.

```
tridentctl get storageclass -o json | jq '[.items[] | {storageClass: .Config.name, backends: [.storage]|unique}]'
```

## Elimine una clase de almacenamiento

Para eliminar una clase de almacenamiento de Kubernetes, ejecute el siguiente comando:

```
kubectl delete storageclass <storage-class>
```

`<storage-class>` debe sustituirse por su clase de almacenamiento.

Todos los volúmenes persistentes que se hayan creado a través de esta clase de almacenamiento permanecerán intactos, y Trident continuará gestionándolos.



Trident aplica un espacio en blanco `fsType` para los volúmenes que crea. En el caso de los back-ends iSCSI, se recomienda aplicar `parameters.fsType` en la clase de almacenamiento. Debe eliminar StorageClasses existentes y volver a crearlos con `parameters.fsType` los especificados.

## Aprovisione y gestione volúmenes

### Aprovisione un volumen

Cree un volumen persistente (VP) y una reclamación de volumen persistente (RVP) que utilice el tipo de almacenamiento de Kubernetes configurado para solicitar acceso al VP. A continuación, puede montar el VP en un pod.

#### Descripción general

1. "*Volumen persistente*" (PV) es un recurso de almacenamiento físico provisionado por el administrador del clúster en un clúster de Kubernetes. La "*Claim de volumen persistente*" (RVP) es una solicitud para acceder al volumen persistente en el clúster.

La RVP se puede configurar para solicitar almacenamiento de un determinado tamaño o modo de acceso. Mediante el StorageClass asociado, el administrador del clúster puede controlar mucho más que el tamaño de los volúmenes persistentes y el modo de acceso, como el rendimiento o el nivel de servicio.

Después de crear el VP y la RVP, puede montar el volumen en un pod.

#### Manifiestos de muestra

## Manifiesto de muestra de volumen persistente

Este manifiesto de ejemplo muestra un PV básico de 10Gi que está asociado con StorageClass `basic-csi`.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-storage
  labels:
    type: local
spec:
  storageClassName: basic-csi
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: "/my/host/path"
```

## Manifiestos de muestra de PersistentVolumeClaim

Estos ejemplos muestran opciones básicas de configuración de PVC.

### PVC con acceso RWO

En este ejemplo se muestra una RVP básica con acceso RWO que está asociada con una clase de almacenamiento denominada `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

### PVC con NVMe/TCP

En este ejemplo, se muestra una PVC básica para NVMe/TCP con acceso RWO asociado con una clase de almacenamiento denominada `protection-gold`.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san-nvme
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: protection-gold
```

## Muestras de manifiesto de POD

Estos ejemplos muestran configuraciones básicas para conectar la RVP a un pod.

### Configuración básica

```
kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/my/mount/path"
          name: pv-storage
```

## Configuración de NVMe/TCP básica

```
---
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: null
  labels:
    run: nginx
  name: nginx
spec:
  containers:
  - image: nginx
    name: nginx
    resources: {}
    volumeMounts:
    - mountPath: "/usr/share/nginx/html"
      name: task-pv-storage
  dnsPolicy: ClusterFirst
  restartPolicy: Always
  volumes:
  - name: task-pv-storage
    persistentVolumeClaim:
      claimName: pvc-san-nvme
```

## Cree el VP y la RVP

### Pasos

1. Cree el VP.

```
kubectl create -f pv.yaml
```

2. Compruebe el estado de PV.

```
kubectl get pv
NAME          CAPACITY  ACCESS MODES  RECLAIM POLICY  STATUS  CLAIM
STORAGECLASS  REASON    AGE
pv-storage    4Gi      RWO           Retain          Available
7s
```

3. Cree la RVP.



```
kubectl create -f pvc.yaml
```

#### 4. Verifique el estado de la RVP.

```
kubectl get pvc
NAME          STATUS VOLUME          CAPACITY ACCESS MODES STORAGECLASS AGE
pvc-storage  Bound  pv-name 2Gi          RWO          5m
```

#### 5. Monte el volumen en un pod.

```
kubectl create -f pv-pod.yaml
```



Puede supervisar el progreso con `kubectl get pod --watch`.

#### 6. Compruebe que el volumen está montado en `/my/mount/path`.

```
kubectl exec -it task-pv-pod -- df -h /my/mount/path
```

#### 7. Ahora puede eliminar el Pod. La aplicación Pod ya no existirá, pero el volumen permanecerá.

```
kubectl delete pod task-pv-pod
```

Consulte el ["Objetos de Kubernetes y Trident"](#) para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los `PersistentVolumeClaim` parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

## Expanda los volúmenes

Trident ofrece a los usuarios de Kubernetes la capacidad de expandir sus volúmenes una vez que se crean. Encuentre información sobre las configuraciones que se necesitan para ampliar los volúmenes iSCSI y NFS.

### Expanda un volumen iSCSI

Puede expandir un volumen persistente iSCSI (PV) mediante el aprovisionador CSI.



La ampliación del volumen iSCSI se admite en el `ontap-san`, `ontap-san-economy`, `solidfire-san` Requiere Kubernetes 1.16 o posterior.

#### Paso 1: Configure el tipo de almacenamiento para que admita la ampliación de volumen

Edite la definición de `StorageClass` para establecer el `allowVolumeExpansion` campo a `true`.

```
cat storageclass-ontapsan.yaml
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
allowVolumeExpansion: True
```

En el caso de un tipo de almacenamiento existente, edítelo para incluir el `allowVolumeExpansion` parámetro.

### **Paso 2: Cree una RVP con el tipo de almacenamiento que ha creado**

Edite la definición de PVC y actualice el `spec.resources.requests.storage` para reflejar el nuevo tamaño deseado, que debe ser mayor que el tamaño original.

```
cat pvc-ontapsan.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: san-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-san
```

Trident crea un volumen persistente (VP) y lo asocia con esta reclamación de volumen persistente (RVP).

```

kubect1 get pvc
NAME          STATUS      VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
san-pvc      Bound       pvc-8a814d62-bd58-4253-b0d1-82f2885db671  1Gi
RWO          ontap-san    8s

kubect1 get pv
NAME          CAPACITY  ACCESS MODES
RECLAIM POLICY  STATUS    CLAIM          STORAGECLASS  REASON    AGE
pvc-8a814d62-bd58-4253-b0d1-82f2885db671  1Gi      RWO
Delete        Bound     default/san-pvc  ontap-san    10s

```

### Paso 3: Defina un pod que fije el PVC

Conecte el VP a un pod para que se cambie su tamaño. Existen dos situaciones a la hora de cambiar el tamaño de un VP iSCSI:

- Si el VP está conectado a un pod, Trident expande el volumen en el backend de almacenamiento, vuelve a escanear el dispositivo y cambia el tamaño del sistema de archivos.
- Cuando se intenta cambiar el tamaño de un VP no conectado, Trident expande el volumen en el back-end de almacenamiento. Una vez que la RVP está Unido a un pod, Trident vuelve a buscar el dispositivo y cambia el tamaño del sistema de archivos. Kubernetes, después, actualiza el tamaño de RVP después de completar correctamente la operación de ampliación.

En este ejemplo, se crea un pod que utiliza `san-pvc`.

```
kubectl get pod
NAME          READY   STATUS    RESTARTS   AGE
ubuntu-pod   1/1     Running   0           65s

kubectl describe pvc san-pvc
Name:          san-pvc
Namespace:     default
StorageClass:  ontap-san
Status:        Bound
Volume:        pvc-8a814d62-bd58-4253-b0d1-82f2885db671
Labels:        <none>
Annotations:   pv.kubernetes.io/bind-completed: yes
               pv.kubernetes.io/bound-by-controller: yes
               volume.beta.kubernetes.io/storage-provisioner:
               csi.trident.netapp.io
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      1Gi
Access Modes:  RWO
VolumeMode:    Filesystem
Mounted By:    ubuntu-pod
```

#### **Paso 4: Expanda el PV**

Para cambiar el tamaño del VP que se ha creado de 1Gi a 2gi, edite la definición de PVC y actualice el `spec.resources.requests.storage` A 2gi.

```

kubect1 edit pvc san-pvc
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: "2019-10-10T17:32:29Z"
  finalizers:
  - kubernetes.io/pvc-protection
  name: san-pvc
  namespace: default
  resourceVersion: "16609"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/san-pvc
  uid: 8a814d62-bd58-4253-b0d1-82f2885db671
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 2Gi
  ...

```

### Paso 5: Validar la expansión

Puede validar correctamente la ampliación operativa comprobando el tamaño de la RVP, el VP y el volumen Trident:

```

kubect1 get pvc san-pvc
NAME          STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
san-pvc      Bound      pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi
RWO          ontap-san    11m
kubect1 get pv
NAME          CAPACITY  ACCESS MODES
RECLAIM POLICY  STATUS    CLAIM          STORAGECLASS  REASON  AGE
pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi      RWO
Delete          Bound      default/san-pvc  ontap-san    12m
tridentctl get volumes -n trident
+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  |  MANAGED  |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-8a814d62-bd58-4253-b0d1-82f2885db671 | 2.0 GiB | ontap-san    |
block    | a9b7bfff-0505-4e31-b6c5-59f492e02d33 | online | true    |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

## Expanda un volumen NFS

Trident admite la expansión de volumen para VP NFS provisionados en `ontap-nas`, `ontap-nas-economy` `ontap-nas-flexgroup` `gcp-cvs` y `azure-netapp-files` **back-ends**.

### Paso 1: Configure el tipo de almacenamiento para que admita la ampliación de volumen

Para cambiar el tamaño de un VP de NFS, el administrador primero tiene que configurar la clase de almacenamiento para permitir la expansión del volumen estableciendo el `allowVolumeExpansion` campo a `true`:

```

cat storageclass-ontapnas.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontapnas
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
allowVolumeExpansion: true

```

Si ya ha creado una clase de almacenamiento sin esta opción, puede simplemente editar la clase de almacenamiento existente mediante `kubect1 edit storageclass` para permitir la expansión de volumen.

## Paso 2: Cree una RVP con el tipo de almacenamiento que ha creado

```
cat pvc-ontapnas.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: ontapnas20mb
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 20Mi
  storageClassName: ontapnas
```

Trident debe crear un PV de NFS de 20MiB TB para esta RVP:

```
kubectl get pvc
NAME                STATUS    VOLUME
CAPACITY            ACCESS MODES  STORAGECLASS  AGE
ontapnas20mb       Bound     pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi
RWO                 ontapnas     9s

kubectl get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME                CAPACITY  ACCESS MODES
RECLAIM POLICY     STATUS    CLAIM                STORAGECLASS  REASON
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi     RWO
Delete             Bound     default/ontapnas20mb  ontapnas
2m42s
```

## Paso 3: Expanda el PV

Para cambiar el tamaño del VP de 20 MiB recién creado a 1 GiB, edite el RVP y establezca `spec.resources.requests.storage` a 1GiB:

```
kubectl edit pvc ontapnas20mb
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: 2018-08-21T18:26:44Z
  finalizers:
  - kubernetes.io/pvc-protection
  name: ontapnas20mb
  namespace: default
  resourceVersion: "1958015"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/ontapnas20mb
  uid: c1bd7fa5-a56f-11e8-b8d7-fa163e59eaab
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  ...
```

#### Paso 4: Validar la expansión

Puede validar el tamaño correctamente trabajado comprobando el tamaño de la RVP, el VP y el volumen Trident:



```

kubect1 get pvc ontapnas20mb
NAME                STATUS      VOLUME
CAPACITY  ACCESS MODES  STORAGECLASS  AGE
ontapnas20mb  Bound        pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi
RWO                ontapnas                4m44s

kubect1 get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME                CAPACITY  ACCESS MODES
RECLAIM POLICY     STATUS    CLAIM                STORAGECLASS  REASON
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi      RWO
Delete            Bound    default/ontapnas20mb  ontapnas
5m35s

tridentctl get volume pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 -n trident
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  | MANAGED |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 | 1.0 GiB | ontapnas      |
file      | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online | true      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

## Importar volúmenes

Es posible importar volúmenes de almacenamiento existentes como un VP de Kubernetes mediante `tridentctl import`.

### Descripción general y consideraciones

Es posible importar un volumen en Trident para lo siguiente:

- Agrupe en contenedores una aplicación y vuelva a utilizar su conjunto de datos existente
- Utilice el clon de un conjunto de datos para una aplicación efímera
- Reconstruya un clúster de Kubernetes que haya fallado
- Migración de datos de aplicaciones durante la recuperación ante desastres

### Consideraciones

Antes de importar un volumen, revise las siguientes consideraciones.

- Trident solo puede importar volúmenes ONTAP de tipo RW (lectura y escritura). Los volúmenes del tipo DP (protección de datos) son volúmenes de destino de SnapMirror. Debe romper la relación de reflejo antes de importar el volumen a Trident.

- Sugerimos importar volúmenes sin conexiones activas. Para importar un volumen que se usa activamente, clone el volumen y, a continuación, realice la importación.



Esto es especialmente importante en el caso de volúmenes de bloque, ya que Kubernetes no sabía que la conexión anterior y podría conectar fácilmente un volumen activo a un pod. Esto puede provocar daños en los datos.

- Aunque `StorageClass` debe especificarse en una RVP, Trident no utiliza este parámetro durante la importación. Durante la creación de volúmenes, se usan las clases de almacenamiento para seleccionar entre los pools disponibles según las características de almacenamiento. Como el volumen ya existe, no se requiere ninguna selección de pool durante la importación. Por lo tanto, la importación no fallará incluso si el volumen existe en un back-end o pool que no coincide con la clase de almacenamiento especificada en la RVP.
- El tamaño del volumen existente se determina y se establece en la RVP. Una vez que el controlador de almacenamiento importa el volumen, se crea el PV con un `ClaimRef` al PVC.
  - La política de reclamaciones se establece inicialmente en `retain` En el PV. Una vez que Kubernetes enlaza correctamente la RVP y el VP, se actualiza la política de reclamaciones para que coincida con la política de reclamaciones de la clase de almacenamiento.
  - Si la política de reclamaciones de la clase de almacenamiento es `delete`, El volumen de almacenamiento se eliminará cuando se elimine el PV.
- De forma predeterminada, Trident administra la RVP y cambia el nombre de FlexVol y LUN en el back-end. Puede pasar `--no-manage` la marca para importar un volumen no gestionado. Si utiliza `--no-manage`, Trident no realiza ninguna operación adicional en la RVP o el VP durante el ciclo de vida de los objetos. El volumen de almacenamiento no se elimina cuando se elimina el VP, y también se ignoran otras operaciones como el clon de volumen y el cambio de tamaño de volumen.



Esta opción es útil si desea usar Kubernetes para cargas de trabajo en contenedores, pero de lo contrario desea gestionar el ciclo de vida del volumen de almacenamiento fuera de Kubernetes.

- Se agrega una anotación a la RVP y al VP que tiene el doble propósito de indicar que el volumen se importó y si se administran la PVC y la VP. Esta anotación no debe modificarse ni eliminarse.

## Importe un volumen

Puede utilizar `tridentctl import` para importar un volumen.

### Pasos

1. Cree el archivo de reclamación de volumen persistente (RVP) (por ejemplo, `pvc.yaml`) Que se utilizará para crear la RVP. El archivo PVC debe incluir `name`, `namespace`, `accessModes`, y `storageClassName`. Opcionalmente, se puede especificar `unixPermissions` En su definición de PVC.

A continuación se muestra un ejemplo de una especificación mínima:

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: my_claim
  namespace: my_namespace
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: my_storage_class

```



No incluya parámetros adicionales, como el nombre del VP o el tamaño del volumen. Esto puede provocar un error en el comando de importación.

- Utilice `tridentctl import` el comando para especificar el nombre del back-end de Trident que contiene el volumen y el nombre que identifica de manera única el volumen en el almacenamiento (por ejemplo: ONTAP FlexVol, Element Volume, ruta Cloud Volumes Service). El `-f` argumento es necesario para especificar la ruta al archivo PVC.

```

tridentctl import volume <backendName> <volumeName> -f <path-to-pvc-
file>

```

## Ejemplos

Revise los siguientes ejemplos de importación de volúmenes para los controladores compatibles.

### NAS de ONTAP y NAS FlexGroup de ONTAP

Trident admite la importación de volúmenes mediante `ontap-nas` los controladores y `ontap-nas-flexgroup`



- La `ontap-nas-economy` el controlador no puede importar y gestionar qtrees.
- La `ontap-nas` y `ontap-nas-flexgroup` las controladoras no permiten nombres de volúmenes duplicados.

Cada volumen creado con `ontap-nas` Driver es una FlexVol en el clúster de ONTAP. Importación de FlexVols con `ontap-nas` el controlador funciona igual. Una FlexVol que ya existe en un clúster de ONTAP se puede importar como `ontap-nas` RVP. Del mismo modo, los volúmenes FlexGroup se pueden importar del mismo modo `ontap-nas-flexgroup` EVs.

### Ejemplos de NAS de ONTAP

A continuación, se muestra un ejemplo de un volumen gestionado y una importación de volumen no gestionada.

## Volumen gestionado

En el ejemplo siguiente se importa un volumen llamado `managed_volume` en un backend llamado `ontap_nas`:

```
tridentctl import volume ontap_nas managed_volume -f <path-to-pvc-file>
```

PROTOCOL	NAME	BACKEND UUID	SIZE	STATE	STORAGE CLASS	MANAGED
file	pvc-bf5ad463-afbb-11e9-8d9f-5254004dfdb7	c5a6f6a4-b052-423b-80d4-8fb491a14a22	1.0 GiB	online	standard	true

## Volumen no gestionado

Cuando se utiliza `--no-manage` el argumento, Trident no cambia el nombre del volumen.

El siguiente ejemplo importa `unmanaged_volume` en la `ontap_nas` backend:

```
tridentctl import volume nas_blog unmanaged_volume -f <path-to-pvc-file> --no-manage
```

PROTOCOL	NAME	BACKEND UUID	SIZE	STATE	STORAGE CLASS	MANAGED
file	pvc-df07d542-afbc-11e9-8d9f-5254004dfdb7	c5a6f6a4-b052-423b-80d4-8fb491a14a22	1.0 GiB	online	standard	false

## SAN de ONTAP

Trident admite la importación de volúmenes mediante `ontap-san` los controladores y `ontap-san-economy`

Trident puede importar volúmenes flexibles de SAN de ONTAP que contengan una única LUN. Esto es coherente con `ontap-san` el controlador, que crea una FlexVol para cada RVP y una LUN dentro de la FlexVol. Trident importa el FlexVol y lo asocia con la definición de PVC.

## Ejemplos de SAN de ONTAP

A continuación, se muestra un ejemplo de un volumen gestionado y una importación de volumen no gestionada.

### Volumen gestionado

Para los volúmenes gestionados, Trident cambia el nombre de FlexVol al `pvc-<uuid>` formato y a la LUN dentro de FlexVol a `lun0`.

El siguiente ejemplo importa el `ontap-san-managed` FlexVol que está presente en el `ontap_san_default` backend:

```
tridentctl import volume ontapsan_san_default ontap-san-managed -f pvc-
basic-import.yaml -n trident -d
```

PROTOCOL	NAME	BACKEND UUID	SIZE	STATE	STORAGE CLASS	MANAGED
block	pvc-d6ee4f54-4e40-4454-92fd-d00fc228d74a	cd394786-ddd5-4470-adc3-10c5ce4ca757	20 MiB	online	basic	true

### Volumen no gestionado

El siguiente ejemplo importa `unmanaged_example_volume` en la `ontap_san` backend:

```
tridentctl import volume -n trident san_blog unmanaged_example_volume
-f pvc-import.yaml --no-manage
```

PROTOCOL	NAME	BACKEND UUID	SIZE	STATE	STORAGE CLASS	MANAGED
block	pvc-1fc999c9-ce8c-459c-82e4-ed4380a4b228	e3275890-7d80-4af6-90cc-c7a0759f555a	1.0 GiB	online	san-blog	false

Si tiene LUN asignadas a iGroups que comparten un IQN con un IQN de nodo de Kubernetes, como se muestra en el ejemplo siguiente, recibirá el error: `LUN already mapped to initiator(s) in this group`. Deberá quitar el iniciador o desasignar la LUN para importar el volumen.

Vserver	Igroup	Protocol	OS Type	Initiators
svm0	k8s-nodename.example.com-fe5d36f2-cded-4f38-9eb0-c7719fc2f9f3	iscsi	linux	iqn.1994-05.com.redhat:4c2e1cf35e0
svm0	unmanaged-example-igroup	mixed	linux	iqn.1994-05.com.redhat:4c2e1cf35e0

**Elemento**

Trident admite el software NetApp Element y la importación de volúmenes NetApp HCI mediante `solidfire-san` el controlador.



El controlador Element admite los nombres de volúmenes duplicados. Sin embargo, Trident devuelve un error si hay nombres de volúmenes duplicados. Como solución alternativa, clone el volumen, proporcione un nombre de volumen único e importe el volumen clonado.

**Ejemplo de elemento**

El siguiente ejemplo importa un `element-managed` volumen en el back-end `element_default`.

```
tridentctl import volume element_default element-managed -f pvc-basic-import.yaml -n trident -d
```

PROTOCOL	NAME	BACKEND UUID	SIZE	STORAGE CLASS	STATE	MANAGED
block	pvc-970ce1ca-2096-4ecd-8545-ac7edc24a8fe	d3ba047a-ea0b-43f9-9c42-e38e58301c49	10 GiB	basic-element	online	true

**Google Cloud Platform**

Trident admite la importación de volúmenes utilizando `gcp-cvs` el controlador.



Para importar un volumen respaldado por NetApp Cloud Volumes Service en Google Cloud Platform, identifique el volumen según la ruta de volumen. La ruta del volumen es la parte de la ruta de exportación del volumen después del `:/`. Por ejemplo, si la ruta de exportación es `10.0.0.1:/adroit-jolly-swift`, la ruta de volumen es `adroit-jolly-swift`.

**Ejemplo de Google Cloud Platform**

El siguiente ejemplo importa a. gcp-cvs volumen en el back-end gcpcvs\_YEppr con la ruta del volumen de adroit-jolly-swift.

```
tridentctl import volume gcpcvs_YEppr adroit-jolly-swift -f <path-to-pvc-
file> -n trident

+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  | MANAGED |
+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-a46ccab7-44aa-4433-94b1-e47fc8c0fa55 | 93 GiB | gcp-storage   | file
| e1a6e65b-299e-4568-ad05-4f0a105c888f | online | true         |
+-----+-----+-----+
+-----+-----+-----+-----+
```

### Azure NetApp Files

Trident admite la importación de volúmenes utilizando azure-netapp-files el controlador.



Para importar un volumen de Azure NetApp Files, identifique el volumen por su ruta de volumen. La ruta del volumen es la parte de la ruta de exportación del volumen después del :/. Por ejemplo, si la ruta de montaje es 10.0.0.2:/importvoll1, la ruta de volumen es importvoll1.

### Ejemplo de Azure NetApp Files

El siguiente ejemplo importa un azure-netapp-files volumen en el back-end azurenetappfiles\_40517 con la ruta del volumen importvoll1.

```
tridentctl import volume azurenetappfiles_40517 importvoll1 -f <path-to-
pvc-file> -n trident

+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  | MANAGED |
+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-0ee95d60-fd5c-448d-b505-b72901b3a4ab | 100 GiB | anf-storage   |
file      | 1c01274f-d94b-44a3-98a3-04c953c9a51e | online | true         |
+-----+-----+-----+
+-----+-----+-----+-----+
```

## Personalizar nombres y etiquetas de volúmenes

Con Trident puede asignar nombres y etiquetas significativos a los volúmenes que cree. Esto le ayuda a identificar y asignar fácilmente volúmenes a sus respectivos recursos de Kubernetes (RVP). También puede definir plantillas en el nivel de back-end para crear nombres de volúmenes y etiquetas personalizadas; los volúmenes que cree, importe o clone respetarán las plantillas.

### Antes de empezar

Nombres de volumen y etiquetas personalizables admiten:

1. Operaciones de creación, importación y clonado de volúmenes.
2. En el caso del controlador económico ontap-nas, solo el nombre del volumen Qtree debe cumplir con la plantilla de nombre.
3. En el caso del controlador ontap-san-economy, solo el nombre de la LUN cumple con la plantilla de nombre.

### Limitaciones

1. Los nombres de volumen personalizables solo son compatibles con los controladores locales de ONTAP.
2. Los nombres de volúmenes personalizables no se aplican a los volúmenes existentes.

### Comportamientos clave de los nombres de volúmenes personalizables

1. Si se produce un fallo debido a una sintaxis no válida en una plantilla de nombre, se produce un error en la creación del backend. Sin embargo, si la aplicación de plantilla falla, el volumen se nombrará de acuerdo con la convención de nomenclatura existente.
2. El prefijo de almacenamiento no es aplicable cuando se asigna el nombre de un volumen mediante una plantilla de nombres en la configuración back-end. Cualquier valor de prefijo deseado se puede agregar directamente a la plantilla.

### Ejemplos de configuración de backend con plantilla de nombre y etiquetas

Las plantillas de nombre personalizado se pueden definir en el nivel raíz y/o de grupo.



## Ejemplo de nivel raíz

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nfs-backend",
  "managementLIF": "<ip address>",
  "svm": "svm0",
  "username": "<admin>",
  "password": "<password>",
  "defaults": {
    "nameTemplate":
      "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.volume.Requ
      estName}}"
  },
  "labels": {"cluster": "ClusterA", "PVC":
    "{{.volume.Namespace}}_{{.volume.RequestName}}"
  }
}
```

## Ejemplo de nivel de pool

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nfs-backend",
  "managementLIF": "<ip address>",
  "svm": "svm0",
  "username": "<admin>",
  "password": "<password>",
  "useREST": true,
  "storage": [
    {
      "labels":{"labelname":"label1", "name": "{{ .volume.Name }}"},
      "defaults":
      {
        "nameTemplate": "pool01_{{ .volume.Name }}_{{ .labels.cluster
}}_{{ .volume.Namespace }}_{{ .volume.RequestName }}"
      }
    },
    {
      "labels":{"cluster":"label2", "name": "{{ .volume.Name }}"},
      "defaults":
      {
        "nameTemplate": "pool02_{{ .volume.Name }}_{{ .labels.cluster
}}_{{ .volume.Namespace }}_{{ .volume.RequestName }}"
      }
    }
  ]
}
```

## Ejemplos de plantillas de nombres

### Ejemplo 1:

```
"nameTemplate": "{{ .config.StoragePrefix }}_{{ .volume.Name }}_{{
.config.BackendName }}"
```

### Ejemplo 2:

```
"nameTemplate": "pool_{{ .config.StoragePrefix }}_{{ .volume.Name }}_{{
slice .volume.RequestName 1 5 }}"
```

## Puntos que considerar

1. En el caso de las importaciones de volúmenes, las etiquetas se actualizan solo si el volumen existente tiene etiquetas en un formato específico. Por ejemplo `{"provisioning":{"Cluster":"ClusterA", "PVC": "pvcname"}}:.`
2. En el caso de importaciones de volúmenes gestionados, el nombre del volumen sigue a la plantilla de nombres definida en el nivel raíz en la definición de backend.
3. Trident no admite el uso de un operador de segmentos con el prefijo de almacenamiento.
4. Si las plantillas no dan como resultado nombres de volúmenes únicos, Trident añadirá algunos caracteres aleatorios para crear nombres de volúmenes únicos.
5. Si el nombre personalizado para un volumen económico NAS supera los 64 caracteres de longitud, Trident asignará un nombre a los volúmenes de acuerdo con la convención de nomenclatura existente. Para el resto de los controladores ONTAP, si el nombre del volumen supera el límite de nombre, se produce un error en el proceso de creación de volúmenes.

## Comparta un volumen NFS en espacios de nombres

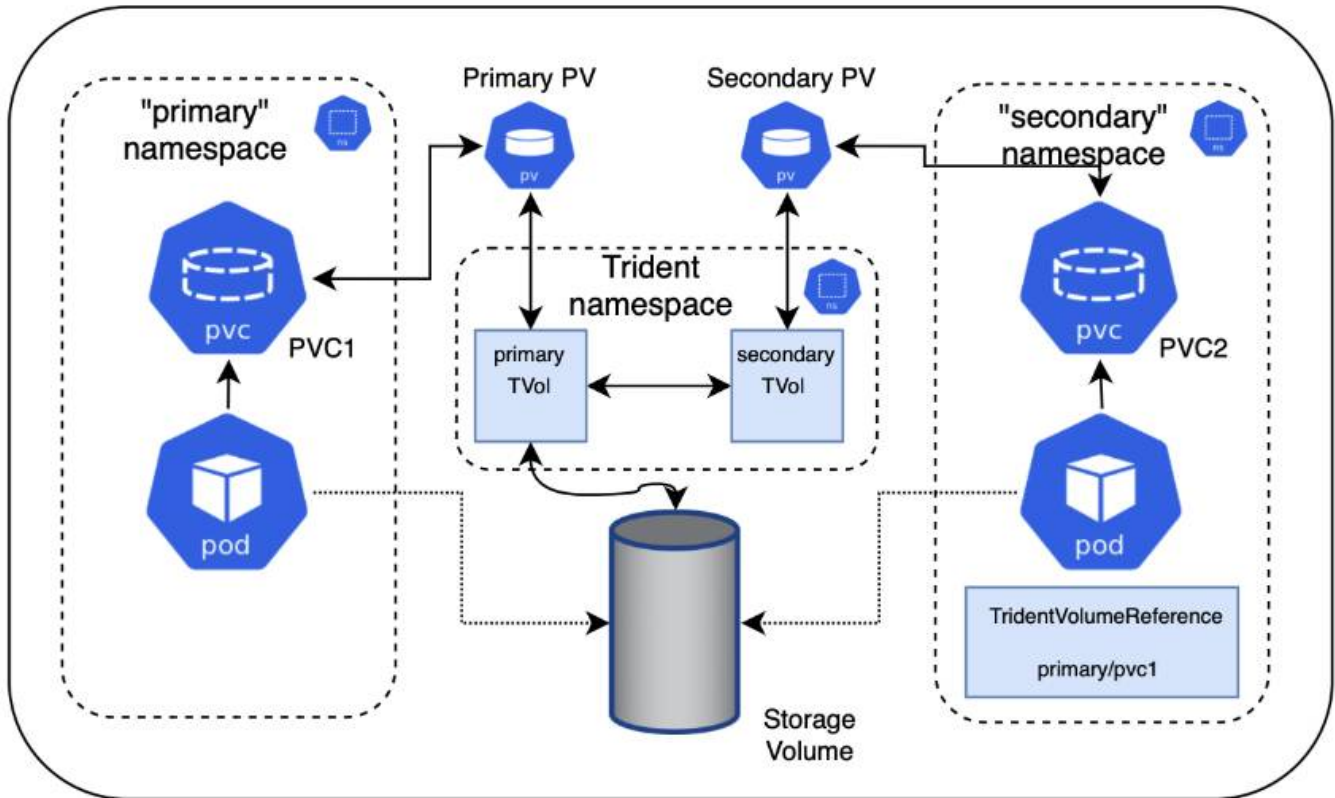
Con Trident, es posible crear un volumen en un espacio de nombres primario y compartirlo en uno o más espacios de nombres secundarios.

### Funciones

TridentVolumeReference CR permite compartir de forma segura los volúmenes NFS ReadWriteMany (RWX) en uno o varios espacios de nombres de Kubernetes. Esta solución nativa de Kubernetes tiene las siguientes ventajas:

- Varios niveles de control de acceso para garantizar la seguridad
- Funciona con todos los controladores de volúmenes NFS de Trident
- No depende de `tridentctl` ni de ninguna otra función de Kubernetes no nativa

Este diagrama ilustra el uso compartido de volúmenes de NFS en dos espacios de nombres de Kubernetes.



## Inicio rápido

Puede configurar el uso compartido del volumen NFS en unos pocos pasos.

1

### Configure la RVP de origen para compartir el volumen

El propietario del espacio de nombres de origen concede permiso para acceder a los datos de la RVP de origen.

2

### Conceder permiso para crear una CR en el espacio de nombres de destino

El administrador del clúster concede permiso al propietario del espacio de nombres de destino para crear el sistema TridentVolumeReference CR.

3

### Cree TridentVolumeReference en el espacio de nombres de destino

El propietario del espacio de nombres de destino crea el TridentVolumeReference CR para hacer referencia al PVC de origen.

4

### Cree el PVC subordinado en el espacio de nombres de destino

El propietario del espacio de nombres de destino crea el PVC subordinado para utilizar el origen de datos desde el PVC de origen.

## Configurar los espacios de nombres de origen y destino

Para garantizar la seguridad, el uso compartido entre espacios de nombres requiere la colaboración y la acción del propietario del espacio de nombres de origen, el administrador de clúster y el propietario del espacio de nombres de destino. La función de usuario se designa en cada paso.

### Pasos

1. **Propietario del espacio de nombres de origen:** cree el PVC (`pvc1`) en el espacio de nombres de origen que concede permiso para compartir con el espacio de nombres de destino (`namespace2`) utilizando el `shareToNamespace` anotación.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc1
  namespace: namespace1
  annotations:
    trident.netapp.io/shareToNamespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi
```

Trident crea el VP y su volumen de almacenamiento NFS de back-end.



- Puede compartir el PVC en varios espacios de nombres utilizando una lista delimitada por comas. Por ejemplo: `trident.netapp.io/shareToNamespace: namespace2, namespace3, namespace4`.
- Puede compartir todos los espacios de nombres mediante `*`. Por ejemplo: `trident.netapp.io/shareToNamespace: *`
- Puede actualizar la RVP para incluir el `shareToNamespace` anotación en cualquier momento.

2. **Administrador de clúster:** cree la función personalizada y kubeconfig para conceder permiso al propietario del espacio de nombres de destino para crear el sistema `TridentVolumeReference` CR en el espacio de nombres de destino.
3. **Propietario del espacio de nombres de destino:** cree un sistema `TridentVolumeReference` CR en el espacio de nombres de destino que haga referencia al espacio de nombres de origen `pvc1`.

```

apiVersion: trident.netapp.io/v1
kind: TridentVolumeReference
metadata:
  name: my-first-tvr
  namespace: namespace2
spec:
  pvcName: pvc1
  pvcNamespace: namespace1

```

4. **Propietario del espacio de nombres de destino:** cree un PVC (`pvc2`) en el espacio de nombres de destino (`namespace2`) utilizando el `shareFromPVC` Anotación para designar el PVC de origen.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  annotations:
    trident.netapp.io/shareFromPVC: namespace1/pvc1
  name: pvc2
  namespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi

```



El tamaño del PVC de destino debe ser menor o igual que el PVC de origen.

## Resultados

Trident lee la `shareFromPVC` anotación en la RVP de destino y crea el VP de destino como volumen subordinado sin ningún recurso de almacenamiento propio que apunte al VP de origen y comparta el recurso de almacenamiento VP de origen. La RVP y el VP de destino aparecen vinculados como normales.

## Elimine un volumen compartido

Es posible eliminar un volumen que se comparte en varios espacios de nombres. Trident eliminará el acceso al volumen en el espacio de nombres de origen y mantendrá el acceso a otros espacios de nombres que compartan el volumen. Cuando se eliminan todos los espacios de nombres que hacen referencia al volumen, Trident lo elimina.

## Uso `tridentctl get` para consultar volúmenes subordinados

Con el `tridentctl` puede ejecutar la `get` comando para obtener volúmenes subordinados. Para obtener más información, consulte el enlace: [./trident-reference/tridentctl.html](#) [`tridentctl` comandos y opciones].

Usage:

```
tridentctl get [option]
```

Indicadores:

- `-h, --help`: Ayuda para volúmenes.
- `--parentOfSubordinate string`: Limite la consulta al volumen de origen subordinado.
- `--subordinateOf string`: Limite la consulta a las subordinadas del volumen.

## Limitaciones

- Trident no puede evitar que los espacios de nombres de destino se escriban en el volumen compartido. Se debe usar el bloqueo de archivos u otros procesos para evitar la sobrescritura de datos de volúmenes compartidos.
- No puede revocar el acceso al PVC de origen quitando el `shareToNamespace` o `shareFromNamespace` anotaciones o eliminar `TridentVolumeReference` CR. Para revocar el acceso, debe eliminar el PVC subordinado.
- Las snapshots, los clones y el mirroring no son posibles en los volúmenes subordinados.

## Si quiere más información

Para obtener más información sobre el acceso de volúmenes entre espacios de nombres:

- Visite ["Uso compartido de volúmenes entre espacios de nombres: Dé la bienvenida al acceso al volumen entre espacios de nombres"](#).
- Vea la demostración en ["NetAppTV"](#).

## Utilice Topología CSI

Trident puede crear y conectar volúmenes de forma selectiva a los nodos presentes en un clúster de Kubernetes utilizando el ["Función de topología CSI"](#).

### Descripción general

Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. En la actualidad, los proveedores de cloud permiten a los administradores de Kubernetes generar nodos basados en zonas. Los nodos se pueden ubicar en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura multizona, Trident utiliza la topología CSI.



Obtenga más información sobre la característica de topología CSI ["aquí"](#).

Kubernetes ofrece dos modos de enlace de volúmenes únicos:

- Con `VolumeBindingMode` Establecer en `Immediate`, Trident crea el volumen sin reconocimiento de topología. La vinculación de volúmenes y el aprovisionamiento dinámico se manejan cuando se crea la RVP. Este es el valor por defecto `VolumeBindingMode` y es adecuado para clusters que no aplican restricciones de topología. Los volúmenes persistentes se crean sin depender de los requisitos de

programación del pod solicitante.

- Con `VolumeBindingMode` establezca en `WaitForFirstConsumer`, La creación y enlace de un volumen persistente para una RVP se retrasa hasta que se programa y crea un pod que usa la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología.



La `WaitForFirstConsumer` el modo de encuadernación no requiere etiquetas de topología. Esto se puede utilizar independientemente de la característica de topología CSI.

### Lo que necesitará

Para utilizar la topología CSI, necesita lo siguiente:

- Un clúster de Kubernetes que ejecuta un ["Compatible con la versión de Kubernetes"](#)

```
kubectl version
Client Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedeaafd99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:50:19Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
Server Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedeaafd99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:41:49Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
```

- Los nodos del clúster deben tener etiquetas que introduzcan el reconocimiento de topología (`topology.kubernetes.io/region`y `topology.kubernetes.io/zone`). Estas etiquetas **deben estar presentes en los nodos del cluster** antes de instalar Trident para que Trident tenga en cuenta la topología.



```
kubectl get nodes -o=jsonpath='{range .items[*]}[.metadata.name],
{.metadata.labels}]{"\n"}{end}' | grep --color "topology.kubernetes.io"
[node1,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kuber-
netes.io/arch":"amd64","kubernetes.io/hostname":"node1","kubernetes.io/
os":"linux","node-
role.kubernetes.io/master":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-a"}]
[node2,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kuber-
netes.io/arch":"amd64","kubernetes.io/hostname":"node2","kubernetes.io/
os":"linux","node-
role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-b"}]
[node3,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kuber-
netes.io/arch":"amd64","kubernetes.io/hostname":"node3","kubernetes.io/
os":"linux","node-
role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-c"}]
```

### Paso 1: Cree un backend con detección de topología

Los back-ends de almacenamiento de Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad. Cada backend puede llevar un bloque opcional `supportedTopologies` que representa una lista de zonas y regiones soportadas. En el caso de `StorageClasses` que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida.

A continuación se muestra un ejemplo de definición de backend:

## YAML

```
---
version: 1
storageDriverName: ontap-san
backendName: san-backend-us-east1
managementLIF: 192.168.27.5
svm: iscsi_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-a
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-b
```

## JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "san-backend-us-east1",
  "managementLIF": "192.168.27.5",
  "svm": "iscsi_svm",
  "username": "admin",
  "password": "password",
  "supportedTopologies": [
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-a"},
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-b"}
  ]
}
```



`supportedTopologies` se utiliza para proporcionar una lista de regiones y zonas por backend. Estas regiones y zonas representan la lista de valores permitidos que se pueden proporcionar en un `StorageClass`. Para `StorageClasses` que contienen un subconjunto de las regiones y zonas proporcionadas en un backend, Trident crea un volumen en el backend.

Puede definir `supportedTopologies` por pool de almacenamiento también. Consulte el siguiente ejemplo:

```

---
version: 1
storageDriverName: ontap-nas
backendName: nas-backend-us-central1
managementLIF: 172.16.238.5
svm: nfs_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-a
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-b
storage:
- labels:
    workload: production
  supportedTopologies:
  - topology.kubernetes.io/region: us-central1
    topology.kubernetes.io/zone: us-central1-a
- labels:
    workload: dev
  supportedTopologies:
  - topology.kubernetes.io/region: us-central1
    topology.kubernetes.io/zone: us-central1-b

```

En este ejemplo, la `region` y `zone` las etiquetas indican la ubicación del pool de almacenamiento. `topology.kubernetes.io/region` y `topology.kubernetes.io/zone` dicte desde donde se pueden consumir los pools de almacenamiento.

## Paso 2: Defina las clases de almacenamiento que tienen en cuenta la topología

En función de las etiquetas de topología que se proporcionan a los nodos del clúster, se puede definir `StorageClase` para que contenga información de topología. Esto determinará los pools de almacenamiento que sirven como candidatos para las solicitudes de RVP y el subconjunto de nodos que pueden usar los volúmenes aprovisionados mediante Trident.

Consulte el siguiente ejemplo:

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
name: netapp-san-us-east1
provisioner: csi.trident.netapp.io
volumeBindingMode: WaitForFirstConsumer
allowedTopologies:
- matchLabelExpressions:
- key: topology.kubernetes.io/zone
  values:
  - us-east1-a
  - us-east1-b
- key: topology.kubernetes.io/region
  values:
  - us-east1
parameters:
  fsType: "ext4"

```

En la definición de StorageClass proporcionada anteriormente, `volumeBindingMode` se establece en `WaitForFirstConsumer`. Las RVP solicitadas con este tipo de almacenamiento no se verán en cuestión hasta que se mencionan en un pod. Y, `allowedTopologies` proporciona las zonas y la región que se van a utilizar. `netapp-san-us-east1`StorageClass` crea RVP en el ``san-backend-us-east1` backend definido anteriormente.

### Paso 3: Cree y utilice un PVC

Con el clase de almacenamiento creado y asignado a un back-end, ahora puede crear RVP.

Vea el ejemplo `spec` a continuación:

```

---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
name: pvc-san
spec:
accessModes:
  - ReadWriteOnce
resources:
  requests:
    storage: 300Mi
storageClassName: netapp-san-us-east1

```

La creación de una RVP con este manifiesto daría como resultado lo siguiente:

```

kubect1 create -f pvc.yaml
persistentvolumeclaim/pvc-san created
kubect1 get pvc
NAME          STATUS      VOLUME      CAPACITY   ACCESS MODES   STORAGECLASS
AGE
pvc-san      Pending
2s
kubect1 describe pvc
Name:          pvc-san
Namespace:     default
StorageClass:  netapp-san-us-east1
Status:        Pending
Volume:
Labels:        <none>
Annotations:   <none>
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:    Filesystem
Mounted By:    <none>
Events:
  Type      Reason              Age   From
  ----      -
  Normal    WaitForFirstConsumer 6s    persistentvolume-controller
waiting
for first consumer to be created before binding

```

Para que Trident cree un volumen y lo enlace a la RVP, use la RVP en un pod. Consulte el siguiente ejemplo:

```

apiVersion: v1
kind: Pod
metadata:
  name: app-pod-1
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: topology.kubernetes.io/region
                operator: In
                values:
                  - us-east1
            preferredDuringSchedulingIgnoredDuringExecution:
              - weight: 1
                preference:
                  matchExpressions:
                    - key: topology.kubernetes.io/zone
                      operator: In
                      values:
                        - us-east1-a
                        - us-east1-b
      securityContext:
        runAsUser: 1000
        runAsGroup: 3000
        fsGroup: 2000
    volumes:
      - name: voll
        persistentVolumeClaim:
          claimName: pvc-san
    containers:
      - name: sec-ctx-demo
        image: busybox
        command: [ "sh", "-c", "sleep 1h" ]
        volumeMounts:
          - name: voll
            mountPath: /data/demo
        securityContext:
          allowPrivilegeEscalation: false

```

Este podSpec indica a Kubernetes que programe el pod de los nodos presentes en el us-east1 region y elija de cualquier nodo que esté presente en el us-east1-a o. us-east1-b zonas.

Consulte la siguiente salida:

```
kubectl get pods -o wide
NAME          READY   STATUS    RESTARTS   AGE   IP              NODE
NOMINATED NODE READINESS GATES
app-pod-1    1/1     Running   0          19s   192.168.25.131  node2
<none>      <none>
kubectl get pvc -o wide
NAME          STATUS   VOLUME                                     CAPACITY
ACCESS MODES STORAGECLASS          AGE   VOLUMEMODE
pvc-san      Bound   pvc-ecb1e1a0-840c-463b-8b65-b3d033e2e62b 300Mi
RWO          netapp-san-us-east1  48s   Filesystem
```

### Actualice los back-ends que se incluirán `supportedTopologies`

Se pueden actualizar los back-ends preexistentes para incluir una lista de `supportedTopologies` uso `tridentctl backend update`. Esto no afectará a los volúmenes que ya se han aprovisionado, y sólo se utilizarán en las siguientes CVP.

### Obtenga más información

- ["Gestione recursos para contenedores"](#)
- ["Selector de nodos"](#)
- ["Afinidad y anti-afinidad"](#)
- ["Tolerancias y taints"](#)

## Trabajar con instantáneas

Las snapshots de volúmenes de Kubernetes de Persistent Volumes (VP) permiten copias puntuales de volúmenes. Es posible crear una copia Snapshot de un volumen creado con Trident, importar una copia de Snapshot creada fuera de Trident, crear un volumen nuevo a partir de una copia de Snapshot existente y recuperar datos de volumen de copias de Snapshot.

### Descripción general

Admite copias de Snapshot de volumen `ontap-nas`, `ontap-nas-flexgroup`, `ontap-san`, `ontap-san-economy`, `solidfire-san`, `gcp-cvs`, y `azure-netapp-files` de windows

### Antes de empezar

Debe tener un controlador de instantánea externo y definiciones de recursos personalizados (CRD) para trabajar con instantáneas. Esta es la responsabilidad del orquestador de Kubernetes (por ejemplo: Kubeadm, GKE, OpenShift).

Si su distribución de Kubernetes no incluye el controlador de instantáneas ni los CRD, consulte [Implemente una controladora Snapshot de volumen](#).



No cree una controladora Snapshot si crea instantáneas de volumen bajo demanda en un entorno de GKE. GKE utiliza un controlador de instantáneas oculto integrado.

## Cree una copia de Snapshot de volumen

### Pasos

1. Cree un `VolumeSnapshotClass`. Para obtener más información, consulte "[VolumeSnapshotClass](#)".
  - Los `driver` puntos al controlador CSI de Trident.
  - `deletionPolicy` puede ser `Delete` o `Retain`. Cuando se establece en `Retain`, la instantánea física subyacente en el clúster de almacenamiento se conserva incluso cuando `VolumeSnapshot` el objeto se ha eliminado.

### Ejemplo

```
cat snap-sc.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

2. Crear una instantánea de una RVP existente.

### Ejemplos

- En este ejemplo, se crea una copia Snapshot de una RVP existente.

```
cat snap.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: pvcl-snap
spec:
  volumeSnapshotClassName: csi-snapclass
  source:
    persistentVolumeClaimName: pvcl
```

- En este ejemplo, se crea un objeto Snapshot de volumen para una RVP denominada `pvcl` y el nombre de la copia de snapshot se establece en `pvcl-snap`. Un `VolumeSnapshot` es análogo a un `PVC` y está asociado a un `VolumeSnapshotContent` objeto que representa la instantánea real.

```
kubectl create -f snap.yaml
volumesnapshot.snapshot.storage.k8s.io/pvcl-snap created

kubectl get volumesnapshots
NAME                AGE
pvcl-snap           50s
```



- Puede identificar el `VolumeSnapshotContent` objeto para `pvc1-snap` `VolumeSnapshot`, describiéndolo. La `Snapshot Content Name` Identifica el objeto `VolumeSnapshotContent` que sirve esta snapshot. La `Ready To Use` El parámetro indica que la snapshot se puede usar para crear una nueva RVP.

```
kubectl describe volumesnapshots pvc1-snap
Name:          pvc1-snap
Namespace:     default
.
.
.
Spec:
  Snapshot Class Name:    pvc1-snap
  Snapshot Content Name:  snapcontent-e8d8a0ca-9826-11e9-9807-
525400f3f660
  Source:
    API Group:
    Kind:       PersistentVolumeClaim
    Name:       pvc1
Status:
  Creation Time:  2019-06-26T15:27:29Z
  Ready To Use:  true
  Restore Size:  3Gi
.
.
```

## Cree una RVP a partir de una snapshot de volumen

Puede utilizar `dataSource` Para crear una RVP con una Snapshot de volumen llamada `<pvc-name>` como la fuente de los datos. Una vez creada la RVP, se puede conectar a un pod y utilizarla como cualquier otro PVC.



La RVP se creará en el mismo back-end que el volumen de origen. Consulte "[KB: La creación de una RVP a partir de una snapshot de RVP de Trident no se puede crear en un back-end alternativo](#)".

En el siguiente ejemplo se crea la RVP con `pvc1-snap` como origen de datos.

```

cat pvc-from-snap.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-from-snap
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: golden
  resources:
    requests:
      storage: 3Gi
  dataSource:
    name: pvcl-snap
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io

```

## Importe una copia de Snapshot de volumen

Trident admite "[Proceso de snapshot aprovisionado previamente de Kubernetes](#)" para permitir que el administrador de clúster cree `VolumeSnapshotContent` un objeto e importe copias de Snapshot creadas fuera de Trident.

### Antes de empezar

Trident debe haber creado o importado el volumen principal de la snapshot.

### Pasos

1. **Cluster admin:** Crear un `VolumeSnapshotContent` objeto que haga referencia a la instantánea backend. De esta forma, se inicia el flujo de trabajo Snapshot en Trident.
  - Especifique el nombre de la instantánea de backend en annotations como `trident.netapp.io/internalSnapshotName: <"backend-snapshot-name">`.
  - Especifique `<name-of-parent-volume-in-trident>/<volume-snapshot-content-name>` en `snapshotHandle`. Esta es la única información proporcionada a Trident por el Snapshotter externo en la `ListSnapshots` llamada.



La `<volumeSnapshotContentName>` No siempre se puede coincidir con el nombre de instantánea de backend debido a restricciones de nomenclatura de CR.

### Ejemplo

En el siguiente ejemplo se crea un `VolumeSnapshotContent` objeto que hace referencia a la instantánea backend `snap-01`.

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotContent
metadata:
  name: import-snap-content
  annotations:
    trident.netapp.io/internalSnapshotName: "snap-01" # This is the
name of the snapshot on the backend
spec:
  deletionPolicy: Retain
  driver: csi.trident.netapp.io
  source:
    snapshotHandle: pvc-f71223b5-23b9-4235-bbfe-e269ac7b84b0/import-
snap-content # <import PV name or source PV name>/<volume-snapshot-
content-name>

```

2. **Administrador del clúster:** Crear el VolumeSnapshot CR que hace referencia al VolumeSnapshotContent objeto. Esto solicita acceso para utilizar el VolumeSnapshot en un espacio de nombres determinado.

### Ejemplo

En el siguiente ejemplo se crea un VolumeSnapshot CR con nombre import-snap que hace referencia a la VolumeSnapshotContent nombre import-snap-content.

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: import-snap
spec:
  # volumeSnapshotClassName: csi-snapclass (not required for pre-
provisioned or imported snapshots)
  source:
    volumeSnapshotContentName: import-snap-content

```

3. **Procesamiento interno (no se requiere acción):** El Snapshotter externo reconoce el recién creado VolumeSnapshotContent y ejecuta la ListSnapshots llamada. Trident crea el TridentSnapshot.
- El dispositivo de instantáneas externo establece el VolumeSnapshotContent para readyToUse y la VolumeSnapshot para true.
  - Trident vuelve readyToUse=true.
4. **Cualquier usuario:** Crear a PersistentVolumeClaim para hacer referencia al nuevo VolumeSnapshot, donde spec.dataSource (o. spec.dataSourceRef) nombre es el VolumeSnapshot nombre.

### Ejemplo

En el siguiente ejemplo se crea una RVP que hace referencia al VolumeSnapshot nombre import-

snap.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-from-snap
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: simple-sc
  resources:
    requests:
      storage: 1Gi
  dataSource:
    name: import-snap
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io
```

### Recuperar datos de volumen mediante copias Snapshot

El directorio de snapshots está oculto de forma predeterminada para facilitar la máxima compatibilidad de los volúmenes aprovisionados con el `ontap-nas` y `ontap-nas-economy` de windows. Habilite el `.snapshot` directorio para recuperar datos de snapshots directamente.

Use la interfaz de línea de comandos de ONTAP para restaurar un volumen en un estado registrado en una snapshot anterior.

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot
vol3_snap_archive
```



Quando se restaura una copia Snapshot, se sobrescribe la configuración de volúmenes existente. Se pierden los cambios que se hagan en los datos del volumen después de crear la copia Snapshot.

### Eliminar un VP con snapshots asociadas

Quando se elimina un volumen persistente con instantáneas asociadas, el volumen Trident correspondiente se actualiza a un “estado de eliminación”. Quite las copias de Snapshot de volumen para eliminar el volumen de Trident.

### Implemente una controladora Snapshot de volumen

Si su distribución de Kubernetes no incluye el controlador de snapshots y los CRD, puede implementarlos de la siguiente manera.

#### Pasos

1. Crear CRD de snapshot de volumen.

```
cat snapshot-setup.sh
#!/bin/bash
# Create volume snapshot CRDs
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
1
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

## 2. Cree la controladora Snapshot.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-
controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-
controller/setup-snapshot-controller.yaml
```



Si es necesario, abra `deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml` y actualícelo namespace en el espacio de nombres.

### Enlaces relacionados

- ["Copias de Snapshot de volumen"](#)
- ["VolumeSnapshotClass"](#)

# Gestione y supervise Trident

## Actualice Trident

### Actualice Trident

A partir de la versión 24,02, Trident sigue una cadencia de lanzamiento de cuatro meses, entregando tres versiones principales cada año. Cada nueva versión se basa en versiones anteriores y proporciona nuevas funciones, mejoras de rendimiento, correcciones de errores y mejoras. Le animamos a actualizar al menos una vez al año para aprovechar las nuevas funciones de Trident.

### Consideraciones antes de la actualización

Al actualizar a la versión más reciente de Trident, tenga en cuenta lo siguiente:

- Solo debe haber una instancia de Trident instalada en todos los espacios de nombres de un clúster de Kubernetes determinado.
- Trident 23,07 y versiones posteriores requieren v1 copias Snapshot de volumen y ya no admite instantáneas alfa o beta.
- Si ha creado Cloud Volumes Service para Google Cloud en "[Tipo de servicio CVS](#)", debe actualizar la configuración de backend para utilizar el `standardsw` nivel de servicio OR `zoneredundantstandardsw` al actualizar desde Trident 23,01. Si no se actualiza el `serviceLevel` en el backend, se podrían producir errores en los volúmenes. Consulte "[Muestras de tipo de servicio CVS](#)" para obtener más información.
- Al actualizar, es importante que proporcione `parameter.fsType` el `StorageClasses` que utiliza Trident. Puede eliminar y volver a crear `StorageClasses` sin interrumpir los volúmenes existentes anteriores.
  - 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 Trident siguen una convención de nomenclatura basada en fechas `YY.MM`, donde "YY" es los dos últimos dígitos del año y "MM" es el mes. Las versiones de DOT siguen `YY.MM.X` una 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 directamente de 23,04 (o cualquier versión de 23,04 puntos) a 24,06.
- Si va a actualizar desde una versión fuera de la ventana de cuatro versiones, realice una actualización de varios pasos. Utilice las instrucciones de actualización de la "[versión anterior](#)" que va a actualizar para actualizar a la versión más reciente que se ajuste a la ventana de cuatro versiones. Por ejemplo, si utiliza 22,01 y desea actualizar a la versión 24,06:

- a. Primera actualización de 22,07 a 23,04.
- b. A continuación, actualice de 23,04 a 24,06.



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 la ["Detalles del problema en GitHub"](#).

## Paso 2: Determine el método de instalación original

Para determinar qué versión utilizaba para instalar originalmente Trident:

1. Uso `kubectl get pods -n trident` para examinar los pods.
  - Si no hay ningún pod de operador, se instaló Trident utilizando `tridentctl`.
  - Si hay un pod de operador, se instaló Trident usando el operador Trident manualmente o usando Helm.
2. Si hay un pod de operador, utilice `kubectl describe torc` para determinar si Trident se instaló con Helm.
  - Si hay una etiqueta Helm, Trident se instaló usando Helm.
  - Si no hay ninguna etiqueta Helm, Trident se instaló manualmente usando el operador Trident.

## Paso 3: Seleccione un método de actualización

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

- ["Actualice con el operador Trident"](#)



Le sugerimos que revise ["Comprender el flujo de trabajo de actualización del operador"](#) antes de actualizar con el operador.

\*

## Actualizar con el operador

### Comprender el flujo de trabajo de actualización del operador

Antes de usar el operador Trident para actualizar Trident, debe comprender los procesos en segundo plano que ocurren durante la actualización. Esto incluye cambios en la controladora Trident, en el pod de controladora y en los pods de nodos, así como en el DaemonSet de nodos que permiten actualizaciones graduales.

### Manejo de actualizaciones del operador Trident

Uno de los ["Ventajas del uso del operador Trident"](#) muchos que instalan y actualizan Trident es la gestión automática de objetos Trident y Kubernetes sin interrumpir los volúmenes montados existentes. De esta forma, Trident puede admitir renovaciones sin tiempos de inactividad o ["actualizaciones sucesivas"](#). En concreto, el operador Trident se comunica con el clúster de Kubernetes para:

- Elimine y vuelva a crear la implementación de Trident Controller y DaemonSet de nodos.
- Sustituya el pod de la controladora de Trident y los pods de nodos de Trident por nuevas versiones.
  - Si no se actualiza un nodo, no impide que se actualicen los nodos restantes.
  - Solo los nodos con un nodo de Trident en ejecución pueden montar volúmenes.



Para obtener más información sobre la arquitectura de Trident en el clúster de Kubernetes, consulte ["Arquitectura de Trident"](#).

### Flujo de trabajo de actualización del operador

Cuando inicie una actualización con el operador Trident:

1. El operador **Trident**:
  - a. Detecta la versión instalada actualmente de Trident (versión  $n$ ).
  - b. Actualiza todos los objetos de Kubernetes, incluidos CRD, RBAC y Trident SVC.
  - c. Elimina la implementación de Trident Controller para la versión  $n$ .
  - d. Crea la implementación de Trident Controller para la versión  $n+1$ .
2. **Kubernetes** crea Trident Controller Pod para  $n+1$ .
3. El operador **Trident**:
  - a. Elimina el conjunto de cambios de nodo Trident para  $n$ . El operador no espera la terminación del Node Pod.
  - b. Crea el inicio del demonio del nodo Trident para  $n+1$ .
4. **Kubernetes** crea pods de nodos Trident en nodos que no ejecutan Trident Node Pod  $n$ . De este modo se garantiza que nunca haya más de un pod de nodo de Trident, de ninguna versión, en un nodo.

### Actualice una instalación de Trident con el operador Trident o Helm

Puede actualizar Trident mediante el operador Trident manualmente o mediante Helm. Puede actualizar de una instalación del operador de Trident a otra instalación del operador de Trident o actualizar de una `tridentctl` instalación a una versión del operador de Trident. Revise ["Seleccione un método de actualización"](#) antes de actualizar una instalación del operador Trident.

#### Actualizar una instalación manual

Puede actualizar desde una instalación de operadores Trident en el ámbito del clúster a otra instalación del operador Trident en el ámbito del clúster. Todas las versiones 21,01 y superiores de Trident utilizan un operador en el ámbito del clúster.



Para actualizar desde Trident que se instaló con el operador de ámbito de espacio de nombres (versiones 20,07 a 20,10), use las instrucciones de actualización de de ["la versión instalada"](#)Trident.

#### Acerca de esta tarea

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



- Para los clústeres que ejecutan Kubernetes 1,24, utilice "bundle\_pre\_1\_25.yaml".
- Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice "bundle\_post\_1\_25.yaml".

### 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 Trident:

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

2. Suprima el operador Trident que se utilizó para instalar la instancia de Trident actual. Por ejemplo, si va a actualizar desde 23,07, ejecute el siguiente comando:

```
kubectl delete -f 23.07.0/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 Trident usando el archivo yaml del paquete correcto para su entorno, donde `<bundle.yaml>` está `bundle_pre_1_25.yaml` o `bundle_post_1_25.yaml` basado en su versión de Kubernetes. Por ejemplo, si está instalando Trident 24,10, ejecute el siguiente comando:

```
kubectl create -f 24.10.0/trident-installer/deploy/<bundle.yaml> -n trident
```

### Actualizar una instalación Helm

Puede actualizar una instalación de Trident Helm.



Cuando actualice un clúster de Kubernetes de 1,24 a 1,25 o una versión posterior que tiene Trident instalado, debe actualizar los valores.yaml para establecer `excludePodSecurityPolicy true` o agregar `--set excludePodSecurityPolicy=true` al `helm upgrade` comando antes de poder actualizar el clúster.

Si ya has actualizado el clúster de Kubernetes de 1,24 a 1,25 sin actualizar el timón de Trident, la actualización de helm fallará. Para que la actualización de HELM se realice, realice estos pasos como requisitos previos:

1. Instale el plugin `helm-mapkubeapis` desde <https://github.com/helm/helm-mapkubeapis>.
2. Realizar una ejecución en seco para la versión de Trident en el espacio de nombres donde está instalado Trident. Esto enumera los recursos, que se limpiarán.

```
helm mapkubeapis --dry-run trident --namespace trident
```

3. Realice una carrera completa con el timón para realizar la limpieza.

```
helm mapkubeapis trident --namespace trident
```

## Pasos

1. Si "[Trident instalado usando Helm](#)" utiliza `helm upgrade trident netapp-trident/trident-operator --version 100.2410.0` para actualizar en un solo paso. Si no ha añadido el repositorio Helm o no puede utilizarlo para actualizar:
  - a. Descargue la versión más reciente de Trident en "[La sección Assets de GitHub](#)".
  - b. Utilice `helm upgrade` el comando donde `trident-operator-24.10.0.tgz` refleja la versión a la que desea actualizar.

```
helm upgrade <name> trident-operator-24.10.0.tgz
```



Si establece opciones personalizadas durante la instalación inicial (como especificar registros privados reflejados para imágenes de Trident y CSI), agregue la `helm upgrade` comando que utiliza `--set` para asegurarse de que estas opciones están incluidas en el comando `upgrade`, de lo contrario, los valores se restablecerán a los valores predeterminados.

2. 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.

## Actualizar desde a. `tridentctl` Instalación para el operador Trident

Puede actualizarlo a la versión más reciente del operador de Trident desde un `tridentctl` instalación. Los back-ends y EVs existentes estarán disponibles automáticamente.



Antes de cambiar entre los métodos de instalación, revise "[Moverse entre los métodos de instalación](#)".

## Pasos

1. Descargue la versión más reciente de Trident.

```
# Download the release required [24.10.0]
mkdir 24.10.0
cd 24.10.0
wget
https://github.com/NetApp/trident/releases/download/v24.10.0/trident-
installer-24.10.0.tar.gz
tar -xf trident-installer-24.10.0.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-name.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 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:          v24.10.0

```

## Actualice con `tridentctl`

Puede actualizar fácilmente una instalación existente de Trident usando `tridentctl`.

### Acerca de esta tarea

La desinstalación y la reinstalación de Trident actúa como una actualización. Al desinstalar Trident, la reclamación de volumen persistente (RVP) y el volumen persistente (PV) que utiliza la implementación de Trident no se eliminan. Los VP que ya se hayan aprovisionado permanecerán disponibles mientras Trident esté desconectado, y Trident aprovisionará volúmenes para cualquier RVP que se creen en ese momento tras su nuevo funcionamiento.

### Antes de empezar

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

### Pasos

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

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

2. Vuelva a instalar Trident. Consulte "[Instale Trident usando tridentctl](#)".



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

## Gestione Trident con tridentctl

```
https://github.com/NetApp/trident/releases["Paquete de instalación de Trident"^] Incluye la `tridentctl` utilidad de línea de comandos para ofrecer un acceso simple a Trident. Los usuarios de Kubernetes con suficiente Privileges pueden usarlo para instalar Trident o gestionar el espacio de nombres que contiene el pod de Trident.
```

### Comandos e indicadores globales

Puede ejecutar `tridentctl help` para obtener una lista de comandos disponibles para `tridentctl` o añada la `--help` marque cualquier comando para obtener una lista de opciones e indicadores para ese comando específico.

```
tridentctl [command] [--optional-flag]
```

La utilidad Trident `tridentctl` admite los siguientes comandos e indicadores globales.

## Comandos

### **create**

Añadir un recurso a Trident.

### **delete**

Quite uno o más recursos de Trident.

### **get**

Obtenga uno o más recursos de Trident.

### **help**

Ayuda sobre cualquier comando.

### **images**

Imprima una tabla de las imágenes de contenedor que Trident necesita.

### **import**

Importe un recurso existente a Trident.

### **install**

Instale Trident.

### **logs**

Imprima los registros desde Trident.

### **send**

Envíe un recurso desde Trident.

### **uninstall**

Desinstale Trident.

### **update**

Modifique un recurso en Trident.

### **update backend state**

Suspender temporalmente las operaciones de backend.

### **upgrade**

Actualice un recurso en Trident.

### **version**

Imprima la versión de Trident.

## Indicadores globales

### **-d, --debug**

Salida de depuración.

### **-h, --help**

Ayuda de `tridentctl`.

### **-k, --kubeconfig string**

Especifique el `KUBECONFIG` Ruta para ejecutar comandos localmente o desde un clúster de Kubernetes a otro.



Como alternativa, puede exportar el `KUBECONFIG` Variable para apuntar a un clúster y un problema de Kubernetes específicos `tridentctl` comandos para ese clúster.

### **-n, --namespace string**

Puesta en marcha de espacio de nombres de Trident.

### **-o, --output string**

Formato de salida. Uno de `json|yaml|name|Wide|ps` (predeterminado).

### **-s, --server string**

Dirección/puerto de la interfaz REST DE Trident.



La interfaz DE REST de Trident se puede configurar para escuchar y servir únicamente en `127.0.0.1` (para IPv4) o `:::1` (para IPv6).

## Opciones de comando y indicadores

### **cree**

Utilice `create` el comando para agregar un recurso a Trident.

```
tridentctl create [option]
```

#### **Opciones**

`backend`: Añadir un backend a Trident.

### **eliminar**

Utilice `delete` el comando para quitar uno o varios recursos de Trident.

```
tridentctl delete [option]
```

#### **Opciones**

`backend`: Eliminar uno o más back-ends de almacenamiento de Trident.

`snapshot`: Elimine una o varias snapshots de volumen de Trident.

`storageclass`: Eliminar una o más clases de almacenamiento de Trident.

volume: Eliminar uno o varios volúmenes de almacenamiento de Trident.

## obtenga

Utilice `get` el comando para obtener uno o varios recursos de Trident.

```
tridentctl get [option]
```

## Opciones

backend: Obtenga uno o más backends de almacenamiento de Trident.

snapshot: Obtenga una o más instantáneas de Trident.

storageclass: Obtenga una o más clases de almacenamiento de Trident.

volume: Obtenga uno o más volúmenes de Trident.

## Indicadores

-h, --help: Ayuda para volúmenes.

--parentOfSubordinate string: Limite la consulta al volumen de origen subordinado.

--subordinateOf string: Limite la consulta a las subordinadas del volumen.

## imágenes

Utilice `images` indicadores para imprimir una tabla de las imágenes de contenedor que necesita Trident.

```
tridentctl images [flags]
```

## Indicadores

-h, --help: Ayuda para imágenes.

-v, --k8s-version string: Versión semántica del clúster de Kubernetes.

## importe volumen

Utilice `import volume` el comando para importar un volumen existente a Trident.

```
tridentctl import volume <backendName> <volumeName> [flags]
```

## Alias

volume, v

## Indicadores

-f, --filename string: Ruta al archivo YLMA o JSON PVC.

-h, --help: Ayuda para el volumen.

--no-manage: Cree sólo PV/PVC. No asuma que se gestiona el ciclo de vida de los volúmenes.

## instale

Utilice los `install` indicadores para instalar Trident.

```
tridentctl install [flags]
```



## Indicadores

`--autosupport-image string`: La imagen del contenedor para la telemetría AutoSupport (por defecto "NetApp/Trident AutoSupport:<current-version>").

`--autosupport-proxy string`: La dirección/puerto de un proxy para enviar telemetría AutoSupport.

`--enable-node-prep`: Intenta instalar los paquetes necesarios en los nodos.

`--generate-custom-yaml`: Generar archivos YAML sin instalar nada.

`-h, --help`: Ayuda para la instalación.

`--http-request-timeout`: Sustituya el tiempo de espera de la solicitud HTTP para la API REST del controlador Trident (por defecto 1m30s).

`--image-registry string`: La dirección/puerto de un registro interno de imágenes.

`--k8s-timeout duration`: El tiempo de espera para todas las operaciones de Kubernetes (por defecto 3m0s).

`--kubelet-dir string`: La ubicación del anfitrión del estado interno de kubelet (por defecto "/var/lib/kubelet").

`--log-format string`: El formato de registro Trident (texto, json) (por defecto "texto").

`--node-prep`: Permite a Trident preparar los nodos del clúster de Kubernetes para gestionar volúmenes mediante el protocolo de almacenamiento de datos especificado. **Actualmente, `iscsi` es el único valor soportado.**

`--pv string`: El nombre del PV heredado utilizado por Trident, se asegura de que no exista (por defecto "Trident").

`--pvc string`: El nombre del PVC heredado utilizado por Trident, se asegura de que esto no exista (por defecto "Trident").

`--silence-autosupport`: No enviar paquetes AutoSupport a NetApp automáticamente (predeterminado true).

`--silent`: Deshabilitar la mayoría de la salida durante la instalación.

`--trident-image string`: La imagen Trident para instalar.

`--use-custom-yaml`: Utilice cualquier archivo YAML existente que exista en el directorio de configuración.

`--use-ipv6`: Utilice IPv6 para la comunicación de Trident.

## registros

Utilice `logs` los indicadores para imprimir los registros de Trident.

```
tridentctl logs [flags]
```

## Indicadores

`-a, --archive`: Crear un archivo de soporte con todos los registros a menos que se especifique lo contrario.

`-h, --help`: Ayuda para registros.

`-l, --log string`: Registro de Trident para mostrar. Uno de Trident|auto|Trident-operator|all (automático por defecto).

`--node string`: El nombre del nodo de Kubernetes desde el que se recopilan los registros de pod de nodo.

`-p, --previous`: Obtenga los logs de la instancia de contenedor anterior si existe.

`--sidecars`: Obtenga los registros para los contenedores sidecar.

## enviar

Utilice `send` el comando para enviar un recurso desde Trident.

```
tridentctl send [option]
```

## Opciones

`autosupport`: Enviar un fichero AutoSupport a NetApp.

## desinstalar

Utilice `uninstall` los indicadores para desinstalar Trident.

```
tridentctl uninstall [flags]
```

## Indicadores

`-h, --help`: Ayuda para la desinstalación.

`--silent`: Desactiva la mayoría de la salida durante la desinstalación.

## actualizar

Utilice `update` el comando para modificar un recurso en Trident.

```
tridentctl update [option]
```

## Opciones

`backend`: Actualizar un backend en Trident.

## actualizar estado de backend

Utilice la `update backend state` comando para suspender o reanudar operaciones de back-end.

```
tridentctl update backend state <backend-name> [flag]
```

## Puntos que considerar

- Si se crea un backend con un `TridentBackendConfig (tbc)`, el backend no se puede actualizar con un `backend.json` archivo.
- Si el `userState` se ha establecido en una `tbc`, no se puede modificar mediante el `tridentctl update backend state <backend-name> --user-state suspended/normal` comando.
- Para recuperar la capacidad de configurar el `userState` `tridentctl` vía `tbc`, el campo debe eliminarse del `tbc userState`. Esto se puede hacer usando `kubectl edit tbc` el comando. Una vez `userState` eliminado el campo, puede utilizar `tridentctl update backend state` el comando para cambiar el `userState` de un backend.
- Utilice el `tridentctl update backend state` para cambiar la `userState`. También puede actualizar el `userState` archivo Using `TridentBackendConfig OR backend.json`; esto desencadena una reinicialización completa del backend y puede llevar mucho tiempo.

## Indicadores

`-h, --help`: Ayuda para el estado de backend.

`--user-state`: Establecer en `suspended` para pausar las operaciones de backend. Establezca en `normal` para reanudar las operaciones de back-end. Cuando se establece en `suspended`:

- `AddVolume Import Volume` y se ponen en pausa.
- `CloneVolume, , ResizeVolume PublishVolume UnPublishVolume, , CreateSnapshot, GetSnapshot RestoreSnapshot, , DeleteSnapshot RemoveVolume, , GetVolumeExternal,`

`ReconcileNodeAccess` seguir estando disponible.

También puede actualizar el estado del backend utilizando `userState` el campo en el archivo de configuración de backend `TridentBackendConfig` o `backend.json`. Para obtener más información, consulte ["Opciones para gestionar back-ends"](#) y ["Realice la gestión del entorno de administración con kubectl"](#)

**Ejemplo:**

## JSON

Siga estos pasos para actualizar el `userState` utilizando el `backend.json` archivo:

1. Edite el `backend.json` archivo para incluir el `userState` campo con su valor establecido en 'SUSPENDED'.
2. Actualice el backend con el `tridentctl backend update` comando y la ruta de acceso al archivo actualizado `backend.json`.

**Ejemplo:** `tridentctl backend update -f /<path to backend JSON file>/backend.json`

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "<redacted>",
  "svm": "nas-svm",
  "backendName": "customBackend",
  "username": "<redacted>",
  "password": "<redacted>",
  "userState": "suspended",
}
```

## YAML

Puede editar el tbc después de que se haya aplicado con el `kubectl edit <tbc-name> -n <namespace>` comando. En el ejemplo siguiente se actualiza el estado del back-end para suspender con la `userState: suspended` opción:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  backendName: customBackend
  storageDriverName: ontap-nas
  managementLIF: <redacted>
  svm: nas-svm
userState: suspended
credentials:
  name: backend-tbc-ontap-nas-secret
```

## versión

Uso `version` indicadores para imprimir la versión de `tridentctl` Y el servicio Trident que se ejecuta.

```
tridentctl version [flags]
```

## Indicadores

- `--client`: Sólo versión de cliente (no se necesita ningún servidor).
- `-h`, `--help`: Ayuda para la versión.

## Compatibilidad con complementos

Tridentctl soporta plugins similares a `kubectl`. Tridentctl detecta un plugin si el nombre del archivo binario del plugin sigue el esquema "tridentctl-<plugin>", y el binario se encuentra en una carpeta que enumera la variable de entorno `PATH`. Todos los plugins detectados se enumeran en la sección de plugins de la ayuda `tridentctl`. Opcionalmente, también puede limitar la búsqueda especificando una carpeta de plugin en la variable de entorno `TRIDENTCTL_PLUGIN_PATH` (Ejemplo `TRIDENTCTL_PLUGIN_PATH=~/.tridentctl-plugins/`). Si se utiliza la variable, `tridentctl` busca solo en la carpeta especificada.

# Supervisar Trident

Trident proporciona un conjunto de puntos finales de métricas de Prometheus que puede utilizar para supervisar el rendimiento de Trident.

## Descripción general

Las métricas que proporciona Trident le permiten hacer lo siguiente:

- Estar al tanto del estado y la configuración de Trident. Puede examinar la eficacia de las operaciones y si puede comunicarse con los back-ends como se esperaba.
- Examine la información de uso del back-end, y comprenda cuántos volúmenes se aprovisionan en un entorno de administración y la cantidad de espacio consumido, etc.
- Mantenga una asignación de la cantidad de volúmenes aprovisionados en los back-ends disponibles.
- Seguimiento del rendimiento. Puede ver cuánto tiempo tarda Trident en comunicarse con los back-ends y realizar operaciones.



De forma predeterminada, las métricas de Trident se exponen en el puerto de destino 8001 en la `/metrics` extremo. Estas métricas están **activadas de forma predeterminada** cuando se instala Trident.

## Lo que necesitará

- Un clúster de Kubernetes con Trident instalado.
- Una instancia Prometheus. Esto puede ser un ["Puesta en marcha de Prometeo en contenedores"](#) También puede optar por ejecutar Prometheus como a. ["aplicación nativa"](#).

## Paso 1: Definir un objetivo Prometheus

Debe definir un destino de Prometheus para recopilar las métricas y obtener información acerca de los back-ends que gestiona Trident, los volúmenes que crea, etc. Esto ["blog"](#) explica cómo puedes usar Prometheus y Grafana con Trident para recuperar métricas. El blog explica cómo puede ejecutar Prometheus como operador

en su clúster de Kubernetes y la creación de un ServiceMonitor para obtener métricas de Trident.

## Paso 2: Cree un Prometheus ServiceMonitor

Para usar las métricas de Trident, debe crear un Prometheus ServiceMonitor que vaya a ver el `trident-csi` el servicio y escucha el `metrics` puerto. Un ejemplo de ServiceMonitor tiene este aspecto:

```
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  name: trident-sm
  namespace: monitoring
  labels:
    release: prom-operator
spec:
  jobLabel: trident
  selector:
    matchLabels:
      app: controller.csi.trident.netapp.io
  namespaceSelector:
    matchNames:
      - trident
  endpoints:
    - port: metrics
      interval: 15s
```

Esta definición de ServiceMonitor recupera las métricas devueltas por el `trident-csi` servicio y busca específicamente el `metrics` punto final del servicio. Como resultado, ahora Prometheus está configurado para comprender las métricas de Trident.

Además de las métricas disponibles directamente desde Trident, kubelet expone muchas `kubelet_volume_*` métricas a través de su propio punto final de métricas. Kubelet puede proporcionar información sobre los volúmenes adjuntos y los pods y otras operaciones internas que realiza. Consulte ["aquí"](#).

## Paso 3: Consulte las métricas de Trident con PromQL

PromQL es adecuado para crear expresiones que devuelvan datos tabulares o de series temporales.

A continuación se muestran algunas consultas PromQL que se pueden utilizar:

### Obtenga información de estado de Trident

- **Porcentaje de respuestas HTTP 2XX de Trident**

```
(sum (trident_rest_ops_seconds_total_count{status_code=~"2.."} OR on()
vector(0)) / sum (trident_rest_ops_seconds_total_count)) * 100
```

- **Porcentaje de respuestas REST de Trident a través del código de estado**

```
(sum (trident_rest_ops_seconds_total_count) by (status_code) / scalar
(sum (trident_rest_ops_seconds_total_count))) * 100
```

- **Duración media en ms de operaciones realizadas por Trident**

```
sum by (operation)
(trident_operation_duration_milliseconds_sum{success="true"}) / sum by
(operation)
(trident_operation_duration_milliseconds_count{success="true"})
```

## Obtenga la información de uso de Trident

- **Tamaño medio del volumen**

```
trident_volume_allocated_bytes/trident_volume_count
```

- **Espacio total por volumen provisionado por cada backend**

```
sum (trident_volume_allocated_bytes) by (backend_uuid)
```

## Obtenga el uso de cada volumen



Esto solo se habilita si también se recopilan las métricas Kubelet.

- **Porcentaje de espacio usado para cada volumen**

```
kubelet_volume_stats_used_bytes / kubelet_volume_stats_capacity_bytes *
100
```

## Más información sobre la telemetría de Trident AutoSupport

De forma predeterminada, Trident envía métricas de Prometheus e información básica de backend a NetApp en una cadencia diaria.

- Para evitar que Trident envíe métricas de Prometheus e información básica de back-end a NetApp, pase el `--silence-autosupport` indicador durante la instalación de Trident.
- Trident también puede enviar registros de contenedores al soporte de NetApp bajo demanda a través ``tridentctl send autosupport`` de . Deberá activar Trident para que cargue sus registros. Antes de enviar registros, debe aceptar NetApp <https://www.netapp.com/company/legal/privacy-policy/>["política de privacidad"].

- A menos que se especifique, Trident recupera los registros de las últimas 24 horas.
- Puede especificar el plazo de retención del registro con `--since` el indicador. Por ejemplo `tridentctl send autosupport --since=1h:.` Esta información se recopila y se envía a través de un `trident-autosupport` contenedor que se instala junto con Trident. Puede obtener la imagen del contenedor en ["AutoSupport de Trident"](#).
- Trident AutoSupport no recopila ni transmite información personal identificable (PII) ni Información personal. Incluye una **"CLUF"** que no es aplicable a la propia imagen del contenedor de Trident. Puede obtener más información sobre el compromiso de NetApp con la seguridad y la confianza de los datos ["aquí"](#).

Un ejemplo de carga útil enviada por Trident tiene el siguiente aspecto:

```
---
items:
- backendUUID: ff3852e1-18a5-4df4-b2d3-f59f829627ed
  protocol: file
  config:
    version: 1
    storageDriverName: ontap-nas
    debug: false
    debugTraceFlags:
    disableDelete: false
    serialNumbers:
    - nwkvzfanek_SN
    limitVolumeSize: ''
  state: online
  online: true
```

- Los mensajes de AutoSupport se envían al extremo AutoSupport de NetApp. Si está utilizando un Registro privado para almacenar imágenes contenedoras, puede utilizar `--image-registry` bandera.
- También puede configurar direcciones URL proxy generando los archivos YLMA de instalación. Esto se puede hacer usando `tridentctl install --generate-custom-yaml` Para crear los archivos YAML y agregar `--proxy-url` argumento para `trident-autosupport` contenedor en `trident-deployment.yaml`.

## Deshabilitar las métricas de Trident

Para **desactivar las métricas** de ser reportadas, debe generar YAMLs personalizados (utilizando la `--generate-custom-yaml` y editarlas para eliminar `--metrics` no se invoca el indicador para el ``trident-main`` contenedor.

## Desinstale Trident

Debe usar el mismo método para desinstalar Trident que utilizó para instalar Trident.

### Acerca de esta tarea

- Si necesita una corrección para los errores observados después de una actualización, problemas de



dependencia o una actualización incorrecta o incompleta, debe desinstalar Trident y volver a instalar la versión anterior usando las instrucciones específicas para ese "versión". Esta es la única forma recomendada de *downgrade* a una versión anterior.

- Para facilitar la actualización y la reinstalación, desinstalar Trident no elimina los CRD ni los objetos relacionados creados por Trident. Si necesita eliminar completamente Trident y todos sus datos, consulte ["Eliminar completamente Trident y CRD"](#).

### Antes de empezar

Si va a decomisionar clústeres de Kubernetes, debe eliminar todas las aplicaciones que usan volúmenes creados por Trident antes de desinstalar. De este modo se garantiza la eliminación de las RVP en los nodos de Kubernetes antes de que se eliminen.

## Determine el método de instalación original

Debe utilizar el mismo método para desinstalar Trident que utilizó para instalarlo. Antes de desinstalar, verifique qué versión utilizó para instalar Trident originalmente.

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

## Desinstale una instalación del operador Trident

Puede desinstalar una instalación de operador trident manualmente o usando Helm.

### Desinstale la instalación manual

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

1. **Edición `TridentOrchestrator` CR y establecer el indicador de desinstalación:**

```
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 desea volver a instalar Trident.

2. **Eliminar `TridentOrchestrator`:** Al eliminar el `TridentOrchestrator` CR que se utilizó para implementar Trident, le indica al operador que desinstale Trident. El operador procesa la eliminación `TridentOrchestrator` y procede a eliminar el despliegue de Trident y el inicio de datos, eliminando los pods de Trident que había creado como parte de la instalación.

```
kubectl delete -f deploy/<bundle.yaml> -n <namespace>
```

## Desinstale la instalación de Helm

Si instaló Trident usando Helm, puede desinstalarlo usando `helm uninstall`.

```
#List the Helm release corresponding to the 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 un tridentctl instalación

Utilice `uninstall` el comando en `tridentctl` para eliminar todos los recursos asociados con Trident, excepto los CRD y los objetos relacionados:

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

# Trident para Docker

## Requisitos previos para la implementación

Tiene que instalar y configurar los requisitos previos del protocolo necesarios en su host antes de poder implementar Trident.

### Compruebe los requisitos

- Compruebe que la implementación se adapte a todas las "requisitos".
- Compruebe que tiene instalada una versión compatible de Docker. Si la versión de Docker no está actualizada, "instálelo o actualícelo".

```
docker --version
```

- Comprobar que los requisitos previos del protocolo están instalados y configurados en el host.

### Herramientas de NFS

Instale las herramientas de NFS mediante los comandos del sistema operativo.

#### RHEL 8 O POSTERIOR

```
sudo yum install -y nfs-utils
```

#### Ubuntu

```
sudo apt-get install -y nfs-common
```



Reinicie los nodos de trabajo después de instalar las herramientas NFS para evitar que se produzcan fallos cuando conecte volúmenes a los contenedores.

### Herramientas iSCSI

Instale las herramientas iSCSI mediante los comandos del sistema operativo.

## RHEL 8 O POSTERIOR

1. Instale los siguientes paquetes del sistema:

```
sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils device-  
mapper-multipath
```

2. Compruebe que la versión de iscsi-initiator-utils sea 6.2.0.874-2.el7 o posterior:

```
rpm -q iscsi-initiator-utils
```

3. Configure el escaneo en manual:

```
sudo sed -i 's/^\(node.session.scan\) .*/\1 = manual/'  
/etc/iscsi/iscsid.conf
```

4. Activar accesos múltiples:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



Asegúrese etc/multipath.conf contiene find\_multipaths no inferior defaults.

5. Asegúrese de que así sea iscsid y.. multipathd están en ejecución:

```
sudo systemctl enable --now iscsid multipathd
```

6. Activar e iniciar iscsi:

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. Instale los siguientes paquetes del sistema:

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools  
scsitools
```

2. Compruebe que la versión Open-iscsi sea 2.0.874-5ubuntu2.10 o posterior (para bionic) o 2.0.874-7.1ubuntu6.1 o posterior (para focal):

```
dpkg -l open-iscsi
```

### 3. Configure el escaneo en manual:

```
sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'  
/etc/iscsi/iscsid.conf
```

### 4. Activar accesos múltiples:

```
sudo tee /etc/multipath.conf <<-EOF  
defaults {  
    user_friendly_names yes  
    find_multipaths no  
}  
EOF  
sudo systemctl enable --now multipath-tools.service  
sudo service multipath-tools restart
```



Asegúrese etc/multipath.conf contiene find\_multipaths no inferior defaults.

### 5. Asegúrese de que así sea open-iscsi y.. multipath-tools están habilitadas y en ejecución:

```
sudo systemctl status multipath-tools  
sudo systemctl enable --now open-iscsi.service  
sudo systemctl status open-iscsi
```

## Herramientas de NVMe

Instale las herramientas NVMe mediante los comandos de su sistema operativo.



- NVMe requiere RHEL 9 o posterior.
- Si la versión del kernel de su nodo de Kubernetes es demasiado antigua o si el paquete NVMe no está disponible para la versión de kernel, es posible que deba actualizar la versión del kernel del nodo a una con el paquete NVMe.

## RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

# Ponga en marcha Trident

Trident para Docker proporciona integración directa con el ecosistema de Docker para las plataformas de almacenamiento de NetApp. Admite el aprovisionamiento y la gestión de recursos de almacenamiento desde la plataforma de almacenamiento hasta hosts Docker, con un marco para añadir plataformas adicionales en el futuro.

Se pueden ejecutar varias instancias de Trident a la vez en el mismo host. Esto permite conexiones simultáneas a varios sistemas de almacenamiento y tipos de almacenamiento, con la capacidad de personalizar el almacenamiento usado para los volúmenes de Docker.

### Lo que necesitará

Consulte la ["requisitos previos para la implementación"](#). Una vez que se cumplan los requisitos previos, estará listo para implementar Trident.

## Método de complemento gestionado por Docker (versión 1.13/17.03 y posteriores)

### Antes de empezar



Si ha utilizado Trident pre Docker 1,13/17,03 en el método de daemon tradicional, asegúrese de detener el proceso de Trident y reiniciar el daemon de Docker antes de utilizar el método de complemento gestionado.

1. Detener todas las instancias en ejecución:

```
killall /usr/local/bin/netappdvp
killall /usr/local/bin/trident
```

2. Reinicie Docker.

```
systemctl restart docker
```

3. Asegúrese de tener instalado Docker Engine 17.03 (nuevo 1.13) o una versión posterior.

```
docker --version
```

Si su versión no está actualizada, ["instale o actualice la instalación"](#).

## Pasos

1. Cree un archivo de configuración y especifique las opciones siguientes:

- `config`: El nombre de archivo predeterminado es `config.json`, sin embargo, puede utilizar cualquier nombre que elija si especifica `config` opción con el nombre de archivo. El archivo de configuración debe estar ubicado en la `/etc/netappdvp` directorio en el sistema host.
- `log-level`: Especifique el nivel de registro (`debug`, `info`, `warn`, `error`, `fatal`). El valor predeterminado es `info`.
- `debug`: Especifique si el registro de depuración está activado. El valor predeterminado es `false`. Reemplaza el nivel de registro si es `TRUE`.
  - i. Cree una ubicación para el archivo de configuración:

```
sudo mkdir -p /etc/netappdvp
```

ii. Cree el archivo de configuración:

```
cat << EOF > /etc/netappdvp/config.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1"
}
EOF
```

2. Inicie Trident utilizando el sistema de complementos gestionados. Reemplace `<version>` por la versión del plugin (`xxx.xx.x`) que está utilizando.

```
docker plugin install --grant-all-permissions --alias netapp
netapp/trident-plugin:<version> config=myConfigFile.json
```

3. Comience a utilizar Trident para consumir almacenamiento del sistema configurado.

- a. Cree un volumen denominado "firstVolume":

```
docker volume create -d netapp --name firstVolume
```

- b. Cree un volumen predeterminado cuando el contenedor comience:

```
docker run --rm -it --volume-driver netapp --volume  
secondVolume:/my_vol alpine ash
```

- c. Quite el volumen "firstVolume":

```
docker volume rm firstVolume
```

## Método tradicional (versión 1.12 o anterior)

### Antes de empezar

1. Asegúrese de que tiene Docker versión 1.10 o posterior.

```
docker --version
```

Si la versión no está actualizada, actualice la instalación.

```
curl -fsSL https://get.docker.com/ | sh
```

O bien, [siga las instrucciones de su distribución](#).

2. Asegúrese de que esté configurado NFS y/o iSCSI para su sistema.

### Pasos

1. Instale y configure el complemento NetApp Docker Volume Plugin:
  - a. Descargue y desembale la aplicación:

```
wget  
https://github.com/NetApp/trident/releases/download/v24.10.0/trident-  
installer-24.10.0.tar.gz  
tar xzf trident-installer-24.10.0.tar.gz
```

- b. Desplazarse a una ubicación en la ruta de la bandeja:



```
sudo mv trident-installer/extras/bin/trident /usr/local/bin/  
sudo chown root:root /usr/local/bin/trident  
sudo chmod 755 /usr/local/bin/trident
```

c. Cree una ubicación para el archivo de configuración:

```
sudo mkdir -p /etc/netappdvp
```

d. Cree el archivo de configuración:

```
cat << EOF > /etc/netappdvp/ontap-nas.json  
{  
  "version": 1,  
  "storageDriverName": "ontap-nas",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.2",  
  "svm": "svm_nfs",  
  "username": "vsadmin",  
  "password": "password",  
  "aggregate": "aggr1"  
}  
EOF
```

2. Después de colocar el binario y crear el archivo de configuración, inicie el daemon de Trident con el archivo de configuración que desee.

```
sudo trident --config=/etc/netappdvp/ontap-nas.json
```



A menos que se especifique, el nombre predeterminado para el controlador de volumen es NetApp.

Después de iniciar el daemon, puede crear y gestionar volúmenes mediante la interfaz CLI de Docker

3. Cree un volumen:

```
docker volume create -d netapp --name trident_1
```

4. Aprovechone un volumen de Docker al iniciar un contenedor:

```
docker run --rm -it --volume-driver netapp --volume trident_2:/my_vol  
alpine ash
```

## 5. Quite un volumen de Docker:

```
docker volume rm trident_1
docker volume rm trident_2
```

## Inicie Trident al iniciar el sistema

Puede encontrar un archivo de ejemplo de unidad para sistemas basados en el sistema en `contrib/trident.service.example` En el Git repo. Para utilizar el archivo con RHEL, realice lo siguiente:

### 1. Copie el archivo en la ubicación correcta.

Debe utilizar nombres únicos para los archivos de unidad si tiene más de una instancia en ejecución.

```
cp contrib/trident.service.example
/usr/lib/systemd/system/trident.service
```

### 2. Edite el archivo, cambie la descripción (línea 2) para que coincida con el nombre del controlador y la ruta del archivo de configuración (línea 9) para reflejar su entorno.

### 3. Vuelva a cargar systemd para que procese los cambios:

```
systemctl daemon-reload
```

### 4. Active el servicio.

Este nombre varía en función de lo que haya nombrado el archivo en el `/usr/lib/systemd/system` directorio.

```
systemctl enable trident
```

### 5. Inicie el servicio.

```
systemctl start trident
```

### 6. Ver el estado.

```
systemctl status trident
```



Siempre que modifique el archivo de unidad, ejecute el `systemctl daemon-reload` comando para que tenga en cuenta los cambios.

# Actualice o desinstale Trident

Puede actualizar Trident para Docker de forma segura sin afectar a los volúmenes que se utilizan. Durante el proceso de actualización, habrá un breve período en el que `docker volume` los comandos dirigidos al plugin no tendrán éxito, y las aplicaciones no podrán montar volúmenes hasta que el plugin vuelva a ejecutarse. En la mayoría de las circunstancias, esto es cuestión de segundos.

## Renovar

Realice los siguientes pasos para actualizar Trident para Docker.

### Pasos

1. Enumere los volúmenes existentes:

```
docker volume ls
DRIVER          VOLUME NAME
netapp:latest   my_volume
```

2. Desactivar el complemento:

```
docker plugin disable -f netapp:latest
docker plugin ls
ID              NAME          DESCRIPTION
ENABLED
7067f39a5df5   netapp:latest nDVP - NetApp Docker Volume
Plugin        false
```

3. Actualizar el complemento:

```
docker plugin upgrade --skip-remote-check --grant-all-permissions
netapp:latest netapp/trident-plugin:21.07
```



La versión 18,01 de Trident sustituye al nDVP. Debe actualizar directamente de la `netapp/ndvp-plugin` imagen a la `netapp/trident-plugin` imagen.

4. Habilitar el plugin:

```
docker plugin enable netapp:latest
```

5. Compruebe que el plugin está habilitado:

```
docker plugin ls
ID                NAME                DESCRIPTION
ENABLED
7067f39a5df5     netapp:latest      Trident - NetApp Docker Volume
Plugin    true
```

6. Compruebe que los volúmenes estén visibles:

```
docker volume ls
DRIVER                VOLUME NAME
netapp:latest        my_volume
```



Si va a actualizar desde una versión anterior de Trident (anterior a 20,10) a Trident 20,10 o posterior, puede que se produzca un error. Para obtener más información, consulte ["Problemas conocidos"](#). Si se encuentra con el error, primero debe deshabilitar el plugin, luego quitar el plugin y luego instalar la versión de Trident requerida pasando un parámetro de configuración adicional: `docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant-all-permissions config=config.json`

## Desinstalar

Siga los pasos que se indican a continuación para desinstalar Trident para Docker.

### Pasos

1. Quite los volúmenes que haya creado el plugin.
2. Desactivar el complemento:

```
docker plugin disable netapp:latest
docker plugin ls
ID                NAME                DESCRIPTION
ENABLED
7067f39a5df5     netapp:latest      nDVP - NetApp Docker Volume
Plugin    false
```

3. Quitar el plugin:

```
docker plugin rm netapp:latest
```

## Trabaje con volúmenes

Es posible crear, clonar y quitar volúmenes fácilmente mediante los comandos estándar

`docker volume` con el nombre de controlador de Trident especificado cuando se necesita.

## Cree un volumen

- Cree un volumen con un controlador con el nombre predeterminado:

```
docker volume create -d netapp --name firstVolume
```

- Cree un volumen con una instancia específica de Trident:

```
docker volume create -d ntap_bronze --name bronzeVolume
```



Si no especifica ninguna "opciones", se utilizan los valores predeterminados del controlador.

- Anule el tamaño de volumen predeterminado. Consulte el siguiente ejemplo para crear un volumen de 20 GIB con un controlador:

```
docker volume create -d netapp --name my_vol --opt size=20G
```



Los tamaños de volumen se expresan como cadenas que contienen un valor entero con unidades opcionales (por ejemplo: 10G, 20 GB, 3 TIB). Si no se especifica ninguna unidad, el valor predeterminado es G. Las unidades de tamaño se pueden expresar como potencias de 2 (B, KiB, MiB, GiB, TiB) o de 10 (B, KB, MB, GB, TB). Las unidades abreviadas utilizan potencias de 2 (G = GiB, T = TiB, ...).

## Quitar un volumen

- Quite el volumen como cualquier otro volumen de Docker:

```
docker volume rm firstVolume
```



Cuando utilice la `solidfire-san` driver, el ejemplo anterior elimina y purga el volumen.

Realice los siguientes pasos para actualizar Trident para Docker.

## Clonar un volumen

Al utilizar `ontap-nas`, `ontap-san`, `solidfire-san` y `gcp-cvs storage drivers`, Trident puede clonar volúmenes. Al utilizar `ontap-nas-flexgroup` los controladores o `ontap-nas-economy`, no se admite la clonación. La creación de un volumen nuevo a partir de un volumen existente dará como resultado la creación de una copia de Snapshot nueva.

- Examine el volumen para enumerar las instantáneas:

```
docker volume inspect <volume_name>
```

- Cree un volumen nuevo a partir de un volumen existente. Esto dará como resultado la creación de una nueva snapshot:

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume>
```

- Cree un volumen nuevo a partir de una snapshot existente en un volumen. Esto no creará una nueva snapshot:

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume> -o fromSnapshot=<source_snap_name>
```

## Ejemplo

```

docker volume inspect firstVolume

[
  {
    "Driver": "ontap-nas",
    "Labels": null,
    "Mountpoint": "/var/lib/docker-volumes/ontap-
nas/netappdvp_firstVolume",
    "Name": "firstVolume",
    "Options": {},
    "Scope": "global",
    "Status": {
      "Snapshots": [
        {
          "Created": "2017-02-10T19:05:00Z",
          "Name": "hourly.2017-02-10_1505"
        }
      ]
    }
  }
]

docker volume create -d ontap-nas --name clonedVolume -o from=firstVolume
clonedVolume

docker volume rm clonedVolume
docker volume create -d ontap-nas --name volFromSnap -o from=firstVolume
-o fromSnapshot=hourly.2017-02-10_1505
volFromSnap

docker volume rm volFromSnap

```

## Acceso a volúmenes creados externamente

Puede acceder a dispositivos de bloque creados externamente (o a sus clones) mediante contenedores utilizando Trident **Only** si no tienen particiones y si su sistema de archivos es compatible con Trident (por ejemplo: Un ext4-formateado /dev/sdc1 no será accesible a través de Trident).

## Opciones de volumen específicas del controlador

Cada controlador de almacenamiento tiene un conjunto diferente de opciones que se pueden especificar al crear un volumen para personalizar el resultado. Consulte a continuación las opciones que se aplican al sistema de almacenamiento configurado.

Usar estas opciones durante la operación de creación de volúmenes es simple. Proporcione la opción y el valor con `-o` Operador durante el funcionamiento de la CLI. Estos sustituyen cualquier valor equivalente al

archivo de configuración JSON.

## Opciones de volumen de ONTAP

Las opciones de creación de volumen para NFS e iSCSI son las siguientes:

Opción	Descripción
size	El tamaño del volumen, de manera predeterminada es 1 GIB.
spaceReserve	Aprovisione el volumen de manera thin o thick, de manera predeterminada, es thin. Los valores válidos son none (con thin provisioning) y. volume (thick-provisioning).
snapshotPolicy	Esto establecerá la política de instantáneas en el valor deseado. El valor predeterminado es none, es decir, no se creará automáticamente instantáneas para el volumen. A menos que el administrador de almacenamiento lo modifique, existe una política llamada "predeterminada" en todos los sistemas de ONTAP que crea y retiene seis copias Snapshot cada hora, dos días y dos semanas. Los datos conservados en una instantánea se pueden recuperar navegando hacia la .snapshot directorio en cualquier directorio del volumen.
snapshotReserve	Esto establecerá la reserva de instantáneas en el porcentaje deseado. El valor predeterminado es no, lo que significa que ONTAP seleccionará la reserva de copias Snapshot (generalmente 5 %) si se seleccionó una política de copias Snapshot o 0 % si la política de copias Snapshot no es ninguna. Es posible establecer el valor predeterminado de snapshotReserve en el archivo de configuración para todos los back-ends de ONTAP, y se puede usar como opción de creación de volúmenes para todos los back-ends de ONTAP excepto ontap-nas-Economy.



Opción	Descripción
<code>splitOnClone</code>	Al clonar un volumen, ONTAP dividirá inmediatamente el clon de su principal. El valor predeterminado es <code>false</code> . Algunos casos de uso para el clonado de volúmenes se sirven mejor dividiendo el clon de su elemento principal inmediatamente después de la creación, ya que es poco probable que haya ninguna oportunidad para la eficiencia del almacenamiento. Por ejemplo, el clonado de una base de datos vacía puede ofrecer un gran ahorro de tiempo y un ahorro reducido en espacio de almacenamiento, por lo que es mejor dividir el clon de inmediato.
<code>encryption</code>	Habilite el cifrado de volúmenes de NetApp (NVE) en el volumen nuevo; el valor predeterminado es <code>false</code> . Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster.  Si NAE está habilitado en el back-end, cualquier volumen provisionado en Trident será habilitado NAE.  Para obtener más información, consulte: <a href="#">"Cómo funciona Trident con NVE y NAE"</a> .
<code>tieringPolicy</code>	Establece la política de organización en niveles que se utilizará para el volumen. Esto decide si los datos se mueven al nivel de cloud cuando quedan inactivos (inactivos).

Las siguientes opciones adicionales son para NFS **sólo**:

Opción	Descripción
<code>unixPermissions</code>	Esto controla el conjunto de permisos para el propio volumen. De forma predeterminada, los permisos se establecerán en <code>---rwxr-xr-x</code> , o en notación numérica <code>0755</code> , y <code>root</code> será el propietario. El texto o el formato numérico funcionará.
<code>snapshotDir</code>	Configuración de esta opción en <code>true</code> hará la <code>.snapshot</code> directorio visible para los clientes que acceden al volumen. El valor predeterminado es <code>false</code> , que significa la visibilidad del <code>.snapshot</code> el directorio está desactivado de forma predeterminada. Algunas imágenes, por ejemplo, la imagen oficial de MySQL, no funcionan como se esperaba cuando el <code>.snapshot</code> el directorio es visible.

Opción	Descripción
exportPolicy	Establece la política de exportación que se utilizará para el volumen. El valor predeterminado es default.
securityStyle	Configura el estilo de seguridad que se usará para acceder al volumen. El valor predeterminado es unix. Los valores válidos son unix y.. mixed.

Las siguientes opciones adicionales son para iSCSI **sólo**:

Opción	Descripción
fileSystemType	Configura el sistema de archivos utilizado para formatear volúmenes iSCSI. El valor predeterminado es ext4. Los valores válidos son ext3, ext4, y. xfs.
spaceAllocation	Configuración de esta opción en false Desactivará la función de asignación de espacio de la LUN. El valor predeterminado es true, Es decir, ONTAP notifica al host cuando el volumen se ha quedado sin espacio y el LUN del volumen no puede aceptar escrituras. Esta opción también permite que ONTAP reclame espacio automáticamente cuando el host elimina los datos.

## Ejemplos

Vea los ejemplos siguientes:

- Cree un volumen de 10 GIB:

```
docker volume create -d netapp --name demo -o size=10G -o encryption=true
```

- Cree un volumen de 100 GIB con Snapshot:

```
docker volume create -d netapp --name demo -o size=100G -o snapshotPolicy=default -o snapshotReserve=10
```

- Cree un volumen con el bit setuid activado:

```
docker volume create -d netapp --name demo -o unixPermissions=4755
```

El tamaño de volumen mínimo es 20 MiB.

Si no se especifica la reserva de instantáneas y la política de instantáneas es `none`, Trident utilice una reserva de instantáneas del 0%.

- Crear un volumen sin política de Snapshot y sin reserva de Snapshot:

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none
```

- Crear un volumen sin política de copias Snapshot y una reserva de copias Snapshot personalizada del 10%:

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none  
--opt snapshotReserve=10
```

- Crear un volumen con una política de Snapshot y una reserva de Snapshot personalizada del 10%:

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy --opt snapshotReserve=10
```

- Cree un volumen con una política de snapshots y acepte la reserva de snapshots predeterminada de ONTAP (generalmente 5 %):

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy
```

## Opciones de volumen del software Element

Las opciones del software Element exponen las políticas de tamaño y calidad de servicio asociadas con el volumen. Cuando se crea el volumen, la política de calidad de servicio asociada con él se especifica mediante el `-o type=service_level` terminología

El primer paso para definir un nivel de servicio de calidad de servicio con el controlador de Element es crear al menos un tipo y especificar las IOPS mínimas, máximas y de ráfaga asociadas con un nombre en el archivo de configuración.

Otras opciones de creación de volúmenes del software Element incluyen las siguientes:

Opción	Descripción
size	El tamaño del volumen, de manera predeterminada es 1 GIB o la entrada de configuración... "Valores predeterminados": {"tamaño": "5G"}.
blocksize	Utilice 512 o 4096, de forma predeterminada en 512 o en la entrada de configuración DefaultBlockSize.

## Ejemplo

Consulte el siguiente archivo de configuración de ejemplo con definiciones de QoS:

```
{
  "...": "...",
  "Types": [
    {
      "Type": "Bronze",
      "Qos": {
        "minIOPS": 1000,
        "maxIOPS": 2000,
        "burstIOPS": 4000
      }
    },
    {
      "Type": "Silver",
      "Qos": {
        "minIOPS": 4000,
        "maxIOPS": 6000,
        "burstIOPS": 8000
      }
    },
    {
      "Type": "Gold",
      "Qos": {
        "minIOPS": 6000,
        "maxIOPS": 8000,
        "burstIOPS": 10000
      }
    }
  ]
}
```

En la configuración anterior, tenemos tres definiciones de normas: Bronce, plata y oro. Estos nombres son arbitrarios.

- Cree un volumen Gold de 10 GIB:

```
docker volume create -d solidfire --name sfGold -o type=Gold -o size=10G
```

- Cree un volumen Bronze de 100 GIB:

```
docker volume create -d solidfire --name sfBronze -o type=Bronze -o
size=100G
```

## Recopilar registros

Puede recopilar registros para obtener ayuda con la solución de problemas. El método que se utiliza para recopilar los registros varía en función de cómo se ejecuta el complemento Docker.

### Recopile registros para solucionar problemas

#### Pasos

1. Si está ejecutando Trident usando el método de plugin administrado recomendado (es decir, usando `docker plugin` comandos), véalos de la siguiente manera:

```
docker plugin ls
ID                NAME                DESCRIPTION
ENABLED
4fb97d2b956b     netapp:latest      nDVP - NetApp Docker Volume
Plugin           false
journalctl -u docker | grep 4fb97d2b956b
```

El nivel de registro estándar debe permitirle diagnosticar la mayoría de los problemas. Si encuentra que no es suficiente, puede habilitar el registro de depuración.

2. Para habilitar el registro de depuración, instale el plugin con el registro de depuración activado:

```
docker plugin install netapp/trident-plugin:<version> --alias <alias>
debug=true
```

O bien, active el registro de depuración cuando el plugin ya esté instalado:

```
docker plugin disable <plugin>
docker plugin set <plugin> debug=true
docker plugin enable <plugin>
```

3. Si ejecuta el binario en el host, los registros están disponibles en el host `/var/log/netappdvp` directorio. Para habilitar el registro de depuración, especifique `-debug` al ejecutar el plugin.

### Sugerencias generales para la solución de problemas

- El problema más común en el que se ejecutan los nuevos usuarios es una configuración errónea que impide que el plugin se inicialice. Cuando esto sucede, es probable que vea un mensaje como este

cuando intente instalar o activar el plugin:

```
Error response from daemon: dial unix /run/docker/plugins/<id>/netapp.sock:
connect: no such file or directory
```

Esto significa que el plugin no se pudo iniciar. Afortunadamente, el complemento se ha creado con una completa capacidad de registro que le ayudará a diagnosticar la mayoría de los problemas que es probable que se encuentren.

- Si hay problemas con el montaje de un PV en un contenedor, asegúrese de que `rpcbind` está instalado y en ejecución. Utilice el administrador de paquetes necesario para el sistema operativo del host y compruebe si `rpcbind` está en ejecución. Puede comprobar el estado del servicio `rpcbind` ejecutando un `systemctl status rpcbind` o su equivalente.

## Gestione múltiples instancias de Trident

Se necesitan varias instancias de Trident cuando se desean que varias configuraciones de almacenamiento estén disponibles de forma simultánea. La clave para varias instancias es darles nombres diferentes mediante el `--alias` opción con el plugin en contenedor, o. `--volume-driver` Opción al crear una instancia de Trident en el host.

### Pasos para el complemento gestionado de Docker (versión 1.13/17.03 o posterior)

1. Inicie la primera instancia que especifique un alias y un archivo de configuración.

```
docker plugin install --grant-all-permissions --alias silver
netapp/trident-plugin:21.07 config=silver.json
```

2. Inicie la segunda instancia, especificando un alias y un archivo de configuración distintos.

```
docker plugin install --grant-all-permissions --alias gold
netapp/trident-plugin:21.07 config=gold.json
```

3. Cree volúmenes que especifiquen el alias como el nombre del controlador.

Por ejemplo, para el volumen Gold:

```
docker volume create -d gold --name ntapGold
```

Por ejemplo, en el caso del volumen Silver:

```
docker volume create -d silver --name ntapSilver
```

## Pasos para tradicional (versión 1.12 o anterior)

1. Inicie el plugin con una configuración NFS mediante un ID de controlador personalizado:

```
sudo trident --volume-driver=netapp-nas --config=/path/to/config-nfs.json
```

2. Inicie el plugin con una configuración iSCSI mediante un ID de controlador personalizado:

```
sudo trident --volume-driver=netapp-san --config=/path/to/config-iscsi.json
```

3. Aprovechone volúmenes Docker para cada instancia de controlador:

Por ejemplo, para NFS:

```
docker volume create -d netapp-nas --name my_nfs_vol
```

Por ejemplo, para iSCSI:

```
docker volume create -d netapp-san --name my_iscsi_vol
```

## Opciones de configuración de almacenamiento

Consulte las opciones de configuración disponibles para las configuraciones de Trident.

### Opciones de configuración global

Estas opciones de configuración se aplican a todas las configuraciones de Trident, independientemente de la plataforma de almacenamiento en uso.

Opción	Descripción	Ejemplo
version	Número de versión del archivo de configuración	1
storageDriverName	Nombre del controlador de almacenamiento	ontap-nas, ontap-san, ontap-nas-economy, ontap-nas-flexgroup, solidfire-san

Opción	Descripción	Ejemplo
<code>storagePrefix</code>	Prefijo opcional para los nombres de volúmenes. Valor predeterminado: <code>netappdvp_</code> .	<code>staging_</code>
<code>limitVolumeSize</code>	Restricción opcional de los tamaños de volumen. Valor por defecto: " (no forzado)	<code>10g</code>



No utilizar `storagePrefix` (Incluido el valor predeterminado) para los back-ends de Element. De forma predeterminada, la `solidfire-san` el controlador ignorará este ajuste y no utilizará un prefijo. Se recomienda utilizar un `tenantID` específico para la asignación de volúmenes de Docker o utilizar los datos de atributos que se rellenan con la versión de Docker, la información del controlador y el nombre sin formato de Docker en casos en los que se pueda haber utilizado cualquier comando de asignación de nombres.

Las opciones predeterminadas están disponibles para evitar tener que especificarlas en cada volumen que cree. La `size` la opción está disponible para todos los tipos de controladoras. Consulte la sección ONTAP Configuration para obtener un ejemplo de cómo establecer el tamaño de volumen predeterminado.

Opción	Descripción	Ejemplo
<code>size</code>	Tamaño predeterminado opcional para los nuevos volúmenes. Valor predeterminado: <code>1G</code>	<code>10G</code>

## Configuración de ONTAP

Además de los valores de configuración global anteriores, al utilizar ONTAP, están disponibles las siguientes opciones de nivel superior.

Opción	Descripción	Ejemplo
<code>managementLIF</code>	Dirección IP de LIF de gestión de ONTAP. Es posible especificar un nombre de dominio completo (FQDN).	<code>10.0.0.1</code>



Opción	Descripción	Ejemplo
dataLIF	<p>Dirección IP de LIF de protocolo.</p> <p><b>Controladores NAS ONTAP:</b> Recomendamos especificar dataLIF. Si no se encuentra, Trident recupera los LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos.</p> <p><b>Controladores SAN ONTAP:</b> No se especifica para iSCSI. Trident utiliza "<a href="#">Asignación de LUN selectiva de ONTAP</a>" para descubrir las LIF iSCSI necesarias para establecer una sesión de rutas múltiples. Se genera una advertencia si dataLIF se define explícitamente.</p>	10.0.0.2
svm	Utilizar máquinas virtuales de almacenamiento (necesaria, si LIF de gestión es una LIF de clúster)	svm_nfs
username	Nombre de usuario para conectarse al dispositivo de almacenamiento	vsadmin
password	Contraseña para conectarse al dispositivo de almacenamiento	secret
aggregate	Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el <code>ontap-nas-flexgroup</code> controlador, esta opción se ignora. Todos los agregados asignados a la SVM se usan para aprovisionar un volumen FlexGroup.	aggr1
limitAggregateUsage	Opcional, fallo en el aprovisionamiento si el uso supera este porcentaje	75%

Opción	Descripción	Ejemplo
nfsMountOptions	Control detallado de las opciones de montaje NFS; valor predeterminado es "-o nfsvers=3". <b>Disponible sólo para ontap-nas y.. ontap-nas-economy controladores.</b> <a href="#">Consulte la información de configuración del host NFS aquí</a> .	-o nfsvers=4
igroupName	Trident crea y gestiona por nodo igroups como netappdvp.  Este valor no se puede cambiar ni omitir.  <b>Disponible sólo para ontap-san conductor.</b>	netappdvp
limitVolumeSize	Tamaño máximo de volumen que se puede solicitar.	300g
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300], y el valor predeterminado es 200.  <b>Para ontap-nas-economy Controlador, esta opción permite personalizar el número máximo de qtrees por FlexVol.</b>	300
sanType	<b>Compatible solo para ontap-san el conductor.</b> Utilice para seleccionar <code>iscsi</code> para iSCSI, <code>nvme</code> para NVMe/TCP o <code>fcp</code> para SCSI over Fibre Channel (FC). <b>'fcp' (SCSI sobre FC) es una función de previsualización técnica en la versión Trident 24,10.</b>	<code>iscsi</code> si está en blanco
limitVolumePoolSize	<b>Compatible ontap-san-economy ontap-san-economy solo para conductores y.</b> Limita el tamaño de FlexVol en los controladores económicos de ONTAP ONTAP-nas y ONTAP-SAN.	300g

Las opciones predeterminadas están disponibles para evitar tener que especificarlas en cada volumen que cree:

Opción	Descripción	Ejemplo
spaceReserve	Modo de reserva de espacio; none (con thin provisioning) o volume (grueso)	none
snapshotPolicy	La política de Snapshot que se va a utilizar, el valor predeterminado es none	none
snapshotReserve	Porcentaje de reserva de Snapshot, el valor predeterminado es « » para aceptar el valor predeterminado de ONTAP	10
splitOnClone	Divida un clon de su elemento principal tras su creación (el valor predeterminado es false	false
encryption	<p>Permite el cifrado de volúmenes de NetApp (NVE) en el volumen nuevo; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster.</p> <p>Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE.</p> <p>Para obtener más información, consulte: <a href="#">"Cómo funciona Trident con NVE y NAE"</a>.</p>	verdadero
unixPermissions	La opción de NAS para volúmenes NFS aprovisionados, de forma predeterminada a. 777	777
snapshotDir	Opción NAS para acceder al .snapshot directorio.	"True" para NFSv4 "false" para NFSv3
exportPolicy	La opción de NAS para la política de exportación de NFS que va a utilizar, de forma predeterminada a. default	default
securityStyle	<p>Opción NAS para acceder al volumen NFS aprovisionado.</p> <p>Compatibilidad con NFS mixed y.. unix estilos de seguridad. El valor predeterminado es unix.</p>	unix
fileSystemType	Opción SAN para seleccionar el tipo de sistema de archivos, de forma predeterminada a. ext4	xfs

Opción	Descripción	Ejemplo
tieringPolicy	Política de organización en niveles que se va a utilizar, el valor predeterminado es none; snapshot-only Para configuraciones anteriores a ONTAP 9,5 SVM-DR	none

## Opciones de escala

La `ontap-nas` y `ontap-san` Los controladores crean un ONTAP FlexVol para cada volumen Docker. ONTAP admite un máximo de 1000 FlexVols por nodo del clúster con un máximo de 12,000 FlexVols. Si los requisitos de su volumen de Docker se ajustan a esa limitación, el `ontap-nas` El controlador es la solución NAS preferida debido a las características adicionales que ofrece FlexVols, como las copias Snapshot granulares en Docker-volume y el clonado.

Si necesita más volúmenes de Docker de los que pueden alojar los límites de FlexVol, seleccione la `ontap-nas-economy` o la `ontap-san-economy` controlador.

La `ontap-nas-economy` El controlador crea volúmenes Docker como ONTAP Qtrees dentro de un pool de FlexVols gestionados automáticamente. Qtrees ofrece un escalado mucho mayor, hasta 100,000 por nodo de clúster y 2,400,000 por clúster, a expensas de algunas funciones. La `ontap-nas-economy` El controlador no admite el clonado o copias Snapshot granulares en volúmenes de Docker.



La `ontap-nas-economy` Actualmente, Docker Swarm no admite el controlador, porque Swarm no orqueste la creación de volúmenes entre varios nodos.

La `ontap-san-economy` El controlador crea volúmenes Docker como LUN de ONTAP en un pool compartido de FlexVols gestionados automáticamente. De este modo, cada FlexVol no está restringido a solo un LUN y ofrece una mejor escalabilidad para cargas DE trabajo SAN. Según la cabina de almacenamiento, ONTAP admite hasta 16384 LUN por clúster. Dado que los volúmenes son LUN en el interior, este controlador admite copias Snapshot granulares en Docker y clonado de volúmenes.

Elija `ontap-nas-flexgroup` el controlador para aumentar el paralelismo hacia un único volumen que pueda crecer hasta alcanzar el rango de petabytes con miles de millones de archivos. Algunos casos de uso ideales para FlexGroups incluyen IA/ML/DL, Big Data y análisis, creación de software, streaming, repositorios de archivos, etc. Trident utiliza todos los agregados asignados a una SVM cuando se aprovisiona un volumen de FlexGroup. La compatibilidad con FlexGroup en Trident también tiene las siguientes consideraciones:

- Requiere ONTAP versión 9.2 o posterior.
- En el momento en el que se ha redactado este documento, FlexGroups solo admite NFS v3.
- Se recomienda habilitar los identificadores de NFSv3 de 64 bits para la SVM.
- El tamaño mínimo de miembro/volumen de FlexGroup recomendado es de 100GiB.
- No se admite la clonado para los volúmenes de FlexGroup.

Para obtener información sobre las instancias de FlexGroup y las cargas de trabajo adecuadas para las instancias de FlexGroup, consulte la ["Prácticas recomendadas y guía de implementación de NetApp FlexGroup para volúmenes"](#).

Para obtener funciones avanzadas y obtener un enorme escalado en el mismo entorno, puede ejecutar varias instancias del complemento para volúmenes de Docker, utilizando una `ontap-nas` y otro uso `ontap-nas-economy`.

## Rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privilegios mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "[Generador de roles personalizados de Trident](#)" para obtener más información sobre la creación de roles personalizados de Trident.

### Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

2. Cree un nombre de usuario para el usuario de Trident:

```
security login create -username <user_name\> -application ontapi  
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver  
<svm_name\> -comment "user_description"
```

3. Asignar el rol al usuario:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

### Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado:**

- a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

(O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > required svm > Settings > Users and Roles**.

- b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.
- c. Seleccione **+Agregar en Roles**.
- d. Defina las reglas para el rol y haga clic en **Guardar**.

2. **Asignar el rol al usuario de Trident:** + Realizar los siguientes pasos en la página **Usuarios y Roles**:

- a. Seleccione Agregar icono + en **Usuarios**.
- b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.
- c. Haga clic en **Guardar**.

Consulte las siguientes páginas si quiere más información:

- ["Roles personalizados para la administración de ONTAP"](#) o ["Definir funciones personalizadas"](#)
- ["Trabajar con roles y usuarios"](#)

## Archivos de configuración de ONTAP de ejemplo

### Ejemplo de NFS para `ontap-nas` el controlador

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "defaults": {
    "size": "10G",
    "spaceReserve": "none",
    "exportPolicy": "default"
  }
}
```

### Ejemplo de NFS para `ontap-nas-flexgroup` el controlador

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "defaults": {
    "size": "100G",
    "spaceReserve": "none",
    "exportPolicy": "default"
  }
}
```

### Ejemplo de NFS para `ontap-nas-economy` el controlador

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1"
}
```

### Ejemplo de iSCSI para `ontap-san` el controlador

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "igroupName": "netappdvp"
}
```

### Ejemplo de NFS para `ontap-san-economy` el controlador

```
{
  "version": 1,
  "storageDriverName": "ontap-san-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi_eco",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "igroupName": "netappdvp"
}
```

## Ejemplo de NVMe/TCP para <code>ontap-san</code> controlador

```
{
  "version": 1,
  "backendName": "NVMeBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nvme",
  "username": "vsadmin",
  "password": "password",
  "sanType": "nvme",
  "useREST": true
}
```

## Configuración del software Element

Además de los valores de configuración global, cuando se utiliza el software Element (HCI/SolidFire de NetApp), existen estas opciones disponibles.

Opción	Descripción	Ejemplo
Endpoint	https://<login>:<password>@<mvip>/json-rpc/<element-version>	https://admin:admin@192.168.160.3/json-rpc/8.0
SVIP	Puerto y dirección IP de iSCSI	10.0.0.7:3260
TenantName	Debe utilizar el inquilino SolidFireF (creado si no encontrado)	docker
InitiatorIFace	Especifique la interfaz cuando restrinja el tráfico de iSCSI a una interfaz no predeterminada	default
Types	Especificaciones de calidad de servicio	Vea el ejemplo siguiente
LegacyNamePrefix	Prefijo para instalaciones actualizadas de Trident. Si utilizó una versión de Trident anterior a la 1.3.2 y realizó una actualización con volúmenes existentes, deberá configurar este valor para acceder a los volúmenes antiguos que se asignaron a través del método de nombre del volumen.	netappdvp-



La `solidfire-san` El controlador no es compatible con Docker Swarm.

## Ejemplo del archivo de configuración del software Element

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://admin:admin@192.168.160.3/json-rpc/8.0",
  "SVIP": "10.0.0.7:3260",
  "TenantName": "docker",
  "InitiatorIFace": "default",
  "Types": [
    {
      "Type": "Bronze",
      "Qos": {
        "minIOPS": 1000,
        "maxIOPS": 2000,
        "burstIOPS": 4000
      }
    },
    {
      "Type": "Silver",
      "Qos": {
        "minIOPS": 4000,
        "maxIOPS": 6000,
        "burstIOPS": 8000
      }
    },
    {
      "Type": "Gold",
      "Qos": {
        "minIOPS": 6000,
        "maxIOPS": 8000,
        "burstIOPS": 10000
      }
    }
  ]
}
```

## Problemas y limitaciones conocidos

Busque información sobre problemas conocidos y limitaciones cuando use Trident con Docker.

**Si se actualiza el complemento Trident Docker Volume Plugin a 20.10 y versiones posteriores, se produce un error de actualización sin dicho archivo o directorio.**

#### Solución alternativa

1. Desactivar el plugin.

```
docker plugin disable -f netapp:latest
```

2. Quitar el plugin.

```
docker plugin rm -f netapp:latest
```

3. Vuelva a instalar el plugin proporcionando el extra `config` parámetro.

```
docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant  
-all-permissions config=config.json
```

**Los nombres de volumen deben tener una longitud mínima de 2 caracteres.**



Esta es una limitación de cliente de Docker. El cliente interpretará un nombre de carácter único como una ruta de Windows. ["Consulte el error 25773"](#).

**Docker Swarm tiene ciertos comportamientos que impiden que Trident ofrezca compatibilidad con cada combinación de almacenamiento y controladores.**

- Docker Swarm actualmente utiliza el nombre del volumen en lugar del ID de volumen como su identificador de volumen único.
- Las solicitudes de volúmenes se envían simultáneamente a cada nodo de un clúster Swarm.
- Los plugins de volúmenes (incluido Trident) deben ejecutarse de forma independiente en cada nodo de un clúster de Swarm. Debido a la forma en que funciona ONTAP y cómo funcionan los `ontap-nas` controladores y `ontap-san`, son los únicos que pueden operar dentro de estas limitaciones.

El resto de los conductores están sujetos a problemas como las condiciones de la carrera que pueden dar lugar a la creación de un gran número de volúmenes para una sola solicitud sin un claro "ganador"; por ejemplo, Element tiene una función que permite que los volúmenes tengan el mismo nombre pero ID diferentes.

NetApp ha proporcionado comentarios al equipo de Docker, pero no tiene ningún indicio de recurso futuro.

**Si se está provisionando un FlexGroup, ONTAP no aprovisiona una segunda FlexGroup si el segundo FlexGroup tiene uno o más agregados en común con el FlexGroup que se está aprovisionando.**

# Prácticas recomendadas y recomendaciones

## Puesta en marcha

Utilice las recomendaciones que se enumeran aquí al implementar Trident.

### Póngalo en marcha a un espacio de nombres dedicado

"Espacios de nombres" proporcionar separación administrativa entre diferentes aplicaciones y constituyen una barrera para el uso compartido de recursos. Por ejemplo, una RVP de un espacio de nombres no se puede consumir de otro. Trident proporciona recursos PV a todos los espacios de nombres del clúster de Kubernetes y, en consecuencia, aprovecha una cuenta de servicio que ha elevado el número de Privileges.

Además, el acceso al pod de Trident puede permitir a un usuario acceder a las credenciales del sistema de almacenamiento y a otra información confidencial. Es importante asegurarse de que los usuarios de aplicaciones y aplicaciones de gestión no tengan la capacidad de acceder a las definiciones de objetos de Trident o a los pods mismos.

### Utilice cuotas y límites de rango para controlar el consumo de almacenamiento

Kubernetes cuenta con dos funciones que, al combinarse, ofrecen un potente mecanismo que limita el consumo de recursos que consumen las aplicaciones. La "mecanismo de cuotas de almacenamiento" permite al administrador implementar límites de consumo globales, específicos para las clases de almacenamiento, de capacidad y de recuento de objetos en función del espacio de nombres. Además, utilizando un "límite de rango" Garantiza que las solicitudes de PVC se encuentren dentro de un valor mínimo y máximo antes de reenviar la solicitud al proveedor.

Estos valores se definen por espacio de nombres, lo que significa que cada espacio de nombres debe tener valores definidos que se ajustan a los requisitos de sus recursos. Consulte aquí para obtener más información acerca de "cómo aprovechar las cuotas".

## Configuración del almacenamiento

Cada plataforma de almacenamiento de la cartera de NetApp tiene unas funciones únicas que benefician a las aplicaciones, en contenedores o no.

### Descripción general de la plataforma

Trident funciona con ONTAP y Element. No existe una plataforma que se adapte mejor a todas las aplicaciones y escenarios que otra, sin embargo, las necesidades de la aplicación y el equipo que administra el dispositivo deben tenerse en cuenta al elegir una plataforma.

Debe seguir las prácticas recomendadas de base para el sistema operativo del host con el protocolo que está aprovechando. Opcionalmente, es posible que desee considerar la incorporación de prácticas recomendadas para las aplicaciones, cuando esté disponible, con configuración de back-end, clase de almacenamiento y RVP para optimizar el almacenamiento para aplicaciones específicas.

### Prácticas recomendadas para ONTAP y Cloud Volumes ONTAP

Conozca las prácticas recomendadas para configurar ONTAP y Cloud Volumes ONTAP para Trident.

Las siguientes recomendaciones son directrices para configurar ONTAP para cargas de trabajo en contenedores, que consumen volúmenes aprovisionados de forma dinámica por Trident. Cada uno de ellos debe considerarse y evaluarse según la idoneidad de su entorno.

### Utilice SVM dedicadas a Trident

Las máquinas virtuales de almacenamiento (SVM) proporcionan separación de tareas administrativas y de aislamiento entre clientes en un sistema ONTAP. Dedicar una SVM a las aplicaciones permite delegar privilegios y aplicar prácticas recomendadas para limitar el consumo de recursos.

Existen varias opciones disponibles para la gestión de la SVM:

- Proporcione la interfaz de gestión del clúster en la configuración del back-end, junto con las credenciales adecuadas, y especifique el nombre de la SVM.
- Cree una interfaz de gestión dedicada para la SVM mediante ONTAP System Manager o la CLI.
- Comparta la función de gestión con una interfaz de datos NFS.

En cada caso, la interfaz debe estar en DNS, y se debe usar el nombre DNS al configurar Trident. Esto permite facilitar algunas situaciones de recuperación ante desastres, por ejemplo, SVM-DR sin retención de identidad de red.

No tiene ninguna preferencia entre tener una LIF de gestión dedicada o compartida para la SVM, sin embargo, debe asegurarse de que las políticas de seguridad de red se alineen con el enfoque que elija. Sin embargo, debería accederse a la LIF de gestión a través de DNS para facilitar la máxima flexibilidad que debería tener ["SVM-DR"](#) Se podrá usar en combinación con Trident.

### Limite el número máximo de volúmenes

Los sistemas de almacenamiento de ONTAP tienen un número máximo de volúmenes, que varía en función de la versión del software y la plataforma de hardware. Consulte ["Hardware Universe de NetApp"](#) Para su plataforma y versión de ONTAP específica, determine los límites exactos. Cuando se agota el número de volúmenes, las operaciones de aprovisionamiento fallan no solo para Trident, sino para todas las solicitudes de almacenamiento.

De Trident `ontap-nas` y `ontap-san` Los controladores aprovisionan un FlexVolume para cada volumen persistente (PV) de Kubernetes que se crea. La `ontap-nas-economy` El controlador crea aproximadamente un FlexVolume por cada 200 VP (configurable entre 50 y 300). La `ontap-san-economy` El controlador crea aproximadamente un FlexVolume por cada 100 VP (configurable entre 50 y 200). Para evitar que Trident consuma todos los volúmenes disponibles en el sistema de almacenamiento, debe establecer un límite en la SVM. Puede hacerlo desde la línea de comandos:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

Valor para `max-volumes` varía en función de varios criterios específicos de su entorno:

- El número de volúmenes existentes en el clúster de ONTAP
- El número de volúmenes que espera aprovisionar fuera de Trident para otras aplicaciones
- El número de volúmenes persistentes que tienen previsto consumir las aplicaciones de Kubernetes

La `max-volumes` El valor es el total de volúmenes aprovisionados en todos los nodos del clúster de ONTAP, no en un nodo ONTAP individual. Como resultado, es posible que encuentre algunas condiciones en las que

un nodo de un clúster de ONTAP pueda tener muchos más o menos volúmenes provisionados de Trident que otro nodo.

Por ejemplo, un clúster ONTAP de dos nodos tiene la capacidad de alojar un máximo de 2000 FlexVolumes. Tener el recuento de volumen máximo establecido en 1250 parece muy razonable. Sin embargo, si solo "agregados" De un nodo se asigna a la SVM, o los agregados asignados de un nodo no se pueden aprovisionar con (por ejemplo, debido a capacidad), el otro nodo se convierte en el destino para todos los volúmenes provisionados de Trident. Esto significa que es posible alcanzar el límite de volumen para ese nodo antes que el `max-volumes`. Se alcanza el valor, lo que repercute tanto en Trident como en otras operaciones de volúmenes que utilizan ese nodo. **Puede evitar esta situación asegurándose de que los agregados de cada nodo del clúster están asignados a la SVM que utiliza Trident en los mismos números.**

### Limite el tamaño máximo de los volúmenes que ha creado Trident

Para configurar el tamaño máximo de los volúmenes que Trident puede crear `limitVolumeSize` parámetro en la `backend.json` definición.

Además de controlar el tamaño del volumen en la cabina de almacenamiento, también se deben aprovechar las capacidades de Kubernetes.

### Limite el tamaño máximo de FlexVols creados por Trident

Para configurar el tamaño máximo para FlexVols utilizados como pools para los controladores ONTAP-san-economy y ONTAP-nas-economy, utilice el `limitVolumePoolSize` parámetro en su `backend.json` definición.

### Configure Trident para utilizar CHAP bidireccional

Puede especificar los nombres de iniciador CHAP y de usuario de destino y las contraseñas en la definición de back-end, y hacer que Trident habilite CHAP en la SVM. Con el `useCHAP` Parámetro en la configuración de back-end, Trident autentica las conexiones iSCSI para los back-ends de ONTAP con CHAP.

### Cree y utilice una política de calidad de servicio de SVM

Al aprovechar una política de calidad de servicio de ONTAP, aplicada a la SVM, se limita el número de IOPS consumibles por los volúmenes provisionados de Trident. Esto ayuda a. "prevenir un matón" O un contenedor fuera de control que no afecta a las cargas de trabajo fuera de la SVM de Trident.

Puede crear una política de calidad de servicio para la SVM en unos pasos. Consulte la documentación de su versión de ONTAP para obtener la información más precisa. El ejemplo siguiente crea una política de calidad de servicio que limita el total de IOPS disponibles para la SVM a 5000.

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

Además, si su versión de ONTAP admite esta función, puede considerar el uso de una calidad de servicio

mínima para garantizar un volumen del rendimiento para cargas de trabajo en contenedores. La calidad de servicio adaptativa no es compatible con una política de nivel de SVM.

El número de IOPS dedicado a las cargas de trabajo de los contenedores depende de muchos aspectos. Entre otras cosas, estas incluyen:

- Otras cargas de trabajo que utilizan la cabina de almacenamiento. Si hay otras cargas de trabajo, no relacionadas con la puesta en marcha de Kubernetes, y que utilizan los recursos de almacenamiento, se debe tener cuidado para garantizar que esas cargas de trabajo no se vean afectadas de forma accidental.
- Cargas de trabajo esperadas que se ejecutan en contenedores. Si las cargas de trabajo que tienen requisitos de IOPS elevados se ejecutan en contenedores, una política de calidad de servicio baja resulta en una mala experiencia.

Es importante recordar que una política de calidad de servicio asignada en el nivel de la SVM da como resultado que todos los volúmenes provisionados a la SVM compartan el mismo pool de IOPS. Si una, o una cifra pequeña, de las aplicaciones con contenedores tienen un requisito elevado de IOPS, podría convertirse en un problema para las otras cargas de trabajo con contenedores. Si este es el caso, puede que se desee considerar utilizar la automatización externa para asignar políticas de calidad de servicio por volumen.



Debe asignar el grupo de políticas QoS al SVM **only** si la versión de ONTAP es anterior a 9.8.

### Cree grupos de políticas de calidad de servicio para Trident

La calidad de servicio garantiza que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo de la competencia. Los grupos de políticas de calidad de servicio de ONTAP proporcionan opciones de calidad de servicio para volúmenes y permiten a los usuarios definir el techo de rendimiento para una o más cargas de trabajo. Para obtener más información sobre la calidad de servicio, consulte ["Rendimiento garantizado con QoS"](#).

Puede especificar grupos de políticas de calidad de servicio en el back-end o en un pool de almacenamiento y se aplican a cada volumen creado en ese pool o back-end.

ONTAP tiene dos tipos de grupos de políticas de calidad de servicio: Tradicionales y adaptativos. Los grupos de políticas tradicionales proporcionan un rendimiento máximo (o mínimo, en versiones posteriores) plano en IOPS. La calidad de servicio adaptativa escala automáticamente el rendimiento al tamaño de la carga de trabajo y mantiene la ratio de IOPS en TB|GB a medida que el tamaño de la carga de trabajo cambia. Esto supone una ventaja significativa cuando se gestionan cientos o miles de cargas de trabajo en una puesta en marcha de gran tamaño.

Tenga en cuenta lo siguiente al crear grupos de políticas de calidad de servicio:

- Debe configurar la `qosPolicy` introduzca la `defaults` bloque de la configuración del back-end. Consulte el siguiente ejemplo de configuración del back-end:

```

---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
- labels:
  performance: extreme
  defaults:
  adaptiveQosPolicy: extremely-adaptive-pg
- labels:
  performance: premium
  defaults:
  qosPolicy: premium-pg

```

- Debe aplicar los grupos de políticas por volumen, de modo que cada volumen obtenga el rendimiento entero según lo especifique el grupo de políticas. No se admiten los grupos de políticas compartidas.

Para obtener más información sobre los grupos de políticas de calidad de servicio, consulte ["Comandos de calidad de servicio de ONTAP 9.8"](#).

### Limite el acceso a recursos de almacenamiento a los miembros del clúster de Kubernetes

La limitación del acceso a los volúmenes NFS y a las LUN de iSCSI creadas por Trident es un componente crucial del sistema de seguridad para la puesta en marcha de Kubernetes. Si lo hace, se evita que los hosts que no forman parte del clúster de Kubernetes accedan a los volúmenes y que potencialmente modifiquen los datos de forma inesperada.

Es importante comprender que los espacios de nombres son el límite lógico de los recursos en Kubernetes. Se supone que los recursos del mismo espacio de nombres se pueden compartir; sin embargo, es importante destacar que no existe ninguna funcionalidad entre espacios de nombres. Esto significa que aunque los VP sean objetos globales, cuando están enlazados a una RVP solo pueden acceder a ellos mediante POD que están en el mismo espacio de nombres. **Es fundamental asegurarse de que los espacios de nombres se utilizan para proporcionar la separación cuando sea apropiado.**

La preocupación principal de la mayoría de las organizaciones con respecto a la seguridad de los datos en un contexto de Kubernetes es que un proceso en un contenedor puede acceder al almacenamiento montado en el host, pero que no está destinado al contenedor. ["Espacios de nombres"](#) están diseñados para evitar este tipo de compromiso. Sin embargo, hay una excepción: Contenedores privilegiados.

Un contenedor con privilegios es uno que se ejecuta con mucho más permisos de nivel de host de lo normal. No se deniegan de forma predeterminada, por lo que debe desactivar la funcionalidad utilizando ["directivas de seguridad de pod"](#).

Para los volúmenes en los que se desea obtener acceso tanto a los hosts de Kubernetes como a los externos,

el almacenamiento se debe gestionar de forma tradicional, con el VP introducido por el administrador, y no gestionado por Trident. Esto garantiza que el volumen de almacenamiento se destruya solo cuando tanto los hosts de Kubernetes como los externos se desconectaron y ya no utilizan el volumen. Además, se puede aplicar una política de exportación personalizada, lo que permite el acceso desde los nodos del clúster de Kubernetes y los servidores objetivo fuera del clúster de Kubernetes.

Para las implementaciones que tienen nodos de infraestructura dedicados (por ejemplo, OpenShift) u otros nodos que no pueden programar aplicaciones de usuario, se deben utilizar directivas de exportación independientes para limitar aún más el acceso a los recursos de almacenamiento. Esto incluye la creación de una directiva de exportación para los servicios que se implementan en dichos nodos de infraestructura (por ejemplo, los servicios de registro y métricas de OpenShift) y aplicaciones estándar que se implementan en nodos que no son de infraestructura.

### Usar una política de exportación dedicada

Debe asegurarse de que existe una política de exportación para cada back-end que solo permita el acceso a los nodos presentes en el clúster de Kubernetes. Trident puede crear y gestionar automáticamente políticas de exportación. De esta forma, Trident limita el acceso a los volúmenes que aprovisiona a los nodos en el clúster de Kubernetes y simplifica la adición o la eliminación de nodos.

También puede crear una política de exportación manualmente y rellenarla con una o varias reglas de exportación que procesarán cada solicitud de acceso a nodo:

- Utilice la `vserver export-policy create` Comando de la interfaz de línea de comandos de ONTAP para crear la política de exportación.
- Añada reglas a la política de exportación mediante la `vserver export-policy rule create` Comando de la CLI de ONTAP.

Si ejecuta estos comandos, puede restringir el acceso de los nodos de Kubernetes a los datos.

### Desactivar `showmount` Para la SVM de la aplicación

La `showmount` Con la función, un cliente NFS puede consultar a la SVM para obtener una lista de exportaciones NFS disponibles. Un pod puesto en marcha en el clúster de Kubernetes puede ejecutar el `showmount -e` Comando en la LIF de datos y recibe una lista de montajes disponibles, incluidos los a los que no tiene acceso. Aunque esto, por sí solo, no supone un compromiso con la seguridad, proporciona información innecesaria, potencialmente que ayuda a un usuario no autorizado a conectarse con una exportación NFS.

Debe desactivar `showmount` Con el comando CLI de ONTAP a nivel de la SVM:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## Mejores prácticas para SolidFire

Conozca las prácticas recomendadas para configurar el almacenamiento de SolidFire para Trident.

### Crear cuenta de SolidFire

Cada cuenta SolidFire representa un propietario de volumen único y recibe su propio conjunto de credenciales de protocolo de autenticación por desafío mutuo (CHAP). Es posible acceder a los volúmenes asignados a una cuenta mediante el nombre de cuenta y las credenciales CHAP relativas o un grupo de acceso de



volúmenes. Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

### Cree una política de calidad de servicio

Utilice las políticas de calidad de servicio de SolidFire si desea crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes.

Puede establecer parámetros de calidad de servicio por cada volumen. El rendimiento de cada volumen se puede garantizar mediante el establecimiento de tres parámetros configurables que definen la calidad de servicio: Min IOPS, Max IOPS y Burst IOPS.

Aquí pueden ver los valores mínimos, máximos y de ráfaga de IOPS en relación con el tamaño de bloque de 4 KB.

Parámetro IOPS	Definición	Espacio valor	Valor predeterminado	Capacidad Valor (4 KB)
IOPS mín	El nivel garantizado de rendimiento de un volumen.	50	50	15000
Tasa máx. De IOPS	El rendimiento no superará este límite.	50	15000	200,000
IOPS de ráfaga	IOPS máximo permitido en un escenario de ráfaga breve.	50	15000	200,000



Aunque Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000, el rendimiento máximo en el mundo real de un volumen se ve limitado por el uso del clúster y el rendimiento por cada nodo.

El tamaño de bloque y el ancho de banda influyen directamente en el número de IOPS. A medida que estos aumenten, el sistema aumentará el ancho de banda hasta el nivel que necesite para procesar los tamaños de bloque más grandes. A medida que aumenta el ancho de banda, se reduce el número de IOPS que el sistema es capaz de conseguir. Consulte "[Calidad de servicio de SolidFire](#)" Para obtener más información sobre la calidad de servicio y el rendimiento.

### Autenticación SolidFire

Element admite dos métodos para la autenticación: CHAP y grupos de acceso de volumen (VAG). CHAP utiliza el protocolo CHAP para autenticar el host al back-end. Los grupos de acceso de volúmenes controlan el acceso a los volúmenes que aprovisiona. NetApp recomienda utilizar CHAP para la autenticación, ya que es más sencillo y sin límites de escalado.



Trident con el proveedor CSI mejorado admite el uso de la autenticación CHAP. Los VAG sólo deben utilizarse en el modo de funcionamiento tradicional no CSI.

La autenticación CHAP (verificación de que el iniciador es el usuario de volumen objetivo) solo se admite con control de acceso basado en la cuenta. Si se utiliza CHAP para la autenticación, hay dos opciones

disponibles: CHAP unidireccional y CHAP bidireccional. CHAP unidireccional autentica el acceso al volumen mediante el nombre de cuenta de SolidFire y el secreto de iniciador. La opción CHAP bidireccional proporciona la manera más segura de autenticar el volumen, ya que el volumen autentica el host a través del nombre de cuenta y el secreto de iniciador, y luego el host autentica el volumen por medio del nombre de cuenta y el secreto de destino.

Sin embargo, si no se puede habilitar CHAP y se requieren los VAG, cree el grupo de acceso y añada los iniciadores de host y los volúmenes al grupo de acceso. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo con o sin autenticación CHAP. Si el iniciador de iSCSI está configurado para utilizar la autenticación CHAP, se utiliza el control de acceso basado en cuentas. Si el iniciador iSCSI no está configurado para utilizar la autenticación CHAP, se utiliza el control de acceso del grupo de acceso de volúmenes.

## ¿Dónde encontrar más información?

A continuación se enumeran algunas de las prácticas recomendadas. Busque en el ["Biblioteca de NetApp"](#) para las versiones más actuales.

### ONTAP

- ["Prácticas recomendadas y guía de implementación de NFS"](#)
- ["Guía de administración de SAN" \(Para iSCSI\)](#)
- ["Configuración exprés de iSCSI para RHEL"](#)

### Software Element

- ["Configuración de SolidFire para Linux"](#)

### NetApp HCI

- ["Requisitos previos de la implementación de NetApp HCI"](#)
- ["Acceda al motor de implementación de NetApp"](#)

### Información sobre las prácticas recomendadas de la aplicación

- ["Prácticas recomendadas para MySQL en ONTAP"](#)
- ["Prácticas recomendadas para MySQL en SolidFire"](#)
- ["NetApp SolidFire y Cassandra"](#)
- ["Prácticas recomendadas de Oracle en SolidFire"](#)
- ["Prácticas recomendadas de PostgreSQL en SolidFire"](#)

No todas las aplicaciones tienen directrices específicas, es importante trabajar con su equipo de NetApp y utilizar el ["Biblioteca de NetApp"](#) para encontrar la documentación más actualizada.

## Integre Trident

Para integrar Trident, los siguientes elementos de diseño y arquitectura requieren integración: Selección y puesta en marcha de controladores, diseño de la clase de almacenamiento, diseño de pools virtuales, reclamación de volumen persistente (RVP) impactos en el aprovisionamiento de almacenamiento, operaciones de volúmenes y

puesta en marcha de servicios OpenShift mediante Trident.

## Selección y despliegue del conductor

Seleccione e implemente un controlador de back-end para el sistema de almacenamiento.

### Controladores de entorno de administración ONTAP

Los controladores de entorno de administración de ONTAP se diferencian por el protocolo utilizado y cómo se aprovisionan los volúmenes en el sistema de almacenamiento. Por lo tanto, tenga cuidado al decidir qué controlador implementar.

En un nivel superior, si la aplicación cuenta con componentes que necesitan almacenamiento compartido (varios POD que acceden al mismo PVC), los controladores basados en NAS serán la opción predeterminada, mientras que los controladores iSCSI basados en bloques satisfacen las necesidades de almacenamiento no compartido. Elija el protocolo según los requisitos de la aplicación y el nivel de comodidad de los equipos de almacenamiento e infraestructura. Por lo general, existe poca diferencia entre ellas para la mayoría de las aplicaciones, con tanta frecuencia la decisión se basa en si se necesita o no almacenamiento compartido (donde más de un pod necesitará acceso simultáneo).

Los controladores de entorno de administración de ONTAP disponibles son:

- `ontap-nas`: Cada PV aprovisionado es un FlexVolume ONTAP completo.
- `ontap-nas-economy`: Cada PV aprovisionado es un qtree, con un número configurable de qtrees por FlexVolume (el valor predeterminado es 200).
- `ontap-nas-flexgroup`: Cada VP aprovisionado como ONTAP FlexGroup completo y se utilizan todos los agregados asignados a una SVM.
- `ontap-san`: Cada PV aprovisionado es una LUN dentro de su propio FlexVolume.
- `ontap-san-economy`: Cada VP aprovisionado es una LUN, con un número configurable de LUN por FlexVolume (el valor predeterminado es 100).

La elección entre los tres controladores NAS tiene algunas ramificaciones a las funciones, que están disponibles para la aplicación.

Tenga en cuenta que, en las siguientes tablas, no todas las capacidades se exponen a través de Trident. El administrador de almacenamiento debe aplicar algunas después del aprovisionamiento si se desea disponer de esta funcionalidad. Las notas al pie de la superíndice distinguen la funcionalidad por característica y controlador.

Unidades NAS de ONTAP	Snapshot	Clones	Políticas de exportación dinámicas	Conexión múltiple	Calidad de servicio	Cambie el tamaño	Replicación
<code>ontap-nas</code>	Sí	Sí	Yespie de página:5[]	Sí	Yespie de página:1[]	Sí	Yespie de página:1[]
<code>ontap-nas-economy</code>	Yespie de página:3[]	Yespie de página:3[]	Yespie de página:5[]	Sí	Yespie de página:3[]	Sí	Yespie de página:3[]
<code>ontap-nas-flexgroup</code>	Yespie de página:1[]	No	Yespie de página:5[]	Sí	Yespie de página:1[]	Sí	Yespie de página:1[]

Trident ofrece 2 controladores SAN para ONTAP, cuyas funcionalidades se muestran a continuación.

Unidades SAN de ONTAP	Snapshot	Clones	Conexión múltiple	CHAP bidireccional	Calidad de servicio	Cambie el tamaño	Replicación
ontap-san	Sí	Sí	Yespie de página:4[]	Sí	Yespie de página:1[]	Sí	Yespie de página:1[]
ontap-san-economy	Sí	Sí	Yespie de página:4[]	Sí	Yespie de página:3[]	Sí	Yespie de página:3[]

Nota al pie de las tablas anteriores: Yes [1]: No administrado por Trident Yes [2]: Administrado por Trident, pero no por PV granular Yes [3]: No gestionado por Trident y no por PV granular Yes [4]: Soportado para volúmenes de bloque sin procesar Yes [5]: Soportado por Trident

Las funciones que no son granulares en los VP se aplican a todo el FlexVolume y todos los VP (es decir, qtrees o LUN de FlexVols compartidos) compartirán un programa común.

Como podemos ver en las tablas anteriores, gran parte de la funcionalidad entre `ontap-nas` y `ontap-nas-economy` es lo mismo. Sin embargo, porque la `ontap-nas-economy` Esta unidad limita la capacidad de controlar la programación con una granularidad VP, lo que puede afectar a su planificación de backup y recuperación ante desastres en concreto. En el caso de los equipos de desarrollo que desean aprovechar la funcionalidad de clonado de PVC en el almacenamiento de ONTAP, esto solo es posible cuando se utiliza la `ontap-nas`, `ontap-san` o `ontap-san-economy` de windows



La `solidfire-san` El controlador también es capaz de clonar EVs.

### Controladores de entorno de administración Cloud Volumes ONTAP

Cloud Volumes ONTAP proporciona control de datos junto con funciones de almacenamiento empresarial para diversos casos de uso, como recursos compartidos de archivos y almacenamiento a nivel de bloque que presta servicio a protocolos NAS y SAN (NFS, SMB/CIFS e iSCSI). Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas`, `ontap-nas-economy`, `ontap-san` y `ontap-san-economy`. Estos son aplicables a Cloud Volume ONTAP para Azure, Cloud Volume ONTAP para GCP.

### Controladores de entorno de administración de Amazon FSX para ONTAP

Amazon FSx para NetApp ONTAP te permite aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp que ya conoces, a la vez que aprovechas la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX para ONTAP es compatible con muchas funciones del sistema de archivos ONTAP y API de administración. Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup`, `ontap-san` y `ontap-san-economy`.

### Controladores de back-end de HCI/SolidFire de NetApp

La `solidfire-san` El controlador que se utiliza con las plataformas HCI/SolidFire de NetApp, ayuda al administrador a configurar un back-end de Element para Trident según los límites de calidad de servicio. Si desea diseñar el back-end de modo que establezca los límites de calidad de servicio específicos en los volúmenes aprovisionados por Trident, utilice la `type` parámetro en el archivo back-end. El administrador

también puede restringir el tamaño del volumen que podría crearse en el almacenamiento mediante el `limitVolumeSize` parámetro. Actualmente, las funciones de almacenamiento de Element, como el cambio de tamaño de volumen y la replicación de volumen, no se admiten mediante el `solidfire-san` controlador. Estas operaciones se deben realizar manualmente mediante la interfaz de usuario web del software Element.

Controlador SolidFire	Snapshot	Clones	Conexión múltiple	CHAP	Calidad de servicio	Cambie el tamaño	Replicación
<code>solidfire-san</code>	Sí	Sí	Yespie de página:2[]	Sí	Sí	Sí	Yespie de página:1[]

Nota al pie de página: Yes [1]: No gestionado por Trident Yes [2]: Compatible con volúmenes de bloque sin procesar

### Controladores de entorno de administración Azure NetApp Files

Trident utiliza `azure-netapp-files` el controlador para administrar "Azure NetApp Files" el servicio.

Puede encontrar más información sobre este controlador y cómo configurarlo en "Configuración de backend de Trident para Azure NetApp Files".

Controlador Azure NetApp Files	Snapshot	Clones	Conexión múltiple	Calidad de servicio	Expanda	Replicación
<code>azure-netapp-files</code>	Sí	Sí	Sí	Sí	Sí	Yespie de página:1[]

Nota al pie de página: YesFootnote:1[]: No administrado por Trident

### Cloud Volumes Service en el controlador back-end de Google Cloud

Trident usa `gcp-cvs` el controlador para asociarse con el Cloud Volumes Service en Google Cloud.

```
`gcp-cvs`El controlador utiliza pools virtuales para abstraer el back-end y permitir que Trident determine la ubicación del volumen. El administrador define los pools virtuales de los `backend.json` archivos. Las clases de almacenamiento utilizan selectores para identificar los pools virtuales por etiqueta.
```

- Si los pools virtuales están definidos en el backend, Trident intentará crear un volumen en los pools de almacenamiento de Google Cloud a los que esos pools virtuales están limitados.
- Si los pools virtuales no están definidos en el backend, Trident seleccionará un pool de almacenamiento de Google Cloud de los pools de almacenamiento disponibles en la región.

Para configurar el backend de Google Cloud en Trident, debe especificar `projectNumber`, `apiRegion` y `apiKey` en el archivo backend. Puede encontrar el número de proyecto en la consola de Google Cloud. La clave API se obtiene del archivo de claves privadas de la cuenta de servicio que creó al configurar el acceso de API para Cloud Volumes Service en Google Cloud.

Para obtener más información sobre los tipos de servicio y los niveles de servicio de Cloud Volumes Service en Google Cloud, consulte ["Obtén más información sobre el soporte de Trident para CVS para GCP"](#).

Controlador de Cloud Volumes Service para Google Cloud	Snapshot	Clones	Conexión múltiple	Calidad de servicio	Expanda	Replicación
gcp-cvs	Sí	Sí	Sí	Sí	Sí	Disponible solo en el tipo de servicio CVS-Performance.



#### Notas de replicación

- Trident no gestiona la replicación.
- El clon se creará en el mismo pool de almacenamiento que el volumen de origen.

## Diseño de clase de almacenamiento

Las clases de almacenamiento individuales deben configurarse y aplicarse para crear un objeto de clase de almacenamiento Kubernetes. En esta sección se analiza cómo diseñar una clase de almacenamiento para su aplicación.

### Utilización de back-end específica

El filtrado se puede usar en un objeto de clase de almacenamiento específico para determinar el pool o conjunto de pools de almacenamiento que se utilizarán con esa clase de almacenamiento específica. Se pueden establecer tres conjuntos de filtros en la clase de almacenamiento: `storagePools`, `additionalStoragePools`, y/o. `excludeStoragePools`.

```
`storagePools`El parámetro ayuda a restringir el almacenamiento al conjunto de pools que coinciden con los atributos especificados.  
`additionalStoragePools`El parámetro se utiliza para ampliar el conjunto de pools que Trident utiliza para el aprovisionamiento junto con el conjunto de pools seleccionados por los atributos y `storagePools` parámetros. Es posible usar un parámetro de forma independiente o ambos juntos para garantizar que se seleccione el conjunto adecuado de pools de almacenamiento.
```

La `excludeStoragePools` el parámetro se utiliza para excluir específicamente el conjunto de pools enumerado que coincide con los atributos.

### Emular las políticas de calidad de servicio

Si desea diseñar clases de almacenamiento para emular políticas de calidad de servicio, cree una clase de almacenamiento con la `media` atributo como `hdd` o `ssd`. Según la `media` Atributo mencionado en la clase de almacenamiento, Trident seleccionará el back-end apropiado `hdd` o `ssd` agregados para coincidir con el atributo de medios y, a continuación, dirigir el aprovisionamiento de los volúmenes al agregado específico. Por

tanto, podemos crear UNA CLASE PREMIUM DE almacenamiento que tendría `media` atributo establecido como `ssd` Las cuales pueden clasificarse como política DE calidad DE servicio PREMIUM. Podemos crear otro ESTÁNDAR de clase de almacenamiento que tenga el conjunto de atributos de medios como "hdd", que podría clasificarse como política DE calidad DE servicio ESTÁNDAR. También podríamos usar el atributo "IOPS" en la clase de almacenamiento para redirigir el aprovisionamiento a un dispositivo Element que se puede definir como una Política de calidad de servicio.

### Utilizar back-end basado en funciones específicas

Las clases de almacenamiento se pueden diseñar para dirigir el aprovisionamiento de volúmenes en un entorno de administración específico, donde se habilitan funciones como `thin provisioning` y `thick`, copias Snapshot, clones y cifrado. Para especificar qué almacenamiento se debe utilizar, cree clases de almacenamiento que especifiquen el back-end adecuado con la función necesaria habilitada.

### Pools virtuales

Los pools virtuales están disponibles para todos los back-ends de Trident. Puede definir pools virtuales para cualquier backend, utilizando cualquier controlador que proporcione Trident.

Los pools virtuales permiten a un administrador crear un nivel de abstracción sobre los back-ends que se puede hacer referencia a través de las clases de almacenamiento, para obtener mayor flexibilidad y colocación eficiente de los volúmenes en back-ends. Pueden definirse distintos back-ends con la misma clase de servicio. Es más, es posible crear varios pools de almacenamiento en el mismo back-end, pero con características diferentes. Cuando se configura una clase de almacenamiento con un selector con etiquetas específicas, Trident elige un back-end que coincide con todas las etiquetas de selector para colocar el volumen. Si las etiquetas de selector de clase de almacenamiento coinciden con varios pools de almacenamiento, Trident elegirá uno de ellos de los que aprovisionar el volumen.

### Diseño de pool virtual

Al crear un back-end, generalmente puede especificar un conjunto de parámetros. Era imposible que el administrador creara otro back-end con las mismas credenciales de almacenamiento y con un conjunto de parámetros diferente. Con la introducción de pools virtuales, este problema se ha aliviado. Los pools virtuales son una abstracción de niveles introducida entre el back-end y la clase de almacenamiento de Kubernetes de modo que el administrador puede definir parámetros junto con etiquetas a las que se puede hacer referencia a través de las clases de almacenamiento de Kubernetes como selector, de forma independiente del back-end. Se pueden definir pools virtuales para todos los back-ends de NetApp compatibles con Trident. Esta lista incluye HCI de SolidFire/NetApp, ONTAP, Cloud Volumes Service en GCP y Azure NetApp Files.



Al definir los pools virtuales, se recomienda no intentar reorganizar el orden de los grupos virtuales existentes en una definición de backend. También es aconsejable no editar/modificar atributos para un pool virtual existente y definir un nuevo pool virtual en su lugar.

### Emulación de distintos niveles de servicio/calidad de servicio

Se pueden diseñar pools virtuales para emular clases de servicio. Al utilizar la implementación de pools virtuales para el servicio Cloud Volume para Azure NetApp Files, examinemos cómo podemos configurar distintas clases de servicio. Configure el backend de Azure NetApp Files con varias etiquetas, que representan diferentes niveles de rendimiento. Configure `servicelevel` aspecto al nivel de rendimiento apropiado y agregar otros aspectos requeridos en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes que se asignarán a diferentes pools virtuales. Con el `parameters.selector` Campo, cada clase de almacenamiento llama a qué pools virtuales se pueden utilizar para alojar un volumen.

## Asignación de un conjunto específico de aspectos

Se pueden diseñar varios pools virtuales con un conjunto específico de aspectos a partir de un único back-end de almacenamiento. Para ello, configure el backend con varias etiquetas y defina los aspectos necesarios en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes usando `parameters.selector` campo que se asignará a diferentes pools virtuales. Los volúmenes que se aprovisionan en el back-end tendrán los aspectos definidos en el pool virtual elegido.

## Las características de PVC que afectan al aprovisionamiento de almacenamiento

Algunos parámetros aparte de la clase de almacenamiento solicitada pueden afectar al proceso de decisiones de aprovisionamiento de Trident al crear una RVP.

### Modo de acceso

Al solicitar un almacenamiento a través de un PVC, uno de los campos obligatorios es el modo de acceso. El modo deseado puede afectar el back-end seleccionado para alojar la solicitud de almacenamiento.

Trident intentará hacer coincidir el protocolo de almacenamiento utilizado con el método de acceso especificado de acuerdo con la siguiente matriz. Es independiente de la plataforma de almacenamiento subyacente.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
ISCSI	Sí	Sí	Sí (bloque sin formato)
NFS	Sí	Sí	Sí

Si se solicita un PVC ReadWriteMany enviado a una implementación de Trident sin un back-end de NFS configurado, no se aprovisionará ningún volumen. Por este motivo, el solicitante debe usar el modo de acceso adecuado para su aplicación.

## Operaciones de volumen

### Modifique los volúmenes persistentes

Los volúmenes persistentes son, con dos excepciones, objetos inmutables en Kubernetes. Una vez creada, la política de reclamaciones y el tamaño se pueden modificar. Sin embargo, esto no impide que algunos aspectos del volumen se modifiquen fuera de Kubernetes. Esto puede ser deseable para personalizar el volumen para aplicaciones específicas, con el fin de garantizar que la capacidad no se consume accidentalmente, o simplemente mover el volumen a una controladora de almacenamiento diferente por cualquier motivo.



Los aprovisionadores de árbol de Kubernetes no admiten las operaciones de cambio de tamaño de volumen para NFS o iSCSI VP en este momento. Trident admite la expansión de los volúmenes NFS e iSCSI.

Los detalles de conexión del VP no se pueden modificar una vez creado.

### Cree snapshots de volumen bajo demanda

Trident admite la creación de instantáneas de volumen bajo demanda y la creación de RVP a partir de instantáneas mediante el marco CSI. Las copias Snapshot proporcionan un método cómodo de mantener copias de un momento específico de los datos y poseen un ciclo de vida independiente del VP de origen de



Kubernetes. Estas instantáneas se pueden utilizar para clonar EVs.

## Crear volúmenes a partir de snapshots

Trident también admite la creación de PersistentVolumes a partir de las snapshots de volúmenes. Para ello, solo tiene que crear una reclamación de volumen persistente y mencionar la `datasource` snapshot necesaria a partir de la que se debe crear el volumen. Trident gestionará la RVP creando un volumen con los datos presentes en la snapshot. Con esta función, es posible duplicar datos entre regiones, crear entornos de prueba, reemplazar un volumen de producción dañado o dañado en su totalidad, o recuperar archivos y directorios específicos y transferirlos a otro volumen adjunto.

## Mueva volúmenes al clúster

Los administradores de almacenamiento pueden mover volúmenes entre agregados y controladoras en el clúster de ONTAP de forma no disruptiva al consumidor de almacenamiento. Esta operación no afecta a Trident ni al clúster de Kubernetes, siempre y cuando el agregado de destino sea una a la que tenga acceso la SVM a la que utiliza Trident. Lo que es más importante, si se acaba de añadir el agregado a la SVM, se deberá actualizar el back-end volviendo a añadirlo a Trident. Esto activará que Trident vuelva a inventariar la SVM con el fin de reconocer el nuevo agregado.

Sin embargo, Trident no admite automáticamente el movimiento de volúmenes entre back-ends. Esto incluye entre las SVM del mismo clúster, entre clústeres o en una plataforma de almacenamiento diferente (aunque dicho sistema de almacenamiento sea una que esté conectado a Trident).

Si se copia un volumen en otra ubicación, es posible que se use la función de importación de volúmenes para importar los volúmenes actuales a Trident.

## Expanda los volúmenes

Trident admite el cambio de tamaño de VP de NFS e iSCSI. De este modo, los usuarios pueden cambiar el tamaño de sus volúmenes directamente desde la capa de Kubernetes. La expansión de volumen es posible para las principales plataformas de almacenamiento de NetApp, como ONTAP, HCI de SolidFire/NetApp y back-ends de Cloud Volumes Service. Para permitir una posible expansión más adelante, establezca `allowVolumeExpansion` en `true` en el StorageClass asociado con el volumen. Siempre que sea necesario cambiar el tamaño del volumen persistente, edite la `spec.resources.requests.storage` anotación en la reclamación Volumen persistente al tamaño de volumen deseado. Trident se ocupa automáticamente de ajustar el tamaño del volumen en el clúster de almacenamiento.

## Importe un volumen existente en Kubernetes

La importación de volúmenes ofrece la posibilidad de importar un volumen de almacenamiento existente en un entorno de Kubernetes. Actualmente es compatible con `ontap-nas`, `ontap-nas-flexgroup`, `solidfire-san`, `azure-netapp-files`, y `gcp-cvs` de windows Esta función es útil cuando se pasa una aplicación existente a Kubernetes o durante escenarios de recuperación ante desastres.

Cuando use la ONTAP y `solidfire-san` los controladores, utilice el comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` para importar un volumen existente a Kubernetes que gestionará Trident. El archivo RVP YAML o JSON utilizado en el comando de importación del volumen señala a una clase de almacenamiento que identifica a Trident como el proveedor. Cuando se utiliza un back-end de HCI/SolidFire de NetApp, asegúrese de que los nombres de los volúmenes sean únicos. Si los nombres de los volúmenes se duplican, clone el volumen en un nombre único de modo que la función de importación de volumen pueda distinguir entre ellos.

Si `azure-netapp-files` se utiliza el controlador o `gcp-cvs`, use el comando `tridentctl import`

`volume <backend-name> <volume path> -f /path/pvc.yaml` para importar el volumen a Kubernetes que gestionará Trident. Esto garantiza una referencia de volumen única.

Cuando se ejecuta el comando anterior, Trident encontrará el volumen en el backend y leerá su tamaño. Añadirá (y sobrescribirá automáticamente si es necesario) el tamaño de volumen de la RVP configurada. A continuación, Trident crea el nuevo VP y Kubernetes enlaza la RVP al VP.

Si se puso en marcha un contenedor de modo que requería la RVP específica importada, este permanecería en estado pendiente hasta que el par PVC/VP se enlaza a través del proceso de importación del volumen. Una vez enlazados el par PVC/PV, el contenedor debería aparecer, siempre que no haya otros problemas.

## Implementar servicios OpenShift

Los servicios de clúster de valor añadido de OpenShift proporcionan una funcionalidad importante a los administradores de clúster y a las aplicaciones que se alojan. Sin embargo, el almacenamiento que utilizan estos servicios puede aprovisionarse con los recursos locales de nodos, esto limita con frecuencia la capacidad, el rendimiento, la capacidad de recuperación y la sostenibilidad del servicio. Sin embargo, al aprovechar una cabina de almacenamiento empresarial para ofrecer la capacidad de estos servicios se puede mejorar considerablemente el servicio. Al igual que sucede con todas las aplicaciones, OpenShift y los administradores de almacenamiento deberían trabajar estrechamente para determinar cuáles son las mejores opciones para cada uno de ellos. La documentación de Red Hat debe utilizarse en gran medida para determinar los requisitos y garantizar que se satisfagan las necesidades de tamaño y rendimiento.

### Servicio de registro

Se ha documentado en la implementación y administración del almacenamiento para el registro ["netapp.io"](#) en la ["blog"](#).

### Servicio de registro

Al igual que otros servicios OpenShift, el servicio de registro se pone en marcha con Ansible, con parámetros de configuración suministrados por el archivo de inventario, también conocido como los hosts, que se proporcionan al libro de estrategia. Hay dos métodos de instalación que se tratarán: Implementar el registro durante la instalación inicial de OpenShift y desplegar el registro después de que OpenShift haya sido instalado.



A partir de Red Hat OpenShift versión 3.9, la documentación oficial recomienda contra NFS para el servicio de registro debido a problemas relacionados con la corrupción de datos. Esto se basa en las pruebas de Red Hat de sus productos. El servidor NFS de ONTAP no tiene estos problemas y puede realizar fácilmente una puesta en marcha de registro. Finalmente, la elección del protocolo para el servicio de registro depende de usted; simplemente sabe que ambos funcionarán bien cuando usen las plataformas de NetApp y no hay motivos para evitar NFS si eso es lo que prefiere.

Si decide utilizar NFS con el servicio de registro, tendrá que establecer la variable Ansible `openshift_enable_unsupported_configurations` para `true` para evitar que el instalador falle.

### Manos a la obra

Opcionalmente, el servicio de registro puede implementarse tanto para aplicaciones como para las operaciones principales del propio clúster OpenShift. Si decide implementar el registro de operaciones, especificando la variable `openshift_logging_use_ops` como `true`, se crearán dos instancias del servicio. Las variables que controlan la instancia de registro de las operaciones contienen "OPS" en ellas, mientras que la instancia de las aplicaciones no.

Configurar las variables de Ansible de acuerdo con el método de puesta en marcha es importante para garantizar que los servicios subyacentes utilizan el almacenamiento correcto. Veamos las opciones para cada uno de los métodos de despliegue.



Las siguientes tablas solo incluyen las variables relevantes para la configuración del almacenamiento en relación con el servicio de registro. Puede encontrar otras opciones en "[Documentación de registro de RedHat OpenShift](#)" que deben revisarse, configurarse y utilizarse en función de la puesta en marcha.

Las variables de la siguiente tabla harán que el libro de estrategia de Ansible cree un VP y una RVP para el servicio de registro con los detalles proporcionados. Este método es significativamente menos flexible que usar la tableta playbook de instalación de componentes después de la instalación de OpenShift; sin embargo, si tiene volúmenes existentes disponibles, es una opción.

Variable	Detalles
<code>openshift_logging_storage_kind</code>	Establezca en <code>nfs</code> Para que el instalador cree un PV de NFS para el servicio de registro.
<code>openshift_logging_storage_host</code>	El nombre de host o la dirección IP del host NFS. Esto debe configurarse en la LIF de datos de su máquina virtual.
<code>openshift_logging_storage_nfs_directory</code>	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se juntan como <code>/openshift_logging</code> , utilizaría esa ruta de acceso para esta variable.
<code>openshift_logging_storage_volume_name</code>	El nombre, por ejemplo <code>pv_ose_logs</code> , Del PV que se va a crear.
<code>openshift_logging_storage_volume_size</code>	Por ejemplo, el tamaño de la exportación NFS <code>100Gi</code> .

Si su clúster OpenShift ya se está ejecutando y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar las siguientes variables.

Variable	Detalles
<code>openshift_logging_es_pvc_dynamic</code>	Establezca esta opción en <code>true</code> para usar volúmenes aprovisionados dinámicamente.
<code>openshift_logging_es_pvc_storage_class_name</code>	El nombre de la clase de almacenamiento que se utilizará en la RVP.
<code>openshift_logging_es_pvc_size</code>	El tamaño del volumen solicitado en la RVP.
<code>openshift_logging_es_pvc_prefix</code>	Prefijo para los EVs que utiliza el servicio de registro.
<code>openshift_logging_es_ops_pvc_dynamic</code>	Establezca en <code>true</code> para utilizar volúmenes aprovisionados de forma dinámica para la instancia de registro de operaciones.
<code>openshift_logging_es_ops_pvc_storage_class_name</code>	Nombre de la clase de almacenamiento para la instancia de registro de operaciones.

Variable	Detalles
<code>openshift_logging_es_ops_pvc_size</code>	El tamaño de la solicitud de volumen para la instancia de operaciones.
<code>openshift_logging_es_ops_pvc_prefix</code>	Prefijo para las RVP de instancia de OPS.

### Despliegue la pila de registro

Si va a implementar el registro como parte del proceso de instalación inicial de OpenShift, sólo tendrá que seguir el proceso de implementación estándar. Ansible configurará y pondrá en marcha los servicios y los objetos de OpenShift necesarios para que el servicio esté disponible tan pronto como finalice Ansible.

No obstante, si se pone en marcha después de la instalación inicial, Ansible deberá usar el libro de estrategia de los componentes. Este proceso puede cambiar ligeramente con diferentes versiones de OpenShift, así que asegúrese de leer y seguir "[Documentación de Red Hat OpenShift Container Platform 3.11](#)" para su versión.

### Servicio de métricas

El servicio de métricas proporciona al administrador información valiosa sobre el estado, la utilización de recursos y la disponibilidad del clúster OpenShift. También es necesaria para la funcionalidad de escala automática en pod y muchas organizaciones usan datos del servicio de mediciones para su cargo y/o para mostrar aplicaciones.

Al igual que sucede con el servicio de registro y OpenShift en su conjunto, Ansible se utiliza para poner en marcha el servicio de métricas. Además, al igual que el servicio de registro, el servicio de métricas se puede implementar durante una configuración inicial del cluster o después de su funcionamiento utilizando el método de instalación de componentes. Las siguientes tablas contienen las variables importantes a la hora de configurar el almacenamiento persistente para el servicio de métricas.



Las siguientes tablas solo contienen las variables relevantes para la configuración del almacenamiento en cuanto se relaciona con el servicio de mediciones. Hay muchas otras opciones en la documentación que se deben revisar, configurar y utilizar de acuerdo con su implementación.

Variable	Detalles
<code>openshift_metrics_storage_kind</code>	Establezca en <code>nfs</code> Para que el instalador cree un PV de NFS para el servicio de registro.
<code>openshift_metrics_storage_host</code>	El nombre de host o la dirección IP del host NFS. Esto debe configurarse en el LIF de datos de su SVM.
<code>openshift_metrics_storage_nfs_directory</code>	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se juntan como <code>/openshift_metrics</code> , utilizaría esa ruta de acceso para esta variable.
<code>openshift_metrics_storage_volume_name</code>	El nombre, por ejemplo <code>pv_ose_metrics</code> , Del PV que se va a crear.
<code>openshift_metrics_storage_volume_size</code>	Por ejemplo, el tamaño de la exportación NFS 100Gi.

Si su clúster OpenShift ya se está ejecutando y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar

las siguientes variables.

Variable	Detalles
<code>openshift_metrics_cassandra_pvc_prefix</code>	Prefijo que se utiliza para las RVP de métricas.
<code>openshift_metrics_cassandra_pvc_size</code>	El tamaño de los volúmenes que se van a solicitar.
<code>openshift_metrics_cassandra_storage_type</code>	El tipo de almacenamiento que se utilizará para las métricas, debe establecerse una dinámica para que Ansible cree RVP con la clase de almacenamiento adecuada.
<code>openshift_metrics_cassandra_pvc_storage_class_name</code>	El nombre de la clase de almacenamiento que se va a utilizar.

### Implementar el servicio de métricas

Con las variables de Ansible definidas en el archivo de hosts/inventario, ponga en marcha el servicio con Ansible. Si va a implementar en el momento de la instalación de OpenShift, el PV se creará y utilizará automáticamente. Si va a poner en marcha mediante los libros de estrategia de componentes, después de la instalación de OpenShift, Ansible crea las RVP necesarias y, después de que Trident haya provisionado almacenamiento para ellos, pone en marcha el servicio.

Las variables anteriores y el proceso de implementación pueden cambiar con cada versión de OpenShift. Asegúrese de revisar y seguir ["Guía de implementación de OpenShift de redhat"](#) para su versión de modo que esté configurada para su entorno.

## Protección de datos y recuperación ante desastres

Conozca las opciones de protección y recuperación para Trident y volúmenes creados mediante Trident. Debería tener una estrategia de protección y recuperación de datos para cada aplicación con un requisito de persistencia.

### Replicación y recuperación de Trident

Puede crear un backup para restaurar Trident en caso de desastre.

#### Replicación de Trident

Trident utiliza CRD de Kubernetes para almacenar y gestionar su propio estado y el clúster etcd de Kubernetes para almacenar sus metadatos.

#### Pasos

1. Realice una copia de seguridad del clúster etcd de Kubernetes mediante ["Kubernetes: Realizar backups de un clúster etcd"](#).
2. Coloque los artefactos de backup en un FlexVol.



Le recomendamos que proteja la SVM en la que reside FlexVol con una relación de SnapMirror con otra SVM.

## Recuperación de Trident

Con los CRD de Kubernetes y la instantánea etcd del clúster de Kubernetes, puede recuperar Trident.

### Pasos

1. Desde la SVM de destino, monte el volumen que contiene los certificados y archivos de datos ETCD de Kubernetes en el host que se configurará como nodo maestro.
2. Copie todos los certificados necesarios correspondientes al clúster de Kubernetes en `/etc/kubernetes/pki` y los archivos del miembro etcd debajo de `/var/lib/etcd`.
3. Restaure el clúster de Kubernetes desde el backup etcd mediante ["Kubernetes: Restaurar un clúster ETCD"](#).
4. Ejecución `kubectl get crd` Para verificar que todos los recursos personalizados de Trident han surgido y recuperado los objetos de Trident para verificar que todos los datos están disponibles.

## Replicación y recuperación de SVM

Trident no puede configurar las relaciones de replicación; sin embargo, el administrador de almacenamiento puede utilizar ["SnapMirror de ONTAP"](#) para replicar una SVM.

En caso de desastre, puede activar la SVM de destino de SnapMirror para empezar a servir datos. Puede volver al primario cuando se restauran los sistemas.

### Acerca de esta tarea

Tenga en cuenta lo siguiente al usar la función de replicación de SVM de SnapMirror:

- Debe crear un back-end distinto para cada SVM con la función SVM-DR habilitada.
- Configure las clases de almacenamiento para seleccionar los back-ends replicados solo cuando sea necesario para evitar tener volúmenes que no necesitan replicación aprovisionados en los back-ends que admitan SVM-DR.
- Los administradores de aplicaciones deben comprender el coste y la complejidad adicionales asociados con la replicación y estudiar detenidamente su plan de recuperación antes de iniciar este proceso.

### Replicación de SVM

Puede utilizar ["ONTAP: Replicación de SnapMirror SVM"](#) Para crear la relación de replicación de SVM.

SnapMirror le permite configurar opciones para controlar lo que se va a replicar. Necesitará saber qué opciones seleccionó al realizar la preformación [Recuperación de SVM mediante Trident](#).

- `"-identity-preserve true"` Replica toda la configuración de la SVM.
- `"-descarte-configs red"` Excluye las LIF y la configuración de red relacionada.
- `"-identity-preserve false"` replica solo los volúmenes y la configuración de seguridad.

### Recuperación de SVM mediante Trident

Trident no detecta automáticamente los fallos de SVM. En caso de desastre, el administrador puede iniciar manualmente la conmutación por error de Trident en la nueva SVM.

### Pasos

1. Cancelar las transferencias programadas y continuas de SnapMirror, interrumpir la relación de replicación, detener la SVM de origen y, a continuación, activar la SVM de destino de SnapMirror.

2. Si especificó `-identity-preserve false` o `-discard-config network` Al configurar la replicación de SVM, actualice el `managementLIF` y `.dataLIF` En el archivo de definición de back-end de Trident.
3. Confirme `storagePrefix` Está presente en el archivo de definición de back-end de Trident. Este parámetro no puede cambiarse. Omitiendo `storagePrefix` provocará que la actualización de backend falle.
4. Actualice todos los back-ends requeridos para reflejar el nuevo nombre de la SVM de destino mediante:

```
./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>
```

5. Si especificó `-identity-preserve false` o `discard-config network`, debe rebotar todos los pods de aplicación.



Si especificó `-identity-preserve true`, todos los volúmenes provisionados por Trident comienzan a servir datos cuando se activa la SVM de destino.

## Replicación y recuperación de volúmenes

Trident no puede configurar las relaciones de replicación de SnapMirror; sin embargo, el administrador de almacenamiento puede utilizar "[Replicación y recuperación SnapMirror de ONTAP](#)" para replicar volúmenes creados por Trident.

Luego, es posible importar los volúmenes recuperados a Trident con "[importación de volumen tridentctl](#)".



La importación no es compatible con `ontap-nas-economy`, `ontap-san-economy`, o `ontap-flexgroup-economy` de windows

## Protección de datos Snapshot

Puede proteger y restaurar datos con:

- Un controlador snapshot externo y CRD para crear snapshots de volúmenes de Kubernetes de volúmenes persistentes (VP).

["Copias de Snapshot de volumen"](#)

- Snapshots de ONTAP para restaurar el contenido completo de un volumen o para recuperar archivos o LUN individuales.

["Snapshots de ONTAP"](#)

## Seguridad

### Seguridad

Utilice las recomendaciones que se indican aquí para asegurarse de que la instalación

de Trident es segura.

### Ejecute Trident en su propio espacio de nombres

Es importante evitar que las aplicaciones, los administradores de aplicaciones, los usuarios y las aplicaciones de gestión accedan a definiciones de objetos de Trident o los pods a fin de garantizar un almacenamiento fiable y bloquear posibles actividades maliciosas.

Para separar el resto de aplicaciones y usuarios de Trident, instale siempre Trident en su propio espacio de nombres de Kubernetes (`trident`). Al colocar Trident en su propio espacio de nombres, se garantiza que solo el personal administrativo de Kubernetes tenga acceso al pod de Trident y a los artefactos (como el back-end y los secretos CHAP, si procede) almacenados en los objetos CRD con nombres. Debe asegurarse de permitir solo el acceso de los administradores al espacio de nombres Trident y, por lo tanto, el acceso a la `tridentctl` aplicación.

### Utilice la autenticación CHAP con los back-ends DE SAN de ONTAP

Trident admite la autenticación basada en CHAP para cargas de trabajo SAN de ONTAP (mediante `ontap-san` y `ontap-san-economy` controladores). NetApp recomienda el uso de CHAP bidireccional con Trident para la autenticación entre un host y el back-end de almacenamiento.

Para los back-ends ONTAP que utilizan los controladores de almacenamiento SAN, Trident puede configurar CHAP bidireccional y gestionar nombres de usuario y secretos CHAP a través de `tridentctl`. Consulte "[Prepárese para configurar el back-end con los controladores SAN de ONTAP](#)" para comprender cómo configura Trident CHAP en back-ends de ONTAP.

### Utilice la autenticación CHAP con NetApp HCI y back-ends de SolidFire

NetApp recomienda poner en marcha CHAP bidireccional para garantizar la autenticación entre un host y los back-ends de NetApp HCI y SolidFire. Trident utiliza un objeto secreto que incluye dos contraseñas CHAP por inquilino. Cuando Trident está instalado, administra los secretos CHAP y los almacena en un `tridentvolume` objeto CR para el VP respectivo. Al crear un VP, Trident utiliza los secretos CHAP para iniciar una sesión iSCSI y comunicarse con el sistema NetApp HCI y SolidFire a través de CHAP.



Los volúmenes que crea Trident no se asocian con ningún grupo de acceso de volúmenes.

### Utilice Trident con NVE y NAE

ONTAP de NetApp proporciona cifrado de datos en reposo para proteger los datos confidenciales en el caso de robo, devolución o reasignación de un disco. Para obtener más información, consulte "[Configure la información general de cifrado de volúmenes de NetApp](#)".

- Si NAE está habilitado en el back-end, cualquier volumen provisionado en Trident será habilitado para NAE.
- Si NAE no está habilitado en el back-end, cualquier volumen provisionado en Trident tendrá la función NVE habilitada, a menos que establezca la marca de cifrado de NVE en `false` la configuración de back-end.



Los volúmenes creados en Trident en un back-end habilitado para NAE deben estar cifrados NVE o NAE.



- Puede establecer el indicador NVE Encryption como `true` En la configuración del back-end de Trident, con el fin de anular el cifrado NAE y utilizar una clave de cifrado específica por volumen.
- Al configurar la marca de cifrado de NVE `false` en un back-end habilitado para NAE, se crea un volumen con la función NAE habilitada. No se puede deshabilitar el cifrado NAE mediante la marca de cifrado de NVE en `false`.

- Se puede crear manualmente un volumen de NVE en Trident mediante la configuración explícita de la marca de cifrado de NVE en `true`.

Para obtener más información sobre las opciones de configuración del back-end, consulte:

- ["Opciones de configuración DE SAN de ONTAP"](#)
- ["Opciones de configuración de NAS de ONTAP"](#)

## Configuración de clave unificada de Linux (LUKS)

Puede habilitar la configuración de clave unificada de Linux (LUKS) para cifrar los volúmenes de ECONOMÍA DE SAN de ONTAP y SAN de ONTAP en Trident. Trident admite la rotación de frase de acceso y la expansión de volumen para volúmenes cifrados con LUKS.

En Trident, los volúmenes cifrados con LUKS utilizan el cifrado y el modo `aes-xts-plain64`, como recomienda "NIST".

### Antes de empezar

- Los nodos de trabajo deben tener instalado `cryptsetup 2.1` o superior (pero inferior a 3.0). Si desea más información, visite ["Gitlab: Cryptsetup"](#).
- Por motivos de rendimiento, recomendamos que los nodos de trabajo admitan las nuevas instrucciones estándar de cifrado avanzado (AES-ni). Para verificar el soporte de AES-ni, ejecute el siguiente comando:

```
grep "aes" /proc/cpuinfo
```

Si no se devuelve nada, su procesador no admite AES-ni. Para obtener más información sobre AES-ni, visite: ["Intel: Instrucciones estándar de cifrado avanzado \(AES-ni\)"](#).

### Active el cifrado LUKS

Puede habilitar el cifrado por volumen en el lado del host usando la configuración de clave unificada de Linux (LUKS) para SAN de ONTAP y volúmenes DE ECONOMÍA SAN de ONTAP.

### Pasos

1. Defina los atributos de cifrado LUKS en la configuración de backend. Para obtener más información sobre las opciones de configuración del back-end para SAN de ONTAP, consulte ["Opciones de configuración DE SAN de ONTAP"](#).

```

"storage": [
  {
    "labels":{"luks": "true"},
    "zone":"us_east_1a",
    "defaults": {
      "luksEncryption": "true"
    }
  },
  {
    "labels":{"luks": "false"},
    "zone":"us_east_1a",
    "defaults": {
      "luksEncryption": "false"
    }
  },
]

```

2. Uso `parameters.selector` Para definir los pools de almacenamiento mediante el cifrado LUKS. Por ejemplo:

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}

```

3. Cree un secreto que contenga la frase de paso LUKS. Por ejemplo:

```

kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA

```

## Limitaciones

Los volúmenes cifrados LUKS no pueden aprovechar la deduplicación y la compresión de ONTAP.

## Configuración de backend para importar volúmenes LUKS

Para importar un volumen LUKS, debe establecer `luksEncryption` en `true` en el backend. `luksEncryption` La opción indica a Trident si el volumen es compatible con LUKS (`true`) o no con LUKS (`false`) como se muestra en el siguiente ejemplo.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

## Configuración de PVC para importar volúmenes LUKS

Para importar volúmenes LUKS dinámicamente, establezca la anotación `trident.netapp.io/luksEncryption` en `true` e incluya una clase de almacenamiento habilitada para LUKS en la RVP como se muestra en este ejemplo.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

## Gire una frase de paso LUKS

Puede girar la frase de paso de LUKS y confirmar la rotación.



No olvide una clave de acceso hasta que haya verificado que ya no hace referencia a ningún volumen, snapshot o secreto. Si se pierde una clave de acceso de referencia, es posible que no se pueda montar el volumen y los datos seguirán estando cifrados e inaccesibles.

### Acerca de esta tarea

LA rotación DE la frase de paso LUKS se produce cuando se crea un pod que monta el volumen después de especificar una nueva frase de paso LUKS. Cuando se crea un nuevo pod, Trident compara la frase de acceso LUKS del volumen con la frase de acceso activa del secreto.

- Si la clave de acceso del volumen no coincide con la clave de acceso activa en el secreto, se produce la rotación.
- Si la clave de acceso del volumen coincide con la clave de acceso activa en el secreto, el `previous-luks-passphrase` se ignora el parámetro.

### Pasos

1. Añada el `node-publish-secret-name` y `node-publish-secret-namespace` Parámetros de `StorageClass`. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifique las bases de datos passhrases existentes en el volumen o la snapshot.

### Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["A"]
```

## Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["A"]
```

3. Actualice el secreto LUKS del volumen para especificar las passphrases nuevas y anteriores. Asegúrese `previous-luke-passphrase-name` y `previous-luks-passphrase` coincidir con la frase de contraseña anterior.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Cree un nuevo pod montando el volumen. Esto es necesario para iniciar la rotación.
5. Compruebe que se ha girado la frase de paso.

## Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["B"]
```

## Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["B"]
```

## Resultados

La frase de contraseña se giró cuando solo se devuelve la nueva frase de contraseña en el volumen y la instantánea.



Si se devuelven dos passphrases, por ejemplo `luksPassphraseNames: ["B", "A"]`, la rotación está incompleta. Puede activar un nuevo pod para intentar completar la rotación.

## Habilite la expansión de volumen

Es posible habilitar la ampliación de volumen en un volumen cifrado LUKS.

### Pasos

1. Habilite el CSINodeExpandSecret puerta de características (beta 1.25+). Consulte ["Kubernetes 1.25: Use Secrets for Node-Driven Expansion of CSI Volumes"](#) para obtener más detalles.
2. Añada el `node-expand-secret-name` y `node-expand-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-{{pvc.name}}
  csi.storage.k8s.io/node-stage-secret-namespace: {{pvc.namespace}}
  csi.storage.k8s.io/node-expand-secret-name: luks-{{pvc.name}}
  csi.storage.k8s.io/node-expand-secret-namespace: {{pvc.namespace}}
allowVolumeExpansion: true
```

### Resultados

Al iniciar la ampliación de almacenamiento en línea, el kubelet pasa las credenciales adecuadas al controlador.

# Protege aplicaciones con Trident Protect

## Más información sobre Trident Protect

NetApp Trident Protect proporciona funcionalidades avanzadas de gestión de datos de aplicaciones que mejoran la funcionalidad y la disponibilidad de aplicaciones de Kubernetes con estado respaldadas por los sistemas de almacenamiento de NetApp ONTAP y el proveedor de almacenamiento CSI de NetApp Trident. Trident Protect simplifica la gestión, la protección y el movimiento de cargas de trabajo en contenedores entre clouds públicos y entornos en las instalaciones. Además, ofrece funciones de automatización mediante su API y la CLI.

Puede proteger aplicaciones con Trident Protect creando recursos personalizados (CRS) o mediante la interfaz de línea de comandos Trident Protect.

### El futuro

Puede obtener más información sobre los requisitos de Trident Protect antes de instalarlos:

- ["Los requisitos de Trident protegen"](#)

## Instale Trident Protect

### Los requisitos de Trident protegen

Comience verificando la preparación de su entorno operativo, clústeres de aplicaciones, aplicaciones y licencias. Asegúrese de que su entorno cumpla los siguientes requisitos para poner en marcha y operar Trident Protect.

#### Trident protege la compatibilidad con Kubernetes

Trident Protect es compatible con una amplia gama de ofertas de Kubernetes totalmente gestionadas y autogestionadas, entre las que se incluyen:

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Cartera de VMware Tanzania
- Subida de Kubernetes

#### La compatibilidad del back-end de almacenamiento con Trident protege

Trident Protect es compatible con los siguientes back-ends de almacenamiento:

- Amazon FSX para ONTAP de NetApp

- Cloud Volumes ONTAP
- Cabinas de almacenamiento ONTAP de NetApp
- NetApp Volumes para Google Cloud
- Azure NetApp Files

Asegúrese de que el back-end de almacenamiento cumple los siguientes requisitos:

- Compruebe que el almacenamiento de NetApp conectado al clúster utilice Astra Trident 24,02 o una versión posterior (se recomienda Trident 24,10).
  - Si Astra Trident es anterior a la versión 24.06.1 y tienes pensado utilizar la funcionalidad de recuperación ante desastres de NetApp SnapMirror, debe habilitar manualmente el aprovisionador de Astra Control.
- Asegúrese de tener el aprovisionador de control de Astra más reciente (instalado y habilitado de forma predeterminada a partir de Astra Trident 24.06.1).
- Asegúrese de tener un back-end de almacenamiento NetApp ONTAP.
- Asegúrese de haber configurado un depósito de almacenamiento de objetos para almacenar backups.
- Cree los espacios de nombres de aplicaciones que desee utilizar para las aplicaciones o las operaciones de gestión de datos de aplicaciones. Trident Protect no crea estos espacios de nombres; si especifica un espacio de nombres no existente en un recurso personalizado, se producirá un error en la operación.

### Requisitos para volúmenes de economía nas

Trident Protect admite las operaciones de backup y restauración en los volúmenes de economía nas. Actualmente no se admiten copias Snapshot, clones y replicación de SnapMirror en volúmenes económicos de nas. Debe habilitar un directorio snapshot para cada volumen económico nas que vaya a utilizar con Trident Protect.



Algunas aplicaciones no son compatibles con volúmenes que usan un directorio Snapshot. Para estas aplicaciones, debe ocultar el directorio Snapshot mediante la ejecución del siguiente comando en el sistema de almacenamiento de ONTAP:

```
nfs modify -vserver <svm> -v3-hide-snapshot enabled
```

Para habilitar el directorio snapshot, ejecute el siguiente comando para cada volumen nas-económico, sustituyéndolo <volume-UUID> por el UUID del volumen que desea cambiar:

```
tridentctl update volume <volume-UUID> --snapshot-dir=true --pool-level  
=true -n trident
```



Es posible habilitar los directorios de snapshots de forma predeterminada para volúmenes nuevos si se configura la opción Trident backend configuration `snapshotDir` en `true`. Los volúmenes existentes no se ven afectados.



## Requisitos para la replicación de SnapMirror

NetApp SnapMirror está disponible para usar con Trident Protect para las siguientes soluciones de ONTAP:

- ASA de NetApp
- AFF de NetApp
- FAS de NetApp
- ONTAP Select de NetApp
- Cloud Volumes ONTAP de NetApp
- Amazon FSX para ONTAP de NetApp

## Requisitos de clústeres de ONTAP para la replicación de SnapMirror

Asegúrese de que el clúster de ONTAP cumple los siguientes requisitos si tiene pensado utilizar la replicación de SnapMirror:

- **El proveedor de control Astra o Trident:** El proveedor de control Astra o Trident deben existir en los clústeres de Kubernetes de origen y de destino que utilizan ONTAP como backend. Trident Protect admite la replicación con tecnología de NetApp SnapMirror mediante clases de almacenamiento respaldadas por los controladores siguientes:
  - `ontap-nas`
  - `ontap-san`
- **Licencias:** Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte ["Información general sobre las licencias de SnapMirror en ONTAP"](#) si desea obtener más información.

## Consideraciones sobre la relación de paridad para la replicación de SnapMirror

Compruebe que el entorno cumple los siguientes requisitos si piensa utilizar la paridad de back-end de almacenamiento:

- **Cluster y SVM:** Los back-ends de almacenamiento ONTAP deben ser peered. Consulte ["Información general sobre relaciones entre iguales de clústeres y SVM"](#) si desea obtener más información.



Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **Trident y SVM:** Las SVM remotas entre iguales deben estar disponibles para el proveedor de control de Astra o Trident en el clúster de destino.
- **Backends administrados:** Necesitas agregar y administrar backends de almacenamiento ONTAP en Trident Protect para crear una relación de replicación.
- **NVMe sobre TCP:** Trident Protect no admite la replicación de NetApp SnapMirror para los back-ends de almacenamiento que están utilizando el protocolo NVMe sobre TCP.

## Configuración de Trident/ONTAP para la replicación de SnapMirror

Trident Protect requiere que configure al menos un back-end de almacenamiento que admita la replicación para los clústeres de origen y destino. Si los clústeres de origen y destino son los mismos, la aplicación de destino debe usar un back-end de almacenamiento diferente al de la aplicación de origen para obtener la mejor resiliencia.

## Consideraciones que tener en cuenta al utilizar KubeVirt

Si tiene previsto utilizar "Virt de KubeVirt" máquinas virtuales con replicación de SnapMirror, debe configurar la virtualización para poder congelar y descongelar sus SVM. Después de configurar la virtualización, las SVM que implemente incluirán las herramientas necesarias para congelar y descongelar. Para obtener más información sobre la configuración de la virtualización, consulte "[Instalación de OpenShift Virtualization](#)".

## Instalar y configurar Trident Protect

Si su entorno cumple los requisitos de protección Trident, puede seguir estos pasos para instalar Trident Protect en el clúster. Puede obtener Trident Protect de NetApp o instalarlo desde su propio registro privado. La instalación desde un registro privado es útil si su clúster no puede acceder a Internet.



De forma predeterminada, Trident Protect recopila información de soporte que ayuda con cualquier caso de soporte de NetApp que pueda abrir, incluidos registros, métricas e información de topología sobre clústeres y aplicaciones gestionadas. Trident Protect envía estos paquetes de soporte a NetApp a diario. Opcionalmente, puede deshabilitar esta recogida de bundles de soporte al instalar Trident Protect. Puede hacerlo manualmente "[generar un bundle de soporte](#)" en cualquier momento.

## Instale Trident Protect de NetApp

1. Añada el repositorio Helm de Trident:

```
helm repo add netapp-trident-protect  
https://netapp.github.io/trident-protect-helm-chart
```

2. Instale los CRD de Trident Protect:

```
helm install trident-protect-crds netapp-trident-protect/trident-  
protect-crds --version 100.2410.0 --create-namespace --namespace  
trident-protect
```

3. Utilice Helm para instalar Trident Protect mediante uno de los siguientes comandos. Sustituya `<name_of_cluster>` por un nombre de clúster, que se asignará al clúster y se utilizará para identificar los backups y las snapshots del clúster:

- Instale Trident Protect normalmente:

```
helm install trident-protect netapp-trident-protect/trident-  
protect --set clusterName=<name_of_cluster> --version 100.2410.0  
--create-namespace --namespace trident-protect
```

- Instale Trident Protect y deshabilite las cargas programadas diarias del bundle de soporte de Trident Protect AutoSupport:

```
helm install trident-protect netapp-trident-protect/trident-  
protect --set autoSupport.enabled=false --set  
clusterName=<name_of_cluster> --version 100.2410.0 --create  
-namespace --namespace trident-protect
```

4. Opcionalmente, congele sus máquinas virtuales. Si utiliza el soporte de KubeVirt para SnapMirror, la congelación de máquinas virtuales le ayuda a gestionarlas de manera eficaz:

```
kubectl set env deployment/trident-protect-controller-manager  
NEPTUNE_VM_FREEZE=true -n trident-protect
```



Debe configurar la virtualización para que funcione la funcionalidad de congelación. Los equipos virtuales desplegados después de esta configuración incluyen los binarios necesarios para congelar y descongelar. Para obtener más información sobre la configuración de la virtualización, consulte "[Instalación de OpenShift Virtualization](#)".

## Instale Trident Protect desde un registro privado

Puede instalar Trident Protect desde un registro de imágenes privado si su clúster de Kubernetes no puede acceder a Internet. En estos ejemplos, reemplace los valores entre paréntesis por información de su entorno:

1. Tire de las siguientes imágenes a su máquina local, actualice las etiquetas y, a continuación, empújelas en su registro privado:

```
netapp/controller:24.10.0
netapp/restic:24.10.0
netapp/kopia:24.10.0
netapp/trident-autosupport:24.10.0
netapp/exehook:24.10.0
netapp/resourcebackup:24.10.0
netapp/resourcerestore:24.10.0
netapp/resourcedelete:24.10.0
bitnami/kubectl:1.30.2
kubebuilder/kube-rbac-proxy:v0.16.0
```

Por ejemplo:

```
docker pull netapp/controller:24.10.0
```

```
docker tag netapp/controller:24.10.0 <private-registry-
url>/controller:24.10.0
```

```
docker push <private-registry-url>/controller:24.10.0
```

2. Cree el espacio de nombres del sistema Trident Protect:

```
kubectl create ns trident-protect
```

3. Inicie sesión en el Registro:

```
helm registry login <private-registry-url> -u <account-id> -p <api-
token>
```

4. Cree un secreto de extracción para utilizarlo en la autenticación del registro privado:

```
kubectl create secret docker-registry regcred --docker
-username=<registry-username> --docker-password=<api-token> -n
trident-protect --docker-server=<private-registry-url>
```

5. Añada el repositorio Helm de Trident:

```
helm repo add netapp-trident-protect
https://netapp.github.io/trident-protect-helm-chart
```

6. Cree un archivo denominado `protectValues.yaml` que contenga los siguientes valores de Trident Protect:

```
image:
  registry: <private-registry-url>
imagePullSecrets:
- name: regcred
controller:
  image:
    registry: <private-registry-url>
rbacProxy:
  image:
    registry: <private-registry-url>
crCleanup:
  imagePullSecrets:
  - name: regcred
webhooksCleanup:
  imagePullSecrets:
  - name: regcred
```

7. Instale los CRD de Trident Protect:

```
helm install trident-protect-crds netapp-trident-protect/trident-
protect-crds --version 100.2410.0 --create-namespace --namespace
trident-protect
```

8. Utilice Helm para instalar Trident Protect mediante uno de los siguientes comandos. Sustituya `<name_of_cluster>` por un nombre de clúster, que se asignará al clúster y se utilizará para identificar los backups y las snapshots del clúster:

- Instale Trident Protect normalmente:

```
helm install trident-protect netapp-trident-protect/trident-protect --set clusterName=<name_of_cluster> --version 100.2410.0 --create-namespace --namespace trident-protect -f protectValues.yaml
```

- Instale Trident Protect y deshabilite las cargas programadas diarias del bundle de soporte de Trident Protect AutoSupport:

```
helm install trident-protect netapp-trident-protect/trident-protect --set autoSupport.enabled=false --set clusterName=<name_of_cluster> --version 100.2410.0 --create-namespace --namespace trident-protect -f protectValues.yaml
```

9. Opcionalmente, congele sus máquinas virtuales. Si utiliza el soporte de KubeVirt para SnapMirror, la congelación de máquinas virtuales le ayuda a gestionarlas de manera eficaz:

```
kubectl set env deployment/trident-protect-controller-manager NEPTUNE_VM_FREEZE=true -n trident-protect
```



Debe configurar la virtualización para que funcione la funcionalidad de congelación. Los equipos virtuales desplegados después de esta configuración incluyen los binarios necesarios para congelar y descongelar. Para obtener más información sobre la configuración de la virtualización, consulte "[Instalación de OpenShift Virtualization](#)".

## Instale el complemento de la CLI Trident Protect

Puede utilizar el plugin de línea de comandos Trident Protect, que es una extensión de la utilidad Trident `tridentctl`, para crear e interactuar con los recursos personalizados de Trident Protect (CRS).

### Instale el complemento de la CLI Trident Protect

Antes de utilizar la utilidad de línea de comandos, debe instalarla en la máquina que utiliza para acceder al clúster. Siga estos pasos, dependiendo de si su máquina utiliza una CPU x64 o ARM.

### Descargar plugin para CPU Linux AMD64

1. Descargue el complemento de la CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-protect-linux-amd64
```

### Descargar plugin para CPU Linux ARM64

1. Descargue el complemento de la CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-protect-linux-arm64
```

### Descargar plugin para CPU Mac AMD64

1. Descargue el complemento de la CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-protect-macos-amd64
```

### Descargar plugin para CPU Mac ARM64

1. Descargue el complemento de la CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-protect-macos-arm64
```

1. Activar permisos de ejecución para el binario:

```
chmod +x tridentctl-protect
```

2. Copie el binario del plugin a una ubicación definida en su variable PATH. Por ejemplo, `/usr/bin` o `/usr/local/bin` (puede que necesite Privileges elevado):

```
cp ./tridentctl-protect /usr/local/bin/
```

3. De manera opcional, puede copiar el binario en una ubicación del directorio inicial. En este caso, es posible que necesite agregar la ubicación a la variable PATH:

```
cp ./tridentctl-protect ~/bin/
```

### Consulte la ayuda del complemento de la CLI de Trident

Puede utilizar las funciones de ayuda del plugin incorporado para obtener ayuda detallada sobre las capacidades del plugin:

#### Pasos

1. Utilice la función de ayuda para ver la guía de uso:

```
tridentctl protect help
```

### Habilite el autocompletado de comandos

Después de instalar el complemento de CLI Trident Protect, puede habilitar la finalización automática para ciertos comandos.



### Active la finalización automática del shell Bash

1. Descargue el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-completion.bash
```

2. Cree un nuevo directorio en el directorio principal para que contenga el script:

```
mkdir -p ~/.bash/completions
```

3. Mueva el script descargado al ~/.bash/completions directorio:

```
mv tridentctl-completion.bash ~/.bash/completions/
```

4. Añada la siguiente línea al ~/.bashrc archivo en su directorio principal:

```
source ~/.bash/completions/tridentctl-completion.bash
```

### Active la finalización automática del shell Z

1. Descargue el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-protect/releases/download/24.10.0/tridentctl-completion.zsh
```

2. Cree un nuevo directorio en el directorio principal para que contenga el script:

```
mkdir -p ~/.zsh/completions
```

3. Mueva el script descargado al ~/.zsh/completions directorio:

```
mv tridentctl-completion.zsh ~/.zsh/completions/
```

4. Añada la siguiente línea al ~/.zprofile archivo en su directorio principal:

```
source ~/.zsh/completions/tridentctl-completion.zsh
```

## Resultado

En su próximo inicio de sesión de shell, puede utilizar el comando auto-completado con el plugin `tridentctl Protect`.

# Gestione Trident Protect

## Gestione la autorización y el control de acceso

Trident Protect utiliza el modelo de Kubernetes de control de acceso basado en roles (RBAC). De forma predeterminada, Trident Protect proporciona un único espacio de nombres del sistema y su cuenta de servicio predeterminada asociada. Si cuenta con una organización con muchos usuarios o con necesidades de seguridad específicas, puede utilizar las funciones de control de acceso basado en roles de Trident Protect para obtener un control más granular sobre el acceso a los recursos y los espacios de nombres.

El administrador de clúster siempre tiene acceso a los recursos del espacio de nombres predeterminado `trident-protect` y también puede acceder a los recursos en el resto de espacios de nombres. Para controlar el acceso a recursos y aplicaciones, es necesario crear espacios de nombres adicionales y agregar recursos y aplicaciones a esos espacios de nombres.

Tenga en cuenta que ningún usuario puede crear CRS de gestión de datos de aplicaciones en el espacio de nombres predeterminado `trident-protect`. Debe crear CRS de gestión de datos de aplicaciones en un espacio de nombres de aplicaciones (como práctica recomendada, crear CRS de gestión de datos de aplicaciones en el mismo espacio de nombres que la aplicación asociada).

Sólo los administradores deben tener acceso a los objetos de recursos personalizados Privileged Trident Protect, que incluyen:



- **AppVault:** Requiere datos de credenciales de bucket
- **Paquete de Protección:** Recopila métricas, registros y otros datos sensibles de Trident
- **BundleSchedule:** Gestiona los horarios de recopilación de registros

Como práctica recomendada, use RBAC para restringir el acceso a los objetos con privilegios a los administradores.

Para obtener más información sobre cómo el RBAC regula el acceso a los recursos y espacios de nombres, consulte la "[Documentación de RBAC de Kubernetes](#)".

Para obtener información sobre las cuentas de servicio, consulte la "[Documentación de la cuenta de servicio de Kubernetes](#)".

## Ejemplo: Administrar el acceso para dos grupos de usuarios

Por ejemplo, una organización tiene un administrador de clústeres, un grupo de usuarios de ingeniería y un grupo de usuarios de marketing. El administrador del clúster debe realizar las siguientes tareas para crear un entorno en el que el grupo de ingeniería y el grupo de marketing tengan acceso solo a los recursos asignados a sus respectivos espacios de nombres.

### Paso 1: Crear un espacio de nombres para contener recursos para cada grupo

La creación de un espacio de nombres permite separar los recursos de forma lógica y controlar mejor quién tiene acceso a dichos recursos.

#### Pasos

1. Cree un espacio de nombres para el grupo de ingeniería:

```
kubectl create ns engineering-ns
```

2. Cree un espacio de nombres para el grupo de marketing:

```
kubectl create ns marketing-ns
```

### Paso 2: Crear nuevas cuentas de servicio para interactuar con los recursos de cada espacio de nombres

Cada nuevo espacio de nombres que cree viene con una cuenta de servicio predeterminada, pero debe crear una cuenta de servicio para cada grupo de usuarios para que pueda dividir aún más Privileges entre grupos en el futuro si es necesario.

#### Pasos

1. Cree una cuenta de servicio para el grupo de ingeniería:

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: eng-user
  namespace: engineering-ns
```

2. Cree una cuenta de servicio para el grupo de marketing:

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: mkt-user
  namespace: marketing-ns
```

### Paso 3: Crear un secreto para cada nueva cuenta de servicio

Un secreto de cuenta de servicio se utiliza para autenticarse con la cuenta de servicio, y se puede eliminar y volver a crear fácilmente si está comprometido.

#### Pasos

1. Cree un secreto para la cuenta de servicio de ingeniería:

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: eng-user
  name: eng-user-secret
  namespace: engineering-ns
  type: kubernetes.io/service-account-token
```

## 2. Cree un secreto para la cuenta de servicio de marketing:

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: mkt-user
  name: mkt-user-secret
  namespace: marketing-ns
  type: kubernetes.io/service-account-token
```

### Paso 4: Cree un objeto RoleBinding para enlazar el objeto ClusterRole a cada nueva cuenta de servicio

Al instalar Trident Protect, se crea un objeto ClusterRole predeterminado. Puede enlazar este ClusterRole a la cuenta de servicio creando y aplicando un objeto RoleBinding.

#### Pasos

##### 1. Enlazar ClusterRole a la cuenta de servicio de ingeniería:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: engineering-ns-tenant-rolebinding
  namespace: engineering-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

##### 2. Enlazar ClusterRole a la cuenta de servicio de marketing:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: marketing-ns-tenant-rolebinding
  namespace: marketing-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: mkt-user
  namespace: marketing-ns
```

### Paso 5: Probar permisos

Compruebe que los permisos son correctos.

#### Pasos

1. Confirme que los usuarios de ingeniería pueden acceder a los recursos de ingeniería:

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n engineering-ns
```

2. Confirme que los usuarios de ingeniería no pueden acceder a los recursos de marketing:

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n marketing-ns
```

### Paso 6: Otorgar acceso a los objetos de AppVault

Para realizar tareas de gestión de datos, como backups e instantáneas, el administrador de clúster debe conceder acceso a los objetos de AppVault a usuarios individuales.

#### Pasos

1. Cree y aplique un archivo YAML de combinación secreta y AppVault que otorgue acceso a un usuario a un AppVault. Por ejemplo, el siguiente CR otorga acceso a un AppVault al usuario `eng-user`:

```

apiVersion: v1
data:
  accessKeyID: <ID_value>
  secretAccessKey: <key_value>
kind: Secret
metadata:
  name: appvault-for-eng-user-only-secret
  namespace: trident-protect
type: Opaque
---
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: appvault-for-eng-user-only
  namespace: trident-protect # Trident protect system namespace
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: testbucket
      endpoint: 192.168.0.1:30000
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-for-eng-user-only-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-for-eng-user-only-secret
  providerType: GenericS3

```

2. Cree y aplique un CR de rol para permitir que los administradores del cluster concedan acceso a recursos específicos en un espacio de nombres. Por ejemplo:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: eng-user-appvault-reader
  namespace: trident-protect
rules:
- apiGroups:
  - protect.trident.netapp.io
  resourceNames:
  - appvault-for-enguser-only
  resources:
  - appvaults
  verbs:
  - get
```

3. Cree y aplique un CR de RoleBinding para enlazar los permisos al usuario eng-user. Por ejemplo:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: eng-user-read-appvault-binding
  namespace: trident-protect
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: eng-user-appvault-reader
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

4. Compruebe que los permisos son correctos.

a. Se ha intentado recuperar la información del objeto AppVault para todos los espacios de nombres:

```
kubectl get appvaults -n trident-protect
--as=system:serviceaccount:engineering-ns:eng-user
```

Debería ver una salida similar a la siguiente:

```
Error from server (Forbidden): appvaults.protect.trident.netapp.io is forbidden: User "system:serviceaccount:engineering-ns:eng-user" cannot list resource "appvaults" in API group "protect.trident.netapp.io" in the namespace "trident-protect"
```

- b. Prueba para ver si el usuario puede obtener la información de AppVault a la que ahora tiene permiso para acceder:

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user get appvaults.protect.trident.netapp.io/appvault-for-eng-user-only -n trident-protect
```

Debería ver una salida similar a la siguiente:

```
yes
```

### Resultado

Los usuarios a los que ha otorgado permisos de AppVault deben poder usar objetos de AppVault autorizados para operaciones de gestión de datos de aplicaciones y no deben poder acceder a ningún recurso fuera de los espacios de nombres asignados ni crear nuevos recursos a los que no tengan acceso.

### Generar un bundle de soporte

Trident Protect permite a los administradores generar paquetes que incluyen información útil para el soporte de NetApp, incluidos registros, métricas e información de topología sobre los clústeres y las aplicaciones que se están gestionando. Si está conectado a Internet, puede cargar paquetes de soporte en el sitio de soporte de NetApp (NSS) mediante un archivo de recursos personalizados (CR).



## Cree un paquete de soporte mediante un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre (por ejemplo, `trident-protect-support-bundle.yaml`).
2. Configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.triggerType:** (*required*) Determina si el paquete de soporte se genera inmediatamente o se programa. La generación de paquetes programada se tiene lugar a LAS 12am UTC. Los posibles valores son los siguientes:
    - Programado
    - Manual
  - **SPEC.uploadEnabled:** (*Opcional*) Controla si el paquete de soporte debe cargarse en el sitio de soporte de NetApp después de que se genere. Si no se especifica, el valor por defecto es `false`. Los posibles valores son los siguientes:
    - verdadero
    - false (predeterminado)
  - **Spec.dataWindowStart:** (*Optional*) Una cadena de fecha en formato RFC 3339 que especifica la fecha y la hora en que debe comenzar la ventana de datos incluidos en el paquete de soporte. Si no se especifica, el valor predeterminado es hace 24 horas. La fecha de ventana más antigua que puede especificar es hace 7 días.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: AutoSupportBundle
metadata:
  name: trident-protect-support-bundle
spec:
  triggerType: Manual
  uploadEnabled: true
  dataWindowStart: 2024-05-05T12:30:00Z
```

3. Después de rellenar `astra-support-bundle.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-support-bundle.yaml
```

## Cree un bundle de soporte mediante la CLI

1. Cree el paquete de soporte, reemplazando valores entre paréntesis con la información del entorno. `trigger-type`Determina si el grupo se crea inmediatamente o si la hora de creación está determinada por la programación, y puede ser `Manual o Scheduled El valor predeterminado es Manual.`

Por ejemplo:

```
tridentctl protect create autosupportbundle <my_bundle_name>  
--trigger-type <trigger_type>
```

## Gestione y proteja aplicaciones

### Utilice objetos de AppVault para gestionar buckets

El recurso personalizado de bloque (CR) para Trident Protect se conoce como AppVault. Los objetos de AppVault son la representación declarativa del flujo de trabajo de Kubernetes de un bloque de almacenamiento. Un AppVault CR contiene las configuraciones necesarias para que un bloque se utilice en operaciones de protección, como backups, snapshots, operaciones de restauración y replicación de SnapMirror. Solo los administradores pueden crear AppVaults.

### Ejemplos de generación de claves y definición de AppVault

Al definir un CR de AppVault, debe incluir credenciales para acceder a los recursos alojados por el proveedor. La forma en que se generan las claves para las credenciales variará según el proveedor. A continuación se muestran ejemplos de generación de claves de línea de comandos para varios proveedores, seguidos de definiciones de AppVault de ejemplo para cada proveedor.

#### Google Cloud

Ejemplo de generación de claves:

```
kubectl create secret generic gcp-creds --from-file=credentials=<mycreds  
-file.json> -n trident-protect
```

Los siguientes ejemplos de definición de AppVault se proporcionan como un CR que puede utilizar y modificar, o un ejemplo de comando de la CLI de Trident Protect que genera el CR de AppVault para usted:

## Ejemplo de AppVault CR

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: gcp-trident-protect-src-bucket-b643cc50-0429-4ad5-971f-
ac4a83621922
  namespace: trident-protect
spec:
  providerType: GCP
  providerConfig:
    gcp:
      bucketName: trident-protect-src-bucket
      projectID: project-id
  providerCredentials:
    credentials:
      valueFromSecret:
        key: credentials
        name: gcp-trident-protect-src-bucket-secret
```

## Ejemplo de creación de AppVault CR mediante la CLI de Trident Protect

```
tridentctl protect create vault gcp my-new-vault --bucket mybucket
--project my-gcp-project --secret <gcp-creds>/<credentials>
```

## Amazon S3

Ejemplo de generación de claves:

```
kubectl create secret generic -n trident-protect s3 --from
-literal=accessKeyID=<secret-name> --from-literal=secretAccessKey
=<generic-s3-trident-protect-src-bucket-secret>
```

Los siguientes ejemplos de definición de AppVault se proporcionan como un CR que puede utilizar y modificar, o un ejemplo de comando de la CLI de Trident Protect que genera el CR de AppVault para usted:

## Ejemplo de AppVault CR

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: amazon-s3-trident-protect-src-bucket-b643cc50-0429-4ad5-971f-
ac4a83621922
  namespace: trident-protect
spec:
  providerType: AWS
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3
```

## Ejemplo de creación de AppVault con CLI

```
tridentctl protect create vault GenericS3 s3vault --bucket <bucket-
name> --secret <secret-name> --endpoint <s3-endpoint>
```

## Microsoft Azure

Ejemplo de generación de claves:

```
kubectl create secret generic <secret-name> --from-literal=accountKey
=<secret-name> -n trident-protect
```

Los siguientes ejemplos de definición de AppVault se proporcionan como un CR que puede utilizar y modificar, o un ejemplo de comando de la CLI de Trident Protect que genera el CR de AppVault para usted:

## Ejemplo de AppVault CR

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: azure-trident-protect-src-bucket-b643cc50-0429-4ad5-971f-
ac4a83621922
  namespace: trident-protect
spec:
  providerType: Azure
  providerConfig:
    azure:
      accountName: account-name
      bucketName: trident-protect-src-bucket
  providerCredentials:
    accountKey:
      valueFromSecret:
        key: accountKey
        name: azure-trident-protect-src-bucket-secret
```

## Ejemplo de creación de AppVault con CLI

```
tridentctl protect create vault Azure <vault-name> --account <account-
name> --bucket <bucket-name> --secret <secret-name>
```

## Valores admitidos para ProviderType y providerConfig

`providerType` Las claves y `providerConfig` de un CR de AppVault requieren valores específicos. En la siguiente tabla, se enumeran los valores admitidos para `providerType` la clave y la clave asociada `providerConfig` que se debe utilizar con cada `providerType` valor.

`providerType` Valor admitido	Clave asociada providerConfig
AWS	s3
Azure	azure
GCP	gcp
GenericS3	s3
OntapS3	s3
StorageGridS3	s3

## Utilice el explorador AppVault para ver la información de AppVault

Puede usar el complemento de la CLI de Trident Protect para ver información sobre los objetos de AppVault que se han creado en el clúster.

### Pasos

1. Ver el contenido de un objeto AppVault:

```
tridentctl protect get appvaultcontent gcp-vault --show-resources all
```

### Ejemplo de salida:

```
+-----+-----+-----+-----+
+-----+
| CLUSTER | APP | TYPE | NAME |
TIMESTAMP |
+-----+-----+-----+-----+
+-----+
|          | mysql | snapshot | mysnap | 2024-
08-09 21:02:11 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815180300 | 2024-
08-15 18:03:06 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:06 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815200300 | 2024-
08-15 20:03:06 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815180300 | 2024-
08-15 18:04:25 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:30 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815200300 | 2024-
08-15 20:04:21 (UTC) |
| production1 | mysql | backup | mybackup5 | 2024-
08-09 22:25:13 (UTC) |
|          | mysql | backup | mybackup | 2024-
08-09 21:02:52 (UTC) |
+-----+-----+-----+-----+
+-----+
```

2. Opcionalmente, para ver AppVaultPath para cada recurso, utilice el indicador `--show-paths`.

El nombre del clúster en la primera columna de la tabla sólo está disponible si se ha especificado un nombre de clúster en la instalación del sistema Trident Protect. Por ejemplo `--set clusterName=production1:`.

## Eliminar un AppVault

Puede eliminar un objeto AppVault en cualquier momento.



No elimine `finalizers` la clave de AppVault CR antes de eliminar el objeto AppVault. Si lo hace, puede dar como resultado datos residuales en el bucket de AppVault y recursos huérfanos en el cluster.

### Antes de empezar

Asegúrese de haber eliminado todas las copias de Snapshot y las copias de seguridad almacenadas en el bloque asociado.

#### Quite un AppVault con la CLI de Kubernetes

1. Elimine el objeto AppVault, sustituyéndolo `appvault_name` por el nombre del objeto AppVault que desea eliminar:

```
kubectl delete appvault <appvault_name> -n trident-protect
```

#### Elimine un AppVault con la CLI de Trident

1. Elimine el objeto AppVault, sustituyéndolo `appvault_name` por el nombre del objeto AppVault que desea eliminar:

```
tridentctl protect delete appvault <appvault_name> -n trident-protect
```

## Defina una aplicación para la gestión

Puede definir una aplicación que desee administrar con Trident Protect creando un CR de aplicación y un CR de AppVault asociado.

### Cree un CR de AppVault

Debe crear un CR de AppVault que se utilizará al realizar operaciones de protección de datos en la aplicación, y el CR de AppVault debe residir en el clúster donde está instalado Trident Protect. AppVault CR es específico de su entorno; para ver ejemplos de AppVault CRS, consulte ["Recursos personalizados de AppVault."](#)

### Crear una aplicación CR

Debe crear un CR de aplicación para cada aplicación que desee gestionar con Trident Protect. Puede agregar una aplicación para la administración mediante la creación manual de una aplicación CR o mediante el uso de la CLI de Trident Protect para crear la CR.

## Agregar una aplicación mediante un CR

1. Cree el archivo CR de la aplicación de destino:

- a. Cree el archivo de recursos personalizados (CR) y asignele un nombre (por ejemplo, `maria-app.yaml`).
- b. Configure los siguientes atributos:
  - **metadata.name:** *(required)* El nombre del recurso personalizado de la aplicación. Tenga en cuenta el nombre que elija porque otros archivos CR necesarios para las operaciones de protección hacen referencia a este valor.
  - **spec.includedNamespaces:** *(required)* Utilice etiquetas de espacio de nombres o un nombre de espacio de nombres para especificar espacios de nombres en los que existen los recursos de la aplicación. El espacio de nombres de la aplicación debe formar parte de esta lista.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: maria
  namespace: my-app-namespace
spec:
  includedNamespaces:
    labelSelector: {}
    namespace: my-app-namespace
```

## Agregue una aplicación mediante la CLI

1. Cree y aplique la definición de la aplicación, sustituyendo los valores entre paréntesis por la información de su entorno. Puede incluir espacios de nombres y recursos en la definición de la aplicación mediante listas separadas por comas con los argumentos que se muestran en el siguiente ejemplo:

```
tridentctl protect create application <my_new_app_cr_name>
--namespaces <namespaces_to_include> --csr
<cluster_scoped_resources_to_include>
```

## Proteja las aplicaciones

Proteger todas las aplicaciones mediante la toma de snapshots y backups a través de una política de protección automatizada o de manera ad hoc.

### Crear una snapshot bajo demanda

Puede crear una snapshot bajo demanda en cualquier momento.



### Cree una instantánea con un CR

1. Cree el archivo de recursos personalizados (CR) y asignele un nombre `trident-protect-snapshot-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.applicationRef:** El nombre de Kubernetes de la aplicación a la instantánea.
  - **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se debe almacenar el contenido de la instantánea (metadatos).
  - **Spec.reclaimer Policy:** (*Optional*) define lo que sucede con el AppArchive de una instantánea cuando se elimina el CR de la instantánea. Esto significa que incluso cuando se define en `Retain`, la instantánea se suprimirá. Opciones válidas:
    - `Retain` (predeterminado)
    - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Delete
```

3. Después de rellenar `trident-protect-snapshot-cr.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-snapshot-cr.yaml
```

### Cree una copia Snapshot mediante la CLI

1. Cree la instantánea, reemplazando valores entre paréntesis con información de su entorno. Por ejemplo:

```
tridentctl protect create snapshot <my_snapshot_name> --appvault
<my_appvault_name> --app <name_of_app_to_snapshot>
```

### Cree un backup bajo demanda

Puede realizar una copia de seguridad de una aplicación en cualquier momento.

## Cree una copia de seguridad con un CR

1. Cree el archivo de recursos personalizados (CR) y asignele un nombre `trident-protect-backup-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.applicationRef:** (*required*) El nombre de Kubernetes de la aplicación para realizar una copia de seguridad.
  - **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.
  - **SPEC.DATAMOVER:** (*Optional*) Una cadena que indica qué herramienta de copia de seguridad usar para la operación de copia de seguridad. Valores posibles (distingue mayúsculas de minúsculas):
    - Restic
    - Kopia (predeterminado)
  - **Spec.reclaimer Policy:** (*Optional*) define lo que sucede con una copia de seguridad cuando se libera de su reclamación. Los posibles valores son los siguientes:
    - Delete
    - Retain (predeterminado)
  - **Spec.snapshotRef:** (*Optional*): Nombre de la instantánea que se utilizará como origen de la copia de seguridad. Si no se proporciona, se creará una instantánea temporal y se realizará una copia de seguridad.

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: Kopia
```

3. Después de rellenar `trident-protect-backup-cr.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-backup-cr.yaml
```

## Cree un backup con la interfaz de línea de comandos

1. Cree el backup sustituyendo valores entre paréntesis con información de su entorno. Por ejemplo:

```
tridentctl protect create backup <my_backup_name> --appvault <my-  
vault-name> --app <name_of_app_to_back_up>
```

### **Cree un programa de protección de datos**

La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener.

## Crear un horario mediante un CR

1. Cree el archivo de recursos personalizados (CR) y asignele un nombre `trident-protect-schedule-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **SPEC.DATAMOVER:** (*Optional*) Una cadena que indica qué herramienta de copia de seguridad usar para la operación de copia de seguridad. Valores posibles (distingue mayúsculas de minúsculas):
    - `Restic`
    - `Kopia` (predeterminado)
  - **Spec.applicationRef:** El nombre de Kubernetes de la aplicación para realizar una copia de seguridad.
  - **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.
  - **Spec.backupRetention:** El número de copias de seguridad a retener. Cero indica que no se debe crear ningún backup.
  - **Spec.snapshotRetention:** El número de instantáneas a retener. Cero indica que no se debe crear ninguna instantánea.
  - **spec.granularity:** La frecuencia con la que debe ejecutarse el horario. Los posibles valores, junto con los campos asociados necesarios:
    - `hourly` (requiere que especifique `spec.minute`)
    - `daily` (requiere que especifique `spec.minute` y `spec.hour`)
    - `weekly` (requiere que especifique `spec.minute`, `spec.hour`, y `spec.dayOfWeek`)
    - `monthly` (requiere que especifique `spec.minute`, `spec.hour`, y `spec.dayOfMonth`)
  - **Spec.dayOfMonth:** (*Optional*) El día del mes (1 - 31) en el que se debe ejecutar el horario. Este campo es necesario si la granularidad se define en `monthly`.
  - **SPEC.DayOfWeek:** (*Optional*) El día de la semana (0 - 7) en el que se debe ejecutar el horario. Los valores de 0 o 7 indican el domingo. Este campo es necesario si la granularidad se define en `weekly`.
  - **SPEC.HOUR:** (*Opcional*) La hora del día (0 - 23) que debe ejecutarse el horario. Este campo es necesario si la granularidad se define en `daily`, `weekly` o `monthly`.
  - **Spec.minute:** (*Optional*) El minuto de la hora (0 - 59) que debe ejecutarse el horario. Este campo es necesario si la granularidad se define en `hourly`, `daily`, `weekly` o `monthly`.

```

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  dataMover: Kopia
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "15"
  snapshotRetention: "15"
  granularity: <monthly>
  dayOfMonth: "1"
  dayOfWeek: "0"
  hour: "0"
  minute: "0"

```

3. Después de rellenar `trident-protect-schedule-cr.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-schedule-cr.yaml
```

### Cree una programación con la CLI

1. Cree el programa de protección, reemplazando los valores entre paréntesis con información de su entorno. Por ejemplo:



Puede usar `tridentctl protect create schedule --help` para ver información de ayuda detallada de este comando.

```

tridentctl protect create schedule <my_schedule_name> --appvault
<my_appvault_name> --app <name_of_app_to_snapshot> --backup
--retention <how_many_backups_to_retain> --data-mover
<kopia_or_restic> --day-of-month <day_of_month_to_run_schedule>
--day-of-week <day_of_month_to_run_schedule> --granularity
<frequency_to_run> --hour <hour_of_day_to_run> --minute
<minute_of_hour_to_run> --recurrence-rule <recurrence> --snapshot
--retention <how_many_snapshots_to_retain>

```

### Eliminar una copia de Snapshot

Elimine las snapshots programadas o bajo demanda que ya no necesite.

## Pasos

1. Elimine el CR de instantánea asociado a la instantánea:

```
kubectl delete snapshot <snapshot_name> -n my-app-namespace
```

## Eliminar una copia de seguridad

Elimine los backups programados o bajo demanda que ya no necesita.

## Pasos

1. Elimine el CR de backup asociado con el backup:

```
kubectl delete backup <backup_name> -n my-app-namespace
```

## Compruebe el estado de una operación de backup

Puede usar la línea de comandos para comprobar el estado de una operación de backup que está en curso, se completa o tiene errores.

## Pasos

1. Utilice el siguiente comando para recuperar el estado de la operación de copia de seguridad, sustituyendo los valores entre corchetes por información de su entorno:

```
kubectl get backup -n <namespace_name> <my_backup_cr_name> -o jsonpath  
='{.status}'
```

## Permita el backup y la restauración para las operaciones de azure-NetApp-files (ANF)

Si ha instalado Trident Protect, puede habilitar la funcionalidad de backup y restauración con gestión eficiente del espacio para back-ends de almacenamiento que utilizan la clase de almacenamiento azure-NetApp-files y se crearon antes de Trident 24,06. Esta funcionalidad funciona con volúmenes NFSv4 y no consume espacio adicional del pool de capacidad.

## Antes de empezar

Asegúrese de lo siguiente:

- Ha instalado Trident Protect.
- Debe haber definido una aplicación en Trident Protect. Esta aplicación tendrá funcionalidad de protección limitada hasta que complete este procedimiento.
- `azure-netapp-files` Seleccionó como clase de almacenamiento predeterminada para el back-end de almacenamiento.

## Expanda para obtener pasos de configuración

1. Haga lo siguiente en Trident si el volumen ANF se creó antes de actualizar a Trident 24,10:

- a. Habilite el directorio de instantáneas para cada VP basado en azure-NetApp-files y asociado con la aplicación:

```
tridentctl update volume <pv name> --snapshot-dir=true -n trident
```

- b. Confirme que el directorio de snapshots se haya habilitado para cada VP asociado:

```
tridentctl get volume <pv name> -n trident -o yaml | grep  
snapshotDir
```

Respuesta:

```
snapshotDirectory: "true"
```

+

Cuando no se habilita el directorio Snapshot, Trident Protect elige la funcionalidad normal de backup, que consume temporalmente el espacio del pool de capacidad durante el proceso de backup. En este caso, asegúrese de que haya espacio suficiente disponible en el pool de capacidad para crear un volumen temporal del tamaño del volumen del que se va a realizar el backup.

### Resultado

La aplicación está lista para backup y restauración con Trident Protect. Otras aplicaciones también pueden utilizar cada RVP para realizar backups y restauraciones de datos.

## Restaurar las aplicaciones

Es posible usar Trident Protect para restaurar la aplicación desde una snapshot o un backup. La restauración a partir de una snapshot existente será más rápida cuando se restaure la aplicación en el mismo clúster.



Al restaurar una aplicación, todos los ganchos de ejecución configurados para la aplicación se restauran con la aplicación. Si hay un enlace de ejecución posterior a la restauración, se ejecuta automáticamente como parte de la operación de restauración.

### Restauración desde un backup a un espacio de nombres diferente

Cuando se restaura un backup en un espacio de nombres diferente con BackupRestore CR, Trident Protect restaura la aplicación en un espacio de nombres nuevo, pero la aplicación restaurada no se protege de forma automática mediante Trident Protect. Para proteger la aplicación restaurada, debe crear una aplicación CR para la aplicación restaurada para que esté protegida por Trident Protect.



Al restaurar un backup en un espacio de nombres diferente con los recursos existentes, no se alterará ningún recurso que comparta los nombres con los que aparecen en el backup. Para restaurar todos los recursos del backup, elimine y vuelva a crear el espacio de nombres objetivo, o restaure el backup en un nuevo espacio de nombres.



## Utilice un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-backup-restore-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.appArchivePath:** La ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Puede utilizar el siguiente comando para buscar esta ruta:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

- **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se almacena el contenido de la copia de seguridad.
- **spec.namespaceMapping:** La asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplace `my-source-namespace` y `my-destination-namespace` con la información de su entorno.
- **Spec.storageClassMapping:** La asignación de la clase de almacenamiento de origen de la operación de restauración a la clase de almacenamiento de destino. Reemplace `destinationStorageClass` y `sourceStorageClass` con la información de su entorno.

```
apiVersion: protect.trident.netapp.io/v1o  
kind: BackupRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appArchivePath: my-backup-path  
  appVaultRef: appvault-name  
  namespaceMapping: [{"source": "my-source-namespace",  
"destination": "my-destination-namespace"}]  
  storageClassMapping:  
    destination: "${destinationStorageClass}"  
    source: "${sourceStorageClass}"
```

3. (*Optional*) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas particulares:
  - **ResourceFilter.resourceSelectionCriteria:** (Requerido para filtrar) Usa `include` or `exclude` para incluir o excluir un recurso definido en `resourceMatchers`. Agregue los siguientes parámetros `resourceMatchers` para definir los recursos que se van a incluir o excluir:
    - **ResourceFilter.resourceMatchers:** Matriz de objetos `resourceMatcher`.
    - **ResourceMatchers[].group:** (*Optional*) Grupo del recurso a filtrar.

- **ResourceMatchers[].kind:** (*Optional*) Tipo de recurso a filtrar.
- **ResourceMatchers[].version:** (*Optional*) Versión del recurso que se va a filtrar.
- **ResourceMatchers[].names:** (*Optional*) Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
- **ResourceMatchers[].namespaces:** (*Optional*) Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
- **ResourceMatchers[].labelSelectors:** (*Optional*) Cadena de selector de etiquetas en el campo Kubernetes metadata.name del recurso tal como se define en el ["Documentación de Kubernetes"](#). Por ejemplo "trident.netapp.io/os=linux":.

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      group: my-resource-group
      kind: my-resource-kind
      version: my-resource-version
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar trident-protect-backup-restore-cr.yaml el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

### Utilice la CLI

1. Restaure la copia de seguridad en un espacio de nombres diferente, sustituyendo valores entre paréntesis por información de su entorno. El namespace-mapping argumento utiliza espacios de nombres separados por dos puntos para asignar espacios de nombres de origen a los espacios de nombres de destino correctos en el formato source1:dest1, source2:dest2. Por ejemplo:

```
tridentctl protect create backuprestore <my_restore_name> --backup
<backup_namespace>/<backup_to_restore> --namespace-mapping
<source_to_destination_namespace_mapping>
```

### Restaure desde un backup al espacio de nombres original

Es posible restaurar un backup en el espacio de nombres original en cualquier momento.

## Utilice un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-backup-ipr-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.appArchivePath:** La ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Puede utilizar el siguiente comando para buscar esta ruta:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

- **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se almacena el contenido de la copia de seguridad.

Por ejemplo:

```
apiVersion: protect.trident.netapp.io/v1  
kind: BackupInplaceRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appArchivePath: my-backup-path  
  appVaultRef: appvault-name
```

3. (*Optional*) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas particulares:

- **ResourceFilter.resourceSelectionCriteria:** (Requerido para filtrar) Usa `include` or `exclude` para incluir o excluir un recurso definido en `resourceMatchers`. Agregue los siguientes parámetros `resourceMatchers` para definir los recursos que se van a incluir o excluir:
  - **ResourceFilter.resourceMatchers:** Matriz de objetos `resourceMatcher`.
    - **ResourceMatchers[].group:** (*Optional*) Grupo del recurso a filtrar.
    - **ResourceMatchers[].kind:** (*Optional*) Tipo de recurso a filtrar.
    - **ResourceMatchers[].version:** (*Optional*) Versión del recurso que se va a filtrar.
    - **ResourceMatchers[].names:** (*Optional*) Nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
    - **ResourceMatchers[].namespaces:** (*Optional*) Espacios de nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
    - **ResourceMatchers[].labelSelectors:** (*Optional*) Cadena de selector de etiquetas en el campo Kubernetes `metadata.name` del recurso tal como se define en el "[Documentación de Kubernetes](#)". Por ejemplo `"trident.netapp.io/os=linux":.`

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      group: my-resource-group
      kind: my-resource-kind
      version: my-resource-version
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar `trident-protect-backup-ipr-cr.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

#### Utilice la CLI

1. Restablezca la copia de seguridad en el espacio de nombres original, sustituyendo valores entre paréntesis por información de su entorno. El `backup` argumento utiliza un espacio de nombres y un nombre de copia de seguridad en el formato `<namespace>/<name>`. Por ejemplo:

```
tridentctl protect create backupinplacerestore <my_restore_name>
--backup <namespace/backup_to_restore>
```

### Restauración desde una copia snapshot a un espacio de nombres diferente

Puede restaurar datos desde una copia Snapshot con un archivo de recurso personalizado (CR) en un espacio de nombres diferente o en el espacio de nombres de origen original. Cuando se restaura una snapshot en un espacio de nombres diferente con SnapshotRestore CR, Trident Protect restaura la aplicación en un espacio de nombres nuevo, pero la aplicación restaurada no queda protegida de forma automática mediante Trident Protect. Para proteger la aplicación restaurada, debe crear una aplicación CR para la aplicación restaurada para que esté protegida por Trident Protect.

## Utilice un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-snapshot-restore-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se almacena el contenido de la instantánea.
  - **Spec.appArchivePath:** La ruta dentro de AppVault donde se almacena el contenido de la instantánea. Puede utilizar el siguiente comando para buscar esta ruta:

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
```

- **spec.namespaceMapping:** La asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplace `my-source-namespace` y `my-destination-namespace` con la información de su entorno.
- **Spec.storageClassMapping:** La asignación de la clase de almacenamiento de origen de la operación de restauración a la clase de almacenamiento de destino. Reemplace `destinationStorageClass` y `sourceStorageClass` con la información de su entorno.

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace",
"destination": "my-destination-namespace"}]
  storageClassMapping:
    destination: "${destinationStorageClass}"
    source: "${sourceStorageClass}"
```

3. (*Optional*) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas particulares:
  - **ResourceFilter.resourceSelectionCriteria:** (Requerido para filtrar) Usa `include` or `exclude` para incluir o excluir un recurso definido en `resourceMatchers`. Agregue los siguientes parámetros `resourceMatchers` para definir los recursos que se van a incluir o excluir:
    - **ResourceFilter.resourceMatchers:** Matriz de objetos `resourceMatcher`.
    - **ResourceMatchers[].group:** (*Optional*) Grupo del recurso a filtrar.

- **ResourceMatchers[].kind:** (*Optional*) Tipo de recurso a filtrar.
- **ResourceMatchers[].version:** (*Optional*) Versión del recurso que se va a filtrar.
- **ResourceMatchers[].names:** (*Optional*) Nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
- **ResourceMatchers[].namespaces:** (*Optional*) Espacios de nombres en el campo Kubernetes metadata.name del recurso que se va a filtrar.
- **ResourceMatchers[].labelSelectors:** (*Optional*) Cadena de selector de etiquetas en el campo Kubernetes metadata.name del recurso tal como se define en el ["Documentación de Kubernetes"](#). Por ejemplo "trident.netapp.io/os=linux":.

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      group: my-resource-group
      kind: my-resource-kind
      version: my-resource-version
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar trident-protect-snapshot-restore-cr.yaml el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

### Utilice la CLI

1. Restaure la instantánea en un espacio de nombres diferente, reemplazando los valores entre paréntesis por información de su entorno.
  - El snapshot argumento utiliza un espacio de nombres y un nombre de instantánea en el formato <namespace>/<name>.
  - El namespace-mapping argumento utiliza espacios de nombres separados por dos puntos para asignar espacios de nombres de origen a los espacios de nombres de destino correctos en el formato source1:dest1, source2:dest2.

Por ejemplo:

```
tridentctl protect create snapshotrestore <my_restore_name>
--snapshot <namespace/snapshot_to_restore> --namespace-mapping
<source_to_destination_namespace_mapping>
```

## **Restauración desde una copia Snapshot al espacio de nombres original**

Es posible restaurar una copia de Snapshot en el espacio de nombres original en cualquier momento.

## Utilice un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-snapshot-ipr-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se almacena el contenido de la instantánea.
  - **Spec.appArchivePath:** La ruta dentro de AppVault donde se almacena el contenido de la instantánea. Puede utilizar el siguiente comando para buscar esta ruta:

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1  
kind: SnapshotInplaceRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appVaultRef: appvault-name  
  appArchivePath: my-snapshot-path
```

3. (*Optional*) Si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas particulares:
  - **ResourceFilter.resourceSelectionCriteria:** (Requerido para filtrar) Usa `include` or `exclude` para incluir o excluir un recurso definido en `resourceMatchers`. Agregue los siguientes parámetros `resourceMatchers` para definir los recursos que se van a incluir o excluir:
    - **ResourceFilter.resourceMatchers:** Matriz de objetos `resourceMatcher`.
      - **ResourceMatchers[].group:** (*Optional*) Grupo del recurso a filtrar.
      - **ResourceMatchers[].kind:** (*Optional*) Tipo de recurso a filtrar.
      - **ResourceMatchers[].version:** (*Optional*) Versión del recurso que se va a filtrar.
      - **ResourceMatchers[].names:** (*Optional*) Nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
      - **ResourceMatchers[].namespaces:** (*Optional*) Espacios de nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
      - **ResourceMatchers[].labelSelectors:** (*Optional*) Cadena de selector de etiquetas en el campo Kubernetes `metadata.name` del recurso tal como se define en el "[Documentación de Kubernetes](#)". Por ejemplo `"trident.netapp.io/os=linux":.`

Por ejemplo:



```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      group: my-resource-group
      kind: my-resource-kind
      version: my-resource-version
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar `trident-protect-snapshot-ipr-cr.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

#### Utilice la CLI

1. Restaure la instantánea en el espacio de nombres original, reemplazando los valores entre paréntesis por información de su entorno. Por ejemplo:

```
tridentctl protect create snapshotinplacerestore <my_restore_name>
--snapshot <snapshot_to_restore>
```

### Compruebe el estado de una operación de restauración

Puede usar la línea de comandos para comprobar el estado de una operación de restauración en curso, que se completó o con errores.

#### Pasos

1. Utilice el siguiente comando para recuperar el estado de la operación de restauración, sustituyendo valores de entre corchetes con información de su entorno:

```
kubectl get backuprestore -n <namespace_name> <my_restore_cr_name> -o
jsonpath='{.status}'
```

### Replicar aplicaciones con NetApp SnapMirror

Con Trident Protect, puede usar las funcionalidades de replicación asíncrona de la tecnología NetApp SnapMirror para replicar datos y cambios de aplicaciones de un back-end de almacenamiento a otro, en el mismo clúster o entre diferentes clústeres.

## Configurar una relación de replicación

La configuración de una relación de replicación implica lo siguiente:

- Elegir con qué frecuencia quieres que Trident Protect tome una instantánea de la aplicación (que incluye los recursos de Kubernetes de la aplicación, así como las instantáneas de volumen de cada uno de los volúmenes de la aplicación)
- Elegir el programa de replicación (incluye recursos de Kubernetes, así como datos de volumen persistentes)
- Establecer la hora para que se realice la snapshot

### Pasos

1. Cree un AppVault para la aplicación de origen en el clúster de origen. Según su proveedor de almacenamiento, modifique un ejemplo en ["Recursos personalizados de AppVault"](#) Para adaptarse a su entorno:

## Cree un AppVault con un CR

- a. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `trident-protect-appvault-primary-source.yaml`).
- b. Configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre del recurso personalizado de AppVault. Tome nota del nombre que elija, ya que otros archivos CR necesarios para una relación de replicación hacen referencia a este valor.
  - **spec.providerConfig:** (*required*) almacena la configuración necesaria para acceder a AppVault utilizando el proveedor especificado. Elija un nombre de `bucketName` y cualquier otro detalle necesario para su proveedor. Tome nota de los valores que elija, ya que otros archivos CR necesarios para una relación de replicación hacen referencia a estos valores. Consulte "[Recursos personalizados de AppVault](#)" para ver ejemplos de CRS de AppVault con otros proveedores.
  - **spec.providerCredentials:** (*required*) almacena referencias a cualquier credencial necesaria para acceder a AppVault utilizando el proveedor especificado.
    - **spec.providerCredentials.valueFromSecret:** (*required*) indica que el valor de la credencial debe provenir de un secreto.
      - **KEY:** (*REQUIRED*) La clave válida del secreto para seleccionar.
      - **Name:** (*required*) Nombre del secreto que contiene el valor para este campo. Debe estar en el mismo espacio de nombres.
    - **spec.providerCredentials.secretAccessKey:** (*required*) La clave de acceso utilizada para acceder al proveedor. El **name** debe coincidir con **spec.providerCredentials.valueFromSecret.name**.
  - **spec.providerType:** (*required*) determina qué proporciona la copia de seguridad; por ejemplo, NetApp ONTAP S3, S3 genérico, Google Cloud o Microsoft Azure. Los posibles valores son los siguientes:
    - `aws`
    - `azure`
    - `gcp`
    - `genérico-s3`
    - `ONTAP-s3`
    - `StorageGRID-s3`
- c. Después de rellenar `trident-protect-appvault-primary-source.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-appvault-primary-source.yaml -n trident-protect
```

## Cree un AppVault con la CLI

- a. Cree AppVault, reemplazando los valores entre paréntesis con información de su entorno:

```
tridentctl protect create vault Azure <vault-name> --account  
<account-name> --bucket <bucket-name> --secret <secret-name>
```

2. Cree la aplicación de origen CR:

### Cree la aplicación de origen mediante un CR

- a. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `trident-protect-app-source.yaml`).
- b. Configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre del recurso personalizado de la aplicación. Tome nota del nombre que elija, ya que otros archivos CR necesarios para una relación de replicación hacen referencia a este valor.
  - **spec.includedNamespaces:** (*required*) Una matriz de espacios de nombres y etiquetas asociadas. Utilice nombres de espacio de nombres y, opcionalmente, reduzca el ámbito de los espacios de nombres con etiquetas para especificar los recursos que existen en los espacios de nombres que se muestran aquí. El espacio de nombres de la aplicación debe formar parte de esta cabina.

#### Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: maria
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: maria
    labelSelector: {}
```

- c. Después de rellenar `trident-protect-app-source.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-app-source.yaml -n my-app-namespace
```

### Cree la aplicación de origen mediante la CLI

- a. Cree la aplicación de origen. Por ejemplo:

```
tridentctl protect create app maria --namespaces maria -n my-app-namespace
```

3. Si lo desea, realice una instantánea de la aplicación de origen. Esta copia Snapshot se utiliza como base de la aplicación en el clúster de destino. Si omite este paso, deberá esperar a que se ejecute la siguiente instantánea programada para que tenga una instantánea reciente.

## Tome una instantánea con un CR

a. Cree un programa de replicación para la aplicación de origen:

- i. Cree el archivo de recursos personalizados (CR) y asigne un nombre (por ejemplo, `trident-protect-schedule.yaml`).
- ii. Configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre del recurso personalizado de horario.
  - **Spec.AppVaultRef:** (*required*) Este valor debe coincidir con el campo `metadata.name` del AppVault para la aplicación de origen.
  - **Spec.ApplicationRef:** (*required*) Este valor debe coincidir con el campo `metadata.name` de la aplicación de origen CR.
  - **Spec.backupRetention:** (*required*) Este campo es obligatorio y el valor debe establecerse en 0.
  - **Spec.enabled:** Debe establecerse en `true`.
  - **spec.granularity:** debe ser establecido en `Custom`.
  - **Spec.recurrenceRule:** Defina una fecha de inicio en la hora UTC y un intervalo de recurrencia.
  - **Spec.snapshotRetention:** Debe establecerse en 2.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  name: appmirror-schedule-0e1f88ab-f013-4bce-8ae9-6afed9df59a1
  namespace: my-app-namespace
spec:
  appVaultRef: generic-s3-trident-protect-src-bucket-04b6b4ec-46a3-420a-b351-45795e1b5e34
  applicationRef: maria
  backupRetention: "0"
  enabled: true
  granularity: custom
  recurrenceRule: |-
    DTSTART:20220101T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  snapshotRetention: "2"
```

- i. Después de rellenar `trident-protect-schedule.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-schedule.yaml -n my-app-namespace
```

#### Tome una instantánea utilizando la CLI

- a. Cree la instantánea, reemplazando valores entre paréntesis con información de su entorno. Por ejemplo:

```
tridentctl protect create snapshot <my_snapshot_name> --appvault <my_appvault_name> --app <name_of_app_to_snapshot>
```

4. Cree una aplicación de origen AppVault CR en el clúster de destino que sea idéntica a la aplicación AppVault CR que aplicó en el clúster de origen y asígnele el nombre (por ejemplo, `trident-protect-appvault-primary-destination.yaml`).

5. Aplicar el CR:

```
kubectl apply -f trident-protect-appvault-primary-destination.yaml -n my-app-namespace
```

6. Cree un AppVault para la aplicación de destino en el clúster de destino. Según su proveedor de almacenamiento, modifique un ejemplo en "[Recursos personalizados de AppVault](#)" Para adaptarse a su entorno:

- a. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `trident-protect-appvault-secondary-destination.yaml`).

- b. Configure los siguientes atributos:

- **metadata.name:** (*required*) El nombre del recurso personalizado de AppVault. Tome nota del nombre que elija, ya que otros archivos CR necesarios para una relación de replicación hacen referencia a este valor.
- **spec.providerConfig:** (*required*) almacena la configuración necesaria para acceder a AppVault utilizando el proveedor especificado. Elija un `bucketName` y cualquier otro detalle necesario para su proveedor. Tome nota de los valores que elija, ya que otros archivos CR necesarios para una relación de replicación hacen referencia a estos valores. Consulte "[Recursos personalizados de AppVault](#)" para ver ejemplos de CRS de AppVault con otros proveedores.
- **spec.providerCredentials:** (*required*) almacena referencias a cualquier credencial necesaria para acceder a AppVault utilizando el proveedor especificado.
  - **spec.providerCredentials.valueFromSecret:** (*required*) indica que el valor de la credencial debe provenir de un secreto.
    - **KEY:** (*REQUIRED*) La clave válida del secreto para seleccionar.
    - **Name:** (*required*) Nombre del secreto que contiene el valor para este campo. Debe estar en el mismo espacio de nombres.
  - **spec.providerCredentials.secretAccessKey:** (*required*) La clave de acceso utilizada para acceder al proveedor. El **name** debe coincidir con

**spec.providerCredentials.valueFromSecret.name.**

- **spec.providerType:** (*required*) determina qué proporciona la copia de seguridad; por ejemplo, NetApp ONTAP S3, S3 genérico, Google Cloud o Microsoft Azure. Los posibles valores son los siguientes:

- aws
- azure
- gcp
- genérico-s3
- ONTAP-s3
- StorageGRID-s3

- c. Después de rellenar `trident-protect-appvault-secondary-destination.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-appvault-secondary-destination.yaml
-n my-app-namespace
```

7. Cree un archivo CR de AppMirrorRelationship:



## Cree una AppMirrorRelationship con un CR

- a. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `trident-protect-relationship.yaml`).
- b. Configure los siguientes atributos:
  - **metadata.name:** (requerido) El nombre del recurso personalizado AppMirrorRelationship.
  - **spec.destinationAppVaultRef:** (*required*) Este valor debe coincidir con el nombre de AppVault para la aplicación de destino en el clúster de destino.
  - **spec.namespaceMapping:** (*required*) Los espacios de nombres de destino y origen deben coincidir con el espacio de nombres de aplicación definido en la aplicación CR respectiva.
  - **Spec.sourceAppVaultRef:** (*required*) Este valor debe coincidir con el nombre de AppVault para la aplicación de origen.
  - **Spec.sourceApplicationName:** (*required*) Este valor debe coincidir con el nombre de la aplicación de origen que definió en la aplicación de origen CR.
  - **Spec.storageClassName:** (*required*) Elija el nombre de una clase de almacenamiento válida en el clúster. La clase de almacenamiento debe tener una relación entre iguales con la clase de almacenamiento que se esté usando en el clúster de origen donde se implementa la aplicación de origen.
  - **Spec.recurrenceRule:** Defina una fecha de inicio en la hora UTC y un intervalo de recurrencia.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr-16061e80-1b05-4e80-9d26-d326dc1953d8
  namespace: my-app-namespace
spec:
  desiredState: Established
  destinationAppVaultRef: generic-s3-trident-protect-dst-bucket-8fe0b902-f369-4317-93d1-ad7f2edc02b5
  namespaceMapping:
    - destination: my-app-namespace
      source: my-app-namespace
  recurrenceRule: |-
    DTSTART:20220101T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  sourceAppVaultRef: generic-s3-trident-protect-src-bucket-b643cc50-0429-4ad5-971f-ac4a83621922
  sourceApplicationName: maria
  sourceApplicationUID: 7498d32c-328e-4ddd-9029-122540866aeb
  storageClassName: sc-vsrm-2
```

- c. Después de rellenar `trident-protect-relationship.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

### Cree una AppMirrorRelationship con la CLI

- a. Cree y aplique el objeto AppMirrorRelationship, reemplazando los valores entre paréntesis con información de su entorno. Por ejemplo:

```
tridentctl protect create appmirrorrelationship  
<name_of_appmirrorrelationship> --destination-app-vault  
<my_vault_name> --recurrence-rule <rule> --source-app  
<my_source_app> --source-app-vault <my_source_app_vault>
```

8. (Optional) Compruebe el estado y el estado de la relación de replicación:

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath  
='{.status}' | jq
```

### Conmutación por error al clúster de destino

Con Trident Protect, puede conmutar al respaldo de aplicaciones replicadas a un clúster de destino. Este procedimiento detiene la relación de replicación y conecta la aplicación en el clúster de destino. Trident Protect no detiene la aplicación en el clúster de origen si estaba operativa.

#### Pasos

1. Abra el archivo AppMirrorRelationship CR (por ejemplo, `trident-protect-relationship.yaml`) y cambie el valor de `spec.desiredState` a `Promoted`.
2. Guarde el archivo CR.
3. Aplicar el CR:

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

4. (Optional) Cree cualquier programación de protección que necesite en la aplicación con fallos.
5. (Optional) Compruebe el estado y el estado de la relación de replicación:

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath  
='{.status}' | jq
```

## Resincronizar una relación de replicación con fallo

La operación de resincronización vuelve a establecer la relación de replicación. Después de realizar una operación de resincronización, la aplicación de origen original se convierte en la aplicación en ejecución y se descartan todos los cambios realizados en la aplicación en ejecución en el clúster de destino.

El proceso detiene la aplicación en el clúster de destino antes de restablecer la replicación.



Se perderán todos los datos escritos en la aplicación de destino durante la conmutación al respaldo.

### Pasos

1. Crear una instantánea de la aplicación de origen.
2. Abra el archivo AppMirrorRelationship CR (por ejemplo, `trident-protect-relationship.yaml`) y cambie el valor de `spec.desiredState` a `Established`.
3. Guarde el archivo CR.
4. Aplicar el CR:

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

5. Si ha creado cualquier programación de protección en el clúster de destino para proteger la aplicación con errores, elimínala. Cualquier programación que permanezca provoca errores de snapshots de volumen.

## Resincronización inversa de una relación de replicación fallida

Cuando se realiza una resincronización inversa de una relación de replicación fallida, la aplicación de destino se convierte en la aplicación de origen y el origen se convierte en el destino. Se mantienen los cambios realizados en la aplicación de destino durante la conmutación por error.

### Pasos

1. Elimine el AppMirrorRelationship CR en el clúster de destino original. Esto hace que el destino se convierta en el origen. Si queda alguna programación de protección en el nuevo clúster de destino, elimínala.
2. Configure una relación de replicación aplicando los archivos CR que utilizó originalmente para configurar la relación con los clusters opuestos.
3. Asegúrese de que los CRS de AppVault están listos en cada clúster.
4. Configure una relación de replicación en el cluster opuesto, configurando valores para la dirección inversa.

## Invertir dirección de replicación de aplicaciones

Al invertir la dirección de replicación, Trident Protect mueve la aplicación al back-end del almacenamiento de destino, a la vez que continúa replicando al back-end del almacenamiento de origen original. Trident Protect detiene la aplicación de origen y replica los datos en el destino antes de conmutar por error a la aplicación de destino.

En esta situación, está intercambiando el origen y el destino.

### Pasos

1. Crear una instantánea de cierre:

### Cree una instantánea de cierre con un CR

- a. Desactive las programaciones de políticas de protección para la aplicación de origen.
- b. Crear un archivo CR de ShutdownSnapshot:
  - i. Cree el archivo de recursos personalizados (CR) y asigne un nombre (por ejemplo, `trident-protect-shutdownsnapshot.yaml`).
  - ii. Configure los siguientes atributos:
    - **metadata.name:** *(required)* El nombre del recurso personalizado.
    - **Spec.AppVaultRef:** *(required)* Este valor debe coincidir con el campo `metadata.name` del AppVault para la aplicación de origen.
    - **Spec.ApplicationRef:** *(required)* Este valor debe coincidir con el campo `metadata.name` del archivo CR de la aplicación de origen.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: ShutdownSnapshot
metadata:
  name: replication-shutdown-snapshot-afc4c564-e700-4b72-86c3-
c08a5dbe844e
  namespace: my-app-namespace
spec:
  appVaultRef: generic-s3-trident-protect-src-bucket-04b6b4ec-
46a3-420a-b351-45795e1b5e34
  applicationRef: maria
```

- c. Después de rellenar `trident-protect-shutdownsnapshot.yaml` el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-shutdownsnapshot.yaml -n my-app-
namespace
```

### Cree una snapshot apagada con la CLI

- a. Cree la instantánea de cierre, reemplazando valores entre paréntesis con información de su entorno. Por ejemplo:

```
tridentctl protect create shutdownsnapshot <my_shutdown_snapshot>
--appvault <my_vault> --app <app_to_snapshot>
```

2. Cuando se complete la copia de Snapshot, se debe obtener el estado de la copia de Snapshot:

```
kubectl get shutdownsnapshot -n my-app-namespace  
<shutdown_snapshot_name> -o yaml
```

3. Busque el valor de **shutdownsnapshot.status.appArchivePath** usando el siguiente comando, y registre la última parte de la ruta del archivo (también llamada nombre base; esto será todo después de la última barra diagonal):

```
k get shutdownsnapshot -n my-app-namespace <shutdown_snapshot_name> -o  
jsonpath='{.status.appArchivePath}'
```

4. Realice una conmutación por error del clúster de destino al clúster de origen con el siguiente cambio:



En el paso 2 del procedimiento de conmutación por error, incluya el `spec.promotedSnapshot` campo en el archivo AppMirrorRelationship CR y establezca su valor en el nombre base que registró en el paso 3 anterior.

5. Realice los pasos de resincronización inversa en [Resincronización inversa de una relación de replicación fallida](#).
6. Habilite las programaciones de protección en el nuevo clúster de origen.

## Resultado

Las siguientes acciones se producen debido a la replicación inversa:

- Se toma una instantánea de los recursos de Kubernetes de la aplicación de origen original.
- Los pods de la aplicación de origen originales se detienen con dignidad al eliminar los recursos de Kubernetes de la aplicación (dejando las RVP y los VP en funcionamiento).
- Después de que los pods se cierran, se toman y replican instantáneas de los volúmenes de la aplicación.
- Las relaciones de SnapMirror se rompen, lo que hace que los volúmenes de destino estén listos para la lectura/escritura.
- Los recursos de Kubernetes de la aplicación se restauran a partir de la instantánea previa al cierre, utilizando los datos del volumen replicados después de que se cerró la aplicación de origen original.
- La replicación se restablece en la dirección inversa.

## Conmutación tras error de las aplicaciones al clúster de origen original

Con Trident Protect, puede obtener un «fallo» tras una operación de recuperación tras fallos utilizando la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Trident protege replica (resincroniza) cualquier cambio de aplicación de nuevo en la aplicación de origen original antes de revertir la dirección de replicación.

Este proceso se inicia desde una relación que ha completado una conmutación al nodo de respaldo a un destino e implica los siguientes pasos:

- Comience con un estado de conmutación al respaldo.
- Vuelva a sincronizar la relación de replicación.



No realice una operación de resincronización normal, ya que esto descartará los datos escritos en el clúster de destino durante el procedimiento de conmutación por error.

- Invierta la dirección de replicación.

### Pasos

1. Realice [Resincronización inversa de una relación de replicación fallida](#) los pasos.
2. Realice [Invertir dirección de replicación de aplicaciones](#) los pasos.

### Eliminar una relación de replicación

Puede eliminar una relación de replicación en cualquier momento. Al eliminar la relación de replicación de la aplicación, se crean dos aplicaciones independientes sin relación entre ellas.

### Pasos

1. Elimine el CR de AppMirrorRelationship:

```
kubectl delete -f trident-protect-relationship.yaml -n my-app-namespace
```

## Migrar aplicaciones

Puede migrar sus aplicaciones entre clústeres o clases de almacenamiento si restaura los datos de backup o Snapshot a otro clúster o tipo de almacenamiento.



Al migrar una aplicación, todos los ganchos de ejecución configurados para la aplicación se migran con la aplicación. Si hay un enlace de ejecución posterior a la restauración, se ejecuta automáticamente como parte de la operación de restauración.

### Operaciones de backup y restauración

Para realizar operaciones de backup y restauración para las siguientes situaciones, se pueden automatizar tareas de backup y restauración específicas.

#### Clone en el mismo clúster

Para clonar una aplicación en el mismo clúster, cree una copia Snapshot o un backup y restaure los datos en el mismo clúster.

### Pasos

1. Debe realizar una de las siguientes acciones:
  - a. ["Crear una copia de Snapshot"](#).
  - b. ["Cree un backup"](#).
2. En el mismo clúster, realice una de las siguientes acciones, según si se ha creado una snapshot o un backup:
  - a. ["Restaure los datos desde la copia Snapshot"](#).
  - b. ["Restaure los datos del backup"](#).

## Clone en otro clúster

Para clonar una aplicación en un clúster diferente (realizar un clon entre clústeres), crear una instantánea o realizar un backup y restaurar los datos en otro clúster. Asegúrese de que Trident Protect está instalado en el clúster de destino.

### Pasos

1. Debe realizar una de las siguientes acciones:
  - a. "Crear una copia de Snapshot".
  - b. "Cree un backup".
2. Asegúrese de que se ha configurado el CR de AppVault para el depósito de almacenamiento de objetos que contiene la copia de seguridad o la instantánea en el clúster de destino.
3. En el clúster de destino, realice una de las siguientes acciones, según si se creó una snapshot o un backup:
  - a. "Restaure los datos desde la copia Snapshot".
  - b. "Restaure los datos del backup".

## Migre aplicaciones de una clase de almacenamiento a otra clase de almacenamiento

Puede migrar aplicaciones de una clase de almacenamiento a otra clase de almacenamiento restaurando una instantánea a otra clase de almacenamiento de destino.

Por ejemplo (excluyendo los secretos de la CR de restauración):

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: "${snapshotRestoreCRName}"
spec:
  appArchivePath: "${snapshotArchivePath}"
  appVaultRef: "${appVaultCRName}"
  namespaceMapping:
    destination: "${destinationNamespace}"
    source: "${sourceNamespace}"
  storageClassMapping:
    destination: "${destinationStorageClass}"
    source: "${sourceStorageClass}"
  resourceFilter:
    resourceMatchers:
      kind: Secret
      version: v1
    resourceSelectionCriteria: exclude
```

## Restaura la instantánea con un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-snapshot-restore-cr.yaml`.
2. En el archivo creado, configure los siguientes atributos:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.appArchivePath:** La ruta dentro de AppVault donde se almacena el contenido de la instantánea. Puede utilizar el siguiente comando para buscar esta ruta:

```
kubectl get snapshots <my-snapshot-name> -n trident-protect -o jsonpath='{.status.appArchivePath}'
```

- **Spec.appVaultRef:** (*required*) El nombre del AppVault donde se almacena el contenido de la instantánea.
- **spec.namespaceMapping:** La asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplace `my-source-namespace` y `my-destination-namespace` con la información de su entorno.

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: trident-protect
spec:
  appArchivePath: my-snapshot-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace",
"destination": "my-destination-namespace"}]
```

3. Opcionalmente, si necesita seleccionar solo ciertos recursos de la aplicación para restaurar, agregue filtros que incluyan o excluyan recursos marcados con etiquetas concretas:
  - **ResourceFilter.resourceSelectionCriteria:** (Requerido para filtrar) Usa `include` or `exclude` para incluir o excluir un recurso definido en `resourceMatchers`. Agregue los siguientes parámetros `resourceMatchers` para definir los recursos que se van a incluir o excluir:
  - **resourceMatchers.group:** (*Optional*) Grupo del recurso a filtrar.
  - **ResourceMatchers.kind:** (*Optional*) Tipo de recurso a filtrar.
  - **ResourceMatchers.version:** (*Optional*) Versión del recurso a filtrar.
  - **resourceMatchers.names:** (*Optional*) Nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
  - **resourceMatchers.namespaces:** (*Optional*) Espacios de nombres en el campo Kubernetes `metadata.name` del recurso que se va a filtrar.
  - **ResourceMatchers.labelSelectors:** (*Optional*) Cadena de selector de etiquetas en el campo



Kubernetes metadata.name del recurso tal como se define en el ["Documentación de Kubernetes"](#). Por ejemplo "trident.netapp.io/os=linux":.

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      group: my-resource-group
      kind: my-resource-kind
      version: my-resource-version
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar trident-protect-snapshot-restore-cr.yaml el archivo con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

### Restaura la instantánea mediante la interfaz de línea de comandos

1. Restaura la instantánea en un espacio de nombres diferente, reemplazando los valores entre paréntesis por información de su entorno.
  - El snapshot argumento utiliza un espacio de nombres y un nombre de instantánea en el formato <namespace>/<name>.
  - El namespace-mapping argumento utiliza espacios de nombres separados por dos puntos para asignar espacios de nombres de origen a los espacios de nombres de destino correctos en el formato source1:dest1, source2:dest2.

Por ejemplo:

```
tridentctl protect create snapshotrestore <my_restore_name>
--snapshot <namespace/snapshot_to_restore> --namespace-mapping
<source_to_destination_namespace_mapping>
```

## Gestionar enlaces de ejecución

Un enlace de ejecución es una acción personalizada que puede configurar para que se ejecute junto con una operación de protección de datos de una aplicación gestionada. Por ejemplo, si dispone de una aplicación de base de datos, puede utilizar un enlace de ejecución para pausar todas las transacciones de la base de datos antes de realizar una

instantánea y reanudar las transacciones una vez completada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

### Tipos de enlaces de ejecución

Trident Protect admite los siguientes tipos de enlaces de ejecución, según cuándo se pueden ejecutar:

- Copia previa de Snapshot
- Possnapshot
- Previo al backup
- Después del backup
- Después de la restauración
- Después de la conmutación al respaldo

### Orden de ejecución

Cuando se ejecuta una operación de protección de datos, los eventos de enlace de ejecución tienen lugar en el siguiente orden:

1. Los ganchos de ejecución de preoperación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos ganchos de prefuncionamiento personalizados como necesite, pero el orden de ejecución de estos enlaces antes de la operación no está garantizado ni configurable.
2. Se realiza la operación de protección de datos.
3. Los enlaces de ejecución de post-operación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces de post-operación personalizados como necesite, pero el orden de ejecución de estos enlaces después de la operación no está garantizado ni configurable.

Si crea varios enlaces de ejecución del mismo tipo (por ejemplo, presnapshot), no se garantiza el orden de ejecución de esos enlaces. Sin embargo, el orden de ejecución de ganchos de diferentes tipos está garantizado. Por ejemplo, el siguiente es el orden de ejecución de una configuración que tiene todos los diferentes tipos de ganchos:

1. Ganchos presnapshot ejecutados
2. Ganchos posteriores a la instantánea ejecutados
3. Ganchos de precopia de seguridad ejecutados
4. Se han ejecutado los enlaces posteriores a la copia de seguridad



El ejemplo de orden anterior solo se aplica cuando se ejecuta un backup que no utiliza una snapshot existente.



Siempre debe probar sus secuencias de comandos de ejecución de enlace antes de habilitarlas en un entorno de producción. Puede utilizar el comando 'kubectl exec' para probar cómodamente los scripts. Después de habilitar los enlaces de ejecución en un entorno de producción, pruebe las copias Snapshot y backups resultantes para garantizar que sean coherentes. Para ello, puede clonar la aplicación en un espacio de nombres temporal, restaurar la instantánea o la copia de seguridad y, a continuación, probar la aplicación.

## Notas importantes sobre los enlaces de ejecución personalizados

Tenga en cuenta lo siguiente al planificar enlaces de ejecución para sus aplicaciones.

- Un enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Muchos enlaces de ejecución pueden hacer referencia al mismo script.
- Trident Protect requiere que los scripts que los enlaces de ejecución utilizan se escriban en formato de scripts de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Trident Protect utiliza la configuración de enlace de ejecución y cualquier criterio de coincidencia para determinar qué enlaces se aplican a una operación de instantánea, copia de seguridad o restauración.



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. Si inicia una operación de copia de seguridad o de instantánea con los enlaces de ejecución asociados pero, a continuación, la cancela, los ganchos pueden ejecutarse si ya se ha iniciado la operación de copia de seguridad o de Snapshot. Esto significa que la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

### Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución para una aplicación, puede agregar filtros al enlace de ejecución para gestionar qué contenedores coincidirá el enlace. Los filtros son útiles para aplicaciones que usan la misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito diferente (como Elasticsearch). Los filtros le permiten crear escenarios donde los enlaces de ejecución se ejecutan en algunos, pero no necesariamente todos los contenedores idénticos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agregue a un enlace de ejecución utiliza una expresión regular para hacer coincidir los contenedores del clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor. Las expresiones regulares para los filtros utilizan la sintaxis expresión regular 2 (RE2), que no admite la creación de un filtro que excluye contenedores de la lista de coincidencias. Para obtener información sobre la sintaxis que soporta Trident Protect para expresiones regulares en filtros de enlace de ejecución, consulte "[Soporte de sintaxis de expresión regular 2 \(RE2\)](#)".



Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

### Ejemplos de gancho de ejecución

Visite el "[Proyecto Verda GitHub de NetApp](#)" para descargar ganchos de ejecución reales para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios enlaces de ejecución personalizados.

### Cree un enlace de ejecución

Puede crear un gancho de ejecución personalizado para una aplicación mediante Trident Protect. Necesita tener permisos de propietario, administrador o miembro para crear enlaces de ejecución.

## Utilice un CR

1. Cree el archivo de recursos personalizados (CR) y asigne un nombre `trident-protect-hook.yaml`.
2. Configure los siguientes atributos para que coincidan con su entorno Trident Protect y la configuración de clúster:
  - **metadata.name:** (*required*) El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
  - **Spec.applicationRef:** (*required*) El nombre de Kubernetes de la aplicación para la que ejecutar el hook de ejecución.
  - **Spec.stage:** (*required*) Una cadena que indica qué etapa durante la acción debe ejecutarse el gancho de ejecución. Los posibles valores son los siguientes:
    - Pre
    - Publicación
  - **Spec.action:** (*required*) Una cadena que indica qué acción tomará el gancho de ejecución, asumiendo que los filtros de enlace de ejecución especificados coinciden. Los posibles valores son los siguientes:
    - Snapshot
    - Backup
    - Restaurar
    - Conmutación al respaldo
  - **Spec.enabled:** (*Optional*) Indica si este enlace de ejecución está habilitado o desactivado. Si no se especifica, el valor predeterminado es TRUE.
  - **Spec.hookSource:** (*required*) Una cadena que contiene el script hook codificado en base64.
  - **SPEC.TIMEOUT:** (*Optional*) Un número que define cuánto tiempo en minutos se permite ejecutar el gancho de ejecución. El valor mínimo es 1 minuto y el valor predeterminado es 25 minutos si no se especifica.
  - **Spec.arguments:** (*Optional*) Una lista YAML de argumentos que puede especificar para el enlace de ejecución.
  - **Spec.matchingCriteria:** (*Optional*) Una lista opcional de pares de valores clave de criterios, cada par que forma un filtro de enlace de ejecución. Puede agregar hasta 10 filtros por gancho de ejecución.
  - **Spec.matchingCriteria.type:** (*Optional*) Una cadena que identifica el tipo de filtro de gancho de ejecución. Los posibles valores son los siguientes:
    - ConteneerImage
    - Nombre del contenedor
    - PodName
    - PodLabel
    - Nombre del espacio de nombre
  - **Spec.matchingCriteria.value:** (*Optional*) Una cadena o expresión regular que identifica el valor del filtro de enlace de ejecución.

Ejemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: ExecHook
metadata:
  name: example-hook-cr
  namespace: my-app-namespace
  annotations:
    astra.netapp.io/astra-control-hook-source-id:
/account/test/hookSource/id
spec:
  applicationRef: my-app-name
  stage: Pre
  action: Snapshot
  enabled: true
  hookSource: IyEvYmluL2Jhc2gKZWNoYAiZXhhbXBsZSBzY3JpcHQiCg==
  timeout: 10
  arguments:
    - FirstExampleArg
    - SecondExampleArg
  matchingCriteria:
    - type: containerName
      value: mysql
    - type: containerImage
      value: bitnami/mysql
    - type: podName
      value: mysql
    - type: namespaceName
      value: mysql-a
    - type: podLabel
      value: app.kubernetes.io/component=primary
    - type: podLabel
      value: helm.sh/chart=mysql-10.1.0
    - type: podLabel
      value: deployment-type=production
```

3. Después de rellenar el archivo CR con los valores correctos, aplique el CR:

```
kubectl apply -f trident-protect-hook.yaml
```

### Utilice la CLI

1. Cree el enlace de ejecución, sustituyendo los valores entre paréntesis por información de su entorno. Por ejemplo:

```
tridentctl protect create exehook <my_exec_hook_name> --action  
<action_type> --app <app_to_use_hook> --stage <pre_or_post_stage>  
--source-file <script-file>
```

## Desinstale Trident Protect

Es posible que necesite eliminar los componentes de Trident Protect si va a actualizar de una versión de prueba a una versión completa del producto.

Para quitar Trident Protect, realice los siguientes pasos.

### Pasos

1. Elimine los archivos CR de Trident Protect:

```
helm uninstall trident-protect-crds
```

2. Quitar Trident Protect:

```
helm uninstall -n trident-protect trident-protect
```

3. Elimine el espacio de nombres Trident Protect:

```
kubectl delete ns trident-protect
```

# Conocimiento y apoyo

## Preguntas frecuentes

Encuentre respuestas a las preguntas frecuentes sobre instalación, configuración, actualización y solución de problemas de Trident.

### Preguntas generales

#### ¿Con qué frecuencia se publica Trident?

A partir de la versión 24,02, Trident se lanza cada cuatro meses: Febrero, junio y octubre.

#### ¿Trident admite todas las funciones que están publicadas en una versión concreta de Kubernetes?

Trident por lo general no admite funciones alfa en Kubernetes. Trident puede ser compatible con las funciones beta en las dos versiones de Trident que se indican a continuación de la versión beta de Kubernetes.

#### ¿Trident tiene alguna dependencia de otros productos de NetApp para su funcionamiento?

Trident no tiene ninguna dependencia de otros productos de software de NetApp y funciona como una aplicación independiente. Sin embargo, debe disponer de un dispositivo de almacenamiento de entorno de administración de NetApp.

#### ¿Cómo puedo obtener información completa sobre la configuración de Trident?

Use el `tridentctl get` comando para obtener más información acerca de la configuración de Trident.

#### ¿Puedo obtener métricas acerca de cómo aprovisiona el almacenamiento Trident?

Sí. Extremos de Prometheus que se pueden utilizar para recopilar información acerca de la operación de Trident, como el número de back-ends gestionados, el número de volúmenes aprovisionados, bytes consumidos, etc. También puede ["Cloud Insights"](#) utilizar para supervisión y análisis.

#### ¿Cambia la experiencia del usuario cuando utiliza Trident como aprovisionador CSI?

No. No hay cambios en lo que respecta a la experiencia del usuario y las funcionalidades. El nombre de aprovisionador utilizado es `csi.trident.netapp.io`. Se recomienda este método de instalación de Trident si desea utilizar todas las funciones nuevas proporcionadas por las versiones actuales y futuras.

## Instale y utilice Trident en un clúster de Kubernetes

#### ¿Trident admite una instalación sin conexión desde un registro privado?

Sí, Trident puede instalarse sin conexión. Consulte ["Obtenga información acerca de la instalación de Trident"](#).

#### ¿Puedo instalar Trident Be de forma remota?

Sí. Trident 18,10 y versiones posteriores admiten la capacidad de instalación remota desde cualquier máquina que `kubectl` tenga acceso al clúster. Después de `kubectl` verificar el acceso (por ejemplo, inicie un `kubectl get nodes` comando desde el equipo remoto para verificar), siga las instrucciones de instalación.

## ¿Puedo configurar la alta disponibilidad con Trident?

Trident se instala como una puesta en marcha de Kubernetes (ReplicaSet) con una instancia, por lo que tiene HA incorporada. No debería aumentar el número de réplicas en la implementación. Si se pierde el nodo donde está instalado Trident o no se puede acceder al pod de otro modo, Kubernetes vuelve a poner en marcha automáticamente el pod en un nodo del clúster en buen estado. Trident es solo el plano de control, por lo que los pods montados en este momento no se ven afectados si se vuelve a poner en marcha Trident.

## ¿Trident necesita acceso al espacio de nombres del sistema kube?

Trident lee desde el servidor de la API de Kubernetes para determinar cuándo las aplicaciones solicitan nuevos RVP, por lo que necesita acceder al sistema kube.

## ¿Cuáles son los roles y Privileges que usa Trident?

El instalador de Trident crea un ClusterRole de Kubernetes, que tiene acceso específico a los recursos PersistentVolume, PersistentVolumeClaim, StorageClass y Secret del clúster de Kubernetes. Consulte ["Personalice la instalación tridentctl"](#).

## ¿Puedo generar localmente los archivos de manifiesto exactos que Trident utiliza para la instalación?

Puede generar y modificar localmente los archivos de manifiesto exactos que Trident utiliza para la instalación, si es necesario. Consulte ["Personalice la instalación tridentctl"](#).

## ¿Puedo compartir la misma SVM back-end de ONTAP para dos instancias de Trident separadas para dos clústeres de Kubernetes separados?

Aunque no se aconseja, puede utilizar la misma SVM de back-end para dos instancias de Trident. Especifique un nombre de volumen único para cada instancia durante la instalación y/o especifique un parámetro único `StoragePrefix` en el `setup/backend.json` archivo. De este modo, se garantiza que no se utiliza el mismo FlexVol para ambas instancias.

## ¿Es posible instalar Trident bajo containerLinux (anteriormente CoreOS)?

Trident es simplemente un pod de Kubernetes y se puede instalar dondequiera que se ejecute Kubernetes.

## ¿Puedo usar Trident con NetApp Cloud Volumes ONTAP?

Sí, Trident es compatible con AWS, Google Cloud y Azure.

## ¿Funciona Trident con Cloud Volumes Services?

Sí, Trident admite el servicio Azure NetApp Files en Azure, así como Cloud Volumes Service en GCP.

## Solución de problemas y soporte técnico

### ¿NetApp admite Trident?

Aunque Trident es de código abierto y se proporciona de forma gratuita, NetApp es totalmente compatible siempre que su backend NetApp sea compatible.

### ¿Cómo levanto un caso de soporte?

Para levantar un caso de soporte, realice una de las siguientes acciones:



1. Póngase en contacto con su responsable técnico de soporte y obtenga ayuda para emitir una incidencia.
2. Levante un caso de soporte con el contacto "[Soporte de NetApp](#)".

### ¿Cómo se genera un bundle del registro de soporte?

Puede crear un paquete de soporte en ejecución `tridentctl logs -a`. Además de los registros capturados en el paquete, capture el registro kubelet para diagnosticar los problemas de montaje en el lado de Kubernetes. Las instrucciones para obtener el registro de Kubelet varían en función de cómo se instale Kubernetes.

### ¿Qué debo hacer si necesito solicitar una nueva función?

Crea un problema "[Trident Github](#)" y menciona **RFE** en el asunto y la descripción del problema.

### ¿Dónde puedo elevar un defecto?

Crear un problema en "[Trident Github](#)". Asegúrese de incluir toda la información y registros necesarios relacionados con el problema.

### ¿Qué sucede si tengo preguntas rápidas sobre Trident sobre las que necesito aclaraciones? ¿Hay una comunidad o un foro?

Si tiene alguna pregunta, problema o solicitud, póngase en contacto con nosotros a través de nuestro Trident "[Canal de discordia](#)" o GitHub.

### La contraseña de mi sistema de almacenamiento ha cambiado y Trident ya no funciona. ¿Cómo puedo recuperarme?

Actualice la contraseña del backend con `tridentctl update backend myBackend -f </path/to_new_backend.json> -n trident`. Sustituya `myBackend` en el ejemplo con su nombre de fondo, y ``/path/to_new_backend.json` con la ruta a la correcta `backend.json` archivo.

### Trident no puede encontrar mi nodo de Kubernetes. ¿Cómo se soluciona esto?

Hay dos situaciones probables por las que Trident no puede encontrar un nodo de Kubernetes. Puede deberse a un problema de red en Kubernetes o a un problema con el DNS. El conjunto de nodos de Trident que se ejecuta en cada nodo de Kubernetes debe poder comunicarse con la controladora Trident para registrar el nodo en Trident. Si se produjeron cambios de red después de instalar Trident, este problema solo se produce con los nuevos nodos de Kubernetes que se añaden al clúster.

### Si el pod de Trident se destruye, ¿perderé los datos?

No se perderán los datos si el pod de Trident se destruye. Los metadatos de Trident se almacenan en objetos CRD. Todos los VP aprovisionados por Trident funcionarán normalmente.

## Actualice Trident

### ¿Puedo actualizar directamente desde una versión anterior a una versión nueva (omitiendo algunas versiones)?

NetApp permite actualizar Trident de una versión principal a la siguiente versión principal inmediata. Puede actualizar de la versión 18.xx a la 19.xx, 19.xx a la 20.xx, etc. Debe realizar pruebas de actualización en un laboratorio antes de la implementación de producción.

## ¿Es posible degradar Trident a una versión anterior?

Si necesita una corrección de los errores observados después de una actualización, problemas de dependencia o una actualización incorrecta o incompleta, debe ["Desinstale Trident"](#) volver a instalar la versión anterior siguiendo las instrucciones específicas para esa versión. Esta es la única forma recomendada de cambiar a una versión anterior.

## Gestione back-ends y volúmenes

### ¿Debo definir tanto las LIF de gestión como las LIF de datos en un archivo de definición del back-end de ONTAP?

El LIF de gestión es obligatorio. Data LIF varía:

- SAN de ONTAP: No se especifica para iSCSI. Trident utiliza ["Asignación de LUN selectiva de ONTAP"](#) para descubrir las LIF iSCSI necesarias para establecer una sesión de rutas múltiples. Se genera una advertencia si `dataLIF` se define explícitamente. Consulte ["Opciones y ejemplos de configuración DE SAN ONTAP"](#) para obtener más información.
- ONTAP nas: Recomendamos especificar `dataLIF`. Si no se encuentra, Trident recupera los LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos. Consulte ["Opciones y ejemplos de configuración NAS de ONTAP"](#) para obtener más información

### ¿Puede Trident configurar CHAP para back-ends de ONTAP?

Sí. Trident admite CHAP bidireccional para back-ends de ONTAP. Esto requiere configuración `useCHAP=true` en la configuración de backend.

### ¿Cómo se gestionan las políticas de exportación con Trident?

Trident puede crear y gestionar dinámicamente políticas de exportación a partir de la versión 20,04. Esto permite al administrador de almacenamiento proporcionar uno o varios bloques CIDR en la configuración back-end y hacer que Trident añada IP de nodo dentro de estos rangos a una política de exportación que cree. De esta manera, Trident administra automáticamente la adición y eliminación de reglas para nodos con IP dentro de los CIDR dados.

### ¿Las direcciones IPv6 se pueden utilizar para los LIF de gestión y datos?

Trident admite definir direcciones IPv6 para:

- `managementLIF` y.. `dataLIF` Para back-ends NAS de ONTAP.
- `managementLIF` Para back-ends DE SAN de ONTAP. No puede especificar `dataLIF` En un entorno de administración SAN de ONTAP.

Trident debe instalarse utilizando el indicador `--use-ipv6` (para `tridentctl` la instalación), `IPv6` (para el operador Trident) o `tridentTPv6` (para la instalación Helm) para que funcione a través de IPv6.

### ¿Se puede actualizar la LIF de gestión en el back-end?

Sí, es posible actualizar la LIF de gestión del back-end mediante el `tridentctl update backend` comando.

## ¿Es posible actualizar la LIF de datos en el back-end?

Puede actualizar el LIF de datos en `ontap-nas` y.. `ontap-nas-economy` solamente.

## ¿Puedo crear varios back-ends en Trident para Kubernetes?

Trident puede admitir muchos back-ends simultáneamente, ya sea con el mismo controlador o con controladores diferentes.

## ¿Cómo almacena Trident las credenciales de backend?

Trident almacena las credenciales de back-end como secretos de Kubernetes.

## ¿Cómo selecciona Trident un backend específico?

Si los atributos back-end no se pueden utilizar para seleccionar automáticamente los grupos adecuados para una clase, el `storagePools` y.. `additionalStoragePools` los parámetros se usan para seleccionar un conjunto específico de pools.

## ¿Cómo me aseguro de que Trident no aprovisiona desde un back-end específico?

```
`excludeStoragePools`El parámetro se utiliza para filtrar el conjunto de pools que Trident utiliza para el aprovisionamiento y eliminará los pools que coincidan.
```

## Si hay varios back-ends del mismo tipo, ¿cómo selecciona Trident qué backend utilizar?

Si hay varios back-ends configurados del mismo tipo, Trident selecciona el backend adecuado en función de los parámetros presentes en `StorageClass` y `PersistentVolumeClaim`. Por ejemplo, si hay varios back-ends de controlador ONTAP-nas, Trident intenta hacer coincidir los parámetros en el `StorageClass` y `PersistentVolumeClaim` combinado y hacer coincidir un backend que puede entregar los requisitos enumerados en `StorageClass` y `PersistentVolumeClaim`. Si hay varios back-ends que coincidan con la solicitud, Trident selecciona uno de ellos al azar.

## ¿Trident admite CHAP bidireccional con Element/SolidFire?

Sí.

## ¿Cómo implementa Trident Qtrees en un volumen de ONTAP? ¿Cuántos qtrees pueden ponerse en marcha en un único volumen?

La `ontap-nas-economy` El controlador crea hasta 200 qtrees en la misma FlexVol (que se puede configurar entre 50 y 300), 100,000 qtrees por nodo del clúster y 2,4 MILLONES por clúster. Al introducir un nuevo `PersistentVolumeClaim` Este servicio es prestado por el conductor económico y busca ver si ya existe una FlexVol que pueda dar servicio al nuevo qtree. Si no existe la FlexVol que pueda dar servicio al qtree, se crea una nueva FlexVol.

## ¿Cómo puedo establecer los permisos de Unix para los volúmenes aprovisionados en NAS de ONTAP?

Puede establecer permisos Unix en el volumen aprovisionado por Trident estableciendo un parámetro en el archivo de definición de backend.

## ¿Cómo puedo configurar un conjunto explícito de opciones de montaje NFS de ONTAP al aprovisionar un volumen?

De forma predeterminada, Trident no establece las opciones de montaje como ningún valor con Kubernetes. Para especificar las opciones de montaje en la clase de almacenamiento de Kubernetes, siga el ejemplo proporcionado ["aquí"](#).

## ¿Cómo se configuran los volúmenes aprovisionados en una política de exportación específica?

Para permitir el acceso de hosts adecuados a un volumen, use el `exportPolicy` parámetro configurado en el archivo de definición de backend.

## ¿Cómo puedo configurar el cifrado de volúmenes mediante Trident con ONTAP?

Puede establecer el cifrado en el volumen aprovisionado por Trident mediante el parámetro `Encryption` del archivo de definición del back-end. Para obtener más información, consulte: ["Cómo funciona Trident con NVE y NAE"](#)

## ¿Cuál es la mejor forma de implementar la calidad de servicio para ONTAP mediante Trident?

Uso `StorageClasses` Para implementar QoS en ONTAP.

## ¿Cómo se especifica el aprovisionamiento ligero o grueso mediante Trident?

Los controladores ONTAP admiten `thin provisioning` o `thick`. Los controladores ONTAP, de manera predeterminada, son `thin provisioning`. Si se desea un aprovisionamiento grueso, debe configurar el archivo de definición back-end o el `StorageClass`. Si se configuran ambas, `StorageClass` tiene prioridad. Configure lo siguiente para ONTAP:

1. Encendido `StorageClass`, establezca la `provisioningType` atributo como grueso.
2. En el archivo de definición del back-end, habilite los volúmenes gruesos mediante la configuración `backend spaceReserve parameter` como volumen.

## ¿Cómo se asegura de que los volúmenes que se están utilizando no se eliminen incluso si se elimina accidentalmente la RVP?

La protección contra RVP se habilita automáticamente en Kubernetes a partir de la versión 1.10.

## ¿Puedo aumentar los RVP de NFS creados por Trident?

Sí. Puede expandir una RVP creada por Trident. Tenga en cuenta que el crecimiento automático del volumen es una función de ONTAP que no se aplica a Trident.

## ¿Puedo importar un volumen mientras está en SnapMirror Data Protection (DP) o en modo sin conexión?

Se produce un error en la importación del volumen si el volumen externo está en modo DP o sin conexión. Recibe el siguiente mensaje de error:

```
Error: could not import volume: volume import failed to get size of
volume: volume <name> was not found (400 Bad Request) command terminated
with exit code 1.
Make sure to remove the DP mode or put the volume online before importing
the volume.
```

## ¿Cómo se traduce la cuota de recursos en un clúster de NetApp?

La cuota de recursos de almacenamiento de Kubernetes debe funcionar siempre que el almacenamiento de NetApp tenga capacidad. Cuando el sistema de almacenamiento de NetApp no puede cumplir con la configuración de la cuota de Kubernetes debido a la falta de capacidad, Trident intenta aprovisionar, pero se produce un error.

## ¿Puedo crear snapshots de volumen con Trident?

Sí. La creación de instantáneas de volumen bajo demanda y volúmenes persistentes desde Snapshots son compatibles con Trident. Para crear VP a partir de instantáneas, asegúrese de que `VolumeSnapshotDataSource` se ha activado la puerta de función.

## ¿Cuáles son los controladores que admiten las snapshots de volumen de Trident?

A partir de ahora, ofrecemos soporte de copias Snapshot bajo demanda para nuestro `ontap-nas`, `ontap-nas-flexgroup`, `ontap-san`, `ontap-san-economy`, `solidfire-san`, `gcp-cvs`, y `azure-netapp-files` controladores de back-end.

## ¿Cómo hago un backup de una copia Snapshot de un volumen aprovisionado por Trident con ONTAP?

Este está disponible en `ontap-nas`, `ontap-san`, y `ontap-nas-flexgroup` de windows También puede especificar un `snapshotPolicy` para la `ontap-san-economy` Controlador en el nivel FlexVol.

También está disponible en `ontap-nas-economy` los controladores, pero en la granularidad de FlexVol, no en la de `qtree`. Para habilitar la capacidad de los volúmenes Snapshot aprovisionados por Trident, se debe establecer la opción del parámetro `backend snapshotPolicy` en la política Snapshot que se desee tal y como se define en el back-end de ONTAP. Trident no conoce las copias Snapshot tomadas por la controladora de almacenamiento.

## ¿Puedo establecer un porcentaje de reserva de snapshots para un volumen aprovisionado mediante Trident?

Sí, puede reservar un porcentaje específico de espacio en disco para almacenar las copias snapshot mediante Trident estableciendo el `snapshotReserve` atributo en el archivo de definición de backend. Si ha configurado `snapshotPolicy` y `snapshotReserve` en el archivo de definición de backend, el porcentaje de reserva de instantánea se establece de acuerdo con el `snapshotReserve` porcentaje mencionado en el archivo backend. Si no se menciona el `snapshotReserve` número de porcentaje, ONTAP toma por defecto el porcentaje de reserva de instantáneas como 5. Si la `snapshotPolicy` opción se define en `none`, el porcentaje de reserva de instantáneas se establece en 0.

## ¿Puedo acceder directamente al directorio de snapshot del volumen y copiar los archivos?

Sí, es posible acceder al directorio Snapshot en el volumen aprovisionado por Trident estableciendo el `snapshotDir` parámetro en el archivo de definición de backend.

## ¿Puedo configurar SnapMirror para volúmenes a través de Trident?

Actualmente, SnapMirror debe configurarse externamente mediante la CLI de ONTAP o System Manager de OnCommand.

## ¿Cómo se restauran los volúmenes persistentes en una snapshot de ONTAP específica?

Para restaurar un volumen a una copia de Snapshot de ONTAP, realice los siguientes pasos:

1. Desactive el pod de la aplicación que utiliza el volumen persistente.
2. Revertir a la snapshot necesaria mediante la interfaz de línea de comandos de ONTAP o System Manager de OnCommand.
3. Reinicie el pod de la aplicación.

## ¿Trident puede aprovisionar volúmenes en SVM que tengan configurado un reflejo de carga compartida?

Se pueden crear reflejos de uso compartido de carga para volúmenes raíz de los SVM que sirven datos mediante NFS. ONTAP actualiza automáticamente los reflejos de uso compartido de carga para los volúmenes creados por Trident. Esto puede provocar retrasos en el montaje de volúmenes. Cuando se crean varios volúmenes mediante Trident, el aprovisionamiento de un volumen depende de que ONTAP actualice el reflejo de uso compartido de carga.

## ¿Cómo puedo separar el uso de la clase de almacenamiento para cada cliente/cliente?

Kubernetes no permite las clases de almacenamiento en espacios de nombres. Sin embargo, puede utilizar Kubernetes para limitar el uso de una clase de almacenamiento específica por espacio de nombres mediante las cuotas de recursos de almacenamiento, que se encuentran por espacio de nombres. Para denegar el acceso a un espacio de nombres específico a un almacenamiento específico, establezca la cuota de recursos en 0 para esa clase de almacenamiento.

# Resolución de problemas

Utilice los punteros que se proporcionan aquí para solucionar problemas que podrían surgir durante la instalación y el uso de Trident.

## Resolución de problemas generales

- Si el pod de Trident no sale correctamente (por ejemplo, cuando el pod de Trident se encuentra atascado en el `ContainerCreating` fase con menos de dos contenedores listos para usar) en ejecución `kubectl -n trident describe deployment trident` y `kubectl -n trident describe pod trident--**` puede proporcionar información adicional. Obtención de registros de kubelet (por ejemplo, mediante `journalctl -xeu kubelet`) también puede ser útil.
- Si no hay suficiente información en los registros de Trident, puede intentar habilitar el modo de depuración para Trident aprobando el `-d` marque el parámetro `install` en función de su opción de instalación.

A continuación, confirme que la depuración se ha configurado mediante `./tridentctl logs -n trident` y buscando `level=debug msg` en el registro.

## Instalado con el operador

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

Así se reiniciarán todos los pods de Trident, que pueden tardar varios segundos. Puede comprobarlo observando la columna "ANTIGÜEDAD" en la salida de `kubectl get pod -n trident`.

Para Trident 20,07 y 20,10, utilice `tprov` en lugar de `torc`.

## Instalado con Helm

```
helm upgrade <name> trident-operator-21.07.1-custom.tgz --set
tridentDebug=true`
```

## Instalado con tridentctl

```
./tridentctl uninstall -n trident
./tridentctl install -d -n trident
```

- También puede obtener registros de depuración para cada back-end incluyendo `debugTraceFlags` en su definición de backend. Por ejemplo, incluya `debugTraceFlags: {"api":true, "method":true, }` Para obtener llamadas API y recorridos de métodos en los registros de Trident. Los back-ends existentes pueden tener `debugTraceFlags` configurado con una `tridentctl backend update`.
- Cuando utilice RedHat CoreOS, asegúrese de ello `iscsid` está activado en los nodos de trabajo e iniciado de forma predeterminada. Esto se puede hacer usando OpenShift MachineConfigs o modificando las plantillas de ignición.
- Un problema común que se puede encontrar cuando se usa Trident con "Azure NetApp Files" es cuando el inquilino y los secretos de cliente provienen de un registro de aplicación con permisos insuficientes. Para ver una lista completa de los requisitos de Trident, consulte "Azure NetApp Files" configuración.
- Si hay problemas con el montaje de un PV en un contenedor, asegúrese de que `rpcbind` está instalado y en ejecución. Utilice el administrador de paquetes necesario para el sistema operativo del host y compruebe si `rpcbind` está en ejecución. Puede comprobar el estado de `rpcbind` ejecutar un `systemctl status rpcbind` o su equivalente.
- Si un back-end de Trident informa que está en la `failed` estado a pesar de haber trabajado antes, es probable que sea por el cambio de las credenciales de SVM/administrador asociadas con el back-end. Actualización de la información del back-end mediante `tridentctl update backend` O rebotando el Pod de Trident se corregirá este problema.
- Si se producen problemas de permisos al instalar Trident con Docker como el tiempo de ejecución de contenedores, intente instalar Trident con el `--in cluster=false` bandera. Esto no utilizará un módulo de instalación y evitará problemas de permisos vistos debido a la `trident-installer` usuario.
- Utilice la `uninstall` parameter `<Uninstalling Trident>` para limpiar después de una ejecución fallida. De forma predeterminada, la secuencia de comandos no elimina los CRD creados por Trident, por lo que es seguro desinstalar e instalar de nuevo incluso en una implementación en ejecución.
- Si desea degradar a una versión anterior de Trident, ejecute primero el `tridentctl uninstall` Comando para quitar Trident. Descargue el contenido que desee "Versión de Trident" e instálela utilizando

```
tridentctl install comando.
```

- Después de una instalación correcta, si un PVC está atascado en el `Pending` fase, en marcha `kubectl describe pvc` Puede proporcionar información adicional acerca de por qué Trident no pudo aprovisionar un VP para esta RVP.

## Implementación incorrecta de Trident con el operador

Si utiliza el operador, el estado de implementación de Trident `TridentOrchestrator` cambios de `Installing` para `Installed`. Si observa la `Failed` y el operador no puede recuperarse por sí solo, debe comprobar los registros del operador ejecutando el siguiente comando:

```
tridentctl logs -l trident-operator
```

Al dejar atrás los registros del contenedor del operador-trident, puede indicar dónde se encuentra el problema. Por ejemplo, uno de estos problemas podría ser la incapacidad de extraer las imágenes contenedoras necesarias de los registros de entrada en un entorno con conexión aérea.

Para comprender por qué la instalación de Trident no ha tenido éxito, debería echar un vistazo al `TridentOrchestrator` estado.



```

kubect1 describe torc trident-2
Name:          trident-2
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Status:
  Current Installation Params:
    IPv6:
    Autosupport Hostname:
    Autosupport Image:
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:
    Image Pull Secrets:          <nil>
    Image Registry:
    k8sTimeout:
    Kubelet Dir:
    Log Format:
    Silence Autosupport:
    Trident Image:
  Message:          Trident is bound to another CR 'trident'
  Namespace:       trident-2
  Status:           Error
  Version:
Events:
  Type          Reason  Age          From          Message
  ----          -
Warning Error    16s (x2 over 16s) trident-operator.netapp.io Trident
is bound to another CR 'trident'

```

Este error indica que ya existe un TridentOrchestrator`Que se utilizó para instalar Trident. Como cada clúster de Kubernetes puede tener una instancia de Trident, el operador se asegura de que en cualquier momento solo exista una activa `TridentOrchestrator que puede crear.

Además, observar el estado de los pods de Trident puede indicar con frecuencia si algo no es correcto.

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

NAME	READY	STATUS	RESTARTS
trident-csi-4p5kq	1/2	ImagePullBackOff	0
trident-csi-6f45bfd8b6-vfrkw	4/5	ImagePullBackOff	0
trident-csi-9q5xc	1/2	ImagePullBackOff	0
trident-csi-9v95z	1/2	ImagePullBackOff	0
trident-operator-766f7b8658-ldzsv	1/1	Running	0

Puede ver claramente que las vainas no pueden inicializarse completamente porque no se obtuvieron una o más imágenes contenedoras.

Para solucionar el problema, debe editar el `TridentOrchestrator` CR. Como alternativa, puede eliminar `TridentOrchestrator`, y cree una nueva con la definición modificada y precisa.

## Puesta en marcha de Trident incorrecta mediante `tridentctl`

Para ayudar a averiguar qué fue lo que salió mal, puede ejecutar el instalador de nuevo utilizando el `-d` argumento, que activa el modo de depuración y le ayuda a comprender cuál es el problema:

```
./tridentctl install -n trident -d
```

Después de solucionar el problema, puede limpiar la instalación de la siguiente manera y, a continuación, ejecutar el `tridentctl install` comando:

```
./tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted cluster role binding.
INFO Deleted cluster role.
INFO Deleted service account.
INFO Removed Trident user from security context constraint.
INFO Trident uninstallation succeeded.
```

## Eliminar completamente Trident y CRD

Puede eliminar completamente Trident y todos los CRD creados y los recursos personalizados asociados.



Esta acción no se puede deshacer. No haga esto a menos que desee una instalación completamente nueva de Trident. Para desinstalar Trident sin eliminar CRD, consulte "[Desinstale Trident](#)".

### Operador de Trident

Para desinstalar Trident y eliminar por completo los CRD mediante el operador Trident:

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

### Timón

Para desinstalar Trident y eliminar por completo los CRD mediante Helm:

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

### `tridentctl`

Para eliminar completamente los CRD después de desinstalar Trident utilizando `tridentctl`

```
tridentctl obliviate crd
```

## Se produce un error al anular el almacenamiento en caché del nodo de NVMe con espacios de nombres de bloque sin configurar RWX o Kubernetes 1,26

Si ejecuta Kubernetes 1,26, la anulación del almacenamiento provisional del nodo puede fallar cuando se usa NVMe/TCP con espacios de nombres de bloque sin configurar de RWX. Los siguientes escenarios proporcionan una solución alternativa al fallo. También puede actualizar Kubernetes a 1,27.

### Se ha eliminado el espacio de nombres y el pod

Piense en un escenario en el que tenga un espacio de nombres gestionado por Trident (volumen persistente NVMe) conectado a un pod. Si elimina el espacio de nombres directamente desde el backend de ONTAP, el proceso de anulación del almacenamiento provisional se bloquea después de intentar eliminar el pod. Este escenario no afecta al clúster de Kubernetes ni a otro funcionamiento.

### Solución alternativa

Desmonte el volumen persistente (que corresponde al espacio de nombres) del nodo correspondiente y elimínelo.

### LIF de datos bloqueadas

If you block (or bring down) all the dataLIFs of the NVMe Trident backend, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Solución alternativa

Abra dataLIFS para restaurar la funcionalidad completa.

## Se ha eliminado la asignación de espacio de nombres

If you remove the `hostNQN` of the worker node from the corresponding subsystem, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Solución alternativa

Añada el `hostNQN` de vuelta al subsistema.

## Soporte técnico

NetApp ofrece compatibilidad con Trident de distintas formas. Hay disponibles amplias opciones de soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un canal Discord.

### Ciclo de vida del soporte de Trident

Trident ofrece tres niveles de soporte en función de su versión. Consulte "[Compatibilidad con la versión del software NetApp para definiciones](#)".

#### Soporte completo

Trident proporciona soporte completo durante doce meses a partir de la fecha de lanzamiento.

#### Soporte limitado

Trident ofrece soporte limitado durante los meses 13 - 24 desde la fecha de lanzamiento.

#### Autosozporte

La documentación de Trident está disponible durante los meses 25 - 36 desde la fecha de lanzamiento.

Versión	Soporte completo	Soporte limitado	Autosozporte
"24,10"	Octubre de 2025	Octubre de 2026	Octubre de 2027
"24,06"	Junio de 2025	Junio de 2026	Junio de 2027
"24,02"	Febrero de 2025	Febrero de 2026	Febrero de 2027
"23,10"	Octubre de 2024	Octubre de 2025	Octubre de 2026

Versión	Soporte completo	Soporte limitado	Autosozporte
"23,07"	Julio de 2024	Julio de 2025	Julio de 2026
"23,04"	—	Abril de 2025	Abril de 2026
"23,01"	—	A enero de 2025	A enero de 2026
"22,10"	—	Octubre de 2024	Octubre de 2025
"22,07"	—	Julio de 2024	Julio de 2025
"22,04"	—	—	Abril de 2025
"22,01"	—	—	A enero de 2025

## Autosozporte

Para obtener una lista completa de artículos de solución de problemas, consulte ["Base de conocimientos de NetApp \(se requiere inicio de sesión\)"](#) .

## Soporte de la comunidad

Hay una vibrante comunidad pública de usuarios de contenedores (incluidos los desarrolladores de Trident) en nuestro ["Canal de discordia"](#). Este es un gran lugar para hacer preguntas generales sobre el proyecto y discutir temas relacionados con compañeros de ideas afines.

## Soporte técnico de NetApp

Si necesita ayuda con Trident, cree un paquete de soporte con `tridentctl logs -a -n trident` y envíelo a `NetApp Support <Getting Help>`.

## Si quiere más información

- ["Recursos de Trident"](#)
- ["Kubernetes Hub"](#)

# Referencia

## Puertos Trident

Obtenga más información sobre los puertos que Trident utiliza para la comunicación.

### Puertos Trident

Trident se comunica a través de los siguientes puertos:

Puerto	Específico
8443	HTTPS de canal posterior
8001	Extremo de métricas de Prometheus
8000	Servidor REST de Trident
17546	Puerto de sonda de presencia/preparación utilizado por los pods demonset de Trident



El puerto de la sonda de nivel de gravedad/preparación se puede cambiar durante la instalación utilizando el `--probe-port` bandera. Es importante asegurarse de que este puerto no esté siendo utilizado por otro proceso en los nodos de trabajo.

## API de REST de Trident

Si bien "[comandos y opciones de tridentctl](#)" es la forma más sencilla de interactuar con la API DE REST DE Trident, puede usar el extremo de REST directamente, si lo prefiere.

### Cuándo utilizar la API DE REST

La API de REST es útil para instalaciones avanzadas que usan Trident como binario independiente en puestas en marcha que no son de Kubernetes.

Para una mayor seguridad, Trident REST API está restringido a localhost de forma predeterminada cuando se ejecuta dentro de un pod. Para cambiar este comportamiento, debe establecer el argumento de Trident `-address` en su configuración de pod.

### Uso de la API DE REST

Para ver ejemplos de cómo se llaman a estas API, pase (`-d` el indicador DEBUG ). Para obtener más información, consulte "[Gestione Trident con tridentctl](#)".

La API funciona de la siguiente manera:

#### OBTENGA

**GET** `<trident-address>/trident/v1/<object-type>`

Muestra todos los objetos de ese tipo.

**GET** <trident-address>/trident/v1/<object-type>/<object-name>

Obtiene los detalles del objeto con nombre.

## PUBLICAR

**POST** <trident-address>/trident/v1/<object-type>

Crea un objeto del tipo especificado.

- Requiere la configuración de JSON para el objeto que se cree. Para conocer la especificación de cada tipo de objeto, consulte "[Gestione Trident con tridentctl](#)".
- Si el objeto ya existe, el comportamiento varía: Los back-ends actualizan el objeto existente, mientras que todos los demás tipos de objeto fallarán la operación.

## ELIMINAR

**DELETE** <trident-address>/trident/v1/<object-type>/<object-name>

Suprime el recurso con nombre.



Seguirán existiendo volúmenes asociados con back-ends o clases de almacenamiento, que deben eliminarse por separado. Para obtener más información, consulte "[Gestione Trident con tridentctl](#)".

# Opciones de línea de comandos

Trident expone varias opciones de línea de comandos para Trident orchestrator. Puede usar estas opciones para modificar la implementación.

## Registro

**-debug**

Activa la salida de depuración.

**-loglevel <level>**

Establece el nivel de registro (debug, info, warn, error, fatal). Por defecto es info.

## Kubernetes

**-k8s\_pod**

Utilice esta opción o **-k8s\_api\_server** Para habilitar la compatibilidad con Kubernetes. Al configurar esto, Trident usa las credenciales de cuenta del servicio de Kubernetes del pod para contactar con el servidor de API. Esto solo funciona cuando Trident se ejecuta como un pod en un clúster de Kubernetes con cuentas de servicio habilitadas.

**-k8s\_api\_server <insecure-address:insecure-port>**

Utilice esta opción o **-k8s\_pod** para habilitar el soporte de Kubernetes. Cuando se especifica, Trident se conecta al servidor API de Kubernetes mediante el puerto y la dirección no seguras que se proporcionan. Esto permite que Trident se implemente fuera de un pod; sin embargo, solo admite conexiones no seguras con el servidor API. Para conectarse de forma segura, implemente Trident en un pod con la **-k8s\_pod** opción.

## Docker

**-volume\_driver <name>**

Nombre del controlador utilizado al registrar el plugin de Docker. De forma predeterminada es `netapp`.

**-driver\_port <port-number>**

Reciba en este puerto en lugar de en un socket de dominio UNIX.

**-config <file>**

Necesario; debe especificar esta ruta de acceso a un archivo de configuración de backend.

## DESCANSO

**-address <ip-or-host>**

Especifica la dirección en la que debe escuchar el servidor REST DE Trident. El valor predeterminado es `localhost`. Cuando se escucha en `localhost` y se ejecuta dentro de un pod Kubernetes, la interfaz REST no es accesible desde fuera del pod. Uso `-address ""` Para hacer que la interfaz DE REST sea accesible desde la dirección IP del pod.



La interfaz DE REST de Trident se puede configurar para escuchar y servir únicamente en `127.0.0.1` (para IPv4) o `:::1` (para IPv6).

**-port <port-number>**

Especifica el puerto en el que debe recibir el servidor REST DE Trident. El valor predeterminado es `8000`.

**-rest**

Habilita la interfaz DE REST. El valor predeterminado es `TRUE`.

## Objetos de Kubernetes y Trident

Puede interactuar con Kubernetes y Trident mediante las API DE REST a través de la lectura y la escritura de objetos de recursos. Existen varios objetos de recursos que dictan la relación entre Kubernetes y Trident, Trident y el almacenamiento, y Kubernetes y el almacenamiento. Algunos de estos objetos se gestionan mediante Kubernetes y los demás se gestionan mediante Trident.

### ¿Cómo interactúan los objetos entre sí?

Quizás la forma más sencilla de comprender los objetos, qué hacen y cómo interactúan sea, es seguir una única solicitud de almacenamiento a un usuario de Kubernetes:

1. Un usuario crea un `PersistentVolumeClaim` solicitando un nuevo `PersistentVolume` De un tamaño concreto de un Kubernetes `StorageClass` previamente configurado por el administrador.
2. Kubernetes `StorageClass` Identifica a Trident como su proveedor y incluye los parámetros que indican a Trident cómo aprovisionar un volumen para la clase solicitada.
3. Trident analiza sus propios recursos `StorageClass` con el mismo nombre que identifica la coincidencia `Backends` y.. `StoragePools` que puede usar para aprovisionar volúmenes para la clase.



4. Trident aprovisiona el almacenamiento en un back-end coincidente y crea dos objetos: Un `PersistentVolume` En Kubernetes, donde se indica cómo encontrar, montar y tratar el volumen, y un volumen en Trident que conserva la relación entre `PersistentVolume` y el almacenamiento real.
5. Kubernetes enlaza con el `PersistentVolumeClaim` a los nuevos `PersistentVolume`. Pods que incluyen `PersistentVolumeClaim` monte ese volumen persistente en cualquier host en el que se ejecute.
6. Un usuario crea un `VolumeSnapshot` De un PVC existente, utilizando un `VolumeSnapshotClass` Eso es lo que apunta a Trident.
7. Trident identifica el volumen asociado con la RVP y crea una copia Snapshot del volumen en su back-end. También crea un `VolumeSnapshotContent` Esto indica a Kubernetes cómo identificar la snapshot.
8. Un usuario puede crear un `PersistentVolumeClaim` uso `VolumeSnapshot` como origen.
9. Trident identifica la instantánea necesaria y realiza el mismo conjunto de pasos involucrados en la creación de un `PersistentVolume` y un `Volume`.



Para obtener más información sobre los objetos de Kubernetes, recomendamos encarecidamente que lea la "[Volúmenes persistentes](#)" De la documentación de Kubernetes.

## Kubernetes `PersistentVolumeClaim` objetos

Un Kubernetes `PersistentVolumeClaim` El objeto es una solicitud de almacenamiento que realiza un usuario de clúster de Kubernetes.

Además de la especificación estándar, Trident permite a los usuarios especificar las siguientes anotaciones específicas del volumen si desean anular los valores predeterminados que se establecen en la configuración de back-end:

Anotación	Opción de volumen	Controladores compatibles
<code>trident.netapp.io/fileSystem</code>	Sistema de archivos	ontap-san, solidfire-san, ontap-san-economy
<code>trident.netapp.io/cloneFromPVC</code>	ClonSourceVolume	ontap-nas, ontap-san, solidfire-san, azure-netapp-files, gcp-cvs, ontap-san-economía
<code>trident.netapp.io/splitOnClone</code>	SplitOnClone	ontap-nas y ontap-san
<code>trident.netapp.io/protocol</code>	protocolo	cualquiera
<code>trident.netapp.io/exportPolicy</code>	Política de exportoPolicy	ontap-nas, ontap-nas-economy y ontap-nas-flexgroup
<code>trident.netapp.io/snapshotPolicy</code>	Política de copias Snapshot	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup y ontap-san
<code>trident.netapp.io/snapshotReserve</code>	Reserva de copias Snapshot	ontap-nas, ontap-nas-flexgroup, ontap-san, gcp-cvs
<code>trident.netapp.io/snapshotDirectory</code>	Snapshot shotDirectory	ontap-nas, ontap-nas-economy y ontap-nas-flexgroup
<code>trident.netapp.io/unixPermissions</code>	Permisos univalados	ontap-nas, ontap-nas-economy y ontap-nas-flexgroup

Anotación	Opción de volumen	Controladores compatibles
<code>trident.netapp.io/blockSize</code>	Tamaño del bloque	solidfire-san

Si el VP creado tiene el `Delete` Reclamar política, Trident elimina el VP y el volumen de respaldo cuando se libera el VP (es decir, cuando el usuario elimina la RVP). Si la acción de eliminación falla, Trident Marca el VP como tal y reintenta periódicamente la operación hasta que esta se complete o se elimine manualmente el VP. Si el VP utiliza `Retain` Política, Trident ignora la operación y asume que el administrador la limpiará desde Kubernetes y el back-end, lo que permitirá realizar un backup o la inspección del volumen antes de su eliminación. Tenga en cuenta que al eliminar el VP, Trident no eliminará el volumen de backup. Debe quitarlo usando la API DE REST (`tridentctl`).

Trident admite la creación de instantáneas de volumen utilizando la especificación CSI: Puede crear una instantánea de volumen y utilizarla como origen de datos para clonar las RVP existentes. De este modo, las copias puntuales de VP pueden exponerse a Kubernetes en forma de snapshots. Las instantáneas pueden utilizarse para crear nuevos VP. Eche un vistazo `On-Demand Volume Snapshots` para ver cómo funcionaría.

Trident también proporciona la `cloneFromPVC` y `splitOnClone` anotaciones para crear clones. Puede utilizar estas anotaciones para clonar una RVP sin tener que utilizar la implementación de CSI.

A continuación se muestra un ejemplo: Si un usuario ya tiene una RVP llamada `mysql`, El usuario puede crear un nuevo PVC llamado `mysqlclone` mediante la anotación, por ejemplo `trident.netapp.io/cloneFromPVC: mysql`. Con este conjunto de anotaciones, Trident clona el volumen correspondiente a la RVP de `mysql`, en lugar de aprovisionar un volumen desde cero.

Considere los siguientes puntos:

- Se recomienda clonar un volumen inactivo.
- Una RVP y su clon deben estar en el mismo espacio de nombres de Kubernetes y tener el mismo tipo de almacenamiento.
- Con la `ontap-nas` y `ontap-san` Controladores, es posible que sea conveniente establecer la anotación de PVC `trident.netapp.io/splitOnClone` en conjunto con `trident.netapp.io/cloneFromPVC`. Con `trident.netapp.io/splitOnClone` establezca en `true`, Trident divide el volumen clonado del volumen principal y, por lo tanto, separa completamente el ciclo de vida del volumen clonado de su principal a costa de perder alguna eficiencia de almacenamiento. No está configurado `trident.netapp.io/splitOnClone` o establecerlo en `false` provoca una reducción del consumo de espacio en el back-end a costa de crear dependencias entre los volúmenes principal y clonado, de modo que no se pueda eliminar el volumen principal, a menos que el clon se elimine primero. Una situación en la que dividir el clon tiene sentido es clonar un volumen de base de datos vacío donde se espera que tanto el volumen como su clon desvíen enormemente y no se beneficien de las eficiencias del almacenamiento ofrecidas por ONTAP.

La `sample-input` el directorio contiene ejemplos de definiciones de PVC para utilizarlas con Trident. Consulte Para obtener una descripción completa de los parámetros y la configuración asociados con los volúmenes de Trident.

## Kubernetes `PersistentVolume` objetos

Un Kubernetes `PersistentVolume` Object representa un fragmento de almacenamiento que se pone a disposición del clúster de Kubernetes. Tiene un ciclo de vida independiente del pod que lo utiliza.



Crea Trident `PersistentVolume` Los objetos y los registra automáticamente con el clúster Kubernetes en función de los volúmenes que aprovisiona. No se espera que usted los gestione usted mismo.

Cuando se crea una RVP que hace referencia a un sistema basado en Trident `StorageClass`, Trident aprovisiona un nuevo volumen utilizando la clase de almacenamiento correspondiente y registra un nuevo VP para ese volumen. Al configurar el volumen aprovisionado y el VP correspondiente, Trident sigue las siguientes reglas:

- Trident genera un nombre PV para Kubernetes y un nombre interno que utiliza para aprovisionar el almacenamiento. En ambos casos, se asegura de que los nombres son únicos en su alcance.
- El tamaño del volumen coincide con el tamaño solicitado en el PVC lo más cerca posible, aunque podría redondearse a la cantidad más cercana asignable, dependiendo de la plataforma.

## Kubernetes `StorageClass` objetos

Kubernetes `StorageClass` los objetos se especifican por nombre en `PersistentVolumeClaims` para aprovisionar el almacenamiento con una serie de propiedades. La clase de almacenamiento identifica el aprovisionador que se usará y define ese conjunto de propiedades en términos que entiende el aprovisionador.

Es uno de los dos objetos básicos que el administrador debe crear y gestionar. El otro es el objeto back-end de Trident.

Un Kubernetes `StorageClass` Objeto que usa Trident tiene el siguiente aspecto:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters:
  <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate
```

Estos parámetros son específicos de Trident y dicen a Trident cómo aprovisionar volúmenes para la clase.

Los parámetros de la clase de almacenamiento son:

Atributo	Tipo	Obligatorio	Descripción
atributos	map[string]string	no	Consulte la sección atributos a continuación
Pools de almacenamiento	Map[string]StringList	no	Asignación de nombres de back-end a listas de pools de almacenamiento dentro

Atributo	Tipo	Obligatorio	Descripción
AdicionalStoragePools	Map[string]StringList	no	Asignación de nombres de back-end a listas de pools de almacenamiento dentro
ExcludeStoragePools	Map[string]StringList	no	Asignación de nombres de back-end a listas de pools de almacenamiento dentro

Los atributos de almacenamiento y sus posibles valores se pueden clasificar en atributos de selección de pools de almacenamiento y atributos de Kubernetes.

### Atributos de selección del pool de almacenamiento

Estos parámetros determinan qué pools de almacenamiento gestionados por Trident se deben utilizar para aprovisionar volúmenes de un determinado tipo.

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
media 1	cadena	hdd, híbrido, ssd	Pool contiene medios de este tipo; híbrido significa ambos	Tipo de medios especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san y solidfire-san
AprovisionaciónTipo	cadena	delgado, grueso	El pool admite este método de aprovisionamiento	Método de aprovisionamiento o especificado	grueso: all ONTAP; thin: all ONTAP y solidfire-san
Tipo de backendType	cadena	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool pertenece a este tipo de backend	Backend especificado	Todos los conductores
snapshot	bool	verdadero, falso	El pool admite volúmenes con Snapshot	Volumen con snapshots habilitadas	ontap-nas, ontap-san, solidfire-san y gcp-cvs
clones	bool	verdadero, falso	Pool admite el clonado de volúmenes	Volumen con clones habilitados	ontap-nas, ontap-san, solidfire-san y gcp-cvs

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
cifrado	bool	verdadero, falso	El pool admite volúmenes cifrados	Volumen con cifrado habilitado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	int	entero positivo	El pool es capaz de garantizar IOPS en este rango	El volumen garantizado de estas IOPS	solidfire-san

Esta versión 1: No es compatible con sistemas ONTAP Select

En la mayoría de los casos, los valores solicitados influyen directamente en el aprovisionamiento; por ejemplo, solicitar un aprovisionamiento de alto rendimiento da lugar a un volumen considerablemente aprovisionado. Sin embargo, un pool de almacenamiento de Element utiliza el valor mínimo y máximo de IOPS que ofrece para establecer los valores de calidad de servicio, en lugar del valor solicitado. En este caso, el valor solicitado se utiliza solo para seleccionar el pool de almacenamiento.

Lo ideal es que pueda usar `attributes` solo para modelar las cualidades del almacenamiento que necesita para satisfacer las necesidades de una clase particular. Trident detecta y selecciona automáticamente pools de almacenamiento que coincidan *all* del `attributes` que especifique.

Si no puede utilizar `attributes` para seleccionar automáticamente los grupos adecuados para una clase, puede utilizar `storagePools` y `additionalStoragePools` parámetros para refinar más los pools o incluso seleccionar un conjunto específico de agrupaciones.

Puede utilizar el `storagePools` el parámetro para restringir aún más el conjunto de pools que coinciden con cualquier especificado `attributes`. En otras palabras, Trident utiliza la intersección de pools identificados por el `attributes` y `storagePools` parámetros para el aprovisionamiento. Es posible usar un parámetro solo o ambos juntos.

Puede utilizar el `additionalStoragePools` Parámetro para ampliar el conjunto de pools que Trident utiliza para el aprovisionamiento, independientemente de cualquier pool que seleccione `attributes` y `storagePools` parámetros.

Puede utilizar el `excludeStoragePools` Parámetro para filtrar el conjunto de pools que Trident utiliza para el aprovisionamiento. Cuando se usa este parámetro, se quitan todos los pools que coinciden.

En la `storagePools` y `additionalStoragePools` parámetros, cada entrada toma el formulario `<backend>:<storagePoolList>`, donde `<storagePoolList>` es una lista de pools de almacenamiento separados por comas para el back-end especificado. Por ejemplo, un valor para `additionalStoragePools` puede parecer `ontapnas_192.168.1.100:aggr1,aggr2;solidfire_192.168.1.101:bronze`. Estas listas aceptan valores regex para los valores de backend y list. Puede utilizar `tridentctl get backend` para obtener la lista de los back-ends y sus pools.

## Atributos de Kubernetes

Trident no afecta a la selección de pools y back-ends de almacenamiento durante el aprovisionamiento dinámico. En su lugar, estos atributos simplemente ofrecen parámetros compatibles con los volúmenes persistentes de Kubernetes. Los nodos de trabajo son responsables de las operaciones de creación del sistema de archivos y pueden requerir utilidades del sistema de archivos, como `xfsprogs`.

Atributo	Tipo	Valores	Descripción	Controladores relevantes	Versión de Kubernetes
Tipo fstype	cadena	ext4, ext3, xfs	El tipo de sistema de archivos para los volúmenes de bloques	solidfire-san, ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economía	Todo
Expansión de allowVolume	booleano	verdadero, falso	Habilite o deshabilite el soporte para aumentar el tamaño de PVC	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy, solidfire-san, gcp-cvs, azure-netapp-files	1.11 o posterior
VolumeBindingMode	cadena	Inmediatamente, WaitForFirstConsumer	Elija cuándo se producen el enlace de volumen y el aprovisionamiento o dinámico	Todo	1.19 - 1.26

- La `fsType` El parámetro se utiliza para controlar el tipo de sistema de archivos deseado para las LUN DE SAN. Además, Kubernetes utiliza también la presencia de `fsType` en una clase de almacenamiento para indicar que existe un sistema de archivos. La propiedad del volumen se puede controlar mediante la `fsGroup` contexto de seguridad de un pod solo if `fsType` está configurado. Consulte "[Kubernetes: Configure un contexto de seguridad para un Pod o contenedor](#)" para obtener información general sobre la configuración de la propiedad del volumen con `fsGroup` contexto. Kubernetes aplicará el `fsGroup` valor solo si:

- `fsType` se establece en la clase de almacenamiento.
- El modo de acceso de PVC es RWO.



Para los controladores de almacenamiento NFS, ya existe un sistema de archivos como parte de la exportación NFS. Para utilizar `fsGroup` la clase de almacenamiento aún debe especificar un `fsType`. Puede configurarlo en `nfs` o cualquier valor que no sea nulo.

- Consulte "[Expanda los volúmenes](#)" para obtener más información sobre la expansión de volumen.
- El paquete de instalación de Trident proporciona varias definiciones de clase de almacenamiento de ejemplo para usar con Trident en `sample-input/storage-class*.yaml`. Al eliminar una clase de almacenamiento Kubernetes, también se elimina el tipo de almacenamiento Trident correspondiente.

## Kubernetes VolumeSnapshotClass objetos

Kubernetes `VolumeSnapshotClass` los objetos son similares `StorageClasses`. Ayudan a definir varias clases de almacenamiento y las instantáneas de volumen hacen referencia a ellas para asociar la snapshot a la clase de snapshot necesaria. Cada copia de Snapshot de volumen se asocia con una sola clase de copia de Snapshot de volumen.

1. `VolumeSnapshotClass` debe ser definido por un administrador para crear snapshots. Una clase de snapshot de volumen se crea con la siguiente definición:

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

La `driver` Especifica a Kubernetes que solicitudes de snapshots de volumen del `csi-snapclass` Trident gestiona la clase. La `deletionPolicy` especifica la acción que se debe realizar cuando se debe eliminar una instantánea. Cuando `deletionPolicy` se establece en `Delete`, los objetos de instantánea del volumen, así como la instantánea subyacente en el clúster de almacenamiento, se eliminan cuando se elimina una instantánea. Como alternativa, establecerlo en `Retain` significa eso `VolumeSnapshotContent` y se conserva la snapshot física.

## Kubernetes VolumeSnapshot objetos

Un Kubernetes `VolumeSnapshot` objeto es una solicitud para crear una copia de snapshot de un volumen. Del mismo modo que la RVP representa una solicitud al usuario para un volumen, un snapshot de volumen es una solicitud al que hace un usuario para crear una copia Snapshot de una RVP existente.

Cuando llega una solicitud Snapshot de volumen, Trident gestiona automáticamente la creación de la snapshot para el volumen en el back-end y expone la snapshot creando un único `VolumeSnapshotContent` objeto. Puede crear instantáneas a partir de EVs existentes y utilizar las instantáneas como `DataSource` al crear nuevas CVP.



El ciclo de vida de un `VolumeSnapshot` es independiente del PVC de origen: Una instantánea persiste incluso después de eliminar el PVC de origen. Cuando se elimina un PVC que tiene instantáneas asociadas, Trident Marca el volumen de respaldo de este PVC con el estado **Eliminación**, pero no lo elimina por completo. El volumen se elimina cuando se eliminan todas las Snapshot asociadas.

## Kubernetes VolumeSnapshotContent objetos

Un Kubernetes `VolumeSnapshotContent` object representa una snapshot tomada de un volumen ya provisionado. Es similar a un `PersistentVolume` y significa una instantánea provisionada en el clúster de almacenamiento. Similar a `PersistentVolumeClaim`. `PersistentVolume` los objetos, cuando se crea una snapshot, el `VolumeSnapshotContent` object mantiene una asignación de uno a uno `VolumeSnapshot` objeto, que solicitó la creación de la snapshot.

La `VolumeSnapshotContent` el objeto contiene detalles que identifican de manera única la instantánea, como la `snapshotHandle`. Este `snapshotHandle` Es una combinación única del nombre del PV y el nombre del `VolumeSnapshotContent` objeto.

Cuando llega una solicitud de Snapshot, Trident crea la snapshot en el back-end. Una vez creada la copia de Snapshot, Trident configura un `VolumeSnapshotContent` Objeto y, por lo tanto, expone la snapshot a la API de Kubernetes.



Por lo general, no es necesario administrar el `VolumeSnapshotContent` objeto. Una excepción a esto es cuando se desea "[importe una copia de snapshot de volumen](#)" crear fuera de Trident.

## Kubernetes CustomResourceDefinition objetos

Los recursos personalizados de Kubernetes son extremos en la API de Kubernetes que define el administrador y que se usan para agrupar objetos similares. Kubernetes admite la creación de recursos personalizados para almacenar un conjunto de objetos. Puede obtener estas definiciones de recursos ejecutando `kubectl get crds`.

Kubernetes almacena en su almacén de metadatos las definiciones de recursos personalizadas (CRD) y los metadatos de objetos asociados. De este modo, no es necesario disponer de un almacén aparte para Trident.

Trident usa `CustomResourceDefinition` objetos para conservar la identidad de objetos de Trident, como los back-ends de Trident, las clases de almacenamiento Trident y los volúmenes de Trident. Trident gestiona estos objetos. Además, el marco de instantáneas de volumen CSI introduce algunos CRD necesarios para definir instantáneas de volumen.

Los multos son una estructura de Kubernetes. Trident crea los objetos de los recursos definidos anteriormente. Como ejemplo simple, cuando se crea un back-end usando `tridentctl`, a correspondiente `tridentbackends` El objeto CRD se crea para el consumo por parte de Kubernetes.

A continuación se indican algunos puntos que hay que tener en cuenta sobre los CRD de Trident:

- Cuando se instala Trident, se crea un conjunto de CRD que se puede utilizar como cualquier otro tipo de recurso.
- Al desinstalar Trident mediante la `tridentctl uninstall` Comando, los pods de Trident se eliminan, pero los CRD creados no se borran. Consulte "[Desinstale Trident](#)" Para comprender cómo Trident se puede eliminar por completo y volver a configurar desde cero.

## Objetos deTrident StorageClass

Trident crea clases de almacenamiento coincidentes para Kubernetes `StorageClass` objetos que especifican `csi.trident.netapp.io` en su campo de aprovisionamiento. El nombre de la clase de almacenamiento coincide con el de Kubernetes `StorageClass` objeto que representa.



Con Kubernetes, estos objetos se crean automáticamente cuando se crea un Kubernetes `StorageClass` Que usa Trident como aprovisionador está registrado.

Las clases de almacenamiento comprenden un conjunto de requisitos para los volúmenes. Trident enlaza estos requisitos con los atributos presentes en cada pool de almacenamiento; si coinciden, ese pool de almacenamiento es un objetivo válido para aprovisionar volúmenes que utilizan esa clase de almacenamiento.



Puede crear configuraciones de clase de almacenamiento para definir clases de almacenamiento directamente mediante la API DE REST. Sin embargo, en el caso de las puestas en marcha de Kubernetes, esperamos que se creen al registrar el nuevo Kubernetes `StorageClass` objetos.

## Objetos de back-end de Trident

Los back-ends representan a los proveedores de almacenamiento, además de los cuales Trident aprovisiona volúmenes; una única instancia de Trident puede gestionar cualquier número de back-ends.



Éste es uno de los dos tipos de objeto que se crean y administran a sí mismo. El otro es Kubernetes `StorageClass` objeto.

Para obtener más información sobre cómo construir estos objetos, consulte ["configuración de los back-ends"](#).

## Objetos deTrident `StoragePool`

Los pools de almacenamiento representan las distintas ubicaciones disponibles para aprovisionar en cada back-end. Para ONTAP, corresponden a los agregados en las SVM. Para HCI/SolidFire de NetApp, corresponden a las bandas de calidad de servicio especificadas por el administrador. Para Cloud Volumes Service, se corresponden con las regiones de proveedores de cloud. Cada pool de almacenamiento tiene un conjunto de atributos de almacenamiento distintos que definen sus características de rendimiento y sus características de protección de datos.

Al contrario de lo que ocurre con otros objetos aquí, los candidatos de pools de almacenamiento siempre se detectan y gestionan automáticamente.

## Objetos deTrident `Volume`

Los volúmenes son la unidad básica de aprovisionamiento y constan de extremos back-end, como recursos compartidos de NFS y LUN iSCSI. En Kubernetes, se corresponden directamente con `PersistentVolumes`. Cuando crea un volumen, asegúrese de que tiene una clase de almacenamiento, que determina dónde se puede aprovisionar ese volumen junto con un tamaño.



- En Kubernetes, estos objetos se gestionan automáticamente. Es posible verlos para ver qué ha aprovisionado Trident.
- Al eliminar un VP con instantáneas asociadas, el volumen Trident correspondiente se actualiza a un estado **Eliminación**. Para que se elimine el volumen de Trident, es necesario quitar las snapshots del volumen.

Una configuración de volumen define las propiedades que debe tener un volumen aprovisionado.

Atributo	Tipo	Obligatorio	Descripción
versión	cadena	no	Versión de la API de Trident ("1")
nombre	cadena	sí	Nombre del volumen que se va a crear
Clase de almacenamiento	cadena	sí	Clase de almacenamiento que se utilizará al aprovisionar el volumen

Atributo	Tipo	Obligatorio	Descripción
tamaño	cadena	sí	El tamaño del volumen que se va a aprovisionar en bytes
protocolo	cadena	no	Tipo de protocolo que se va a utilizar; "archivo" o "bloque"
InternalName	cadena	no	Nombre del objeto en el sistema de almacenamiento, generado por Trident
ClonSourceVolume	cadena	no	ONTAP (nas, san) y SolidFire-*: Nombre del volumen desde el que se va a clonar
SplitOnClone	cadena	no	ONTAP (nas, san): Divide el clon entre su primario
Política de copias Snapshot	cadena	no	ONTAP-*: Política de instantánea a utilizar
Reserva de copias Snapshot	cadena	no	ONTAP-*: Porcentaje del volumen reservado para instantáneas
Política de exportoPolicy	cadena	no	ontap-nas*: Política de exportación que se va a utilizar
Snapshot shotDirectory	bool	no	ontap-nas*: Si el directorio de instantáneas está visible
Permisos univalados	cadena	no	ontap-nas*: Permisos iniciales de UNIX
Tamaño del bloque	cadena	no	SolidFire-*: Tamaño de bloque/sector
Sistema de archivos	cadena	no	Tipo de sistema de archivos

Genera Trident `internalName` al crear el volumen. Esto consta de dos pasos. En primer lugar, prepens el prefijo de almacenamiento (ya sea el predeterminado `trident` o el prefijo de la configuración del back-end) al nombre del volumen, lo que genera el nombre del formulario `<prefix>-<volume-name>`. A continuación, procede a desinfectar el nombre y a reemplazar los caracteres no permitidos en el backend. En los back-ends de ONTAP, reemplaza guiones con guiones bajos (de esta forma, el nombre interno se convierte en `<prefix>_<volume-name>`). En los back-ends de Element, reemplaza guiones bajos por guiones.

Puede utilizar configuraciones de volumen para aprovisionar directamente los volúmenes mediante la API REST, pero en las puestas en marcha de Kubernetes esperamos que la mayoría de los usuarios usen el Kubernetes estándar `PersistentVolumeClaim` método. Trident crea este objeto de volumen automáticamente como parte del proceso de aprovisionamiento.

## Objetos de Trident Snapshot

Las Snapshot son una copia de un momento específico de los volúmenes, que se pueden usar para aprovisionar nuevos volúmenes o restaurar el estado. En Kubernetes, se corresponden directamente con `VolumeSnapshotContent` objetos. Cada copia de Snapshot se asocia con un volumen, que es el origen de los datos de la copia de Snapshot.

Cada uno `Snapshot` object incluye las propiedades que se enumeran a continuación:

Atributo	Tipo	Obligatorio	Descripción
versión	Cadena	Sí	Versión de la API de Trident ("1")
nombre	Cadena	Sí	Nombre del objeto Snapshot de Trident
InternalName	Cadena	Sí	Nombre del objeto Snapshot de Trident en el sistema de almacenamiento
Nombre de volumen	Cadena	Sí	Nombre del volumen persistente para el que se crea la snapshot
VolumeInternalName	Cadena	Sí	Nombre del objeto de volumen de Trident asociado en el sistema de almacenamiento



En Kubernetes, estos objetos se gestionan automáticamente. Es posible verlos para ver qué ha aprovisionado Trident.

Cuando un Kubernetes `VolumeSnapshot` Se crea la solicitud del objeto, Trident funciona mediante la creación de un objeto Snapshot en el sistema de almacenamiento que realiza backups. La `internalName` de este objeto snapshot se genera combinando el prefijo `snapshot-` con la UID de la `VolumeSnapshot` objeto (por ejemplo, `snapshot-e8d8a0ca-9826-11e9-9807-525400f3f660`). `volumeName` y `volumeInternalName` para rellenar, obtendrá los detalles del volumen de backup.

## Objeto Trident ResourceQuota

El desamonset de Trident consume una `system-node-critical` clase de prioridad, la clase de prioridad más alta disponible en Kubernetes, para garantizar que Trident pueda identificar y limpiar volúmenes durante el apagado de nodo correcto y permitir que los pods de inicio de datos de Trident se adelanten a las cargas de trabajo con una prioridad más baja en los clústeres donde hay una alta presión de recursos.

Para ello, Trident emplea un `ResourceQuota` objeto para garantizar que se satisfaga una clase de prioridad «crítica para el sistema en el inicio de datos de Trident. Antes de la implementación y la creación de `daemonset`, Trident busca `ResourceQuota` el objeto y, si no se detecta, lo aplica.

Si necesita más control sobre la cuota de recursos predeterminada y la clase de prioridad, puede generar una `custom.yaml` o configure el `ResourceQuota` Objeto mediante el gráfico Helm.

A continuación se muestra un ejemplo de un objeto "ResourceQuota" object que da prioridad al demonset de Trident.

```
apiVersion: <version>
kind: ResourceQuota
metadata:
  name: trident-csi
  labels:
    app: node.csi.trident.netapp.io
spec:
  scopeSelector:
    matchExpressions:
      - operator : In
        scopeName: PriorityClass
        values: ["system-node-critical"]
```

Para obtener más información sobre las cuotas de recursos, consulte ["Kubernetes: Cuotas de recursos"](#).

### **Limpie ResourceQuota si la instalación falla**

En el raro caso en que la instalación falle después del ResourceQuota se crea el objeto, primero se intenta ["desinstalar"](#) y, a continuación, vuelva a instalar.

Si esto no funciona, quite manualmente la ResourceQuota objeto.

### **Quitar ResourceQuota**

Si prefiere controlar su propia asignación de recursos, puede eliminar el objeto Trident ResourceQuota mediante el comando:

```
kubectrl delete quota trident-csi -n trident
```

## **Pod Security Standards (PSS) y las restricciones de contexto de seguridad (SCC)**

Los estándares de seguridad de Kubernetes Pod (PSS) y las políticas de seguridad de Pod (PSP) definen los niveles de permisos y restringen el comportamiento de los POD. OpenShift Security Context restriction (SCC) define de forma similar la restricción de POD específica para OpenShift Kubernetes Engine. Para proporcionar esta personalización, Trident permite ciertos permisos durante la instalación. En las siguientes secciones se detallan los permisos establecidos por Trident.



PSS reemplaza las políticas de seguridad de Pod (PSP). PSP quedó obsoleto en Kubernetes v1.21 y se eliminará en la versión 1.25. Para obtener más información, consulte ["Kubernetes: Seguridad"](#).

## Contexto de Kubernetes Security y campos relacionados necesarios

Permiso	Descripción
Privilegiado	CSI requiere que los puntos de montaje sean bidireccionales, lo que significa que el receptáculo del nodo Trident debe ejecutar un contenedor privilegiado. Para obtener más información, consulte <a href="#">"Kubernetes: Propagación de montaje"</a> .
Conexión a redes del host	Necesario para el daemon de iSCSI. <code>iscsiadm</code> Gestiona los montajes iSCSI y utiliza la conexión a redes host para comunicarse con el daemon iSCSI.
IPC del host	NFS utiliza la comunicación entre procesos (IPC) para comunicarse con NFSD.
PID del host	Necesario para iniciar <code>rpc-statd</code> para NFS. Trident consulta los procesos de host para determinar <code>rpc-statd</code> si se están ejecutando antes de montar los volúmenes de NFS.
Funcionalidades	La <code>SYS_ADMIN</code> la capacidad se proporciona como parte de las capacidades predeterminadas para los contenedores con privilegios. Por ejemplo, Docker establece estas funcionalidades para los contenedores con privilegios: <code>CapPrm: 0000003fffffffffff</code> <code>CapEff: 0000003fffffffffff</code>
Seccomp	El perfil de Seccomp siempre está «sin confinar» en contenedores privilegiados; por lo tanto, no se puede activar en Trident.
SELinux	En OpenShift, los contenedores con privilegios se ejecutan en el <code>spc_t</code> dominio («Super Privileged Container») y los contenedores sin privilegios se ejecutan en el <code>container_t</code> dominio. Activado <code>containerd</code> , con <code>container-selinux</code> instalado, todos los contenedores se ejecutan en el <code>spc_t</code> dominio, lo que desactiva efectivamente SELinux. Por lo tanto, Trident no <code>seLinuxOptions</code> agrega a los contenedores.
DAC	Los contenedores con privilegios deben ejecutarse como root. Los contenedores no privilegiados se ejecutan como root para acceder a los sockets unix necesarios para CSI.

## Estándares de seguridad para POD (PSS)

Etiqueta	Descripción	Predeterminado
pod-security.kubernetes.io/enforce	Permite admitir la controladora Trident y los nodos en el espacio de nombres de instalación. No cambie la etiqueta de espacio de nombres.	enforce: privileged
pod-security.kubernetes.io/enforce-version		enforce-version: <version of the current cluster or highest version of PSS tested.>



El cambio de las etiquetas del espacio de nombres puede provocar que los POD no se programen, un "error al crear: ..." O bien, "Advertencia: trident-csi-...". Si esto sucede, compruebe si la etiqueta de espacio de nombres para `privileged` se ha cambiado. En ese caso, vuelva a instalar Trident.

## Directivas de seguridad de POD (PSP)

Campo	Descripción	Predeterminado
<code>allowPrivilegeEscalation</code>	Los contenedores con privilegios deben permitir la escala de privilegios.	true
<code>allowedCSIDrivers</code>	Trident no utiliza volúmenes efímeros de CSI en línea.	Vacío
<code>allowedCapabilities</code>	Los contenedores Trident no con privilegios no requieren más funcionalidades de las que se establece de forma predeterminada y se conceden todas las funcionalidades posibles a los contenedores con privilegios.	Vacío
<code>allowedFlexVolumes</code>	Trident no utiliza "Controlador FlexVolume", por lo tanto, no se incluyen en la lista de volúmenes permitidos.	Vacío
<code>allowedHostPaths</code>	El pod del nodo Trident monta el sistema de archivos raíz del nodo, por lo que no hay ninguna ventaja para configurar esta lista.	Vacío
<code>allowedProcMountTypes</code>	Trident no utiliza ninguna ProcMountTypes.	Vacío
<code>allowedUnsafeSysctls</code>	Trident no requiere que no sea seguro sysctls.	Vacío
<code>defaultAddCapabilities</code>	No es necesario añadir capacidades a contenedores con privilegios.	Vacío
<code>defaultAllowPrivilegeEscalation</code>	En cada POD de Trident, se permite el escalado de privilegios.	false

<b>Campo</b>	<b>Descripción</b>	<b>Predeterminado</b>
<code>forbiddenSysctls</code>	No <code>sysctls</code> se permiten.	Vacío
<code>fsGroup</code>	Los contenedores Trident se ejecutan como raíz.	<code>RunAsAny</code>
<code>hostIPC</code>	El montaje de volúmenes NFS requiere que el IPC del host se comunique con <code>nfsd</code>	<code>true</code>
<code>hostNetwork</code>	<code>lscsiadm</code> requiere que la red del host se comunique con el demonio iSCSI.	<code>true</code>
<code>hostPID</code>	Se requiere el PID del host para comprobar si <code>rpc-statd</code> está ejecutándose en el nodo.	<code>true</code>
<code>hostPorts</code>	Trident no utiliza puertos de host.	Vacío
<code>privileged</code>	Los pods de nodo Trident deben ejecutar un contenedor privilegiado para montar volúmenes.	<code>true</code>
<code>readOnlyRootFilesystem</code>	Los contenedores de nodos Trident deben escribir en el sistema de archivos del nodo.	<code>false</code>
<code>requiredDropCapabilities</code>	Los pods de nodo de Trident ejecutan un contenedor privilegiado y no pueden soltar las funcionalidades.	<code>none</code>
<code>runAsGroup</code>	Los contenedores Trident se ejecutan como raíz.	<code>RunAsAny</code>
<code>runAsUser</code>	Los contenedores Trident se ejecutan como raíz.	<code>runAsAny</code>
<code>runtimeClass</code>	Trident no utiliza <code>RuntimeClasses</code> .	Vacío
<code>seLinux</code>	Trident no está configurado <code>seLinuxOptions</code> Debido a que actualmente existen diferencias en el modo en que los tiempos de ejecución de contenedores y las distribuciones de Kubernetes se encargan de SELinux.	Vacío
<code>supplementalGroups</code>	Los contenedores Trident se ejecutan como raíz.	<code>RunAsAny</code>
<code>volumes</code>	Los pods de Trident requieren estos complementos de volumen.	<code>hostPath</code> , <code>projected</code> , <code>emptyDir</code>

## Restricciones de contexto de seguridad (SCC)

Etiquetas	Descripción	Predeterminado
<code>allowHostDirVolumePlugin</code>	Los contenedores de nodos Trident montan el sistema de archivos raíz del nodo.	<code>true</code>
<code>allowHostIPC</code>	El montaje de volúmenes NFS requiere que el IPC del host se comunique con <code>nfsd</code> .	<code>true</code>
<code>allowHostNetwork</code>	<code>lscsiadm</code> requiere que la red del host se comunique con el demonio iSCSI.	<code>true</code>
<code>allowHostPID</code>	Se requiere el PID del host para comprobar si <code>rpc-statd</code> está ejecutándose en el nodo.	<code>true</code>
<code>allowHostPorts</code>	Trident no utiliza puertos de host.	<code>false</code>
<code>allowPrivilegeEscalation</code>	Los contenedores con privilegios deben permitir la escala de privilegios.	<code>true</code>
<code>allowPrivilegedContainer</code>	Los pods de nodo Trident deben ejecutar un contenedor privilegiado para montar volúmenes.	<code>true</code>
<code>allowedUnsafeSysctls</code>	Trident no requiere que no sea seguro <code>sysctls</code> .	<code>none</code>
<code>allowedCapabilities</code>	Los contenedores Trident no con privilegios no requieren más funcionalidades de las que se establece de forma predeterminada y se conceden todas las funcionalidades posibles a los contenedores con privilegios.	Vacío
<code>defaultAddCapabilities</code>	No es necesario añadir capacidades a contenedores con privilegios.	Vacío
<code>fsGroup</code>	Los contenedores Trident se ejecutan como raíz.	<code>RunAsAny</code>
<code>groups</code>	Este SCC es específico de Trident y está vinculado a su usuario.	Vacío
<code>readOnlyRootFilesystem</code>	Los contenedores de nodos Trident deben escribir en el sistema de archivos del nodo.	<code>false</code>
<code>requiredDropCapabilities</code>	Los pods de nodo de Trident ejecutan un contenedor privilegiado y no pueden soltar las funcionalidades.	<code>none</code>



<b>Etiquetas</b>	<b>Descripción</b>	<b>Predeterminado</b>
runAsUser	Los contenedores Trident se ejecutan como raíz.	RunAsAny
seLinuxContext	Trident no está configurado <code>seLinuxOptions</code> Debido a que actualmente existen diferencias en el modo en que los tiempos de ejecución de contenedores y las distribuciones de Kubernetes se encargan de SELinux.	Vacío
seccompProfiles	Los contenedores privilegiados siempre funcionan "sin confinar".	Vacío
supplementalGroups	Los contenedores Trident se ejecutan como raíz.	RunAsAny
users	Se proporciona una entrada para vincular este SCC al usuario Trident en el espacio de nombres Trident.	n.a.
volumes	Los pods de Trident requieren estos complementos de volumen.	hostPath, downwardAPI, projected, emptyDir

# Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

## Derechos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Código abierto

Puede revisar los derechos de autor y las licencias de terceros utilizados en el software de NetApp para Trident en el archivo de avisos de cada versión en <https://github.com/NetApp/trident/>.

## 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 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.