Prepare el nodo de trabajo

Trident

NetApp
January 14, 2026

Tabla de contenidos

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 utiliza: `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 utiliza `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 FC" 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 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 de Linux compatible con RHEL, con `solidfire-san` el controlador y Element OS 12,5 o anterior, asegúrese de que el algoritmo de autenticación CHAP se haya configurado en MD5 en `/etc/iscsi/iscsid.conf`. Los algoritmos CHAP seguros compatibles con FIPS SHA1, SHA-256 y SHA3-256 están disponibles con Element 12,7.

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

- Cuando se utilicen los nodos de trabajo que ejecutan RHEL/RedHat CoreOS con VP iSCSI, especifique `discard` mountOption en StorageClass para realizar la recuperación 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 de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

4. Asegúrese de que `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 de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

5. Asegúrese de que `open-iscsi` y `multipath-tools` están activados 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 detectar los puertos de destino con `iscsiadm` antes de iniciar `open-iscsi` el daemon iSCSI. También puede modificar el `iscsi` servicio para que se inicie `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 los `iscsiSelfHealingInterval` parámetros y `iscsiSelfHealingWaitTime` durante la instalación del timón o la 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 los `iscsi-self-healing-interval` parámetros y `iscsi-self-healing-wait-time` 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.

Instale las herramientas FC

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

- Cuando se utilicen nodos de trabajador que ejecutan RHEL/RedHat CoreOS con VP FC, especifique `discard` mountOption en StorageClass para realizar la recuperación de espacio en línea. Consulte "Documentación de redhat".

RHEL 8 O POSTERIOR

1. Instale los siguientes paquetes del sistema:

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Activar accesos múltiples:

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

> Asegúrese de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

3. Asegúrese de que `multipathd` se está ejecutando:

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

Ubuntu

1. Instale los siguientes paquetes del sistema:

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

2. 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 de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

3. Asegúrese de que `multipath-tools` está activado y en ejecución:

```
sudo systemctl status multipath-tools
```

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 aprovisionado 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 se utilicen nodos de trabajador que ejecutan RHEL/RedHat CoreOS con VP FC, especifique `discard` mountOption en StorageClass para realizar la recuperación de espacio en línea. Consulte "Documentación de redhat".

RHEL 8 O POSTERIOR

1. Instale los siguientes paquetes del sistema:

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Activar accesos múltiples:

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

> Asegúrese de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

3. Asegúrese de que `multipathd` se está ejecutando:

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

Ubuntu

1. Instale los siguientes paquetes del sistema:

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

2. 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 de `etc/multipath.conf` que contiene `find_multipaths no` en `defaults`.

3. Asegúrese de que `multipath-tools` está activado y en ejecución:

```
sudo systemctl status multipath-tools
```

Cree una configuración de backend

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

Consulte:

- "Prepárese para configurar el back-end con los controladores SAN de ONTAP"
- "Opciones y ejemplos de configuración SAN de 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"
  storagePools: "ontap-san-backend:.*"
  fsType: "ext4"
allowVolumeExpansion: True
```

Información de copyright

Información de la marca comercial