Controladores NAS de ONTAP

Trident

NetApp
July 01, 2026

Tabla de contenidos

Controladores NAS de ONTAP

Descripción general del controlador NAS de ONTAP

Conoce cómo configurar un backend de ONTAP con los controladores NAS de ONTAP y Cloud Volumes ONTAP.

Detalles del controlador NAS de ONTAP

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

Controlador	Protocolo	volumeMode	Modos de acceso admitidos	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`
`ontap-nas-flexgroup`	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`

- Usa `ontap-san-economy` solo si esperas que el recuento de uso de volúmenes persistentes sea mayor que "límites de volúmenes compatibles de ONTAP".
- Usa `ontap-nas-economy` solo si se espera que el recuento de uso de volúmenes persistentes sea mayor que "límites de volúmenes compatibles de ONTAP" y no se puede usar el controlador `ontap-san-economy`.
- No uses `ontap-nas-economy` si crees que vas a necesitar protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda usar FlexVol autogrow en todos los controladores ONTAP, excepto ontap-san. Como solución alternativa, Trident admite el uso de snapshot reserve y escala los volúmenes FlexVol en consecuencia.

Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente usando el `admin`usuario del clúster o un `vsadmin`usuario de SVM, o un usuario con un nombre diferente que tenga el mismo rol.

Para las implementaciones de Amazon FSx for NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, usando el usuario del clúster `fsxadmin` o un `vsadmin`usuario de SVM, o un usuario con un nombre diferente que tenga el mismo rol. El `fsxadmin`usuario es un reemplazo limitado para el usuario administrador del clúster.

Si usas el parámetro `limitAggregateUsage`, se requieren permisos de administrador de clúster. Cuando usas Amazon FSx for NetApp ONTAP con Trident, el parámetro `limitAggregateUsage` no funcionará con las cuentas de usuario `vsadmin` y `fsxadmin`. La operación de configuración fallará si especificas este parámetro.

Aunque es posible crear un rol más restrictivo dentro de ONTAP que un controlador Trident pueda usar, no lo recomendamos. La mayoría de las nuevas versiones de Trident llamarán a APIs adicionales que habría que tener en cuenta, lo que hace que las actualizaciones sean difíciles y propensas a errores.

Prepárate para configurar un backend con controladores ONTAP NAS

Entiende los requisitos, las opciones de autenticación y las políticas de exportación para configurar un backend ONTAP con drivers ONTAP NAS. A partir de la versión 25.10, NetApp Trident es compatible con "Sistema de almacenamiento NetApp AFX". NetApp AFX storage systems difieren de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. En la configuración del backend de Trident, no necesitas especificar que tu sistema es AFX. Cuando seleccionas `ontap-nas` como `storageDriverName`, Trident detecta automáticamente los sistemas AFX.

Sólo el `ontap-nas` controlador (con protocolo NFS) es compatible con los sistemas AFX; el protocolo SMB no es compatible.

Requisitos

- Para todos los backends de ONTAP, Trident requiere que al menos un agregado esté asignado a la SVM.
- Puedes ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, podrías configurar una clase Gold que use el `ontap-nas` controlador y una clase Bronze que use el `ontap-nas-economy` otro.
- Todos tus nodos worker de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulta "aquí" para más detalles.
- Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows. Consulta Prepárate para aprovisionar volúmenes SMB para más detalles.

Autentica el backend de ONTAP

Trident ofrece dos modos de autenticación para un backend ONTAP.

- Basado en credenciales: este modo requiere permisos suficientes en el backend de ONTAP. Se recomienda usar una cuenta asociada a un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin` para garantizar la máxima compatibilidad con las versiones de ONTAP.
- Basado en certificado: este modo requiere un certificado instalado en el backend para que Trident se comunique con un clúster de ONTAP. Aquí, la definición del backend debe contener valores codificados en Base64 del certificado del cliente, la clave y el certificado de la CA de confianza si se usa (recomendado).

Puedes actualizar los backends existentes para pasar de métodos basados en credenciales a métodos basados en certificados y viceversa. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a otro método de autenticación, debes eliminar el método existente de la configuración del backend.

Si intentas proporcionar **tanto credenciales como certificados**, la creación del backend fallará con un error que indica que se proporcionó más de un método de autenticación en el archivo de configuración.

Habilita la autenticación basada en credenciales

Trident requiere las credenciales de un administrador con ámbito de SVM o de clúster para comunicarse con el backend de ONTAP. Se recomienda usar roles estándar predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad futura con versiones de ONTAP que podrían exponer APIs de funciones para futuras versiones de Trident. Se puede crear y usar un rol personalizado de inicio de sesión de seguridad con Trident, pero no se recomienda.

Un ejemplo de definición de backend se verá así:

YAML

```yaml
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
        "name": "secret-backend-creds"
    }
}
```

Ten en cuenta que la definición del backend es el único lugar donde se almacenan las credenciales en texto plano. Después de crear el backend, los nombres de usuario y contraseñas se codifican con Base64 y se guardan como secretos de Kubernetes. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. Así que es una operación solo para el administrador, que debe realizar el administrador de Kubernetes o de almacenamiento.

Habilita la autenticación basada en certificados

Los backends, tanto nuevos como existentes, pueden usar un certificado y comunicarse con el backend de ONTAP. Se requieren tres parámetros en la definición del 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 usas una CA de confianza, tienes que proporcionar este parámetro. Esto se puede ignorar si no usas una CA de confianza.

Un flujo de trabajo típico implica los siguientes pasos.

Pasos

1. Genera un certificado y una clave de cliente. Al generarlos, asigna el nombre común (CN) al usuario de ONTAP con el que te vas a autenticar.

```
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. Agrega un certificado de CA de confianza al clúster de ONTAP. Esto puede que ya lo haya gestionado el administrador de almacenamiento. Ignora esto si no se usa 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. Instala el certificado y la clave del cliente (del 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. Confirma que el rol de inicio de sesión de seguridad de ONTAP admite `cert` el 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. Prueba la autenticación usando el certificado generado. Reemplaza <ONTAP Management LIF> y <vserver name> con la IP de la LIF de administración y el nombre de la SVM. Debes asegurarte de que el LIF tenga su política de servicio configurada 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. Codifica el certificado, la clave y el certificado de CA confiable con Base64.

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

7. Crea un backend usando los valores obtenidos en el 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...Vaaalllluuuueeee",
"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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Actualiza los métodos de autenticación o rota las credenciales

Puedes actualizar un backend existente para usar un método de autenticación diferente o para rotar sus credenciales. Esto funciona en ambos sentidos: los backends que usan nombre de usuario y contraseña pueden actualizarse para usar certificados; los backends que utilizan certificados pueden actualizarse para usar nombre de usuario y contraseña. Para hacer esto, debes eliminar el método de autenticación existente y agregar el nuevo método de autenticación. Luego usa el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutar `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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

> Al rotar contraseñas, el administrador de almacenamiento debe primero actualizar la contraseña del usuario en ONTAP. Luego, se realiza una actualización del backend. Al rotar certificados, se pueden agregar varios certificados al usuario. Después, el backend se actualiza para usar el nuevo certificado, y luego se puede eliminar el certificado antiguo del clúster de ONTAP.

Actualizar un backend no interrumpe el acceso a los volúmenes ya creados ni afecta las conexiones de volumen realizadas después. Una actualización correcta del backend indica que Trident puede comunicarse con el backend de ONTAP y gestionar futuras operaciones de volumen.

Crear rol ONTAP personalizado para Trident

Puedes crear un rol de clúster de ONTAP con privilegios mínimos para que no tengas que usar el rol de admin de ONTAP para realizar operaciones en Trident. Cuando incluyes el nombre de usuario en una configuración de backend de Trident, Trident usa el rol de clúster de ONTAP que creaste para realizar las operaciones.

Consulta "Generador de roles personalizados de Trident" para más información sobre cómo crear roles personalizados de Trident.

Usando ONTAP CLI

1. Crea un nuevo rol usando el siguiente comando:

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

2. Crea un nombre de usuario para el usuario 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. Asigna el rol al usuario:

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

Usando System Manager

Realiza los siguientes pasos en ONTAP System Manager:

1. **Crea un rol personalizado**:
   a. Para crear un rol personalizado a nivel de cluster, selecciona **Cluster > Settings**.

      (O) Para crear un rol personalizado a nivel de SVM, selecciona **Storage > Storage VMs > `required SVM`> Settings > Users and Roles**.

   b. Selecciona el icono de flecha (→) junto a **Users and Roles**.
   c. Selecciona **+Add** en **Roles**.
   d. Define las reglas para el rol y haz clic en **Guardar**.
2. **Asigna el rol al usuario Trident**: + Realiza los siguientes pasos en la página **Usuarios y roles**:
   a. Selecciona el icono Add **+** en **Usuarios**.
   b. Selecciona el nombre de usuario requerido y elige un rol en el menú desplegable de **Role**.
   c. Haz clic en **Guardar**.

Consulta las siguientes páginas para obtener más información:

- "Roles personalizados para la administración de ONTAP" o "Define roles personalizados"
- "Trabaja con roles y usuarios"

Gestiona las políticas de exportación de NFS

Trident utiliza políticas de exportación NFS para controlar el acceso a los volúmenes que aprovisiona.

Trident ofrece dos opciones cuando trabajas con políticas de exportación:

- Trident puede gestionar dinámicamente la política de exportación por sí mismo; en este modo de funcionamiento, el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Trident añade automáticamente a la política de exportación las direcciones IP de nodo aplicables que estén dentro de estos rangos en el momento de la publicación. Como alternativa, cuando no se especifican CIDR, se añadirán a la política de exportación todas las direcciones IP de unidifusión de ámbito global que se encuentren en el nodo al que se está publicando el volumen.
- Los administradores de almacenamiento pueden crear una política de exportación y agregar reglas manualmente. Trident utiliza la política de exportación predeterminada a menos que se especifique un nombre de política de exportación diferente en la configuración.

Gestiona dinámicamente las políticas de exportación

Trident ofrece la capacidad de gestionar dinámicamente las políticas de exportación para los backends de ONTAP. Esto le da al administrador de almacenamiento la posibilidad de especificar un espacio de direcciones permitido para las direcciones IP de los nodos de trabajo, en vez de definir reglas explícitas manualmente. Esto simplifica mucho la gestión de las políticas de exportación; las modificaciones en 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 trabajo que están montando volúmenes y tienen direcciones IP dentro del rango especificado, lo que permite una gestión automatizada y detallada.

> No uses Network Address Translation (NAT) cuando uses políticas de exportación dinámicas. Con NAT, el controlador de almacenamiento ve la dirección NAT del frontend y no la dirección IP real del host, así que se denegará el acceso cuando no se encuentre coincidencia en las reglas de exportación.

Ejemplo

Hay dos opciones de configuración que deben utilizarse. Aquí tienes 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, debes asegurarte de que la unión raíz de tu SVM tenga una política de exportación previamente creada con una regla de exportación que permita el bloque CIDR del nodo (como la política de exportación predeterminada). Sigue siempre la práctica recomendada por NetApp de dedicar una SVM para Trident.

Aquí tienes una explicación de cómo funciona esta función usando el ejemplo de arriba:

- `autoExportPolicy` se establece en `true`. Esto indica que Trident crea una política de exportación para cada volumen aprovisionado con este backend para la `svm1` SVM y gestiona la adición y eliminación de reglas usando bloques de direcciones `autoexportCIDRs`. Hasta que un volumen se conecta a un nodo, el volumen utiliza una política de exportación vacía sin reglas para evitar el acceso no deseado a ese volumen. Cuando un volumen se publica en un nodo, Trident crea una política de exportación con el mismo nombre que el qtree subyacente que contiene la dirección IP del nodo dentro del bloque CIDR especificado. Estas direcciones IP también se añadirán a la política de exportación utilizada por el volumen principal FlexVol.
  - Por ejemplo:
    - UUID de backend 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy` establecer en `true`
    - prefijo de almacenamiento `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - El qtree llamado trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c crea una política de exportación para el FlexVol llamado `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 llamada `trident_empty` en la SVM. Las reglas para la política de exportación del FlexVol serán un superconjunto de cualquier regla contenida en las políticas de exportación del qtree. La política de exportación vacía se reutilizará para cualquier volumen que no esté adjunto.
- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y su valor predeterminado es ["0.0.0.0/0", "::/0"]. Si no se define, Trident agrega todas las direcciones unicast de alcance global que se encuentran en los nodos de trabajo con publicaciones.

En este ejemplo, el espacio de direcciones `192.168.0.0/24` se proporciona. Esto indica que las direcciones IP de los nodos de Kubernetes que estén dentro de este rango de direcciones con publicaciones se añadirán 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 compara con los bloques de direcciones proporcionados en `autoExportCIDRs`. Al momento de publicar, después de filtrar las IP, Trident crea las reglas de la política de exportación para las direcciones IP de cliente del nodo al que está publicando.

Puedes actualizar `autoExportPolicy` y `autoExportCIDRs` para los backends después de crearlos. Puedes añadir nuevos CIDR para un backend que se gestiona automáticamente o eliminar los CIDR existentes. Ten cuidado al eliminar los CIDR para asegurarte de que no se interrumpan las conexiones existentes. También puedes elegir deshabilitar `autoExportPolicy` para un backend y volver a una política de exportación creada manualmente. Esto requerirá configurar el parámetro `exportPolicy` en la configuración del backend.

Después de que Trident crea o actualiza un backend, puedes verificar el backend usando `tridentctl` o el correspondiente `tridentbackend` CRD:

```
./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>
      fileSystemType: ext4
```

Al eliminar un nodo, Trident revisa todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar esta dirección IP de nodo de las políticas de exportación de los backends administrados, Trident evita montajes no autorizados, a menos que esta IP sea reutilizada por un nuevo nodo en el clúster.

Para los backends preexistentes, actualizar el backend con `tridentctl update backend` asegura que Trident gestione las políticas de exportación automáticamente. Esto crea dos nuevas políticas de exportación nombradas según el UUID y el nombre del qtree del backend cuando sean necesarias. Los volúmenes que están presentes en el backend usarán las nuevas políticas de exportación después de desmontarlos y volver a montarlos.

Al eliminar un backend con políticas de exportación autogestionadas, se eliminará la política de exportación creada dinámicamente. Si el backend se vuelve a crear, se trata como un backend nuevo y resultará en la creación de una nueva política de exportación.

Si se actualiza la dirección IP de un nodo activo, debes reiniciar el pod de Trident en el nodo. Trident actualizará la política de exportación para los backends que administra para reflejar este cambio de IP.

Prepárate para aprovisionar volúmenes SMB

Con un poco de preparación adicional, puedes aprovisionar volúmenes SMB usando `ontap-nas`drivers.

Debes configurar tanto los protocolos NFS como SMB/CIFS en la SVM para crear un `ontap-nas-economy` volumen SMB para clústeres ONTAP locales. Si no configuras alguno de estos protocolos, la creación del volumen SMB fallará.

`autoExportPolicy` no es compatible con volúmenes SMB.

Antes de empezar

Antes de que puedas aprovisionar volúmenes SMB, debes tener lo siguiente.

- Un clúster de Kubernetes con un nodo controlador Linux y al menos un nodo trabajador Windows que ejecuta Windows Server 2022. Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows.
- Al menos un secreto de Trident con tus credenciales de Active Directory. Para generar un secreto `smbcreds`:

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

- Un proxy CSI configurado como un servicio de Windows. Para configurar un `csi-proxy`, consulta "GitHub: CSI Proxy" o "GitHub: CSI Proxy para Windows" para nodos de Kubernetes que se ejecutan en Windows.

Pasos

1. Para ONTAP local, puedes crear opcionalmente un recurso compartido SMB o Trident puede crear uno para ti.

   Se requieren recursos compartidos SMB para Amazon FSx for ONTAP.

   Puedes crear los recursos compartidos de administrador de SMB de dos maneras: usando el complemento "Microsoft Management Console" Shared Folders o usando la CLI de ONTAP. Para crear los recursos compartidos de SMB usando la CLI de ONTAP:

   a. Si es necesario, crea la estructura de ruta del directorio para el recurso compartido.

      El `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. Crea un recurso compartido 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. Verifica que se creó el recurso compartido:

```
vserver cifs share show -share-name share_name
```

      Consulta "Crear un recurso compartido SMB" para obtener detalles completos.

2. Al crear el backend, debes configurar lo siguiente para especificar los volúmenes SMB. Para todas las

opciones de configuración del backend de FSx for ONTAP, consulta "Opciones de configuración de FSx for ONTAP y ejemplos".

Parámetro	Descripción	Ejemplo
`smbShare`	Puedes especificar uno de los siguientes: el nombre de un recurso compartido SMB creado usando Microsoft Management Console o la CLI de ONTAP, un nombre para permitir que Trident cree el recurso compartido SMB, o puedes dejar el parámetro en blanco para evitar el acceso compartido común a los volúmenes. Este parámetro es opcional para ONTAP local. Este parámetro es obligatorio para los backends de Amazon FSx for ONTAP y no puede estar en blanco.	`smb-share`
`nasType`	**Debe establecerse en `smb`.** Si es nulo, el valor predeterminado es `nfs`.	`smb`
`securityStyle`	Estilo de seguridad para nuevos volúmenes. **Debe configurarse en `ntfs` o `mixed` para volúmenes SMB.**	`ntfs` o `mixed` para volúmenes SMB
`unixPermissions`	Modo para nuevos volúmenes. **Debe dejarse vacío para volúmenes SMB.**	""

Habilita SMB seguro

A partir de la versión 25.06, NetApp Trident admite el aprovisionamiento seguro de volúmenes SMB creados mediante `ontap-nas` y `ontap-nas-economy` backends. Cuando SMB seguro está habilitado, puedes proporcionar acceso controlado a los recursos compartidos SMB para usuarios y grupos de usuarios de Active Directory (AD) usando listas de control de acceso (ACL).

Puntos para recordar

- No se admite la importación `ontap-nas-economy` de volúmenes.
- Solo se admiten clones de solo lectura para `ontap-nas-economy` volúmenes.
- Si Secure SMB está habilitado, Trident ignorará el recurso compartido SMB mencionado en el backend.
- Actualizar la anotación de PVC, la anotación de la storage class y el campo backend no actualiza la ACL del recurso compartido SMB.
- La ACL de recurso compartido SMB especificada en la anotación del PVC clonado tendrá prioridad sobre las del PVC de origen.
- Asegúrate de proporcionar usuarios de AD válidos al habilitar SMB seguro. Los usuarios no válidos no se añadirán a la ACL.
- Si proporcionas el mismo usuario de AD en el backend, la clase de almacenamiento y el PVC con diferentes permisos, la prioridad de permisos será: PVC, clase de almacenamiento y luego backend.
- SMB seguro es compatible para `ontap-nas`importaciones de volúmenes administrados y no aplica a importaciones de volúmenes no administrados.

Pasos

1. Especifica adAdminUser en TridentBackendConfig como se muestra en el siguiente ejemplo:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. Añade la anotación en la clase de almacenamiento.

   Agrega la `trident.netapp.io/smbShareAdUser` anotación a la clase de almacenamiento para habilitar SMB seguro sin fallar. El valor de usuario especificado para la anotación `trident.netapp.io/smbShareAdUser` debe ser el mismo que el nombre de usuario especificado en el `smbcreds` secreto. Puedes elegir una de las siguientes para `smbShareAdUserPermission`: `full_control`, `change` o `read`. El permiso predeterminado es `full_control`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. Crea un PVC.

   El siguiente ejemplo crea una PVC:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Opciones de configuración y ejemplos de ONTAP NAS

Aprende a crear y usar controladores NAS de ONTAP con tu instalación de Trident. Esta sección ofrece ejemplos de configuración de backends y detalles para asignar backends a StorageClasses. A partir de la versión 25.10, NetApp Trident es compatible con "NetApp sistemas de almacenamiento AFX". Los sistemas de almacenamiento NetApp AFX se diferencian de otros sistemas basados en ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento.

> Sólo el `ontap-nas` controlador (con protocolo NFS) es compatible con NetApp AFX systems; el protocolo SMB no es compatible.

Opciones de configuración del backend

En la configuración del backend de Trident, no necesitas especificar que tu sistema es un sistema de almacenamiento AFX de NetApp. Cuando seleccionas `ontap-nas` como `storageDriverName`, Trident detecta automáticamente el sistema de almacenamiento AFX. Algunos parámetros de configuración del backend no aplican a los sistemas de almacenamiento AFX.

La siguiente tabla muestra las opciones de configuración del backend:

Parámetro	Descripción	Predeterminado
`version`		Siempre 1

Parámetro	Descripción	Predeterminado
`storageDriverName`	Nombre del controlador de almacenamiento Para los sistemas AFX de NetApp, solo `ontap-nas` es compatible.	`ontap-nas`, `ontap-nas-economy`, o `ontap-nas-flexgroup`
`backendName`	Nombre personalizado o el backend de almacenamiento	Nombre del driver + "_" + dataLIF
`managementLIF`	Dirección IP de un clúster o de una LIF de administración de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Para una conmutación de sitios sin interrupciones de MetroCluster, consulta el Ejemplo de MetroCluster.	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	Dirección IP del LIF de protocolo. NetApp recomienda especificar `dataLIF`. Si no se proporciona, Trident obtiene los dataLIF del SVM. Puedes especificar un nombre de dominio completo (FQDN) para las operaciones de montaje NFS, lo que te permite crear un DNS de round-robin para balancear la carga entre varios dataLIF. Se puede cambiar después de la configuración inicial. Consulta . Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. **Omite para MetroCluster.** Consulta la Ejemplo de MetroCluster.	Dirección especificada o derivada de SVM, si no se especifica (no recomendado)
`svm`	Máquina virtual de almacenamiento a usar **Omitir para MetroCluster.** Consulta la Ejemplo de MetroCluster.	Se deriva si se especifica un SVM `managementLIF`
`autoExportPolicy`	Habilita la creación y actualización automática de políticas de exportación [Boolean]. Usando las opciones `autoExportPolicy` y `autoExportCIDRs`, Trident puede gestionar las políticas de exportación automáticamente.	false
`autoExportCIDRs`	Lista de CIDR para filtrar las direcciones IP de los nodos de Kubernetes cuando `autoExportPolicy` está habilitado. Usando las opciones `autoExportPolicy` y `autoExportCIDRs`, Trident puede gestionar las políticas de exportación automáticamente.	["0.0.0.0/0", "::/0"]`
`labels`	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes	""

Parámetro	Descripción	Predeterminado
`clientCertificate`	Valor codificado en Base64 del certificado del cliente. Usado para auth basada en certificados	""
`clientPrivateKey`	Valor codificado en Base64 de la clave privada del cliente. Usado para auth basada en certificados	""
`trustedCACertificate`	Valor codificado en Base64 del certificado de CA de confianza. Opcional. Usado para auth basada en certificados	""
`username`	Nombre de usuario para conectarse al clúster/SVM. Se usa para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulta "Autentica Trident en un SVM backend usando credenciales de Active Directory".	
`password`	Contraseña para conectarte al clúster/SVM. Se usa para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulta "Autentica Trident en un SVM backend usando credenciales de Active Directory".	
`storagePrefix`	Prefijo utilizado al aprovisionar nuevos volúmenes en la SVM. No se puede actualizar después de configurarlo Al usar ontap-nas-economy y un storagePrefix que tiene 24 caracteres o más, los qtrees no tendrán el prefijo de almacenamiento incorporado, aunque estará en el nombre del volumen.	"Trident"

Parámetro	Descripción	Predeterminado
`aggregate`	Agregado para aprovisionamiento (opcional; si se configura, debe asignarse a la SVM). Para el `ontap-nas-flexgroup` driver, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles se puede usar para aprovisionar un FlexGroup volumen. Cuando el agregado se actualiza en SVM, se actualiza automáticamente en Trident mediante el sondeo de SVM sin tener que reiniciar el Trident Controller. Cuando has configurado un agregado específico en Trident para aprovisionar volúmenes, si el agregado se renombra o se mueve fuera de la SVM, el backend pasará a estado fallido en Trident mientras sondea el agregado de la SVM. Debes cambiar el agregado por uno que esté presente en la SVM o eliminarlo por completo para que el backend vuelva a estar en línea. **No especifiques para sistemas de almacenamiento AFX.**	""
`limitAggregateUsage`	Falla el aprovisionamiento si el uso es superior a este porcentaje. **No aplica a Amazon FSx for ONTAP**. **No especifiques para sistemas de almacenamiento AFX.**	"" (no aplicado por defecto)

Parámetro	Descripción	Predeterminado
flexgroupAggregateList	Lista de agregados para aprovisionamiento (opcional; si se configura, debe asignarse a la SVM). Todos los agregados asignados a la SVM se utilizan para aprovisionar un volumen FlexGroup. Compatible con el controlador de almacenamiento **ontap-nas-flexgroup**. Cuando la lista de agregados se actualiza en SVM, la lista se actualiza en Trident automáticamente mediante el sondeo de SVM sin tener que reiniciar el controlador Trident. Cuando has configurado una lista de agregados específica en Trident para aprovisionar volúmenes, si la lista de agregados se renombra o se mueve fuera de SVM, el backend pasará a estado de error en Trident mientras sondea el agregado de SVM. Debes cambiar la lista de agregados por una que esté presente en SVM o eliminarla por completo para que el backend vuelva a estar en línea.	""
`limitVolumeSize`	Falla el aprovisionamiento si el tamaño del volumen solicitado supera este valor.	"" (no aplicado por defecto)
`debugTraceFlags`	Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, {"api":false, "method":true} no uses `debugTraceFlags` a menos que estés resolviendo problemas y necesites un volcado de registro detallado.	null
`nasType`	Configura la creación de volúmenes NFS o SMB. Las opciones son `nfs`, `smb` o null. Si lo configuras en null, se usarán volúmenes NFS por defecto. **Si se especifica, siempre se establece en `nfs` para sistemas de almacenamiento AFX**.	`nfs`
`nfsMountOptions`	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para volúmenes persistentes de Kubernetes normalmente se especifican en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident usará las opciones de montaje especificadas en el archivo de configuración del backend de almacenamiento. Si no se especifican opciones de montaje en la clase de almacenamiento ni en el archivo de configuración, Trident no establecerá ninguna opción de montaje en un volumen persistente asociado.	""

Parámetro	Descripción	Predeterminado
`qtreesPerFlexvol`	Máximo de Qtrees por FlexVol, debe estar en el rango [50, 300]	"200"
`smbShare`	Puedes especificar uno de los siguientes: el nombre de un recurso compartido SMB creado usando Microsoft Management Console o la CLI de ONTAP, un nombre para permitir que Trident cree el recurso compartido SMB, o puedes dejar el parámetro en blanco para evitar el acceso compartido común a los volúmenes. Este parámetro es opcional para ONTAP local. Este parámetro es obligatorio para los backends de Amazon FSx for ONTAP y no puede estar en blanco.	`smb-share`
`useREST`	Parámetro booleano para usar las ONTAP REST APIs. `useREST`Cuando se establece en `true`, Trident usa las ONTAP REST APIs para comunicarse con el backend; cuando se establece en `false`, Trident usa llamadas ONTAPI (ZAPI) para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 y versiones posteriores. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a la aplicación `ontapi`. Esto se cumple con los roles predefinidos `vsadmin` y `cluster-admin`. A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posteriores, `useREST`está configurado en `true`de forma predeterminada; cambia `useREST` a `false` para usar llamadas ONTAPI (ZAPI). **Si se especifica, siempre se establece en `true` para sistemas de almacenamiento AFX**.	`true` para ONTAP 9.15.1 o posterior, de lo contrario `false`.
`limitVolumePoolSize`	Tamaño máximo solicitable de FlexVol al utilizar Qtrees en el backend ontap-nas-economy.	"" (no aplicado por defecto)
`denyNewVolumePools`	Restringe `ontap-nas-economy` a los backends crear nuevos volúmenes FlexVol para contener sus Qtrees. Solo se usan FlexVols preexistentes para aprovisionar nuevos PV.	
`adAdminUser`	Usuario o grupo de usuarios administradores de Active Directory con acceso total a los recursos compartidos SMB. Usa este parámetro para otorgar derechos de administrador al recurso compartido SMB con control total.	

Opciones de configuración de backend para aprovisionar volúmenes

Puedes controlar el aprovisionamiento predeterminado usando estas opciones en la `defaults` sección de la configuración. Por ejemplo, mira los ejemplos de configuración abajo.

Parámetro	Descripción	Predeterminado
`spaceAllocation`	Asignación de espacio para Qtrees	"true"
`spaceReserve`	Modo de reserva de espacio; "ninguno" (fino) o "volumen" (grueso)	"none"
`snapshotPolicy`	Política de SnapVault a utilizar	"none"
`qosPolicy`	Grupo de políticas de QoS para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por cada pool de almacenamiento/backend	""
`adaptiveQosPolicy`	Grupo de políticas de QoS adaptativo para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento/backend. No compatible con ontap-nas-economy.	""
`snapshotReserve`	Porcentaje de volumen reservado para instantáneas	"0" si `snapshotPolicy` es "none", de lo contrario ""
`splitOnClone`	Divide un clon de su padre al momento de su creación	"false"
`encryption`	Habilita NetApp Volume Encryption (NVE) en el nuevo volumen; el valor predeterminado es `false`. NVE debe tener licencia y estar habilitado en el clúster para usar esta opción. Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NAE habilitado. Para más información, consulta: "Cómo funciona Trident con NVE y NAE".	"false"
`tieringPolicy`	Política de organización en niveles para usar "none"	
`unixPermissions`	Modo para nuevos volúmenes	"777" para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
`snapshotDir`	Controla el acceso al `.snapshot` directorio	`true`, `false` (establecer explícitamente).
`exportPolicy`	Política de exportación a usar	"default"
`securityStyle`	Estilo de seguridad para nuevos volúmenes. NFS admite `mixed` y `unix` estilos de seguridad. SMB admite `mixed` y `ntfs` estilos de seguridad.	NFS predeterminado es `unix`. SMB predeterminado es `ntfs`.
`nameTemplate`	Plantilla para crear nombres de volúmenes personalizados.	""

Usar grupos de políticas de QoS con Trident requiere ONTAP 9.8 o una versión posterior. Deberías usar un grupo de políticas de QoS no compartido y asegurarte de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de QoS compartido impone el límite máximo para el rendimiento total de todas las cargas de trabajo.

Ejemplos de aprovisionamiento de volumen

Aquí tienes un ejemplo con 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"
```

Para `ontap-nas` y `ontap-nas-flexgroups`, Trident ahora usa un nuevo cálculo para asegurarse de que el FlexVol tenga el tamaño correcto con el porcentaje de snapshotReserve y el PVC. Cuando el usuario solicita un PVC, Trident crea el FlexVol original con más espacio usando el nuevo cálculo. Este cálculo asegura que el usuario reciba el espacio escribible que pidió en el PVC, y no menos espacio del que solicitó. Antes de la v21.07, cuando el usuario solicitaba un PVC (por ejemplo, 5 GiB), con el snapshotReserve al 50 por ciento, solo obtenía 2.5 GiB de espacio escribible. Esto es porque lo que el usuario pedía era todo el volumen y `snapshotReserve` es un porcentaje de eso. Con Trident 21.07, lo que el usuario pide es el espacio escribible y Trident define el número de `snapshotReserve` como el porcentaje del volumen completo. Esto no aplica a `ontap-nas-economy`. Mira el siguiente ejemplo para ver cómo funciona esto:

El cálculo es el siguiente:

```
Total volume size = <PVC requested size> / (1 - (<snapshotReserve
percentage> / 100))
```

Para snapshotReserve = 50%, y una solicitud de PVC de 5 GiB, el tamaño total del volumen es 5/0.5 = 10 GiB y el tamaño disponible es 5 GiB, que es lo que el usuario pidió en la solicitud de PVC. El `volume show` comando debería mostrar resultados similares a este ejemplo:

Los backends existentes de instalaciones anteriores aprovisionarán volúmenes como se explicó arriba cuando actualices Trident. Para los volúmenes que creaste antes de actualizar, deberías redimensionar sus volúmenes para que se note el cambio. Por ejemplo, un PVC de 2 GiB con `snapshotReserve=50` antes generaba un volumen que proporcionaba 1 GiB de espacio escribible. Redimensionar el volumen a 3 GiB, por ejemplo, le da a la aplicación 3 GiB de espacio escribible en un volumen de 6 GiB.

Ejemplos de configuración mínima

Los siguientes ejemplos muestran configuraciones básicas que dejan la mayoría de los parámetros en sus valores predeterminados. Esta es la forma más fácil de definir un backend.

> Si estás usando Amazon FSx en NetApp ONTAP con Trident, la recomendación es especificar nombres DNS para los LIF en vez de direcciones IP.

Ejemplo de ONTAP NAS economy

```
---
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 ONTAP NAS FlexGroup

```
---
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

Puedes configurar el backend para evitar tener que actualizar manualmente la definición del backend después de la conmutación de sitios y la conmutación de vuelta durante "Replicación y recuperación de SVM".

Para una conmutación de sitios sin interrupciones, especifica la SVM usando `managementLIF` y omite los parámetros `dataLIF` y `svm`. Por ejemplo:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

Ejemplo de volúmenes 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 mínima de backend. `clientCertificate`, `clientPrivateKey` y `trustedCACertificate` (opcional, si usas una CA de confianza) se rellenan en `backend.json` y toman los valores codificados en 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

Este ejemplo muestra cómo puedes indicarle a Trident que use políticas de exportación dinámicas para crear y gestionar la política de exportación automáticamente. Esto funciona igual para los controladores `ontap-nas-economy` 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` usando 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 for ONTAP usando volúmenes SMB

El `smbShare` parámetro es necesario para FSx for ONTAP usando volúmenes SMB.

```
---
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}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

Ejemplos de backends 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 grupos virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo "Comentarios". Los comentarios se establecen en FlexVol para `ontap-nas` o en FlexGroup para `ontap-nas-flexgroup`. Trident copia todas las etiquetas presentes en un pool virtual al volumen de almacenamiento al aprovisionar. 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` valores, y algunos pools anulan los valores predeterminados.

Ejemplo de ONTAP NAS

```
---
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 ONTAP NAS FlexGroup

```
---
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 ONTAP NAS economy

```
---
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"
```

Asigna backends a StorageClasses

Las siguientes definiciones de StorageClass hacen referencia a Ejemplos de backends con pools virtuales. Usando el campo `parameters.selector`, cada StorageClass indica qué grupos virtuales pueden usarse para alojar un volumen. El volumen tendrá los aspectos definidos en el grupo virtual elegido.

- El `protection-gold` StorageClass se asignará al primer y segundo pool virtual en el `ontap-nas-flexgroup` backend. Estos son los únicos pools que ofrecen protección de nivel oro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- El `protection-not-gold` StorageClass se asignará al tercer y cuarto pool virtual en el `ontap-nas-flexgroup` backend. 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"
```

- El `app-mysqldb` StorageClass se mapeará al cuarto pool virtual en el `ontap-nas` backend. Este es el único pool que ofrece configuración de pool de almacenamiento para app tipo mysqldb.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- El `protection-silver-creditpoints-20k` StorageClass se asignará al tercer pool virtual en el `ontap-nas-flexgroup` backend. 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"
```

- El `creditpoints-5k` StorageClass se asignará al tercer pool virtual en el `ontap-nas` backend y al segundo pool virtual en el `ontap-nas-economy` backend. Estas son las únicas ofertas de grupos 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 grupo virtual se selecciona y se asegurará de que se cumpla el requisito de almacenamiento.

Actualiza `dataLIF` después de la configuración inicial

Puedes cambiar el dataLIF después de la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON del backend con el dataLIF actualizado.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-
with-updated-dataLIF>
```

Si los PVC están conectados a uno o varios pods, tienes que desactivar todos los pods correspondientes y luego volverlos a activar para que el nuevo dataLIF surta efecto.

Ejemplos seguros de SMB

Configuración del backend con el controlador ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuración del backend con el controlador ontap-nas-economy

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuración de backend con storage pool

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
  - labels:
      app: msoffice
    defaults:
      adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Ejemplo de clase de almacenamiento con el controlador ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Asegúrate de agregar `annotations` para habilitar SMB seguro. SMB seguro no funciona sin las anotaciones, independientemente de las configuraciones establecidas en el Backend o PVC.

Ejemplo de clase de almacenamiento con el controlador ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Ejemplo de PVC con un único usuario AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Ejemplo de PVC con varios usuarios AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```