# Controladores NAS ONTAP

## Trident

NetApp
January 15, 2026

# Tabla de contenidos

# Controladores NAS ONTAP

## Descripción general del controlador NAS de ONTAP

Aprenda a configurar un backend de ONTAP con ONTAP y los controladores NAS de 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 compatibles son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

| Conductor | Protocolo | modo de volumen | 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` |
| `ontap-nas-flexgroup` | NFS SMB | Sistema de archivos | RWO, ROX, RWX, RWOP | "", `nfs` , `smb` |

- Usar `ontap-san-economy` solo si se espera que el recuento de uso de volumen persistente sea superior a"límites de volumen ONTAP compatibles" .
- Usar `ontap-nas-economy` solo si se espera que el recuento de uso de volumen persistente sea superior a"límites de volumen ONTAP compatibles" y el `ontap-san-economy` El controlador no se puede utilizar.
- No usar `ontap-nas-economy` Si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda usar el crecimiento automático de Flexvol en todos los controladores ONTAP , excepto en ontap-san. Como solución alternativa, Trident admite el uso de reserva de instantáneas y escala los volúmenes Flexvol en consecuencia.

### Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el `admin` usuario del clúster o un `vsadmin` Usuario de SVM, o un usuario con un nombre diferente que tenga la misma función.

Para implementaciones de Amazon FSx for NetApp ONTAP , Trident requiere ejecutarse como administrador de ONTAP o SVM, utilizando el clúster. `fsxadmin` usuario o un `vsadmin` Usuario de SVM, o un usuario con un nombre diferente que tenga la misma función. El `fsxadmin` El usuario es un reemplazo limitado para el usuario administrador del clúster.

Si utiliza el `limitAggregateUsage` Se requieren permisos de administrador de clúster para este parámetro. Al utilizar Amazon FSx for NetApp ONTAP con Trident, `limitAggregateUsage` El parámetro no funcionará con el `vsadmin` y `fsxadmin` cuentas de usuario. La operación de configuración fallará si especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que pueda usar un controlador Trident , no lo recomendamos. La mayoría de las nuevas versiones de Trident utilizarán API adicionales que habría que tener en cuenta, lo que dificultaría las actualizaciones y las haría propensas a errores.

# Prepárese para configurar un backend con controladores NAS ONTAP .

Comprenda los requisitos, las opciones de autenticación y las políticas de exportación para configurar un backend ONTAP con controladores ONTAP NAS.

## Requisitos

- Para todos los backends de ONTAP , Trident requiere que se asigne al menos un agregado al 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 utilice la `ontap-nas` conductor y una clase Bronce que utiliza el `ontap-nas-economy` uno.
- Todos tus nodos de trabajo de Kubernetes deben tener instaladas las herramientas NFS apropiadas. Referirse a"aquí" Para más detalles.
- Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows. Referirse a Preparar el aprovisionamiento de volúmenes SMB Para más detalles.

## Autenticar 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 a un rol de inicio de sesión de seguridad predefinido, como por ejemplo: `admin` o `vsadmin` para garantizar la máxima compatibilidad con las versiones de ONTAP .
- Basado en certificados: Este modo requiere un certificado instalado en el backend para que Trident se comunique con un clúster ONTAP . Aquí, la definición del backend debe contener valores codificados en Base64 del certificado del cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puedes actualizar los sistemas backend existentes para alternar entre métodos basados en credenciales y métodos 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 backend.

Si intenta 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.

### Habilitar la autenticación basada en credenciales

Trident requiere las credenciales de un administrador con ámbito SVM/ámbito de clúster para comunicarse

con el backend de ONTAP . Se recomienda utilizar roles estándar predefinidos, tales como: `admin` o `vsadmin` . Esto garantiza la compatibilidad con versiones futuras de ONTAP que podrían exponer API de funciones para ser utilizadas por futuras versiones de Trident . Se puede crear y usar un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Un ejemplo de definición de backend se vería 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"
    }
}
```

Tenga en cuenta que la definición del backend es el único lugar donde las credenciales se almacenan en texto plano. Una vez creado el backend, los nombres de usuario y las contraseñas se codifican con Base64 y se almacenan como secretos de Kubernetes. La creación/actualización de un backend es el único paso que requiere conocer las credenciales. Por lo tanto, se trata de una operación exclusiva para administradores, que debe ser realizada por el administrador de Kubernetes/almacenamiento.

### Habilitar la autenticación basada en certificados

Los backends nuevos y 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 del 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, este parámetro debe proporcionarse. Esto puede ignorarse si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico comprende los siguientes pasos.

**Pasos**

1. Generar un certificado y una clave de cliente. Al generar, configure el Nombre Común (CN) con el usuario ONTAP con el que se autenticará.

```
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. Agregar certificado de CA de confianza al clúster ONTAP . Es posible que esto ya lo gestione el administrador de almacenamiento. Ignorar 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 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. Confirme que el rol de inicio de sesión de seguridad de ONTAP es compatible. `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. Prueba de autenticación utilizando el certificado generado. Reemplace < ONTAP Management LIF> y <vserver name> con la IP de Management LIF y el nombre de SVM. Debe asegurarse de que la LIF tenga configurada su política de servicio para `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 el certificado, la clave y el certificado 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. Crea el backend utilizando 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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

### Actualizar los métodos de autenticación o rotar 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 sistemas de gestión de backends que utilizan nombre de usuario/contraseña pueden actualizarse para usar certificados; los sistemas de gestión de backends que utilizan certificados pueden actualizarse para basarse en 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 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 las contraseñas, el administrador de almacenamiento primero debe actualizar la contraseña del usuario en ONTAP. A continuación se realiza una actualización del servidor. Al rotar los certificados, se pueden agregar varios certificados al usuario. Posteriormente, se actualiza el sistema backend para utilizar el nuevo certificado, tras lo cual se puede eliminar el certificado antiguo del clúster ONTAP .

La actualización de un backend no interrumpe el acceso a los volúmenes que ya se han creado, ni afecta a las

conexiones de volumen realizadas posteriormente. Una actualización exitosa del backend indica que Trident puede comunicarse con el backend de ONTAP y gestionar futuras operaciones de volumen.

**Cree un rol ONTAP personalizado para Trident.**

Puede crear un rol de clúster ONTAP con privilegios mínimos para que no tenga que usar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluyes el nombre de usuario en una configuración de backend de Trident , Trident utiliza el rol de clúster ONTAP que creaste para realizar las operaciones.

Referirse a"Generador de roles personalizados de Trident" Para obtener más información sobre la creación de roles personalizados de Trident .

**Uso de la CLI de ONTAP**

1. Crea un nuevo rol utilizando 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 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. Asigna el rol al usuario:

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

**Usando el Administrador del sistema**

Realice los siguientes pasos en ONTAP System Manager:

1. **Crea un rol personalizado**:
   a. Para crear un rol personalizado a nivel de clúster, seleccione **Clúster > Configuración**.

      (O) Para crear un rol personalizado a nivel de SVM, seleccione **Almacenamiento > Máquinas virtuales de almacenamiento > `required SVM` > Configuración > Usuarios y roles**.

   b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.
   c. Seleccione ****Agregar** en **Roles**.
   d. Define las reglas para el rol y haz clic en **Guardar**.
2. **Asigna el rol al usuario de Trident *: + Realiza los siguientes pasos en la página *Usuarios y roles**:
   a. Seleccione el icono Agregar ***+** debajo de **Usuarios**.
   b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.
   c. Haga clic en **Guardar**.

Para obtener más información, consulte las siguientes páginas:

- "Roles personalizados para la administración de ONTAP"o"Definir roles personalizados"
- "Trabajar con roles y usuarios"

## Gestionar las políticas de exportación NFS

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

Trident ofrece dos opciones al trabajar con políticas de exportación:

- Trident puede gestionar dinámicamente la propia 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 automáticamente a la política de exportación, en el momento de la publicación, las direcciones IP de los nodos aplicables que se encuentren dentro de estos rangos. Alternativamente, cuando no se especifican CIDR, todas las IP de unidifusión de ámbito global que se encuentren en el nodo al que se publica el volumen se agregarán a la política de exportación.
- 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.

### Gestionar dinámicamente las políticas de exportación

Trident ofrece la capacidad de gestionar dinámicamente las políticas de exportación para los sistemas backend de ONTAP . Esto proporciona al administrador de almacenamiento la capacidad de especificar un espacio de direcciones permitido para las IP de los nodos de trabajo, en lugar de definir reglas explícitas manualmente. Simplifica enormemente la gestión de la política de exportación; las modificaciones a 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 únicamente a los nodos de trabajo que están montando volúmenes y tienen direcciones IP dentro del rango especificado, lo que permite una gestión automatizada y de grano fino.

> 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 front-end y no la dirección IP real del host, por lo que el acceso se denegará cuando no se encuentre ninguna coincidencia en las reglas de exportación.

#### Ejemplo

Existen dos opciones de configuración que deben utilizarse. Aquí tenéis 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 utilizar esta función, debe asegurarse de que la unión raíz en su SVM tenga una política de exportación creada previamente con una regla de exportación que permita el bloque CIDR del nodo (como la política de exportación predeterminada). Siga siempre las mejores prácticas recomendadas NetApp para dedicar una SVM a Trident.

Aquí tienes una explicación de cómo funciona esta función utilizando el ejemplo anterior:

- `autoExportPolicy`está configurado para `true`. Esto indica que Trident crea una política de exportación para cada volumen aprovisionado con este backend para el `svm1` SVM y gestionar la adición y eliminación de reglas utilizando `autoexportCIDRs` bloques de direcciones. 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 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 del nodo dentro del bloque CIDR especificado. Estas direcciones IP también se añadirán a la política de exportación utilizada por el FlexVol volume principal.
  - Por ejemplo:
    - UUID del backend 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`empezar a `true`
    - prefijo de almacenamiento `trident`
    - UUID de PVC a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - El qtree denominado trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c crea una política de exportación para el FlexVol denominado `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 de FlexVol serán un superconjunto de cualquier regla contenida en las políticas de exportación de qtree. La política de exportación vacía será reutilizada por cualquier volumen que no esté adjunto.
- `autoExportCIDRs`Contiene una lista de bloques de direcciones. Este campo es opcional y por defecto es ["0.0.0.0/0", "::/0"]. Si no se define, Trident agrega todas las direcciones unicast de ámbito global que se encuentren en los nodos de trabajo con publicaciones.

En este ejemplo, el `192.168.0.0/24` Se proporciona espacio de direcciones. Esto indica que las direcciones IP de los nodos de Kubernetes que se encuentren 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 compara con los bloques de direcciones proporcionados en `autoExportCIDRs` En el momento de la publicación, después de filtrar las direcciones IP, Trident crea las reglas de política de exportación para las direcciones IP de los clientes del nodo al que está publicando.

Puedes actualizar `autoExportPolicy` y `autoExportCIDRs` para los backends después de crearlos. Puede agregar nuevos CIDR para un backend que se administra automáticamente o eliminar los CIDR existentes. Tenga cuidado al eliminar CIDR para asegurarse de que no se pierdan las conexiones existentes. También puedes optar por desactivar `autoExportPolicy` para un backend y recurrir a una política de exportación creada manualmente. Esto requerirá configurar el `exportPolicy` parámetro en la configuración de tu backend.

Después de que Trident crea o actualiza un backend, puede comprobar el backend mediante `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
```

Cuando se elimina un nodo, Trident revisa todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar la IP de este 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 existentes, actualizar el backend con `tridentctl update backend` garantiza que Trident gestione automáticamente las políticas de exportación. Esto crea dos nuevas políticas de exportación que reciben el nombre del UUID del backend y del nombre del qtree cuando sea necesario. Los volúmenes que se encuentren en el backend utilizarán las políticas de exportación recién creadas después de desmontarlos y volverlos a montar.

> Eliminar un backend con políticas de exportación autogestionadas eliminará la política de exportación creada dinámicamente. Si se vuelve a crear el backend, se tratará como un backend nuevo 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 para los backends que administra para reflejar este cambio de IP.

## Preparar el aprovisionamiento de volúmenes SMB

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

> Debes configurar los protocolos NFS y SMB/CIFS en la SVM para crear una `ontap-nas-economy` Volumen SMB para clústeres ONTAP locales. Si no se configura alguno de estos protocolos, la creación del volumen SMB fallará.

> `autoExportPolicy`No es compatible con volúmenes SMB.

**Antes de empezar**

Antes de poder aprovisionar volúmenes SMB, debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo controlador Linux y al menos un nodo de trabajo 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 que contenga sus credenciales de Active Directory. Para generar secretos `smbcreds` :

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

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

**Pasos**

1. Para ONTAP local, opcionalmente puede crear un recurso compartido SMB o Trident puede crearlo por usted.

   > Se requieren recursos compartidos SMB para Amazon FSx para ONTAP.

   Puedes crear los recursos compartidos de administración SMB de dos maneras: utilizando…"Consola de administración de Microsoft" Complemento de carpetas compartidas o mediante la CLI de ONTAP . Para crear los recursos compartidos SMB mediante la CLI de ONTAP :

   a. Si es necesario, cree la estructura de rutas de directorio para el recurso compartido.

      El `vserver cifs share create` El comando verifica 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 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. Verifique que se haya creado el recurso compartido:

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

Referirse a"Crear un recurso compartido SMB" Para más detalles.

2. Al crear el backend, debe configurar lo siguiente para especificar los volúmenes SMB. Para conocer todas las opciones de configuración del backend de FSx para ONTAP , consulte"Opciones de configuración y ejemplos de FSx para ONTAP" .

| Parámetro | Descripción | Ejemplo |
|---|---|---|
| `smbShare` | Puede especificar una de las siguientes opciones: el nombre de un recurso compartido SMB creado mediante la Consola de administración de Microsoft o la CLI de ONTAP ; un nombre para permitir que Trident cree el recurso compartido SMB; o puede 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 para ONTAP y no puede estar en blanco. | `smb-share` |
| `nasType` | **Debe configurarse 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.** | "" |

### Habilitar 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, puede proporcionar acceso controlado a los recursos compartidos SMB para usuarios y grupos de usuarios de Active Directory (AD) mediante listas de control de acceso (ACL).

#### Puntos para recordar

- Importador `ontap-nas-economy` No se admiten 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.

- La actualización de la anotación PVC, la anotación de la clase de almacenamiento y el campo backend no actualiza la ACL del recurso compartido SMB.
- Las ACL de recursos compartidos SMB especificadas en la anotación del PVC clonado tendrán prioridad sobre las del PVC de origen.
- Asegúrese de proporcionar usuarios de AD válidos al habilitar SMB seguro. Los usuarios no válidos no se agregarán a la ACL.
- Si se proporciona 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, por último, backend.
- Se admite Secure SMB para `ontap-nas` Se aplica a las importaciones de volumen gestionadas y no a las importaciones de volumen no gestionadas.

**Pasos**

1. Especifique 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. Agregue la anotación en la clase de almacenamiento.

   Añade el `trident.netapp.io/smbShareAdUser` Anotación a la clase de almacenamiento para habilitar SMB seguro sin fallos. 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 opciones 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 tubo de PVC.

   El siguiente ejemplo crea un 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 y ejemplos de configuración de ONTAP NAS

Aprenda a crear y utilizar controladores NAS ONTAP con su instalación de Trident . Esta sección proporciona ejemplos de configuración de backend y detalles para mapear backends a StorageClasses.

## Opciones de configuración del backend

Consulte la siguiente tabla para ver las opciones de configuración del backend:

| Parámetro | Descripción | Por defecto |
|---|---|---|
| `version` | | Siempre 1 |
| `storageDriverName` | Nombre del controlador de almacenamiento | `ontap-nas`, `ontap-nas-economy` , o `ontap-nas-flexgroup` |
| `backendName` | Nombre personalizado o el backend de almacenamiento | Nombre del controlador + "_" + dataLIF |
| `managementLIF` | Dirección IP de un clúster o 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 la bandera IPv6. Las direcciones IPv6 deben definirse entre corchetes, como por ejemplo: `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . Para una transición fluida a MetroCluster , consulteEjemplo de MetroCluster . | "10.0.0.1", "[2001:1234:abcd::fefe]" |
| `dataLIF` | Dirección IP del protocolo LIF. NetApp recomienda especificar `dataLIF` . Si no se proporcionan, Trident obtiene los dataLIF del SVM. Puede especificar un nombre de dominio completo (FQDN) para usarlo en las operaciones de montaje NFS, lo que le permite crear un DNS round-robin para equilibrar la carga entre varios dataLIF. Puede modificarse después de la configuración inicial. Referirse a . Se puede configurar para usar direcciones IPv6 si Trident se instaló usando la bandera IPv6. Las direcciones IPv6 deben definirse entre corchetes, como por ejemplo: `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . **Omitir para Metrocluster.** Ver elEjemplo de MetroCluster . | Dirección especificada o derivada de SVM, si no se especifica (no recomendado). |
| `svm` | Máquina virtual de almacenamiento a utilizar **Omitir para Metrocluster.** Ver elEjemplo de MetroCluster . | Derivado si se trata de una SVM `managementLIF` se especifica |
| `autoExportPolicy` | Habilitar la creación y actualización automática de políticas de exportación [Booleano]. Utilizando el `autoExportPolicy` y `autoExportCIDRs` Con algunas opciones, Trident puede gestionar las políticas de exportación automáticamente. | FALSO |
| `autoExportCIDRs` | Lista de CIDR para filtrar las direcciones IP de los nodos de Kubernetes cuando `autoExportPolicy` está habilitado. Utilizando el `autoExportPolicy` y `autoExportCIDRs` Con algunas opciones, Trident puede gestionar las políticas de exportación automáticamente. | ["0.0.0.0/0", "::/0"]` |

| Parámetro | Descripción | Por defecto |
| --- | --- | --- |
| `labels` | Conjunto de etiquetas arbitrarias con formato JSON para aplicar a los volúmenes | "" |
| `clientCertificate` | Valor codificado en Base64 del certificado del cliente. Se utiliza para la autenticación basada en certificados. | "" |
| `clientPrivateKey` | Valor codificado en Base64 de la clave privada del cliente. Se utiliza para la autenticación basada en certificados. | "" |
| `trustedCACertificate` | Valor codificado en Base64 del certificado de CA de confianza. Opcional. Se utiliza para la autenticación basada en certificados. | "" |
| `username` | Nombre de usuario para conectarse al clúster/SVM. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory". | |
| `password` | Contraseña para conectarse al cluster/SVM. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory". | |
| `storagePrefix` | Prefijo utilizado al aprovisionar nuevos volúmenes en la SVM. No se puede actualizar después de configurarlo.<br><br>Cuando se utiliza ontap-nas-economy y un prefijo de almacenamiento de 24 caracteres o más, los qtrees no tendrán el prefijo de almacenamiento incrustado, aunque sí estará en el nombre del volumen. | "tridente" |

| Parámetro | Descripción | Por defecto |
| --- | --- | --- |
| `aggregate` | Agregado para aprovisionamiento (opcional; si se establece, debe asignarse a la SVM). Para el `ontap-nas-flexgroup` conductor, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles se puede utilizar para aprovisionar un volumen FlexGroup .<br><br>Cuando se actualiza el agregado en SVM, se actualiza automáticamente en Trident mediante sondeos a SVM sin necesidad de reiniciar el controlador Trident . Cuando se ha configurado un agregado específico en Trident para aprovisionar volúmenes, si el agregado se renombra o se mueve fuera del SVM, el backend pasará a un estado de error en Trident mientras consulta el agregado del SVM. Debe cambiar el agregado por uno que esté presente en la SVM o eliminarlo por completo para volver a poner en línea el backend. | "" |
| `limitAggregateUsage` | Fallará el aprovisionamiento si el uso supera este porcentaje. **No se aplica a Amazon FSx para ONTAP**. | " (no se aplica por defecto) |
| Lista agregada de flexgroup | Lista de agregados para el aprovisionamiento (opcional; si se establece, debe asignarse a la SVM). Todos los agregados asignados al SVM se utilizan para aprovisionar un volumen FlexGroup . Compatible con el controlador de almacenamiento **ontap-nas-flexgroup**.<br><br>Cuando se actualiza la lista agregada en SVM, la lista se actualiza automáticamente en Trident mediante sondeos a SVM sin necesidad de reiniciar el controlador Trident . Cuando se ha configurado una lista agregada específica en Trident para aprovisionar volúmenes, si la lista agregada se renombra o se mueve fuera de SVM, el backend pasará a un estado de error en Trident mientras consulta el agregado de SVM. Debe cambiar la lista agregada por una que esté presente en la SVM o eliminarla por completo para volver a poner en línea el backend. | "" |

| Parámetro | Descripción | Por defecto |
| --- | --- | --- |
| `limitVolumeSize` | Fallará el aprovisionamiento si el tamaño de volumen solicitado supera este valor. También restringe el tamaño máximo de los volúmenes que administra para los qtrees, y el `qtreesPerFlexvol` Esta opción permite personalizar el número máximo de qtrees por FlexVol volume. | " (no se aplica por defecto) |
| `debugTraceFlags` | Indicadores de depuración para usar al solucionar problemas. Ejemplo: {"api":false, "method":true} No usar `debugTraceFlags` a menos que esté solucionando problemas y necesite un registro detallado. | nulo |
| `nasType` | Configure la creación de volúmenes NFS o SMB. Las opciones son `nfs` , `smb` o nulo. Si se establece en nulo, se utilizarán volúmenes NFS por defecto. | `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 recurrirá a 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 o en el archivo de configuración, Trident no establecerá ninguna opción de montaje en un volumen persistente asociado. | "" |
| `qtreesPerFlexvol` | Número máximo de Qtrees por FlexVol, debe estar en el rango [50, 300] | "200" |
| `smbShare` | Puede especificar una de las siguientes opciones: el nombre de un recurso compartido SMB creado mediante la Consola de administración de Microsoft o la CLI de ONTAP ; un nombre para permitir que Trident cree el recurso compartido SMB; o puede 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 para ONTAP y no puede estar en blanco. | `smb-share` |

| Parámetro | Descripción | Por defecto |
|---|---|---|
| `useREST` | Parámetro booleano para utilizar las API REST de ONTAP . `useREST`Cuando se configura para `true` Trident utiliza las API REST de ONTAP para comunicarse con el backend; cuando se configura en `false` Trident utiliza 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 `ontapi` solicitud. Esto se satisface mediante lo predefinido. `vsadmin` y `cluster-admin` roles. A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posterior, `useREST` está configurado para `true` por defecto; cambiar `useREST` a `false` para utilizar llamadas ONTAPI (ZAPI). | `true`para ONTAP 9.15.1 o posterior, de lo contrario `false`. |
| `limitVolumePoolSize` | Tamaño máximo de FlexVol que se puede solicitar al usar Qtrees en el backend ontap-nas-economy. | " (no se aplica por defecto) |
| `denyNewVolumePools` | Restringe `ontap-nas-economy` backends que crean nuevos volúmenes FlexVol para contener sus Qtrees. Solo se utilizan Flexvols preexistentes para el aprovisionamiento de nuevos PV. | |
| `adAdminUser` | Usuario o grupo de usuarios administradores de Active Directory con acceso completo a los recursos compartidos SMB. Utilice este parámetro para otorgar derechos de administrador al recurso compartido SMB con control total. | |

## Opciones de configuración de backend para el aprovisionamiento de volúmenes

Puedes controlar el aprovisionamiento predeterminado utilizando estas opciones en el `defaults` sección de la configuración. Para ver un ejemplo, consulte los ejemplos de configuración a continuación.

| Parámetro | Descripción | Por defecto |
|---|---|---|
| `spaceAllocation` | Asignación de espacio para Qtrees | "verdadero" |
| `spaceReserve` | Modo de reserva de espacio: "ninguno" (delgado) o "volumen" (grueso). | "ninguno" |
| `snapshotPolicy` | Política de instantáneas a utilizar | "ninguno" |
| `qosPolicy` | Grupo de políticas QoS que se asignará a los volúmenes creados. Elija una de las opciones qosPolicy o adaptiveQosPolicy por grupo de almacenamiento/backend. | "" |

| Parámetro | Descripción | Por defecto |
|---|---|---|
| `adaptiveQosPolicy` | Grupo de políticas QoS adaptativas para asignar a los volúmenes creados. Elija una de las opciones qosPolicy o adaptiveQosPolicy por grupo de almacenamiento/backend. No compatible con ontap-nas-economy. | "" |
| `snapshotReserve` | Porcentaje de volumen reservado para instantáneas | "0" si `snapshotPolicy` es "ninguno", de lo contrario "" |
| `splitOnClone` | Separar un clon de su progenitor al crearlo | "FALSO" |
| `encryption` | Habilite el cifrado de volumen de NetApp (NVE) en el nuevo volumen; el valor predeterminado es `false` . Para utilizar esta opción, NVE debe estar licenciado y habilitado en el clúster. Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NAE habilitado. Para obtener más información, consulte:"Cómo funciona Trident con NVE y NAE" . | "FALSO" |
| `tieringPolicy` | Política de niveles para usar "ninguno" | |
| `unixPermissions` | Modo para nuevos volúmenes | "777" para volúmenes NFS; vacío (no aplicable) para volúmenes SMB |
| `snapshotDir` | Controla el acceso a `.snapshot` directorio | "verdadero" para NFSv4, "falso" para NFSv3 |
| `exportPolicy` | Política de exportación a utilizar | "por defecto" |
| `securityStyle` | Estilo de seguridad para nuevos volúmenes. NFS admite `mixed` y `unix` Estilos de seguridad. Las PYMES son compatibles con el soporte. `mixed` y `ntfs` Estilos de seguridad. | El valor predeterminado de NFS es `unix` . El valor predeterminado de SMB es `ntfs` . |
| `nameTemplate` | Plantilla para crear nombres de volumen personalizados. | "" |

El uso de grupos de políticas QoS con Trident requiere ONTAP 9.8 o posterior. Debe utilizar un grupo de políticas QoS no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas QoS compartidas impone un límite máximo al rendimiento total de todas las cargas de trabajo.

**Ejemplos de aprovisionamiento por volumen**

Aquí tenéis 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 utiliza un nuevo cálculo para garantizar 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 mediante el nuevo cálculo. Este cálculo garantiza que el usuario reciba el espacio de escritura solicitado en el PVC, y no menos espacio del solicitado. Antes de la versión v21.07, cuando el usuario solicitaba un PVC (por ejemplo, 5 GiB), con el snapshotReserve al 50 %, obtenía solo 2,5 GiB de espacio de escritura. Esto se debe a que lo que el usuario solicitó fue el volumen completo y `snapshotReserve` es un porcentaje de eso. Con Trident 21.07, lo que el usuario solicita es el espacio de escritura y Trident define el `snapshotReserve` número como porcentaje del volumen total. 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 PVC = 5 GiB, el tamaño total del volumen es 5/.5 = 10 GiB y el tamaño disponible es 5 GiB, que es lo que el usuario solicitó en la solicitud de PVC El `volume show` El comando debería mostrar resultados similares a este ejemplo:


Los backends existentes de instalaciones anteriores aprovisionarán volúmenes como se explicó anteriormente al actualizar Trident. Para los volúmenes creados antes de la actualización, debe redimensionarlos para que se observe el cambio. Por ejemplo, un PVC de 2 GiB con `snapshotReserve=50` Anteriormente se obtuvo un volumen que proporciona 1 GiB de espacio de escritura. Por ejemplo, al redimensionar el volumen a 3 GiB, la aplicación obtiene 3 GiB de espacio de escritura en un volumen de 6 GiB.

## Ejemplos de configuración mínima

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

> Si está utilizando Amazon FSx en NetApp ONTAP con Trident, se recomienda 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 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**

Puede configurar el backend para evitar tener que actualizar manualmente la definición del backend después del cambio de estado y el cambio de estado durante"replicación y recuperación de SVM" .

Para una conmutación y recuperación sin interrupciones, especifique el SVM utilizando `managementLIF` y omitir el `dataLIF` y `svm` parámetros. 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 mínimo de configuración de backend. `clientCertificate` , `clientPrivateKey` , y `trustedCACertificate` (opcional, si se utiliza una CA de confianza) se rellenan en `backend.json` y tome los valores codificados en base64 del certificado del 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 puede configurar Trident para que utilice políticas de exportación dinámicas para crear y gestionar automáticamente la política de exportación. Esto funciona igual para el `ontap-nas-economy` y `ontap-nas-flexgroup` conductores.

```
---
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` utilizando 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 con volúmenes SMB

El `smbShare` Este parámetro es necesario para FSx para ONTAP que utiliza 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 plantilla de nombre**

```
---
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 grupos de almacenamiento, tales 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 están configurados en FlexVol para `ontap-nas` o FlexGroup para `ontap-nas-flexgroup` . Trident copia todas las etiquetas presentes en un grupo virtual al volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por grupo virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los grupos de almacenamiento establecen sus propias configuraciones. `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 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"
```

## Asignar backends a StorageClasses

Las siguientes definiciones de StorageClass hacen referencia aEjemplos de backends con pools virtuales . Utilizando el `parameters.selector` En cada campo, cada StorageClass especifica qué grupos virtuales se pueden usar para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- El `protection-gold` StorageClass se asignará al primer y segundo grupo virtual en el `ontap-nas-flexgroup` backend. Estas son las únicas piscinas 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 grupo virtual en el `ontap-nas-flexgroup` backend. Estas son las únicas piscinas que ofrecen un nivel de protección distinto al oro.

```
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 asignará al cuarto grupo virtual en el `ontap-nas` backend. Este es el único pool que ofrece configuración de pool de almacenamiento para aplicaciones 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"
```

- El `protection-silver-creditpoints-20k` StorageClass se asignará al tercer grupo virtual en el `ontap-nas-flexgroup` backend. Este es el único fondo 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 grupo virtual en el `ontap-nas` backend y el segundo grupo virtual en el `ontap-nas-economy` backend. Estas son las únicas ofertas de pool 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 garantiza que se cumplan los requisitos de almacenamiento.

## Actualizar `dataLIF` después de la configuración inicial

Puede cambiar el dataLIF después de la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON de 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, debe desconectar todos los pods correspondientes y luego volver a conectarlos para que el nuevo dataLIF surta efecto.

## Ejemplos de seguridad para pymes

### 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 de 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 del backend con grupo de almacenamiento**

```
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 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
```

Asegúrese de agregar `annotations` para habilitar SMB seguro. El protocolo SMB seguro no funciona sin las anotaciones, independientemente de las configuraciones establecidas en el backend o en el PVC.

**Ejemplo de clase de almacenamiento con 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 solo usuario de 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 múltiples usuarios de 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
```