# Controladores SAN de ONTAP

## Trident

NetApp
July 01, 2026

# Tabla de contenidos

# Controladores SAN de ONTAP

## Descripción general del controlador SAN de ONTAP

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

### Detalles del controlador SAN de ONTAP

Trident proporciona los siguientes controladores de almacenamiento SAN 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-san` | iSCSI SCSI sobre FC | Bloque | RWO, ROX, RWX, RWOP | Sin sistema de archivos; dispositivo de bloque sin formato |
| `ontap-san` | iSCSI SCSI sobre FC | Sistema de archivos | RWO, RWOP<br><br>ROX y RWX no están disponibles en el modo de volumen de sistema de archivos. | `xfs`, `ext3`, `ext4` |
| `ontap-san` | NVMe/TCP<br><br>Consulta Consideraciones adicionales para NVMe/TCP. | Bloque | RWO, ROX, RWX, RWOP | Sin sistema de archivos; dispositivo de bloque sin formato |
| `ontap-san` | NVMe/TCP<br><br>Consulta Consideraciones adicionales para NVMe/TCP. | Sistema de archivos | RWO, RWOP<br><br>ROX y RWX no están disponibles en el modo de volumen de sistema de archivos. | `xfs`, `ext3`, `ext4` |
| `ontap-san-economy` | iSCSI | Bloque | RWO, ROX, RWX, RWOP | Sin sistema de archivos; dispositivo de bloque sin formato |

| Controlador | Protocolo | volumeMode | Modos de acceso admitidos | Sistemas de archivos compatibles |
|---|---|---|---|---|
| `ontap-san-economy` | iSCSI | Sistema de archivos | RWO, RWOP<br><br>ROX y RWX no están disponibles en el modo de volumen de sistema de archivos. | `xfs`, `ext3`, `ext4` |

- 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.

## Consideraciones adicionales para NVMe/TCP

Trident admite el protocolo non-volatile memory express (NVMe) usando el `ontap-san` driver, incluyendo:

- IPv6
- Instantáneas y clones de volúmenes NVMe
- Cambiar el tamaño de un volumen NVMe
- Importar un volumen NVMe que se creó fuera de Trident para que su ciclo de vida pueda ser gestionado por Trident

- Multipathing nativo de NVMe
- Apagado correcto o incorrecto de los nodos K8s (24.06)

Trident no admite:

- DH-HMAC-CHAP que es compatible de forma nativa con NVMe
- Mapeador de dispositivos (DM) multipathing
- Cifrado LUKS

NVMe solo es compatible con las API REST de ONTAP y no es compatible con ONTAPI (ZAPI).

# Prepárate para configurar el backend con controladores SAN de ONTAP

Entiende los requisitos y las opciones de autenticación para configurar un backend de ONTAP con controladores SAN de ONTAP.

## Requisitos

Para todos los backends de ONTAP, Trident requiere que al menos un agregado esté asignado a la SVM.

"Sistemas ASA r2" se diferencian de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. En los sistemas ASA r2, se utilizan zonas de disponibilidad de almacenamiento en lugar de agregados. Consulta el "esto" artículo de base de conocimientos sobre cómo asignar agregados a SVMs en sistemas ASA r2.

Recuerda que también puedes ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, podrías configurar una `san-dev` clase que use el `ontap-san` controlador y una `san-default` clase que use el `ontap-san-economy` otro.

Todos tus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulta "Prepara el nodo trabajador" para más detalles.

## Autentica el backend de ONTAP

Trident ofrece dos modos de autenticación para un backend ONTAP.

- Basado en credenciales: el nombre de usuario y la contraseña de un usuario de ONTAP con los permisos necesarios. Se recomienda usar 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: Trident también puede comunicarse con un clúster de ONTAP usando un certificado instalado en el backend. 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-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

**JSON**

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

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=admin"
```

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
```

> Después de ejecutar este comando, ONTAP solicita la introducción del certificado. Pega el contenido del `k8senv.pem` archivo generado en el paso 1, luego introduce `END` para completar la instalación.

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

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.

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

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

**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 backend update`.

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

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

> 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"

## Autentica conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para los `ontap-san` y `ontap-san-economy` controladores. Esto requiere habilitar la opción `useCHAP` en la definición de tu backend. Cuando se establece en `true`, Trident configura la seguridad del iniciador predeterminado de la SVM como CHAP bidireccional y establece el nombre de usuario y los secretos desde el archivo del backend. NetApp recomienda usar CHAP bidireccional para autenticar conexiones. Mira la siguiente configuración de ejemplo:

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
```

El `useCHAP`parámetro es una opción booleana que solo se puede configurar una vez. Se establece en falso de forma predeterminada. Después de que lo configuras en verdadero, ya no puedes ponerlo en falso.

Además de `useCHAP=true`, los `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername` y `chapUsername` campos deben incluirse en la definición del backend. Los secretos se pueden cambiar después de crear un backend ejecutando `tridentctl update`.

#### Cómo funciona

Al establecer `useCHAP` en true, el administrador de almacenamiento le indica a Trident que configure CHAP en el backend de almacenamiento. Esto incluye lo siguiente:

- Configurar CHAP en la SVM:
  - Si el tipo de seguridad del iniciador predeterminado de la SVM es ninguno (establecido de manera predeterminada) **y** no hay LUN preexistentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en `CHAP` y procederá a configurar el nombre de usuario y los secretos del iniciador y del destino CHAP.
  - Si la SVM contiene LUNs, Trident no habilitará CHAP en la SVM. Esto garantiza que el acceso a los LUNs que ya están presentes en la SVM no esté restringido.
- Configurar el iniciador CHAP y el nombre de usuario y los secretos del destino; estas opciones deben especificarse en la configuración del backend (como se muestra arriba).

Después de que se crea el backend, Trident crea un CRD correspondiente `tridentbackend` y almacena los secretos y nombres de usuario CHAP como secretos de Kubernetes. Todos los PV que Trident cree en este backend se montarán y conectarán mediante CHAP.

#### Rotar credenciales y actualizar backends

Puedes actualizar las credenciales CHAP actualizando los parámetros CHAP en el archivo `backend.json`. Esto requerirá actualizar los secretos CHAP y usar el comando `tridentctl update` para reflejar estos cambios.

Al actualizar los secretos CHAP de un backend, debes usar `tridentctl` para actualizar el backend. No actualices las credenciales en el clúster de almacenamiento usando la CLI de ONTAP o el System Manager de ONTAP, ya que Trident no podrá detectar estos cambios.

```
cat backend-san.json
{
    "version": 1,
    "storageDriverName": "ontap-san",
    "backendName": "ontap_san_chap",
    "managementLIF": "192.168.0.135",
    "svm": "ontap_iscsi_svm",
    "useCHAP": true,
    "username": "vsadmin",
    "password": "password",
    "chapInitiatorSecret": "cl9qxUpDaTeD",
    "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
    "chapTargetUsername": "iJF4heBRT0TCwxyz",
    "chapUsername": "uh2aNCLSd6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+----------------+----------------+--------------------------------------
+--------+---------+
|   NAME         | STORAGE DRIVER |                 UUID                 |
STATE   | VOLUMES |
+----------------+----------------+--------------------------------------
+--------+---------+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online |       7 |
+----------------+----------------+--------------------------------------
+--------+---------+
```

Las conexiones existentes no se verán afectadas; seguirán activas si Trident actualiza las credenciales en la SVM. Las nuevas conexiones usan las credenciales actualizadas y las conexiones existentes siguen activas. Desconectar y volver a conectar los PV antiguos hará que usen las credenciales actualizadas.

# Opciones de configuración y ejemplos de ONTAP SAN

Aprende cómo crear y usar controladores ONTAP SAN con tu instalación de Trident. Esta sección ofrece ejemplos de configuración de backends y detalles para asignar backends a StorageClasses. "Sistemas ASA r2" se diferencian de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. Estas variaciones afectan el uso de ciertos parámetros como se indica. "Conoce más sobre las diferencias entre los sistemas ASA r2 y otros sistemas ONTAP". En la configuración del backend de Trident, no necesitas especificar que tu sistema es ASA r2. Cuando seleccionas `ontap-`

`san` como `storageDriverName`, Trident detecta automáticamente el ASA r2 u otros sistemas ONTAP. Algunos parámetros de configuración del backend no aplican a los sistemas ASA r2, como se indica en la tabla de abajo.

> Solo el controlador `ontap-san` (con protocolos iSCSI, NVMe/TCP y FC) es compatible con los sistemas ASA r2.

## Opciones de configuración del backend

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

| Parámetro | Descripción | Predeterminado |
|---|---|---|
| `version` | | Siempre 1 |
| `storageDriverName` | Nombre del controlador de almacenamiento | `ontap-san` o `ontap-san-economy` |
| `backendName` | Nombre personalizado o el backend de almacenamiento | Nombre del driver + "_" + dataLIF |
| `managementLIF` | Dirección IP de un LIF de gestión de clúster o SVM.<br><br>Se puede especificar un nombre de dominio completo (FQDN).<br><br>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]`.<br><br>Para una conmutación de sitios sin interrupciones de MetroCluster, consulta el Ejemplo de MetroCluster.<br><br>> Si usas credenciales "vsadmin", `managementLIF` debe ser el de la SVM; si usas credenciales "admin", `managementLIF` debe ser el del clúster. | "10.0.0.1", "[2001:1234:abcd::fefe]" |
| `dataLIF` | Dirección IP del LIF de protocolo. 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]`. **No especifiques para iSCSI.** Trident usa "Mapa LUN selectivo de ONTAP" para descubrir los LIF de iSCSI necesarios para establecer una sesión multipath. Se genera una advertencia si `dataLIF` se define explícitamente. **Omite para MetroCluster.** Consulta la Ejemplo de MetroCluster. | Derivado por la SVM |

| Parámetro | Descripción | Predeterminado |
| --- | --- | --- |
| `svm` | Máquina virtual de almacenamiento a usar **Omitir para MetroCluster.** Consulta la Ejemplo de MetroCluster. | Se deriva si se especifica un SVM `managementLIF` |
| `useCHAP` | Usa CHAP para autenticar iSCSI para los controladores ONTAP SAN [parámetro booleano]. Establécelo en `true` para que Trident configure y use CHAP bidireccional como la autenticación predeterminada para el SVM dado en el backend. Consulta "Prepárate para configurar el backend con controladores SAN de ONTAP" para más detalles. **No es compatible con FCP o NVMe/TCP.** | `false` |
| `chapInitiatorSecret` | Secreto del iniciador de CHAP. Requerido si `useCHAP=true` | "" |
| `labels` | Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes | "" |
| `chapTargetInitiatorSecret` | Secreto del iniciador de destino CHAP. Requerido si `useCHAP=true` | "" |
| `chapUsername` | Nombre de usuario de entrada. Requerido si `useCHAP=true` | "" |
| `chapTargetUsername` | Nombre de usuario de destino. Requerido si `useCHAP=true` | "" |
| `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. Se usa para la autenticación basada en certificados. | "" |
| `username` | Nombre de usuario necesario para comunicarte con el clúster ONTAP. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, mira "Autentica Trident en un SVM backend usando credenciales de Active Directory". | "" |
| `password` | Contraseña necesaria para comunicarte con el clúster ONTAP. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, mira "Autentica Trident en un SVM backend usando credenciales de Active Directory". | "" |
| `svm` | Máquina virtual de almacenamiento que vas a usar | Se deriva si se especifica un SVM `managementLIF` |

| Parámetro | Descripción | Predeterminado |
| --- | --- | --- |
| `storagePrefix` | Prefijo utilizado al aprovisionar nuevos volúmenes en la SVM. No se puede modificar después. Para actualizar este parámetro, tendrás que crear un nuevo backend. | `trident` |
| `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.<br><br>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.<br><br>**No especificar para sistemas ASA r2**. | "" |
| `limitAggregateUsage` | Falla el aprovisionamiento si el uso es superior a este porcentaje. Si estás usando un backend de Amazon FSx para NetApp ONTAP, no especifiques `limitAggregateUsage`. Los `fsxadmin` y `vsadmin` no tienen los permisos necesarios para recuperar el uso agregado y limitarlo usando Trident. **No especificar para sistemas ASA r2**. | "" (no aplicado por defecto) |
| `limitVolumeSize` | Falla el aprovisionamiento si el tamaño del volumen solicitado supera este valor. También restringe el tamaño máximo de los volúmenes que gestiona para LUNs. | "" (no aplicado por defecto) |
| `lunsPerFlexvol` | Máximo de LUNs por FlexVol, debe estar en el rango [50, 200] | `100` |
| `debugTraceFlags` | Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, {"api":false, "method":true} no lo uses a menos que estés solucionando problemas y necesites un volcado detallado del registro. | `null` |

| Parámetro | Descripción | Predeterminado |
| --- | --- | --- |
| `useREST` | Parámetro booleano para usar las ONTAP REST APIs.<br><br>`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).<br><br>`useREST` está totalmente calificado para NVMe/TCP.<br><br>NVMe solo es compatible con las API REST de ONTAP y no es compatible con ONTAPI (ZAPI).<br><br>**Si se especifica, siempre configúralo en `true` para sistemas ASA r2**. | `true` para ONTAP 9.15.1 o posterior, de lo contrario `false`. |
| `sanType` | Usa para seleccionar `iscsi` para iSCSI, `nvme` para NVMe/TCP o `fcp` para SCSI sobre Fibre Channel (FC). | `iscsi` si está en blanco |

| Parámetro | Descripción | Predeterminado |
|---|---|---|
| `formatOptions` | Usa `formatOptions` para especificar argumentos de la línea de comandos para el comando `mkfs`, que se aplicarán cada vez que se formatee un volumen. Esto te permite formatear el volumen según tus preferencias. Asegúrate de especificar formatOptions similar a las opciones del comando mkfs, excluyendo la ruta del dispositivo. Ejemplo: "-E nodiscard"<br><br>**Compatible con `ontap-san` y `ontap-san-economy` controladores con el protocolo iSCSI. Además, compatible con sistemas ASA r2 cuando usas los protocolos iSCSI y NVMe/TCP.** | |
| `limitVolumePoolSize` | Tamaño máximo solicitable de FlexVol al utilizar LUNs en el backend de ontap-san-economy. | "" (no aplicado por defecto) |
| `denyNewVolumePools` | Restringe `ontap-san-economy` a los backends crear nuevos volúmenes FlexVol para contener sus LUN. Solo se usan FlexVols preexistentes para aprovisionar nuevos PV. | |

#### Recomendaciones para usar formatOptions

Trident recomienda las siguientes opciones para acelerar el proceso de formateo:

- **-E nodiscard (ext3, ext4):** No intentes descartar bloques al momento de ejecutar mkfs (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento disperso o Thin-Provisioning). Esto reemplaza la opción obsoleta "-K" y es aplicable a los sistemas de archivos ext3 y ext4.
- **-K (xfs):** No intentes descartar bloques durante la ejecución de mkfs. Esta opción es aplicable al sistema de archivos xfs.

#### Autentica Trident en un SVM backend usando credenciales de Active Directory

Puedes configurar Trident para que se autentique en una SVM de backend usando credenciales de Active Directory (AD). Antes de que una cuenta de AD pueda acceder a la SVM, tienes que configurar el acceso del controlador de dominio de AD al clúster o a la SVM. Para la administración del clúster con una cuenta de AD, tienes que crear un domain tunnel. Consulta "Configura el acceso al controlador de dominio de Active Directory en ONTAP" para más detalles.

**pasos**

1. Configura los ajustes de Domain Name System (DNS) para un SVM de backend:

   ```
   vserver services dns create -vserver <svm_name> -dns-servers
   <dns_server_ip1>,<dns_server_ip2>
   ```

2. Ejecuta el siguiente comando para crear una cuenta de equipo para la SVM en Active Directory:

   ```
   vserver active-directory create -vserver DataSVM -account-name ADSERVER1
   -domain demo.netapp.com
   ```

3. Usa este comando para crear un usuario o grupo de AD para administrar el clúster o SVM

```
security login create -vserver <svm_name> -user-or-group-name
<ad_user_or_group> -application <application> -authentication-method domain
-role vsadmin
```

4. En el archivo de configuración del backend de Trident, establece los parámetros `username` y `password` en el nombre de usuario o grupo de AD y la contraseña, respectivamente.

## 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 LUNs | "verdadero" **Si se especifica, configúralo en `true` para sistemas ASA r2**. |
| `spaceReserve` | Modo de reserva de espacio; "ninguno" (thin) o "volumen" (thick). **Configúralo en `none` sistemas ASA r2**. | "none" |
| `snapshotPolicy` | Política de SnapVault que se va a usar. **Establece en `none` para sistemas ASA r2**. | "none" |
| `qosPolicy` | Grupo de políticas de QoS para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento/backend. 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. | "" |
| `adaptiveQosPolicy` | Grupo de políticas de QoS adaptativo para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por cada pool de almacenamiento/backend | "" |
| `snapshotReserve` | Porcentaje de volumen reservado para instantáneas. **No especificar para sistemas ASA r2**. | "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". | "falso" **Si se especifica, configúralo en `true` para sistemas ASA r2**. |

| Parámetro | Descripción | Predeterminado |
|---|---|---|
| `luksEncryption` | Activa el cifrado LUKS. Consulta "Usa Linux Unified Key Setup (LUKS)". | "" **Establécelo en `false` para sistemas ASA r2.** |
| `tieringPolicy` | Política de niveles para usar "none" **No especificar para sistemas ASA r2.** | |
| `nameTemplate` | Plantilla para crear nombres de volúmenes personalizados. | "" |

#### Ejemplos de aprovisionamiento de volumen

Aquí tienes un ejemplo con valores predeterminados definidos:

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

> Para todos los volúmenes creados usando el `ontap-san` driver, Trident añade un 10 por ciento extra de capacidad al FlexVol para alojar los metadatos del LUN. El LUN se aprovisionará con el tamaño exacto que el usuario solicite en la PVC. Trident añade un 10 por ciento al FlexVol (se muestra como tamaño disponible en ONTAP). Ahora los usuarios obtendrán la cantidad de capacidad utilizable que solicitaron. Este cambio también evita que los LUN se vuelvan de solo lectura a menos que se utilice completamente el espacio disponible. Esto no aplica a ontap-san-economy.

Para los backends que definen `snapshotReserve`, Trident calcula el tamaño de los volúmenes de la siguiente manera:

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

El 1.1 es el 10 % adicional que Trident añade a la FlexVol para alojar los metadatos del LUN. Para `snapshotReserve` = 5 %, y una solicitud de PVC de 5 GiB, el tamaño total del volumen es 5.79 GiB y el tamaño disponible es 5.5 GiB. El `volume show` comando debería mostrar resultados similares a este ejemplo:


Actualmente, cambiar el tamaño es la única manera de usar el nuevo cálculo para un volumen existente.

## 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, NetApp recomienda que especifiques nombres DNS para las LIFs en vez de direcciones IP.

**Ejemplo de ONTAP SAN**

Esta es una configuración básica usando el `ontap-san` driver.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

#### Ejemplo de 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 y reversión sin problemas, especifica el SVM usando `managementLIF` y omite los parámetros `svm`. Por ejemplo:

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

#### Ejemplo de ONTAP SAN economy

```
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
username: vsadmin
password: <password>
```

**Ejemplo de autenticación basada en certificados**

En este ejemplo de configuración básica `clientCertificate`, `clientPrivateKey` y `trustedCACertificate` (opcional, si usas una CA confiable) se completan en `backend.json` y toman los valores codificados en base64 del certificado del cliente, la clave privada y el certificado de CA confiable, respectivamente.

```
---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

### Ejemplos de CHAP bidireccional

Estos ejemplos crean un backend con `useCHAP` configurado en `true`.

#### Ejemplo de ONTAP SAN CHAP

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

#### Ejemplo de ONTAP SAN economy CHAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

#### Ejemplo de NVMe/TCP

Debes tener una SVM configurada con NVMe en tu backend de ONTAP. Esta es una configuración básica de backend para NVMe/TCP.

```
---
version: 1
backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true
```

#### Ejemplo de SCSI sobre FC (FCP)

Debes tener una SVM configurada con FC en tu backend de ONTAP. Esta es una configuración básica de backend para FC.

```
---
version: 1
backendName: fcp-backend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_fc
username: vsadmin
password: password
sanType: fcp
useREST: true
```

**Ejemplo de configuración de backend con nameTemplate**

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap-san-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
"{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

**formatOptions ejemplo para el controlador ontap-san-economy**

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard
```

## Ejemplos de backends con pools virtuales

En estos archivos de definición de backend de ejemplo, se establecen valores predeterminados específicos para todos los grupos 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 el volumen FlexVol. Trident copia todas las etiquetas presentes en un pool virtual al volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de

almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los pools de almacenamiento establecen sus propios `spaceReserve`, `spaceAllocation` y `encryption` valores, y algunos pools anulan los valores predeterminados.

### Ejemplo de ONTAP SAN

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "40000"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
      adaptiveQosPolicy: adaptive-extreme
  - labels:
      protection: silver
      creditpoints: "20000"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
      qosPolicy: premium
  - labels:
      protection: bronze
      creditpoints: "5000"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
```

**Ejemplo de ONTAP SAN economy**

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
labels:
  store: san_economy_store
region: us_east_1
storage:
  - labels:
      app: oracledb
      cost: "30"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
  - labels:
      app: postgresdb
      cost: "20"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
  - labels:
      app: mysqldb
      cost: "10"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
  - labels:
      department: legal
      creditpoints: "5000"
    zone: us_east_1c
```

```
    defaults:
      spaceAllocation: "true"
      encryption: "false"
```

**Ejemplo de NVMe/TCP**

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:
      app: testApp
      cost: "20"
    defaults:
      spaceAllocation: "false"
      encryption: "false"
```

## Asigna backends a StorageClasses

Las siguientes definiciones de StorageClass se refieren 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 pool virtual en el `ontap-san` backend. Este es el único pool que ofrece 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 segundo y tercer pool virtual en `ontap-san` backend. Estos son los únicos pools 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 tercer pool virtual en `ontap-san-economy` backend. Este es el único pool que ofrece configuración de pool de almacenamiento para la 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 segundo pool virtual en `ontap-san` 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 grupo virtual en el `ontap-san` backend y al cuarto grupo virtual en el `ontap-san-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"
```

- El `my-test-app-sc` StorageClass se asignará al `testAPP` grupo virtual en el `ontap-san` driver con `sanType: nvme`. Este es el único grupo que ofrece `testApp`.

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

Trident decidirá qué grupo virtual se selecciona y se asegurará de que se cumpla el requisito de almacenamiento.