Controladores SAN de ONTAP

Trident

NetApp
January 15, 2026

Tabla de contenidos

Controladores SAN de ONTAP

Descripción general del controlador SAN de ONTAP

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

Conductor	Protocolo	modo de volumen	Modos de acceso compatibles	Sistemas de archivos compatibles
`ontap-san`	iSCSI SCSI sobre FC	Bloquear	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloques sin formato
`ontap-san`	iSCSI SCSI sobre FC	Sistema de archivos	RWO, RWOP Los parámetros ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3` , `ext4`
`ontap-san`	NVMe/TCP Referirse aConsideraciones adicionales para NVMe/TCP .	Bloquear	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloques sin formato
`ontap-san`	NVMe/TCP Referirse aConsideraciones adicionales para NVMe/TCP .	Sistema de archivos	RWO, RWOP Los parámetros ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3` , `ext4`

Conductor	Protocolo	modo de volumen	Modos de acceso compatibles	Sistemas de archivos compatibles
`ontap-san-economy`	iSCSI	Bloquear	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloques sin formato
`ontap-san-economy`	iSCSI	Sistema de archivos	RWO, RWOP Los parámetros ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3` , `ext4`

- 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.

Consideraciones adicionales para NVMe/TCP

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

- IPv6
- Instantáneas y clones de volúmenes NVMe
- Redimensionar un volumen NVMe
- Importar un volumen NVMe creado fuera de Trident para que su ciclo de vida pueda ser gestionado por Trident.
- Multiruta nativa de NVMe
- Apagado correcto o incorrecto de los nodos K8s (24.06)

Trident no admite:

- DH-HMAC-CHAP compatible de forma nativa con NVMe
- Multiruta del mapeador de dispositivos (DM)
- Cifrado LUKS

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

Prepárese para configurar el backend con los controladores SAN de ONTAP.

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

Requisitos

Para todos los backends de ONTAP , Trident requiere que se asigne al menos un agregado al 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. Referirse a"este" Artículo de la base de conocimientos sobre cómo asignar agregados a SVM 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 un `san-dev` clase que utiliza la `ontap-san` conductor y un `san-default` clase que utiliza la `ontap-san-economy` uno.

Todos los nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Referirse a "Preparar el nodo de trabajo" Para más detalles.

Autenticar el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP .

- Basado en credenciales: El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos necesarios. Se recomienda utilizar 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: Trident también puede comunicarse con un clúster ONTAP utilizando 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 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-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"
}
```

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 o 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=admin"
```

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

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.

```
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.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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

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 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 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"

Autenticar conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para la `ontap-san` y `ontap-san-economy`

conductores. Esto requiere habilitar el `useCHAP` opción en la definición de tu backend. Cuando se configura para `true` Trident configura la seguridad del iniciador predeterminado de la SVM en CHAP bidireccional y establece el nombre de usuario y los secretos desde el archivo de backend. NetApp recomienda utilizar CHAP bidireccional para autenticar las conexiones. Consulte la siguiente configuración de ejemplo:

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

El `useCHAP` El parámetro es una opción booleana que solo se puede configurar una vez. Está configurado como falso por defecto. Una vez que lo hayas configurado como verdadero, no podrás configurarlo como falso.

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

Cómo funciona

Mediante la configuración `useCHAP` Para que sea verdadero, el administrador de almacenamiento le indica a Trident que configure CHAP en el backend de almacenamiento. Esto incluye lo siguiente:

- Configuración de CHAP en la SVM:
  - Si el tipo de seguridad del iniciador predeterminado de la SVM es ninguno (establecido por defecto) **y** no hay LUN preexistentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en `CHAP` y proceda a configurar el iniciador CHAP y el nombre de usuario y las claves de destino.
  - Si la SVM contiene LUN, Trident no habilitará CHAP en la SVM. Esto garantiza que el acceso a las LUN que ya están presentes en la SVM no se vea restringido.
- Configurar el nombre de usuario y las claves secretas del iniciador y del destino CHAP; estas opciones deben especificarse en la configuración del backend (como se muestra arriba).

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

Rotar credenciales y actualizar backends

Puede actualizar las credenciales CHAP actualizando los parámetros CHAP en el archivo `backend.json`

archivo. Esto requerirá actualizar los secretos CHAP y utilizar el `tridentctl update` orden para reflejar estos cambios.

> Al actualizar los secretos CHAP para un backend, debe usar `tridentctl` para actualizar el backend. No actualice las credenciales en el clúster de almacenamiento mediante ONTAP CLI o ONTAP System Manager, 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 utilizan las credenciales actualizadas y las conexiones existentes permanecen activas. Desconectar y volver a conectar los PV antiguos hará que utilicen las credenciales actualizadas.

Opciones y ejemplos de configuración de SAN de ONTAP

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

"Sistemas ASA r2"Se diferencia de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa

de almacenamiento. Estas variaciones afectan al uso de ciertos parámetros, tal como se indica. "Obtenga más información sobre las diferencias entre los sistemas ASA r2 y otros sistemas ONTAP .".

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

En la configuración del backend de Trident , no es necesario especificar que su sistema sea ASA r2. Cuando seleccionas `ontap-san` como el `storageDriverName` Trident detecta automáticamente el ASA r2 o el sistema ONTAP tradicional. Algunos parámetros de configuración del backend no son aplicables a los sistemas ASA r2, como se indica en la tabla siguiente.

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-san`o `ontap-san-economy`
`backendName`	Nombre personalizado o el backend de almacenamiento	Nombre del controlador + "_" + dataLIF
`managementLIF`	Dirección IP de un clúster o LIF de gestión 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 . > Si está utilizando credenciales "vsadmin", `managementLIF` debe ser la del SVM; si se utilizan credenciales de "administrador", `managementLIF` debe ser el del grupo.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parámetro	Descripción	Por defecto
`dataLIF`	Dirección IP del protocolo LIF. 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]` . **No especificar para iSCSI.** Trident utiliza"Mapa selectivo de LUN de ONTAP" para descubrir los LIF iSCSI necesarios para establecer una sesión de múltiples rutas. Se genera una advertencia si `dataLIF` está definido explícitamente. **Omitir para Metrocluster.** Ver elEjemplo de MetroCluster .	Derivado por la SVM
`svm`	Máquina virtual de almacenamiento a utilizar **Omitir para Metrocluster.** Ver elEjemplo de MetroCluster .	Derivado si se trata de una SVM `managementLIF` se especifica
`useCHAP`	Utilice CHAP para autenticar iSCSI para controladores SAN ONTAP [Booleano]. Empezar a `true` para que Trident configure y utilice CHAP bidireccional como autenticación predeterminada para el SVM proporcionado en el backend. Referirse a "Prepárese para configurar el backend con los controladores SAN de ONTAP." Para más detalles. **No compatible con FCP ni NVMe/TCP.**	`false`
`chapInitiatorSecret`	Secreto del iniciador de CHAP. Requerido si `useCHAP=true`	""
`labels`	Conjunto de etiquetas arbitrarias con formato JSON para aplicar a los volúmenes	""
`chapTargetInitiatorSecret`	Secreto del iniciador del objetivo CHAP. Requerido si `useCHAP=true`	""
`chapUsername`	Nombre de usuario entrante. Requerido si `useCHAP=true`	""
`chapTargetUsername`	Nombre de usuario objetivo. Requerido si `useCHAP=true`	""
`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.	""

Parámetro	Descripción	Por defecto
`username`	Nombre de usuario necesario para comunicarse con el clúster ONTAP . 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 necesaria para comunicarse con el clúster ONTAP . 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".	""
`svm`	máquina virtual de almacenamiento a utilizar	Derivado si se trata de una SVM `managementLIF` se especifica
`storagePrefix`	Prefijo utilizado al aprovisionar nuevos volúmenes en la SVM. No se puede modificar posteriormente. Para actualizar este parámetro, deberá crear un nuevo backend.	`trident`
`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 . 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. **No especificar para sistemas ASA r2**.	""

Parámetro	Descripción	Por defecto
`limitAggregateUsage`	Fallará el aprovisionamiento si el uso supera este porcentaje. Si utiliza un backend de Amazon FSx for NetApp ONTAP , no especifique `limitAggregateUsage` . El proporcionado `fsxadmin` y `vsadmin` No contienen los permisos necesarios para recuperar el uso agregado y limitarlo mediante Trident. **No especificar para sistemas ASA r2**.	" (no se aplica 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 las LUN.	" (no se aplica por defecto)
`lunsPerFlexvol`	Número máximo de LUN por Flexvol, debe estar en el rango [50, 200]	`100`
`debugTraceFlags`	Indicadores de depuración para usar al solucionar problemas. Ejemplo: {"api":false, "method":true} No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	`null`

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). `useREST`está totalmente cualificado para NVMe/TCP. NVMe solo es compatible con las API REST de ONTAP y no con ONTAPI (ZAPI). **Si se especifica, siempre se establecerá en `true` para sistemas ASA r2**.	`true`para ONTAP 9.15.1 o posterior, de lo contrario `false`.
`sanType`	Utilice para seleccionar `iscsi` para iSCSI, `nvme` para NVMe/TCP o `fcp` para SCSI sobre Fibre Channel (FC).	`iscsi`si está en blanco

Parámetro	Descripción	Por defecto
`formatOptions`	Usar `formatOptions` para especificar los argumentos de la línea de comandos para el `mkfs` comando que se aplicará siempre que se formatee un volumen. Esto le permite formatear el volumen según sus preferencias. Asegúrese de especificar las opciones de formato de forma similar a las opciones del comando mkfs, excluyendo la ruta del dispositivo. Ejemplo: "-E no descartar" **Compatible con `ontap-san` y `ontap-san-economy` controladores con protocolo iSCSI. Además, se admite para sistemas ASA r2 cuando se utilizan los protocolos iSCSI y NVMe/TCP.**	
`limitVolumePoolSize`	Tamaño máximo de FlexVol solicitable al usar LUN en el backend ontap-san-economy.	" (no se aplica por defecto)
`denyNewVolumePools`	Restringe `ontap-san-economy` Los sistemas backend crean nuevos volúmenes FlexVol para contener sus LUN. Solo se utilizan Flexvols preexistentes para el aprovisionamiento de nuevos PV.	

Recomendaciones para el uso de formatOptions

Trident recomienda la siguiente opción para agilizar el proceso de formateo:

-E no descartar:

- Conservar, no intentar descartar bloques en el momento de mkfs (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento disperso/de aprovisionamiento ligero). Esto reemplaza la opción obsoleta "-K" y es aplicable a todos los sistemas de archivos (xfs, ext3 y ext4).

Autenticar Trident en un SVM backend mediante credenciales de Active Directory

Puede configurar Trident para autenticarse en un SVM de backend usando credenciales de Active Directory (AD). Antes de que una cuenta de AD pueda acceder a la SVM, debe configurar el acceso del controlador de dominio de AD al clúster o SVM. Para la administración de un clúster con una cuenta de AD, debe crear un túnel de dominio. Referirse a "Configurar el acceso al controlador de dominio de Active Directory en ONTAP" Para más detalles.

pasos

1. Configurar los ajustes del Sistema de nombres de dominio (DNS) para un SVM de backend:

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

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

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

3. Utilice 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 , configure el `username` y `password` parámetros al nombre de usuario o grupo de AD y la contraseña, respectivamente.

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 LUN	"verdadero" **Si se especifica, establecer en `true` para sistemas ASA r2**.
`spaceReserve`	Modo de reserva de espacio: "ninguno" (delgado) o "volumen" (grueso). **Empezar a `none` para sistemas ASA r2**.	"ninguno"
`snapshotPolicy`	Política de instantáneas a utilizar. **Empezar a `none` para sistemas ASA r2**.	"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. 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.	""
`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.	""
`snapshotReserve`	Porcentaje de volumen reservado para instantáneas. **No especificar para sistemas ASA r2**.	"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" **Si se especifica, establecer en `true` para sistemas ASA r2**.

Parámetro	Descripción	Por defecto
`luksEncryption`	Habilitar el cifrado LUKS. Referirse a"Utilice la configuración de clave unificada de Linux (LUKS)." .	" **Configurado a `false` para sistemas ASA r2**.
`tieringPolicy`	Política de jerarquización para usar "ninguna" **No especificar para sistemas ASA r2** .	
`nameTemplate`	Plantilla para crear nombres de volumen personalizados.	""

Ejemplos de aprovisionamiento por volumen

Aquí tenéis 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 utilizando el `ontap-san` El controlador Trident agrega un 10 por ciento de capacidad adicional al FlexVol para dar cabida a los metadatos de LUN. La LUN se aprovisionará con el tamaño exacto que el usuario solicite en el PVC. Trident añade un 10 por ciento al FlexVol (se muestra como Tamaño disponible en ONTAP). Los usuarios ahora obtendrán la cantidad de capacidad utilizable que solicitaron. Este cambio también evita que las LUN se conviertan en de solo lectura a menos que se utilice todo el espacio disponible. Esto no se aplica a ontap-san-economy.

Para 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 por ciento adicional que Trident agrega al FlexVol para acomodar los metadatos del LUN. Para `snapshotReserve` = 5%, y solicitud de PVC = 5 GiB, el tamaño total del volumen es 5,79 GiB y el tamaño disponible es 5,5 GiB. El `volume show` El comando debería mostrar resultados similares a este ejemplo:

Actualmente, la única forma de utilizar el nuevo cálculo para un volumen existente es redimensionándolo.

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 utiliza Amazon FSx en NetApp ONTAP con Trident, NetApp recomienda que especifique nombres DNS para las LIF en lugar de direcciones IP.

Ejemplo de SAN de ONTAP

Esta es una configuración básica que utiliza `ontap-san` conductor.

```
---
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

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 `svm` parámetros. Por ejemplo:

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

Ejemplo económico de ONTAP SAN

```
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 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
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 bidireccionales

Estos ejemplos crean un backend con `useCHAP` empezar a `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 economía ONTAP SAN 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

Debe tener una SVM configurada con NVMe en su backend 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)

Debe tener un SVM configurado con FC en su backend 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 plantilla de nombre

```
---
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}}"
```

Ejemplo de opciones de formato 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, 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 se configuran en el FlexVol volume. 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 SAN de ONTAP

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

Ejemplo económico de ONTAP SAN

```
---
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"
```

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 grupo virtual en el `ontap-san` backend. Esta es la única piscina 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 grupo virtual en `ontap-san` 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 tercer grupo virtual en `ontap-san-economy` 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 segundo grupo virtual en `ontap-san` 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 `ontap-san` backend y el cuarto grupo virtual en el `ontap-san-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"
```

- El `my-test-app-sc` StorageClass se asignará a `testAPP` piscina virtual en la `ontap-san` conductor con `sanType: nvme` . Esta es la única oferta de piscina `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 garantiza que se cumplan los requisitos de almacenamiento.