Controladores para SAN de ONTAP

Trident

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/trident-2410/trident-use/ontap-san.html on September 26, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Controladores para SAN de ONTAP . . . 1
- Información general del controlador de SAN de ONTAP . . . 1
  - Información sobre el controlador de SAN de ONTAP . . . 1
  - Permisos de usuario . . . 2
  - Consideraciones adicionales para NVMe/TCP . . . 2
- Prepárese para configurar el back-end con los controladores SAN de ONTAP . . . 3
  - Requisitos . . . 3
  - Autentique el backend de ONTAP . . . 3
  - Autentica conexiones con CHAP bidireccional . . . 8
- Opciones y ejemplos de configuración SAN de ONTAP . . . 10
  - Opciones de configuración del back-end . . . 10
  - Opciones de configuración de back-end para el aprovisionamiento de volúmenes . . . 14
  - Ejemplos de configuración mínima . . . 17
  - Ejemplos de back-ends con pools virtuales . . . 21
  - Asigne los back-ends a StorageClass . . . 25

Controladores para SAN de ONTAP

Información general del controlador de SAN de ONTAP

Obtenga más información sobre la configuración de un entorno de administración de ONTAP con controladores SAN de ONTAP y Cloud Volumes ONTAP.

Información sobre el controlador de SAN de ONTAP

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

Controlador	Protocolo	VolumeMode	Modos de acceso compatibles	Sistemas de archivos compatibles
`ontap-san`	SCSI iSCSI sobre FC (versión preliminar técnica en Trident 24,10)	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
`ontap-san`	SCSI iSCSI sobre FC (versión preliminar técnica en Trident 24,10)	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3`, , `ext4`
`ontap-san`	NVMe/TCP Consulte Consideraciones adicionales para NVMe/TCP.	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
`ontap-san`	NVMe/TCP Consulte Consideraciones adicionales para NVMe/TCP.	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3`, , `ext4`

Controlador	Protocolo	VolumeMode	Modos de acceso compatibles	Sistemas de archivos compatibles
`ontap-san-economy`	ISCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
`ontap-san-economy`	ISCSI	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	`xfs`, `ext3`, , `ext4`

- Utilice `ontap-san-economy` solo si se espera que el recuento de uso de volúmenes persistentes sea superior a "Límites de volumen ONTAP compatibles".
- Utilice `ontap-nas-economy` solo si se espera que el recuento de uso de volúmenes persistentes sea superior a "Límites de volumen ONTAP compatibles" y `ontap-san-economy` no se puede utilizar el controlador.
- No utilice `ontap-nas-economy` si anticipa la necesidad de protección de datos, recuperación ante desastres o movilidad.

Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el usuario del clúster o `vsadmin` un usuario de SVM, `admin` o bien como usuario con un nombre distinto que tenga el mismo rol. Para puestas en marcha de Amazon FSx para NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, utilizando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o como un usuario con un nombre distinto que tenga el mismo rol. `fsxadmin`El usuario es un sustituto limitado para el usuario administrador del clúster.

Si se usa `limitAggregateUsage` el parámetro, se requieren permisos de administrador del clúster. Cuando se usa Amazon FSx para NetApp ONTAP con Trident, el `limitAggregateUsage` parámetro no funcionará con `vsadmin` las cuentas de usuario y. `fsxadmin` La operación de configuración generará un error si se especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que puede utilizar un controlador Trident, no lo recomendamos. La mayoría de las nuevas versiones de Trident denominan API adicionales que se tendrían que tener en cuenta, por lo que las actualizaciones son complejas y propensas a errores.

Consideraciones adicionales para NVMe/TCP

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

- IPv6
- Snapshots y clones de volúmenes NVMe
- Cambiar el tamaño de un volumen NVMe

- Se importa un volumen NVMe que se creó fuera de Trident para que su ciclo de vida se pueda gestionar mediante Trident
- Multivía nativa de NVMe
- Cierre correcto o sin complicaciones de los K8s nodos (24,06)

Trident no admite:

- DH-HMAC-CHAP que es compatible con NVMe de forma nativa
- Rutas múltiples del asignador de dispositivos (DM)
- Cifrado LUKS

Prepárese para configurar el back-end con los controladores SAN de ONTAP

Conozca los requisitos y las opciones de autenticación para configurar un back-end de ONTAP con controladores SAN de ONTAP.

Requisitos

Para todos los back-ends de ONTAP, Trident requiere al menos un agregado asignado a la SVM.

Recuerde que también puede ejecutar más de un controlador y crear clases de almacenamiento que señalen a uno o a otro. Por ejemplo, puede configurar una `san-dev` clase que utilice `ontap-san` el controlador y una clase que utilice el `ontap-san-economy` controlador `san-default`.

Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulte "Prepare el nodo de trabajo" para obtener más información.

Autentique 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 ONTAP con los permisos requeridos. 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 certificado: Trident también puede comunicarse con un clúster de ONTAP mediante un certificado instalado en el back-end. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puede actualizar los back-ends existentes para moverse entre métodos basados en credenciales y 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 back-end.

> Si intenta proporcionar **tanto credenciales como certificados**, la creación de backend fallará y se producirá un error en el que se haya proporcionado más de un método de autenticación en el archivo de configuración.

Habilite la autenticación basada en credenciales

Trident requiere que las credenciales se comuniquen con un administrador de SVM o con el ámbito del clúster para que se comunique con el back-end de ONTAP. Se recomienda hacer uso de roles estándar, predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones que podrán utilizarse en futuras versiones de Trident. Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Una definición de backend de ejemplo tendrá este aspecto:

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 de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. Una vez creado el back-end, 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 conocimiento de las credenciales. Por tanto, es una operación de solo administración que deberá realizar el administrador de Kubernetes o almacenamiento.

Habilite la autenticación basada en certificados

Los back-ends nuevos y existentes pueden utilizar un certificado y comunicarse con el back-end de ONTAP. Se necesitan tres parámetros en la definición de 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 se utiliza una CA

de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico implica los pasos siguientes.

Pasos

1. Genere una clave y un certificado de cliente. Al generar, establezca el nombre común (CN) en el usuario de ONTAP para autenticarse como.

```
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. Añada un certificado de CA de confianza al clúster ONTAP. Es posible que ya sea gestionado por el administrador de almacenamiento. Ignore 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 de cliente (desde el 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 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. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión 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 certificados, claves y certificados 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. Cree un backend utilizando los valores obtenidos del paso anterior.

```
cat cert-backend.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaallllluuuueeee",
"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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Actualice los métodos de autenticación o gire las credenciales

Puede actualizar un back-end existente para utilizar un método de autenticación diferente o para rotar sus credenciales. Esto funciona de las dos maneras: Los back-ends que utilizan nombre de usuario/contraseña se pueden actualizar para usar certificados. Los back-ends que utilizan certificados pueden actualizarse a 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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

> Cuando gira contraseñas, el administrador de almacenamiento debe actualizar primero la contraseña del usuario en ONTAP. A esto le sigue una actualización de back-end. Al rotar certificados, se pueden agregar varios certificados al usuario. A continuación, el back-end se actualiza para usar el nuevo certificado, siguiendo el cual se puede eliminar el certificado antiguo del clúster de ONTAP.

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que Trident puede comunicarse con el back-end de ONTAP y manejar operaciones de volumen futuras.

Crear rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privileges mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "Generador de roles personalizados de Trident"para obtener más información sobre la creación de roles personalizados de Trident.

Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

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

2. Cree 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. Asignar el rol al usuario:

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

Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado**:
   a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

      (O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > `required SVM`> Settings > Users and Roles**.

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

Consulte las siguientes páginas si quiere más información:

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

Autentica conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para `ontap-san` los controladores y. `ontap-san-economy` Esto requiere la activación de `useCHAP` la opción en la definición de 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 del archivo back-end. 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` parámetro es una opción booleana que puede configurarse una sola vez. De forma predeterminada, se establece en FALSE. Después de configurarlo en true, no puede establecerlo en false.

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

Cómo funciona

Al configurarse `useCHAP` en true, el administrador de almacenamiento le ordena a Trident que configure CHAP en el back-end de almacenamiento. Esto incluye lo siguiente:

- Configuración de CHAP en la SVM:
  - Si el tipo de seguridad de iniciador predeterminado de la SVM es none (establecido de forma predeterminada) **y** no hay LUN preexistentes ya presentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en `CHAP` y continuará configurando el iniciador CHAP y el nombre de usuario y los secretos de destino.
  - Si la SVM contiene LUN, Trident no habilitará CHAP en la SVM. De este modo se garantiza que no se restrinja el acceso a las LUN que ya están presentes en la SVM.
- Configurar el iniciador de CHAP, el nombre de usuario y los secretos de destino; estas opciones deben especificarse en la configuración del back-end (como se muestra más arriba).

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

Rotar las credenciales y actualizar los back-ends

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

Al actualizar los secretos CHAP para un backend, debe utilizar `tridentctl` para actualizar el backend. No actualice las credenciales en el clúster de almacenamiento a través de la interfaz de usuario de CLI/ONTAP, ya que Trident no podrá recoger 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 las credenciales se actualizan mediante Trident en la SVM. Las nuevas conexiones utilizan las credenciales actualizadas y las conexiones existentes siguen activas. Al desconectar y volver a conectar los VP antiguos, se utilizarán las credenciales actualizadas.

Opciones y ejemplos de configuración SAN de ONTAP

Aprenda a crear y utilizar controladores SAN de ONTAP con su instalación de Trident. Esta sección proporciona ejemplos de configuración de backend y detalles para la asignación de back-ends a StorageClasses.

Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
`version`		Siempre 1
`storageDriverName`	Nombre del controlador de almacenamiento	`ontap-nas`, , , , `ontap-nas-economy` `ontap-nas-flexgroup` `ontap-san` , `ontap-san-economy`
`backendName`	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos
`managementLIF`	La dirección IP de un clúster o una LIF de gestión de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` como . Para una conmutación de sitios MetroCluster fluida, consulte [mcc-best].	“10.0.0.1”, “[2001:1234:abcd::fefe]”
`dataLIF`	Dirección IP de LIF de protocolo. Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` como . **No especifique para iSCSI.** Trident utiliza "Asignación de LUN selectiva de ONTAP" para descubrir las LIF iSCSI necesarias para establecer una sesión de rutas múltiples. Se genera una advertencia si `dataLIF` se define explícitamente. **Omitir para MetroCluster.** Consulte la [mcc-best].	Derivado del SVM
`svm`	Máquina virtual de almacenamiento para usar **Omitir para MetroCluster.** Consulte la [mcc-best].	Derivada si se especifica una SVM `managementLIF`
`useCHAP`	Use CHAP para autenticar iSCSI para los controladores SAN de ONTAP [Boolean]. Establezca como `true` para que Trident configure y utilice CHAP bidireccional como la autenticación predeterminada para la SVM especificada en el back-end. Consulte "Prepárese para configurar el back-end con los controladores SAN de ONTAP" para obtener más información.	`false`
`chapInitiatorSecret`	Secreto CHAP del iniciador. Obligatorio si `useCHAP=true`	""
`labels`	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
`chapTargetInitiatorSecret`	Secreto CHAP del iniciador de destino. Obligatorio si `useCHAP=true`	""
`chapUsername`	Nombre de usuario entrante. Obligatorio si `useCHAP=true`	""

Parámetro	Descripción	Predeterminado
`chapTargetUsername`	Nombre de usuario de destino. Obligatorio si `useCHAP=true`	""
`clientCertificate`	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
`clientPrivateKey`	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
`trustedCACertificate`	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
`username`	El nombre de usuario necesario para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
`password`	La contraseña necesaria para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
`svm`	Máquina virtual de almacenamiento que usar	Derivada si se especifica una SVM `managementLIF`
`storagePrefix`	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede modificar más adelante. Para actualizar este parámetro, deberá crear un nuevo backend.	`trident`
`aggregate`	Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el `ontap-nas-flexgroup` controlador, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles puede usarse para aprovisionar un volumen FlexGroup. Cuando el agregado se actualiza en SVM, se actualiza automáticamente en Trident sondeando SVM sin tener que reiniciar la controladora Trident. Cuando se haya configurado un agregado específico en Trident para aprovisionar volúmenes, si se cambia el nombre de este agregado o se saca de la SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar el agregado por uno presente en la SVM o quitarlo por completo para que el back-end vuelva a estar en línea.	""

Parámetro	Descripción	Predeterminado
`limitAggregateUsage`	Error al aprovisionar si el uso supera este porcentaje. Si estás usando un backend de Amazon FSx for NetApp ONTAP, no especifiques `limitAggregateUsage`. El proporcionado `fsxadmin` y `vsadmin` no contiene los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Trident.	"" (no se aplica de forma predeterminada)
`limitVolumeSize`	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. Además, restringe el tamaño máximo de los volúmenes que gestiona para las LUN.	"" (no se aplica de forma predeterminada)
`lunsPerFlexvol`	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	`100`
`debugTraceFlags`	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {“api”:false, “method”:true} no lo utilice a menos que esté solucionando problemas y requiera un volcado de log detallado.	`null`
`useREST`	Parámetro booleano para usar las API DE REST de ONTAP. `useREST` Cuando se define en `true`, Trident utiliza las API REST DE ONTAP para comunicarse con el backend; cuando se define en `false`, Trident utiliza llamadas de ONTAP ZAPI para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a `ontap` la aplicación. 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 posterior, `useREST` se establece en `true` de forma predeterminada; cambie `useREST` a `false` Usar llamadas ZAPI de ONTAP. `useREST` Está totalmente cualificado para NVMe/TCP.	`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 over Fibre Channel (FC). **'fcp' (SCSI sobre FC) es una función de previsualización técnica en la versión Trident 24,10.**	`iscsi` si está en blanco

Parámetro	Descripción	Predeterminado
`formatOptions`	Puede `formatOptions` usarse para especificar argumentos de línea de comandos para `mkfs` el comando, que se aplicará cada vez que se formatee un volumen. Esto permite formatear el volumen según sus preferencias. Asegúrese de especificar las opciones formatOptions similares a las de los comandos mkfs, excluyendo la ruta del dispositivo. Ejemplo: «-E nodiscard» **Compatible `ontap-san` `ontap-san-economy` solo para conductores y.**	
`limitVolumePoolSize`	Tamaño máximo de FlexVol solicitable al usar LUN en back-end económico de ONTAP-san.	"" (no se aplica de forma predeterminada)
`denyNewVolumePools`	Restringe `ontap-san-economy` los back-ends para que no creen nuevos volúmenes de FlexVol para contener sus LUN. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	

Recomendaciones para utilizar formatOptions

Trident recomienda la siguiente opción para acelerar el proceso de formato:

-E nodiscard:

- Keep, no intente descartar bloques en mkfs time (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento ligero/Thin-Provisioning). Esto reemplaza la opción anticuada “-K” y es aplicable a todos los sistemas de archivos (xfs, ext3 y ext4).

Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado mediante estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
`spaceAllocation`	Asignación de espacio para las LUN	verdadero
`spaceReserve`	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	ninguno
`snapshotPolicy`	Política de Snapshot que se debe usar	ninguno

Parámetro	Descripción	Predeterminado
`qosPolicy`	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento. Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.	""
`adaptiveQosPolicy`	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
`snapshotReserve`	Porcentaje de volumen reservado para las Snapshot	«0» si `snapshotPolicy` no es «ninguno», de lo contrario «
`splitOnClone`	Divida un clon de su elemento principal al crearlo	"falso"
`encryption`	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son `false`. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE. Para obtener más información, consulte: "Cómo funciona Trident con NVE y NAE".	"falso"
`luksEncryption`	Active el cifrado LUKS. Consulte "Usar la configuración de clave unificada de Linux (LUKS)". El cifrado LUKS no es compatible con NVMe/TCP.	""
`securityStyle`	Estilo de seguridad para nuevos volúmenes	`unix`
`tieringPolicy`	Política de organización en niveles para utilizar ninguna	«Solo Snapshot» para la configuración SVM-DR anterior a ONTAP 9,5
`nameTemplate`	Plantilla para crear nombres de volúmenes personalizados.	""

Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los 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 con `ontap-san` el controlador, Trident añade un 10 % de capacidad adicional al FlexVol para acomodar los metadatos del LUN. La LUN se aprovisionará con el tamaño exacto que el usuario solicite en la RVP. Trident agrega un 10 % a FlexVol (se muestra como tamaño disponible en ONTAP). Los usuarios obtienen ahora la cantidad de capacidad utilizable que soliciten. Este cambio también impide que las LUN se conviertan en de solo lectura a menos que se utilice completamente el espacio disponible. Esto no se aplica a ontap-san-economy.

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

```
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
          _pvc_89f1c156_3801_4de4_9f9d_034d54c395f4
                                   online     RW         10GB     5.00GB    0%
          _pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d
                                   online     RW       5.79GB     5.50GB    0%
          _pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba
                                   online     RW          1GB    511.8MB    0%
3 entries were displayed.
```

En la actualidad, el cambio de tamaño es la única manera de utilizar el nuevo cálculo para un volumen existente.

Ejemplos de configuración mínima

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.

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

Ejemplo de SAN ONTAP

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

```
---
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 economía de SAN ONTAP

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

1. ejemplo

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

Para lograr una conmutación de sitios y una conmutación de estado sin problemas, especifique la SVM con `managementLIF` y omita `dataLIF` los parámetros y. `svm` Por ejemplo:

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

Ejemplo de autenticación basada en certificados

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

```
---
version: 1
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` el valor definido en `true`.

Ejemplo de CHAP de SAN de ONTAP

```
---
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 CHAP de economía de SAN ONTAP

```
---
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 el back-end de ONTAP. Esta es una configuración de back-end básica 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 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}}_{{.volume.R
equestName}}"
},
"labels": {"cluster": "ClusterA", "PVC":
"{{.volume.Namespace}}_{{.volume.RequestName}}"}
```

Ejemplo de formatOptions para el controlador <code> ONTAP-san-economy</code>

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

Ejemplos de back-ends con pools virtuales

En estos archivos de definición de backend de ejemplo, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` at none, `spaceAllocation` at false y `encryption` at false. Los pools virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo de comentarios. Los comentarios se establecen en la FlexVol. Trident copia todas las etiquetas presentes en un pool virtual en el 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` valores , `spaceAllocation` y `encryption`, y algunos pools sustituyen a los valores predeterminados.

Ejemplo de SAN 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 de economía de SAN ONTAP

```
---
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'
```

Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass hacen referencia a la Ejemplos de back-ends con pools virtuales. En este `parameters.selector` campo, cada StorageClass llama la atención sobre los pools virtuales que se pueden usar para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- `protection-gold`StorageClass se asignará al primer pool virtual del `ontap-san` backend. Este es el único pool que ofrece protección de nivel Gold.

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

- `protection-not-gold`StorageClass se asignará al segundo y tercer pool virtual en `ontap-san` el backend. Estos son los únicos pools que ofrecen un nivel de protección distinto del oro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- `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 aplicación 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"
```

- `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"
```

- `creditpoints-5k`StorageClass se asignará al tercer pool virtual en backend y al cuarto pool virtual en `ontap-san` el `ontap-san-economy` backend. Estas son las únicas ofertas de grupo 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"
```

- `my-test-app-sc`StorageClass se asignará al `testAPP` pool virtual del `ontap-san` controlador 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 pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.