Controladores para NAS de ONTAP

Trident

NetApp
January 14, 2026

Tabla de contenidos

Controladores para NAS de ONTAP

Información general del controlador de NAS de ONTAP

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

Información sobre el controlador de NAS de ONTAP

Trident proporciona los siguientes controladores de almacenamiento NAS 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-nas`	BLOQUE DE MENSAJES DEL SERVIDOR NFS	Sistema de archivos	RWO, ROX, RWX, RWOP	« », `nfs`, `smb`
`ontap-nas-economy`	BLOQUE DE MENSAJES DEL SERVIDOR NFS	Sistema de archivos	RWO, ROX, RWX, RWOP	« », `nfs`, `smb`
`ontap-nas-flexgroup`	BLOQUE DE MENSAJES DEL SERVIDOR NFS	Sistema de archivos	RWO, ROX, RWX, RWOP	« », `nfs`, `smb`

- 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.

Prepárese para configurar un back-end con controladores NAS de ONTAP

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

Requisitos

- Para todos los back-ends de ONTAP, Trident requiere al menos un agregado asignado a la SVM.
- Puede ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, puede configurar una clase Gold que utilice el `ontap-nas` controlador y una clase Bronze que utilice la clase `ontap-nas-economy` One.
- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulte "aquí"si desea obtener más información.
- Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte Prepárese para aprovisionar los volúmenes de SMB para obtener más información.

Autentique el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP.

- Basado en Credenciales: Este modo requiere permisos suficientes para el backend de ONTAP. Se recomienda utilizar una cuenta asociada a un rol de inicio de sesión de seguridad predefinido, `admin` como o `vsadmin` para garantizar la máxima compatibilidad con las versiones de ONTAP.
- Basado en certificado: Este modo requiere un certificado instalado en el back-end para que Trident se comunique con un clúster de ONTAP. 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

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "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/mejora 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=vsadmin"
```

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 vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

5. 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. Debe asegurarse de que el LIF tenga su política de servicio establecida en `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. 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-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

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 update backend`.

```
cat cert-backend-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

> 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"

Gestione las políticas de exportación de NFS

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

Trident proporciona dos opciones al trabajar con políticas de exportación:

- Trident puede gestionar de manera dinámica la política de exportación; en este modo de funcionamiento, el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Trident agrega IP de nodo aplicables que se encuentran en estos rangos a la política de exportación de forma automática en el momento de la publicación. Como alternativa, cuando no se especifica ningún CIDR, todas las IP de unidifusión de ámbito global que se encuentran en el nodo en el que se publica el volumen se agregarán a la política de exportación.
- Los administradores de almacenamiento pueden crear una normativa de exportación y añadir reglas manualmente. Trident utiliza la política de exportación predeterminada a menos que se especifique otro nombre de política de exportación en la configuración.

Gestione de forma dinámica políticas de exportación

Trident proporciona la capacidad de gestionar dinámicamente políticas de exportación para back-ends de ONTAP. De este modo, el administrador de almacenamiento puede especificar un espacio de direcciones permitido para las IP de nodos de trabajo, en lugar de definir reglas explícitas de forma manual. Simplifica en gran medida la gestión de políticas de exportación; las modificaciones de la política de exportación ya no requieren intervención manual en el clúster de almacenamiento. Además, esto ayuda a restringir el acceso al clúster de almacenamiento solo a los nodos de trabajador que se montan volúmenes y que tienen IP en el rango especificado, lo que permite una gestión automatizada y precisa.

> No utilice la traducción de direcciones de red (NAT) cuando utilice políticas de exportación dinámicas. Con NAT, el controlador de almacenamiento ve la dirección NAT de frontend y no la dirección de host IP real, por lo que el acceso se denegará cuando no se encuentre ninguna coincidencia en las reglas de exportación.

> En Trident 24,10, `ontap-nas` el controlador de almacenamiento seguirá funcionando como en las versiones anteriores; no se ha realizado ningún cambio en el controlador ONTAP-nas. Solo `ontap-nas-economy` el controlador de almacenamiento tendrá control de acceso granular basado en el volumen en Trident 24,10.

Ejemplo

Hay dos opciones de configuración que deben utilizarse. He aquí un ejemplo de definición de backend:

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
- 192.168.0.0/24
autoExportPolicy: true
```

> Al usar esta función, debe asegurarse de que la unión raíz de la SVM tenga una política de exportación creada previamente con una regla de exportación que permite el bloque CIDR de nodo (como la política de exportación predeterminada). Siga siempre las prácticas recomendadas por NetApp para dedicar una SVM para Trident.

A continuación se ofrece una explicación del funcionamiento de esta función utilizando el ejemplo anterior:

- `autoExportPolicy` se establece en `true`. Esto indica que Trident crea una política de exportación para cada volumen aprovisionado con este back-end para `svm1` la SVM y administra la adición y eliminación de reglas mediante `autoexportCIDRs` bloques de direcciones. Hasta que un volumen se conecta a un nodo, el volumen usa una política de exportación vacía sin reglas para evitar el acceso no deseado a ese volumen. Cuando se publica un volumen en un nodo, Trident crea una política de exportación con el mismo nombre que el qtree subyacente que contiene la IP de nodo en el bloque CIDR especificado. Estas IP también se agregarán a la política de exportación utilizada por la FlexVol principal.
  - Por ejemplo:
    - UUID de backend 403b5326-8482-40dB-96d0-d83fb3f4daec
    - `autoExportPolicy` establezca en `true`
    - prefijo de almacenamiento `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - el qtree denominado Trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c crea una política de exportación para la FlexVol llamada `trident-403b5326-8482-40db96d0-d83fb3f4daec`, una política de exportación para el qtree llamado `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`y una política de exportación vacía denominada `trident_empty` en la SVM. Las reglas de la política de exportación de FlexVol serán un superconjunto de reglas contenidas en las políticas de exportación de qtree. La política de exportación vacía será reutilizada por cualquier volumen que no esté asociado.
- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y se establece de forma predeterminada en ["0.0.0.0/0", ":/0"]. Si no se define, Trident agrega todas las direcciones unicast de ámbito global que se encuentran en los nodos de trabajo con publicaciones.

En este ejemplo, `192.168.0.0/24` se proporciona el espacio de la dirección. Esto indica que las IP de nodo de Kubernetes que se encuentran dentro de este rango de direcciones con publicaciones se agregarán a la política de exportación que crea Trident. Cuando Trident registra un nodo en el que se ejecuta, recupera las

direcciones IP del nodo y las comprueba con respecto a los bloques de direcciones proporcionados en `autoExportCIDRs`. En el momento de la publicación, después de filtrar las IP, Trident crea las reglas de política de exportación para las IP del cliente para el nodo en el que está publicando.

Puede actualizar `autoExportPolicy` y `autoExportCIDRs` para los back-ends después de crearlos. Puede añadir CIDR nuevos para un back-end que se gestiona o elimina automáticamente CIDR existentes. Tenga cuidado al eliminar CIDR para asegurarse de que las conexiones existentes no se hayan caído. También puede optar por desactivar `autoExportPolicy` un backend y recurrir a una política de exportación creada manualmente. Esto requerirá definir el `exportPolicy` parámetro en la configuración de backend.

Después de que Trident cree o actualice un backend, puede comprobar el backend utilizando `tridentctl` o el CRD correspondiente `tridentbackend`:

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileSystemType: ext4
```

Cuando se elimina un nodo, Trident comprueba todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar esta IP de nodo de las políticas de exportación de los back-ends gestionados, Trident evita los montajes no autorizados, a menos que un nuevo nodo del clúster reutilice esta IP.

Para los back-ends existentes anteriormente, al actualizar el backend con `tridentctl update backend` se garantiza que Trident administre las políticas de exportación automáticamente. Esto crea dos nuevas políticas de exportación llamadas después del UUID del back-end y el nombre de qtree cuando son necesarias. Los volúmenes presentes en el back-end utilizarán las políticas de exportación recién creadas después de desmontarlas y montarlas de nuevo.

Si se elimina un back-end con políticas de exportación gestionadas automáticamente, se eliminará la política de exportación creada de forma dinámica. Si se vuelve a crear el back-end, se trata como un nuevo back-end y dará lugar a la creación de una nueva política de exportación.

Si se actualiza la dirección IP de un nodo activo, debe reiniciar el pod de Trident en el nodo. A continuación, Trident actualizará la política de exportación de los back-ends que gestiona para reflejar este cambio de IP.

Prepárese para aprovisionar los volúmenes de SMB

Con un poco de preparación adicional, puede aprovisionar volúmenes SMB por medio `ontap-nas` de controladores.

Debe configurar tanto los protocolos NFS como SMB/CIFS en la SVM para crear `ontap-nas-economy` un volumen SMB para ONTAP en las instalaciones. Si no se configura ninguno de estos protocolos, se producirá un error en la creación del volumen de SMB.

`autoExportPolicy` No es compatible con los volúmenes de SMB.

Antes de empezar

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

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

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

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

Pasos

1. Para la ONTAP en las instalaciones, puede crear un recurso compartido de SMB, o bien Trident puede crearlo para usted.

   Los recursos compartidos de SMB se requieren para Amazon FSx para ONTAP.

   Puede crear los recursos compartidos de administrador de SMB de dos maneras mediante el "Consola de administración de Microsoft"complemento Carpetas compartidas o mediante la CLI de ONTAP. Para crear los recursos compartidos de SMB mediante la CLI de ONTAP:

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

      El `vserver cifs share create` comando comprueba la ruta especificada en la opción -path durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

b. Cree un recurso compartido de SMB asociado con la SVM especificada:

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

c. Compruebe que se ha creado el recurso compartido:

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

Consulte "Cree un recurso compartido de SMB"para obtener información detallada.

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

Parámetro	Descripción	Ejemplo
`smbShare`	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	`smb-share`
`nasType`	**Debe establecerse en `smb`.** Si es nulo, el valor por defecto es `nfs`.	`smb`
`securityStyle`	Estilo de seguridad para nuevos volúmenes. **Debe establecerse en `ntfs` o `mixed` para volúmenes SMB.**	`ntfs` O `mixed` para volúmenes de SMB
`unixPermissions`	Modo para volúmenes nuevos. **Se debe dejar vacío para volúmenes SMB.**	""

Opciones y ejemplos de configuración NAS de ONTAP

Aprenda a crear y utilizar controladores NAS 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`	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 Ejemplo de MetroCluster.	“10.0.0.1”, “[2001:1234:abcd::fefe]”
`dataLIF`	Dirección IP de LIF de protocolo. Recomendamos especificar `dataLIF`. Si no se encuentra, Trident recupera los LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos. Se puede cambiar después del ajuste inicial. Consulte . 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 . **Omitir para MetroCluster.** Consulte la Ejemplo de MetroCluster.	Dirección especificada o derivada de la SVM, si no se especifica (no recomendada)
`svm`	Máquina virtual de almacenamiento para usar **Omitir para MetroCluster.** Consulte la Ejemplo de MetroCluster.	Derivada si se especifica una SVM `managementLIF`
`autoExportPolicy`	Habilite la creación y actualización automática de la política de exportación [Boolean]. Mediante las `autoExportPolicy` opciones y `autoExportCIDRs`, Trident puede gestionar automáticamente las políticas de exportación.	falso
`autoExportCIDRs`	Lista de CIDRs para filtrar las IP del nodo de Kubernetes contra cuando `autoExportPolicy` se habilita. Mediante las `autoExportPolicy` opciones y `autoExportCIDRs`, Trident puede gestionar automáticamente las políticas de exportación.	[«0,0.0,0/0», «:/0»]

Parámetro	Descripción	Predeterminado
`labels`	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
`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`	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
`password`	Contraseña para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
`storagePrefix`	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede actualizar después de configurarlo Al utilizar ONTAP-nas-economy y un prefijo de almacenamiento con 24 caracteres o más, los qtrees no tendrán el prefijo de almacenamiento incrustado, pero estarán en el nombre del volumen.	«trident»

Parámetro	Descripción	Predeterminado
`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.	""
`limitAggregateUsage`	Error al aprovisionar si el uso supera este porcentaje. **No se aplica a Amazon FSX para ONTAP**	"" (no se aplica de forma predeterminada)
Lista de Agregados de Flexgroup	Lista de agregados para el aprovisionamiento (opcional; si se ha definido, debe asignarse a la SVM). Todos los agregados asignados a la SVM se usan para aprovisionar un volumen FlexGroup. Compatible con el controlador de almacenamiento **ONTAP-nas-FlexGroup**. Cuando la lista de agregados se actualiza en SVM, la lista se actualiza automáticamente en Trident sondeando la SVM sin tener que reiniciar la controladora Trident. Cuando se configuró una lista de agregado específica en Trident para aprovisionar volúmenes, si se cambia el nombre de la lista de agregados o se sale de SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar la lista de agregados por una que esté presente en la SVM o quitarla por completo para que el back-end vuelva a estar en línea.	""

Parámetro	Descripción	Predeterminado
`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 qtrees y la `qtreesPerFlexvol` opción permite personalizar el número máximo de qtrees por FlexVol.	"" (no se aplica de forma predeterminada)
`debugTraceFlags`	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {“api”:false, “method”:true} no lo utilice `debugTraceFlags` a menos que esté solucionando problemas y requiera un volcado de log detallado.	nulo
`nasType`	Configure la creación de volúmenes NFS o SMB. Las opciones son `nfs` `smb` o nulas. El valor predeterminado es nulo en volúmenes de NFS.	`nfs`
`nfsMountOptions`	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident volverá a utilizar las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento. Si no se especifican opciones de montaje en la clase almacenamiento o el archivo de configuración, Trident no definirá ninguna opción de montaje en un volumen persistente asociado.	""
`qtreesPerFlexvol`	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	«200»
`smbShare`	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	`smb-share`

Parámetro	Descripción	Predeterminado
`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.	`true` Para ONTAP 9.15.1 o posterior, de lo contrario `false`.
`limitVolumePoolSize`	Tamaño máximo de FlexVol que se puede solicitar cuando se utilizan qtrees en el back-end económico de ONTAP-nas.	"" (no se aplica de forma predeterminada)
`denyNewVolumePools`	Restringe `ontap-nas-economy` los back-ends de la creación de nuevos volúmenes de FlexVol para contener sus Qtrees. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	

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 Qtrees	verdadero
`spaceReserve`	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	ninguno
`snapshotPolicy`	Política de Snapshot que se debe usar	ninguno
`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	""
`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. no admitido por ontap-nas-Economy.	""
`snapshotReserve`	Porcentaje de volumen reservado para las Snapshot	«0» si `snapshotPolicy` no es «ninguno», de lo contrario «

Parámetro	Descripción	Predeterminado
`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"
`tieringPolicy`	Política de organización en niveles para utilizar ninguna	«Solo Snapshot» para la configuración SVM-DR anterior a ONTAP 9,5
`unixPermissions`	Modo para volúmenes nuevos	«777» para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
`snapshotDir`	Controla el acceso al `.snapshot` directorio	“True” para NFSv4 “false” para NFSv3
`exportPolicy`	Política de exportación que se va a utilizar	"predeterminado"
`securityStyle`	Estilo de seguridad para nuevos volúmenes. Compatibilidad y `unix` estilos de seguridad de NFS `mixed`. Compatibilidad y `ntfs` estilos de seguridad de SMB `mixed`.	El valor por defecto de NFS es `unix`. El valor por defecto de SMB es `ntfs`.
`nameTemplate`	Plantilla para crear nombres de volúmenes personalizados.	""

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.

Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados definidos:

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: '10'
```

For `ontap-nas` and `ontap-nas-flexgroups`, Trident ahora utiliza un nuevo cálculo para garantizar que el tamaño del FlexVol se ajusta correctamente con el porcentaje de reserva de instantáneas y la RVP. Cuando el usuario solicita una RVP, Trident crea la FlexVol original con más espacio mediante el nuevo cálculo. Este cálculo garantiza que el usuario recibe el espacio de escritura que solicitó en el PVC y no menos espacio que el que solicitó. Antes de v21.07, cuando el usuario solicita una RVP (por ejemplo, 5GIB) con el 50 por ciento de snapshotReserve, solo obtiene 2,5 GIB de espacio editable. Esto se debe a que lo que el usuario solicitó es todo el volumen y `snapshotReserve` es un porcentaje de ello. Con Trident 21,07, lo que el usuario solicita es el espacio de escritura y Trident define `snapshotReserve` la cantidad como el porcentaje de todo el volumen. Esto no se aplica a `ontap-nas-economy`. Vea el siguiente ejemplo para ver cómo funciona:

El cálculo es el siguiente:

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

Para snapshotReserve = 50 % y la solicitud de RVP = 5 GIB, el tamaño total del volumen es 2/.5 = 10 GIB y el tamaño disponible es de 5 GIB, lo que es lo que solicitó el usuario en la solicitud de RVP. El `volume show` comando debería mostrar resultados similares a este ejemplo:

Los back-ends existentes de instalaciones anteriores aprovisionarán los volúmenes tal y como se explicó anteriormente al actualizar Trident. En el caso de los volúmenes que creó antes de actualizar, debe cambiar el tamaño de sus volúmenes para que se observe el cambio. Por ejemplo, una RVP de 2GiB GB con `snapshotReserve=50` versiones anteriores dio como resultado un volumen que proporciona 1GiB GB de espacio editable. Cambiar el tamaño del volumen a 3 GIB, por ejemplo, proporciona a la aplicación 3 GIB de espacio editable en un volumen de 6 GIB.

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 ONTAP de NetApp con Trident, la recomendación es especificar nombres DNS para las LIF en lugar de direcciones IP.

Ejemplo de economía de NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Ejemplo de FlexGroup NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Ejemplo de MetroCluster

Puede configurar el backend para evitar tener que actualizar manualmente la definición 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-nas
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

Ejemplo de volúmenes de SMB

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Ejemplo de autenticación basada en certificados

Este es un ejemplo de configuración de backend mínimo. `clientCertificate` `clientPrivateKey`, , Y `trustedCACertificate` (opcional, si 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
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

Ejemplo de política de exportación automática

En este ejemplo, se muestra cómo puede indicar a Trident que utilice políticas de exportación dinámicas para crear y gestionar la política de exportación automáticamente. Esto funciona igual para `ontap-nas-economy` los controladores y. `ontap-nas-flexgroup`

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

Ejemplo de direcciones IPv6

Este ejemplo se muestra `managementLIF` usando una dirección IPv6.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

Ejemplo de Amazon FSx para ONTAP mediante volúmenes de bloque de mensajes del servidor

```
`smbShare`El parámetro es necesario para FSx para ONTAP mediante
volúmenes de SMB.
```

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

Ejemplo de configuración de backend con nameTemplate

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

Ejemplos de back-ends con pools virtuales

En los archivos de definición de backend de ejemplo que se muestran a continuación, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` 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 FlexVol for `ontap-nas` o FlexGroup para `ontap-nas-flexgroup`. 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 NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: 'false'
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
    app: msoffice
    cost: '100'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
    adaptiveQosPolicy: adaptive-premium
- labels:
    app: slack
    cost: '75'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    department: legal
    creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    app: wordpress
```

```
    cost: '50'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
    app: mysqldb
    cost: '25'
  zone: us_east_1d
  defaults:
    spaceReserve: volume
    encryption: 'false'
    unixPermissions: '0775'
```

Ejemplo de FlexGroup NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
    protection: gold
    creditpoints: '50000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    protection: gold
    creditpoints: '30000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    protection: silver
    creditpoints: '20000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
    protection: bronze
    creditpoints: '10000'
  zone: us_east_1d
  defaults:
```

```
    spaceReserve: volume
    encryption: 'false'
    unixPermissions: '0775'
```

Ejemplo de economía de NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: nas_economy_store
region: us_east_1
storage:
- labels:
    department: finance
    creditpoints: '6000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    protection: bronze
    creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
    department: engineering
    creditpoints: '3000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
    department: humanresource
    creditpoints: '2000'
  zone: us_east_1d
  defaults:
    spaceReserve: volume
```

```
    encryption: 'false'
    unixPermissions: '0775'
```

Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass se refieren a 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 y segundo pool virtual del `ontap-nas-flexgroup` backend. Estos son los únicos pools que ofrecen 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 tercer y cuarto pool virtual del `ontap-nas-flexgroup` backend. Estos son los únicos pools que ofrecen un nivel de protección distinto al Gold.

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

- `app-mysqldb`StorageClass se asignará al cuarto pool virtual del `ontap-nas` 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 tercer pool virtual del `ontap-nas-flexgroup` backend. Este es el único pool que ofrece protección de nivel plata y 20000 puntos de crédito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
```

- `creditpoints-5k`StorageClass se asignará al tercer pool virtual del `ontap-nas` backend y al segundo pool virtual del backend `ontap-nas-economy`. 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"
```

Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

`dataLIF`Actualice tras la configuración inicial

Puede cambiar la LIF de datos tras la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON back-end con LIF de datos actualizadas.

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

Si los RVP están conectados a uno o varios pods, deben recuperar todos los pods correspondientes y, a continuación, traerlos para que surta efecto el nuevo LIF de datos.