Drivers NAS do ONTAP

Trident

NetApp
July 01, 2026

Índice

Drivers NAS do ONTAP

Visão geral do driver ONTAP NAS

Saiba mais sobre como configurar um backend ONTAP com os drivers NAS do ONTAP e do Cloud Volumes ONTAP.

Detalhes do driver ONTAP NAS

Trident fornece os seguintes drivers de armazenamento NAS para se comunicar com o ONTAP cluster. Os modos de acesso suportados são: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Driver	Protocolo	volumeMode	Modos de acesso suportados	Sistemas de arquivos suportados
`ontap-nas`	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`
`ontap-nas-economy`	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`
`ontap-nas-flexgroup`	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`

- Use `ontap-san-economy` somente se a contagem de uso de volume persistente prevista for maior que "limites de volume ONTAP suportados".
- Use `ontap-nas-economy` somente se a contagem de uso de volume persistente prevista for maior que "limites de volume ONTAP suportados" e o driver `ontap-san-economy` não puder ser usado.
- Não utilize `ontap-nas-economy` se você prevê a necessidade de proteção de dados, recuperação de desastres ou mobilidade.
- NetApp não recomenda usar o crescimento automático do FlexVol em todos os drivers ONTAP, exceto ontap-san. Como alternativa, Trident oferece suporte ao uso de reserva de snapshot e dimensiona os volumes FlexVol de acordo.

Permissões do usuário

Trident espera ser executado como administrador do ONTAP ou do SVM, normalmente usando o `admin` usuário do cluster ou um `vsadmin` usuário do SVM, ou um usuário com um nome diferente que tenha a mesma função.

Para implantações do Amazon FSx for NetApp ONTAP, Trident espera ser executado como administrador do ONTAP ou do SVM, usando o usuário do cluster `fsxadmin` ou um usuário do SVM `vsadmin`, ou um usuário com um nome diferente que tenha a mesma função. O `fsxadmin` usuário é um substituto limitado para o usuário administrador do cluster.

Se você usar o `limitAggregateUsage`parâmetro, são necessárias permissões de administrador do cluster. Ao usar Amazon FSx for NetApp ONTAP com Trident, o `limitAggregateUsage`parâmetro não funcionará com as contas de usuário `vsadmin`e `fsxadmin`. A operação de configuração falhará se você especificar este parâmetro.

Embora seja possível criar uma função mais restritiva dentro do ONTAP que um driver Trident possa usar, não recomendamos isso. A maioria das novas versões do Trident chamará APIs adicionais que precisariam ser consideradas, dificultando as atualizações e tornando-as propensas a erros.

Prepare-se para configurar um backend com drivers ONTAP NAS

Compreenda os requisitos, as opções de autenticação e as políticas de exportação para configurar um backend ONTAP com drivers ONTAP NAS. A partir da versão 25.10, NetApp Trident oferece suporte "NetApp AFX sistema de storage". NetApp AFX storage systems diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage. Na configuração do backend do Trident, não é necessário especificar que seu sistema é AFX. Ao selecionar `ontap-nas` como o `storageDriverName`, o Trident detecta automaticamente os sistemas AFX.

Apenas o `ontap-nas`driver (com o protocolo NFS) é compatível com sistemas AFX; o protocolo SMB não é compatível.

Requisitos

- Para todos os backends ONTAP, Trident exige que pelo menos um agregado seja atribuído à SVM.
- Você pode executar mais de um driver e criar classes de armazenamento que apontem para um ou outro. Por exemplo, você pode configurar uma classe Gold que usa o driver `ontap-nas` e uma classe Bronze que usa o `ontap-nas-economy`.
- Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas NFS apropriadas instaladas. Consulte "aqui" para mais detalhes.
- Trident suporta volumes SMB montados em pods executados apenas em nós Windows. Consulte Prepare-se para provisionar volumes SMB para obter detalhes.

Autenticar o backend ONTAP

Trident oferece dois modos de autenticação de um backend ONTAP.

- Baseado em credenciais: Este modo requer permissões suficientes no backend do ONTAP. Recomenda-se usar uma conta associada a uma função de login de segurança predefinida, como `admin` ou `vsadmin` para garantir a máxima compatibilidade com as versões do ONTAP.
- Baseado em certificado: Este modo requer um certificado instalado no backend para o Trident se comunicar com um cluster ONTAP. Nesse caso, a definição do backend deve conter os valores codificados em Base64 do certificado do cliente, da chave e do certificado da CA confiável, se utilizado (recomendado).

Você pode atualizar os backends existentes para alternar entre métodos baseados em credenciais e

baseados em certificados. No entanto, apenas um método de autenticação é suportado por vez. Para mudar para um método de autenticação diferente, você deve remover o método existente da configuração do backend.

> Se você tentar fornecer **tanto credenciais quanto certificados**, a criação do backend falhará com um erro informando que mais de um método de autenticação foi fornecido no arquivo de configuração.

Ativar autenticação baseada em credenciais

Trident requer as credenciais de um administrador com escopo de SVM/cluster para se comunicar com o backend do ONTAP. Recomenda-se o uso de funções padrão predefinidas, como `admin` ou `vsadmin`. Isso garante a compatibilidade futura com versões do ONTAP que possam expor APIs de recursos a serem usadas por versões futuras do Trident. Uma função de login de segurança personalizada pode ser criada e usada com Trident, mas não é recomendada.

Uma definição de backend de exemplo será semelhante a esta:

YAML

```yaml
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
        "name": "secret-backend-creds"
    }
}
```

Lembre-se de que a definição do backend é o único local onde as credenciais são armazenadas em texto simples. Após a criação do backend, nomes de usuário/senhas são codificados em Base64 e armazenados como segredos do Kubernetes. A criação/atualização de um backend é a única etapa que requer

conhecimento das credenciais. Assim, trata-se de uma operação exclusiva do administrador, a ser realizada pelo administrador de storage do Kubernetes.

Habilitar autenticação baseada em certificado

Novos e existentes backends podem usar um certificado e se comunicar com o backend do ONTAP. Três parâmetros são necessários na definição do backend.

- clientCertificate: Valor codificado em Base64 do certificado do cliente.
- clientPrivateKey: Valor codificado em Base64 da chave privada associada.
- trustedCACertificate: valor codificado em Base64 do certificado CA confiável. Se uma CA confiável estiver sendo usada, este parâmetro deve ser fornecido. Isso pode ser ignorado se nenhuma CA confiável for usada.

Um fluxo de trabalho típico envolve as seguintes etapas.

Passos

1. Gere um certificado de cliente e uma chave. Ao gerar, defina o Nome Comum (CN) para o usuário ONTAP que será usado para autenticação.

```
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. Adicione um certificado de CA confiável ao cluster ONTAP. Isso pode já ter sido configurado pelo administrador de storage. Ignore se nenhuma CA confiável for utilizada.

```
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 o certificado do cliente e a chave (do passo 1) no cluster 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 se a função de login de segurança do ONTAP suporta `cert` método de autenticação.

```
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. Teste a autenticação usando o certificado gerado. Substitua <ONTAP Management LIF> e <vserver name> pelo endereço IP da Management LIF e pelo nome da SVM. Você deve garantir que o LIF tenha sua política de serviço definida como `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 o certificado, a chave e o certificado da CA confiável com Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Crie o backend usando os valores obtidos na etapa 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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Atualize os métodos de autenticação ou altere as credenciais

Você pode atualizar um backend existente para usar um método de autenticação diferente ou para rotacionar suas credenciais. Isso funciona nos dois sentidos: backends que utilizam nome de usuário/senha podem ser atualizados para usar certificados; backends que utilizam certificados podem ser atualizados para usar nome de usuário/senha. Para fazer isso, você deve remover o método de autenticação existente e adicionar o novo método de autenticação. Em seguida, use o arquivo backend.json atualizado contendo os parâmetros necessários para executar `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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Ao rotacionar senhas, o administrador de storage deve primeiro atualizar a senha do usuário no ONTAP. Em seguida, é feita uma atualização no backend. Ao rotacionar certificados, vários certificados podem ser adicionados ao usuário. O backend é então atualizado para usar o novo certificado, após o que o certificado antigo pode ser excluído do cluster ONTAP.

A atualização do backend não interrompe o acesso aos volumes já criados, nem afeta as conexões de volume feitas posteriormente. Uma atualização bem-sucedida do backend indica que Trident pode se comunicar com o ONTAP backend e lidar com operações de volume futuras.

Criar função ONTAP personalizada para Trident

Você pode criar uma função de cluster ONTAP com privilégios mínimos para que não precise usar a função de administrador do ONTAP para executar operações no Trident. Ao incluir o nome de usuário em um arquivo de configuração de backend do Trident, o Trident usa a função de cluster ONTAP que você criou para executar as operações.

Consulte "Gerador de funções personalizadas Trident" para obter mais informações sobre como criar funções personalizadas do Trident.

Usando ONTAP CLI

1. Crie uma nova função usando o seguinte comando:

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

2. Crie um nome de usuário para o usuário do 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. Mapeie a função para o usuário:

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

Usando System Manager

Execute as seguintes etapas no ONTAP System Manager:

1. **Crie uma função personalizada**:
   a. Para criar uma função personalizada no nível do cluster, selecione **Cluster > Settings**.

      (Ou) Para criar uma função personalizada no nível da SVM, selecione **Storage > Storage VMs > `required SVM`> Settings > Users and Roles**.

   b. Selecione o ícone de seta (→) ao lado de **Users and Roles**.
   c. Selecione **+Adicionar** em **Roles**.
   d. Defina as regras para a função e clique em **Save**.
2. **Mapeie a função ao usuário Trident**: + Execute as seguintes etapas na página **Usuários e Funções**:
   a. Selecione o ícone Adicionar **+** em **Usuários**.
   b. Selecione o nome de usuário desejado e selecione uma função no menu suspenso para **Função**.
   c. Clique em **Salvar**.

Consulte as seguintes páginas para obter mais informações:

- "Funções personalizadas para administração do ONTAP" ou "Definir funções personalizadas"
- "Trabalhe com funções e usuários"

Gerenciar políticas de exportação NFS

Trident usa políticas de exportação NFS para controlar o acesso aos volumes que provisiona.

Trident oferece duas opções ao trabalhar com políticas de exportação:

- Trident pode gerenciar dinamicamente a própria política de exportação; nesse modo de operação, o administrador de storage especifica uma lista de blocos CIDR que representam endereços IP admissíveis. Trident adiciona automaticamente os IPs de nó aplicáveis que se enquadram nesses intervalos à política de exportação no momento da publicação. Alternativamente, quando nenhum CIDR é especificado, todos os IPs unicast de escopo global encontrados no nó para o qual o volume está sendo publicado serão adicionados à política de exportação.
- Os administradores de storage podem criar uma política de exportação e adicionar regras manualmente. Trident usa a política de exportação padrão, a menos que um nome de política de exportação diferente seja especificado na configuração.

Gerencie dinamicamente as políticas de exportação

Trident oferece a capacidade de gerenciar dinamicamente políticas de exportação para backends ONTAP. Isso fornece ao administrador de storage a capacidade de especificar um espaço de endereços permitido para os endereços IP dos nós de trabalho, em vez de definir regras explícitas manualmente. Isso simplifica muito o gerenciamento de políticas de exportação; as modificações na política de exportação não exigem mais intervenção manual no cluster de storage. Além disso, isso ajuda a restringir o acesso ao cluster de storage apenas aos nós de trabalho que estão montando volumes e possuem endereços IP no intervalo especificado, oferecendo um gerenciamento detalhado e automatizado.

> Não utilize Network Address Translation (NAT) ao usar políticas de exportação dinâmicas. Com NAT, o controlador de storage vê o endereço NAT de frontend e não o endereço IP real do host, portanto, o acesso será negado quando nenhuma correspondência for encontrada nas regras de exportação.

Exemplo

Existem duas opções de configuração que devem ser usadas. Veja um exemplo de definição 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
```

> Ao usar este recurso, você deve garantir que a junção raiz em sua SVM tenha uma política de exportação previamente criada com uma regra de exportação que permita o bloco CIDR do nó (como a política de exportação padrão). Sempre siga a prática recomendada pela NetApp de dedicar uma SVM ao Trident.

Aqui está uma explicação de como esse recurso funciona usando o exemplo acima:

- `autoExportPolicy` está definido como `true`. Isso indica que Trident cria uma política de exportação

para cada volume provisionado com este backend para o `svm1` SVM e lida com a adição e exclusão de regras usando `autoexportCIDRs` blocos de endereços. Até que um volume seja anexado a um nó, o volume usa uma política de exportação vazia, sem regras, para impedir o acesso indesejado a esse volume. Quando um volume é publicado em um nó, Trident cria uma política de exportação com o mesmo nome da qtree subjacente, contendo o endereço IP do nó dentro do bloco CIDR especificado. Esses IPs também serão adicionados à política de exportação usada pelo volume pai FlexVol.

  - Por exemplo:
    - UUID do backend 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`definido para `true`
    - prefixo de storage `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - qtree denominada trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c cria uma política de exportação para a FlexVol denominada `trident-403b5326-8482-40db96d0-d83fb3f4daec`, uma política de exportação para a qtree denominada `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`, e uma política de exportação vazia denominada `trident_empty` no SVM. As regras para a política de exportação da FlexVol serão um superconjunto de quaisquer regras contidas nas políticas de exportação da qtree. A política de exportação vazia será reutilizada por quaisquer volumes que não estejam anexados.

- `autoExportCIDRs` contém uma lista de blocos de endereços. Este campo é opcional e ele é definido por padrão como ["0.0.0.0/0", "::/0"]. Se não for definido, Trident adiciona todos os endereços unicast de escopo global encontrados nos nós de trabalho com publicações.

Neste exemplo, o `192.168.0.0/24` espaço de endereços é fornecido. Isso indica que os IPs dos nós do Kubernetes que se enquadram nesse intervalo de endereços com publicações serão adicionados à política de exportação que o Trident cria. Quando o Trident registra um nó no qual está sendo executado, ele recupera os endereços IP do nó e os compara com os blocos de endereços fornecidos em `autoExportCIDRs`. No momento da publicação, após filtrar os IPs, o Trident cria as regras da política de exportação para os endereços IP dos clientes do nó para o qual está publicando.

Você pode atualizar `autoExportPolicy` e `autoExportCIDRs` para backends após criá-los. Você pode adicionar novos CIDRs para um backend que é gerenciado automaticamente ou excluir CIDRs existentes. Tenha cuidado ao excluir CIDRs para garantir que conexões existentes não sejam interrompidas. Você também pode optar por desativar `autoExportPolicy` para um backend e voltar para uma política de exportação criada manualmente. Isso exigirá a configuração do parâmetro `exportPolicy` no seu arquivo de configuração do backend.

Após Trident criar ou atualizar um backend, você pode verificar o backend usando `tridentctl` ou o correspondente `tridentbackend` CRD:

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

Quando um nó é removido, Trident verifica todas as políticas de exportação para remover as regras de acesso correspondentes ao nó. Ao remover esse endereço IP do nó das políticas de exportação dos backends gerenciados, Trident impede montagens não autorizadas, a menos que esse endereço IP seja reutilizado por um novo nó no cluster.

Para backends preexistentes, atualizar o backend com `tridentctl update backend` garante que Trident gerencie as políticas de exportação automaticamente. Isso cria duas novas políticas de exportação nomeadas de acordo com o UUID do backend e o nome da qtree quando necessário. Volumes presentes no backend usarão as novas políticas de exportação após serem desmontados e montados novamente.

> ⓘ A exclusão de um backend com políticas de exportação gerenciadas automaticamente excluirá a política de exportação criada dinamicamente. Se o backend for recriado, ele será tratado como um novo backend e resultará na criação de uma nova política de exportação.

Se o endereço IP de um nó ativo for atualizado, você deve reiniciar o pod do Trident nesse nó. Trident então atualizará a política de exportação dos backends que gerencia para refletir essa alteração de IP.

Prepare-se para provisionar volumes SMB

Com um pouco de preparação adicional, você pode provisionar volumes SMB usando `ontap-nas` drivers.

> ⓘ Você deve configurar ambos os protocolos NFS e SMB/CIFS na SVM para criar um `ontap-nas-economy` volume SMB para clusters ONTAP locais. A falha ao configurar qualquer um desses protocolos fará com que a criação do volume SMB falhe.

> ⓘ `autoExportPolicy` não é compatível com volumes SMB.

Antes de começar

Antes de poder provisionar volumes SMB, você deve ter o seguinte.

- Um cluster Kubernetes com um nó controlador Linux e pelo menos um nó de trabalho Windows executando Windows Server 2022. Trident suporta volumes SMB montados em pods executados apenas em nós Windows.
- Pelo menos um segredo Trident contendo suas credenciais do Active Directory. Para gerar o segredo `smbcreds`:

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

- Um proxy CSI configurado como um serviço do Windows. Para configurar um `csi-proxy`, consulte "GitHub: CSI Proxy" ou "GitHub: CSI Proxy para Windows" para nós do Kubernetes em execução no Windows.

Passos

1. Para o ONTAP local, você pode opcionalmente criar um compartilhamento SMB ou o Trident pode criar um para você.

   Os compartilhamentos SMB são necessários para Amazon FSx for ONTAP.

   Você pode criar os compartilhamentos administrativos SMB de duas maneiras: usando o "Microsoft Management Console" snap-in Shared Folders ou usando a ONTAP CLI. Para criar os compartilhamentos SMB usando a ONTAP CLI:

   a. Se necessário, crie a estrutura de caminho de diretórios para o compartilhamento.

      O `vserver cifs share create` comando verifica o caminho especificado na opção -path durante a criação do compartilhamento. Se o caminho especificado não existir, o comando falha.

   b. Crie um compartilhamento SMB associado à SVM especificada:

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

   c. Verifique se o compartilhamento foi criado:

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

   Consulte "Criar um compartilhamento SMB" para obter detalhes completos.

2. Ao criar o backend, você deve configurar o seguinte para especificar os volumes SMB. Para todas as opções de configuração do backend do FSx para ONTAP, consulte "Opções e exemplos de configuração do FSx for ONTAP".

Parâmetro	Descrição	Exemplo
`smbShare`	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Microsoft Management Console ou ONTAP CLI; um nome para permitir que o Trident crie o compartilhamento SMB; ou você pode deixar o parâmetro em branco para impedir o acesso comum aos volumes. Este parâmetro é opcional para ONTAP on-premises. Este parâmetro é obrigatório para Amazon FSx for ONTAP backends e não pode ficar em branco.	`smb-share`
`nasType`	**Deve ser definido como `smb`.** Se for nulo, o padrão é `nfs`.	`smb`
`securityStyle`	Estilo de segurança para novos volumes. **Deve ser definido como `ntfs` ou `mixed` para volumes SMB.**	`ntfs` ou `mixed` for SMB volumes
`unixPermissions`	Modo para novos volumes. **Deve ser deixado em branco para volumes SMB.**	""

Ativar SMB seguro

A partir da versão 25.06, NetApp Trident oferece suporte ao provisionamento seguro de volumes SMB criados usando `ontap-nas` e `ontap-nas-economy` backends. Quando o SMB seguro está habilitado, você pode fornecer acesso controlado aos compartilhamentos SMB para usuários e grupos de usuários do Active Directory (AD) usando listas de controle de acesso (ACLs).

Pontos a lembrar

- A importação de `ontap-nas-economy` volumes não é suportada.
- Apenas clones somente leitura são suportados para `ontap-nas-economy` volumes.
- Se o Secure SMB estiver ativado, Trident ignorará o compartilhamento SMB mencionado no backend.
- A atualização da anotação PVC, da anotação da storage class e do campo backend não atualiza a ACL de compartilhamento SMB.
- A ACL de compartilhamento SMB especificada na anotação do PVC clonado terá precedência sobre as do PVC de origem.
- Certifique-se de fornecer usuários válidos do Active Directory ao habilitar o SMB seguro. Usuários inválidos não serão adicionados à ACL.
- Se você fornecer o mesmo usuário do AD no backend, na storage class e no PVC com permissões diferentes, a prioridade de permissão será: PVC, storage class e, em seguida, backend.
- Secure SMB é compatível com `ontap-nas`importações de volumes gerenciados e não se aplica a importações de volumes não gerenciados.

Passos

1. Especifique adAdminUser em TridentBackendConfig conforme mostrado no exemplo a seguir:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. Adicione a anotação na storage class.

   Adicione a `trident.netapp.io/smbShareAdUser` anotação à storage class para habilitar SMB seguro sem falhas. O valor de usuário especificado para a anotação `trident.netapp.io/smbShareAdUser` deve ser o mesmo que o nome de usuário especificado no `smbcreds` secret. Você pode escolher um dos seguintes para `smbShareAdUserPermission`: `full_control`, `change` ou `read`. A permissão padrão é `full_control`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. Crie um PVC.

   O exemplo a seguir cria um PVC:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Opções e exemplos de configuração do ONTAP NAS

Aprenda a criar e usar drivers ONTAP NAS com sua instalação do Trident. Esta seção fornece exemplos de configuração de backend e detalhes para mapear backends para StorageClasses. A partir da versão 25.10, NetApp Trident oferece suporte "NetApp sistemas de storage AFX". NetApp AFX sistemas de storage diferem de outros sistemas baseados em ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage.

Apenas o `ontap-nas`driver (com protocolo NFS) é compatível com sistemas AFX da NetApp; o protocolo SMB não é compatível.

Opções de configuração do backend

Na configuração do backend do Trident, não é necessário especificar que seu sistema é um NetApp AFX sistema de storage. Ao selecionar `ontap-nas` como o `storageDriverName`, o Trident detecta automaticamente o sistema de storage AFX. Alguns parâmetros de configuração do backend não se aplicam a sistemas de storage AFX.

A tabela a seguir exibe as opções de configuração do backend:

Parâmetro	Descrição	Padrão
`version`		Sempre 1
`storageDriverName`	Nome do driver de armazenamento Para sistemas NetApp AFX, apenas `ontap-nas` é suportado.	`ontap-nas`, `ontap-nas-economy`, ou `ontap-nas-flexgroup`

Parâmetro	Descrição	Padrão
`backendName`	Nome personalizado ou o storage backend	Nome do driver + "_" + dataLIF
`managementLIF`	Endereço IP de um cluster ou LIF de gerenciamento de SVM. Um nome de domínio totalmente qualificado (FQDN) pode ser especificado. Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Para um switchover MetroCluster perfeito, consulte o Exemplo do MetroCluster.	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	Endereço IP do protocolo LIF. NetApp recomenda especificar `dataLIF`. Caso não seja fornecido, Trident busca os dataLIFs da SVM. Você pode especificar um nome de domínio totalmente qualificado (FQDN) para ser usado nas operações de montagem NFS, permitindo criar um DNS round-robin para balancear a carga entre vários dataLIFs. Pode ser alterado após a configuração inicial. Consulte . Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. **Omita para MetroCluster.** Consulte o Exemplo do MetroCluster.	Endereço especificado ou derivado de SVM, caso não seja especificado (não recomendado)
`svm`	Máquina virtual de storage a ser usada **Omitir para MetroCluster.** Consulte o Exemplo do MetroCluster.	Derivado se uma SVM `managementLIF` for especificada
`autoExportPolicy`	Ativar a criação e atualização automática de políticas de exportação [Booleano]. Usando as opções `autoExportPolicy` e `autoExportCIDRs`, Trident pode gerenciar políticas de exportação automaticamente.	falso
`autoExportCIDRs`	Lista de CIDRs para filtrar os IPs dos nós do Kubernetes quando `autoExportPolicy` estiver habilitado. Usando as opções `autoExportPolicy` e `autoExportCIDRs`, Trident pode gerenciar políticas de exportação automaticamente.	["0.0.0.0/0", "::/0"]`
`labels`	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
`clientCertificate`	Valor codificado em Base64 do certificado do cliente. Usado para autenticação baseada em certificado	""
`clientPrivateKey`	Valor codificado em Base64 da chave privada do cliente. Usado para autenticação baseada em certificado	""

Parâmetro	Descrição	Padrão
`trustedCACertificate`	Valor codificado em Base64 do certificado da CA confiável. Opcional. Usado para autenticação baseada em certificado	""
`username`	Nome de usuário para conectar-se ao cluster/SVM. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory".	
`password`	Senha para conectar-se ao cluster/SVM. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory".	
`storagePrefix`	Prefixo usado ao provisionar novos volumes no SVM. Não pode ser atualizado após ser definido Ao usar o ontap-nas-economy e um storagePrefix com 24 ou mais caracteres, as qtrees não terão o storage prefix incorporado, embora ele esteja presente no nome do volume.	"Trident"
`aggregate`	Agregado para provisionamento (opcional; se definido, deve ser atribuído à SVM). Para o `ontap-nas-flexgroup` driver, esta opção é ignorada. Se não for atribuído, qualquer um dos agregados disponíveis pode ser usado para provisionar um FlexGroup volume. Quando o agregado é atualizado no SVM, ele é atualizado automaticamente no Trident por meio de polling no SVM, sem a necessidade de reiniciar o Trident Controller. Quando você configurou um agregado específico no Trident para provisionar volumes, se o agregado for renomeado ou movido para fora do SVM, o backend entrará em estado de falha no Trident durante o polling do agregado no SVM. Você deve alterar o agregado para um que esteja presente no SVM ou removê-lo completamente para que o backend volte a ficar online. **Não especifique para sistemas de storage AFX.**	""

Parâmetro	Descrição	Padrão
`limitAggregateUsage`	O provisionamento falhará se o uso ultrapassar essa porcentagem. **Não se aplica ao Amazon FSx para ONTAP**. **Não especifique para sistemas de storage AFX.**	"" (não aplicado por padrão)
flexgroupAggregateList	Lista de agregados para provisionamento (opcional; se definida, deve ser atribuída à SVM). Todos os agregados atribuídos à SVM são usados para provisionar um FlexGroup volume. Compatível com o driver de storage **ontap-nas-flexgroup**. Quando a lista de agregados é atualizada no SVM, a lista é atualizada automaticamente no Trident por meio de polling do SVM, sem a necessidade de reiniciar o Trident Controller. Quando você configurou uma lista de agregados específica no Trident para provisionar volumes, se a lista de agregados for renomeada ou movida para fora do SVM, o backend entrará em estado de falha no Trident enquanto faz polling do agregado do SVM. Você deve alterar a lista de agregados para uma que esteja presente no SVM ou removê-la completamente para que o backend volte a ficar online.	""
`limitVolumeSize`	O provisionamento falha se o tamanho do volume solicitado for superior a este valor.	"" (não aplicado por padrão)
`debugTraceFlags`	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, {"api":false, "method":true} não use `debugTraceFlags` a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
`nasType`	Configurar a criação de volumes NFS ou SMB. As opções são `nfs`, `smb` ou null. Definir como null define volumes NFS por padrão. **Se especificado, defina sempre como `nfs` para sistemas de armazenamento AFX**.	`nfs`

Parâmetro	Descrição	Padrão
`nfsMountOptions`	Lista separada por vírgulas de opções de montagem NFS. As opções de montagem para volumes persistentes do Kubernetes são normalmente especificadas nas classes de armazenamento, mas se nenhuma opção de montagem for especificada em uma classe de armazenamento, Trident usará as opções de montagem especificadas no arquivo de configuração do backend de storage. Se nenhuma opção de montagem for especificada na classe de armazenamento ou no arquivo de configuração, Trident não definirá nenhuma opção de montagem em um volume persistente associado.	""
`qtreesPerFlexvol`	Máximo de Qtrees por FlexVol, deve estar no intervalo [50, 300]	"200"
`smbShare`	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Microsoft Management Console ou ONTAP CLI; um nome para permitir que o Trident crie o compartilhamento SMB; ou você pode deixar o parâmetro em branco para impedir o acesso comum aos volumes. Este parâmetro é opcional para ONTAP on-premises. Este parâmetro é obrigatório para Amazon FSx for ONTAP backends e não pode ficar em branco.	`smb-share`
`useREST`	Parâmetro booleano para usar as ONTAP REST APIs. `useREST` Quando definido como `true`, Trident usa as ONTAP REST APIs para se comunicar com o backend; quando definido como `false`, Trident usa chamadas ONTAPI (ZAPI) para se comunicar com o backend. Este recurso requer ONTAP 9.11.1 e versões posteriores. Além disso, a função de login do ONTAP utilizada deve ter acesso ao aplicativo `ontapi`. Isso é atendido pelas funções predefinidas `vsadmin` e `cluster-admin`. A partir da versão 24.06 do Trident e ONTAP 9.15.1 ou posterior, `useREST` é definido como `true` por padrão; altere `useREST` para `false` para usar chamadas ONTAPI (ZAPI). **Se especificado, defina sempre como `true` para sistemas de armazenamento AFX**.	`true`para ONTAP 9.15.1 ou posterior, caso contrário `false`.
`limitVolumePoolSize`	Tamanho máximo solicitável de FlexVol ao usar Qtrees no backend ontap-nas-economy.	"" (não aplicado por padrão)
`denyNewVolumePools`	Restringe `ontap-nas-economy` os backends de criarem novos volumes FlexVol para conter seus Qtrees. Somente FlexVols preexistentes são usados para provisionar novos PVs.	

Parâmetro	Descrição	Padrão
`adAdminUser`	Usuário ou grupo de usuários administradores do Active Directory com acesso total aos compartilhamentos SMB. Use este parâmetro para conceder direitos de administrador ao compartilhamento SMB com controle total.	

Opções de configuração de backend para provisionamento de volumes

Você pode controlar o provisionamento padrão usando essas opções na seção `defaults` do arquivo de configuração. Para um exemplo, veja os exemplos de configuração abaixo.

Parâmetro	Descrição	Padrão
`spaceAllocation`	Alocação de espaço para Qtrees	"true"
`spaceReserve`	Modo de reserva de espaço; "none" (fino) ou "volume" (grosso)	"none"
`snapshotPolicy`	Política do Snapshot a ser usada	"none"
`qosPolicy`	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha uma de qosPolicy ou adaptiveQosPolicy por pool de storage/backend	""
`adaptiveQosPolicy`	Grupo de políticas de QoS adaptável para atribuir aos volumes criados. Escolha um dos qosPolicy ou adaptiveQosPolicy por pool de storage/backend. Não compatível com ontap-nas-economy.	""
`snapshotReserve`	Percentual do volume reservado para snapshots	"0" se `snapshotPolicy` for "none", caso contrário ""
`splitOnClone`	Separar um clone de seu progenitor no momento da criação	"false"
`encryption`	Habilite NetApp Volume Encryption (NVE) no novo volume; o padrão é `false`. A NVE deve estar licenciada e habilitada no cluster para usar esta opção. Se a NAE estiver habilitada no backend, qualquer volume provisionado no Trident terá a NAE habilitada. Para mais informações, consulte: "Como Trident funciona com NVE e NAE".	"false"
`tieringPolicy`	Política de tiering para usar "none"	
`unixPermissions`	Modo para novos volumes	"777" para volumes NFS; vazio (não aplicável) para volumes SMB
`snapshotDir`	Controla o acesso ao `.snapshot` diretório	`true`, `false` (Definido explicitamente).
`exportPolicy`	Política de exportação a ser usada	"default"

Parâmetro	Descrição	Padrão
`securityStyle`	Estilo de segurança para novos volumes. NFS suporta `mixed` e `unix` estilos de segurança. SMB suporta `mixed` e `ntfs` estilos de segurança.	NFS default é `unix`. SMB default é `ntfs`.
`nameTemplate`	Modelo para criar nomes de volume personalizados.	""

> O uso de grupos de políticas de QoS com Trident requer ONTAP 9.8 ou posterior. Você deve usar um grupo de políticas de QoS não compartilhado e garantir que o grupo de políticas seja aplicado a cada componente individualmente. Um grupo de políticas de QoS compartilhado impõe o limite máximo para a taxa de transferência total de todas as cargas de trabalho.

Exemplos de provisionamento de volume

Aqui está um exemplo com valores padrão definidos:

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

Para `ontap-nas` e `ontap-nas-flexgroups`, o Trident agora usa um novo cálculo para garantir que o FlexVol seja dimensionado corretamente com a porcentagem de snapshotReserve e o PVC. Quando o usuário solicita um PVC, o Trident cria o FlexVol original com mais espaço usando o novo cálculo. Esse cálculo garante que o usuário receba o espaço gravável solicitado no PVC, e não menos espaço do que o solicitado. Antes da v21.07, quando o usuário solicitava um PVC (por exemplo, 5 GiB), com o snapshotReserve em 50 por cento, ele recebia apenas 2,5 GiB de espaço gravável. Isso ocorre porque o que

o usuário solicitava era o volume total e `snapshotReserve` é uma porcentagem disso. Com o Trident 21.07, o que o usuário solicita é o espaço gravável e o Trident define o número de `snapshotReserve` como a porcentagem do volume total. Isso não se aplica a `ontap-nas-economy`. Veja o exemplo a seguir para ver como isso funciona:

O cálculo é o seguinte:

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

Para snapshotReserve = 50%, e solicitação de PVC = 5 GiB, o tamanho total do volume é 5/0,5 = 10 GiB e o tamanho disponível é 5 GiB, que é o que o usuário solicitou na solicitação de PVC. O comando `volume show` deve exibir resultados semelhantes a este exemplo:

Os backends existentes de instalações anteriores provisionarão volumes conforme explicado acima ao atualizar Trident. Para volumes que você criou antes da atualização, você deve redimensionar seus volumes para que a alteração seja observada. Por exemplo, um PVC de 2 GiB com `snapshotReserve=50` anteriormente resultava em um volume que fornece 1 GiB de espaço gravável. Redimensionar o volume para 3 GiB, por exemplo, fornece ao aplicativo 3 GiB de espaço gravável em um volume de 6 GiB.

Exemplos de configuração mínima

Os exemplos a seguir mostram configurações básicas que deixam a maioria dos parâmetros com os valores padrão. Esta é a maneira mais fácil de definir um backend.

> Se você estiver usando Amazon FSx no NetApp ONTAP com Trident, a recomendação é especificar nomes DNS para LIFs em vez de endereços IP.

Exemplo de economia ONTAP NAS

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

Exemplo de FlexGroup ONTAP NAS

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

Exemplo do MetroCluster

Você pode configurar o backend para evitar ter que atualizar manualmente a definição do backend após switchover e switchback durante "Replicação e recuperação de SVM".

Para switchover e switchback sem interrupções, especifique a SVM usando `managementLIF` e omita os parâmetros `dataLIF` e `svm`. Por exemplo:

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

Exemplo de volumes 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
```

Exemplo de autenticação baseada em certificado

Este é um exemplo mínimo de configuração de backend. `clientCertificate`, `clientPrivateKey` e `trustedCACertificate` (opcional, se estiver usando uma CA confiável) são preenchidos em `backend.json` e recebem os valores codificados em base64 do certificado do cliente, da chave privada e do certificado da CA confiável, 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_
```

Exemplo de política de exportação automática

Este exemplo mostra como você pode instruir Trident a usar políticas de exportação dinâmicas para criar e gerenciar a política de exportação automaticamente. Isso funciona da mesma forma para os `ontap-nas-economy` e `ontap-nas-flexgroup`drivers.

```
---
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
```

Exemplo de endereços IPv6

Este exemplo mostra `managementLIF` usando um endereço 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
```

Amazon FSx para ONTAP usando exemplo de volumes SMB

O `smbShare` parâmetro é necessário para Amazon FSx para ONTAP usando volumes 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_
```

Exemplo de configuração de backend com 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}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

Exemplos de backends com pools virtuais

Nos arquivos de definição de backend de exemplo mostrados abaixo, valores padrão específicos são definidos para todos os pools de storage, como `spaceReserve` em none, `spaceAllocation` em false e `encryption` em false. Os pools virtuais são definidos na seção de storage.

Trident define rótulos de provisionamento no campo "Comentários". Os comentários são definidos em FlexVol para `ontap-nas` ou FlexGroup para `ontap-nas-flexgroup`. Trident copia todos os rótulos presentes em um pool virtual para o volume de armazenamento durante o provisionamento. Para conveniência, administradores de storage podem definir rótulos por pool virtual e agrupar volumes por rótulo.

Nestes exemplos, alguns pools de storage definem seus próprios `spaceReserve`, `spaceAllocation`, e `encryption` valores, e alguns pools substituem os valores padrão.

Exemplo de ONTAP NAS

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

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

Exemplo de ONTAP NAS FlexGroup

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

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

Exemplo de economia ONTAP NAS

```
---
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"
```

Mapear back-ends para StorageClasses

As seguintes definições de StorageClass referem-se a Exemplos de backends com pools virtuais. Usando o campo `parameters.selector`, cada StorageClass especifica quais pools virtuais podem ser usados para hospedar um volume. O volume terá os aspectos definidos no pool virtual escolhido.

- O `protection-gold` StorageClass corresponderá ao primeiro e ao segundo pool virtual no `ontap-nas-flexgroup` backend. Esses são os únicos pools que oferecem proteção de nível ouro.

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

- O `protection-not-gold` StorageClass corresponderá ao terceiro e quarto pool virtual no `ontap-nas-flexgroup` backend. Esses são os únicos pools que oferecem nível de proteção diferente de gold.

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

- O `app-mysqldb` StorageClass será mapeado para o quarto pool virtual no `ontap-nas` backend. Este é o único pool que oferece configuração de pool de storage para app do tipo mysqldb.

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

- O `protection-silver-creditpoints-20k` StorageClass será mapeado para o terceiro pool virtual no `ontap-nas-flexgroup` backend. Este é o único pool que oferece proteção de nível prata e 20000 pontos 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"
```

- O `creditpoints-5k` StorageClass corresponderá ao terceiro pool virtual no `ontap-nas` backend e ao segundo pool virtual no `ontap-nas-economy` backend. Essas são as únicas ofertas de pool com 5000 creditpoints.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

Trident decidirá qual pool virtual será selecionado e garantirá que o requisito de storage seja atendido.

Atualize `dataLIF` após a configuração inicial

Você pode alterar o dataLIF após a configuração inicial executando o seguinte comando para fornecer o novo arquivo JSON de backend com o dataLIF atualizado.

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

Se os PVCs estiverem conectados a um ou mais pods, você deve desligar todos os pods correspondentes e então ligá-los novamente para que o novo dataLIF entre em vigor.

Exemplos seguros de SMB

Configuração de backend com o driver ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuração de backend com o driver ontap-nas-economy

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuração de backend com pool de storage

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
  - labels:
      app: msoffice
    defaults:
      adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Exemplo de classe de armazenamento com o driver ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Certifique-se de adicionar `annotations` para habilitar o SMB seguro. O SMB seguro não funciona sem as anotações, independentemente das configurações definidas no Backend ou no PVC.

Exemplo de classe de armazenamento com o driver ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Exemplo de PVC com um único usuário AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Exemplo de PVC com vários usuários de AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

Informações sobre direitos autorais

Informações sobre marcas comerciais