Drivers ONTAP NAS

Trident

NetApp
January 15, 2026

Índice

Drivers ONTAP NAS

Visão geral do driver ONTAP NAS

Aprenda a configurar um backend ONTAP com os drivers ONTAP NAS do ONTAP e do Cloud Volumes ONTAP .

Detalhes do driver ONTAP NAS

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

Motorista	Protocolo	modo de volume	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`

- Usar `ontap-san-economy` somente se a contagem de uso de volume persistente prevista for maior que"limites de volume ONTAP suportados" .
- Usar `ontap-nas-economy` somente se a contagem de uso de volume persistente prevista for maior que"limites de volume ONTAP suportados" e o `ontap-san-economy` O driver não pode ser usado.
- Não use `ontap-nas-economy` Se você prevê a necessidade de proteção de dados, recuperação de desastres ou mobilidade.
- A NetApp não recomenda o uso do Flexvol autogrow em todos os drivers ONTAP , exceto no ontap-san. Como solução alternativa, o Trident suporta o uso de reserva de snapshots e dimensiona os volumes Flexvol de acordo.

Permissões do usuário

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

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

Se você usar o `limitAggregateUsage` Para configurar o parâmetro, são necessárias permissões de administrador do cluster. Ao usar o Amazon FSx for NetApp ONTAP com Trident, o `limitAggregateUsage` O parâmetro não funcionará com o `vsadmin` e `fsxadmin` contas de usuário. 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 precisarão ser consideradas, tornando as atualizações difíceis e 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.

Requisitos

- Para todos os backends ONTAP , o 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 poderia configurar uma classe Gold que usa o `ontap-nas` motorista e uma classe Bronze que usa o `ontap-nas-economy` um.
- Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas NFS apropriadas instaladas. Consulte"aqui" para mais detalhes.
- O Trident suporta volumes SMB montados em pods executados apenas em nós Windows. Consulte Prepare-se para provisionar volumes SMB para mais detalhes.

Autenticar o backend ONTAP

O 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 servidor para que o Trident se comunique com um cluster ONTAP . Aqui, 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 sistemas de backend existentes para alternar entre métodos baseados em credenciais e métodos 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

O 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 futuras do ONTAP que possam expor APIs de recursos a serem usadas por versões futuras do Trident . É possível criar e usar uma função de login de segurança personalizada com o Trident, mas isso não é recomendado.

Uma definição de backend de exemplo terá a seguinte aparência:

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 lugar onde as credenciais são armazenadas em texto simples. Após a criação do backend, os 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 exige conhecimento das credenciais. Sendo assim, trata-se de uma operação exclusiva para administradores, a ser realizada pelo administrador do Kubernetes/armazenamento.

Habilitar autenticação baseada em certificado

Novos e existentes sistemas de backend podem usar um certificado e se comunicar com o backend ONTAP . São necessários três parâmetros na definição do backend.

- clientCertificate: Valor do certificado do cliente codificado em Base64.
- clientPrivateKey: Valor codificado em Base64 da chave privada associada.

- trustedCACertificate: Valor codificado em Base64 do certificado da Autoridade Certificadora (CA) confiável. Caso esteja utilizando uma Autoridade Certificadora (CA) confiável, este parâmetro deve ser fornecido. Isso pode ser ignorado se nenhuma Autoridade Certificadora (CA) confiável for utilizada.

Um fluxo de trabalho típico envolve as seguintes etapas.

Passos

1. Gere um certificado e uma chave de cliente. Ao gerar o código, 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 CA confiável ao cluster ONTAP . Isso pode já estar sendo tratado pelo administrador de armazenamento. Ignore se nenhuma Autoridade Certificadora (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 e a chave do cliente (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 é compatível. `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 do Management LIF e pelo nome do SVM. Você deve garantir que a política de serviço do LIF esteja 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 em 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: os sistemas internos que utilizam nome de usuário/senha podem ser atualizados para usar certificados; os sistemas internos que utilizam certificados podem ser atualizados para usar nome de usuário/senha. Para isso, você deve remover o método de autenticação existente e adicionar o novo método de autenticação. Em seguida, utilize o arquivo backend.json atualizado, que contém os parâmetros necessários, para executar o comando. `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 armazenamento deve primeiro atualizar a senha do usuário no ONTAP. Em seguida, é realizada uma atualização do sistema interno. Ao rotacionar certificados, vários certificados podem ser adicionados ao usuário. Em seguida, o sistema de backend é atualizado para usar o novo certificado, após o que o certificado antigo pode ser excluído do cluster ONTAP .

A atualização de um backend não interrompe o acesso a volumes já criados, nem afeta as conexões de volume feitas posteriormente. Uma atualização bem-sucedida do backend indica que o Trident pode se

comunicar com o backend ONTAP e lidar com futuras operações em grande volume.

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 uma 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 .

Utilizando a CLI do ONTAP

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. Atribua a função ao usuário:

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

Utilizando o Gerenciador de Sistemas

Execute as seguintes etapas no ONTAP System Manager:

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

      (Ou) Para criar uma função personalizada no nível da SVM, selecione **Armazenamento > VMs de armazenamento > `required SVM` > Configurações > Usuários e funções**.

   b. Selecione o ícone de seta (→) ao lado de **Usuários e Funções**.
   c. Selecione **+Adicionar** em **Funções**.
   d. Defina as regras para a função e clique em **Salvar**.
2. **Atribua a função ao usuário do 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, em seguida, selecione uma função no menu suspenso **Função**.
   c. Clique em **Salvar**.

Consulte as páginas seguintes para obter mais informações:

- "Funções personalizadas para administração do ONTAP"ou"Defina funções personalizadas"
- "Trabalhar com funções e usuários"

Gerenciar políticas de exportação NFS

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

A Trident oferece duas opções para trabalhar com políticas de exportação:

- O Trident pode gerenciar dinamicamente a própria política de exportação; nesse modo de operação, o administrador de armazenamento especifica uma lista de blocos CIDR que representam endereços IP admissíveis. O Trident adiciona automaticamente à política de exportação, no momento da publicação, os endereços IP dos nós aplicáveis que se enquadram nesses intervalos. Alternativamente, quando nenhum CIDR for 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 armazenamento podem criar uma política de exportação e adicionar regras manualmente. O Trident utiliza a política de exportação padrão, a menos que um nome de política de exportação diferente seja especificado na configuração.

Gerenciar políticas de exportação dinamicamente

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

> Não utilize Network Address Translation (NAT) ao usar políticas de exportação dinâmicas. Com NAT, o controlador de armazenamento vê o endereço NAT de front-end 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 utilizadas. Aqui está 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 utilizar 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). Siga sempre as melhores práticas recomendadas pela NetApp para dedicar uma SVM ao Trident.

Segue abaixo uma explicação de como essa funcionalidade opera, utilizando o exemplo acima:

- `autoExportPolicy`está definido para `true`. Isso indica que o Trident cria uma política de exportação para cada volume provisionado com esse backend para o `svm1` SVM e lidar com a adição e exclusão de regras usando `autoexportCIDRs` blocos de endereço. Até que um volume seja anexado a um nó, ele utiliza uma política de exportação vazia, sem regras para impedir o acesso indesejado a esse volume. Quando um volume é publicado em um nó, o 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 FlexVol volume pai.
  - Por exemplo:
    - UUID do backend 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`definido para `true`
    - prefixo de armazenamento `trident`
    - UUID do PVC a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - qtree chamado trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c cria uma política de exportação para o FlexVol chamado `trident-403b5326-8482-40db96d0-d83fb3f4daec`, uma política de exportação para a qtree chamada `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` e uma política de exportação vazia chamada `trident_empty` na SVM. As regras para a política de exportação FlexVol serão um superconjunto de quaisquer regras contidas nas políticas de exportação 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 o valor padrão é ["0.0.0.0/0", "::/0"]. Caso não esteja definido, o Trident adiciona todos os endereços unicast de escopo global encontrados nos nós de trabalho com publicações.

Neste exemplo, o `192.168.0.0/24` O espaço de endereçamento é fornecido. Isso indica que os endereços IP dos nós do Kubernetes que se enquadram nesse intervalo de endereços com publicações serão adicionados à política de exportação criada Trident . Quando o Trident registra um nó no qual está sendo executado, ele recupera os endereços IP do nó e os verifica em relação aos blocos de endereços fornecidos

em `autoExportCIDRs` No momento da publicação, após filtrar os IPs, o Trident cria as regras de política de exportação para os IPs do cliente para o nó no qual está publicando.

Você pode atualizar `autoExportPolicy` e `autoExportCIDRs` para os backends depois de 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 as conexões existentes não sejam interrompidas. Você também pode optar por desativar. `autoExportPolicy` para um backend e recorrer a uma política de exportação criada manualmente como alternativa. Isso exigirá a configuração do `exportPolicy` parâmetro na sua configuração de backend.

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

Para backends já existentes, atualize o backend com `tridentctl update backend` Garante que o Trident gerencie as políticas de exportação automaticamente. Isso cria duas novas políticas de exportação com os nomes do UUID e da árvore de consulta (qtree) do backend, quando necessárias. Os volumes presentes no servidor usarão as políticas de exportação recém-criadas após serem desmontados e montados novamente.

> Excluir 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 deverá reiniciar o pod do Trident nesse nó. A Trident

atualizará então a política de exportação dos servidores 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` motoristas.

> Você deve configurar os protocolos NFS e SMB/CIFS na SVM para criar um `ontap-nas-economy` Volume SMB para clusters ONTAP locais. A falha na configuração de 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 precisa ter o seguinte.

- Um cluster Kubernetes com um nó controlador Linux e pelo menos um nó de trabalho Windows executando o Windows Server 2022. O 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 segredos `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: Proxy CSI" ou"GitHub: CSI Proxy para Windows" para nós do Kubernetes executados no Windows.

Passos

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

   > Os compartilhamentos SMB são necessários para o Amazon FSx para ONTAP.

   Você pode criar os compartilhamentos administrativos SMB de duas maneiras: usando o"Console de gerenciamento da Microsoft" Acesse as Pastas Compartilhadas pelo snap-in ou usando a CLI do ONTAP . Para criar compartilhamentos SMB usando a CLI do ONTAP :

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

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

   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 FSx para ONTAP , consulte"Opções e exemplos de configuração do FSx para ONTAP" .

Parâmetro	Descrição	Exemplo
`smbShare`	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Console de Gerenciamento da Microsoft ou a CLI do ONTAP ; 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 compartilhados. Este parâmetro é opcional para o ONTAP local. Este parâmetro é obrigatório para backends do Amazon FSx para ONTAP e não pode estar em branco.	`smb-share`
`nasType`	**Deve ser configurado para `smb` .** Se for nulo, o valor padrão é `nfs` .	`smb`
`securityStyle`	Estilo de segurança para novos volumes. **Deve ser configurado para `ntfs` ou `mixed` para volumes SMB.**	`ntfs`ou `mixed` para volumes SMB
`unixPermissions`	Modo para novos volumes. **Deve ficar vazio para volumes SMB.**	""

Ativar SMB seguro

A partir da versão 25.06, o NetApp Trident oferece suporte ao provisionamento seguro de volumes SMB criados usando `ontap-nas` e `ontap-nas-economy` back-ends. 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 serem lembrados

- Importando `ontap-nas-economy` O volume não é suportado.
- Somente clones somente leitura são suportados para `ontap-nas-economy` volumes.
- Se o SMB seguro estiver ativado, o Trident ignorará o compartilhamento SMB mencionado no backend.

- A atualização da anotação PVC, da anotação da classe de armazenamento e do campo de 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 Active Directory no backend, na classe de armazenamento e no PVC com permissões diferentes, a prioridade de permissão será: PVC, classe de armazenamento e, por último, backend.
- O Secure SMB é compatível com `ontap-nas` Importações de volume gerenciadas e não aplicáveis a importações de volume não gerenciadas.

Passos

1. Especifique o usuário adAdminUser no 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 classe de armazenamento.

   Adicione o `trident.netapp.io/smbShareAdUser` Anotação na classe de armazenamento para habilitar o SMB seguro sem falhas. O valor do usuário especificado para a anotação `trident.netapp.io/smbShareAdUser` deve ser o mesmo que o nome de usuário especificado no `smbcreds` segredo. Você pode escolher uma das seguintes opções 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. Criar 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.

Opções de configuração do backend

Consulte a tabela a seguir para obter as opções de configuração do backend:

Parâmetro	Descrição	Padrão
`version`		Sempre 1
`storageDriverName`	Nome do driver de armazenamento	`ontap-nas`, `ontap-nas-economy` , ou `ontap-nas-flexgroup`
`backendName`	Nome personalizado ou o backend de armazenamento	Nome do motorista + "_" + 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 o Trident foi instalado usando a opção IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como por exemplo: `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . Para uma transição perfeita para o MetroCluster , consulte oExemplo MetroCluster .	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	Endereço IP do protocolo LIF. A NetApp recomenda especificar `dataLIF` . Caso não sejam fornecidos, o Trident obtém 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 várias dataLIFs. Pode ser alterado após a configuração inicial. Consulte . Pode ser configurado para usar endereços IPv6 se o Trident foi instalado usando a opção IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como por exemplo: `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . **Omitir para Metrocluster.** Veja oExemplo MetroCluster .	Endereço especificado ou derivado de SVM, caso não seja especificado (não recomendado).
`svm`	Máquina virtual de armazenamento a ser usada **Omitir para Metrocluster.** Veja oExemplo MetroCluster .	Derivado de uma SVM `managementLIF` é especificado
`autoExportPolicy`	Ativar a criação e atualização automática da política de exportação [Booleano]. Usando o `autoExportPolicy` e `autoExportCIDRs` O Trident pode gerenciar políticas de exportação automaticamente, dependendo das opções disponíveis.	falso

Parâmetro	Descrição	Padrão
`autoExportCIDRs`	Lista de CIDRs para filtrar os IPs dos nós do Kubernetes quando `autoExportPolicy` está habilitado. Usando o `autoExportPolicy` e `autoExportCIDRs` O Trident pode gerenciar políticas de exportação automaticamente, dependendo das opções disponíveis.	["0.0.0.0/0", "::/0"]`
`labels`	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
`clientCertificate`	Valor do certificado do cliente codificado em Base64. Utilizado para autenticação baseada em certificado.	""
`clientPrivateKey`	Valor da chave privada do cliente codificado em Base64. Utilizado para autenticação baseada em certificado.	""
`trustedCACertificate`	Valor codificado em Base64 do certificado da Autoridade Certificadora (CA) confiável. Opcional. Utilizado para autenticação baseada em certificado.	""
`username`	Nome de usuário para conectar ao cluster/SVM. Usado para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autenticar o Trident em um SVM de backend usando credenciais do Active Directory".	
`password`	Senha para conectar ao cluster/SVM. Usado para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autenticar 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 depois de configurado. Ao usar o ontap-nas-economy e um storagePrefix com 24 ou mais caracteres, as qtrees não terão o prefixo de armazenamento incorporado, embora ele esteja presente no nome do volume.	"tridente"

Parâmetro	Descrição	Padrão
`aggregate`	Agregado para provisionamento (opcional; se definido, deve ser atribuído à SVM). Para o `ontap-nas-flexgroup` motorista, esta opção é ignorada. Caso não esteja atribuído, qualquer um dos agregados disponíveis pode ser usado para provisionar um volume FlexGroup . 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 Controlador Trident . Quando você configura 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 a consulta ao agregado do SVM. Você deve alterar o agregado para um que esteja presente na SVM ou removê-lo completamente para que o backend volte a ficar online.	""
`limitAggregateUsage`	O provisionamento falhará se a utilização for superior a esta percentagem. **Não se aplica ao Amazon FSx para ONTAP**.	"" (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 volume FlexGroup . Compatível com o driver de armazenamento **ontap-nas-flexgroup**. Quando a lista agregada é atualizada no SVM, a lista é atualizada automaticamente no Trident por meio de polling no SVM, sem a necessidade de reiniciar o Controlador Trident . Quando você configura uma lista de agregação específica no Trident para provisionar volumes, se a lista de agregação for renomeada ou movida para fora do SVM, o backend entrará em estado de falha no Trident durante a consulta da lista de agregação do SVM. Você deve alterar a lista agregada para uma que esteja presente na SVM ou removê-la completamente para que o backend volte a funcionar.	""

Parâmetro	Descrição	Padrão
`limitVolumeSize`	O provisionamento falhará se o tamanho do volume solicitado for superior a este valor. Também restringe o tamanho máximo dos volumes que gerencia para qtrees, e o `qtreesPerFlexvol` Essa opção permite personalizar o número máximo de qtrees por FlexVol volume.	"" (não aplicado por padrão)
`debugTraceFlags`	Sinalizadores de depuração a serem usados na resolução de problemas. Exemplo: {"api":false, "method":true} Não use `debugTraceFlags` a menos que você esteja solucionando problemas e precise de um despejo de logs detalhado.	nulo
`nasType`	Configure a criação de volumes NFS ou SMB. As opções são `nfs` , `smb` ou nulo. Definir como nulo utiliza, por padrão, volumes NFS.	`nfs`
`nfsMountOptions`	Lista de opções de montagem NFS separadas por vírgulas. 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, o Trident usará as opções de montagem especificadas no arquivo de configuração do backend de armazenamento. Se nenhuma opção de montagem for especificada na classe de armazenamento ou no arquivo de configuração, o Trident não definirá nenhuma opção de montagem em um volume persistente associado.	""
`qtreesPerFlexvol`	Número 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 Console de Gerenciamento da Microsoft ou a CLI do ONTAP ; 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 compartilhados. Este parâmetro é opcional para o ONTAP local. Este parâmetro é obrigatório para backends do Amazon FSx para ONTAP e não pode estar em branco.	`smb-share`

Parâmetro	Descrição	Padrão
`useREST`	Parâmetro booleano para usar APIs REST do ONTAP . `useREST` Quando definido para `true` O Trident usa APIs REST do ONTAP para se comunicar com o backend; quando configurado para `false` O Trident utiliza chamadas ONTAPI (ZAPI) para se comunicar com o backend. Este recurso requer o ONTAP 9.11.1 e posterior. Além disso, a função de login do ONTAP utilizada deve ter acesso ao `ontapi` aplicativo. Isso é satisfeito pelo predefinido `vsadmin` e `cluster-admin` papéis. A partir da versão Trident 24.06 e do ONTAP 9.15.1 ou posterior, `useREST` está definido para `true` por padrão; alterar `useREST` para `false` para usar chamadas ONTAPI (ZAPI).	`true` para ONTAP 9.15.1 ou posterior, caso contrário `false` .
`limitVolumePoolSize`	Tamanho máximo de FlexVol solicitável ao usar Qtrees no backend ontap-nas-economy.	"" (não aplicado por padrão)
`denyNewVolumePools`	Restringe `ontap-nas-economy` backends da criação de novos volumes FlexVol para conter suas Qtrees. Apenas os Flexvols preexistentes são usados para provisionar novos PVs.	
`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 em `defaults` seção da configuração. Para ver um exemplo, consulte os exemplos de configuração abaixo.

Parâmetro	Descrição	Padrão
`spaceAllocation`	Alocação de espaço para Qtrees	"verdadeiro"
`spaceReserve`	Modo de reserva de espaço; "nenhum" (fino) ou "volume" (grosso)	"nenhum"
`snapshotPolicy`	Política de instantâneo a ser usada	"nenhum"
`qosPolicy`	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha qosPolicy ou adaptiveQosPolicy por pool de armazenamento/backend.	""
`adaptiveQosPolicy`	Grupo de políticas de QoS adaptativas a serem atribuídas aos volumes criados. Escolha uma das opções qosPolicy ou adaptiveQosPolicy para cada pool de armazenamento/backend. Não suportado por ontap-nas-economy.	""

Parâmetro	Descrição	Padrão
`snapshotReserve`	Percentagem do volume reservada para instantâneos	"0" se `snapshotPolicy` é "nenhum", caso contrário ""
`splitOnClone`	Separar um clone de seu progenitor no momento da criação.	"falso"
`encryption`	Ative a Criptografia de Volume NetApp (NVE) no novo volume; o padrão é `false` . Para usar esta opção, o NVE precisa estar licenciado e habilitado no cluster. Se o NAE estiver habilitado no backend, qualquer volume provisionado no Trident terá o NAE habilitado. Para mais informações, consulte:"Como o Trident funciona com NVE e NAE" .	"falso"
`tieringPolicy`	Política de níveis para usar "nenhum"	
`unixPermissions`	Modo para novos volumes	"777" para volumes NFS; vazio (não aplicável) para volumes SMB.
`snapshotDir`	Controla o acesso ao `.snapshot` diretório	"verdadeiro" para NFSv4 "falso" para NFSv3
`exportPolicy`	Política de exportação a ser utilizada	"padrão"
`securityStyle`	Estilo de segurança para novos volumes. Suporte a NFS `mixed` e `unix` estilos de segurança. Suporte para PMEs `mixed` e `ntfs` estilos de segurança.	O padrão do NFS é `unix` . O padrão SMB é `ntfs` .
`nameTemplate`	Modelo para criar nomes de volume personalizados.	""

A utilização de grupos de políticas de QoS com o Trident requer o 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 em 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 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 versão 21.07, quando o usuário solicita um PVC (por exemplo, 5 GiB), com o snapshotReserve em 50%, ele obtém apenas 2,5 GiB de espaço gravável. Isso ocorre porque o que o usuário solicitou foi o volume completo 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 `snapshotReserve` número como 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/.5 = 10 GiB e o tamanho disponível é 5 GiB, que é o que o usuário solicitou na solicitação de PVC O `volume show` O comando deve exibir resultados semelhantes a este exemplo:

Os backends existentes de instalações anteriores provisionarão volumes conforme explicado acima ao atualizar o Trident. Para volumes criados antes da atualização, você deve redimensioná-los para que a alteração seja observada. Por exemplo, um PVC de 2 GiB com `snapshotReserve=50` O resultado anterior era um volume que fornecia 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 o 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 grupo flexível 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 MetroCluster

Você pode configurar o backend para evitar a necessidade de atualizar manualmente a definição do backend após a troca de modo (switchover) e o retorno ao modo anterior (switchback)."Replicação e recuperação de SVM" .

Para uma transição perfeita e um retorno perfeito, especifique a SVM usando `managementLIF` e omitir o `dataLIF` e `svm` parâmetros. 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 extraem 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 o Trident a usar políticas de exportação dinâmicas para criar e gerenciar a política de exportação automaticamente. Isso funciona da mesma forma para o `ontap-nas-economy` e `ontap-nas-flexgroup` motoristas.

```
---
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 endereço 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
```

Exemplo de uso de volumes SMB no Amazon FSx para ONTAP

O `smbShare` Este parâmetro é necessário para o 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 armazenamento, como: `spaceReserve` em nenhum, `spaceAllocation` em falso, e `encryption` falso. Os pools virtuais são definidos na seção de armazenamento.

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

Nesses exemplos, alguns dos pools de armazenamento definem seus próprios limites. `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 FlexGroup NAS 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"
```

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 backends para StorageClasses

As seguintes definições de StorageClass referem-se aExemplos de backends com pools virtuais . Usando o `parameters.selector` No campo `StorageClass`, cada `StorageClass` especifica quais pools virtuais podem ser usados para hospedar um volume. O volume terá os aspectos definidos na piscina virtual escolhida.

- O `protection-gold` A StorageClass será mapeada para o primeiro e o segundo pool virtual no `ontap-nas-flexgroup` backend. Essas são as únicas piscinas 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` A StorageClass será mapeada para o terceiro e quarto pool virtual no `ontap-nas-flexgroup` backend. Essas são as únicas pools que oferecem um nível de proteção diferente do ouro.

```
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` A classe de armazenamento será mapeada para o quarto pool virtual no `ontap-nas` backend. Este é o único pool que oferece configuração de pool de armazenamento para aplicativos 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` A StorageClass será mapeada para o terceiro pool virtual no `ontap-nas-flexgroup` backend. Este é o único pool que oferece proteção de nível prata e 20.000 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` A StorageClass será mapeada para o terceiro pool virtual no `ontap-nas` backend e o segundo pool virtual no `ontap-nas-economy` backend. Essas são as únicas ofertas de piscina com 5000 pontos de crédito.

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

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

Atualizar `dataLIF` após a configuração inicial

Você pode alterar o dataLIF após a configuração inicial executando o seguinte comando para fornecer ao novo arquivo JSON de backend 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, em seguida, ligá-los novamente para que o novo dataLIF entre em vigor.

Exemplos de segurança 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 armazenamento

```
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