Motoristas ONTAP SAN

Trident

NetApp
January 15, 2026

Índice

Motoristas ONTAP SAN

Visão geral do driver ONTAP SAN

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

Detalhes do driver ONTAP SAN

A Trident fornece os seguintes drivers de armazenamento SAN 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-san`	iSCSI SCSI sobre FC	Bloquear	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto
`ontap-san`	iSCSI SCSI sobre FC	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume do sistema de arquivos.	`xfs`, `ext3` , `ext4`
`ontap-san`	NVMe/TCP ConsulteConsiderações adicionais para NVMe/TCP .	Bloquear	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto
`ontap-san`	NVMe/TCP ConsulteConsiderações adicionais para NVMe/TCP .	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume do sistema de arquivos.	`xfs`, `ext3` , `ext4`
`ontap-san-economy`	iSCSI	Bloquear	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto

Motorista	Protocolo	modo de volume	Modos de acesso suportados	Sistemas de arquivos suportados
`ontap-san-economy`	iSCSI	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume do sistema de arquivos.	`xfs`, `ext3` , `ext4`

- 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.

Considerações adicionais para NVMe/TCP

O Trident suporta o protocolo de memória não volátil expressa (NVMe) usando o `ontap-san` motorista incluindo:

- IPv6
- Instantâneos e clones de volumes NVMe
- Redimensionar um volume NVMe
- Importar um volume NVMe criado fora do Trident para que seu ciclo de vida possa ser gerenciado pelo Trident.

- Multicaminhamento nativo NVMe
- Encerramento correto ou incorreto dos nós K8s (24.06)

O Trident não suporta:

- DH-HMAC-CHAP que é suportado nativamente por NVMe
- Mapeamento de dispositivos (DM) com múltiplos caminhos
- Criptografia LUKS

> O NVMe é compatível apenas com APIs REST ONTAP e não com ONTAPI (ZAPI).

Prepare-se para configurar o backend com os drivers ONTAP SAN.

Compreenda os requisitos e as opções de autenticação para configurar um backend ONTAP com drivers ONTAP SAN.

Requisitos

Para todos os backends ONTAP , o Trident exige que pelo menos um agregado seja atribuído à SVM.

> "Sistemas ASA r2"diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de armazenamento. Nos sistemas ASA r2, as zonas de disponibilidade de armazenamento são usadas em vez de agregados. Consulte"esse" Artigo da Base de Conhecimento sobre como atribuir agregados a SVMs em sistemas ASA r2.

Lembre-se de que você também pode executar mais de um driver e criar classes de armazenamento que apontem para um ou outro. Por exemplo, você poderia configurar um `san-dev` classe que usa o `ontap-san` motorista e um `san-default` classe que usa o `ontap-san-economy` um.

Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas iSCSI apropriadas instaladas. Consulte "Prepare o nó de trabalho" para mais detalhes.

Autenticar o backend ONTAP

O Trident oferece dois modos de autenticação de um backend ONTAP .

- Com base em credenciais: o nome de usuário e a senha de um usuário do ONTAP com as permissões necessárias. Recomenda-se o uso de uma função de login de segurança predefinida, como `admin` ou `vsadmin` Para garantir a máxima compatibilidade com as versões do ONTAP .
- Com base em certificado: o Trident também pode se comunicar com um cluster ONTAP usando um certificado instalado no backend. 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-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

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 ou 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=admin"
```

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

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.

```
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.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
"trustedCACertificate": "QNFinfO...SiqOyN",
"storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |       0 |
+------------+----------------+--------------------------------------
+--------+---------+
```

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 fazer 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 backend update`.

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

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

> 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"

Autenticar conexões com CHAP bidirecional

O Trident pode autenticar sessões iSCSI com CHAP bidirecional para o `ontap-san` e `ontap-san-economy` motoristas. Isso requer a ativação do `useCHAP` opção na sua definição de backend. Quando definido para `true` O Trident configura a segurança do iniciador padrão da SVM para CHAP bidirecional e define o nome de usuário e os segredos a partir do arquivo de backend. A NetApp recomenda o uso do protocolo CHAP bidirecional para autenticar conexões. Veja a seguinte configuração de exemplo:

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

> O `useCHAP` O parâmetro é uma opção booleana que pode ser configurada apenas uma vez. Por padrão, está definido como falso. Depois de definir como verdadeiro, você não poderá definir como falso.

Além de `useCHAP=true` , o `chapInitiatorSecret` , `chapTargetInitiatorSecret` , `chapTargetUsername` , e `chapUsername` Os campos devem ser incluídos na definição do backend. Os segredos podem ser alterados após a criação de um backend executando o seguinte comando: `tridentctl update` .

Como funciona

Ao configurar `useCHAP` Para confirmar, o administrador de armazenamento instrui o Trident a configurar o CHAP no backend de armazenamento. Isso inclui o seguinte:

- Configurando o CHAP no SVM:
  - Se o tipo de segurança do iniciador padrão da SVM for "nenhum" (definido por padrão) **e** não houver LUNs preexistentes no volume, o Trident definirá o tipo de segurança padrão como `CHAP` e prossiga para a configuração do iniciador CHAP e do nome de usuário e segredos de destino.
  - Se a SVM contiver LUNs, o Trident não habilitará o CHAP na SVM. Isso garante que o acesso aos LUNs já presentes na SVM não seja restringido.
- Configurar o nome de usuário e os segredos do iniciador e do alvo CHAP; essas opções devem ser especificadas na configuração do backend (como mostrado acima).

Após a criação do backend, o Trident cria um correspondente. `tridentbackend` O CRD armazena os segredos CHAP e os nomes de usuário como segredos do Kubernetes. Todos os PVs criados pelo Trident neste backend serão montados e conectados via CHAP.

Gire as credenciais e atualize os backends

Você pode atualizar as credenciais CHAP atualizando os parâmetros CHAP em `backend.json` arquivo. Isso exigirá a atualização dos segredos CHAP e o uso do `tridentctl update` comando para refletir essas mudanças.

> Ao atualizar os segredos CHAP de um backend, você deve usar `tridentctl` para atualizar o backend. Não atualize as credenciais no cluster de armazenamento usando a CLI do ONTAP ou o ONTAP System Manager, pois o Trident não conseguirá detectar essas alterações.

```
cat backend-san.json
{
    "version": 1,
    "storageDriverName": "ontap-san",
    "backendName": "ontap_san_chap",
    "managementLIF": "192.168.0.135",
    "svm": "ontap_iscsi_svm",
    "useCHAP": true,
    "username": "vsadmin",
    "password": "password",
    "chapInitiatorSecret": "cl9qxUpDaTeD",
    "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
    "chapTargetUsername": "iJF4heBRT0TCwxyz",
    "chapUsername": "uh2aNCLSd6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+----------------+----------------+--------------------------------------
+--------+---------+
|   NAME         | STORAGE DRIVER |                 UUID                 |
STATE   | VOLUMES |
+----------------+----------------+--------------------------------------
+--------+---------+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online |       7 |
+----------------+----------------+--------------------------------------
+--------+---------+
```

As conexões existentes permanecerão inalteradas; elas continuarão ativas se as credenciais forem atualizadas pelo Trident no SVM. Novas conexões utilizam as credenciais atualizadas e as conexões existentes permanecem ativas. Desconectar e reconectar os sistemas fotovoltaicos antigos fará com que eles passem a usar as credenciais atualizadas.

Opções e exemplos de configuração do ONTAP SAN

Aprenda como criar e usar drivers ONTAP SAN com sua instalação do Trident . Esta

seção fornece exemplos de configuração de backend e detalhes para mapear backends para StorageClasses.

"Sistemas ASA r2"Diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de armazenamento. Essas variações afetam o uso de certos parâmetros, conforme indicado. "Saiba mais sobre as diferenças entre os sistemas ASA r2 e outros sistemas ONTAP.".

> Somente o `ontap-san` O driver (com protocolos iSCSI e NVMe/TCP) é compatível com sistemas ASA r2.

Na configuração do backend Trident , não é necessário especificar que seu sistema é um ASA r2. Ao selecionar `ontap-san` como o `storageDriverName` O Trident detecta automaticamente o ASA r2 ou o sistema ONTAP tradicional. Alguns parâmetros de configuração de backend não se aplicam aos sistemas ASA r2, conforme indicado na tabela abaixo.

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-san`ou `ontap-san-economy`
`backendName`	Nome personalizado ou o backend de armazenamento	Nome do motorista + "_" + dataLIF
`managementLIF`	Endereço IP de um cluster ou LIF de gerenciamento de SVM. É possível especificar um nome de domínio totalmente qualificado (FQDN). 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 . > Se você estiver usando as credenciais "vsadmin", `managementLIF` deve ser a do SVM; se estiver usando credenciais de "administrador", `managementLIF` deve ser o do cluster.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parâmetro	Descrição	Padrão
`dataLIF`	Endereço IP do protocolo LIF. 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]` . **Não especifique para iSCSI.** Trident usa"Mapa LUN Seletivo ONTAP" para descobrir as LIFs iSCSI necessárias para estabelecer uma sessão de múltiplos caminhos. Um aviso é gerado se `dataLIF` está explicitamente definido. **Omitir para Metrocluster.** Veja oExemplo MetroCluster .	Derivado pelo SVM
`svm`	Máquina virtual de armazenamento a ser usada **Omitir para Metrocluster.** Veja oExemplo MetroCluster .	Derivado de uma SVM `managementLIF` é especificado
`useCHAP`	Usar CHAP para autenticar iSCSI para drivers ONTAP SAN [Booleano]. Definir para `true` Para que o Trident configure e utilize o CHAP bidirecional como autenticação padrão para a SVM fornecida no backend. Consulte "Prepare-se para configurar o backend com os drivers ONTAP SAN." para mais detalhes. **Não compatível com FCP ou NVMe/TCP.**	`false`
`chapInitiatorSecret`	Segredo do iniciador CHAP. Obrigatório se `useCHAP=true`	""
`labels`	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
`chapTargetInitiatorSecret`	Segredo iniciador do alvo CHAP. Obrigatório se `useCHAP=true`	""
`chapUsername`	Nome de usuário de entrada. Obrigatório se `useCHAP=true`	""
`chapTargetUsername`	Nome de usuário alvo. Obrigatório se `useCHAP=true`	""
`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 necessário para se comunicar com o cluster ONTAP . 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".	""

Parâmetro	Descrição	Padrão
`password`	Senha necessária para se comunicar com o cluster ONTAP . 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".	""
`svm`	Máquina virtual de armazenamento para usar	Derivado de uma SVM `managementLIF` é especificado
`storagePrefix`	Prefixo usado ao provisionar novos volumes no SVM. Não pode ser modificado posteriormente. Para atualizar esse parâmetro, você precisará criar um novo backend.	`trident`
`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. **Não especificar para sistemas ASA r2**.	""
`limitAggregateUsage`	O provisionamento falhará se a utilização for superior a esta percentagem. Se você estiver usando um backend Amazon FSx for NetApp ONTAP , não especifique. `limitAggregateUsage` . O fornecido `fsxadmin` e `vsadmin` Não possuem as permissões necessárias para recuperar o uso agregado e limitá-lo usando o Trident. **Não especificar para sistemas ASA r2**.	"" (não aplicado por 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 LUNs.	"" (não aplicado por padrão)

Parâmetro	Descrição	Padrão
`lunsPerFlexvol`	Número máximo de LUNs por Flexvol, deve estar no intervalo [50, 200]	`100`
`debugTraceFlags`	Sinalizadores de depuração a serem usados na resolução de problemas. Exemplo: {"api":false, "method":true} Não utilize a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	`null`
`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). `useREST`Está totalmente qualificado para NVMe/TCP. O NVMe é compatível apenas com APIs REST ONTAP e não com ONTAPI (ZAPI). **Se especificado, sempre defina como `true` para sistemas ASA r2**.	`true`para ONTAP 9.15.1 ou posterior, caso contrário `false`.
`sanType`	Use para selecionar `iscsi` para iSCSI, `nvme` para NVMe/TCP ou `fcp` para SCSI sobre Fibre Channel (FC).	`iscsi`se estiver em branco

Parâmetro	Descrição	Padrão
`formatOptions`	Usar `formatOptions` para especificar argumentos de linha de comando para o `mkfs` comando, que será aplicado sempre que um volume for formatado. Isso permite formatar o volume de acordo com suas preferências. Certifique-se de especificar as opções de formatação semelhantes às opções do comando mkfs, excluindo o caminho do dispositivo. Exemplo: "-E nodiscard" **Compatível com `ontap-san` e `ontap-san-economy` drivers com protocolo iSCSI. Além disso, é compatível com sistemas ASA r2 ao usar os protocolos iSCSI e NVMe/TCP.**	
`limitVolumePoolSize`	Tamanho máximo de FlexVol solicitável ao usar LUNs no backend ontap-san-economy.	"" (não aplicado por padrão)
`denyNewVolumePools`	Restringe `ontap-san-economy` backends da criação de novos volumes FlexVol para conter seus LUNs. Apenas os Flexvols preexistentes são usados para provisionar novos PVs.	

Recomendações para usar formatOptions

A Trident recomenda a seguinte opção para agilizar o processo de formatação:

-E nodiscard:

- Mantenha os blocos salvos e não tente descartá-los durante a criação do sistema de arquivos (o descarte inicial de blocos é útil em dispositivos de estado sólido e em armazenamento com provisionamento esparso/dinâmico). Esta opção substitui a opção obsoleta "-K" e é aplicável a todos os sistemas de arquivos (xfs, ext3 e ext4).

Autenticar o Trident em um SVM de backend usando credenciais do Active Directory

Você pode configurar o Trident para autenticar em um SVM de backend usando credenciais do Active Directory (AD). Antes que uma conta do AD possa acessar o SVM, você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM. Para administração de cluster com uma conta do AD, você deve criar um túnel de domínio. Consulte "Configurar o acesso do controlador de domínio do Active Directory no ONTAP" para mais detalhes.

passos

1. Configurar as definições do Sistema de Nomes de Domínio (DNS) para um SVM de backend:

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

2. Execute o seguinte comando para criar uma conta de computador para o SVM no Active Directory:

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

3. Use este comando para criar um usuário ou grupo do AD para gerenciar o cluster ou SVM

```
security login create -vserver <svm_name> -user-or-group-name
<ad_user_or_group> -application <application> -authentication-method domain
-role vsadmin
```

4. No arquivo de configuração do backend do Trident , defina o `username` e `password` parâmetros para o nome do usuário ou grupo do AD e senha, respectivamente.

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 LUNs	"verdadeiro" **Se especificado, defina como `true` para sistemas ASA r2**.
`spaceReserve`	Modo de reserva de espaço: "nenhum" (fino) ou "volume" (grosso). **Definir para `none` para sistemas ASA r2**.	"nenhum"
`snapshotPolicy`	Política de instantâneo a ser utilizada. **Definir para `none` para sistemas ASA r2**.	"nenhum"
`qosPolicy`	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha uma das opções qosPolicy ou adaptiveQosPolicy para cada pool de armazenamento/backend. 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.	""
`adaptiveQosPolicy`	Grupo de políticas de QoS adaptativas a serem atribuídas aos volumes criados. Escolha qosPolicy ou adaptiveQosPolicy por pool de armazenamento/backend.	""
`snapshotReserve`	Percentagem do volume reservada para instantâneos. **Não especificar para sistemas ASA r2**.	"0" se `snapshotPolicy` é "nenhum", caso contrário ""
`splitOnClone`	Separar um clone de seu progenitor no momento da criação.	"falso"

Parâmetro	Descrição	Padrão
`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" **Se especificado, defina como `true` para sistemas ASA r2**.
`luksEncryption`	Ative a criptografia LUKS. Consulte"Use o Linux Unified Key Setup (LUKS)" .	"" **Definido para `false` para sistemas ASA r2**.
`tieringPolicy`	Política de escalonamento para usar "nenhum" **Não especificar para sistemas ASA r2**.	
`nameTemplate`	Modelo para criar nomes de volume personalizados.	""

Exemplos de provisionamento em volume

Aqui está um exemplo com valores padrão definidos:

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

Para todos os volumes criados usando o `ontap-san` O driver Trident adiciona 10% a mais de capacidade ao FlexVol para acomodar os metadados do LUN. O LUN será provisionado com o tamanho exato que o usuário solicitar no PVC. O Trident adiciona 10% ao FlexVol (mostrado como tamanho disponível no ONTAP). Os usuários agora receberão a quantidade de capacidade utilizável que solicitaram. Essa alteração também impede que as LUNs se tornem somente leitura, a menos que o espaço disponível esteja totalmente utilizado. Isso não se aplica a ontap-san-economy.

Para back-ends que definem `snapshotReserve` O Trident calcula o tamanho dos volumes da seguinte forma:

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

O 1.1 representa os 10% extras que a Trident adiciona ao FlexVol para acomodar os metadados do LUN Para `snapshotReserve` = 5%, e solicitação de PVC = 5 GiB, o tamanho total do volume é 5,79 GiB e o tamanho disponível é 5,5 GiB. O `volume show` O comando deve exibir resultados semelhantes a este exemplo:

Atualmente, o redimensionamento é a única maneira de usar o novo cálculo para um volume existente.

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 NetApp recomenda que você especifique nomes DNS para LIFs em vez de endereços IP.

Exemplo de SAN ONTAP

Esta é uma configuração básica usando o `ontap-san` motorista.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

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 `svm` parâmetros. Por exemplo:

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

Exemplo de economia ONTAP SAN

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

Exemplo de autenticação baseada em certificado

Neste exemplo de configuração básica `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
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

Exemplos CHAP bidirecionais

Esses exemplos criam um backend com `useCHAP` definido para `true` .

Exemplo ONTAP SAN CHAP

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

Exemplo de economia ONTAP SAN CHAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

Exemplo NVMe/TCP

Você precisa ter uma SVM configurada com NVMe no seu backend ONTAP . Esta é uma configuração básica de backend para NVMe/TCP.

```
---
version: 1
backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true
```

Exemplo de SCSI sobre FC (FCP)

Você precisa ter uma SVM configurada com FC em seu backend ONTAP . Esta é uma configuração básica de backend para FC.

```
---
version: 1
backendName: fcp-backend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_fc
username: vsadmin
password: password
sanType: fcp
useREST: true
```

Exemplo de configuração de backend com nameTemplate

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

Exemplo de formatOptions para o driver ontap-san-economy

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

Exemplos de backends com pools virtuais

Nesses arquivos de definição de backend de exemplo, 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 são definidos no FlexVol volume. 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 SAN ONTAP

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

Exemplo de economia ONTAP SAN

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
labels:
  store: san_economy_store
region: us_east_1
storage:
  - labels:
      app: oracledb
      cost: "30"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
  - labels:
      app: postgresdb
      cost: "20"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
  - labels:
      app: mysqldb
      cost: "10"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
  - labels:
      department: legal
      creditpoints: "5000"
    zone: us_east_1c
```

```
    defaults:
      spaceAllocation: "true"
      encryption: "false"
```

Exemplo NVMe/TCP

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:
      app: testApp
      cost: "20"
    defaults:
      spaceAllocation: "false"
      encryption: "false"
```

Mapear backends para StorageClasses

As seguintes definições de StorageClass referem-se a:Exemplos 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 pool virtual no `ontap-san` backend. Esta é a única piscina que oferece 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 segundo e terceiro pool virtual em `ontap-san` 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 StorageClass será mapeada para o terceiro pool virtual em `ontap-san-economy` 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 segundo pool virtual em `ontap-san` 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 em `ontap-san` backend e o quarto pool virtual no `ontap-san-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"
```

- O `my-test-app-sc` A classe de armazenamento será mapeada para o `testAPP` piscina virtual no `ontap-san` motorista com `sanType: nvme` . Esta é a única piscina que oferece `testApp` .

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

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

Informações sobre direitos autorais

Informações sobre marcas comerciais