



Segurança

Trident

NetApp
October 30, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/trident-2606/trident-reco/security-reco.html> on October 30, 2026. Always check docs.netapp.com for the latest.

Índice

Segurança	1
Recomendações de segurança do Trident	1
Execute Trident em seu próprio namespace	1
Use autenticação CHAP com backends SAN do ONTAP	1
Use autenticação CHAP com NetApp HCI e SolidFire backends	1
Use Trident com NVE e NAE	1
Configuração unificada de chave do Trident Linux (LUKS)	2
Ativar criptografia LUKS	2
Configuração de backend para importação de volumes LUKS	4
Configuração de PVC para importação de volumes LUKS	4
Rotacionar uma frase secreta LUKS	5
Habilitar expansão de volume	7
A criptografia Kerberos em trânsito do Trident	7
Configurar criptografia Kerberos em trânsito com volumes ONTAP locais	7
Configurar criptografia Kerberos em trânsito com volumes do Azure NetApp Files	11

Segurança

Recomendações de segurança do Trident

Utilize as recomendações listadas aqui para garantir que sua instalação do Trident seja segura.

Execute Trident em seu próprio namespace

É importante impedir que aplicativos, administradores de aplicativos, usuários e aplicativos de gerenciamento acessem as definições de objetos do Trident ou os pods para garantir um armazenamento confiável e bloquear possíveis atividades maliciosas.

Para separar os outros aplicativos e usuários do Trident, sempre instale Trident em seu próprio namespace do Kubernetes (`trident`). Colocar Trident em seu próprio namespace garante que apenas a equipe administrativa do Kubernetes tenha acesso ao pod do Trident e aos artefatos (como segredos de backend e CHAP, se aplicável) armazenados nos objetos CRD do namespace. Você deve garantir que somente os administradores tenham acesso ao namespace do Trident e, assim, acesso ao `tridentctl` aplicativo.

Use autenticação CHAP com backends SAN do ONTAP

Trident oferece suporte à autenticação baseada em CHAP para cargas de trabalho ONTAP SAN (usando os drivers `ontap-san` e `ontap-san-economy`). NetApp recomenda o uso de CHAP bidirecional com Trident para autenticação entre um host e o backend de storage.

Para backends ONTAP que utilizam os drivers de armazenamento SAN, Trident pode configurar o CHAP bidirecional e gerenciar nomes de usuário e segredos CHAP por meio de `tridentctl`. Consulte ["Prepare-se para configurar o backend com os drivers ONTAP SAN"](#) para entender como o Trident configura o CHAP em backends ONTAP.

Use autenticação CHAP com NetApp HCI e SolidFire backends

NetApp recomenda implantar CHAP bidirecional para garantir autenticação entre um host e os backends NetApp HCI e SolidFire. Trident usa um objeto secreto que inclui duas senhas CHAP por tenant. Quando Trident é instalado, ele gerencia os segredos CHAP e os armazena em um `tridentvolume` objeto CR para o respectivo PV. Quando você cria um PV, Trident usa os segredos CHAP para iniciar uma sessão iSCSI e se comunicar com o sistema NetApp HCI e SolidFire via CHAP.



Os volumes criados pelo Trident não estão associados a nenhum Volume Access Group.

Use Trident com NVE e NAE

NetApp ONTAP fornece criptografia de dados em repouso para proteger dados confidenciais caso um disco seja roubado, devolvido ou reutilizado. Para obter detalhes, consulte ["Configurar visão geral da criptografia de volume NetApp"](#).

- Se o NAE estiver habilitado no backend, qualquer volume provisionado no Trident será habilitado para NAE.
 - Você pode definir o sinalizador de criptografia NVE para "" criar volumes com NAE habilitado.
- Se o NAE não estiver habilitado no backend, qualquer volume provisionado no Trident terá o NVE

habilitado, a menos que o sinalizador de criptografia NVE esteja definido como `false` (o valor padrão) na configuração do backend.

Volumes criados no Trident em um backend habilitado para NAE devem ser criptografados com NVE ou NAE.



- Você pode definir o sinalizador de criptografia NVE `true` na configuração do backend Trident para substituir a criptografia NAE e usar uma chave de criptografia específica para cada volume.
- Definir o sinalizador de criptografia NVE para `false` em um backend com NAE habilitado cria um volume com NAE habilitado. Você não pode desabilitar a criptografia NAE definindo o sinalizador de criptografia NVE para `false`.

- Você pode criar manualmente um volume NVE no Trident definindo explicitamente o sinalizador de criptografia NVE como `true`.

Para obter mais informações sobre as opções de configuração do backend, consulte:

- ["Opções de configuração do ONTAP SAN"](#)
- ["Opções de configuração do ONTAP NAS"](#)

Configuração unificada de chave do Trident Linux (LUKS)

Você pode habilitar o Linux Unified Key Setup (LUKS) para criptografar volumes ONTAP SAN e ONTAP SAN ECONOMY no Trident. Trident oferece suporte à rotação de senha e expansão de volume para volumes criptografados com LUKS.

No Trident, os volumes criptografados com LUKS usam a cifra e o modo `aes-xts-plain64`, conforme recomendado por ["NIST"](#).



A criptografia LUKS não é compatível com sistemas ASA r2. Para obter informações sobre sistemas ASA r2, consulte ["Saiba mais sobre os sistemas de armazenamento ASA r2"](#).

Antes de começar

- Os nós de trabalho devem ter `cryptsetup 2.1` ou superior (mas inferior a 3.0) instalado. Para mais informações, visite ["Gitlab: cryptsetup"](#).
- Por motivos de desempenho, NetApp recomenda que os nós de trabalho suportem Advanced Encryption Standard New Instructions (AES-NI). Para verificar o suporte a AES-NI, execute o seguinte comando:

```
grep "aes" /proc/cpuinfo
```

Se nada for retornado, seu processador não suporta AES-NI. Para mais informações sobre AES-NI, visite: ["Intel: instruções do Padrão de Criptografia Avançada \(AES-NI\)"](#).

Ativar criptografia LUKS

Você pode habilitar a criptografia por volume, do lado do host, usando o Linux Unified Key Setup (LUKS) para volumes ONTAP SAN e ONTAP SAN ECONOMY.

Passos

1. Defina os atributos de criptografia LUKS na configuração do backend. Para obter mais informações sobre as opções de configuração do backend para ONTAP SAN, consulte ["Opções de configuração do ONTAP SAN"](#).

```
{
  "storage": [
    {
      "labels": {
        "luks": "true"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "true"
      }
    },
    {
      "labels": {
        "luks": "false"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "false"
      }
    }
  ]
}
```

2. Use `parameters.selector` para definir os pools de armazenamento usando criptografia LUKS. Por exemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Crie um segredo que contenha a senha LUKS. Por exemplo:

```
kubectl -n trident create -f luks-pvc1.yaml
```

```

apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA

```

Limitações

Volumes criptografados com LUKS não podem aproveitar a deduplicação e a compressão do ONTAP.

Configuração de backend para importação de volumes LUKS

Para importar um volume LUKS, você deve definir `luksEncryption` para `true` no backend. A opção `luksEncryption` informa ao Trident se o volume é compatível com LUKS (`true` ou não compatível com LUKS (`false`, conforme mostrado no exemplo a seguir.

```

version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'

```

Configuração de PVC para importação de volumes LUKS

Para importar volumes LUKS dinamicamente, defina a anotação `trident.netapp.io/luksEncryption` para `true` e inclua uma classe de armazenamento habilitada para LUKS no PVC, conforme mostrado neste exemplo.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:

```

```

accessModes:
  - ReadWriteOnce
resources:
  requests:
    storage: 1Gi
storageClassName: luks-sc

```

Rotacionar uma frase secreta LUKS

Você pode alternar a senha LUKS e confirmar a rotação.



Não se esqueça de uma senha até verificar se ela não está mais sendo referenciada por nenhum volume, snapshot ou segredo. Se uma senha referenciada for perdida, você poderá não conseguir montar o volume e os dados permanecerão criptografados e inacessíveis.

Sobre esta tarefa

A rotação da senha LUKS ocorre quando um pod que monta o volume é criado após a especificação de uma nova senha LUKS. Quando um novo pod é criado, Trident compara a senha LUKS no volume com a senha ativa no segredo.

- Se a senha no volume não corresponder à senha ativa no segredo, a rotação ocorrerá.
- Se a senha no volume corresponder à senha ativa no segredo, o `previous-luks-passphrase` parâmetro será ignorado.

Passos

1. Adicione os `node-publish-secret-name` e `node-publish-secret-namespace` parâmetros `StorageClass`. Por exemplo:

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}

```

2. Identifique as frases secretas existentes no volume ou no snapshot.

Volume

```

tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

```

```
...luksPassphraseNames: ["A"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["A"]
```

3. Atualize o segredo LUKS do volume para especificar as senhas nova e anterior. Certifique-se de que `previous-luke-passphrase-name` e `previous-luks-passphrase` correspondam à senha anterior.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Crie um novo pod montando o volume. Isso é necessário para iniciar a rotação.
5. Verifique se a senha foi rotacionada.

Volume

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["B"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["B"]
```

Resultados

A senha foi rotacionada quando apenas a nova senha foi retornada no volume e no snapshot.



Se duas senhas forem retornadas, por exemplo `luksPassphraseNames: ["B", "A"]`, a rotação estará incompleta. Você pode acionar um novo pod para tentar concluir a rotação.

Habilitar expansão de volume

Você pode habilitar a expansão de volume em um volume criptografado com LUKS.

Passos

1. Ative o `CSINodeExpandSecret` feature gate (beta 1.25+). Consulte "[Kubernetes 1.25: use segredos para expansão de volumes CSI orientada a nós](#)" para obter detalhes.
2. Adicione os `node-expand-secret-name` e `node-expand-secret-namespace` parâmetros `StorageClass`. Por exemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Resultados

Ao iniciar a expansão de storage online, o kubelet passa as credenciais apropriadas para o driver.

A criptografia Kerberos em trânsito do Trident

Usando criptografia em trânsito Kerberos, você pode melhorar a segurança do acesso aos dados habilitando a criptografia para o tráfego entre seu cluster gerenciado e o storage backend.

Trident oferece suporte à criptografia Kerberos para ONTAP como backend de storage:

- **On-premise ONTAP** - Trident oferece suporte à criptografia Kerberos em conexões NFSv3 e NFSv4 de clusters Red Hat OpenShift e Kubernetes upstream para volumes ONTAP locais.

Você pode criar, excluir, redimensionar, criar snapshots, clonar, clonar em modo somente leitura e importar volumes que utilizam criptografia NFS.

Configurar criptografia Kerberos em trânsito com volumes ONTAP locais

Você pode habilitar a criptografia Kerberos no tráfego de storage entre seu cluster gerenciado e um backend de storage ONTAP local.



A criptografia Kerberos para o tráfego NFS com backends de storage ONTAP locais só é compatível usando o driver de storage `ontap-nas`.

Antes de começar

- Certifique-se de ter acesso ao utilitário `tridentctl`.
- Certifique-se de ter acesso de administrador ao backend de storage ONTAP.
- Certifique-se de saber o nome do(s) volume(s) que você compartilhará do backend de storage ONTAP.
- Certifique-se de ter preparado a máquina virtual de storage ONTAP para suportar a criptografia Kerberos para volumes NFS. Consulte ["Habilite o Kerberos em um dataLIF"](#) para obter instruções.
- Certifique-se de que todos os volumes NFSv4 que você usa com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de Domínio NFSv4 da NetApp (página 13) do ["NetApp NFSv4 Melhorias e Guia de Práticas Recomendadas"](#).

Adicionar ou modificar políticas de exportação do ONTAP

Você precisa adicionar regras às políticas de exportação ONTAP existentes ou criar novas políticas de exportação que ofereçam suporte à criptografia Kerberos para o volume raiz da máquina virtual de storage ONTAP, bem como para quaisquer volumes ONTAP compartilhados com o cluster Kubernetes upstream. As regras de política de exportação que você adicionar, ou as novas políticas de exportação que você criar, precisam oferecer suporte aos seguintes protocolos de acesso e permissões de acesso:

Protocolos de acesso

Configure a política de exportação com os protocolos de acesso NFS, NFSv3 e NFSv4.

Detalhes de acesso

Você pode configurar uma das três versões diferentes de criptografia Kerberos, dependendo das suas necessidades para o volume:

- **Kerberos 5** - (autenticação e criptografia)
- **Kerberos 5i** - (autenticação e criptografia com proteção de identidade)
- **Kerberos 5p** - (autenticação e criptografia com proteção de identidade e privacidade)

Configure a regra de política de exportação do ONTAP com as permissões de acesso apropriadas. Por exemplo, se os clusters forem montar os volumes NFS com uma combinação de criptografia Kerberos 5i e Kerberos 5p, use as seguintes configurações de acesso:

Tipo	Acesso somente leitura	Acesso de leitura/gravação	Acesso de superusuário
UNIX	Habilitado	Habilitado	Habilitado
Kerberos 5i	Habilitado	Habilitado	Habilitado
Kerberos 5p	Habilitado	Habilitado	Habilitado

Consulte a seguinte documentação para saber como criar políticas de exportação do ONTAP e regras de políticas de exportação:

- ["Criar uma política de exportação"](#)
- ["Adicionar uma regra a uma política de exportação"](#)

Crie um backend de storage

Você pode criar uma configuração de backend de storage Trident que inclua a capacidade de criptografia

Kerberos.

Sobre esta tarefa

Ao criar um arquivo de configuração de storage backend que configura a criptografia Kerberos, você pode especificar uma das três versões diferentes de criptografia Kerberos usando o `spec.nfsMountOptions` parâmetro:

- `spec.nfsMountOptions: sec=krb5` (autenticação e criptografia)
- `spec.nfsMountOptions: sec=krb5i` (autenticação e criptografia com proteção de identidade)
- `spec.nfsMountOptions: sec=krb5p` (autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será usada.

Passos

1. No cluster gerenciado, crie um arquivo de configuração de backend de storage usando o exemplo a seguir. Substitua os valores entre colchetes `<>` com as informações do seu ambiente:

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Use o arquivo de configuração que você criou na etapa anterior para criar o backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se a criação do backend falhar, há algo errado com a configuração do backend. Você pode visualizar os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode executar o comando `create` novamente.

Crie uma storage class

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Sobre esta tarefa

Ao criar um objeto de classe de armazenamento, você pode especificar uma das três versões diferentes de criptografia Kerberos usando o `mountOptions` parâmetro:

- `mountOptions: sec=krb5` (autenticação e criptografia)
- `mountOptions: sec=krb5i` (autenticação e criptografia com proteção de identidade)
- `mountOptions: sec=krb5p` (autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será usada. Se o nível de criptografia que você especificou na configuração do backend de storage for diferente do nível que você especificar no objeto da classe de storage, o objeto da classe de storage terá precedência.

Passos

1. Crie um objeto Kubernetes StorageClass, usando o seguinte exemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions:
  - sec=krb5i #can be krb5, krb5i, or krb5p
parameters:
  backendType: ontap-nas
  storagePools: ontapnas_pool
  trident.netapp.io/nasType: nfs
allowVolumeExpansion: true
```

2. Crie a classe de armazenamento:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Certifique-se de que a classe de armazenamento foi criada:

```
kubectl get sc ontap-nas-sc
```

Você deverá ver uma saída semelhante à seguinte:

NAME	PROVISIONER	AGE
ontap-nas-sc	csi.trident.netapp.io	15h

Provisionar volumes

Após criar um backend de armazenamento e uma classe de armazenamento, você pode provisionar um volume. Para obter instruções, consulte ["Provisionar um volume"](#).

Configurar criptografia Kerberos em trânsito com volumes do Azure NetApp Files

Você pode habilitar a criptografia Kerberos no tráfego de armazenamento entre seu cluster gerenciado e um único back-end de armazenamento Azure NetApp Files ou um pool virtual de back-ends de armazenamento Azure NetApp Files.

Antes de começar

- Certifique-se de ter habilitado Trident no cluster Red Hat OpenShift gerenciado.
- Certifique-se de ter acesso ao utilitário `tridentctl`.
- Certifique-se de ter preparado o backend de armazenamento Azure NetApp Files para criptografia Kerberos, observando os requisitos e seguindo as instruções em ["Documentação do Azure NetApp Files"](#).
- Certifique-se de que todos os volumes NFSv4 que você usa com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de Domínio NFSv4 da NetApp (página 13) do ["NetApp NFSv4 Melhorias e Guia de Práticas Recomendadas"](#).

Crie um backend de storage

Você pode criar uma configuração de back-end de armazenamento do Azure NetApp Files que inclua a capacidade de criptografia Kerberos.

Sobre esta tarefa

Ao criar um arquivo de configuração de backend de storage que configura a criptografia Kerberos, você pode defini-lo para que seja aplicado em um dos dois níveis possíveis:

- O **nível de backend de armazenamento** usando o `spec.kerberos` campo
- O **nível do pool virtual** usando o `spec.storage.kerberos` campo

Ao definir a configuração no nível do pool virtual, o pool é selecionado usando o rótulo na storage class.

Em qualquer um dos níveis, você pode especificar uma das três versões diferentes de criptografia Kerberos:

- kerberos: sec=krb5 (autenticação e criptografia)
- kerberos: sec=krb5i (autenticação e criptografia com proteção de identidade)
- kerberos: sec=krb5p (autenticação e criptografia com proteção de identidade e privacidade)

Passos

1. No cluster gerenciado, crie um arquivo de configuração de backend de storage usando um dos exemplos a seguir, dependendo de onde você precisa definir o backend de storage (nível do backend de storage ou nível do pool virtual). Substitua os valores entre colchetes <> com as informações do seu ambiente:

Exemplo de nível de storage backend

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

Exemplo de nível de pool virtual

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
        kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

2. Use o arquivo de configuração que você criou na etapa anterior para criar o backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se a criação do backend falhar, há algo errado com a configuração do backend. Você pode visualizar os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode executar o comando `create` novamente.

Crie uma storage class

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Passos

1. Crie um objeto Kubernetes StorageClass, usando o seguinte exemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: azure-netapp-files
  trident.netapp.io/nasType: nfs
  selector: type=encryption
```

2. Crie a classe de armazenamento:

```
kubectl create -f sample-input/storage-class-sc-nfs.yaml
```

3. Certifique-se de que a classe de armazenamento foi criada:

```
kubectl get sc -sc-nfs
```

Você deverá ver uma saída semelhante à seguinte:

NAME	PROVISIONER	AGE
sc-nfs	csi.trident.netapp.io	15h

Provisionar volumes

Após criar um backend de armazenamento e uma classe de armazenamento, você pode provisionar um volume. Para obter instruções, consulte "[Provisionar um volume](#)".

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.