Segurança

Trident

NetApp
January 14, 2026

Índice

Segurança

Segurança

Use as recomendações listadas aqui para garantir que a instalação do Trident esteja segura.

Execute o Trident em seu próprio namespace

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

Para separar as outras aplicações e usuários do Trident, sempre instale o Trident em seu próprio namespace do Kubernetes (`trident`). A colocação do Trident em seu próprio namespace garante que somente o pessoal administrativo do Kubernetes tenha acesso ao pod Trident e aos artefatos (como segredos de back-end e CHAP, se aplicável) armazenados nos objetos CRD com namespaces. Você deve garantir que você permita que apenas administradores acessem o namespace Trident e, assim, acessem o `tridentctl` aplicativo.

Use a autenticação CHAP com backends ONTAP SAN

O Trident é compatível com autenticação baseada em CHAP para cargas de trabalho SAN ONTAP (usando os `ontap-san` drivers e `ontap-san-economy`). A NetApp recomenda o uso de CHAP bidirecional com Trident para autenticação entre um host e o back-end de storage.

Para backends ONTAP que usam os drivers de armazenamento SAN, o Trident pode configurar CHAP bidirecional e gerenciar nomes de usuário e segredos do CHAP através `tridentctl`do . "Prepare-se para configurar o back-end com drivers SAN ONTAP"Consulte para compreender como o Trident configura o CHAP nos backends ONTAP.

Use a autenticação CHAP com backends NetApp HCI e SolidFire

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

Os volumes criados pelo Trident não estão associados a nenhum Grupo de Acesso por volume.

Use o Trident com NVE e NAE

O NetApp ONTAP fornece criptografia de dados em repouso para proteger dados confidenciais caso um disco seja roubado, retornado ou reutilizado. Para obter detalhes, "Configurar a visão geral da encriptação de volume do NetApp"consulte .

- Se o NAE estiver ativado no back-end, qualquer volume provisionado no Trident será habilitado para NAE.
  - Você pode definir o sinalizador de criptografia NVE como `""` para criar volumes habilitados para NAE.
- Se o NAE não estiver habilitado no back-end, qualquer volume provisionado no Trident será habilitado para NVE, a menos que o sinalizador de criptografia NVE esteja definido como `false` (o valor padrão) na

configuração do back-end.

> Os volumes criados no Trident em um back-end habilitado para NAE devem ser criptografados com NVE ou NAE.
>
> - Você pode definir o sinalizador de criptografia NVE como `true` na configuração de back-end do Trident para substituir a criptografia NAE e usar uma chave de criptografia específica por volume.
> - Definir o sinalizador de criptografia NVE como `false` em um back-end habilitado para NAE cria um volume habilitado para NAE. Não é possível desativar a criptografia NAE definindo o sinalizador de criptografia NVE como `false`.

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

Para obter mais informações sobre opções de configuração de back-end, consulte:

- "Opções de configuração do ONTAP SAN"
- "Opções de configuração do ONTAP nas"

Configuração de chave unificada do Linux (LUKS)

Você pode ativar a configuração de chave unificada do Linux (LUKS) para criptografar volumes DE ECONOMIA DE SAN ONTAP e SAN ONTAP no Trident. O Trident suporta rotação de senhas e expansão de volume para volumes criptografados com LUKS.

No Trident, os volumes criptografados por LUKS usam a cifra e o modo aes-xts-plain64, conforme recomendado "NIST"pelo .

Antes de começar

- Os nós de trabalho devem ter o cryptsetup 2,1 ou superior (mas inferior a 3,0) instalado. Para obter mais informações, visite "Gitlab: Cryptsetup".
- Por motivos de desempenho, a NetApp recomenda que os nós de trabalho suportem as novas instruções padrão de criptografia avançada (AES-NI). Para verificar o suporte ao AES-NI, execute o seguinte comando:

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

Se nada for devolvido, o processador não suporta AES-NI. Para obter mais informações sobre o AES-NI, visite: "Intel: Advanced Encryption Standard Instructions (AES-NI)".

Ativar encriptação LUKS

Você pode ativar a criptografia por volume no lado do host usando o LUKS (Configuração de chave unificada do Linux) para volumes ECONÔMICOS SAN ONTAP e SAN ONTAP.

Passos

1. Defina atributos de criptografia LUKS na configuração de back-end. Para obter mais informações sobre

opções de configuração de back-end para SAN ONTAP, "Opções de configuração do ONTAP SAN"consulte .

```
{
  "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 a 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 frase-passe 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

Os volumes criptografados com LUKS não podem aproveitar a deduplicação e a compactação do ONTAP.

Configuração de back-end para importação de volumes LUKS

Para importar um volume LUKS, você deve definir `luksEncryption` como(`true` no back-end. A `luksEncryption` opção informa ao Trident se o volume é compatível com LUKS (`true`) ou não 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` como `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
```

Rode uma frase-passe LUKS

Pode rodar a frase-passe LUKS e confirmar a rotação.

> Não se esqueça de uma frase-passe até ter verificado que ela não é mais referenciada por qualquer volume, instantâneo ou segredo. Se uma frase-passe referenciada for perdida, talvez você não consiga montar o volume e os dados permanecerão criptografados e inacessíveis.

Sobre esta tarefa

A rotação da frase-passe LUKS ocorre quando um pod que monta o volume é criado após uma nova frase-passe LUKS ser especificada. Quando um novo pod é criado, o Trident compara a frase-passe LUKS no volume com a frase-passe ativa no segredo.

- Se a frase-passe no volume não corresponder à frase-passe ativa no segredo, ocorre rotação.
- Se a frase-passe no volume corresponder à frase-passe ativa no segredo, o `previous-luks-passphrase` parâmetro é ignorado.

Passos

1. Adicione os `node-publish-secret-name` parâmetros e `node-publish-secret-namespace` 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. Identificar senhas existentes no volume ou instantâneo.

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 para o volume para especificar as senhas novas e anteriores. Certifique-se `previous-luke-passphrase-name` e `previous-luks-passphrase` faça a correspondência da frase-passe 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 de montagem do volume. Isto é necessário para iniciar a rotação.
5. Verifique se a senha foi girada.

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 frase-passe foi girada quando apenas a nova frase-passe é retornada no volume e no instantâneo.

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

Ative a expansão de volume

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

Passos

1. Ative a `CSINodeExpandSecret` porta de recurso (beta 1,25 ou mais). "Kubernetes 1,25: Use segredos para a expansão orientada por nós de volumes CSI"Consulte para obter detalhes.
2. Adicione os `node-expand-secret-name` parâmetros e `node-expand-secret-namespace` 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

Quando você inicia a expansão de armazenamento on-line, o kubelet passa as credenciais apropriadas para o driver.

Criptografia em trânsito Kerberos

Usando a criptografia em trânsito Kerberos, você pode melhorar a segurança de acesso aos dados habilitando a criptografia para o tráfego entre o cluster gerenciado e o back-end de armazenamento.

O Trident oferece suporte à criptografia Kerberos para ONTAP como um back-end de armazenamento:

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

Você pode criar, excluir, redimensionar, snapshot, clone, clone somente leitura e importar volumes que usam criptografia NFS.

Configurar a criptografia Kerberos em trânsito com volumes ONTAP no local

Você pode ativar a criptografia Kerberos no tráfego de armazenamento entre o cluster gerenciado e um back-end de armazenamento ONTAP no local.

> A criptografia Kerberos para tráfego NFS com backends de armazenamento ONTAP on-premise só é suportada usando o `ontap-nas` driver de armazenamento.

Antes de começar

- Certifique-se de que tem acesso ao `tridentctl` utilitário.
- Verifique se você tem acesso de administrador ao back-end de storage do ONTAP.
- Certifique-se de saber o nome do volume ou volumes que você compartilhará no back-end de storage do ONTAP.
- Certifique-se de que você preparou a VM de armazenamento ONTAP para oferecer suporte à criptografia Kerberos para volumes NFS. "Ative o Kerberos em um dataLIF"Consulte para obter instruções.
- Certifique-se de que todos os volumes NFSv4 usados com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do "Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4".

Adicionar ou modificar políticas de exportação do ONTAP

Você precisa adicionar regras às políticas de exportação existentes do ONTAP ou criar novas políticas de exportação que suportem a criptografia Kerberos para o volume raiz da VM de armazenamento do ONTAP, bem como quaisquer volumes do ONTAP compartilhados com o cluster do 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

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

Aceder aos detalhes

Você pode configurar uma das três versões diferentes da criptografia Kerberos, dependendo de 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 estiverem montando os volumes NFS com uma mistura de criptografia Kerberos 5i e kerberos 5P, use as seguintes configurações de acesso:

Tipo	Acesso somente leitura	Acesso de leitura/escrita	Acesso ao superusuário
UNIX	Ativado	Ativado	Ativado
Kerberos 5i	Ativado	Ativado	Ativado
Kerberos 5p	Ativado	Ativado	Ativado

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

- "Crie uma política de exportação"
- "Adicione uma regra a uma política de exportação"

Crie um back-end de storage

Você pode criar uma configuração de back-end de armazenamento Trident que inclua o recurso de criptografia Kerberos.

Sobre esta tarefa

Quando você cria um arquivo de configuração de back-end de armazenamento que configura a criptografia Kerberos, você pode especificar uma das três versões diferentes da 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 back-end de storage usando o exemplo a seguir. Substitua os valores entre parêntesis> por 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, algo está errado com a configuração do backend. Você pode exibir os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

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

Crie uma classe de armazenamento

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 da 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 especificado na configuração de back-end de armazenamento for diferente do nível especificado no objeto de classe de armazenamento, o objeto de classe de armazenamento terá precedência.

Passos

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

```
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 deve ver saída semelhante ao seguinte:

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

Volumes de provisionamento

Depois de criar um back-end de storage e uma classe de storage, agora é possível provisionar um volume. Para obter instruções, "Provisionar um volume" consulte .

Configurar a criptografia Kerberos em trânsito com volumes Azure NetApp Files

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

Antes de começar

- Certifique-se de que você ativou o Trident no cluster gerenciado do Red Hat OpenShift.
- Certifique-se de que tem acesso ao `tridentctl` utilitário.
- Certifique-se de que preparou o back-end 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 usados com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do "Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4".

Crie um back-end de storage

Você pode criar uma configuração de back-end de armazenamento Azure NetApp Files que inclua o recurso de criptografia Kerberos.

Sobre esta tarefa

Quando você cria um arquivo de configuração de back-end de armazenamento que configura a criptografia Kerberos, você pode defini-lo para que ele seja aplicado em um dos dois níveis possíveis:

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

Quando você define a configuração no nível do pool virtual, o pool é selecionado usando o rótulo na classe de armazenamento.

Em ambos os níveis, você pode especificar uma das três versões diferentes da 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 back-end de storage usando um dos exemplos a seguir, dependendo de onde você precisa definir o back-end de storage (nível de back-end de armazenamento ou nível de pool virtual). Substitua os valores entre parêntesis> por informações do seu ambiente:

Exemplo de nível de back-end de storage

```
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, algo está errado com a configuração do backend. Você pode exibir os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

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

Crie uma classe de armazenamento

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

Passos

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

```
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 deve ver saída semelhante ao seguinte:

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

Volumes de provisionamento

Depois de criar um back-end de storage e uma classe de storage, agora é possível provisionar um volume. Para obter instruções, "Provisionar um volume" consulte .

Informações sobre direitos autorais

Informações sobre marcas comerciais