



Sicurezza

Trident

NetApp
July 01, 2026

Sommario

Sicurezza	1
Sicurezza	1
Esegui Trident nel suo namespace	1
Utilizzare l'autenticazione CHAP con i backend ONTAP SAN	1
Utilizzare l'autenticazione CHAP con NetApp HCI e SolidFire backends	1
Usa Trident con NVE e NAE	1
Linux Unified Key Setup (LUKS)	2
Abilita la crittografia LUKS	2
Configurazione backend per l'importazione di volumi LUKS	4
Configurazione PVC per l'importazione di volumi LUKS	4
Ruota una passphrase LUKS	5
Abilita l'espansione del volume	7
Crittografia in volo Kerberos	8
Configura la crittografia Kerberos in volo con i volumi ONTAP on-premise	8
Configura la crittografia Kerberos in volo con i volumi Azure NetApp Files	12

Sicurezza

Sicurezza

Utilizzare le raccomandazioni elencate qui per garantire che l'installazione di Trident sia sicura.

Esegui Trident nel suo namespace

È importante impedire alle applicazioni, agli amministratori delle applicazioni, agli utenti e alle applicazioni di gestione di accedere alle definizioni degli oggetti Trident o ai pod per garantire uno storage affidabile e bloccare potenziali attività dannose.

Per separare le altre applicazioni e gli altri utenti da Trident, installa sempre Trident nel proprio namespace Kubernetes (`trident`). Mettere Trident nel proprio namespace garantisce che solo il personale amministrativo di Kubernetes abbia accesso al pod Trident e agli artefatti (come backend e segreti CHAP, se applicabile) archiviati negli oggetti CRD con namespace. Devi assicurarti di consentire solo agli amministratori l'accesso al namespace Trident e quindi l'accesso all'applicazione `tridentctl`.

Utilizzare l'autenticazione CHAP con i backend ONTAP SAN

Trident supporta l'autenticazione basata su CHAP per i carichi di lavoro ONTAP SAN (utilizzando i `ontap-san` e `ontap-san-economy` driver). NetApp consiglia di utilizzare CHAP bidirezionale con Trident per l'autenticazione tra un host e il backend di storage.

Per i backend ONTAP che utilizzano i driver di storage SAN, Trident può configurare il CHAP bidirezionale e gestire i nomi utente e i segreti CHAP tramite `tridentctl`. Fare riferimento a ["Prepararsi a configurare il backend con i driver ONTAP SAN"](#) per comprendere come Trident configura il CHAP sui backend ONTAP.

Utilizzare l'autenticazione CHAP con NetApp HCI e SolidFire backends

NetApp consiglia di implementare CHAP bidirezionale per garantire l'autenticazione tra un host e i backend NetApp HCI e SolidFire. Trident utilizza un oggetto segreto che include due password CHAP per tenant. Quando Trident è installato, gestisce i segreti CHAP e li memorizza in un oggetto CR `tridentvolume` per il rispettivo PV. Quando si crea un PV, Trident utilizza i segreti CHAP per avviare una sessione iSCSI e comunicare con il sistema NetApp HCI e SolidFire tramite CHAP.



I volumi che vengono creati da Trident non sono associati ad alcun Volume Access Group.

Usa Trident con NVE e NAE

NetApp ONTAP fornisce la crittografia dei dati a riposo per proteggere i dati sensibili in caso di furto, restituzione o riutilizzo di un disco. Per dettagli, consultare ["Panoramica sulla configurazione della crittografia del volume NetApp"](#).

- Se NAE è abilitato sul backend, qualsiasi volume fornito in Trident sarà NAE-enabled.
 - È possibile impostare il flag di crittografia NVE su `""` per creare volumi abilitati per NAE.
- Se NAE non è abilitato sul backend, qualsiasi volume fornito in Trident sarà abilitato per NVE, a meno che il flag di crittografia NVE non sia impostato su `false` (il valore predefinito) nella configurazione del backend.

I volumi creati in Trident su un backend abilitato NAE devono essere crittografati NVE o NAE.



- È possibile impostare il flag di crittografia NVE su `true` nella configurazione del backend Trident per ignorare la crittografia NAE e utilizzare una chiave di crittografia specifica per ogni volume.
- Impostando il flag di crittografia NVE `false` su un backend abilitato per NAE si crea un volume abilitato per NAE. Non è possibile disabilitare la crittografia NAE impostando il flag di crittografia NVE a `false`.

- È possibile creare manualmente un volume NVE in Trident impostando esplicitamente il flag di crittografia NVE su `true`.

Per maggiori informazioni sulle opzioni di configurazione del backend, fare riferimento a:

- ["Opzioni di configurazione SAN ONTAP"](#)
- ["Opzioni di configurazione NAS ONTAP"](#)

Linux Unified Key Setup (LUKS)

È possibile abilitare Linux Unified Key Setup (LUKS) per crittografare i volumi ONTAP SAN e ONTAP SAN ECONOMY su Trident. Trident supporta la rotazione della passphrase e l'espansione del volume per i volumi crittografati con LUKS.

In Trident, i volumi crittografati con LUKS utilizzano il cifrario e la modalità `aes-xts-plain64`, come raccomandato da ["NIST"](#).



La crittografia LUKS non è supportata per i sistemi ASA r2. Per informazioni sui sistemi ASA r2, vedere ["Scopri i sistemi di storage ASA r2"](#).

Prima di iniziare

- I nodi worker devono avere installato `cryptsetup 2.1` o superiore (ma inferiore a 3.0). Per ulteriori informazioni, visitare ["Gitlab: cryptsetup"](#).
- Per motivi di prestazioni, NetApp raccomanda che i nodi worker supportino Advanced Encryption Standard New Instructions (AES-NI). Per verificare il supporto di AES-NI, eseguire il seguente comando:

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

Se non viene restituito nulla, il processore non supporta AES-NI. Per ulteriori informazioni su AES-NI, visitare: ["Intel: Advanced Encryption Standard Instructions \(AES-NI\)"](#).

Abilita la crittografia LUKS

È possibile abilitare la crittografia per volume, lato host, utilizzando Linux Unified Key Setup (LUKS) per ONTAP SAN e ONTAP SAN ECONOMY volumi.

Passaggi

1. Definire gli attributi di crittografia LUKS nella configurazione backend. Per ulteriori informazioni sulle opzioni di configurazione backend per ONTAP SAN, fare riferimento a ["Opzioni di configurazione SAN"](#)

ONTAP".

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

2. Utilizzare `parameters.selector` per definire i pool di archiviazione utilizzando la crittografia LUKS. Ad esempio:

```
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. Crea un segreto che contenga la passphrase LUKS. Ad esempio:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

Limitazioni

I volumi crittografati LUKS non possono sfruttare la deduplicazione e la compressione di ONTAP.

Configurazione backend per l'importazione di volumi LUKS

Per importare un volume LUKS, è necessario impostare `luksEncryption` su `true` sul backend. L'opzione `luksEncryption` indica a Trident se il volume è LUKS-compliant (`true` o non LUKS-compliant (`false`), come mostrato nell'esempio seguente.

```
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'
```

Configurazione PVC per l'importazione di volumi LUKS

Per importare i volumi LUKS in modo dinamico, impostare l'annotazione `trident.netapp.io/luksEncryption` a `true` e includere una storage class abilitata per LUKS nel PVC come mostrato in questo esempio.

```
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
```

Ruota una passphrase LUKS

È possibile ruotare la passphrase LUKS e confermare la rotazione.



Non dimenticare una passphrase finché non hai verificato che non sia più referenziata da alcun volume, snapshot o segreto. Se una passphrase referenziata viene persa, potresti non essere in grado di montare il volume e i dati rimarranno crittografati e inaccessibili.

Informazioni su questa attività

La rotazione della passphrase LUKS avviene quando viene creato un pod che monta il volume dopo che è stata specificata una nuova passphrase LUKS. Quando viene creato un nuovo pod, Trident confronta la passphrase LUKS sul volume con la passphrase attiva nel secret.

- Se la passphrase sul volume non corrisponde alla passphrase attiva nel secret, si verifica la rotazione.
- Se la passphrase sul volume corrisponde alla passphrase attiva nel segreto, il `previous-luks-passphrase` parametro viene ignorato.

Passaggi

1. Aggiungere i `node-publish-secret-name` e `node-publish-secret-namespace` parametri StorageClass. Ad esempio:

```

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. Identificare le passphrase esistenti sul volume o sullo 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. Aggiornare il segreto LUKS per il volume per specificare la nuova e la precedente passphrase. Assicurarsi che `previous-luke-passphrase-name` e `previous-luks-passphrase` corrispondano alla passphrase precedente.

```

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. Crea un nuovo pod che monta il volume. Questo è necessario per avviare la rotazione.

5. Verificare che la passphrase sia stata ruotata.

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"]
```

Risultati

La passphrase è stata ruotata quando sul volume e sullo snapshot viene restituita solo la nuova passphrase.



Se vengono restituite due passphrase, ad esempio `luksPassphraseNames: ["B", "A"]`, la rotazione è incompleta. Puoi attivare un nuovo pod per tentare di completare la rotazione.

Abilita l'espansione del volume

È possibile abilitare l'espansione del volume su un volume crittografato con LUKS.

Passaggi

1. Abilita la funzionalità `CSINodeExpandSecret` feature gate (beta 1.25+). Consultare ["Kubernetes 1.25: utilizzare i Secrets per l'espansione dei volumi CSI basata sui nodi"](#) per i dettagli.
2. Aggiungere i `node-expand-secret-name` e `node-expand-secret-namespace` parametri `StorageClass`. Ad esempio:

```
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
```

Risultati

Quando si avvia l'espansione dello storage online, il kubelet passa le credenziali appropriate al driver.

Crittografia in volo Kerberos

Utilizzando la crittografia Kerberos in volo, puoi migliorare la sicurezza dell'accesso ai dati abilitando la crittografia per il traffico tra il tuo cluster gestito e il backend di storage.

Trident supporta la crittografia Kerberos per ONTAP come storage backend:

- **On-premise ONTAP** - Trident supporta la crittografia Kerberos su connessioni NFSv3 e NFSv4 da cluster Red Hat OpenShift e Kubernetes upstream a volumi ONTAP on-premise.

È possibile creare, eliminare, ridimensionare, creare snapshot, clonare, clonare in sola lettura e importare volumi che utilizzano NFS con crittografia.

Configura la crittografia Kerberos in volo con i volumi ONTAP on-premise

È possibile abilitare la crittografia Kerberos sul traffico di storage tra il cluster gestito e un backend di storage ONTAP on-premise.



La crittografia Kerberos per il traffico NFS con backend di storage on-premise ONTAP è supportata solo utilizzando il `ontap-nas` storage driver.

Prima di iniziare

- Assicurati di avere accesso all' `tridentctl` utility.
- Assicurati di avere accesso come amministratore al backend di storage ONTAP.
- Assicurati di conoscere il nome del volume o dei volumi che condividerai dal backend di storage ONTAP.
- Assicurarsi di aver preparato la macchina virtuale di storage ONTAP per supportare la crittografia Kerberos per i volumi NFS. Consulta ["Abilitare Kerberos su un dataLIF"](#) per le istruzioni.
- Assicurarsi che i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Fare riferimento alla sezione NetApp NFSv4 Domain Configuration (pagina 13) di ["NetApp Miglioramenti NFSv4 e Guida alle Best Practice"](#).

Aggiungi o modifica le policy di esportazione ONTAP

È necessario aggiungere regole alle policy di esportazione ONTAP esistenti o creare nuove policy di esportazione che supportino la crittografia Kerberos per il volume root della storage VM ONTAP, così come per qualsiasi volume ONTAP condiviso con il cluster Kubernetes upstream. Le regole delle policy di esportazione che aggiungi, o le nuove policy di esportazione che crei, devono supportare i seguenti protocolli di accesso e permessi di accesso:

Protocolli di accesso

Configura la policy di esportazione con i protocolli di accesso NFS, NFSv3 e NFSv4.

Dettagli di accesso

È possibile configurare una delle tre diverse versioni della crittografia Kerberos, a seconda delle esigenze per il volume:

- **Kerberos 5** - (autenticazione e crittografia)

- **Kerberos 5i** - (autenticazione e crittografia con protezione dell'identità)
- **Kerberos 5p** - (autenticazione e crittografia con protezione dell'identità e della privacy)

Configurare la regola della policy di esportazione ONTAP con le autorizzazioni di accesso appropriate. Ad esempio, se i cluster monteranno i volumi NFS con un misto di crittografia Kerberos 5i e Kerberos 5p, utilizzare le seguenti impostazioni di accesso:

Tipo	Accesso in sola lettura	Accesso in lettura/scrittura	Accesso come superutente
UNIX	Abilitato	Abilitato	Abilitato
Kerberos 5i	Abilitato	Abilitato	Abilitato
Kerberos 5p	Abilitato	Abilitato	Abilitato

Consultare la seguente documentazione per informazioni su come creare le policy di esportazione ONTAP e le regole delle policy di esportazione:

- ["Creare una policy di esportazione"](#)
- ["Aggiungere una regola a una policy di esportazione"](#)

Creare un backend di storage

È possibile creare una configurazione del backend di storage Trident che includa la funzionalità di crittografia Kerberos.

Informazioni su questa attività

Quando si crea un file di configurazione del backend di archiviazione che configura la crittografia Kerberos, è possibile specificare una delle tre diverse versioni della crittografia Kerberos utilizzando il parametro `spec.nfsMountOptions`:

- `spec.nfsMountOptions: sec=krb5` (autenticazione e crittografia)
- `spec.nfsMountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `spec.nfsMountOptions: sec=krb5p` (autenticazione e crittografia con protezione dell'identità e della privacy)

Specificare un solo livello Kerberos. Se si specifica più di un livello di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione.

Passaggi

1. Sul cluster gestito, creare un file di configurazione del backend di storage utilizzando il seguente esempio. Sostituire i valori tra parentesi <> con le informazioni del proprio 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. Utilizzare il file di configurazione creato nel passo precedente per creare il backend:

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

Se la creazione del backend fallisce, c'è qualcosa di sbagliato nella configurazione del backend. Puoi visualizzare i log per determinarne la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una storage class

È possibile creare una storage class per il provisioning dei volumi con crittografia Kerberos.

Informazioni su questa attività

Quando si crea un oggetto classe di archiviazione, è possibile specificare una delle tre diverse versioni della crittografia Kerberos utilizzando il parametro `mountOptions`:

- `mountOptions: sec=krb5` (autenticazione e crittografia)
- `mountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `mountOptions: sec=krb5p` (autenticazione e crittografia con protezione dell'identità e della privacy)

Specificare un solo livello Kerberos. Se si specifica più di un livello di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione. Se il livello di crittografia specificato nella configurazione del backend di storage è diverso dal livello specificato nell'oggetto storage class, l'oggetto storage class ha la precedenza.

Passaggi

1. Crea un oggetto StorageClass Kubernetes, utilizzando il seguente esempio:

```
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. Crea la classe di archiviazione:

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

3. Assicurati che la storage class sia stata creata:

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

Dovresti vedere un output simile al seguente:

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

Provisioning dei volumi

Dopo aver creato un backend di archiviazione e una classe di archiviazione, è possibile eseguire il provisioning di un volume. Per istruzioni, consultare ["Effettua il provisioning di un volume"](#).

Configura la crittografia Kerberos in volo con i volumi Azure NetApp Files

È possibile abilitare la crittografia Kerberos sul traffico di archiviazione tra il cluster gestito e un singolo backend di archiviazione Azure NetApp Files o un pool virtuale di backend di archiviazione Azure NetApp Files.

Prima di iniziare

- Assicurarsi di aver abilitato Trident sul cluster gestito Red Hat OpenShift.
- Assicurarsi di avere accesso all' `tridentctl` utility.
- Assicurarsi di aver preparato il backend di archiviazione Azure NetApp Files per la crittografia Kerberos, prendendo nota dei requisiti e seguendo le istruzioni in ["Documentazione di Azure NetApp Files"](#).
- Assicurarsi che i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Fare riferimento alla sezione NetApp NFSv4 Domain Configuration (pagina 13) di ["NetApp Miglioramenti NFSv4 e Guida alle Best Practice"](#).

Creare un backend di storage

È possibile creare una configurazione del backend di storage di Azure NetApp Files che include la funzionalità di crittografia Kerberos.

Informazioni su questa attività

Quando si crea un file di configurazione del backend di archiviazione che configura la crittografia Kerberos, è possibile definirlo in modo che venga applicato a uno dei due livelli possibili:

- Il **livello di backend dello storage** utilizzando il `spec.kerberos` campo
- Il **livello del pool virtuale** utilizzando il campo `spec.storage.kerberos`

Quando si definisce la configurazione a livello di pool virtuale, il pool viene selezionato utilizzando l'etichetta nella storage class.

A entrambi i livelli, puoi specificare una delle tre diverse versioni della crittografia Kerberos:

- `kerberos: sec=krb5` (autenticazione e crittografia)
- `kerberos: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `kerberos: sec=krb5p` (autenticazione e crittografia con protezione dell'identità e della privacy)

Passaggi

1. Sul cluster gestito, creare un file di configurazione del backend di archiviazione utilizzando uno dei seguenti esempi, a seconda di dove è necessario definire il backend di archiviazione (livello di backend di archiviazione o livello di pool virtuale). Sostituire i valori tra parentesi `<>` con le informazioni del proprio ambiente:

Esempio a livello di backend di 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
```

Esempio di livello di pool virtuale

```

---
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. Utilizzare il file di configurazione creato nel passo precedente per creare il backend:

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

Se la creazione del backend fallisce, c'è qualcosa di sbagliato nella configurazione del backend. Puoi visualizzare i log per determinarne la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una storage class

È possibile creare una storage class per il provisioning dei volumi con crittografia Kerberos.

Passaggi

1. Crea un oggetto StorageClass Kubernetes, utilizzando il seguente esempio:

```
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. Crea la classe di archiviazione:

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

3. Assicurati che la storage class sia stata creata:

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

Dovresti vedere un output simile al seguente:

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

Provisioning dei volumi

Dopo aver creato un backend di archiviazione e una classe di archiviazione, è possibile eseguire il provisioning di un volume. Per istruzioni, consultare "[Effettua il provisioning di un volume](#)".

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.