



Driver SAN ONTAP

Trident

NetApp
October 29, 2026

Sommario

- Driver SAN ONTAP 1
 - Panoramica del driver ONTAP SAN 1
 - Dettagli del driver ONTAP SAN 1
 - Permessi utente 2
 - Considerazioni aggiuntive per NVMe/TCP 2
 - Prepararsi a configurare il backend con i driver ONTAP SAN 3
 - Requisiti 3
 - Autenticare il backend ONTAP 3
 - Autenticare le connessioni con CHAP bidirezionale 8
 - Opzioni ed esempi di configurazione SAN ONTAP 10
 - Opzioni di configurazione del backend 10
 - Opzioni di configurazione del backend per il provisioning dei volumi 16
 - Esempi di configurazione minima 18
 - Esempi di backend con pool virtuali 22
 - Mappa i backend a StorageClasses 25

Driver SAN ONTAP

Panoramica del driver ONTAP SAN

Scopri come configurare un backend ONTAP con i driver ONTAP e Cloud Volumes ONTAP SAN.

Dettagli del driver ONTAP SAN

Trident fornisce i seguenti driver di storage SAN per comunicare con il cluster ONTAP. Le modalità di accesso supportate sono: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Driver	Protocollo	volumeMode	Modalità di accesso supportate	File system supportati
ontap-san	iSCSI SCSI su FC	Blocco	RWO, ROX, RWX, RWOP	Nessun file system; dispositivo a blocchi raw
ontap-san	iSCSI SCSI su FC	Filesystem	RWO, RWOP ROX e RWX non sono disponibili nella modalità volume file system.	xfs, ext3, ext4
ontap-san	NVMe/TCP Fai riferimento a Considerazioni aggiuntive per NVMe/TCP .	Blocco	RWO, ROX, RWX, RWOP	Nessun file system; dispositivo a blocchi raw
ontap-san	NVMe/TCP Fai riferimento a Considerazioni aggiuntive per NVMe/TCP .	Filesystem	RWO, RWOP ROX e RWX non sono disponibili nella modalità volume file system.	xfs, ext3, ext4
ontap-san-economy	iSCSI	Blocco	RWO, ROX, RWX, RWOP	Nessun file system; dispositivo a blocchi raw
ontap-san-economy	iSCSI	Filesystem	RWO, RWOP ROX e RWX non sono disponibili nella modalità volume file system.	xfs, ext3, ext4



- Utilizzare `ontap-san-economy` solo se si prevede che il conteggio dell'utilizzo del volume

persistente sia superiore a ["limiti di volume ONTAP supportati"](#).

- Utilizzare `ontap-nas-economy` solo se si prevede che il conteggio dell'utilizzo del volume persistente sia superiore a ["limiti di volume ONTAP supportati"](#) e il `ontap-san-economy` driver non può essere utilizzato.
- Non utilizzare `ontap-nas-economy` se si prevede la necessità di protezione dei dati, disaster recovery o mobilità.
- NetApp non consiglia di utilizzare l'autogrow di FlexVol in tutti i driver ONTAP, ad eccezione di `ontap-san`. Come soluzione alternativa, Trident supporta l'utilizzo della riserva di snapshot e ridimensiona di conseguenza i volumi FlexVol.

Permessi utente

Trident prevede di essere eseguito come amministratore ONTAP o SVM, in genere utilizzando l'admin`utente del cluster o un `vsadmin`utente SVM, oppure un utente con un nome diverso che ha lo stesso ruolo. Per le distribuzioni Amazon FSx for NetApp ONTAP, Trident prevede di essere eseguito come amministratore ONTAP o SVM, utilizzando l'utente del cluster `fsxadmin o un `vsadmin`utente SVM, oppure un utente con un nome diverso che ha lo stesso ruolo. L' `fsxadmin`utente è un sostituto limitato per l'utente amministratore del cluster.



Se si utilizza il `limitAggregateUsage` parametro, sono richieste le autorizzazioni di amministratore del cluster. Quando si utilizza Amazon FSx for NetApp ONTAP con Trident, il `limitAggregateUsage` parametro non funzionerà con gli account utente `vsadmin` e `fsxadmin`. L'operazione di configurazione non andrà a buon fine se si specifica questo parametro.

Sebbene sia possibile creare un ruolo più restrittivo all'interno di ONTAP che un driver Trident può utilizzare, lo sconsigliamo. La maggior parte delle nuove versioni di Trident richiamerà API aggiuntive di cui bisognerebbe tenere conto, rendendo gli aggiornamenti difficili e soggetti a errori.

Considerazioni aggiuntive per NVMe/TCP

Trident supporta il protocollo non-volatile memory express (NVMe) utilizzando il `ontap-san` driver, incluso:

- IPv6
- Snapshot e cloni di volumi NVMe
- Ridimensionamento di un volume NVMe
- Importazione di un volume NVMe creato al di fuori di Trident in modo che il suo ciclo di vita possa essere gestito da Trident
- Multipathing nativo NVMe
- Arresto regolare o non regolare dei nodi K8s (24.06)

Trident non supporta:

- DH-HMAC-CHAP che è supportato nativamente da NVMe
- Multipathing del device mapper (DM)
- Crittografia LUKS



NVMe è supportato solo con le API REST di ONTAP e non è supportato con ONTAPI (ZAPI).

Prepararsi a configurare il backend con i driver ONTAP SAN

Comprendere i requisiti e le opzioni di autenticazione per la configurazione di un backend ONTAP con driver ONTAP SAN.

Requisiti

Per tutti i backend ONTAP, Trident richiede che almeno un aggregato sia assegnato all'SVM.



"Sistemi ASA r2" differiscono dagli altri sistemi ONTAP (ASA, AFF e FAS) nell'implementazione del loro livello di storage. Nei sistemi ASA r2, vengono utilizzate zone di disponibilità dello storage al posto degli aggregati. Fare riferimento all'["questo"](#) articolo della Knowledge Base su come assegnare gli aggregati alle SVM nei sistemi ASA r2.

Ricorda che puoi anche eseguire più di un driver e creare classi di archiviazione che puntano all'uno o all'altro. Ad esempio, puoi configurare una `san-dev` classe che utilizza il `ontap-san` driver e una `san-default` classe che utilizza il `ontap-san-economy` driver.

Tutti i nodi worker di Kubernetes devono avere installati gli strumenti iSCSI appropriati. Per i dettagli, fai riferimento a ["Prepara il nodo worker"](#).

Autenticare il backend ONTAP

Trident offre due modalità di autenticazione per un backend ONTAP.

- Basato su credenziali: il nome utente e la password di un utente ONTAP con le autorizzazioni richieste. Si consiglia di utilizzare un ruolo di login di sicurezza predefinito, come `admin` o `vsadmin` per garantire la massima compatibilità con le versioni di ONTAP.
- Basato su certificato: Trident può anche comunicare con un cluster ONTAP utilizzando un certificato installato sul backend. In questo caso, la definizione del backend deve contenere i valori codificati in Base64 del certificato client, della chiave e del certificato CA attendibile, se utilizzato (consigliato).

È possibile aggiornare i backend esistenti per passare tra metodi basati su credenziali e metodi basati su certificati. Tuttavia, è supportato solo un metodo di autenticazione alla volta. Per passare a un diverso metodo di autenticazione, è necessario rimuovere il metodo esistente dalla configurazione del backend.



Se si tenta di fornire **sia le credenziali che i certificati**, la creazione del backend fallirà con un errore che indica che è stato fornito più di un metodo di autenticazione nel file di configurazione.

Abilitare l'autenticazione basata su credenziali

Trident richiede le credenziali di un amministratore SVM-scoped/cluster-scoped per comunicare con il backend ONTAP. Si consiglia di utilizzare ruoli standard, predefiniti come `admin` o `vsadmin`. Questo garantisce la compatibilità futura con le versioni ONTAP che potrebbero esporre API di funzionalità da utilizzare nelle future versioni di Trident. È possibile creare e utilizzare un ruolo di accesso di sicurezza personalizzato con Trident, ma non è consigliato.

Un esempio di definizione di backend sarà simile al seguente:

YAML

```
---  
version: 1  
backendName: ExampleBackend  
storageDriverName: ontap-san  
managementLIF: 10.0.0.1  
svm: svm_nfs  
username: vsadmin  
password: password
```

JSON

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

Tenete presente che la definizione del backend è l'unico posto in cui le credenziali vengono archiviate in testo normale. Dopo la creazione del backend, nomi utente e password vengono codificati in Base64 e archiviati come segreti Kubernetes. La creazione o l'aggiornamento di un backend è l'unico passaggio che richiede la conoscenza delle credenziali. Pertanto, si tratta di un'operazione riservata all'amministratore, da eseguire dall'amministratore di Kubernetes/storage.

Abilita l'autenticazione basata sul certificato

I backend nuovi ed esistenti possono utilizzare un certificato e comunicare con il backend ONTAP. Sono richiesti tre parametri nella definizione del backend.

- `clientCertificate`: Valore codificato in Base64 del certificato client.
- `clientPrivateKey`: Valore codificato in Base64 della chiave privata associata.
- `trustedCACertificate`: Valore codificato in Base64 del certificato della CA fidata. Se si utilizza una CA fidata, questo parametro deve essere fornito. Questo può essere ignorato se non si utilizza una CA fidata.

Un tipico flusso di lavoro prevede i seguenti passaggi.

Passaggi

1. Generare un certificato e una chiave client. Durante la generazione, impostare Common Name (CN) sull'utente ONTAP con cui autenticarsi.

```
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. Aggiungere un certificato CA attendibile al cluster ONTAP. Questa operazione potrebbe essere già gestita dall'amministratore dello storage. Ignorare se non viene utilizzata una CA attendibile.

```
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. Installare il certificato e la chiave del client (dal punto 1) sul cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```



Dopo aver eseguito questo comando, ONTAP richiede l'inserimento del certificato. Incolla il contenuto del `k8senv.pem` file generato nel passaggio 1, quindi inserisci `END` per completare l'installazione.

4. Confermare che il ruolo di login di sicurezza ONTAP supporta `cert` il metodo di autenticazione.

```
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. Verifica l'autenticazione utilizzando il certificato generato. Sostituisci `<ONTAP Management LIF>` e `<vserver name>` con l'IP LIF di gestione e il nome 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. Codifica il certificato, la chiave e il certificato CA affidabile con Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
```

```
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Crea il backend utilizzando i valori ottenuti nel passaggio precedente.

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "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 |
+-----+-----+-----+
+-----+-----+

```

Aggiorna i metodi di autenticazione o ruota le credenziali

È possibile aggiornare un backend esistente per utilizzare un metodo di autenticazione diverso o per ruotare le credenziali. Questo funziona in entrambi i modi: i backend che utilizzano nome utente/password possono essere aggiornati per utilizzare certificati; i backend che utilizzano certificati possono essere aggiornati per utilizzare nome utente/password. Per fare ciò, è necessario rimuovere il metodo di autenticazione esistente e aggiungere il nuovo metodo di autenticazione. Quindi utilizzare il file backend.json aggiornato contenente i parametri richiesti per eseguire `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 |
+-----+-----+-----+
+-----+-----+

```



Quando si ruotano le password, l'amministratore dello storage deve prima aggiornare la password dell'utente su ONTAP. Questo è seguito da un aggiornamento del backend. Quando si ruotano i certificati, è possibile aggiungere più certificati all'utente. Il backend viene quindi aggiornato per utilizzare il nuovo certificato, dopo di che il vecchio certificato può essere eliminato dal cluster ONTAP.

L'aggiornamento di un backend non interrompe l'accesso ai volumi già creati, né influisce sulle connessioni al volume effettuate successivamente. Un aggiornamento del backend riuscito indica che Trident può comunicare con il backend ONTAP e gestire le future operazioni sui volumi.

Crea un ruolo personalizzato ONTAP per Trident

È possibile creare un ruolo di cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore ONTAP per eseguire operazioni in Trident. Quando si include il nome utente in una configurazione backend di Trident, Trident utilizza il ruolo di cluster ONTAP creato per eseguire le operazioni.

Fare riferimento a ["Generatore di ruoli personalizzati Trident"](#) per ulteriori informazioni sulla creazione di ruoli personalizzati Trident.

Utilizzo di ONTAP CLI

1. Crea un nuovo ruolo utilizzando il seguente comando:

```
security login role create <role_name\> -cmddirname "command" -access all
-vserver <svm_name\>
```

2. Crea un nome utente per l'utente 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. Assegna il ruolo all'utente:

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

Utilizzo di System Manager

Eseguire i seguenti passaggi in ONTAP System Manager:

1. Crea un ruolo personalizzato:

- Per creare un ruolo personalizzato a livello di cluster, selezionare **Cluster > Settings**.

(Oppure) Per creare un ruolo personalizzato a livello SVM, selezionare **Archiviazione > Storage VM > required svm> Impostazioni > Utenti e ruoli**.

- Selezionare l'icona della freccia (→) accanto a **Users and Roles**.
- Seleziona **+Add in Roles**.
- Definisci le regole per il ruolo e fai clic su **Save**.

2. Mappa il ruolo all'utente Trident: + Esegui i seguenti passaggi nella pagina **Utenti e ruoli**:

- Selezionare l'icona Aggiungi + sotto **Utenti**.
- Selezionare il nome utente richiesto e selezionare un ruolo nel menu a discesa per **Role**.
- Fare clic su **Save**.

Per maggiori informazioni, consultare le seguenti pagine:

- ["Ruoli personalizzati per l'amministrazione di ONTAP"](#) o ["Definisci ruoli personalizzati"](#)
- ["Lavorare con ruoli e utenti"](#)

Autenticare le connessioni con CHAP bidirezionale

Trident può autenticare le sessioni iSCSI con CHAP bidirezionale per i `ontap-san` e `ontap-san-economy` driver. Ciò richiede l'abilitazione dell'opzione `useCHAP` nella definizione del backend. Quando impostato su `true`, Trident configura la sicurezza dell'initiator predefinito dell'SVM su CHAP bidirezionale e imposta il nome utente e i segreti dal file di backend. NetApp consiglia di utilizzare CHAP bidirezionale per autenticare le connessioni. Vedere la seguente configurazione di esempio:

```
---  
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
```



Il `useCHAP` parametro è un'opzione booleana che può essere configurata una sola volta. Per impostazione predefinita, è impostato su `false`. Dopo averlo impostato su `true`, non è possibile impostarlo su `false`.

Oltre a `useCHAP=true`, i campi `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername` e `chapUsername` devono essere inclusi nella definizione del backend. I segreti possono essere modificati dopo la creazione di un backend eseguendo `tridentctl update`.

Come funziona

Impostando `useCHAP` su `true`, l'amministratore dello storage indica a Trident di configurare CHAP sul backend dello storage. Ciò include quanto segue:

- Configurazione di CHAP sull'SVM:
 - Se il tipo di sicurezza predefinito dell'iniziatore SVM è `none` (impostato per impostazione predefinita) e non sono presenti LUN preesistenti nel volume, Trident imposterà il tipo di sicurezza predefinito su CHAP e procederà alla configurazione del nome utente e dei segreti dell'iniziatore e del target CHAP.
 - Se l'SVM contiene LUN, Trident non abiliterà CHAP sull'SVM. Questo garantisce che l'accesso alle LUN già presenti sull'SVM non sia limitato.
- Configurazione del nome utente e dei segreti dell'iniziatore e del target CHAP; queste opzioni devono essere specificate nella configurazione del backend (come mostrato sopra).

Dopo la creazione del backend, Trident crea un corrispondente `tridentbackend` CRD e memorizza i segreti CHAP e i nomi utente come segreti Kubernetes. Tutti i PV creati da Trident su questo backend verranno montati e collegati tramite CHAP.

Ruota le credenziali e aggiorna i backend

È possibile aggiornare le credenziali CHAP aggiornando i parametri CHAP nel `backend.json` file. Ciò richiederà l'aggiornamento dei segreti CHAP e l'utilizzo del `tridentctl update` comando per riflettere queste modifiche.



Quando si aggiornano i segreti CHAP per un backend, è necessario utilizzare `tridentctl` per aggiornare il backend. Non aggiornare le credenziali sul cluster di storage utilizzando ONTAP CLI o ONTAP System Manager, poiché Trident non sarà in grado di rilevare queste modifiche.

```
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-4378-8a33-1a472ffbeeb5c |
online | 7 |
+-----+-----+-----+-----+
+-----+-----+

```

Le connessioni esistenti non saranno interessate; continueranno a rimanere attive se le credenziali vengono aggiornate da Trident sulla SVM. Le nuove connessioni utilizzano le credenziali aggiornate e le connessioni esistenti continuano a rimanere attive. La disconnessione e la riconnessione dei vecchi PV comporterà l'utilizzo delle credenziali aggiornate.

Opzioni ed esempi di configurazione SAN ONTAP

Crea e usa i driver SAN ONTAP con la tua installazione di Trident. Questa sezione fornisce esempi di configurazione del backend e dettagli per la mappatura dei backend a StorageClasses. ["Sistemi ASA r2"](#) differiscono dagli altri sistemi ONTAP (ASA, AFF e FAS) nell'implementazione del loro livello di storage. Queste variazioni influiscono sull'uso di alcuni parametri come indicato. ["Scopri di più sulle differenze tra i sistemi ASA r2 e gli altri sistemi ONTAP"](#). Nella configurazione del backend di Trident, non devi specificare che il tuo sistema è ASA r2. Quando selezioni `ontap-san` come `storageDriverName`, Trident rileva automaticamente ASA r2 o altri sistemi ONTAP. Alcuni parametri di configurazione del backend non sono applicabili ai sistemi ASA r2 come indicato nella tabella seguente.



Solo il `ontap-san` driver (con protocolli iSCSI, NVMe/TCP e FC) è supportato per i sistemi ASA r2.

Opzioni di configurazione del backend

A partire dalla versione 26.06, puoi abilitare il posizionamento bilanciato di ONTAP così che ONTAP selezioni l'aggregato per i nuovi volumi. Consulta ["Usa un posizionamento bilanciato con i backend ONTAP"](#) per i requisiti e gli esempi.

Consulta la tabella seguente per le opzioni di configurazione del backend:

Parametro	Descrizione	Predefinito
version		Sempre 1
storageDriverName	Nome del driver di archiviazione. Non puoi modificarlo dopo la creazione. Per aggiornare questo parametro, devi creare un nuovo backend.	ontap-san o ontap-san-economy
backendName	Nome personalizzato o lo storage backend	Nome driver + "_" + dataLIF
managementLIF	<p>Indirizzo IP di un cluster o di una LIF di gestione SVM.</p> <p>È possibile specificare un domain name pienamente qualificato (FQDN).</p> <p>Può essere impostato per usare indirizzi IPv6 se hai installato Trident usando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p> <p>Per un passaggio senza interruzioni di MetroCluster, vedere Esempio di MetroCluster.</p> <div>  <p>Se si utilizzano le credenziali "vsadmin", managementLIF deve essere quella dell'SVM; se si utilizzano le credenziali "admin", managementLIF deve essere quella del cluster.</p> </div>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Indirizzo IP del protocollo LIF. Può essere impostato per usare indirizzi IPv6 se hai installato Trident usando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Non specificare per iSCSI. Trident utilizza "ONTAP Selective LUN Map" per rilevare i LIF iSCSI necessari per stabilire una sessione multipath. Viene generato un avviso se dataLIF è definito esplicitamente. Omettere per MetroCluster. Vedi il Esempio di MetroCluster.</p>	Derivato dall'SVM
svm	Macchina virtuale di storage da utilizzare Ometti per MetroCluster. Vedi il Esempio di MetroCluster .	Derivato se viene specificato un SVM managementLIF

Parametro	Descrizione	Predefinito
useCHAP	Utilizzare CHAP per autenticare iSCSI per i driver SAN ONTAP [Booleano]. Impostare su <code>true</code> per consentire a Trident di configurare e utilizzare CHAP bidirezionale come autenticazione predefinita per l'SVM specificato nel backend. Per i dettagli, fai riferimento a "Prepararsi a configurare il backend con i driver ONTAP SAN" . Non supportato per FCP o NVMe/TCP.	<code>false</code>
chapInitiatorSecret	Segreto dell'iniziatore CHAP. Obbligatorio se <code>useCHAP=true</code>	<code>""</code>
labels	Set di etichette arbitrarie in formato JSON da applicare ai volumi	<code>""</code>
chapTargetInitiatorSecret	Segreto dell'iniziatore di destinazione CHAP. Obbligatorio se <code>useCHAP=true</code>	<code>""</code>
chapUsername	Nome utente in entrata. Obbligatorio se <code>useCHAP=true</code>	<code>""</code>
chapTargetUsername	Nome utente di destinazione. Obbligatorio se <code>useCHAP=true</code>	<code>""</code>
clientCertificate	Valore codificato in Base64 del certificato client. Utilizzato per l'autenticazione basata su certificato	<code>""</code>
clientPrivateKey	Valore codificato in Base64 della chiave privata del client. Utilizzato per l'autenticazione basata su certificato	<code>""</code>
trustedCACertificate	Valore codificato in Base64 del certificato CA attendibile. Opzionale. Utilizzato per l'autenticazione basata su certificato.	<code>""</code>
username	Nome utente necessario per comunicare con il cluster ONTAP. Utilizzata per l'autenticazione basata sulle credenziali. Per l'autenticazione Active Directory, vedere "Autenticare Trident a un backend SVM utilizzando le credenziali di Active Directory" .	<code>""</code>
password	Password necessaria per comunicare con il cluster ONTAP. Utilizzata per l'autenticazione basata sulle credenziali. Per l'autenticazione Active Directory, vedere "Autenticare Trident a un backend SVM utilizzando le credenziali di Active Directory" .	<code>""</code>
svm	Macchina virtuale di storage da utilizzare	Derivato se viene specificato un <code>SVM managementLIF</code>
storagePrefix	Prefisso utilizzato durante il provisioning di nuovi volumi nell'SVM. Non può essere modificato in seguito. Per aggiornare questo parametro, devi creare un nuovo backend.	<code>trident</code>

Parametro	Descrizione	Predefinito
aggregate	<p>Aggregato per il provisioning (facoltativo; se impostato, deve essere assegnato all'SVM). Per il <code>ontap-nas-flexgroup</code> driver, questa opzione viene ignorata. Se non assegnato, è possibile utilizzare uno qualsiasi degli aggregati disponibili per il provisioning di un volume FlexGroup.</p> <div>  <p>Quando l'aggregato viene aggiornato in SVM, viene aggiornato automaticamente anche in Trident tramite polling di SVM, senza dover riavviare il Trident Controller. Quando hai configurato un aggregato specifico in Trident per il provisioning dei volumi, se l'aggregato viene rinominato o spostato fuori da SVM, il backend passa allo stato di errore in Trident durante il polling dell'aggregato SVM. Devi cambiare l'aggregato con uno presente su SVM oppure rimuoverlo del tutto per riportare online il backend.</p> </div> <p>Non specificare per i sistemi ASA r2.</p> <p>Non specificare quando <code>useBalancedPlacement</code> è impostato su <code>true</code>.</p>	""
useBalancedPlacement	<p>Delega la selezione dell'aggregato per i nuovi volumi a ONTAP [Boolean]. Richiede ONTAP 9.19.1 o versioni successive e <code>useREST</code> impostato su <code>true</code>. Non può essere combinato con <code>aggregate</code>.</p> <p>Consulta "Usa un posizionamento bilanciato con i backend ONTAP" per i requisiti e gli esempi.</p>	false
limitAggregateUsage	<p>Il provisioning fallisce se l'utilizzo supera questa percentuale. Se si utilizza un Amazon FSx for NetApp ONTAP backend, non specificare <code>limitAggregateUsage</code>. I <code>fsxadmin</code> e <code>vsadmin</code> forniti non contengono le autorizzazioni necessarie per recuperare l'utilizzo aggregato e limitarlo tramite Trident. Non specificare per i sistemi ASA r2.</p>	"" (non applicato per impostazione predefinita)
limitVolumeSize	<p>Il provisioning fallisce se la dimensione del volume richiesto supera questo valore. Limita anche la dimensione massima dei volumi che gestisce per LUN.</p>	"" (non applicato per impostazione predefinita)
lunsPerFlexvol	<p>Numero massimo di LUN per FlexVol, deve essere nell'intervallo [50, 200]</p>	100

Parametro	Descrizione	Predefinito
debugTraceFlags	Flag di debug da usare per la risoluzione dei problemi. Esempio, {"api":false, "method":true} non usare a meno che non si stia eseguendo una risoluzione dei problemi e sia necessario un dump dettagliato del registro.	null
useREST	<p>Parametro booleano per utilizzare le API REST di ONTAP.</p> <div> <p><code>`useREST`</code> Quando impostato su <code>`true`</code>, Trident utilizza le ONTAP REST APIs per comunicare con il backend; quando impostato su <code>`false`</code>, Trident utilizza le chiamate ONTAPI (ZAPI) per comunicare con il backend. Questa funzione richiede ONTAP 9.11.1 e versioni successive. Inoltre, il ruolo di login ONTAP utilizzato deve avere accesso all'applicazione <code>`ontapi`</code>. Questo è soddisfatto dai ruoli predefiniti <code>`vsadmin`</code> e <code>`cluster-admin`</code>. A partire dalla release Trident 24.06 e ONTAP 9.15.1 o versioni successive, <code>`useREST`</code> è impostato su <code>`true`</code> per impostazione predefinita; modificare <code>`useREST`</code> su <code>`false`</code> per utilizzare le chiamate ONTAPI (ZAPI).</p> </div> <p>useREST è pienamente qualificato per NVMe/TCP.</p> <div>  <p>NVMe è supportato solo con le API REST di ONTAP e non è supportato con ONTAPI (ZAPI).</p> </div> <p>Se specificato, impostare sempre su <code>true</code> per i sistemi ASA r2.</p>	true per ONTAP 9.15.1 o versioni successive, altrimenti false.
sanType	Utilizzare per selezionare iscsi per iSCSI, nvme per NVMe/TCP o fcp per SCSI over Fibre Channel (FC).	iscsi se vuoto

Parametro	Descrizione	Predefinito
formatOptions	<p>Usa <code>formatOptions</code> per specificare gli argomenti della riga di comando per il comando <code>mkfs</code>, che viene applicato ogni volta che un volume viene formattato. Questo ti permette di formattare il volume secondo le tue preferenze. Assicurati di specificare le <code>formatOptions</code> in modo simile alle opzioni del comando <code>mkfs</code>, escludendo il percorso del dispositivo. Esempio: <code>"-E nodiscard"</code></p> <p>Supportato per <code>ontap-san</code> e <code>ontap-san-economy</code> driver con protocollo iSCSI. Inoltre, supportato per sistemi ASA r2 quando si utilizzano i protocolli iSCSI e NVMe/TCP.</p>	
limitVolumePoolSize	Dimensione massima richiedibile FlexVol quando si usano LUN nel backend <code>ontap-san-economy</code> .	"" (non applicato per impostazione predefinita)
denyNewVolumePools	Restringe i backend dal <code>ontap-san-economy</code> creare nuovi volumi FlexVol per contenere le loro LUN. Solo i FlexVol preesistenti vengono utilizzati per il provisioning di nuovi PV.	

Raccomandazioni per l'utilizzo di formatOptions

Trident raccomanda le seguenti opzioni per accelerare il processo di formattazione:

- **-E nodiscard (ext3, ext4):** Non tentare di scartare i blocchi al momento di `mkfs` (scartare i blocchi inizialmente è utile sui dispositivi a stato solido e sullo storage sparse / con thin provisioning). Questo sostituisce l'opzione deprecata `"-K"` ed è applicabile ai file system `ext3`, `ext4`.
- **-K (xfs):** Non tentare di scartare i blocchi al momento di `mkfs`. Questa opzione è applicabile al file system `xfs`.

Autenticare Trident a un backend SVM utilizzando le credenziali di Active Directory

È possibile configurare Trident per autenticarsi a un backend SVM utilizzando le credenziali di Active Directory (AD). Prima che un account AD possa accedere all'SVM, è necessario configurare l'accesso del domain controller AD al cluster o all'SVM. Per l'amministrazione del cluster con un account AD, è necessario creare un domain tunnel. Per i dettagli, fai riferimento a ["Configurare l'accesso del domain controller Active Directory in ONTAP"](#).

passi

1. Configurare le impostazioni del Domain Name System (DNS) per una SVM di backend:

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

2. Eseguire il seguente comando per creare un account computer per la SVM in Active Directory:

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

3. Utilizzare questo comando per creare un utente o un gruppo AD per gestire il cluster o SVM

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

4. Nel file di configurazione del backend Trident, impostare i parametri `username` e `password` rispettivamente sul nome utente o del gruppo AD e sulla password.

Opzioni di configurazione del backend per il provisioning dei volumi

È possibile controllare il provisioning predefinito utilizzando queste opzioni nella `defaults` sezione della configurazione. Per un esempio, vedere gli esempi di configurazione riportati di seguito.

Parametro	Descrizione	Predefinito
<code>spaceAllocation</code>	Allocazione dello spazio per le LUN	"true" Se specificato, impostare su true per sistemi ASA r2.
<code>spaceReserve</code>	Modalità di prenotazione dello spazio; "none" (con thin provisioning) o "volume" (con thick provisioning). Impostare su none per sistemi ASA r2.	"none"
<code>snapshotPolicy</code>	Policy di Snapshot da utilizzare. Impostare su none per sistemi ASA r2.	"none"
<code>qosPolicy</code>	Gruppo di policy QoS da assegnare ai volumi creati. Scegliere uno tra <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> per pool di storage/backend. L'utilizzo di gruppi di policy QoS con Trident richiede ONTAP 9.8 o versioni successive. È consigliabile utilizzare un gruppo di policy QoS non condiviso e assicurarsi che il gruppo di policy venga applicato a ciascun componente singolarmente. Un gruppo di policy QoS condiviso impone il limite massimo per il throughput di tutti i carichi di lavoro.	""
<code>adaptiveQosPolicy</code>	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegliere uno tra <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> per storage pool/backend	""
<code>snapshotReserve</code>	Percentuale di volume riservata alle snapshot. Non specificare per i sistemi ASA r2.	"0" se <code>snapshotPolicy</code> è "none", altrimenti ""
<code>splitOnClone</code>	Dividere un clone dal suo genitore al momento della creazione	"false"
<code>encryption</code>	Abilita NetApp Volume Encryption (NVE) sul nuovo volume; il valore predefinito è <code>false</code> . NVE deve essere concesso in licenza e abilitato sul cluster per usare questa opzione. Se NAE è abilitato sul backend, qualsiasi volume effettuato il provisioning in Trident è abilitato per NAE. Per ulteriori informazioni, consulta: "Come funziona Trident con NVE e NAE" .	"false" Se specificato, impostare su true per i sistemi ASA r2.
<code>luksEncryption</code>	Abilita la crittografia LUKS. Fai riferimento a "Usa Linux Unified Key Setup (LUKS)" .	"" Impostato su false per i sistemi ASA r2.

Parametro	Descrizione	Predefinito
tieringPolicy	Criterio di tiering da utilizzare "none" Non specificare per i sistemi ASA r2.	
nameTemplate	Modello per creare nomi di volume personalizzati.	""

Esempi di provisioning del volume

Ecco un esempio con i valori predefiniti:

```

---
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'

```



Per tutti i volumi creati utilizzando il `ontap-san` driver, Trident aggiunge un ulteriore 10% di capacità al FlexVol per ospitare i metadati del LUN. Il LUN viene predisposto con la dimensione esatta richiesta dall'utente nel PVC. Trident aggiunge il 10% al FlexVol (mostrato come Dimensione disponibile in ONTAP). Ora ottieni la quantità di capacità utilizzabile che hai richiesto. Questa modifica impedisce anche che i LUN diventino di sola lettura, a meno che lo spazio disponibile non sia completamente utilizzato. Questo non si applica a `ontap-san-economy`.

Per i backend che definiscono `snapshotReserve`, Trident calcola la dimensione dei volumi come segue:

```

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

```

L'1,1 è il 10 per cento in più che Trident aggiunge a FlexVol per ospitare i metadati della LUN. Per `snapshotReserve = 5%` e `PVC request = 5 GiB`, la dimensione totale del volume è 5,79 GiB e la dimensione

disponibile è 5,5 GiB. Il comando `volume show` dovrebbe mostrare risultati simili a questo esempio:

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

Attualmente, il ridimensionamento è l'unico modo per utilizzare il nuovo calcolo per un volume esistente.

Esempi di configurazione minima

Gli esempi seguenti mostrano configurazioni di base che lasciano la maggior parte dei parametri ai valori predefiniti. Questo è il modo più semplice per definire un backend.



Se si utilizza Amazon FSx su NetApp ONTAP con Trident, NetApp consiglia di specificare i nomi DNS per i LIF invece degli indirizzi IP.

▼ Esempio SAN ONTAP

Questa è una configurazione di base che utilizza il `ontap-san` driver.

```
---
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>
```

▼ Esempio di MetroCluster

È possibile configurare il backend per evitare di dover aggiornare manualmente la definizione del backend dopo lo switchover e lo switchback durante ["Replica e recovery SVM"](#).

Per un passaggio e un ritorno senza interruzioni, specificare l'SVM utilizzando `managementLIF` e omettere i `svm` parametri. Ad esempio:

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

▼ Esempio di economia SAN ONTAP

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

▼ Esempio di autenticazione basata su certificato

In questo esempio di configurazione di base `clientCertificate`, `clientPrivateKey`, e `trustedCACertificate` (facoltativo, se si utilizza una CA attendibile) sono popolati in `backend.json` e accettano rispettivamente i valori codificati in base64 del certificato client, della chiave privata e del certificato CA attendibile.

```
---
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
```

▼ Esempi di CHAP bidirezionale

Questi esempi creano un backend con `useCHAP` impostato su `true`.

Esempio 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>
```

Esempio di CHAP economy 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>
```

▼ Esempio di posizionamento bilanciato

Questo esempio abilita il posizionamento bilanciato di ONTAP, così che ONTAP selezioni l'aggregato per i nuovi volumi. Il posizionamento bilanciato richiede ONTAP 9.19.1 o versioni successive. Per i dettagli, fai riferimento a ["Usa un posizionamento bilanciato con i backend ONTAP"](#).

```
---
version: 1
storageDriverName: ontap-san
backendName: san-balanced-placement
managementLIF: 10.0.0.1
svm: svm_iscsi
username: vsadmin
password: <password>
useBalancedPlacement: true
```

▼ Esempio NVMe/TCP

È necessario disporre di una SVM configurata con NVMe sul backend ONTAP. Questa è una configurazione di base del backend per 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

```

▼ Esempio di SCSI su FC (FCP)

È necessario disporre di una SVM configurata con FC sul backend ONTAP. Questa è una configurazione di base del backend per 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

```

▼ Esempio di configurazione del backend con 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}}"

```

▼ formatOptions example per il driver ontap-san-economy

```

---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""

```

```

svm: svm1
username: ""
password: "!"
storagePrefix: wheelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard

```

Esempi di backend con pool virtuali

In questi file di definizione backend di esempio, vengono impostati valori predefiniti specifici per tutti i pool di storage, come `spaceReserve` a `none`, `spaceAllocation` a `false` e `encryption` a `false`. I pool virtuali sono definiti nella sezione `storage`.

Trident imposta le etichette di provisioning nel campo "Commenti". I commenti vengono impostati sul FlexVol volume. Trident copia tutte le etichette presenti su un pool virtuale sul volume di storage al momento del provisioning. Per comodità, gli amministratori dello storage possono definire etichette per pool virtuale e raggruppare i volumi in base all'etichetta.

In questi esempi, alcuni pool di storage impostano i propri `spaceReserve`, `spaceAllocation` e `encryption` valori, mentre alcuni pool sovrascrivono i valori predefiniti.

▼ Esempio 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"

```

▼ Esempio di economia SAN ONTAP

```

---
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"

```

▼ Esempio 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"
```

Mappa i backend a StorageClasses

Le seguenti StorageClass definizioni si riferiscono a [Esempi di backend con pool virtuali](#). Utilizzando il campo `parameters.selector`, ciascuna StorageClass indica quali pool virtuali puoi usare per ospitare un volume. Ora il volume ha le caratteristiche definite nel pool virtuale scelto.

- Il `protection-gold` StorageClass mappa il primo pool virtuale nel `ontap-san` backend. Questo è l'unico pool che offre protezione di livello oro.

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

- La `protection-not-gold` StorageClass corrisponde al secondo e al terzo pool virtuale nel `ontap-san` backend. Questi sono gli unici pool che offrono un livello di protezione diverso da gold.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- La `app-mysqldb` StorageClass corrisponde al terzo pool virtuale nel `ontap-san-economy` backend. Questo è l'unico pool che offre la configurazione del pool di storage per le app di tipo `mysqldb`.

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

- La `protection-silver-creditpoints-20k` `StorageClass` corrisponde al secondo pool virtuale nel `ontap-san` backend. Questo è l'unico pool che offre protezione di livello argento e 20000 punti credito.

```
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"
```

- La `creditpoints-5k` `StorageClass` corrisponde al terzo pool virtuale nel `ontap-san` backend e al quarto pool virtuale nel `ontap-san-economy` backend. Queste sono le uniche offerte di pool con 5000 creditpoints.

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

- La `my-test-app-sc` `StorageClass` corrisponde al `testAPP` pool virtuale nel `ontap-san` driver con `sanType: nvme`. Questo è l'unico pool che offre `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"
```

Trident decide quale pool virtuale viene selezionato e garantisce che il requisito di storage sia soddisfatto.

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.