



Driver NAS ONTAP

Trident

NetApp
October 29, 2026

Sommario

Driver NAS ONTAP	1
Panoramica del driver ONTAP NAS	1
Dettagli del driver ONTAP NAS	1
Permessi utente	1
Prepararsi a configurare un backend con i driver ONTAP NAS	2
Requisiti	2
Autenticare il backend ONTAP	2
Gestisci le policy di esportazione NFS	7
Prepararsi al provisioning dei volumi SMB	10
Opzioni ed esempi di configurazione NAS ONTAP	14
Opzioni di configurazione del backend	14
Opzioni di configurazione del backend per il provisioning dei volumi	19
Esempi di configurazione minima	22
Esempi di backend con pool virtuali	26
Mappa i backend a StorageClasses	29
Aggiorna dataLIF dopo la configurazione iniziale	31
Esempi di SMB sicuro	31

Driver NAS ONTAP

Panoramica del driver ONTAP NAS

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

Dettagli del driver ONTAP NAS

Trident fornisce i seguenti driver di storage NAS 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-nas	NFS SMB	Filesystem	RWO, ROX, RWX, RWOP	"", nfs, smb
ontap-nas-economy	NFS SMB	Filesystem	RWO, ROX, RWX, RWOP	"", nfs, smb
ontap-nas-flexgroup	NFS SMB	Filesystem	RWO, ROX, RWX, RWOP	"", nfs, smb



- 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 richiederà API aggiuntive di cui bisognerebbe tenere conto, rendendo gli aggiornamenti difficili e soggetti a errori.

Prepararsi a configurare un backend con i driver ONTAP NAS

Comprendere i requisiti, le opzioni di autenticazione e le policy di esportazione per la configurazione di un backend ONTAP con driver ONTAP NAS. A partire dalla versione 25.10, NetApp Trident supporta ["NetApp AFX sistema storage"](#). NetApp AFX storage systems differiscono dagli altri sistemi ONTAP (ASA, AFF e FAS) nell'implementazione del loro livello di storage. Nella configurazione del backend Trident non è necessario specificare che il sistema è AFX. Quando si seleziona `ontap-nas` come `storageDriverName`, Trident rileva automaticamente i sistemi AFX.



Solo il `ontap-nas` driver (con protocollo NFS) è supportato per i sistemi AFX; il protocollo SMB non è supportato.

Requisiti

- Per tutti i backend ONTAP, Trident richiede che almeno un aggregato sia assegnato all'SVM.
- È possibile eseguire più di un driver e creare classi di archiviazione che puntano all'uno o all'altro. Ad esempio, si può configurare una classe Gold che utilizza il `ontap-nas` driver e una classe Bronze che utilizza il `ontap-nas-economy` driver.
- Su tutti i nodi worker di Kubernetes devono essere installati gli strumenti NFS appropriati. Per ulteriori dettagli, consulta ["qui"](#).
- Trident supporta volumi SMB montati solo su pod in esecuzione su nodi Windows. Per i dettagli, fai riferimento a [Prepararsi al provisioning dei volumi SMB](#).

Autenticare il backend ONTAP

Trident offre due modalità di autenticazione per un backend ONTAP.

- Basato su credenziali: Questa modalità richiede autorizzazioni sufficienti al backend ONTAP. Si consiglia di utilizzare un account associato a un ruolo di login di sicurezza predefinito, come `admin` o `vsadmin` per garantire la massima compatibilità con le versioni ONTAP.
- Basato su certificato: Questa modalità richiede un certificato installato sul backend per Trident per comunicare con un cluster ONTAP. 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-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
    "name": "secret-backend-creds"
  }
}
```

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/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 su certificati

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=vsadmin"
```

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
```

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

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

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. È necessario assicurarsi che il LIF abbia la sua service policy impostata su `default-data-management`.

```
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-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |                               UUID                               |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```

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 update backend`.

```
cat cert-backend-updated.json
```

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
```

NAME	STORAGE DRIVER	UUID
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214
STATE	VOLUMES	
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:**

- a. 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**.

- b. Selezionare l'icona della freccia (→) accanto a **Users and Roles**.

- c. Seleziona **+Add in Roles**.

- d. 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**:

- a. Selezionare l'icona Aggiungi **+** sotto **Utenti**.

- b. Selezionare il nome utente richiesto e selezionare un ruolo nel menu a discesa per **Role**.

- c. 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"](#)

Gestisci le policy di esportazione NFS

Trident utilizza le policy di esportazione NFS per controllare l'accesso ai volumi che fornisce.

Trident offre due opzioni quando si lavora con le policy di esportazione:

- Trident può gestire dinamicamente la policy di esportazione stessa; in questa modalità operativa, l'amministratore dello storage specifica un elenco di blocchi CIDR che rappresentano gli indirizzi IP ammissibili. Trident aggiunge automaticamente gli IP dei nodi che rientrano in questi intervalli alla policy di esportazione al momento della pubblicazione. In alternativa, quando non vengono specificati CIDR, tutti gli IP unicast a livello globale trovati sul nodo a cui si sta pubblicando il volume verranno aggiunti alla policy di esportazione.
- Gli amministratori dello storage possono creare una policy di esportazione e aggiungere regole manualmente. Trident utilizza la policy di esportazione predefinita a meno che nella configurazione non venga specificato un nome diverso per la policy di esportazione.

Gestisci dinamicamente le policy di esportazione

Trident offre la possibilità di gestire dinamicamente le policy di esportazione per i backend ONTAP. Questo offre all'amministratore dello storage la possibilità di specificare uno spazio di indirizzi consentito per gli IP dei nodi worker, invece di definire manualmente regole esplicite. Questo semplifica notevolmente la gestione delle policy di esportazione; le modifiche alla policy di esportazione non richiedono più l'intervento manuale sul cluster di storage. Inoltre, questo aiuta a limitare l'accesso al cluster di storage solo ai nodi worker che stanno montando i volumi e hanno IP nell'intervallo specificato, supportando una gestione automatizzata e a grana fine.



Non utilizzare il Network Address Translation (NAT) quando si usano le policy di esportazione dinamiche. Con il NAT, lo storage controller vede l'indirizzo NAT del frontend e non l'indirizzo IP effettivo dell'host, quindi l'accesso sarà negato quando non viene trovata alcuna corrispondenza nelle regole di esportazione.

Esempio

Ci sono due opzioni di configurazione che devono essere utilizzate. Ecco un esempio di definizione backend:

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
  - 192.168.0.0/24
autoExportPolicy: true
```



Quando si utilizza questa funzione, è necessario assicurarsi che la giunzione principale nell'SVM abbia una policy di esportazione precedentemente creata con una regola di esportazione che permetta il blocco CIDR del nodo (ad esempio la policy di esportazione predefinita). Seguire sempre la best practice raccomandata da NetApp di dedicare un SVM per Trident.

Ecco una spiegazione di come funziona questa funzione utilizzando l'esempio sopra:

- `autoExportPolicy` è impostato su `true`. Questo indica che Trident crea una policy di esportazione per ogni volume fornito con questo backend per la SVM `svm1` e gestisce l'aggiunta e l'eliminazione delle regole utilizzando blocchi di indirizzi `autoExportCIDRs`. Fino a quando un volume non è collegato a un nodo, il volume utilizza una policy di esportazione vuota senza regole per impedire accessi indesiderati a quel volume. Quando un volume viene pubblicato su un nodo, Trident crea una policy di esportazione con lo stesso nome del qtree sottostante contenente l'IP del nodo all'interno del blocco CIDR specificato. Questi IP verranno anche aggiunti alla policy di esportazione utilizzata dal volume FlexVol padre
 - Ad esempio:
 - UUID backend `403b5326-8482-40db-96d0-d83fb3f4daec`
 - `autoExportPolicy` impostato su `true`
 - prefisso storage `trident`
 - PVC UUID `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
 - Il qtree denominato `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` crea una policy di esportazione per il FlexVol denominato `trident-403b5326-8482-40db96d0-d83fb3f4daec`, una policy di esportazione per il qtree denominato `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` e una policy di esportazione vuota denominata `trident_empty` sull'SVM. Le regole per la policy di esportazione del FlexVol saranno un superset di tutte le regole contenute nelle policy di esportazione dei qtree. La policy di esportazione vuota sarà riutilizzata da tutti i volumi che non sono collegati.
- `autoExportCIDRs` contiene un elenco di blocchi di indirizzi. Questo campo è opzionale e il valore predefinito è `["0.0.0.0/0", "::/0"]`. Se non è definito, Trident aggiunge tutti gli indirizzi unicast con ambito globale trovati sui nodi worker con pubblicazioni.

In questo esempio, viene fornito lo spazio di indirizzi `192.168.0.0/24`. Ciò indica che gli IP dei nodi Kubernetes che rientrano in questo intervallo di indirizzi con pubblicazioni saranno aggiunti alla export policy che Trident crea. Quando Trident registra un nodo su cui viene eseguito, recupera gli indirizzi IP del nodo e li controlla rispetto ai blocchi di indirizzi forniti in `autoExportCIDRs`. Al momento della pubblicazione, dopo aver filtrato gli IP, Trident crea le regole di export policy per gli IP client del nodo su cui sta pubblicando.

È possibile aggiornare `autoExportPolicy` e `autoExportCIDRs` per i backend dopo averli creati. È possibile aggiungere nuovi CIDR per un backend gestito automaticamente o eliminare i CIDR esistenti. Prestare attenzione quando si eliminano i CIDR per garantire che le connessioni esistenti non vengano interrotte. È anche possibile scegliere di disabilitare `autoExportPolicy` per un backend e tornare a una policy di esportazione creata manualmente. Questo richiederà l'impostazione del parametro `exportPolicy` nella configurazione del backend.

Dopo che Trident ha creato o aggiornato un backend, puoi verificare il backend utilizzando `tridentctl` o il corrispondente `tridentbackend` CRD:

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
```

```

autoExportPolicy: true
backendName: ontap_nas_auto_export
chapInitiatorSecret: ""
chapTargetInitiatorSecret: ""
chapTargetUsername: ""
chapUsername: ""
dataLIF: 192.168.0.135
debug: false
debugTraceFlags: null
defaults:
  encryption: "false"
  exportPolicy: <automatic>
  fileSystemType: ext4

```

Quando un nodo viene rimosso, Trident controlla tutte le policy di esportazione per rimuovere le regole di accesso corrispondenti al nodo. Rimuovendo questo IP del nodo dalle policy di esportazione dei backend gestiti, Trident impedisce i montaggi non autorizzati, a meno che questo IP non venga riutilizzato da un nuovo nodo nel cluster.

Per i backend già esistenti, l'aggiornamento del backend con `tridentctl update backend` garantisce che Trident gestisca automaticamente le policy di esportazione. Questo crea due nuove policy di esportazione denominate in base all'UUID del backend e al nome del qtree quando necessario. I volumi presenti sul backend utilizzeranno le nuove policy di esportazione dopo essere stati smontati e rimontati.



L'eliminazione di un backend con policy di esportazione gestite automaticamente eliminerà la policy di esportazione creata dinamicamente. Se il backend viene ricreato, viene trattato come un nuovo backend e comporterà la creazione di una nuova policy di esportazione.

Se l'indirizzo IP di un nodo live viene aggiornato, è necessario riavviare il pod Trident sul nodo. Trident aggiornerà quindi la policy di esportazione per i backend che gestisce per riflettere questa modifica dell'IP.

Prepararsi al provisioning dei volumi SMB

Con una piccola preparazione aggiuntiva, è possibile eseguire il provisioning dei volumi SMB utilizzando `ontap-nas` driver.



È necessario configurare entrambi i protocolli NFS e SMB/CIFS sull'SVM per creare un volume SMB `ontap-nas-economy` per i cluster ONTAP on-premises. La mancata configurazione di uno di questi protocolli causerà il fallimento della creazione del volume SMB.



`autoExportPolicy` non è supportato per i volumi SMB.

Prima di iniziare

Per poter eseguire il provisioning dei volumi SMB, è necessario disporre di quanto segue.

- Un cluster Kubernetes con un nodo controller Linux e almeno un nodo worker Windows che esegue Windows Server 2022. Trident supporta volumi SMB montati solo su pod in esecuzione su nodi Windows.
- Almeno un secret di Trident contenente le credenziali di Active Directory. Per generare il secret `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- Un CSI proxy configurato come servizio Windows. Per configurare un `csi-proxy`, fare riferimento a ["GitHub: CSI Proxy"](#) o ["GitHub: CSI Proxy per Windows"](#) per i nodi Kubernetes in esecuzione su Windows.

Passaggi

1. Per ONTAP on-premises, puoi facoltativamente creare una condivisione SMB oppure Trident può crearne una per te.



Le condivisioni SMB sono necessarie per Amazon FSx per ONTAP.

È possibile creare le condivisioni SMB admin in due modi: utilizzando lo snap-in ["Microsoft Management Console"](#) Shared Folders o utilizzando la ONTAP CLI. Per creare le condivisioni SMB utilizzando la ONTAP CLI:

- a. Se necessario, crea la struttura del percorso della directory per la condivisione.

Il `vserver cifs share create` comando controlla il percorso specificato nell'opzione `-path` durante la creazione della condivisione. Se il percorso specificato non esiste, il comando fallisce.

- b. Crea una condivisione SMB associata alla SVM specificata:

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

- c. Verificare che la condivisione sia stata creata:

```
vserver cifs share show -share-name share_name
```



Consultare ["Creare una condivisione SMB"](#) per tutti i dettagli.

2. Quando si crea il backend, è necessario configurare quanto segue per specificare i volumi SMB. Per tutte le opzioni di configurazione del backend FSx per ONTAP, fare riferimento a ["Opzioni ed esempi di configurazione di FSx per ONTAP"](#).

Parametro	Descrizione	Esempio
smbShare	È possibile specificare uno dei seguenti valori: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI; un nome per consentire a Trident di creare la condivisione SMB; oppure è possibile lasciare il parametro vuoto per impedire l'accesso condiviso ai volumi. Questo parametro è facoltativo per ONTAP on-premises. Questo parametro è obbligatorio per Amazon FSx for ONTAP backends e non può essere vuoto.	smb-share
nasType	Deve essere impostato su smb. Se nullo, il valore predefinito è nfs.	smb
securityStyle	Stile di sicurezza per i nuovi volumi. Deve essere impostato su ntfs o mixed per i volumi SMB.	ntfs o mixed per i volumi SMB
unixPermissions	Modalità per nuovi volumi. Deve essere lasciato vuoto per i volumi SMB.	""

Abilita SMB sicuro

A partire dalla release 25.06, NetApp Trident supporta il provisioning sicuro dei volumi SMB creati utilizzando `ontap-nas` e `ontap-nas-economy` backends. Quando è abilitato l'SMB sicuro, è possibile fornire un accesso controllato alle condivisioni SMB per gli utenti e i gruppi di utenti di Active Directory (AD) utilizzando le Access Control Lists (ACLs).

Punti da ricordare

- L'importazione `ontap-nas-economy` di volumi non è supportata.
- Sono supportati solo i cloni di sola lettura per i volumi `ontap-nas-economy`.
- Se Secure SMB è abilitato, Trident ignorerà la condivisione SMB menzionata nel backend.
- L'aggiornamento dell'annotazione PVC, dell'annotazione storage class e del campo backend non aggiorna l'ACL della condivisione SMB.
- Le ACL di condivisione SMB specificate nell'annotazione del PVC clone avranno la precedenza su quelle nel PVC di origine.
- Assicurati di fornire utenti AD validi quando abiliti SMB sicuro. Gli utenti non validi non verranno aggiunti all'ACL.
- Se si fornisce lo stesso utente AD nel backend, storage class e PVC con autorizzazioni diverse, la priorità delle autorizzazioni sarà: PVC, storage class e poi backend.
- Secure SMB è supportato per `ontap-nas` le importazioni di volumi gestiti e non è applicabile alle importazioni di volumi non gestiti.

Passaggi

1. Specificare `adAdminUser` in `TridentBackendConfig` come mostrato nel seguente esempio:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
```

```

name: backend-tbc-ontap
namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret

```

2. Aggiungi l'annotazione nella storage class.

Aggiungere l'annotazione `trident.netapp.io/smbShareAdUser` alla storage class per abilitare SMB sicuro senza errori. Il valore utente specificato per l'annotazione `trident.netapp.io/smbShareAdUser` deve essere lo stesso del nome utente specificato nel smbcreds secret. È possibile scegliere una delle seguenti opzioni per `smbShareAdUserPermission`: `full_control`, `change` o `read`. L'autorizzazione predefinita è `full_control`.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate

```

1. Crea un PVC.

Il seguente esempio crea un PVC:

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4

```

```

namespace: trident
annotations:
  trident.netapp.io/snapshotDirectory: "true"
  trident.netapp.io/smbShareAccessControl: |
    read:
      - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc

```

Opzioni ed esempi di configurazione NAS ONTAP

Crea e usa i driver NAS ONTAP con la tua installazione di Trident. Questa sezione fornisce esempi di configurazione del backend e dettagli per la mappatura dei backend a StorageClasses. A partire dalla versione 25.10, NetApp Trident supporta ["Sistemi storage NetApp AFX"](#). I sistemi storage NetApp AFX differiscono dagli altri sistemi basati su ONTAP (ASA, AFF e FAS) nell'implementazione del loro livello di storage.



Solo il `ontap-nas` driver (con protocollo NFS) è supportato per i sistemi NetApp AFX; il protocollo SMB non è supportato.

Opzioni di configurazione del backend

Nella configurazione del backend di Trident, non è necessario specificare che il sistema è un NetApp AFX storage system. Quando si seleziona `ontap-nas` come `storageDriverName`, Trident rileva automaticamente il sistema storage AFX. Alcuni parametri di configurazione del backend non sono applicabili ai sistemi storage AFX.

A partire dalla versione 26.06, puoi abilitare il posizionamento bilanciato di ONTAP così che ONTAP selezioni l'aggregato per i nuovi volumi. Il posizionamento bilanciato è richiesto per i sistemi storage AFX su ONTAP 9.19.1 o versioni successive. Consulta ["Usa un posizionamento bilanciato con i backend ONTAP"](#) per i requisiti e gli esempi.

La tabella seguente mostra le opzioni di configurazione del backend:

Parametro	Descrizione	Predefinito
<code>version</code>		Sempre 1

Parametro	Descrizione	Predefinito
storageDriverName	<p>Nome del driver di archiviazione.</p> <p>Non puoi modificarlo dopo la creazione. Per aggiornare questo parametro, devi creare un nuovo backend.</p> <div>  <p>Per i sistemi NetApp AFX, è supportato solo ontap-nas.</p> </div>	ontap-nas, ontap-nas-economy, o ontap-nas-flexgroup
backendName	Nome personalizzato o lo storage backend	Nome driver + "_" + dataLIF
managementLIF	<p>Indirizzo IP di un cluster o di una LIF di gestione SVM. È possibile specificare un fully-qualified domain name (FQDN). 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]. Per un passaggio senza interruzioni di MetroCluster, vedere Esempio di MetroCluster.</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Indirizzo IP del protocollo LIF. NetApp consiglia di specificare dataLIF. Se non fornito, Trident recupera i dataLIF dall'SVM. Puoi specificare un fully-qualified domain name (FQDN) da usare per le operazioni di mount NFS, permettendoti di creare un DNS round-robin per bilanciare il carico tra più dataLIF. Può essere modificato dopo l'impostazione iniziale. Fai riferimento a . 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]. Omettere per MetroCluster. Vedi il Esempio di MetroCluster.</p>	Indirizzo specificato o derivato da SVM, se non specificato (non consigliato)
svm	Macchina virtuale di storage da utilizzare Ometti per MetroCluster. Vedi il Esempio di MetroCluster .	Derivato se viene specificato un SVM managementLIF
autoExportPolicy	Abilita la creazione e l'aggiornamento automatici delle policy di esportazione [Boolean]. Utilizzando le autoExportPolicy e autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.	falso
autoExportCIDRs	Elenco di CIDR in base ai quali filtrare gli IP dei nodi Kubernetes quando autoExportPolicy è abilitato. Utilizzando le autoExportPolicy e autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.	["0.0.0.0/0", ":::0"]
labels	Set di etichette arbitrarie in formato JSON da applicare ai volumi	""

Parametro	Descrizione	Predefinito
clientCertificate	Valore codificato in Base64 del certificato client. Utilizzato per l'autenticazione basata su certificato	""
clientPrivateKey	Valore codificato in Base64 della chiave privata del client. Utilizzato per l'autenticazione basata su certificato	""
trustedCACertificate	Valore codificato in Base64 del certificato CA attendibile. Opzionale. Utilizzato per l'autenticazione basata su certificato	""
username	Nome utente per connettersi al cluster/SVM. Utilizzata per l'autenticazione basata su credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident a un backend SVM utilizzando le credenziali di Active Directory" .	
password	Password per connettersi al cluster/SVM. Utilizzata per l'autenticazione basata su credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident a un backend SVM utilizzando le credenziali di Active Directory" .	
storagePrefix	<p>Prefisso utilizzato durante il provisioning di nuovi volumi nell'SVM. Non può essere aggiornato dopo averlo impostato</p> <div>  <p>Quando usi ontap-nas-economy e un storagePrefix di 24 o più caratteri, i qtree non hanno il prefisso di storage incluso, anche se è presente nel nome del volume.</p> </div>	"Trident"

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 dalla 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 di storage AFX.</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> <p>Se specificato, impostalo sempre su <code>true</code> per i sistemi storage AFX su ONTAP 9.19.1 o versioni successive.</p>	<code>false</code> ; <code>true</code> per sistemi di storage AFX su ONTAP 9.19.1 o versioni successive
limitAggregateUsage	<p>Il provisioning fallisce se l'utilizzo supera questa percentuale. Non si applica ad Amazon FSx per ONTAP. Non specificare per i sistemi di storage AFX.</p>	"" (non applicato per impostazione predefinita)

Parametro	Descrizione	Predefinito
flexgroupAggregateList	<p>Elenco di aggregati per il provisioning (facoltativo; se impostato, deve essere assegnato alla SVM). Tutti gli aggregati assegnati alla SVM vengono utilizzati per il provisioning di un FlexGroup volume. Supportato per il driver di storage ontap-nas-flexgroup.</p> <div>  <p>Quando l'elenco degli aggregati viene aggiornato in SVM, l'elenco viene aggiornato automaticamente in Trident tramite polling di SVM, senza dover riavviare il Trident Controller. Quando hai configurato un elenco specifico di aggregati in Trident per il provisioning dei volumi, se l'elenco degli aggregati 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'elenco degli aggregati con uno presente su SVM oppure rimuoverlo del tutto per riportare online il backend.</p> </div>	""
limitVolumeSize	Il provisioning fallisce se la dimensione del volume richiesto supera questo valore.	"" (non applicato per impostazione predefinita)
debugTraceFlags	Flag di debug da usare per la risoluzione dei problemi. Ad esempio, {"api":false, "method":true} non utilizzare debugTraceFlags a meno che non si stia risolvendo un problema e si richieda un dump dettagliato del log.	null
nasType	Configura la creazione di volumi NFS o SMB. Le opzioni sono <code>nfs</code> , <code>smb</code> o <code>null</code> . Impostando su <code>null</code> , vengono creati di default volumi NFS. Se specificato, impostare sempre su <code>nfs</code> per i sistemi di storage AFX.	<code>nfs</code>
nfsMountOptions	Elenco separato da virgole delle opzioni di montaggio NFS. Le opzioni di montaggio per i volumi persistenti di Kubernetes sono normalmente specificate nelle classi di storage, ma se non vengono specificate opzioni di montaggio in una classe di storage, Trident utilizza le opzioni di montaggio specificate nel file di configurazione del backend di storage. Se non vengono specificate opzioni di montaggio nella classe di storage o nel file di configurazione, Trident non imposta alcuna opzione di montaggio su un volume persistente associato.	""
qtreesPerFlexvol	Numero massimo di Qtree per FlexVol, deve essere nell'intervallo [50, 300]	"200"

Parametro	Descrizione	Predefinito
smbShare	È possibile specificare uno dei seguenti valori: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI; un nome per consentire a Trident di creare la condivisione SMB; oppure è possibile lasciare il parametro vuoto per impedire l'accesso condiviso ai volumi. Questo parametro è facoltativo per ONTAP on-premises. Questo parametro è obbligatorio per Amazon FSx for ONTAP backends e non può essere vuoto.	smb-share
useREST	Parametro booleano per utilizzare le API REST di ONTAP. <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). Se specificato, impostare sempre su <code>true</code> per i sistemi di storage AFX.	<code>true</code> per ONTAP 9.15.1 o versioni successive, altrimenti <code>false</code> .
limitVolumePoolSize	Dimensione massima richiedibile FlexVol quando si utilizzano Qtrees nel backend <code>ontap-nas-economy</code> .	"" (non applicato per impostazione predefinita)
denyNewVolumePools	Restringe <code>ontap-nas-economy</code> i backend dal creare nuovi volumi FlexVol per contenere i loro Qtree. Solo i FlexVol preesistenti vengono utilizzati per il provisioning di nuovi PV.	
adAdminUser	Utente o gruppo di utenti amministratore di Active Directory con accesso completo alle condivisioni SMB. Utilizzare questo parametro per fornire diritti di amministratore alla condivisione SMB con controllo completo.	

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
spaceAllocation	Allocazione dello spazio per Qtrees	"true"
spaceReserve	Modalità di prenotazione dello spazio; "none" (thin) o "volume" (thick)	"none"

Parametro	Descrizione	Predefinito
snapshotPolicy	policy di Snapshot da utilizzare	"none"
qosPolicy	Gruppo di policy QoS da assegnare ai volumi creati. Scegliere uno tra qosPolicy o adaptiveQosPolicy per storage pool/backend	""
adaptiveQosPolicy	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegliere uno tra qosPolicy o adaptiveQosPolicy per pool di storage/backend. Non supportato da ontap-nas-economy.	""
snapshotReserve	Percentuale di volume riservata alle snapshot	"0" se snapshotPolicy è "none", altrimenti ""
splitOnClone	Dividere un clone dal suo genitore al momento della creazione	"false"
encryption	Abilita NetApp Volume Encryption (NVE) sul nuovo volume; il valore predefinito è false. 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"
tieringPolicy	Policy di tiering da utilizzare "none"	
unixPermissions	Modalità per nuovi volumi	"777" per i volumi NFS; vuoto (non applicabile) per i volumi SMB
snapshotDir	Controlla l'accesso alla .snapshot directory	true, false (Impostato esplicitamente).
exportPolicy	Policy di esportazione da utilizzare	"default"
securityStyle	Stile di sicurezza per i nuovi volumi. NFS supporta mixed e unix stili di sicurezza. SMB supporta mixed e ntfs stili di sicurezza.	L'impostazione predefinita di NFS è unix. L'impostazione predefinita di SMB è ntfs.
nameTemplate	Modello per creare nomi di volume personalizzati.	""



L'utilizzo di gruppi di policy QoS con Trident richiede ONTAP 9.8 o versioni successive. Dovresti utilizzare un gruppo di policy QoS non condiviso e assicurarti che il gruppo di policy venga applicato a ciascun componente individualmente. Un gruppo di policy QoS condiviso impone il limite massimo per il throughput di tutti i carichi di lavoro.

Esempi di provisioning del volume

Ecco un esempio con i valori predefiniti:

```
---
version: 1
```

```

storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: "10"

```

Per `ontap-nas` e `ontap-nas-flexgroups`, Trident ora utilizza un nuovo calcolo per garantire che il FlexVol sia dimensionato correttamente con la percentuale di `snapshotReserve` e il PVC. Quando l'utente richiede un PVC, Trident crea il FlexVol originale con più spazio utilizzando il nuovo calcolo. Questo calcolo garantisce che l'utente riceva lo spazio scrivibile richiesto nel PVC e non meno spazio di quanto richiesto. Prima della v21.07, quando l'utente richiedeva un PVC (ad esempio, 5 GiB), con la `snapshotReserve` al 50 per cento, otteneva solo 2,5 GiB di spazio scrivibile. Questo perché ciò che l'utente richiedeva era l'intero volume e `snapshotReserve` era una percentuale di quello. Con Trident 21.07, ciò che l'utente richiede è lo spazio scrivibile e Trident definisce il numero di `snapshotReserve` come percentuale dell'intero volume. Questo non si applica a `ontap-nas-economy`. Vedi il seguente esempio per capire come funziona:

Il calcolo è il seguente:

```

Total volume size = <PVC requested size> / (1 - (<snapshotReserve
percentage> / 100))

```

Per `snapshotReserve` = 50% e richiesta PVC = 5 GiB, la dimensione totale del volume è $5/0,5 = 10$ GiB e la dimensione disponibile è 5 GiB, che è quanto richiesto dall'utente nella richiesta PVC. 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_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

2 entries were displayed.

Per i backend esistenti da installazioni precedenti, esegui il provisioning dei volumi come spiegato sopra durante l'aggiornamento di Trident. Per i volumi che hai creato prima dell'aggiornamento, dovresti ridimensionare i volumi affinché la modifica venga rilevata. Ad esempio, un PVC da 2 GiB con `snapshotReserve=50` in precedenza generava un volume che forniva 1 GiB di spazio scrivibile. Ridimensionando il volume a 3 GiB, ad esempio, l'applicazione avrà a disposizione 3 GiB di spazio scrivibile su un volume da 6 GiB.

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, si consiglia di specificare i nomi DNS per i LIF anziché gli indirizzi IP.

▼ Esempio di economia NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

▼ Esempio di ONTAP NAS FlexGroup

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
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 parametri `dataLIF` e `svm`. Ad esempio:

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

▼ Esempio di volumi SMB

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

▼ Esempio di autenticazione basata su certificato

Questo è un esempio di configurazione minima del backend. `clientCertificate`, `clientPrivateKey`, e `trustedCACertificate` (facoltativo, se si utilizza una CA attendibile) vengono 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
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

▼ Esempio di policy di esportazione automatica

Questo esempio mostra come istruire Trident a utilizzare policy di esportazione dinamiche per creare e gestire automaticamente la policy di esportazione. Questo funziona allo stesso modo per i driver `ontap-nas-economy` e `ontap-nas-flexgroup`.

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

▼ 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-nas
backendName: nas-balanced-placement
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
useBalancedPlacement: true
```

▼ Esempio di indirizzi IPv6

Questo esempio mostra `managementLIF` l'utilizzo di un indirizzo IPv6.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
```

```
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

▼ Esempio di Amazon FSx for ONTAP che utilizza volumi SMB

Il smbShare parametro è obbligatorio per Amazon FSx for ONTAP che utilizza volumi SMB.

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

▼ Esempio di configurazione del backend con nameTemplate

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-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}}"
```

Esempi di backend con pool virtuali

Nei file di definizione del backend di esempio mostrati di seguito, 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 sono impostati su FlexVol per `ontap-nas` o FlexGroup per `ontap-nas-flexgroup`. 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 NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
      zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
      adaptiveQosPolicy: adaptive-premium
  - labels:
      app: slack
      cost: "75"
      zone: us_east_1b
    defaults:
      spaceReserve: none
```

```

    encryption: "true"
    unixPermissions: "0755"
- labels:
    department: legal
    creditpoints: "5000"
zone: us_east_1b
defaults:
    spaceReserve: none
    encryption: "true"
    unixPermissions: "0755"
- labels:
    app: wordpress
    cost: "50"
zone: us_east_1c
defaults:
    spaceReserve: none
    encryption: "true"
    unixPermissions: "0775"
- labels:
    app: mysqlldb
    cost: "25"
zone: us_east_1d
defaults:
    spaceReserve: volume
    encryption: "false"
    unixPermissions: "0775"

```

▼ Esempio di ONTAP NAS FlexGroup

```

---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
    spaceReserve: none
    encryption: "false"
labels:
    store: flexgroup_store
    k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
    protection: gold

```

```

    creditpoints: "50000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
- labels:
    protection: gold
    creditpoints: "30000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
- labels:
    protection: silver
    creditpoints: "20000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
- labels:
    protection: bronze
    creditpoints: "10000"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"

```

▼ Esempio di economia NAS ONTAP

```

---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: nas_economy_store
  region: us_east_1

```

```

storage:
- labels:
  department: finance
  creditpoints: "6000"
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: "true"
    unixPermissions: "0755"
- labels:
  protection: bronze
  creditpoints: "5000"
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: "true"
    unixPermissions: "0755"
- labels:
  department: engineering
  creditpoints: "3000"
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: "true"
    unixPermissions: "0775"
- labels:
  department: humanresource
  creditpoints: "2000"
  zone: us_east_1d
  defaults:
    spaceReserve: volume
    encryption: "false"
    unixPermissions: "0775"

```

Mappa i backend a StorageClasses

Le seguenti definizioni di StorageClass 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. Il volume ha le caratteristiche definite nel pool virtuale scelto.

- La `protection-gold` StorageClass corrisponde al primo e al secondo pool virtuale nel `ontap-nas-flexgroup` backend. Questi sono gli unici pool che offrono la 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 terzo e al quarto pool virtuale nel `ontap-nas-flexgroup` 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 quarto pool virtuale nel `ontap-nas` backend. Questo è l'unico pool che offre la configurazione del pool di storage per 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 terzo pool virtuale nel `ontap-nas-flexgroup` 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-nas` backend e al secondo pool virtuale nel `ontap-nas-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"
```

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

Aggiorna dataLIF dopo la configurazione iniziale

È possibile modificare il dataLIF dopo la configurazione iniziale eseguendo il comando seguente per fornire il nuovo file JSON backend con il dataLIF aggiornato.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-with-updated-dataLIF>
```



Se i PVC sono collegati a uno o più pod, è necessario disattivare tutti i pod corrispondenti e quindi riattivarli affinché il nuovo dataLIF abbia effetto.

Esempi di SMB sicuro

Configurazione del backend con driver ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
```

```
name: backend-tbc-ontap-invest-secret
```

Configurazione backend con driver ontap-nas-economy

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configurazione backend con pool di storage

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
    - labels:
        app: msoffice
      defaults:
        adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Esempio di storage class con driver ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```



Assicurati di aggiungere annotations per abilitare SMB sicuro. SMB sicuro non funziona senza le annotazioni, indipendentemente dalle configurazioni impostate nel Backend o nel PVC.

Esempio di storage class con driver ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Esempio di PVC con un singolo utente AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

```

name: my-pvc4
namespace: trident
annotations:
  trident.netapp.io/smbShareAccessControl: |
    change:
      - tridentADtest
    read:
      - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc

```

Esempio di PVC con più utenti AD

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:

```

storage: 1Gi

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.