Driver ONTAP SAN

Trident

NetApp
January 15, 2026

Sommario

Driver ONTAP SAN

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 archiviazione SAN per comunicare con il cluster ONTAP . Le modalità di accesso supportate sono: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

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

Autista	Protocollo	Modalità volume	Modalità di accesso supportate	Sistemi di file supportati
`ontap-san-economy`	iSCSI	File system	RWO, RWOP ROX e RWX non sono disponibili nella modalità volume Filesystem.	`xfs`, `ext3` , `ext4`

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

Permessi utente

Trident prevede di essere eseguito come amministratore ONTAP o SVM, in genere utilizzando `admin` utente del cluster o un `vsadmin` Utente SVM o 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 il cluster `fsxadmin` utente o un `vsadmin` Utente SVM o un utente con un nome diverso che ha lo stesso ruolo. IL `fsxadmin` L'utente è un sostituto limitato dell'utente amministratore del cluster.

Se usi il `limitAggregateUsage` parametro, sono richieste le autorizzazioni di amministratore del cluster. Quando si utilizza Amazon FSx for NetApp ONTAP con Trident, il `limitAggregateUsage` il parametro non funzionerà con il `vsadmin` E `fsxadmin` account utente. Se si specifica questo parametro, l'operazione di configurazione non riuscirà.

Sebbene sia possibile creare un ruolo più restrittivo all'interno di ONTAP utilizzabile da un conducente Trident , non lo consigliamo. La maggior parte delle nuove versioni di Trident richiameranno API aggiuntive di cui bisognerebbe tenere conto, rendendo gli aggiornamenti difficili e soggetti a errori.

Considerazioni aggiuntive per NVMe/TCP

Trident supporta il protocollo NVMe (Non-Volatile Memory Express) utilizzando `ontap-san` autista 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 supportato nativamente da NVMe
- Multipathing del mappatore di dispositivi (DM)
- Crittografia LUKS

NVMe è supportato solo con le API REST ONTAP e non 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 archiviazione. Nei sistemi ASA r2, al posto degli aggregati vengono utilizzate zone di disponibilità dello storage. Fare riferimento a"Questo" Articolo della Knowledge Base su come assegnare 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, potresti configurare un `san-dev` classe che utilizza il `ontap-san` autista e un `san-default` classe che utilizza il `ontap-san-economy` uno.

Tutti i nodi worker di Kubernetes devono avere installati gli strumenti iSCSI appropriati. Fare riferimento a "Preparare il nodo worker" per i dettagli.

Autenticare il backend ONTAP

Trident offre due modalità di autenticazione di un backend ONTAP .

- Basato su credenziali: nome utente e password di un utente ONTAP con le autorizzazioni richieste. Si consiglia di utilizzare un ruolo di accesso di sicurezza predefinito, ad esempio `admin` O `vsadmin` per garantire la massima compatibilità con le versioni ONTAP .
- Basato su certificato: Trident può anche comunicare con un cluster ONTAP utilizzando un certificato installato sul backend. Qui, la definizione del backend deve contenere 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 da metodi basati su credenziali a metodi basati su certificati. Tuttavia, è supportato solo un metodo di autenticazione alla volta. Per passare a un metodo di autenticazione diverso, è necessario rimuovere il metodo esistente dalla configurazione del backend.

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

Abilita l'autenticazione basata sulle credenziali

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

Un esempio di definizione del backend sarà simile a questo:

YAML

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

JSON

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

Tieni presente che la definizione del backend è l'unico posto in cui le credenziali vengono archiviate in testo normale. Dopo aver creato il backend, i nomi utente e le password vengono codificati con Base64 e memorizzati come segreti Kubernetes. La creazione o l'aggiornamento di un backend è l'unico passaggio che richiede la conoscenza delle credenziali. Si tratta pertanto di un'operazione riservata esclusivamente all'amministratore, che deve essere eseguita dall'amministratore di Kubernetes/archiviazione.

Abilita l'autenticazione basata sul certificato

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

- clientCertificate: valore codificato in Base64 del certificato client.
- clientPrivateKey: valore codificato in Base64 della chiave privata associata.
- trustedCACertificate: valore codificato in Base64 del certificato CA attendibile. Se si utilizza una CA

attendibile, è necessario fornire questo parametro. Questo può essere ignorato se non viene utilizzata alcuna CA attendibile.

Un flusso di lavoro tipico prevede i seguenti passaggi.

Passi

1. Genera un certificato client e una chiave. Durante la generazione, impostare il nome comune (CN) sull'utente ONTAP con cui effettuare l'autenticazione.

```
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 dell'archiviazione. Ignora se non viene utilizzata alcuna 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 client e la chiave (dal passaggio 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. Conferma che il ruolo di accesso alla sicurezza ONTAP supporta `cert` 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. Sostituire < ONTAP Management LIF> e <nome vserver> con l'IP Management LIF 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 attendibile con Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Creare il backend utilizzando i valori ottenuti dal passaggio precedente.

```
cat cert-backend.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"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. 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 dell'archiviazione deve prima aggiornare la password per l'utente su ONTAP. Segue un aggiornamento del backend. Durante la rotazione dei certificati, è possibile aggiungere più certificati all'utente. Il backend viene quindi aggiornato per utilizzare il nuovo certificato, dopodiché 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 ai volumi effettuate in seguito. Un aggiornamento del backend riuscito indica che Trident può comunicare con il backend ONTAP e gestire le future operazioni sui volumi.

Crea un ruolo ONTAP personalizzato per Trident

È possibile creare un ruolo 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 Trident , Trident utilizza il ruolo del 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 > Impostazioni**.

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

   b. Selezionare l'icona della freccia (→) accanto a **Utenti e ruoli**.
   c. Selezionare **+Aggiungi** in **Ruoli**.
   d. Definisci le regole per il ruolo e clicca su **Salva**.
2. **Assegnare il ruolo all'utente Trident *: + Eseguire i seguenti passaggi nella pagina *Utenti e ruoli**:
   a. Selezionare Aggiungi icona **+** in **Utenti**.
   b. Selezionare il nome utente richiesto e selezionare un ruolo nel menu a discesa per **Ruolo**.
   c. Fare clic su **Salva**.

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 `ontap-san` E `ontap-san-economy` conducenti. Ciò richiede l'abilitazione del `useCHAP` opzione nella definizione del backend. Quando impostato su `true` Trident configura la sicurezza dell'iniziatore predefinito dell'SVM su CHAP bidirezionale e imposta il nome utente e i segreti dal file 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` Il parametro è un'opzione booleana che può essere configurata solo una volta. Per impostazione predefinita è impostato su falso. Dopo averlo impostato su true, non è possibile impostarlo su false.

Inoltre `useCHAP=true` , IL `chapInitiatorSecret` , `chapTargetInitiatorSecret` , `chapTargetUsername` , E `chapUsername` i campi 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 dell'archiviazione indica a Trident di configurare CHAP sul backend di archiviazione. Ciò include quanto segue:

- Impostazione di CHAP sull'SVM:
  - Se il tipo di sicurezza dell'iniziatore predefinito dell'SVM è nessuno (impostato per impostazione predefinita) **e** non ci sono LUN preesistenti già presenti nel volume, Trident imposterà il tipo di sicurezza predefinito su `CHAP` e procedere alla configurazione dell'iniziatore CHAP e del nome utente e dei segreti di destinazione.
  - Se l'SVM contiene LUN, Trident non abiliterà CHAP sull'SVM. Ciò garantisce che l'accesso ai LUN già presenti sulla SVM non sia limitato.
- Configurazione dell'iniziatore CHAP e del nome utente e dei segreti di destinazione; queste opzioni devono essere specificate nella configurazione del backend (come mostrato sopra).

Dopo aver creato il 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 in `backend.json` file. Ciò richiederà l'aggiornamento dei segreti CHAP e l'utilizzo di `tridentctl update` comando per riflettere questi cambiamenti.

Quando si aggiornano i segreti CHAP per un backend, è necessario utilizzare `tridentctl` per aggiornare il backend. Non aggiornare le credenziali sul cluster di archiviazione 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-4378-8a33-1a472ffbeb5c |
online |       7 |
+----------------+----------------+--------------------------------------
+--------+---------+
```

Le connessioni esistenti non saranno interessate e continueranno a rimanere attive se le credenziali vengono aggiornate da Trident sull'SVM. Le nuove connessioni utilizzano le credenziali aggiornate, mentre le connessioni esistenti continuano a rimanere attive. Scollegando e ricollegando i vecchi PV, questi utilizzeranno le credenziali aggiornate.

Opzioni ed esempi di configurazione SAN ONTAP

Scopri come creare e utilizzare i driver ONTAP SAN con la tua installazione Trident . Questa sezione fornisce esempi di configurazione del backend e dettagli per il mapping dei backend alle StorageClass.

"Sistemi ASA r2"differiscono dagli altri sistemi ONTAP (ASA, AFF e FAS) nell'implementazione del loro livello di archiviazione. Tali variazioni incidono sull'utilizzo di determinati parametri come indicato. "Scopri di più sulle

differenze tra i sistemi ASA r2 e gli altri sistemi ONTAP".

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

Nella configurazione del backend Trident non è necessario specificare che il sistema è ASA r2. Quando selezioni `ontap-san` come il `storageDriverName` , Trident rileva automaticamente il ASA r2 o il tradizionale sistema ONTAP . Alcuni parametri di configurazione del backend non sono applicabili ai sistemi ASA r2, come indicato nella tabella seguente.

Opzioni di configurazione del backend

Per le opzioni di configurazione del backend, consultare la seguente tabella:

Parametro	Descrizione	Predefinito
`version`		Sempre 1
`storageDriverName`	Nome del driver di archiviazione	`ontap-san`O `ontap-san-economy`
`backendName`	Nome personalizzato o backend di archiviazione	Nome del driver + "_" + dataLIF
`managementLIF`	Indirizzo IP di un cluster o di un LIF di gestione SVM. È possibile specificare un nome di dominio completo (FQDN). Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando 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 a MetroCluster , vedereEsempio MetroCluster . > Se si utilizzano le credenziali "vsadmin", `managementLIF` deve essere quello dell'SVM; se si utilizzano le credenziali "admin", `managementLIF` deve essere quello del cluster.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parametro	Descrizione	Predefinito
`dataLIF`	Indirizzo IP del protocollo LIF. Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando 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.** Usi Trident"Mappa LUN selettiva ONTAP" per scoprire gli iSCSI LIF necessari per stabilire una sessione multi-percorso. Viene generato un avviso se `dataLIF` è definito esplicitamente. **Omettere per Metrocluster.** Vedi ilEsempio MetroCluster .	Derivato dall'SVM
`svm`	Macchina virtuale di archiviazione da utilizzare **Ometti per Metrocluster.** Vedi ilEsempio MetroCluster .	Derivato se un SVM `managementLIF` è specificato
`useCHAP`	Utilizzare CHAP per autenticare iSCSI per i driver ONTAP SAN [Booleano]. Impostato su `true` affinché Trident configuri e utilizzi CHAP bidirezionale come autenticazione predefinita per l'SVM fornito nel backend. Fare riferimento a "Prepararsi a configurare il backend con i driver ONTAP SAN" per i dettagli. **Non supportato per FCP o NVMe/TCP.**	`false`
`chapInitiatorSecret`	Segreto dell'iniziatore CHAP. Obbligatorio se `useCHAP=true`	""
`labels`	Insieme di etichette arbitrarie formattate in JSON da applicare ai volumi	""
`chapTargetInitiatorSecret`	Segreto dell'iniziatore del target CHAP. Obbligatorio se `useCHAP=true`	""
`chapUsername`	Nome utente in entrata. Obbligatorio se `useCHAP=true`	""
`chapTargetUsername`	Nome utente di destinazione. Obbligatorio se `useCHAP=true`	""
`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 necessario per comunicare con il cluster ONTAP . Utilizzato per l'autenticazione basata sulle credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident su un SVM backend utilizzando le credenziali di Active Directory".	""

Parametro	Descrizione	Predefinito
`password`	Password necessaria per comunicare con il cluster ONTAP . Utilizzato per l'autenticazione basata sulle credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident su un SVM backend utilizzando le credenziali di Active Directory".	""
`svm`	Macchina virtuale di archiviazione da utilizzare	Derivato se un SVM `managementLIF` è specificato
`storagePrefix`	Prefisso utilizzato durante il provisioning di nuovi volumi nell'SVM. Non può essere modificato in seguito. Per aggiornare questo parametro, sarà necessario creare un nuovo backend.	`trident`
`aggregate`	Aggregato per il provisioning (facoltativo; se impostato, deve essere assegnato all'SVM). Per il `ontap-nas-flexgroup` driver, questa opzione viene ignorata. Se non assegnato, è possibile utilizzare uno qualsiasi degli aggregati disponibili per eseguire il provisioning di un volume FlexGroup . Quando l'aggregato viene aggiornato in SVM, viene aggiornato automaticamente in Trident interrogando SVM senza dover riavviare Trident Controller. Dopo aver configurato un aggregato specifico in Trident per il provisioning dei volumi, se l'aggregato viene rinominato o spostato fuori dall'SVM, il backend passerà allo stato di errore in Trident durante l'interrogazione dell'aggregato SVM. Per riportare online il backend, è necessario modificare l'aggregato con uno presente sull'SVM oppure rimuoverlo del tutto. **Non specificare per i sistemi ASA r2**.	""
`limitAggregateUsage`	Il provisioning non riesce se l'utilizzo è superiore a questa percentuale. Se si utilizza un backend Amazon FSx for NetApp ONTAP , non specificare `limitAggregateUsage` . Il fornito `fsxadmin` E `vsadmin` non contengono le autorizzazioni richieste per recuperare l'utilizzo aggregato e limitarlo tramite Trident. **Non specificare per i sistemi ASA r2**.	"" (non applicato di default)
`limitVolumeSize`	Il provisioning non riesce se la dimensione del volume richiesto è superiore a questo valore. Limita inoltre la dimensione massima dei volumi gestiti per le LUN.	"" (non applicato di default)
`lunsPerFlexvol`	Numero massimo di LUN per Flexvol, deve essere compreso nell'intervallo [50, 200]	`100`

Parametro	Descrizione	Predefinito
`debugTraceFlags`	Flag di debug da utilizzare durante la risoluzione dei problemi. Esempio: {"api":false, "method":true} Non utilizzare a meno che non si stia risolvendo un problema e si necessiti di un dump di registro dettagliato.	`null`
`useREST`	Parametro booleano per utilizzare le API REST ONTAP . `useREST`Quando impostato su `true` , Trident utilizza le API REST ONTAP per comunicare con il backend; quando impostato su `false` Trident utilizza chiamate ONTAPI (ZAPI) per comunicare con il backend. Questa funzionalità richiede ONTAP 9.11.1 e versioni successive. Inoltre, il ruolo di accesso ONTAP utilizzato deve avere accesso a `ontapi` applicazione. Ciò è soddisfatto dal predefinito `vsadmin` E `cluster-admin` ruoli. A partire dalla versione Trident 24.06 e ONTAP 9.15.1 o successiva, `useREST` è impostato su `true` per impostazione predefinita; modifica `useREST` A `false` per utilizzare le chiamate ONTAPI (ZAPI). `useREST`è completamente qualificato per NVMe/TCP. NVMe è supportato solo con le API REST ONTAP e non con ONTAPI (ZAPI). **Se specificato, impostare sempre su `true` per sistemi ASA r2**.	`true`per ONTAP 9.15.1 o successivo, altrimenti `false`.
`sanType`	Utilizzare per selezionare `iscsi` per iSCSI, `nvme` per NVMe/TCP o `fcp` per SCSI su Fibre Channel (FC).	`iscsi`se vuoto

Parametro	Descrizione	Predefinito
`formatOptions`	Utilizzo `formatOptions` per specificare gli argomenti della riga di comando per `mkfs` comando, che verrà applicato ogni volta che un volume viene formattato. Ciò consente di formattare il volume in base alle proprie preferenze. Assicurarsi di specificare formatOptions in modo simile a quello delle opzioni del comando mkfs, escludendo il percorso del dispositivo. Esempio: "-E nodiscard" **Supportato per `ontap-san` E `ontap-san-economy` driver con protocollo iSCSI. Inoltre, supportato per i sistemi ASA r2 quando si utilizzano i protocolli iSCSI e NVMe/TCP.**	
`limitVolumePoolSize`	Dimensione massima FlexVol richiedibile quando si utilizzano LUN nel backend ontap-san-economy.	"" (non applicato di default)
`denyNewVolumePools`	Limita `ontap-san-economy` backend dalla creazione di nuovi volumi FlexVol per contenere i loro LUN. Per il provisioning di nuovi PV vengono utilizzati solo i Flexvol preesistenti.	

Consigli per l'utilizzo di formatOptions

Trident consiglia la seguente opzione per velocizzare il processo di formattazione:

-E nodiscard:

- Mantieni, non tentare di scartare i blocchi in fase di mkfs (scartare i blocchi inizialmente è utile su dispositivi a stato solido e storage sparse/thin-provisioned). Sostituisce l'opzione obsoleta "-K" ed è applicabile a tutti i file system (xfs, ext3 ed ext4).

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

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

passi

1. Configurare le impostazioni del Domain Name System (DNS) per un SVM 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 l'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 `username` E `password` parametri rispettivamente per il nome utente o gruppo AD e la password.

Opzioni di configurazione del backend per il provisioning dei volumi

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

Parametro	Descrizione	Predefinito
`spaceAllocation`	Assegnazione dello spazio per LUN	"true" **Se specificato, impostare su `true` per sistemi ASA r2**.
`spaceReserve`	Modalità di prenotazione dello spazio: "nessuno" (sottile) o "volume" (spesso). **Impostato su `none` per sistemi ASA r2**.	"nessuno"
`snapshotPolicy`	Criterio di snapshot da utilizzare. **Impostato su `none` per sistemi ASA r2**.	"nessuno"
`qosPolicy`	Gruppo di criteri QoS da assegnare ai volumi creati. Scegliere tra qosPolicy o adaptiveQosPolicy per ogni pool di archiviazione/backend. Per utilizzare i gruppi di policy QoS con Trident è necessario ONTAP 9.8 o versione successiva. È necessario utilizzare un gruppo di policy QoS non condiviso e assicurarsi che il gruppo di policy venga applicato individualmente a ciascun componente. Un gruppo di policy QoS condiviso impone il limite massimo per la produttività totale di tutti i carichi di lavoro.	""
`adaptiveQosPolicy`	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegli uno tra qosPolicy o adaptiveQosPolicy per pool di archiviazione/backend	""
`snapshotReserve`	Percentuale di volume riservata agli snapshot. **Non specificare per i sistemi ASA r2**.	"0" se `snapshotPolicy` è "nessuno", altrimenti ""
`splitOnClone`	Dividere un clone dal suo genitore al momento della creazione	"falso"
`encryption`	Abilita NetApp Volume Encryption (NVE) sul nuovo volume; l'impostazione predefinita è `false` . Per utilizzare questa opzione, NVE deve essere concesso in licenza e abilitato sul cluster. Se NAE è abilitato sul backend, qualsiasi volume fornito in Trident sarà abilitato per NAE. Per maggiori informazioni, fare riferimento a:"Come funziona Trident con NVE e NAE" .	"false" **Se specificato, impostare su `true` per sistemi ASA r2**.

Parametro	Descrizione	Predefinito
`luksEncryption`	Abilita la crittografia LUKS. Fare riferimento a"Utilizzare Linux Unified Key Setup (LUKS)" .	"" **Impostato su `false` per sistemi ASA r2**.
`tieringPolicy`	Criterio di suddivisione in livelli per utilizzare "nessuno" **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 definiti:

```
---
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 `ontap-san` driver, Trident aggiunge un ulteriore 10 percento di capacità al FlexVol per ospitare i metadati LUN. La LUN verrà fornita con le dimensioni esatte richieste dall'utente nel PVC. Trident aggiunge il 10 percento al FlexVol (mostrato come dimensione disponibile in ONTAP). Gli utenti riceveranno ora la quantità di capacità utilizzabile richiesta. Questa modifica impedisce inoltre che i LUN diventino di sola lettura, a meno che lo spazio disponibile non sia completamente utilizzato. Ciò 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 percento in più Trident aggiunge al FlexVol per ospitare i metadati LUN. Per `snapshotReserve` = 5% e richiesta PVC = 5 GiB, la dimensione totale del volume è 5,79 GiB e la dimensione disponibile è 5,5 GiB. IL `volume show` il comando dovrebbe mostrare risultati simili a questo esempio:

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 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 anziché gli indirizzi IP.

Esempio ONTAP SAN

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

```
---
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 MetroCluster

È possibile configurare il backend per evitare di dover aggiornare manualmente la definizione del backend dopo il passaggio e il ritorno durante"Replica e ripristino SVM" .

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

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

Esempio di economia ONTAP SAN

```
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) vengono popolati in `backend.json` e prendere 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 CHAP bidirezionali

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 economico 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 NVMe/TCP

È necessario disporre di una SVM configurata con NVMe sul backend ONTAP . Questa è una configurazione backend di base 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 SCSI su FC (FCP)

È necessario disporre di un SVM configurato con FC sul backend ONTAP . Questa è una configurazione backend di base 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}}"
```

Esempio di formatOptions per il driver ontap-san-economy

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
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 archiviazione, ad esempio `spaceReserve` a nessuno, `spaceAllocation` a falso, e `encryption` a falso. 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 nel volume di archiviazione al momento del provisioning. Per comodità, gli amministratori di storage possono definire etichette per pool virtuale e raggruppare i volumi in base all'etichetta.

In questi esempi, alcuni dei pool di archiviazione impostano i propri `spaceReserve` , `spaceAllocation` , E `encryption` valori e alcuni pool sovrascrivono i valori predefiniti.

Esempio ONTAP SAN

```
---
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 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>
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 su StorageClasses

Le seguenti definizioni StorageClass fanno riferimento aEsempi di backend con pool virtuali . Utilizzando il `parameters.selector` campo, ogni StorageClass richiama quali pool virtuali possono essere utilizzati per ospitare un volume. Il volume avrà gli aspetti definiti nel pool virtuale scelto.

- IL `protection-gold` StorageClass verrà mappato sul primo pool virtuale nel `ontap-san` backend. Questa è l'unica piscina che offre una protezione di livello Gold.

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

- IL `protection-not-gold` StorageClass verrà mappato sul secondo e terzo pool virtuale in `ontap-san` backend. Questi sono gli unici pool che offrono un livello di protezione diverso dall'oro.

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

- IL `app-mysqldb` StorageClass verrà mappato sul terzo pool virtuale in `ontap-san-economy` backend. Questo è l'unico pool che offre la configurazione del pool di archiviazione per l'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"
```

- IL `protection-silver-creditpoints-20k` StorageClass verrà mappato sul secondo pool virtuale in `ontap-san` backend. Questo è l'unico pool che offre protezione di livello Silver e 20.000 punti di 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"
```

- IL `creditpoints-5k` StorageClass verrà mappato sul terzo pool virtuale in `ontap-san` backend e il quarto pool virtuale nel `ontap-san-economy` backend. Queste sono le uniche offerte di pool con 5000 punti di credito.

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

- IL `my-test-app-sc` StorageClass verrà mappato su `testAPP` piscina virtuale nel `ontap-san` autista con `sanType: nvme` . Questa è l'unica piscina 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 deciderà quale pool virtuale selezionare e garantirà che i requisiti di archiviazione siano soddisfatti.

Informazioni sul copyright

Informazioni sul marchio commerciale