Best practice e consigli

Trident

NetApp
November 03, 2026

This PDF was generated from https://docs.netapp.com/it-it/trident-2410/trident-reco/deploy-reco.html on November 03, 2026. Always check docs.netapp.com for the latest.

Sommario

Best practice e consigli . . . 1
- Implementazione . . . 1
  - Eseguire l’implementazione in uno spazio dei nomi dedicato . . . 1
  - Utilizza quote e limiti di intervallo per controllare il consumo dello storage . . . 1
- Configurazione dello storage . . . 1
  - Panoramica della piattaforma . . . 1
  - Best practice per ONTAP e Cloud Volumes ONTAP . . . 1
  - Best practice di SolidFire . . . 6
  - Dove trovare ulteriori informazioni? . . . 7
- Integra Trident . . . 8
  - Selezione e implementazione dei driver . . . 8
  - Design di classe storage . . . 11
  - Progettazione di un pool virtuale . . . 12
  - Operazioni di volume . . . 13
  - Implementare i servizi OpenShift . . . 15
  - Servizio di metriche . . . 17
- Protezione dei dati e disaster recovery . . . 18
  - Replica e recovery di Trident . . . 18
  - Replica e recovery di SVM . . . 19
  - Replica e recovery dei volumi . . . 20
  - Protezione dei dati Snapshot . . . 20
- Sicurezza . . . 20
  - Sicurezza . . . 20
  - Linux Unified Key Setup (LUKS) . . . 22
  - Crittografia Kerberos in-flight . . . 27

Best practice e consigli

Implementazione

Durante la distribuzione di Trident, utilizza i consigli elencati di seguito.

Eseguire l'implementazione in uno spazio dei nomi dedicato

"Spazi dei nomi" separazione amministrativa tra diverse applicazioni e costituisce un ostacolo alla condivisione delle risorse. Ad esempio, un PVC di uno spazio dei nomi non può essere utilizzato da un altro. Trident fornisce risorse PV a tutti i namespace nel cluster Kubernetes e sfrutta di conseguenza un account di servizio che ha elevato il Privileges.

Inoltre, l'accesso al pod Trident potrebbe consentire a un utente di accedere alle credenziali del sistema di storage e ad altre informazioni sensibili. È importante assicurarsi che gli utenti delle applicazioni e le applicazioni di gestione non abbiano la possibilità di accedere alle definizioni degli oggetti Trident o ai pod stessi.

Utilizza quote e limiti di intervallo per controllare il consumo dello storage

Kubernetes dispone di due funzionalità che, se combinate, offrono un potente meccanismo per limitare il consumo di risorse da parte delle applicazioni. "meccanismo di quota dello storage"Consente all'amministratore di implementare limiti di consumo di capacità e conteggio degli oggetti globali e specifici della classe di storage in base al namespace. Inoltre, l'utilizzo di un "limite di intervallo" assicura che le richieste di PVC siano entro un valore minimo e massimo prima che la richiesta sia inoltrata al fornitore.

Questi valori sono definiti in base allo spazio dei nomi, il che significa che ogni spazio dei nomi deve avere valori definiti che sono in linea con i requisiti delle risorse. Vedere qui per informazioni su "come sfruttare le quote".

Configurazione dello storage

Ogni piattaforma di storage del portfolio NetApp dispone di funzionalità uniche che offrono vantaggi alle applicazioni, containerizzate o meno.

Panoramica della piattaforma

Trident funziona con ONTAP ed Element. Non esiste una piattaforma più adatta a tutte le applicazioni e gli scenari rispetto all'altra, tuttavia, è necessario tenere conto delle esigenze dell'applicazione e del team che amministra il dispositivo quando si sceglie una piattaforma.

Seguire le Best practice di base per il sistema operativo host con il protocollo che si sta sfruttando. Se lo si desidera, si consiglia di includere Best practice applicative, se disponibili, con impostazioni di backend, classe di storage e PVC per ottimizzare lo storage per applicazioni specifiche.

Best practice per ONTAP e Cloud Volumes ONTAP

Scopri le Best practice per la configurazione di ONTAP e Cloud Volumes ONTAP per Trident.

I seguenti consigli sono linee guida per la configurazione di ONTAP per i carichi di lavoro containerizzati, che consumano volumi che vengono forniti dinamicamente da Trident. Ciascuno di essi deve essere considerato e

valutato per l'adeguatezza nel proprio ambiente.

Utilizzare SVM dedicate a Trident

Le macchine virtuali di storage (SVM) forniscono isolamento e separazione amministrativa tra tenant su un sistema ONTAP. Dedicare una SVM alle applicazioni consente la delega dei privilegi e l'applicazione di Best practice per limitare il consumo delle risorse.

Sono disponibili diverse opzioni per la gestione di SVM:

- Fornire l'interfaccia di gestione del cluster nella configurazione back-end, insieme alle credenziali appropriate, e specificare il nome SVM.
- Creare un'interfaccia di gestione dedicata per la SVM utilizzando Gestione di sistema di ONTAP o l'interfaccia CLI.
- Condividere il ruolo di gestione con un'interfaccia dati NFS.

In ogni caso, l'interfaccia deve essere in DNS e il nome DNS deve essere utilizzato durante la configurazione di Trident. In questo modo è possibile semplificare alcuni scenari di disaster recovery, ad esempio SVM-DR, senza utilizzare la conservazione delle identità di rete.

Non esiste alcuna preferenza tra avere una LIF di gestione dedicata o condivisa per SVM, tuttavia, è necessario assicurarsi che le policy di sicurezza della rete siano allineate con l'approccio scelto. In ogni caso, la LIF di gestione deve essere accessibile via DNS per facilitare la massima flessibilità dovrebbe "SVM-DR" essere utilizzata insieme a Trident.

Limitare il numero massimo di volumi

I sistemi storage ONTAP hanno un numero massimo di volumi, che varia in base alla versione software e alla piattaforma hardware. Per determinare i limiti esatti, fare riferimento alla "NetApp Hardware Universe" per la piattaforma e la versione ONTAP in uso. Una volta esaurito il numero di volumi, le operazioni di provisioning non vengono eseguite solo per Trident, ma per tutte le richieste di storage.

Trident `ontap-nas` e `ontap-san` driver forniscono un FlexVolume per ogni Kubernetes Persistent Volume (PV) creato. Il `ontap-nas-economy` driver crea circa un FlexVolume per ogni 200 PVS (configurabile tra 50 e 300). Il `ontap-san-economy` driver crea circa un FlexVolume per ogni 100 PVS (configurabile tra 50 e 200). Per evitare che Trident utilizzi tutti i volumi disponibili sul sistema storage, è necessario impostare un limite per SVM. È possibile eseguire questa operazione dalla riga di comando:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

Il valore per `max-volumes` varia in base a diversi criteri specifici dell'ambiente:

- Il numero di volumi esistenti nel cluster ONTAP
- Il numero di volumi che si prevede di eseguire il provisioning al di fuori di Trident per altre applicazioni
- Il numero di volumi persistenti che si prevede siano utilizzati dalle applicazioni Kubernetes

```
`max-volumes`Il valore corrisponde ai volumi totali con provisioning
distribuiti in tutti i nodi del cluster ONTAP, non su un singolo nodo
ONTAP. Di conseguenza, potrebbero verificarsi alcune condizioni in cui
```

```
un nodo del cluster ONTAP potrebbe avere volumi con provisioning Trident
molto più o meno elevati rispetto a un altro nodo.
```

Ad esempio, un cluster ONTAP a due nodi può ospitare un massimo di 2000 FlexVolumes. Il fatto che il numero massimo di volumi sia impostato su 1250 appare molto ragionevole. Tuttavia, se alla SVM viene assegnato solo un nodo oppure se "aggregati" gli aggregati assegnati da un nodo non sono compatibili con il provisioning (ad esempio a causa della capacità), l'altro nodo diventa la destinazione per tutti i volumi con provisioning Trident. Ciò significa che è possibile raggiungere il limite del volume per quel nodo prima che venga raggiunto il `max-volumes` valore, con conseguente impatto sulle operazioni Trident e sugli altri volumi che utilizzano tale nodo. **È possibile evitare questa situazione assicurandosi che gli aggregati di ciascun nodo del cluster siano assegnati alla SVM utilizzata da Trident in numeri uguali.**

Limitare le dimensioni massime dei volumi creati da Trident

Per configurare le dimensioni massime per i volumi che possono essere creati da Trident, utilizzare il `limitVolumeSize` parametro nella `backend.json` definizione.

Oltre a controllare le dimensioni del volume nell'array di storage, è necessario sfruttare le funzionalità di Kubernetes.

Limitare le dimensioni massime dei FlexVol creati da Trident

Per configurare le dimensioni massime per i FlexVol utilizzati come pool per i driver ONTAP-san-Economy e ONTAP-nas-Economy, utilizzare il `limitVolumePoolSize` parametro nella `backend.json` definizione.

Configurare Trident per l'utilizzo di CHAP bidirezionale

È possibile specificare i nomi utente e le password dell'iniziatore CHAP e di destinazione nella definizione di backend e impostare Trident per abilitare CHAP su SVM. Utilizzando il `useCHAP` parametro nella configurazione backend, Trident autentica le connessioni iSCSI per i backend ONTAP con CHAP.

Creare e utilizzare una policy di QoS SVM

L'utilizzo di una policy di qualità del servizio ONTAP, applicata alla SVM, limita il numero di IOPS consumabili dai volumi sottoposti a provisioning Trident. In questo modo è possibile impedire a un "prevenire un bullismo" container fuori controllo di influenzare i carichi di lavoro esterni alla SVM di Trident.

È possibile creare una policy QoS per SVM in pochi passaggi. Per informazioni più precise, consultare la documentazione relativa alla versione di ONTAP in uso. Nell'esempio riportato di seguito viene creata una policy di QoS che limita a 5000 gli IOPS totali disponibili per la SVM.

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

Inoltre, se la tua versione di ONTAP lo supporta, puoi considerare l'utilizzo di un QoS minimo per garantire una

quantità di throughput per i carichi di lavoro containerizzati. QoS adattiva non è compatibile con una policy di livello SVM.

Il numero di IOPS dedicati ai carichi di lavoro containerizzati dipende da molti aspetti. Tra le altre cose, queste includono:

- Altri carichi di lavoro che utilizzano lo storage array. Se sono presenti altri carichi di lavoro, non correlati all'implementazione di Kubernetes, che utilizzano le risorse di storage, è necessario prestare attenzione a garantire che tali carichi di lavoro non vengano accidentalmente influenzati negativamente.
- Carichi di lavoro previsti eseguiti in container. Se i carichi di lavoro con requisiti IOPS elevati verranno eseguiti in container, una policy QoS bassa comporta un'esperienza negativa.

È importante ricordare che una policy di QoS assegnata a livello di SVM comporta la condivisione dello stesso pool di IOPS di tutti i volumi forniti a SVM. Se una, o un numero limitato, delle applicazioni containerizzate presenta un elevato requisito di IOPS, potrebbe diventare un problema per gli altri carichi di lavoro containerizzati. In questo caso, è possibile utilizzare l'automazione esterna per assegnare policy QoS per volume.

> È necessario assegnare il gruppo di criteri QoS a SVM **only** se la versione di ONTAP è precedente alla 9.8.

Creare gruppi di policy QoS per Trident

La qualità del servizio (QoS) garantisce che le performance dei carichi di lavoro critici non vengano degradate da carichi di lavoro concorrenti. I gruppi di policy QoS di ONTAP offrono opzioni di QoS per i volumi e consentono agli utenti di definire il limite massimo di throughput per uno o più carichi di lavoro. Per ulteriori informazioni su QoS, fare riferimento a "Garanzia di throughput con QoS". È possibile specificare i gruppi di policy QoS nel backend o in un pool di storage, che vengono applicati a ciascun volume creato in quel pool o backend.

ONTAP dispone di due tipi di gruppi di policy QoS: Tradizionale e adattiva. I gruppi di policy tradizionali forniscono un throughput massimo (o minimo, nelle versioni successive) costante negli IOPS. La QoS adattiva scala automaticamente il throughput in base alle dimensioni del carico di lavoro, mantenendo il rapporto tra IOPS e TB|GB in base alle dimensioni del carico di lavoro. Questo offre un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

Quando si creano gruppi di criteri QoS, considerare quanto segue:

- È necessario impostare la `qosPolicy` chiave nel `defaults` blocco della configurazione backend. Vedere il seguente esempio di configurazione del backend:

```
  ---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
```

```
storage:
- labels:
    performance: extreme
  defaults:
    adaptiveQosPolicy: extremely-adaptive-pg
- labels:
    performance: premium
  defaults:
    qosPolicy: premium-pg
```

- È necessario applicare i gruppi di criteri per volume, in modo che ogni volume ottenga l'intero throughput come specificato dal gruppo di criteri. I gruppi di criteri condivisi non sono supportati.

Per ulteriori informazioni sui gruppi di criteri QoS, fare riferimento a "Comandi QoS di ONTAP 9.8".

Limitare l'accesso alle risorse di storage ai membri del cluster Kubernetes

Limitare l'accesso ai volumi NFS e alle LUN iSCSI create da Trident è un componente critico della posizione di sicurezza per l'implementazione di Kubernetes. In questo modo si impedisce agli host che non fanno parte del cluster Kubernetes di accedere ai volumi e di modificare i dati in modo imprevisto.

È importante comprendere che gli spazi dei nomi sono il limite logico delle risorse in Kubernetes. L'ipotesi è che le risorse nello stesso namespace siano in grado di essere condivise, tuttavia, cosa importante, non esiste alcuna funzionalità di spazio dei nomi incrociato. Ciò significa che anche se i PVS sono oggetti globali, quando sono associati a un PVC sono accessibili solo da pod che si trovano nello stesso namespace. **È fondamentale assicurarsi che gli spazi dei nomi siano utilizzati per fornire la separazione quando appropriato.**

La preoccupazione principale per la maggior parte delle organizzazioni in relazione alla sicurezza dei dati in un contesto Kubernetes è che un processo in un container può accedere allo storage montato sull'host, ma non è destinato al container. "Spazi dei nomi" sono progettati per evitare questo tipo di compromesso. Tuttavia, esiste un'eccezione: I container con privilegi.

Un container con privilegi è un container che viene eseguito con un numero di autorizzazioni a livello di host sostanzialmente superiore al normale. Per impostazione predefinita, tali funzioni non vengono negate; pertanto, è necessario disattivarle utilizzando "policy di sicurezza pod".

Per i volumi in cui si desidera accedere sia da Kubernetes che da host esterni, lo storage deve essere gestito in modo tradizionale, con il PV introdotto dall'amministratore e non gestito da Trident. In questo modo, il volume di storage viene distrutto solo quando Kubernetes e gli host esterni si sono disconnessi e non utilizzano più il volume. Inoltre, è possibile applicare una policy di esportazione personalizzata, che consente l'accesso dai nodi del cluster Kubernetes e dai server di destinazione all'esterno del cluster Kubernetes.

Per le implementazioni che hanno nodi di infrastruttura dedicati (ad esempio, OpenShift) o altri nodi che non sono in grado di pianificare le applicazioni utente, è necessario utilizzare policy di esportazione separate per limitare ulteriormente l'accesso alle risorse di storage. Ciò include la creazione di una policy di esportazione per i servizi implementati nei nodi dell'infrastruttura (ad esempio, i servizi OpenShift Metrics e Logging) e le applicazioni standard implementate nei nodi non dell'infrastruttura.

Utilizzare una policy di esportazione dedicata

È necessario verificare l'esistenza di una policy di esportazione per ciascun backend che consenta l'accesso

solo ai nodi presenti nel cluster Kubernetes. Trident può creare e gestire automaticamente le policy di esportazione. In questo modo, Trident limita l'accesso ai volumi che fornisce ai nodi nel cluster Kubernetes e semplifica l'aggiunta/eliminazione dei nodi.

In alternativa, è anche possibile creare manualmente una policy di esportazione e compilarla con una o più regole di esportazione che elaborano ogni richiesta di accesso al nodo:

- Utilizzare il `vserver export-policy create` comando CLI di ONTAP per creare il criterio di esportazione.
- Aggiungere regole al criterio di esportazione utilizzando il `vserver export-policy rule create` comando CLI di ONTAP.

L'esecuzione di questi comandi consente di limitare i nodi Kubernetes che hanno accesso ai dati.

Disabilitazione `showmount` per l'applicazione SVM

Questa `showmount` funzionalità consente a un client NFS di richiedere all'SVM un elenco di esportazioni NFS disponibili. Un pod sul cluster Kubernetes può impartire un `showmount -e` comando sulla LIF dati e ricevere un elenco di mount disponibili, compresi quelli ai quali non ha accesso. Sebbene questo, di per sé, non sia un compromesso in termini di sicurezza, fornisce informazioni non necessarie che potrebbero aiutare un utente non autorizzato a connettersi a un'esportazione NFS.

Puoi disabilitare il `showmount` sistema utilizzando il comando ONTAP CLI a livello di SVM:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

Best practice di SolidFire

Scopri le Best practice per la configurazione dello storage SolidFire per Trident.

Crea account SolidFire

Ogni account SolidFire rappresenta un unico proprietario di volume e riceve un proprio set di credenziali CHAP (Challenge-Handshake Authentication Protocol). È possibile accedere ai volumi assegnati a un account utilizzando il nome dell'account e le relative credenziali CHAP o un gruppo di accesso al volume. A un account possono essere assegnati fino a duemila volumi, ma un volume può appartenere a un solo account.

Creare una policy QoS

Utilizzare le policy di qualità del servizio (QoS) di SolidFire se si desidera creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi.

È possibile impostare i parametri QoS in base al volume. Le performance per ciascun volume possono essere garantite impostando tre parametri configurabili che definiscono la QoS: Min IOPS, Max IOPS e Burst IOPS.

Di seguito sono riportati i possibili valori IOPS minimi, massimi e burst per la dimensione del blocco di 4 Kb.

Parametro IOPS	Definizione	Valore min	Valore predefinito	Valore max.(4Kb)
IOPS minimi	Il livello garantito di performance per un volume.	50	50	15000

Parametro IOPS	Definizione	Valore min	Valore predefinito	Valore max.(4Kb)
IOPS max	Le performance non supereranno questo limite.	50	15000	200.000
IOPS burst	IOPS massimi consentiti in uno scenario a burst breve.	50	15000	200.000

Anche se i massimi IOPS e burst IOPS possono essere impostati su 200,000, le performance massime reali di un volume sono limitate dall'utilizzo del cluster e dalle performance per nodo.

La dimensione dei blocchi e la larghezza di banda influiscono direttamente sul numero di IOPS. All'aumentare delle dimensioni dei blocchi, il sistema aumenta la larghezza di banda fino al livello necessario per elaborare blocchi di dimensioni maggiori. All'aumentare della larghezza di banda, il numero di IOPS che il sistema è in grado di raggiungere diminuisce. Fare riferimento a "Qualità del servizio SolidFire" per ulteriori informazioni su QoS e prestazioni.

Autenticazione SolidFire

Element supporta due metodi di autenticazione: CHAP e VAG (Volume Access Group). CHAP utilizza il protocollo CHAP per autenticare l'host nel backend. I gruppi di accesso ai volumi controllano l'accesso ai volumi previsti dall'IT. NetApp consiglia di utilizzare CHAP per l'autenticazione, poiché è più semplice e non ha limiti di scalabilità.

Trident con il provisioning CSI avanzato supporta l'utilizzo dell'autenticazione CHAP. I VAG devono essere utilizzati solo nella modalità operativa tradizionale non CSI.

L'autenticazione CHAP (verifica che l'iniziatore sia l'utente del volume desiderato) è supportata solo con il controllo degli accessi basato su account. Se si utilizza CHAP per l'autenticazione, sono disponibili due opzioni: CHAP unidirezionale e CHAP bidirezionale. CHAP unidirezionale autentica l'accesso al volume utilizzando il nome account SolidFire e il segreto dell'iniziatore. L'opzione CHAP bidirezionale rappresenta il metodo più sicuro per autenticare il volume, in quanto il volume autentica l'host tramite il nome account e il segreto dell'iniziatore, quindi l'host autentica il volume tramite il nome account e il segreto di destinazione.

Tuttavia, se non è possibile attivare CHAP e sono richiesti VAG, creare il gruppo di accesso e aggiungere gli iniziatori host e i volumi al gruppo di accesso. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo con o senza autenticazione CHAP. Se iSCSI Initiator è configurato per utilizzare l'autenticazione CHAP, viene utilizzato il controllo degli accessi basato sull'account. Se iSCSI Initiator non è configurato per utilizzare l'autenticazione CHAP, viene utilizzato il controllo di accesso del gruppo di accesso al volume.

Dove trovare ulteriori informazioni?

Di seguito sono elencate alcune delle Best practice. Cercare "Libreria NetApp" le versioni più recenti di .

ONTAP

- "Guida alle Best practice e all'implementazione di NFS"
- "Guida all'amministrazione SAN" (Per iSCSI)
- "Configurazione iSCSI Express per RHEL"

Software Element

- "Configurazione di SolidFire per Linux"

NetApp HCI

- "Prerequisiti per l'implementazione di NetApp HCI"
- "Accedi al NetApp Deployment Engine"

Informazioni sulle Best practice applicative

- "Best practice per MySQL su ONTAP"
- "Best practice per MySQL su SolidFire"
- "NetApp SolidFire e Cassandra"
- "Best practice Oracle su SolidFire"
- "Best practice PostgreSQL su SolidFire"

Non tutte le applicazioni dispongono di linee guida specifiche, è importante collaborare con il team NetApp e utilizzare "Libreria NetApp" per trovare la documentazione più aggiornata.

Integra Trident

Per integrare Trident, i seguenti elementi di design e architettura richiedono l'integrazione: Selezione e implementazione dei driver, design della classe di storage, design dei pool virtuali, impatto della rivendicazione del volume persistente (PVC) sul provisioning dello storage, sulle operazioni dei volumi e sull'implementazione dei servizi OpenShift con Trident.

Selezione e implementazione dei driver

Selezionare e implementare un driver back-end per il sistema storage.

Driver backend ONTAP

I driver di back-end ONTAP si differenziano in base al protocollo utilizzato e al modo in cui i volumi vengono forniti nel sistema di storage. Pertanto, prendere in considerazione attentamente quando si decide quale driver implementare.

A un livello superiore, se l'applicazione dispone di componenti che richiedono storage condiviso (diversi pod che accedono allo stesso PVC), i driver basati su NAS sarebbero la scelta predefinita, mentre i driver iSCSI basati su blocchi soddisfano le esigenze dello storage non condiviso. Scegli il protocollo in base ai requisiti dell'applicazione e al livello di comfort dei team di storage e infrastruttura. In generale, la differenza tra le due applicazioni è minima, quindi spesso la decisione si basa sulla necessità o meno di uno storage condiviso (in cui più di un pod necessitano di accesso simultaneo).

I driver backend ONTAP disponibili sono:

- `ontap-nas`: Ogni PV fornito è un FlexVolume ONTAP completo.
- `ontap-nas-economy`: Ogni PV sottoposto a provisioning è un qtree con un numero configurabile di qtree per FlexVolume (l'impostazione predefinita è 200).

- `ontap-nas-flexgroup`: Vengono utilizzati ogni PV sottoposto a provisioning come ONTAP FlexGroup completo e tutti gli aggregati assegnati a una SVM.
- `ontap-san`: Ogni PV sottoposto a provisioning è un LUN all'interno del proprio FlexVolume.
- `ontap-san-economy`: Ogni PV sottoposto a provisioning è una LUN, con un numero configurabile di LUN per FlexVolume (il valore predefinito è 100).

La scelta tra i tre driver NAS ha alcune ramificazioni alle funzionalità, che sono rese disponibili per l'applicazione.

Si noti che, nelle tabelle seguenti, non tutte le funzionalità sono esposte tramite Trident. Alcuni devono essere applicati dall'amministratore dello storage dopo il provisioning, se si desidera questa funzionalità. Le note a piè di pagina in superscript distinguono le funzionalità per funzionalità e driver.

Driver NAS ONTAP	Snapshot	Cloni	Policy di esportazione dinamiche	Multi-attach	QoS	Ridimensionare	Replica
`ontap-nas`	Sì	Sì	Yes[5]	Sì	Yes[1]	Sì	Yes[1]
`ontap-nas-economy`	Nota a piè di pagina:3[]	Nota a piè di pagina:3[]	Yes[5]	Sì	Nota a piè di pagina:3[]	Sì	Nota a piè di pagina:3[]
`ontap-nas-flexgroup`	Yes[1]	NO	Yes[5]	Sì	Yes[1]	Sì	Yes[1]

Trident offre driver SAN 2 per ONTAP, le cui funzionalità sono mostrate di seguito.

Driver SAN ONTAP	Snapshot	Cloni	Multi-attach	CHAP bidirezionale	QoS	Ridimensionare	Replica
`ontap-san`	Sì	Sì	Yes[4]	Sì	Yes[1]	Sì	Yes[1]
`ontap-san-economy`	Sì	Sì	Yes[4]	Sì	Nota a piè di pagina:3[]	Sì	Nota a piè di pagina:3[]

> Nota a piè di pagina: 1[]: Non gestito da Trident nota a piè di pagina:2[]: Gestito da Trident, ma non granulare PV nota a piè di pagina:3[]: Non gestito da Trident e non granulare PV nota a piè di pagina:4[]: Supportato per volumi a blocchi grezzi Nota a piè di pagina:5[]: Supportato da Trident

Le funzionalità non granulari PV vengono applicate all'intero FlexVolume e tutti i PVS (ovvero qtree o LUN in FlexVol condivisi) condividono una pianificazione comune.

Come si può vedere nelle tabelle precedenti, gran parte della funzionalità tra `ontap-nas` e `ontap-nas-economy` è la stessa. Tuttavia, poiché il `ontap-nas-economy` conducente limita la capacità di controllare la pianificazione con granularità per PV, ciò può influire in particolare sul disaster recovery e sulla pianificazione del backup. Per i team di sviluppo che desiderano sfruttare la funzionalità di clonazione in PVC sullo storage ONTAP, ciò è possibile solo quando si utilizzano i `ontap-nas` driver , `ontap-san` o. `ontap-san-economy`

Il `solidfire-san` driver è anche in grado di clonare PVC.

Driver backend Cloud Volumes ONTAP

Cloud Volumes ONTAP offre il controllo dei dati e funzionalità di storage di livello Enterprise per diversi casi di utilizzo, tra cui condivisioni di file e storage a livello di blocco che servono protocolli NAS e SAN (NFS, SMB/CIFS e iSCSI). I driver compatibili per Cloud Volume ONTAP sono `ontap-nas`, `ontap-nas-economy` `ontap-san` e `ontap-san-economy`. Questi sono validi per Cloud Volume ONTAP per Azure, Cloud Volume ONTAP per GCP.

Driver backend Amazon FSX per ONTAP

Amazon FSX per NetApp ONTAP ti permette di sfruttare le caratteristiche, le performance e le capacità amministrative di NetApp che conosci bene, sfruttando al contempo la semplicità, l'agilità, la sicurezza e la scalabilità dello storage dei dati su AWS. FSX per ONTAP supporta molte funzioni di file system ONTAP e API di amministrazione. I driver compatibili per Cloud Volume ONTAP sono `ontap-nas`, , `ontap-nas-economy` `ontap-nas-flexgroup` `ontap-san` e `ontap-san-economy`.

Driver backend NetApp HCI/SolidFire

Il `solidfire-san` driver utilizzato con le piattaforme NetApp HCI/SolidFire consente all'amministratore di configurare un backend di elementi per Trident in base ai limiti della qualità del servizio. Per progettare il backend in modo da impostare limiti specifici per la qualità del servizio sui volumi forniti da Trident, utilizza il `type` parametro nel file back-end. L'amministratore può anche limitare le dimensioni del volume che è possibile creare sullo storage utilizzando il `limitVolumeSize` parametro. Al momento, le funzionalità dello storage degli elementi come il ridimensionamento dei volumi e la replica dei volumi non sono supportate tramite il `solidfire-san` driver. Queste operazioni devono essere eseguite manualmente tramite l'interfaccia utente Web di Element Software.

Driver SolidFire	Snapshot	Cloni	Multi-attach	CAP	QoS	Ridimensionare	Replica
`solidfire-san`	Sì	Sì	Yes[2]	Sì	Sì	Sì	Yes[1]

> Nota a piè di pagina: Yes[1]: Non gestito da Trident Yes[2]: Supportato per i volumi di blocchi grezzi

Driver backend Azure NetApp Files

Trident utilizza il `azure-netapp-files` driver per gestire il servizio "Azure NetApp Files".

Ulteriori informazioni su questo driver e su come configurarlo sono disponibili in "Configurazione back-end Trident per Azure NetApp Files".

Driver Azure NetApp Files	Snapshot	Cloni	Multi-attach	QoS	Espandere	Replica
`azure-netapp-files`	Sì	Sì	Sì	Sì	Sì	Yes[1]

> Nota a piè di pagina: Yes[1]: Non gestito da Trident

Driver backend Cloud Volumes Service su Google Cloud

Trident utilizza il `gcp-cvs` driver per il collegamento con Cloud Volumes Service in Google Cloud.

Il `gcp-cvs` driver utilizza pool virtuali per astrarre il backend e consentire a Trident di determinare il posizionamento del volume. L'amministratore definisce i pool virtuali nei `backend.json` file. Le classi di storage utilizzano selettori per identificare i pool virtuali in base all'etichetta.

- Se i pool virtuali sono definiti nel back-end, Trident tenterà di creare un volume nei pool storage di Google Cloud a cui tali pool virtuali sono limitati.
- Se i pool virtuali non sono definiti nel back-end, Trident selezionerà un pool di storage Google Cloud dai pool di storage disponibili nell'area.

Per configurare il backend di Google Cloud su Trident, è necessario specificare `projectNumber`, `apiRegion`, e `apiKey` nel file backend. Il numero del progetto si trova nella console di Google Cloud. La chiave API viene presa dal file della chiave privata dell'account di servizio creato durante la configurazione dell'accesso API per Cloud Volumes Service su Google Cloud.

Per informazioni dettagliate sui tipi di servizio e sui livelli di servizio di Cloud Volumes Service su Google Cloud, fare riferimento alla "Scopri di più sul supporto Trident per CVS per GCP".

Driver Cloud Volumes Service per Google Cloud	Snapshot	Cloni	Multi-attach	QoS	Espandere	Replica
`gcp-cvs`	Sì	Sì	Sì	Sì	Sì	Disponibile solo sul tipo di servizio CVS-Performance.

Note sulla replica

- La replica non è gestita da Trident.
- Il clone verrà creato nello stesso pool di storage del volume di origine.

Design di classe storage

È necessario configurare e applicare singole classi di storage per creare un oggetto Kubernetes Storage Class. In questa sezione viene descritto come progettare una classe di storage per l'applicazione.

Utilizzo specifico del back-end

Il filtraggio può essere utilizzato all'interno di un oggetto specifico della classe di storage per determinare quale pool o insieme di pool di storage utilizzare con tale classe di storage specifica. In Classe di archiviazione è possibile impostare tre set di filtri: `storagePools`, , `additionalStoragePools` E/o `excludeStoragePools`.

Il `storagePools` parametro consente di limitare lo spazio di archiviazione all'insieme di pool che corrispondono a qualsiasi attributo specificato. Il `additionalStoragePools` parametro viene utilizzato per estendere l'insieme di pool utilizzati da Trident per il provisioning insieme all'insieme di pool selezionati dagli attributi e dai `storagePools` parametri. È possibile utilizzare i parametri singolarmente o entrambi insieme

per assicurarsi che sia selezionato il set appropriato di pool di storage.

Il `excludeStoragePools` parametro viene utilizzato per escludere in modo specifico l'insieme di pool elencato che corrispondono agli attributi.

Emulare le policy di QoS

Se si desidera progettare classi di archiviazione in modo da emulare i criteri di qualità del servizio, creare una classe di archiviazione con l' `media`attributo come `hdd` o `ssd`. In base all' `media`attributo menzionato nella classe storage, Trident selezionerà il back-end appropriato che serve `hdd` o `ssd` aggregati per corrispondere all'attributo multimediale, quindi indirizzerà il provisioning dei volumi sull'aggregato specifico. Pertanto, possiamo creare una classe di storage PREMIUM con `media` un attributo impostato come `ssd` classificabile come policy PREMIUM QoS. È possibile creare un altro STANDARD di classe storage con l'attributo media impostato come `hdd' che potrebbe essere classificato come policy standard di QoS. Potremmo anche utilizzare l'attributo ``IOPS'' nella classe di storage per reindirizzare il provisioning a un'appliance Element che può essere definita come policy QoS.

Utilizzare il back-end in base a funzionalità specifiche

Le classi di storage possono essere progettate per indirizzare il provisioning dei volumi su un backend specifico in cui sono abilitate funzionalità come thin provisioning e thick provisioning, snapshot, cloni e crittografia. Per specificare lo storage da utilizzare, creare classi di storage che specifichino il backend appropriato con la funzionalità richiesta attivata.

Pool virtuali

I pool virtuali sono disponibili per tutti i backend Trident. È possibile definire pool virtuali per qualsiasi backend, utilizzando qualsiasi driver fornito da Trident.

I pool virtuali consentono a un amministratore di creare un livello di astrazione sui backend a cui si può fare riferimento attraverso le classi di storage, per una maggiore flessibilità e un posizionamento efficiente dei volumi sui backend. È possibile definire backend diversi con la stessa classe di servizio. Inoltre, è possibile creare più pool di storage sullo stesso backend, ma con caratteristiche diverse. Quando una classe di archiviazione è configurata con un selettore con le etichette specifiche, Trident sceglie un backend che corrisponde a tutte le etichette del selettore per posizionare il volume. Se le etichette del selettore della classe di archiviazione corrispondono a più pool di archiviazione, Trident sceglierà uno di essi da cui eseguire il provisioning del volume.

Progettazione di un pool virtuale

Durante la creazione di un backend, in genere è possibile specificare un set di parametri. Per l'amministratore non era possibile creare un altro backend con le stesse credenziali di storage e con un set di parametri diverso. Con l'introduzione dei pool virtuali, questo problema è stato risolto. Virtual Pools è un'astrazione di livello introdotta tra il backend e Kubernetes Storage Class, in modo che l'amministratore possa definire i parametri insieme alle etichette a cui si può fare riferimento attraverso le classi di storage di Kubernetes come un selettore, in modo indipendente dal backend. È possibile definire pool virtuali per tutti i backend NetApp supportati con Trident. L'elenco include SolidFire/NetApp HCI, ONTAP, Cloud Volumes Service su GCP e Azure NetApp Files.

Quando si definiscono i pool virtuali, si consiglia di non tentare di riorganizzare l'ordine dei pool virtuali esistenti in una definizione di backend. Si consiglia inoltre di non modificare/modificare gli attributi di un pool virtuale esistente e di non definire un nuovo pool virtuale.

Emulazione di diversi livelli di servizio/QoS

È possibile progettare pool virtuali per l'emulazione delle classi di servizio. Utilizzando l'implementazione del pool virtuale per il servizio volume cloud per Azure NetApp Files, esaminiamo come possiamo configurare diverse classi di servizio. Configurare il backend Azure NetApp Files con più etichette, che rappresentano diversi livelli di prestazioni. Impostare `servicelevel` Aspect al livello di prestazioni appropriato e aggiungere altri aspetti richiesti sotto ogni etichetta. Creare ora diverse classi di storage Kubernetes che si mappano a diversi pool virtuali. A tale `parameters.selector` scopo, ogni StorageClass definisce i pool virtuali che possono essere utilizzati per ospitare un volume.

Assegnazione di un insieme specifico di aspetti

È possibile progettare più pool virtuali con un set specifico di aspetti da un singolo backend di storage. A tale scopo, configurare il backend con più etichette e impostare gli aspetti richiesti sotto ciascuna etichetta. Ora creare diverse classi di storage Kubernetes utilizzando il `parameters.selector` campo che dovrebbero essere mappate a diversi pool virtuali. I volumi con cui viene eseguito il provisioning sul back-end avranno gli aspetti definiti nel pool virtuale scelto.

Caratteristiche del PVC che influiscono sul provisioning dello storage

Alcuni parametri oltre la classe di archiviazione richiesta possono influire sul processo decisionale di provisioning Trident durante la creazione di un PVC.

Modalità di accesso

Quando si richiede lo storage tramite PVC, uno dei campi obbligatori è la modalità di accesso. La modalità desiderata può influire sul backend selezionato per ospitare la richiesta di storage.

Trident tenterà di corrispondere al protocollo di storage utilizzato con il metodo di accesso specificato secondo la matrice seguente. Ciò è indipendente dalla piattaforma di storage sottostante.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
ISCSI	Sì	Sì	Sì (blocco raw)
NFS	Sì	Sì	Sì

Una richiesta di ReadWriteMany PVC inviata a un'implementazione Trident senza un backend NFS configurato non comporterà il provisioning di alcun volume. Per questo motivo, il richiedente deve utilizzare la modalità di accesso appropriata per la propria applicazione.

Operazioni di volume

Modificare i volumi persistenti

I volumi persistenti sono, con due eccezioni, oggetti immutabili in Kubernetes. Una volta creata, la policy di recupero e le dimensioni possono essere modificate. Tuttavia, ciò non impedisce che alcuni aspetti del volume vengano modificati al di fuori di Kubernetes. Ciò può essere utile per personalizzare il volume per applicazioni specifiche, per garantire che la capacità non venga accidentalmente consumata o semplicemente per spostare il volume in un controller di storage diverso per qualsiasi motivo.

> Attualmente, i provisioning in-tree di Kubernetes non supportano le operazioni di ridimensionamento dei volumi per NFS o iSCSI PVS. Trident supporta l'espansione dei volumi NFS e iSCSI.

I dettagli di connessione del PV non possono essere modificati dopo la creazione.

Creazione di snapshot di volumi on-demand

Trident supporta la creazione di snapshot del volume on-demand e la creazione di PVC dalle snapshot utilizzando il framework CSI. Gli snapshot offrono un metodo pratico per mantenere copie point-in-time dei dati e hanno un ciclo di vita indipendente dal PV di origine in Kubernetes. Queste snapshot possono essere utilizzate per clonare i PVC.

Creare volumi da snapshot

Trident supporta anche la creazione di PersistentVolumes dalle istantanee di volume. A tale scopo, è sufficiente creare un'istruzione PersistentVolumeClaim e indicare `datasource` come lo snapshot richiesto da cui creare il volume. Trident gestirà questo PVC creando un volume con i dati presenti sullo snapshot. Con questa funzionalità, è possibile duplicare i dati tra regioni, creare ambienti di test, sostituire un volume di produzione danneggiato o corrotto nella sua interezza o recuperare file e directory specifici e trasferirli in un altro volume collegato.

Spostare i volumi nel cluster

Gli amministratori dello storage hanno la possibilità di spostare i volumi tra aggregati e controller nel cluster ONTAP senza interruzioni per il consumatore di storage. Questa operazione non influisce su Trident o sul cluster Kubernetes, a condizione che l'aggregato di destinazione sia uno a cui ha accesso la SVM utilizzata da Trident. Inoltre, se l'aggregato è stato appena aggiunto alla SVM, sarà necessario aggiornare il backend aggiungendolo nuovamente a Trident. In questo modo, Trident eseguirà il re-inventario della SVM in modo che venga riconosciuto il nuovo aggregato.

Tuttavia, lo spostamento dei volumi tra i backend non è supportato automaticamente da Trident. Si tratta di attività comprese fra SVM dello stesso cluster, fra cluster o in una diversa piattaforma storage (anche se il sistema storage è connesso a Trident).

Se un volume viene copiato in un'altra posizione, è possibile utilizzare la funzione di importazione del volume per importare i volumi correnti in Trident.

Espandere i volumi

Trident supporta il ridimensionamento di PVS NFS e iSCSI. Ciò consente agli utenti di ridimensionare i propri volumi direttamente attraverso il livello Kubernetes. L'espansione dei volumi è possibile per tutte le principali piattaforme di storage NetApp, inclusi i backend ONTAP, SolidFire/NetApp HCI e Cloud Volumes Service. Per consentire una possibile espansione in un secondo momento, impostare `allowVolumeExpansion` su `true` in StorageClass associato al volume. Ogni volta che è necessario ridimensionare il volume persistente, modificare l' `spec.resources.requests.storage`annotazione nella rivendicazione volume persistente sulla dimensione del volume richiesta. Trident si occuperà automaticamente del ridimensionamento del volume sul cluster di storage.

Importare un volume esistente in Kubernetes

L'importazione dei volumi consente di importare un volume di storage esistente in un ambiente Kubernetes. Attualmente è supportato dai `ontap-nas` `azure-netapp-files` driver , , `ontap-nas-flexgroup`, `solidfire-san` e `gcp-cvs` . Questa funzionalità è utile quando si esegue il porting di un'applicazione esistente in Kubernetes o durante scenari di disaster recovery.

Quando si utilizzano ONTAP e driver, utilizzare il comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` per importare un volume esistente in Kubernetes e

`solidfire-san` gestirlo da Trident. Il file PVC YAML o JSON utilizzato nel comando volume di importazione punta a una classe di archiviazione che identifica Trident come provisioner. Quando si utilizza un backend NetApp HCI/SolidFire, assicurarsi che i nomi dei volumi siano univoci. Se i nomi dei volumi sono duplicati, clonare il volume con un nome univoco in modo che la funzione di importazione dei volumi possa distinguerli.

Se viene utilizzato il `azure-netapp-files` driver OR `gcp-cvs`, utilizzare il comando `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` per importare il volume in Kubernetes che sarà gestito da Trident. In questo modo si garantisce un riferimento di volume univoco.

Quando viene eseguito il comando sopra indicato, Trident trova il volume del backend e ne legge le dimensioni. Aggiungerà automaticamente (e sovrascriverà se necessario) le dimensioni del volume del PVC configurato. Trident crea quindi il nuovo PV e Kubernetes lega il PVC al PV.

Se un container fosse stato implementato in modo da richiedere lo specifico PVC importato, rimarrebbe in sospeso fino a quando la coppia PVC/PV non sarà legata tramite il processo di importazione del volume. Una volta rilegata la coppia PVC/PV, il container dovrebbe salire, a condizione che non vi siano altri problemi.

Implementare i servizi OpenShift

I servizi cluster OpenShift a valore aggiunto offrono funzionalità importanti agli amministratori dei cluster e alle applicazioni ospitate. Lo storage utilizzato da questi servizi può essere fornito utilizzando le risorse locali del nodo, tuttavia, questo spesso limita la capacità, le performance, la ripristinabilità e la sostenibilità del servizio. Sfruttando un array di storage Enterprise per fornire la capacità a questi servizi è possibile migliorare drasticamente il servizio, tuttavia, come per tutte le applicazioni, OpenShift e gli amministratori dello storage dovrebbero collaborare strettamente per determinare le opzioni migliori per ciascuno di essi. La documentazione di Red Hat deve essere sfruttata in maniera significativa per determinare i requisiti e garantire che le esigenze di dimensionamento e performance siano soddisfatte.

Servizio di registro

La distribuzione e la gestione dello storage per il Registro di sistema sono state documentate "netapp.io"in "blog".

Servizio di registrazione

Come altri servizi OpenShift, il servizio di logging viene implementato utilizzando Ansible con i parametri di configurazione forniti dal file di inventario, chiamati host, forniti al playbook. Sono previsti due metodi di installazione: Distribuzione del logging durante l'installazione iniziale di OpenShift e distribuzione del logging dopo l'installazione di OpenShift.

A partire dalla versione 3.9 di Red Hat OpenShift, la documentazione ufficiale consiglia NFS per il servizio di logging a causa di problemi legati alla corruzione dei dati. Questo si basa sui test Red Hat dei loro prodotti. Il server ONTAP NFS non presenta questi problemi e può facilmente ripristinare una distribuzione di registrazione. In definitiva, la scelta del protocollo per il servizio di logging dipende da voi, sappiate che entrambi funzioneranno benissimo quando si utilizzano le piattaforme NetApp e che non vi è alcun motivo per evitare NFS se questa è la vostra preferenza.

Se scegli di utilizzare NFS con il servizio di logging, dovrai impostare la variabile Ansible `openshift_enable_unsupported_configurations` su `true` per impedire il guasto del programma di installazione.

Inizia subito

Il servizio di logging può, facoltativamente, essere implementato per entrambe le applicazioni e per le operazioni principali del cluster OpenShift stesso. Se si sceglie di distribuire la registrazione delle operazioni, specificando la variabile `openshift_logging_use_ops` come `true`, verranno create due istanze del servizio. Le variabili che controllano l'istanza di logging per le operazioni contengono "Ops" al loro interno, mentre l'istanza per le applicazioni non lo fa.

La configurazione delle variabili Ansible in base al metodo di implementazione è importante per garantire che venga utilizzato lo storage corretto da parte dei servizi sottostanti. Esaminiamo le opzioni per ciascun metodo di distribuzione.

> Le tabelle seguenti contengono solo le variabili rilevanti per la configurazione dello storage in relazione al servizio di registrazione. È possibile trovare altre opzioni in cui esaminare, configurare e utilizzare in "Documentazione di registrazione di RedHat OpenShift"base alla distribuzione.

Le variabili riportate nella tabella seguente determineranno la creazione di un PV e di un PVC per il servizio di registrazione utilizzando i dettagli forniti. Questo metodo è notevolmente meno flessibile rispetto all'utilizzo del playbook di installazione dei componenti dopo l'installazione di OpenShift, tuttavia, se si dispone di volumi esistenti, si tratta di un'opzione.

Variabile	Dettagli
`openshift_logging_storage_kind`	Impostare su `nfs` per fare in modo che il programma di installazione crei un PV NFS per il servizio di registrazione.
`openshift_logging_storage_host`	Il nome host o l'indirizzo IP dell'host NFS. Questa opzione deve essere impostata sul LIF dei dati per la macchina virtuale.
`openshift_logging_storage_nfs_directory`	Il percorso di montaggio per l'esportazione NFS. Ad esempio, se il volume è collegato come `/openshift_logging`, è possibile utilizzare tale percorso per questa variabile.
`openshift_logging_storage_volume_name`	Il nome, ad esempio `pv_ose_logs`, del PV da creare.
`openshift_logging_storage_volume_size`	La dimensione dell'esportazione NFS, ad esempio `100Gi`.

Se il cluster OpenShift è già in esecuzione e quindi Trident è stato implementato e configurato, l'installatore può utilizzare il provisioning dinamico per creare i volumi. È necessario configurare le seguenti variabili.

Variabile	Dettagli
`openshift_logging_es_pvc_dynamic`	Impostare su true per utilizzare volumi con provisioning dinamico.
`openshift_logging_es_pvc_storage_class_name`	Il nome della classe di storage che verrà utilizzata nel PVC.
`openshift_logging_es_pvc_size`	La dimensione del volume richiesto nel PVC.
`openshift_logging_es_pvc_prefix`	Prefisso dei PVC utilizzati dal servizio di registrazione.

Variabile	Dettagli
`openshift_logging_es_ops_pvc_dynamic`	Impostato su `true` per utilizzare i volumi con provisioning dinamico per l'istanza di logging Ops.
`openshift_logging_es_ops_pvc_storage_class_name`	Il nome della classe di storage per l'istanza di logging di Ops.
`openshift_logging_es_ops_pvc_size`	La dimensione della richiesta di volume per l'istanza Ops.
`openshift_logging_es_ops_pvc_prefix`	Un prefisso per i PVC di istanza di Ops.

Implementare lo stack di logging

Se si sta implementando la registrazione come parte del processo di installazione iniziale di OpenShift, è sufficiente seguire il processo di distribuzione standard. Ansible configurerà e implementerà i servizi e gli oggetti OpenShift necessari in modo che il servizio sia disponibile non appena Ansible sarà completato.

Tuttavia, se si esegue l'implementazione dopo l'installazione iniziale, Ansible dovrà utilizzare il playbook dei componenti. Questo processo potrebbe cambiare leggermente con le diverse versioni di OpenShift, quindi assicurati di leggere e seguire le istruzioni "Documentazione di RedHat OpenShift Container Platform 3.11" per la tua versione.

Servizio di metriche

Il servizio Metrics fornisce all'amministratore informazioni preziose sullo stato, l'utilizzo delle risorse e la disponibilità del cluster OpenShift. È inoltre necessario per la funzionalità di scalabilità automatica di Pod e molte organizzazioni utilizzano i dati del servizio di metriche per le proprie applicazioni di riaccredito e/o visualizzazione.

Come nel caso del servizio di registrazione e di OpenShift nel suo complesso, Ansible viene utilizzato per implementare il servizio di metriche. Inoltre, come il servizio di logging, il servizio di metriche può essere implementato durante una configurazione iniziale del cluster o dopo il suo funzionamento utilizzando il metodo di installazione dei componenti. Le seguenti tabelle contengono le variabili importanti per la configurazione dello storage persistente per il servizio di metriche.

> Le tabelle seguenti contengono solo le variabili rilevanti per la configurazione dello storage in relazione al servizio di metriche. La documentazione contiene molte altre opzioni che devono essere esaminate, configurate e utilizzate in base all'implementazione.

Variabile	Dettagli
`openshift_metrics_storage_kind`	Impostare su `nfs` per fare in modo che il programma di installazione crei un PV NFS per il servizio di registrazione.
`openshift_metrics_storage_host`	Il nome host o l'indirizzo IP dell'host NFS. Questa opzione deve essere impostata sul valore LIF dei dati per SVM.
`openshift_metrics_storage_nfs_directory`	Il percorso di montaggio per l'esportazione NFS. Ad esempio, se il volume è collegato come `/openshift_metrics`, è possibile utilizzare tale percorso per questa variabile.

Variabile	Dettagli
`openshift_metrics_storage_volume_name`	Il nome, ad esempio `pv_ose_metrics`, del PV da creare.
`openshift_metrics_storage_volume_size`	La dimensione dell'esportazione NFS, ad esempio `100Gi`.

Se il cluster OpenShift è già in esecuzione e quindi Trident è stato implementato e configurato, l'installatore può utilizzare il provisioning dinamico per creare i volumi. È necessario configurare le seguenti variabili.

Variabile	Dettagli
`openshift_metrics_cassandra_pvc_prefix`	Prefisso da utilizzare per i PVC di metriche.
`openshift_metrics_cassandra_pvc_size`	Le dimensioni dei volumi da richiedere.
`openshift_metrics_cassandra_storage_type`	Il tipo di storage da utilizzare per le metriche, deve essere impostato su dinamico per Ansible per creare PVC con la classe di storage appropriata.
`openshift_metrics_cassanda_pvc_storage_class_name`	Il nome della classe di storage da utilizzare.

Implementare il servizio di metriche

Con le variabili Ansible appropriate definite nel file di host/inventario, implementare il servizio utilizzando Ansible. Se si esegue l'implementazione al momento dell'installazione di OpenShift, il PV verrà creato e utilizzato automaticamente. Se stai eseguendo l'implementazione utilizzando i playbook dei componenti, dopo l'installazione di OpenShift, Ansible crea tutti i PVC necessari e, dopo che Trident ha eseguito il provisioning dello storage per loro, implementa il servizio.

Le variabili di cui sopra e il processo di implementazione possono cambiare con ogni versione di OpenShift. Verificare che la versione in uso sia configurata per l'ambiente in uso e seguirla"Guida all'implementazione di OpenShift di RedHat".

Protezione dei dati e disaster recovery

Scopri le opzioni di protezione e recovery per Trident e volumi creati con Trident. È necessario disporre di una strategia di protezione e ripristino dei dati per ogni applicazione con un requisito di persistenza.

Replica e recovery di Trident

È possibile creare un backup per ripristinare Trident in caso di emergenza.

Replica Trident

Trident utilizza i CRD Kubernetes per memorizzare e gestire il proprio stato, mentre il cluster etcd Kubernetes memorizza i propri metadati.

Fasi

1. Eseguire il backup di ccd del cluster Kubernetes utilizzando "Kubernetes: Backup di un cluster etcd".

2. Posizionare gli artefatti di backup su un FlexVol.

> Si consiglia di proteggere la SVM in cui risiede FlexVol con una relazione SnapMirror con un'altra SVM.

Ripristino Trident

Grazie ai Kubernetes CRD e allo snapshot etcd del cluster Kubernetes, puoi ripristinare Trident.

Fasi

1. Dalla SVM di destinazione, montare il volume contenente i file di dati e i certificati Kubernetes etcd sull'host che verrà configurato come nodo master.
2. Copiare tutti i certificati richiesti relativi al cluster Kubernetes in `/etc/kubernetes/pki` e i file membri etcd in `/var/lib/etcd`.
3. Ripristinare il cluster Kubernetes dal backup etcd utilizzando "Kubernetes: Ripristino di un cluster etcd".
4. Eseguire `kubectl get crd` per verificare che tutte le risorse personalizzate di Trident siano state create e recuperare gli oggetti Trident per verificare che tutti i dati siano disponibili.

Replica e recovery di SVM

Trident non può configurare le relazioni di replica, tuttavia, l'amministratore dello storage può utilizzare "SnapMirror di ONTAP" per replicare una SVM.

In caso di disastro, è possibile attivare la SVM di destinazione di SnapMirror per iniziare a fornire i dati. Una volta ripristinati i sistemi, è possibile tornare al sistema primario.

A proposito di questa attività

Quando si utilizza la funzione di replica SVM di SnapMirror, considerare quanto segue:

- È necessario creare un backend distinto per ogni SVM con SVM-DR abilitato.
- Configurare le classi di storage in modo che selezionino i backend replicati solo quando necessario, per evitare volumi che non richiedono il provisioning della replica sui backend che supportano SVM-DR.
- Gli amministratori delle applicazioni devono comprendere i costi e la complessità aggiuntivi associati alla replica e considerare attentamente il piano di ripristino prima di iniziare questo processo.

Replica SVM

Puoi utilizzare "ONTAP: Replica SVM SnapMirror" per creare una relazione di replica della SVM.

SnapMirror consente di impostare le opzioni per il controllo degli elementi da replicare. È necessario sapere quali opzioni sono state selezionate durante la preformatura Ripristino di SVM mediante Trident.

- "-identity-preserve true" Replica l'intera configurazione della SVM.
- "-discard-configs network" Sono escluse le LIF e le relative impostazioni di rete.
- "-identity-preserve false" replica solo i volumi e la configurazione di protezione.

Ripristino di SVM mediante Trident

Trident non rileva automaticamente i guasti della SVM. In caso di disastro, l'amministratore può avviare manualmente il failover di Trident sulla nuova SVM.

Fasi

1. Annullare i trasferimenti SnapMirror pianificati e in corso, interrompere la relazione di replica, arrestare la SVM di origine e attivare la SVM di destinazione di SnapMirror.
2. Se hai specificato `-identity-preserve false` o `-discard-config network` durante la configurazione della replica SVM, aggiorna il `managementLIF` e `dataLIF` il file di definizione di backend Trident.
3. Verificare `storagePrefix` che sia presente nel file di definizione del backend Trident. Questo parametro non può essere modificato. Omettendo `storagePrefix` si causerà un errore nell'aggiornamento del backend.
4. Aggiornare tutti i backend richiesti per riflettere il nuovo nome SVM di destinazione utilizzando:

```
./tridentctl update backend <backend-name> -f <backend-json-file> -n
<namespace>
```

5. Se è stato specificato `-identity-preserve false` o `discard-config network`, è necessario rimbalzare tutti i pod di applicazioni.

> Se specificato `-identity-preserve true`, tutti i volumi con provisioning da Trident iniziano a fornire i dati quando viene attivata la SVM di destinazione.

Replica e recovery dei volumi

Trident non può configurare le relazioni di replica di SnapMirror, tuttavia l'amministratore dello storage può utilizzare "Replica e ripristino di ONTAP SnapMirror" per replicare i volumi creati da Trident.

È quindi possibile importare i volumi recuperati in Trident utilizzando "importazione di volumi tridentctl".

> L'importazione non è supportata sui `ontap-nas-economy` driver , , `ontap-san-economy`o `ontap-flexgroup-economy` .

Protezione dei dati Snapshot

È possibile proteggere e ripristinare i dati utilizzando:

- Un controller di snapshot esterno e CRD per creare snapshot di volumi Kubernetes di volumi persistenti (PVS).

  "Snapshot dei volumi"

- ONTAP Snapshot per ripristinare l'intero contenuto di un volume o recuperare singoli file o LUN.

  "Istantanee di ONTAP"

Sicurezza

Sicurezza

Utilizzare i consigli elencati di seguito per assicurarsi che l'installazione di Trident sia

sicura.

Eseguire Trident nel proprio namespace

È importante impedire ad applicazioni, amministratori dell'applicazione, utenti e applicazioni di gestione di accedere alle definizioni di oggetti Trident o ai pod, per garantire uno storage affidabile e bloccare le potenziali attività pericolose.

Per separare le altre applicazioni e gli utenti da Trident, installare sempre Trident nel proprio spazio dei nomi Kubernetes (`trident`). Inserendo Trident nel proprio namespace, solo il personale amministrativo di Kubernetes potrà accedere al pod Trident e agli artefatti (come ad esempio backend e CHAP secrets, se applicabili) memorizzati negli oggetti CRD con nome. È necessario assicurarsi che solo gli amministratori possano accedere allo spazio dei nomi Trident e quindi all' `tridentctl`applicazione.

Utilizza l'autenticazione CHAP con i backend SAN ONTAP

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

Per i backend ONTAP che utilizzano i driver di archiviazione SAN, Trident può impostare il CHAP bidirezionale e gestire i nomi utente e i segreti CHAP tramite `tridentctl`. Fare riferimento a "Prepararsi a configurare il backend con i driver SAN ONTAP" per informazioni sulla configurazione del protocollo CHAP in Trident sui backend ONTAP.

Utilizza l'autenticazione CHAP con backend NetApp HCI e SolidFire

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

I volumi creati da Trident non sono associati ad alcun gruppo di accesso ai volumi.

USA Trident con NVE e NAE

NetApp ONTAP offre la crittografia dei dati inattivi per proteggere i dati sensibili in caso di furto, restituzione o riordinamento di un disco. Per ulteriori informazioni, fare riferimento alla "Panoramica sulla configurazione di NetApp Volume Encryption".

- Se NAE è abilitato sul backend, qualsiasi volume sottoposto a provisioning in Trident sarà abilitato NAE.
- Se NAE non è abilitato sul back-end, qualsiasi volume con provisioning in Trident sarà abilitato NVE a meno che non imposti il flag di crittografia NVE su `false` nella configurazione di back-end.

I volumi creati in Trident su un back-end abilitato per NAE devono essere crittografati NVE o NAE.

- Puoi impostare il flag di crittografia NVE su `true` nella configurazione di back-end Trident per ignorare la crittografia NAE e utilizzare una chiave di crittografia specifica in base al volume.
- L'impostazione del flag di crittografia NVE su `false` un backend abilitato per NAE crea un

volume abilitato per NAE. Non è possibile disattivare la crittografia NAE impostando il flag di crittografia NVE su `false`.

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

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

- "Opzioni di configurazione SAN ONTAP"
- "Opzioni di configurazione NAS ONTAP"

Linux Unified Key Setup (LUKS)

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

In Trident, i volumi crittografati con LUKS utilizzano il Cypher e la modalità aes-xts-plain64, come consigliato da "NIST".

Prima di iniziare

- Sui nodi di lavoro deve essere installata la crittografia 2.1 o superiore (ma inferiore a 3.0). Per ulteriori informazioni, visitare il sito "Gitlab: Crittsetup".
- Per motivi di performance, consigliamo ai nodi di lavoro di supportare Advanced Encryption Standard New Instructions (AES-NI). Per verificare il supporto AES-NI, eseguire il seguente comando:

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

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

Attivare la crittografia LUKS

È possibile attivare la crittografia lato host per volume utilizzando la configurazione unificata delle chiavi di Linux per volumi SAN ONTAP e SAN ONTAP.

Fasi

1. Definire gli attributi di crittografia LUKS nella configurazione del back-end. Per ulteriori informazioni sulle opzioni di configurazione back-end per SAN ONTAP, consultare "Opzioni di configurazione SAN ONTAP".

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

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

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

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Creare un segreto contenente la passphrase LUKS. Ad esempio:

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

Limitazioni

I volumi crittografati con LUKS non possono sfruttare la deduplica e la compressione ONTAP.

Configurazione back-end per l'importazione di volumi LUKS

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

```
version: 1
storageDriverName: ontap-san
```

```
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

Configurazione PVC per l'importazione di volumi LUKS

Per importare volumi LUKS in modo dinamico, impostare l'annotazione `trident.netapp.io/luksEncryption` su `true` e includere una classe di storage abilitata LUKS nel PVC, come illustrato in questo esempio.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

Ruotare una passphrase LUKS

È possibile ruotare la passphrase LUKS e confermare la rotazione.

> Non dimenticare una passphrase fino a quando non viene verificata la mancanza di riferimenti da qualsiasi volume, snapshot o segreto. In caso di perdita di una passphrase di riferimento, potrebbe non essere possibile montare il volume e i dati resteranno crittografati e inaccessibili.

A proposito di questa attività

La rotazione della passphrase LUKS si verifica quando viene creato un pod che monta il volume dopo aver specificato una nuova passphrase LUKS. Quando viene creato un nuovo pod, Trident confronta la passphrase LUKS del volume con la passphrase attiva nel segreto.

- Se la passphrase sul volume non corrisponde alla passphrase attiva nel segreto, si verifica la rotazione.

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

Fasi

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

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identificare le passphrase esistenti sul volume o sullo snapshot.

Volume

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. Aggiornare il segreto LUKS per il volume per specificare le passphrase nuove e precedenti. Verificare che `previous-luke-passphrase-name` `previous-luks-passphrase`la password precedente corrisponda a quella specificata.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
```

```
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Creare un nuovo pod per il montaggio del volume. Questa operazione è necessaria per avviare la rotazione.
5. Verificare che la passphrase sia stata ruotata.

Volume

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```

Risultati

La passphrase è stata ruotata quando viene restituita solo la nuova passphrase nel volume e nello snapshot.

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

Abilitare l'espansione dei volumi

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

Fasi

1. Abilitare la `CSINodeExpandSecret` porta Feature (beta 1,25+). Per ulteriori informazioni, fare riferimento alla "Kubernetes 1.25: Utilizza Secrets per l'espansione basata su nodi di volumi CSI" sezione.
2. Aggiungere i `node-expand-secret-name` parametri e `node-expand-secret-namespace` StorageClass. Ad esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
```

```
    csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
    csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
    csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
    csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Risultati

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

Crittografia Kerberos in-flight

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

Trident supporta la crittografia Kerberos per ONTAP come backend di storage:

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

Puoi creare, eliminare, ridimensionare, creare snapshot, clonare clone di sola lettura e importare i volumi che utilizzano la crittografia NFS.

Configura la crittografia Kerberos in-flight con i volumi ONTAP in sede

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

> La crittografia Kerberos per il traffico NFS con backend di archiviazione ONTAP in sede è supportata solo utilizzando il `ontap-nas` driver di archiviazione.

Prima di iniziare

- Assicurarsi di avere accesso all' `tridentctl` utilità.
- Assicurarsi di disporre dell'accesso come amministratore al back-end dello storage ONTAP.
- Conoscere il nome del volume o dei volumi che si desidera condividere dal back-end dello storage ONTAP.
- Verificare di aver preparato la VM di storage ONTAP per supportare la crittografia Kerberos per i volumi NFS. Fare riferimento alla "Attivare Kerberos su una LIF dati" per le istruzioni.
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Aggiungere o modificare criteri di esportazione ONTAP

Devi aggiungere regole alle policy di esportazione ONTAP esistenti o creare nuove policy di esportazione che supportino la crittografia Kerberos per il volume root delle macchine virtuali di storage ONTAP, oltre a qualsiasi volume ONTAP condiviso con il cluster Kubernetes upstream. Le regole dei criteri di esportazione aggiunte o i nuovi criteri di esportazione creati devono supportare i seguenti protocolli di accesso e autorizzazioni di accesso:

Protocolli di accesso

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

Dettagli di accesso

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

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

Configurare la regola dei criteri di esportazione ONTAP con le autorizzazioni di accesso appropriate. Ad esempio, se i cluster montano i volumi NFS con una combinazione di crittografia Kerberos 5i e Kerberos 5p, utilizza le seguenti impostazioni di accesso:

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

Per informazioni su come creare policy di esportazione e regole delle policy di esportazione di ONTAP, consulta la seguente documentazione:

- "Creare una policy di esportazione"
- "Aggiungere una regola a un criterio di esportazione"

Creazione di un backend dello storage

È possibile creare una configurazione backend dello storage Trident che include la funzionalità di crittografia Kerberos.

A proposito di questa attività

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

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

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

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando l'esempio seguente. Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

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

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

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

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

A proposito di questa attività

Quando si crea un oggetto classe di archiviazione, è possibile specificare una delle tre diverse versioni della

crittografia Kerberos utilizzando il `mountOptions` parametro:

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

Specificare un solo livello Kerberos. Se si specificano più livelli di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione. Se il livello di crittografia specificato nella configurazione backend di archiviazione è diverso dal livello specificato nell'oggetto della classe di archiviazione, l'oggetto della classe di archiviazione ha la precedenza.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Creare la classe di storage:

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

3. Assicurarsi che la classe di archiviazione sia stata creata:

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

   L'output dovrebbe essere simile a quanto segue:

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

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un volume. Per istruzioni, fare riferimento alla "Provisioning di un volume".

Configurare la crittografia Kerberos in-flight con i volumi Azure NetApp Files

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

Prima di iniziare

- Assicurati di aver abilitato Trident sul cluster gestito di Red Hat OpenShift.
- Assicurarsi di avere accesso all' `tridentctl` utilità.
- Assicurarsi di aver preparato il backend di archiviazione Azure NetApp Files per la crittografia Kerberos annotando i requisiti e seguendo le istruzioni riportate in "Documentazione Azure NetApp Files".
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Creazione di un backend dello storage

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

A proposito di questa attività

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

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

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

In entrambi i livelli, è possibile specificare una delle tre diverse versioni della crittografia Kerberos:

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

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando uno dei seguenti esempi, a seconda del punto in cui occorre definire il backend dello storage (livello di backend dello storage o livello del pool virtuale). Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

Esempio di livello di backend di archiviazione

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
```

```
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

Esempio di livello del pool virtuale

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
```

```
    networkFeatures: Standard
    capacityPools: <CAPACITY_POOL>
    resourceGroups: <RESOURCE_GROUP>
    netappAccounts: <NETAPP_ACCOUNT>
    virtualNetwork: <VIRTUAL_NETWORK>
    subnet: <SUBNET>
    nasType: nfs
    storage:
      - labels:
          type: encryption
        kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
    credentials:
      name: backend-tbc-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

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

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

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

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Creare la classe di storage:

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

3. Assicurarsi che la classe di archiviazione sia stata creata:

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

L'output dovrebbe essere simile a quanto segue:

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

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un volume. Per istruzioni, fare riferimento alla "Provisioning di un volume".

Informazioni sul copyright

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

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ 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 CONSEQUENZIALE (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.