Sicurezza

Astra Trident

NetApp
November 14, 2025

This PDF was generated from https://docs.netapp.com/it-it/trident-2304/trident-reco/security-reco.html on November 14, 2025. Always check docs.netapp.com for the latest.

Sommario

Sicurezza . . . 1
- Sicurezza . . . 1
  - Eseguire Astra Trident nel proprio namespace . . . 1
  - Utilizza l'autenticazione CHAP con i backend SAN ONTAP . . . 1
  - Utilizza l'autenticazione CHAP con backend NetApp HCI e SolidFire . . . 1
  - Utilizzare Astra Trident con NVE e NAE . . . 2
- Linux Unified Key Setup (LUKS) . . . 2
  - Attivare la crittografia LUKS . . . 3
  - Configurazione back-end per l'importazione di volumi LUKS . . . 4
  - Ruotare una passphrase LUKS . . . 4
  - Abilitare l'espansione dei volumi . . . 6

Sicurezza

Sicurezza

Utilizza i consigli elencati di seguito per assicurarti che l'installazione di Astra Trident sia sicura.

Eseguire Astra Trident nel proprio namespace

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

Per separare le altre applicazioni e gli utenti da Astra Trident, installare sempre Astra Trident nel proprio spazio dei nomi Kubernetes (`trident`). L'inserimento di Astra Trident nel proprio spazio dei nomi garantisce che solo il personale amministrativo di Kubernetes abbia accesso al pod Astra Trident e agli artefatti (come i segreti di backend e CHAP, se applicabili) memorizzati negli oggetti CRD con spazio dei nomi.
È necessario garantire che solo gli amministratori possano accedere allo spazio dei nomi Astra Trident e quindi a. `tridentctl` applicazione.

Utilizza l'autenticazione CHAP con i backend SAN ONTAP

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

Per i backend ONTAP che utilizzano i driver di storage SAN, Astra Trident può configurare CHAP bidirezionale e gestire i nomi utente e i segreti CHAP attraverso `tridentctl`.
Vedere "qui" Per capire come Astra Trident configura CHAP sui backend ONTAP.

> Il supporto CHAP per i backend ONTAP è disponibile con Trident 20.04 e versioni successive.

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. Astra Trident utilizza un oggetto segreto che include due password CHAP per tenant. Quando Trident viene installato come provider CSI, gestisce i segreti CHAP e li memorizza in un `tridentvolume` Oggetto CR per il rispettivo PV. Quando si crea un PV, CSI Astra Trident utilizza i segreti CHAP per avviare una sessione iSCSI e comunicare con il sistema NetApp HCI e SolidFire su CHAP.

> I volumi creati da CSI Trident non sono associati a alcun gruppo di accesso al volume.

Nel frontend non CSI, l'attacco di volumi come dispositivi sui nodi di lavoro viene gestito da Kubernetes. Dopo la creazione del volume, Astra Trident effettua una chiamata API al sistema NetApp HCI/SolidFire per recuperare i segreti se il segreto per quel tenant non esiste già. Astra Trident poi passa i segreti su Kubernetes. Il kubelet situato su ciascun nodo accede ai segreti tramite l'API Kubernetes e li utilizza per eseguire/abilitare CHAP tra ciascun nodo che accede al volume e il sistema NetApp HCI/SolidFire in cui si trovano i volumi.

Utilizzare Astra 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 a. "Panoramica sulla configurazione di NetApp Volume Encryption".

- Se NAE è attivato sul backend, qualsiasi volume fornito in Astra Trident sarà abilitato per NAE.
- Se NAE non è attivato sul backend, qualsiasi volume fornito in Astra Trident sarà abilitato per NVE, a meno che non si imposta il flag di crittografia NVE su `false` nella configurazione back-end.

> I volumi creati in Astra Trident su un backend abilitato NAE devono essere crittografati con NVE o NAE.
>
> - È possibile impostare il flag di crittografia NVE su `true` Nella configurazione backend Trident per eseguire l'override della crittografia NAE e utilizzare una chiave di crittografia specifica per volume.
> - Impostazione del flag di crittografia NVE su `false` Su un backend abilitato NAE verrà creato un volume abilitato NAE. Non è possibile disattivare la crittografia NAE impostando il flag di crittografia NVE su `false`.

- È possibile creare manualmente un volume NVE in Astra 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)

È possibile abilitare la configurazione delle chiavi unificate Linux (LUKS) per crittografare i volumi SAN ONTAP e SAN ONTAP SU Astra Trident. Astra Trident supporta la rotazione delle passphrase e l'espansione dei volumi con crittografia LUKS.

In Astra Trident, i volumi con crittografia LUKS utilizzano il cifrario aes-xts-plain64 e la modalità, 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, visita: "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 ONTAP SAN, fare riferimento a. "Opzioni di configurazione SAN ONTAP".

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

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

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
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` a.(`true` sul back-end. Il `luksEncryption` Option indica ad Astra Trident se il volume è conforme a LUKS (`true`) O non conforme a 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'
```

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, Astra Trident confronta la passphrase LUKS sul 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` il parametro viene ignorato.

Fasi

1. Aggiungere il `node-publish-secret-name` e. `node-publish-secret-namespace` Parametri StorageClass. Ad esempio:

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

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

Volume

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

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

Snapshot

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

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

3. Aggiornare il segreto LUKS per il volume per specificare le passphrase nuove e precedenti. Assicurarsi `previous-luke-passphrase-name` e. `previous-luks-passphrase` associare la passphrase precedente.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. 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, ad esempio, vengono restituite due passphrase `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. Attivare il `CSINodeExpandSecret` feature gate (beta 1.25+). Fare riferimento a. "Kubernetes 1.25: Utilizza Secrets per l'espansione basata su nodi di volumi CSI" per ulteriori informazioni.
2. Aggiungere il `node-expand-secret-name` e. `node-expand-secret-namespace` Parametri StorageClass. Ad esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
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.

Informazioni sul copyright

Copyright © 2025 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.