Inizia con la gestione delle chiavi esterne

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software-128/storage/concept_system_manage_key_get_started_with_external_key_management.html on November 12, 2025. Always check docs.netapp.com for the latest.

Sommario

Inizia con la gestione delle chiavi esterne

Inizia con la gestione delle chiavi esterne

La gestione delle chiavi esterne (EKM) garantisce una gestione sicura delle chiavi di autenticazione (AK) in combinazione con un server di chiavi esterne (EKS) esterno al cluster. Gli AK vengono utilizzati per bloccare e sbloccare le unità auto-crittografanti (SED) quando"crittografia a riposo" è abilitato sul cluster. L'EKS garantisce la generazione e l'archiviazione sicura degli AK. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito da OASIS, per comunicare con l'EKS.

- "Impostare la gestione esterna"
- "Crittografia software di reimpostazione della chiave principale a riposo"
- "Recupera le chiavi di autenticazione inaccessibili o non valide"
- "Comandi API di gestione delle chiavi esterne"

Trova maggiori informazioni

- "API CreateCluster che può essere utilizzata per abilitare la crittografia del software a riposo"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Impostare la gestione delle chiavi esterne

È possibile seguire questi passaggi e utilizzare i metodi API Element elencati per configurare la funzionalità di gestione delle chiavi esterne.

Cosa ti servirà

- Se si sta configurando la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, è stata abilitata la crittografia software a riposo utilizzando"Crea cluster" metodo su un nuovo cluster che non contiene volumi.

Passi

1. Stabilire una relazione di fiducia con l'External Key Server (EKS).
   a. Creare una coppia di chiavi pubblica/privata per il cluster Element che verrà utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API:"Crea coppia di chiavi pubbliche e private"
   b. Ottieni la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. Il CSR consente al server delle chiavi di verificare che il cluster Element che accederà alle chiavi sia autenticato come cluster Element. Chiamare il seguente metodo API:"Ottieni richiesta di firma del certificato del client"
   c. Utilizzare EKS/Autorità di certificazione per firmare il CSR recuperato. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un fornitore di chiavi definisce dove

ottenere una chiave, mentre un server definisce gli attributi specifici dell'EKS con cui verrà comunicata.

a. Crea un fornitore di chiavi in cui risiederanno i dettagli del server delle chiavi chiamando il seguente metodo API:"CreateKeyProviderKmip"

b. Creare un server di chiavi che fornisca il certificato firmato e il certificato di chiave pubblica dell'Autorità di certificazione chiamando i seguenti metodi API:"CreateKeyServerKmip" "TestKeyServerKmip"

   Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

c. Aggiungere il server delle chiavi al contenitore del provider delle chiavi chiamando i seguenti metodi API:"AggiungiKeyServerAlProviderKmip" "TestKeyProviderKmip"

   Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

3. Come passaggio successivo per la crittografia a riposo, eseguire una delle seguenti operazioni:

   a. (Per la crittografia hardware a riposo) Abilita"crittografia hardware a riposo" fornendo l'ID del fornitore di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il"Abilita crittografia a riposo" Metodo API.

      È necessario abilitare la crittografia a riposo tramite"API" . Abilitando la crittografia a riposo tramite il pulsante Element UI esistente, la funzionalità tornerà a utilizzare chiavi generate internamente.

   b. (Per la crittografia software a riposo) Per"crittografia software a riposo" per utilizzare il fornitore di chiavi appena creato, passare l'ID del fornitore di chiavi al"RekeySoftwareEncryptionAtRestMasterKey" Metodo API.

Trova maggiori informazioni

- "Abilitare e disabilitare la crittografia per un cluster"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Crittografia software di reimpostazione della chiave principale a riposo

È possibile utilizzare l'API Element per rigenerare una chiave esistente. Questo processo crea una nuova chiave master sostitutiva per il server di gestione delle chiavi esterno. Le chiavi principali vengono sempre sostituite da nuove chiavi principali e non vengono mai duplicate o sovrascritte.

Potrebbe essere necessario rinominare la chiave come parte di una delle seguenti procedure:

- Creare una nuova chiave come parte di un passaggio dalla gestione delle chiavi interne alla gestione delle chiavi esterne.
- Crea una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.

Questo processo è asincrono e restituisce una risposta prima che l'operazione di reimpostazione delle chiavi sia completata. Puoi usare il"Ottieni risultato asincrono" metodo per interrogare il sistema per vedere quando il processo è stato completato.

Cosa ti servirà

- Hai abilitato la crittografia software a riposo utilizzando"Crea cluster" metodo su un nuovo cluster che non contiene volumi e non ha I/O. Utilizzare il collegamento:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] per confermare che lo stato è `enabled` prima di procedere.
- Hai"ha stabilito un rapporto di fiducia" tra il cluster SolidFire e un External Key Server (EKS). Esegui il"TestKeyProviderKmip" metodo per verificare che sia stata stabilita una connessione con il fornitore della chiave.

Passi

1. Esegui il"ListKeyProvidersKmip" comando e copia l'ID del fornitore della chiave(`keyProviderID`).
2. Esegui il"RekeySoftwareEncryptionAtRestMasterKey" con il `keyManagementType` parametro come `external` E `keyProviderID` come numero ID del fornitore della chiave dal passaggio precedente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copia il `asyncHandle` valore dal `RekeySoftwareEncryptionAtRestMasterKey` risposta al comando.
4. Esegui il"Ottieni risultato asincrono" comando con il `asyncHandle` valore del passaggio precedente per confermare la modifica nella configurazione. Dalla risposta al comando dovresti vedere che la vecchia configurazione della chiave principale è stata aggiornata con le nuove informazioni sulla chiave. Copiare l'ID del nuovo fornitore di chiavi per utilizzarlo in un passaggio successivo.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Esegui il `GetSoftwareEncryptionatRestInfo` comando per confermare i nuovi dettagli della chiave, incluso il `keyProviderID` , sono stati aggiornati.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Trova maggiori informazioni

- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Recupera le chiavi di autenticazione inaccessibili o non valide

Occasionalmente può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, verrà generato un errore del cluster (denominato codice di errore del cluster). Qui vengono descritti i due casi più probabili.

Il cluster non è in grado di sbloccare le unità a causa di un errore del cluster KmipServerFault.

Ciò può verificarsi quando il cluster si avvia per la prima volta e il server delle chiavi non è accessibile o la chiave richiesta non è disponibile.

1. Seguire i passaggi di ripristino indicati nei codici di errore del cluster (se presenti).

Potrebbe essere impostato un errore sliceServiceUnhealthy perché le unità dei metadati sono state contrassegnate come non riuscite e impostate sullo stato "Disponibile".

Passaggi per la cancellazione:

1. Aggiungere nuovamente le unità.
2. Dopo 3 o 4 minuti, verificare che il `sliceServiceUnhealthy` il guasto è stato risolto.

Vedere"codici di errore del cluster" per maggiori informazioni.

Comandi API di gestione delle chiavi esterne

Elenco di tutte le API disponibili per la gestione e la configurazione di EKM.

Utilizzato per stabilire una relazione di fiducia tra il cluster e i server esterni di proprietà del cliente:

- Crea coppia di chiavi pubbliche e private
- Ottieni richiesta di firma del certificato del client

Utilizzato per definire i dettagli specifici dei server esterni di proprietà del cliente:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Utilizzato per creare e gestire i fornitori di chiavi che gestiscono server di chiavi esterni:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AggiungiKeyServerAlProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Per informazioni sui metodi API, vedere "Informazioni di riferimento API".

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.