Inizia a utilizzare la gestione esterna delle chiavi

Element Software

NetApp
April 17, 2024

Sommario

Inizia a utilizzare la gestione esterna delle chiavi

EKM (External Key Management) offre una gestione sicura delle chiavi di autenticazione (AK) insieme a un server esterno delle chiavi (EKS) off-cluster. Gli AKS vengono utilizzati per bloccare e sbloccare i dischi con crittografia automatica (SED) quando "crittografia a riposo" è attivato sul cluster. EKS fornisce generazione e storage sicuri di AKS. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito DA OASIS, per comunicare con EKS.

- "Configurare la gestione esterna"
- "Ridigita la chiave master di crittografia software a riposo"
- "Ripristino di chiavi di autenticazione inaccessibili o non valide"
- "Comandi API esterni per la gestione delle chiavi"

Trova ulteriori informazioni

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

Impostare la gestione esterna delle chiavi

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

Di cosa hai bisogno

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

Fasi

1. Stabilire una relazione di trust con EKS (External Key Server).
   a. Creare una coppia di chiavi pubbliche/private per il cluster di elementi che viene utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API: "CreatePublicPrivateKeyPair"
   b. Ottenere la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. La CSR consente al server delle chiavi di verificare che il cluster di elementi che accederà alle chiavi sia autenticato come cluster di elementi. Chiamare il seguente metodo API: "GetClientCertificateSignRequest"
   c. Utilizzare EKS/Certificate Authority per firmare la CSR recuperata. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un provider di chiavi definisce dove ottenere una chiave e un server definisce gli attributi specifici di EKS con cui verrà comunicata.
   a. Creare un provider di chiavi in cui risiedono i dettagli del server di chiavi chiamando il seguente metodo API: "CreateKeyProviderKmip"

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

   Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.

c. Aggiungere il server delle chiavi nel contenitore del provider di chiavi chiamando i seguenti metodi API: "AddKeyServerToProviderKmip" "TestKeyProviderKmip"

   Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.

3. Eseguire una delle seguenti operazioni come fase successiva per la crittografia a riposo:

   a. (Per la crittografia hardware a riposo) Enable (attiva) "crittografia hardware a riposo" Fornendo l'ID del provider di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il "EnableEncryptionAtRest" Metodo API.

   > È necessario attivare la crittografia a riposo tramite "API". Attivando la crittografia a riposo utilizzando il pulsante dell'interfaccia utente Element esistente, la funzione torna a utilizzare le chiavi generate internamente.

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

Trova ulteriori informazioni

- "Attivare e disattivare la crittografia per un cluster"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ridigita la chiave master di crittografia software a riposo

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

Potrebbe essere necessario eseguire una nuova chiave nell'ambito di una delle seguenti procedure:

- Creare una nuova chiave come parte di un cambiamento dalla gestione interna delle chiavi alla gestione esterna delle chiavi.
- Creare una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.

> Questo processo è asincrono e restituisce una risposta prima del completamento dell'operazione di rekey. È possibile utilizzare "GetAsyncResult" metodo per eseguire il polling del sistema per verificare il completamento del processo.

Di cosa hai bisogno

- È stata attivata la crittografia software a riposo utilizzando "CreateCluster" Metodo su un nuovo cluster che non contiene volumi e non dispone di i/O. Utilizzare il `GetSoftwareEncryptionatRestInfo` per confermare che lo stato è `enabled` prima di procedere.

- Lo hai fatto "instaurazione di una relazione di fiducia" Tra il cluster SolidFire e un server di chiavi esterne (EKS). Eseguire "TestKeyProviderKmip" metodo per verificare che sia stabilita una connessione con il provider di chiavi.

Fasi

1. Eseguire "ListKeyProvidersKmip" Comando e copia dell'ID del provider di chiavi (`keyProviderID`).
2. Eseguire "RekeySoftwareEncryptionAtRestMasterKey" con `keyManagementType` parametro as `external` e. `keyProviderID` Come numero ID del provider di chiavi del passaggio precedente:

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

3. Copiare il `asyncHandle` valore di `RekeySoftwareEncryptionAtRestMasterKey` risposta del comando.
4. Eseguire "GetAsyncResult" con il `asyncHandle` valore del passaggio precedente per confermare la modifica della configurazione. Dalla risposta del comando, dovresti vedere che la configurazione della vecchia chiave master è stata aggiornata con le nuove informazioni sulla chiave. Copiare il nuovo ID del provider 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. Eseguire `GetSoftwareEncryptionatRestInfo` per confermare i dettagli della nuova 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 ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ripristino di chiavi di autenticazione inaccessibili o non valide

Occasionalmente, può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, viene generato un guasto del cluster (indicato come codice di guasto del cluster). I due casi più probabili sono descritti qui.

Il cluster non è in grado di sbloccare i dischi a causa di un errore del cluster KmipServerFault.

Questo 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 le fasi di ripristino riportate nei codici di guasto del cluster (se presenti).

Un errore sliceServiceUnhealthy potrebbe essere impostato perché i dischi metadati sono stati contrassegnati come guasti e posizionati nello stato "Available" (disponibile).

Procedura per la cancellazione:

1. Aggiungere di nuovo i dischi.
2. Dopo 3-4 minuti, controllare che il `sliceServiceUnhealthy` il guasto è stato cancellato.

Vedere "codici di guasto del cluster" per ulteriori informazioni.

Comandi API esterni per la gestione delle chiavi

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

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

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

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

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServerKmip
- TestKeyServerKmip

Utilizzato per la creazione e la manutenzione di provider di chiavi che gestiscono server di chiavi esterni:

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

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