Commencez la gestion des clés externes

Element Software

NetApp
November 12, 2025

Sommaire

Commencez la gestion des clés externes

Commencez la gestion des clés externes

La gestion des clés externes (EKM) assure une gestion sécurisée des clés d'authentification (AK) en conjonction avec un serveur de clés externes hors cluster (EKS). Les clés AK servent à verrouiller et déverrouiller les disques à chiffrement automatique (SED) lorsque"chiffrement au repos" est activé sur le cluster. L'EKS assure la génération et le stockage sécurisés des AK. Le cluster utilise le protocole d'interopérabilité de gestion des clés (KMIP), un protocole standard défini par OASIS, pour communiquer avec l'EKS.

- "Mettre en place une gestion externe"
- "Réinitialisation du chiffrement logiciel au repos, clé principale"
- "Récupérer les clés d'authentification inaccessibles ou invalides"
- "Commandes de l'API de gestion des clés externes"

Trouver plus d'informations

- "L'API CreateCluster permet d'activer le chiffrement logiciel au repos."
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Configurer la gestion des clés externes

Vous pouvez suivre ces étapes et utiliser les méthodes de l'API Element répertoriées pour configurer votre fonctionnalité de gestion des clés externes.

Ce dont vous aurez besoin

- Si vous configurez la gestion des clés externes en combinaison avec le chiffrement logiciel au repos, vous avez activé le chiffrement logiciel au repos à l'aide de"Créer un cluster" méthode sur un nouveau cluster ne contenant pas de volumes.

Étapes

1. Établir une relation de confiance avec le serveur de clés externe (EKS).
   a. Créez une paire de clés publique/privée pour le cluster Element qui sera utilisée pour établir une relation de confiance avec le serveur de clés en appelant la méthode API suivante :"Créer une paire de clés publique/privée"
   b. Obtenez la demande de signature de certificat (CSR) que l'autorité de certification doit signer. Le CSR permet au serveur de clés de vérifier que le cluster Element qui accédera aux clés est authentifié en tant que cluster Element. Appelez la méthode API suivante :"Demande de signature du certificat client"
   c. Utilisez l'autorité de certification EKS pour signer la CSR récupérée. Consultez la documentation tierce pour plus d'informations.
2. Créez un serveur et un fournisseur sur le cluster pour communiquer avec EKS. Un fournisseur de clés définit où une clé doit être obtenue, et un serveur définit les attributs spécifiques de l'EKS avec lequel la

communication sera établie.

a. Créez un fournisseur de clés où résideront les détails du serveur de clés en appelant la méthode API suivante :"CréerKeyProviderKmip"

b. Créez un serveur de clés fournissant le certificat signé et le certificat de clé publique de l'autorité de certification en appelant les méthodes API suivantes :"CréerKeyServerKmip" "TestKeyServerKmip"

   Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.

c. Ajoutez le serveur de clés au conteneur du fournisseur de clés en appelant les méthodes API suivantes :"AjouterKeyServerToProviderKmip" "TestKeyProviderKmip"

   Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.

3. Prochaine étape pour le chiffrement au repos :

a. (Pour le chiffrement matériel au repos) Activer"chiffrement matériel au repos" en fournissant l'identifiant du fournisseur de clés qui contient le serveur de clés utilisé pour stocker les clés en appelant le"Activer le chiffrement au repos" Méthode API.

> Vous devez activer le chiffrement au repos via le"API" . L'activation du chiffrement au repos à l'aide du bouton existant de l'interface utilisateur Element aura pour conséquence que la fonctionnalité utilise à nouveau des clés générées en interne.

b. (Pour le chiffrement logiciel au repos) Afin de"Cryptage logiciel au repos" Pour utiliser le fournisseur de clés nouvellement créé, transmettez l'ID du fournisseur de clés à"RekeySoftwareEncryptionAtRestMasterKey" Méthode API.

Trouver plus d'informations

- "Activer et désactiver le chiffrement pour un cluster"
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Réinitialisation du chiffrement logiciel au repos, clé principale

Vous pouvez utiliser l'API Element pour modifier une clé existante. Ce processus crée une nouvelle clé principale de remplacement pour votre serveur de gestion de clés externe. Les clés maîtresses sont toujours remplacées par de nouvelles clés maîtresses et ne sont jamais dupliquées ni écrasées.

Vous pourriez avoir besoin de ressaisir vos identifiants dans le cadre de l'une des procédures suivantes :

- Créer une nouvelle clé dans le cadre d'une transition de la gestion des clés internes à la gestion des clés externes.
- Créer une nouvelle clé en réaction à un événement lié à la sécurité ou pour s'en protéger.

> Ce processus est asynchrone et renvoie une réponse avant que l'opération de renouvellement de clé ne soit terminée. Vous pouvez utiliser le"GetAsyncResult" méthode permettant d'interroger le système pour savoir quand le processus est terminé.

Ce dont vous aurez besoin

- Vous avez activé le chiffrement logiciel au repos à l'aide de"Créer un cluster" méthode sur un nouveau cluster qui ne contient pas de volumes et n'a pas d'E/S. Utilisez le lien :../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] pour confirmer que l'état est `enabled` avant de continuer.
- Tu as"ont établi une relation de confiance" entre le cluster SolidFire et un serveur de clés externe (EKS). Exécutez le"TestKeyProviderKmip" méthode permettant de vérifier qu'une connexion au fournisseur de clés est établie.

Étapes

1. Exécutez le"ListKeyProvidersKmip" commande et copiez l'ID du fournisseur de clés(`keyProviderID`).
2. Exécutez le"RekeySoftwareEncryptionAtRestMasterKey" avec le `keyManagementType` paramètre comme `external` et `keyProviderID` comme numéro d'identification du fournisseur de clés de l'étape précédente :

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

3. Copiez le `asyncHandle` la valeur de la `RekeySoftwareEncryptionAtRestMasterKey` Réponse à la commande.
4. Exécutez le"GetAsyncResult" commande avec le `asyncHandle` valeur de l'étape précédente pour confirmer la modification de la configuration. La réponse à la commande devrait indiquer que l'ancienne configuration de la clé principale a été mise à jour avec les nouvelles informations de clé. Copiez le nouvel identifiant du fournisseur de clés pour l'utiliser ultérieurement.

```
{
   "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. Exécutez le `GetSoftwareEncryptionatRestInfo` commande pour confirmer que les nouveaux détails clés, y compris le `keyProviderID` , ont été mises à jour.

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

Trouver plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Récupérer les clés d'authentification inaccessibles ou invalides

Il peut arriver, de temps à autre, qu'une erreur nécessite l'intervention de l'utilisateur. En cas d'erreur, un défaut de cluster (appelé code de défaut de cluster) sera généré. Les deux cas les plus probables sont décrits ici.

Le cluster ne peut pas déverrouiller les disques en raison d'une erreur de cluster KmipServerFault.

Cela peut se produire lors du premier démarrage du cluster, lorsque le serveur de clés est inaccessible ou que la clé requise est indisponible.

1. Suivez les étapes de récupération indiquées dans les codes d'erreur du groupe (le cas échéant).

Une erreur sliceServiceUnhealthy peut être déclenchée car les disques de métadonnées ont été marqués comme défaillants et placés dans l'état « Disponible ».

Étapes à suivre pour obtenir le résultat :

1. Ajoutez à nouveau les disques.
2. Après 3 à 4 minutes, vérifiez que le `sliceServiceUnhealthy` Le problème a disparu.

Voir"codes d'erreur du groupe d'outils" pour plus d'informations.

Commandes de l'API de gestion des clés externes

Liste de toutes les API disponibles pour la gestion et la configuration d'EKM.

Utilisé pour établir une relation de confiance entre le cluster et les serveurs externes appartenant au client :

- Créer une paire de clés publique/privée
- Demande de signature du certificat client

Utilisé pour définir les détails spécifiques des serveurs externes appartenant au client :

- CréerKeyServerKmip
- ModifierKeyServerKmip
- SupprimerKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Utilisé pour créer et maintenir des fournisseurs de clés qui gèrent des serveurs de clés externes :

- CréerKeyProviderKmip
- DeleteKeyProviderKmip
- AjouterKeyServerToProviderKmip
- SupprimerKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Pour plus d'informations sur les méthodes de l'API, consultez "Informations de référence de l'API".

Informations sur le copyright

Informations sur les marques commerciales