Commencez par une gestion externe des clés

Element Software

NetApp
January 15, 2024

Sommaire

Commencez par une gestion externe des clés

La gestion externe des clés (EKM) assure la gestion de la clé d'authentification sécurisée (AK) en association avec un serveur de clés externe hors cluster (EKS). Les clés de verrouillage sont utilisées pour verrouiller et déverrouiller les disques à autocryptage (SED) lorsque "chiffrement des données au repos" est activé sur le cluster. Le EKS fournit une génération et un stockage sécurisés des clés de sécurité. Le cluster utilise le protocole KMIP (Key Management Interoperability Protocol), un protocole standard défini PAR OASIS, pour communiquer avec le EKS.

- "Configurer la gestion externe"
- "Chiffrement logiciel de nouvelle clé pour la clé principale REST"
- "Récupérer les clés d'authentification inaccessibles ou non valides"
- "Commandes d'API de gestion externe des clés"

Trouvez plus d'informations

- "CreateCluster API pouvant être utilisée pour activer le chiffrement logiciel au repos"
- "Documentation SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Configurez la gestion externe des clés

Procédez comme suit et utilisez les méthodes de l'API Element répertoriées pour configurer votre fonctionnalité de gestion externe des clés.

Ce dont vous avez besoin

- Si vous configurez la gestion externe des clés en association avec le chiffrement logiciel au repos, vous avez activé le chiffrement logiciel au repos à l'aide du "CreateCluster" méthode sur un nouveau cluster qui ne contient pas de volumes.

Étapes

1. Établissez une relation de confiance avec le serveur de clés externe (EKS).
   a. Créez une paire de clés publique/privée pour le cluster Element qui est utilisé pour établir une relation de confiance avec le serveur clé en appelant la méthode API suivante : "CreatePublicPrivateKeypair"
   b. Obtenir la demande de signature de certificat (CSR) que l'autorité de certification doit signer. La RSC permet au serveur de clés de vérifier que le cluster d'éléments qui accédera aux clés est authentifié comme cluster d'éléments. Appelez la méthode API suivante : "GetClientCertificateSignRequest"
   c. Utilisez EKS/Certificate Authority pour signer la RSC récupérée. Pour plus d'informations, consultez la documentation d'un fournisseur tiers.
2. Créez un serveur et un fournisseur sur le cluster pour communiquer avec EKS. Un fournisseur clé définit l'endroit où une clé doit être obtenue et un serveur définit les attributs spécifiques de l'EKS qui seront communiqués.
   a. Créez un fournisseur de clés où résident les détails du serveur de clés en appelant la méthode API suivante : "CreateKeyProviderKmip"

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 : "CreateKeyServerKmip" "TestKeyServerKmip"

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

c. Ajoutez le serveur de clés dans le conteneur du fournisseur de clés en appelant les méthodes d'API suivantes :"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

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

3. Pour le chiffrement au repos, effectuez l'une des opérations suivantes :

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

      Vous devez activer le chiffrement au repos via le "API". L'activation du chiffrement au repos à l'aide du bouton de l'interface utilisateur d'Element entraîne la restauration de la fonctionnalité à l'aide de clés générées en interne.

   b. (Pour le chiffrement logiciel au repos) dans l'ordre de "chiffrement logiciel pour les données au repos" Pour utiliser le nouveau fournisseur de clés créé, transmettez l'ID du fournisseur de clés au "RekeySoftwareEncryptionAtResteMasterKey" Méthode API.

Trouvez plus d'informations

- "Activez et désactivez le cryptage pour un cluster"
- "Documentation SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Chiffrement logiciel de nouvelle clé pour la clé principale REST

Vous pouvez utiliser l'API Element pour re-saisir une clé existante. Ce processus crée une nouvelle clé principale de remplacement pour votre serveur de gestion de clés externe. Les clés principales sont toujours remplacées par de nouvelles clés principales et ne sont jamais dupliquées ou remplacées.

Vous devrez peut-être procéder à une nouvelle clé dans le cadre de l'une des procédures suivantes :

- Créez une nouvelle clé dans le cadre d'un changement de gestion interne des clés à gestion externe des clés.
- Créez une nouvelle clé comme réaction ou comme protection contre un événement lié à la sécurité.

Ce processus est asynchrone et renvoie une réponse avant la fin de l'opération de renouvellement de clé. Vous pouvez utiliser le "GetAsyncResult" méthode d'interrogation du système pour voir quand le processus est terminé.

Ce dont vous avez besoin

- Vous avez activé le chiffrement logiciel au repos à l'aide du "CreateCluster" D'une nouvelle méthode située

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.

- Vous avez "établissement d'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 "ListeKeyProvidersKmip" Commande et copie l'ID du fournisseur de clés (`keyProviderID`).
2. Exécutez le "RekeySoftwareEncryptionAtResteMasterKey" avec le `keyManagementType` ens. paramètre `external` et `keyProviderID` Comme numéro d'ID du fournisseur de clés de l'étape précédente :

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

3. Copiez le `asyncHandle` valeur du `RekeySoftwareEncryptionAtRestMasterKey` réponse de la commande.
4. Exécutez le "GetAsyncResult" commande avec `asyncHandle` valeur de l'étape précédente pour confirmer le changement de configuration. À partir de la réponse de commande, vous devriez voir que l'ancienne configuration de clé principale a été mise à jour avec de nouvelles informations de clé. Copiez le nouvel ID de 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 de clé, y compris le `keyProviderID`, ont été mis 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
   },
}
```

Trouvez plus d'informations

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

Récupérer les clés d'authentification inaccessibles ou non valides

Parfois, une erreur peut se produire et nécessiter l'intervention de l'utilisateur. En cas d'erreur, un défaut du bloc d'instruments (appelé code inconvénient du bloc d'instruments) est généré. Les deux cas les plus probables sont décrits ici.

Le cluster ne parvient pas à déverrouiller les lecteurs en raison d'une défaillance du cluster KmipServerFault.

Cela peut se produire lorsque le cluster démarre et que le serveur de clés est inaccessible ou que la clé requise n'est pas disponible.

1. Suivre les étapes de récupération des codes inconvénient du tableau de bord (le cas échéant).

Il est possible de définir une défaillance sliceServiceIsain, car les lecteurs de métadonnées ont été marqués comme défectueux et placés dans l'état « disponible ».

Étapes à supprimer :

1. Ajoutez à nouveau les lecteurs.
2. Au bout de 3 à 4 minutes, vérifier que le `sliceServiceUnhealthy` le défaut a disparu.

Voir "codes d'anomalie du bloc d'instruments" pour en savoir plus.

Commandes d'API de gestion externe des clés

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 appartenant à un client externe :

- CreatePublicPrivateKeypair
- GetClientCertificateSignRequest

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

- CreateKeyServerKmip
- ModityKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServoersKmip
- TestKeyServerKmip

Utilisé pour la création et la maintenance de fournisseurs clés qui gèrent des serveurs de clés externes :

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListeKeyProvidersKmip
- RekeySoftwareEncryptionAtResteMasterKey
- TestKeyProviderKmip

Pour plus d’informations sur les méthodes API, voir "Informations de référence API".

Informations sur le copyright

Informations sur les marques commerciales