Comece a gerenciar chaves externas.

Element Software

NetApp
November 12, 2025

Índice

Comece a gerenciar chaves externas.

Comece a gerenciar chaves externas.

O gerenciamento de chaves externas (EKM) fornece gerenciamento seguro de chaves de autenticação (AK) em conjunto com um servidor de chaves externas fora do cluster (EKS). Os AKs são usados para bloquear e desbloquear unidades de criptografia automática (SEDs) quando"criptografia em repouso" está habilitado no cluster. O EKS proporciona a geração e o armazenamento seguros dos AKs. O cluster utiliza o Key Management Interoperability Protocol (KMIP), um protocolo padrão definido pela OASIS, para se comunicar com o EKS.

- "Configurar gestão externa"
- "Recodificar criptografia de software em repouso chave mestra"
- "Recuperar chaves de autenticação inacessíveis ou inválidas"
- "Comandos da API de gerenciamento de chaves externas"

Encontre mais informações

- "A API CreateCluster pode ser usada para habilitar a criptografia de software em repouso."
- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Configurar gerenciamento de chaves externas

Você pode seguir esses passos e usar os métodos da API Element listados para configurar seu recurso de gerenciamento de chaves externas.

O que você vai precisar

- Se você estiver configurando o gerenciamento de chaves externas em conjunto com a criptografia de software em repouso, você habilitou a criptografia de software em repouso usando o"CriarCluster" método em um novo cluster que não contém volumes.

Passos

1. Estabelecer uma relação de confiança com o Servidor de Chaves Externo (EKS).
   a. Crie um par de chaves pública/privada para o cluster Element que será usado para estabelecer uma relação de confiança com o servidor de chaves, chamando o seguinte método da API:"CriarParDeChavesPúblicasPrivadas"
   b. Obtenha a solicitação de assinatura de certificado (CSR) que a Autoridade Certificadora precisa assinar. O CSR permite que o servidor de chaves verifique se o cluster Element que acessará as chaves está autenticado como o cluster Element correto. Chame o seguinte método da API:"Solicitação de assinatura de certificado de cliente"
   c. Utilize a Autoridade Certificadora/EKS para assinar o CSR recuperado. Consulte a documentação de terceiros para obter mais informações.
2. Crie um servidor e um provedor no cluster para se comunicar com o EKS. Um provedor de chaves define

onde uma chave deve ser obtida, e um servidor define os atributos específicos do EKS com os quais a comunicação será realizada.

a. Crie um provedor de chaves onde os detalhes do servidor de chaves residirão, chamando o seguinte método da API:"CriarProvedorDeChavesKmip"

b. Crie um servidor de chaves que forneça o certificado assinado e o certificado de chave pública da Autoridade de Certificação, chamando os seguintes métodos da API:"CriarKeyServerKmip" "TestKeyServerKmip"

   Se o teste falhar, verifique a conectividade e a configuração do seu servidor. Em seguida, repita o teste.

c. Adicione o servidor de chaves ao contêiner do provedor de chaves chamando os seguintes métodos da API:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

   Se o teste falhar, verifique a conectividade e a configuração do seu servidor. Em seguida, repita o teste.

3. Como próximo passo para a criptografia em repouso, realize uma das seguintes ações:

   a. (Para criptografia de hardware em repouso) Ativar"criptografia de hardware em repouso" fornecendo o ID do provedor de chaves que contém o servidor de chaves usado para armazenar as chaves, chamando o"Habilitar criptografia em repouso" Método da API.

      > Você deve habilitar a criptografia em repouso por meio do"API" . Habilitar a criptografia em repouso usando o botão existente na interface do usuário do Element fará com que o recurso volte a usar chaves geradas internamente.

   b. (Para criptografia de software em repouso) Para que"criptografia de software em repouso" Para utilizar o provedor de chaves recém-criado, passe o ID do provedor de chaves para o"RekeySoftwareEncryptionAtRestMasterKey" Método da API.

Encontre mais informações

- "Ativar e desativar a criptografia para um cluster"
- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Recodificar criptografia de software em repouso chave mestra

Você pode usar a API Element para redefinir a chave de uma chave existente. Este processo cria uma nova chave mestra de substituição para o seu servidor externo de gerenciamento de chaves. As chaves mestras são sempre substituídas por novas chaves mestras e nunca duplicadas ou sobrescritas.

Você poderá precisar trocar as teclas como parte de um dos seguintes procedimentos:

- Criar uma nova chave como parte de uma mudança do gerenciamento de chaves interno para o gerenciamento de chaves externo.
- Crie uma nova chave como reação a um evento relacionado à segurança ou como proteção contra ele.

Esse processo é assíncrono e retorna uma resposta antes que a operação de recriptografia seja concluída. Você pode usar o"ObterResultadoAssíncrono" Método para consultar o sistema e verificar quando o processo foi concluído.

O que você vai precisar

- Você habilitou a criptografia de software em repouso usando o"CriarCluster" método em um novo cluster que não contém volumes e não possui operações de E/S. Use o `GetSoftwareEncryptionatRestInfo` para confirmar que o estado é `enabled` antes de prosseguir.
- Você tem"estabelecer uma relação de confiança" entre o cluster SolidFire e um servidor de chaves externo (EKS). Execute o"TestKeyProviderKmip" Método para verificar se a conexão com o provedor de chaves foi estabelecida.

Passos

1. Execute o"ListKeyProvidersKmip" comando e copie o ID do provedor de chave(`keyProviderID`).
2. Execute o"RekeySoftwareEncryptionAtRestMasterKey" com o `keyManagementType` parâmetro como `external` e `keyProviderID` como o número de identificação do provedor de chaves da etapa anterior:

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

3. Copie o `asyncHandle` valor do `RekeySoftwareEncryptionAtRestMasterKey` resposta ao comando.
4. Execute o"ObterResultadoAssíncrono" comando com o `asyncHandle` Utilize o valor da etapa anterior para confirmar a alteração na configuração. A partir da resposta do comando, você deverá ver que a configuração da chave mestra antiga foi atualizada com as novas informações da chave. Copie o novo ID do provedor de chaves para usar em uma etapa posterior.

```
{
   "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. Execute o `GetSoftwareEncryptionatRestInfo` comando para confirmar novos detalhes importantes, incluindo o `keyProviderID` , foram atualizados.

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

Encontre mais informações

- "Gerencie o armazenamento com a API Element."
- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Recuperar chaves de autenticação inacessíveis ou inválidas

Ocasionalmente, pode ocorrer um erro que exige intervenção do usuário. Em caso de erro, será gerado um erro de cluster (denominado código de falha de cluster). Os dois casos mais prováveis são descritos aqui.

O cluster não consegue desbloquear as unidades devido a uma falha de cluster KmipServerFault.

Isso pode ocorrer quando o cluster é inicializado e o servidor de chaves está inacessível ou a chave necessária não está disponível.

1. Siga os passos de recuperação indicados nos códigos de falha do cluster (se houver).

Uma falha sliceServiceUnhealthy pode ser registrada porque as unidades de metadados foram marcadas como defeituosas e colocadas no estado "Disponível".

Passos para limpar:

1. Adicione as unidades novamente.
2. Após 3 a 4 minutos, verifique se o `sliceServiceUnhealthy` O problema foi resolvido.

Ver"códigos de falha do painel" para mais informações.

Comandos da API de gerenciamento de chaves externas

Lista de todas as APIs disponíveis para gerenciar e configurar o EKM.

Utilizado para estabelecer uma relação de confiança entre o cluster e servidores externos pertencentes ao cliente:

- CriarParDeChavesPúblicasPrivadas
- Solicitação de assinatura de certificado de cliente

Utilizado para definir os detalhes específicos de servidores externos pertencentes ao cliente:

- CriarKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Utilizado para criar e manter provedores de chaves que gerenciam servidores de chaves externos:

- CriarProvedorDeChavesKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoverKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Para obter informações sobre os métodos da API, consulte "Informações de referência da API".

Informações sobre direitos autorais

Informações sobre marcas comerciais