Autentique mutuamente o cluster e um servidor KMIP

ONTAP 9

NetApp
January 17, 2025

Índice

Autentique mutuamente o cluster e um servidor KMIP

Autenticando mutuamente o cluster e uma visão geral do servidor KMIP

Autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP (Key Management Interoperability Protocol), permite que o gerenciador de chaves se comunique com o cluster usando KMIP em SSL. Você o faz quando um aplicativo ou uma determinada funcionalidade (por exemplo, a funcionalidade criptografia de armazenamento) exige chaves seguras para fornecer acesso seguro aos dados.

Gerar uma solicitação de assinatura de certificado para o cluster

Você pode usar o comando certificado de segurança `generate-csr` para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

O que você vai precisar

Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size
   512|1024|1536|2048 -country country -state state -locality locality
   -organization organization -unit unit -email-addr email_of_contact -hash
   -function SHA1|SHA256|MD5
   ```

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O comando a seguir cria uma CSR com uma chave privada de 2.048 bits gerada pela função de hash SHA256 para uso pelo grupo Software no departamento DE TI de uma empresa cujo nome comum personalizado é server1.companyname.com, localizada em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contatos do SVM é web@example.com. O sistema apresenta a CSR e a chave privada na saída.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copie a solicitação de certificado da saída CSR e, em seguida, envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

   Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA para o cluster

Para permitir que um servidor SSL autentique o cluster ou a máquina virtual de armazenamento (SVM) como um cliente SSL, instale um certificado digital com o tipo de cliente no cluster ou SVM. Em seguida, você fornece o certificado cliente-CA ao administrador do servidor SSL para instalação no servidor.

O que você vai precisar

Você já deve ter instalado o certificado raiz do servidor SSL no cluster ou SVM com o `server-ca` tipo de certificado.

Passos

1. Para usar um certificado digital autoassinado para autenticação de cliente, use o `security certificate create` comando com o `type client` parâmetro.
2. Para usar um certificado digital assinado pela CA para autenticação de cliente, execute as seguintes etapas:

   a. Gere uma solicitação de assinatura de certificado digital (CSR) usando o comando de certificado de segurança `generate-csr`.

      O ONTAP exibe a saída CSR, que inclui uma solicitação de certificado e uma chave privada, e lembra que você deve copiar a saída para um arquivo para referência futura.

   b. Envie a solicitação de certificado da saída CSR em um formulário eletrônico (como e-mail) para uma CA confiável para assinatura.

      Você deve manter uma cópia da chave privada e do certificado assinado pela CA para referência futura.

   Após processar sua solicitação, a CA envia o certificado digital assinado.

   a. Instale o certificado assinado pela CA usando o `security certificate install` comando com o `-type client` parâmetro.
   b. Digite o certificado e a chave privada quando você for solicitado e pressione **Enter**.
   c. Insira quaisquer certificados raiz ou intermediários adicionais quando for solicitado e pressione **Enter**.

      Você instala um certificado intermediário no cluster ou SVM se uma cadeia de certificados que começa na CA raiz confiável e termina com o certificado SSL emitido para você estiver faltando os certificados intermediários. Um certificado intermediário é um certificado subordinado emitido pela raiz confiável especificamente para emitir certificados de servidor de entidade final. O resultado é uma cadeia de certificados que começa na CA raiz confiável, passa pelo certificado intermediário e termina com o certificado SSL emitido para você.

3. Forneça o `client-ca` certificado do cluster ou SVM ao administrador do servidor SSL para instalação no servidor.

   O comando show do certificado de segurança com os `-instance` parâmetros e `-type client-ca` exibe as `client-ca` informações do certificado.

Instale um certificado de cliente assinado pela CA para o servidor KMIP

O subtipo de certificado do Key Management Interoperability Protocol (KMIP) (o parâmetro -subtype kmip-cert), juntamente com os tipos cliente e servidor-CA, especifica que o certificado é usado para autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP.

Sobre esta tarefa

Instale um certificado KMIP para autenticar um servidor KMIP como um servidor SSL no cluster.

Passos

1. Use o `security certificate install` comando com os `-type server-ca` parâmetros e `-subtype kmip-cert` para instalar um certificado KMIP para o servidor KMIP.
2. Quando lhe for solicitado, introduza o certificado e, em seguida, prima Enter.

   O ONTAP lembra que você deve manter uma cópia do certificado para referência futura.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Informações sobre direitos autorais

Informações sobre marcas comerciais