Autentique mutuamente el clúster y un servidor KMIP

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/system-admin/mutually-authenticating-cluster-kmip-server-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Autentique mutuamente el clúster y un servidor KMIP 1
Autenticar mutuamente el clúster y una información general del servidor KMIP 1
Genere una solicitud de firma de certificación para el clúster de 1
Instale un certificado de servidor firmado por CA para el clúster 2
Instale un certificado de cliente firmado por CA para el servidor KMIP 3

Autentique mutuamente el clúster y un servidor KMIP

Autenticar mutuamente el clúster y una información general del servidor KMIP

Al autenticar mutuamente el clúster y un gestor de claves externo, como un servidor de protocolo de interoperabilidad de gestión de claves (KMIP), el administrador de claves puede comunicarse con el clúster mediante KMIP a través de SSL. Esto se hace cuando una aplicación o determinada funcionalidad (por ejemplo, la funcionalidad de cifrado del almacenamiento) requieren claves seguras para ofrecer un acceso seguro a los datos.

Genere una solicitud de firma de certificación para el clúster de

Puede utilizar el certificado de seguridad `generate-csr` Comando para generar una solicitud de firma de certificación (CSR). Después de procesar la solicitud, la entidad de certificación (CA) envía el certificado digital firmado.

Lo que necesitará

Debe ser un administrador de clúster o un administrador de SVM para ejecutar esta tarea.

Pasos

1. Genere una 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 obtener una sintaxis de comando completa, consulte las páginas man.

   El siguiente comando crea una CSR con una clave privada de 2,048 bits generada por la función de hashing SHA256 para que la utilice el grupo Software del departamento DE TI de una empresa cuyo nombre común personalizado es server1.companyname.com, ubicado en Sunnyvale, California, EE. UU. La dirección de correo electrónico del administrador de contacto de la SVM es web@example.com. El sistema muestra la CSR y la clave privada en la salida.

```
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 la solicitud de certificado de la salida CSR y envíela en formato electrónico (por ejemplo, correo electrónico) a una CA de terceros de confianza para su firma.

   Después de procesar la solicitud, la CA envía el certificado digital firmado. Debe conservar una copia de la clave privada y el certificado digital firmado por la CA.

Instale un certificado de servidor firmado por CA para el clúster

Para habilitar un servidor SSL que autentique el clúster o la máquina virtual de almacenamiento (SVM) como cliente SSL, se instala un certificado digital con el tipo de cliente en el clúster o la SVM. A continuación, proporcionará el certificado de CA de cliente al administrador del servidor SSL para su instalación en el servidor.

Lo que necesitará

Ya debe haber instalado el certificado raíz del servidor SSL en el clúster o la SVM con el `server-ca` tipo de certificado.

Pasos

1. Para usar un certificado digital autofirmado para la autenticación de clientes, use `security certificate create` con el `type client` parámetro.
2. Para utilizar un certificado digital firmado por CA para la autenticación de clientes, complete los siguientes pasos:

   a. Genere una solicitud de firma de certificación (CSR) digital mediante el certificado de seguridad `generate-csr` comando.

      ONTAP muestra el resultado de CSR, que incluye una solicitud de certificado y una clave privada, y le recuerda que debe copiar el resultado en un archivo para futura referencia.

   b. Envíe la solicitud de certificado de la salida de CSR en un formulario electrónico (como por ejemplo, correo electrónico) a una CA de confianza para su firma.

      Debe conservar una copia de la clave privada y el certificado firmado por CA para referencia futura.

   Después de procesar la solicitud, la CA envía el certificado digital firmado.

   a. Instale el certificado firmado por la CA con el `security certificate install` con el `-type client` parámetro.
   b. Introduzca el certificado y la clave privada cuando se le solicite y, a continuación, pulse **Intro**.
   c. Introduzca cualquier certificado raíz o intermedio adicional cuando se le solicite y, a continuación, pulse **Intro**.

      Puede instalar un certificado intermedio en el clúster o la SVM si a una cadena de certificados que comienza en la CA raíz de confianza y finaliza con el certificado SSL emitido para usted, le faltan los certificados intermedios. Un certificado intermedio es un certificado subordinado emitido por el raíz de confianza específicamente para emitir certificados de servidor de entidades finales. El resultado es una cadena de certificados que comienza en la CA raíz de confianza, atraviesa el certificado intermedio y termina con el certificado SSL que se le emitió.

3. Proporcione el `client-ca` Certificado del clúster o SVM al administrador del servidor SSL para su instalación en el servidor.

   El comando Security certificate show con el `-instance` y.. `-type client-ca` los parámetros muestran la `client-ca` información del certificado.

Instale un certificado de cliente firmado por CA para el servidor KMIP

El subtipo de certificado del protocolo de interoperabilidad de gestión de claves (KMIP) (el parámetro -subtipo kmip-cert), junto con los tipos de CA del cliente y del servidor, especifica que el certificado se utiliza para autenticar mutuamente el clúster y un gestor de claves externo, como un servidor KMIP.

Acerca de esta tarea

Instale un certificado KMIP para autenticar un servidor KMIP como servidor SSL en el clúster.

Pasos

1. Utilice la `security certificate install` con el `-type server-ca` y.. `-subtype kmip-cert` Parámetros para instalar un certificado KMIP en el servidor KMIP.
2. Cuando se le solicite, introduzca el certificado y pulse Intro.

   ONTAP le recuerda que debe conservar una copia del certificado para futuras consultas.

```
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::>
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.