



对集群和KMIP服务器进行相互身份验证

ONTAP 9

NetApp
April 24, 2024

目录

- 对集群和KMIP服务器进行相互身份验证..... 1
 - 对集群和 KMIP 服务器进行相互身份验证概述..... 1
 - 为集群生成证书签名请求..... 1
 - 为集群安装 CA 签名的服务器证书..... 2
 - 为 KMIP 服务器安装 CA 签名的客户端证书..... 3

对集群和KMIP服务器进行相互身份验证

对集群和 KMIP 服务器进行相互身份验证概述

通过对集群和外部密钥管理器（例如密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）服务器）进行相互身份验证，可以使密钥管理器使用基于 SSL 的 KMIP 与集群进行通信。如果某个应用程序或某些功能（例如存储加密功能）需要使用安全密钥来提供安全数据访问，则可以执行此操作。

为集群生成证书签名请求

您可以使用安全证书 `generate-csr` 用于生成证书签名请求(CSR)的命令。处理请求后，证书颁发机构（CA）会向您发送签名数字证书。

您需要的内容

要执行此任务，您必须是集群管理员或 SVM 管理员。

步骤

1. 生成 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
```

有关完整的命令语法，请参见手册页。

以下命令将使用 SHA256 哈希函数生成的 2,048 位专用密钥创建一个 CSR，以供自定义公用名为 `server1.companyname.com` 的公司 IT 部门的软件组使用，该公司位于美国加利福尼亚州的森尼韦尔。SVM 联系管理员的电子邮件地址为 `web@example.com`。系统将在输出中显示 CSR 和私钥。

```

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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxtAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+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. 复制 CSR 输出中的证书请求，然后以电子形式（如电子邮件）将其发送到可信的第三方 CA 进行签名。

处理完您的请求后，CA 会向您发送已签名的数字证书。您应保留一份私钥和 CA 签名数字证书的副本。

为集群安装 CA 签名的服务器证书

要使 SSL 服务器能够将集群或 Storage Virtual Machine（SVM）作为 SSL 客户端进行身份验证，您需要在集群或 SVM 上安装客户端类型的数字证书。然后，将 client-ca 证书提供给 SSL 服务器管理员，以便在服务器上安装。

您需要的内容

您必须已使用在集群或 SVM 上安装 SSL 服务器的根证书 server-ca 证书类型。

步骤

1. 要使用自签名数字证书进行客户端身份验证、请使用 `security certificate create` 命令 `type client` 参数。
2. 要使用 CA 签名的数字证书进行客户端身份验证，请完成以下步骤：

- a. 使用安全证书生成数字证书签名请求(CSR) `generate-csr` 命令：

ONTAP 将显示 CSR 输出，其中包括证书请求和私钥，并提醒您将输出复制到文件中以供将来参考。

- b. 以电子形式（如电子邮件）将 CSR 输出中的证书请求发送到可信 CA 进行签名。

您应保留一份私钥和 CA 签名证书的副本，以供日后参考。

处理完您的请求后，CA 会向您发送已签名的数字证书。

- a. 使用安装CA签名证书 `security certificate install` 命令 `-type client` 参数。
- b. 出现提示时，输入证书和私钥，然后按 * 输入 *。
- c. 出现提示时，输入任何其他根证书或中间证书，然后按 * 输入 *。

如果某个证书链从可信根 CA 开始，并以向您颁发的 SSL 证书结束，但缺少中间证书，则您需要在集群或 SVM 上安装中间证书。中间证书是由受信任根专门为问题描述最终实体服务器证书颁发的从属证书。结果是证书链，该证书链从可信根 CA 开始，经过中间证书，并以向您颁发的 SSL 证书结束。

3. 提供 `client-ca` 将集群或SVM的证书发给SSL服务器的管理员、以便在服务器上安装。

带有的 `security certificate show` 命令 `-instance` 和 `-type client-ca` 参数显示 `client-ca` 证书信息。

为 KMIP 服务器安装 CA 签名的客户端证书

密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）的证书子类型（`-subtype kmip-cert` 参数）以及 `client` 和 `server-ca` 类型指定使用此证书对集群和外部密钥管理器（例如 KMIP 服务器）进行相互身份验证。

关于此任务

安装 KMIP 证书以将 KMIP 服务器作为 SSL 服务器向集群进行身份验证。

步骤

1. 使用 `security certificate install` 命令 `-type server-ca` 和 `-subtype kmip-cert` 用于为KMIP服务器安装KMIP证书的参数。
2. 出现提示时，输入证书，然后按 Enter 键。

ONTAP 会提醒您保留一份证书副本，以供日后参考。

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

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIICPDCCAAUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZyB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

...

-----END CERTIFICATE-----

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

```
cluster1::>
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。