安装FXOS机箱管理器的受信任证书

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 生成CSR
- 导入证书颁发机构证书链
- 导入服务器的签名身份证书
- 配置机箱管理器以使用新证书

验证

故障排除

相关信息

简介

本文档介绍如何生成CSR并安装身份证书，以便在FP 4100/9300系列设备上与FXOS机箱管理器配合使用。

先决条件

要求

Cisco 建议您了解以下主题：

- 从命令行配置Firepower可扩展操作系统(FXOS)
- 使用证书签名请求(CSR)
- 私钥基础设施(PKI)概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower(FP)4100和9300系列硬件
- FXOS版本2.10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

初始配置后，将生成自签名SSL证书，用于机箱管理器Web应用。因为该证书是自签名证书，所以客户端浏览器不会自动信任该证书。当新客户端浏览器首次访问机箱管理器Web界面时，浏览器会抛出与您的连接类似的SSL警告，说明该连接不是专用的，并要求用户在访问机箱管理器之前接受证书。此过程允许安装由受信任证书颁发机构签名的证书，这允许客户端浏览器信任连接，并在没有警告的情况下打开Web界面。

配置

生成 CSR

执行以下步骤以获取包含设备（允许客户端浏览器正确识别服务器）的IP地址或完全限定域名(FQDN)的证书：

- 创建密钥环并选择私钥的模数大小。

注意：密钥环名称可以是任何输入。在这些示例中，使用firepower_cert。

本示例创建密钥大小为1024位的密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
```

- 配置CSR字段CSR可以只使用基本选项（如主题名称）生成。这也会提示输入证书请求密码。

本示例创建并显示一个证书请求，该请求包含用于密钥环的IPv4地址，并具有基本选项：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04Certificate r
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
```

- 也可以使用更高级的选项生成CSR，这些选项允许将区域设置和组织等信息嵌入到证书中。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* #  set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
```

- 导出CSR以提供给您的证书颁发机构。复制以(and includes)开头(BEGIN CERTIFICATE REQUEST)-----以(and includes)结-----(and includes)结尾的输出-----END CERTIFICATE REQUEST-----。

```
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
Ore/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/OOKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```

导入证书颁发机构证书链



注意：所有证书必须采用Base64格式才能导入FXOS。如果从证书颁发机构收到的证书或证书链采用不同的格式，则必须首先使用SSL工具（如OpenSSL）对其进行转换。

- 创建新的信任点以保存证书链。



注意：信任点名称可以是任何输入。示例中使用firepower_chain。

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl9O3O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0QOGCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc4OwhuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```



注意：对于使用中间证书的证书颁发机构，必须组合根证书和中间证书。在文本文件中，将根证书粘贴在顶部，然后粘贴链中的每个中间证书（包括所有BEGIN CERTIFICATE和END CERTIFICATE标志）。 然后，在ENDOFBUF描述之前粘贴整个文件。

导入服务器的签名身份证书

- 将上一步中创建的信任点与为CSR创建的密钥环相关联。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
```

- 粘贴证书颁发机构提供的身份证书的内容。

```
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq > hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcG
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6 > mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7
Firepower-chassis /security/keyring* # commit-buffer
```

配置机箱管理器以使用新证书

证书现已安装，但尚未将Web服务配置为使用它。

```
Firepower-chassis# scope system Firepower-chassis /system # scope services Firepower-chassis /system/se
Firepower-chassis /system/services* # commit-buffer
```

验证

使用本部分可确认配置能否正常运行。

- show https — 输出显示与HTTPS服务器关联的密钥环。它可反映前面提到的步骤中创建的名称。如果仍然显示默认值，则未将其更新为使用新证书。

<#root>

```
Firepower-chassis /system/services #

show https

 Name: https Admin State: Enabled Port: 443 Operational port: 443 Key Ring: kring7984 Cipher suite mode
```

- show keyring <keyring_name> detail — 输出显示导入的证书的内容，并显示证书是否有效。

<#root>

```
fp4120 /security #

scope security

fp4120 /security #

show keyring

kring7984

 detail

 Keyring kring7984: RSA key modulus: Mod2048 Trustpoint CA: tPoint10

Certificate status: Valid

 Certificate: Data: Version: 3 (0x2) Serial Number: 45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:

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

MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBg

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

 Zeroized: No
```

- 在Web浏览器的地址栏中输入https://<FQDN_or_IP>/，浏览到Firepower 机箱管理器，并验证是否显示新的受信任证书。

警告：浏览器还会根据地址栏中的输入验证证书的使用者名称，因此，如果向完全限定域名颁发证书，则必须在浏览器中通过这种方式访问证书。如果通过IP地址访问它，则即使使用受信任证书，也会引发其他SSL错误（公用名无效）。

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- 访问FXOS CLI
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。