导入SSL证书到NAC性能分析器

目录

简介

仿形铣床系统基于Web的UI能使用数字证书，以便嵌入式Web服务器的真实性在Cisco NAC Profiler服务器的可以由浏览器验证，当为对HTTPS服务的仿形铣床用户界面的访问连接。系统有效利用其中一Web浏览器验证PKI和数字证书的最普通的应用程序SSL Web服务器是地道的，以便用户感到安全他们的交互作用用Web服务器是，实际上，委托和他们的通信与它安全。这是使用巩固电子商务和其他安全通信的今天与许多类型网站使用SSL的同一机制。

仿形铣床系统装备允许访问对UI，但是没有内置SSL Web服务器验证作为委托的“自己签署的”数字证书。直到默认证书用一个替换创建与环境特定属性，例如服务器名和由Certificate Authority (CA)签字，访问仿形铣床UI显示警告类似于此示例，表明的Web浏览器浏览器不认可发出证书并且无法的CA验证它作为可信的站点。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 美洲台服务器

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

主要主要任务：安装证书

多数浏览器要求用户提供另外的输入继续连接，可以是麻烦的。

为了为仿形铣床接口的SSL安全完全利用强化的安全买得起使用数字证书，必须做对NP的SSL子系统配置的变动。默认情况下由系统使用与委托发出的那些认证机关，并且是特定对安装的那些更改要求专用密钥和数字证书更换。在此步骤以后，浏览器启动一HTTPS会话用服务器并且立即把用户带对UI登录过程绕过证书警告。

两个选项

有此的两个选择在NP系统：

1. 使用Openssl工具套件居民在设备生成在NP的服务器系统和被使用的PCs可以安装通过Web UI管理系统的签名证书。

此选项可以用于在商业CA供应商当前没有内部CA并且选择不取决于收取一成本提供一签字的数字证书由多数商业浏览器自动地认可的环境。

2. 请使用Openssl工具套件生成提交对一内部或外部商务CA服务，归还一立即可用的NP系统的一证书签名请求，签字的数字证书为在系统的使用。

它典型地是组织的内部安全策略的问题仿形铣床系统安装做确定选项使用在一个特定环境。两个选项的更多的指导信息在本文档的剩余部分提供。

选项 1：请使用在Beacon/NPS的Openssl工具套件生成符号

在开始略述的步骤之前，验证是重要的仿形铣床系统适当地配置使用企业名称服务，并且DNS条目被做这样系统有完全合格的域名(FQDN)。为了验证这是实际情形，请保证您能开始一UI会话用有一旦HA系统的系统(即而不是IP地址的https://beacon.bspruce.com/beacon) (或VIP的) FQDN的仿形铣床系统在URL，当您浏览对UI时。

当没有希望提交CSR到签字的时，设备CA此步骤用于案件。此步骤完全允许一签名证书的创建与Openssl工具套件的在设备-什么都不需要提交到另一个系统或商业CA生成仿形铣床系统的一签名证书。

此步骤成功取决于跟随它如指定。命令语法是长和易出错的。保证您是在正确目录在说明上指定，在您执行命令前。必须相等地输入为CA证书和证书签名请求生成的Dns的信息，例如国家、州、城市、服务器名等等，(区分大小写)，因此是肯定做笔记，当您完成步骤保证进程顺利去。

1. 启动SSH或控制台会话到NP设备并且举起对根访问权限。对于HA系统，请保证您是在主系统通过启动SSH对VIP。在第一次使用Openssl之前，必须初始化Openssl使用的某种文件结构。完成这些步骤初始化Openssl ：
2. 更改目录对/etc/pki/CA用此命令：
   ```
   cd /etc/pki/CA/
   ```
   创建呼叫**newcerts的**新目录，并且发出这些命令：
   ```
   mkdir newcerts touch index.txt
   ```

3. 使用vi创建一个新的文件命名了**序列**;插入**01**在文件，并且确认更改。(：wq!)更改此目录：cd /etc/pki/tls/certs
4. 生成系统的一新的专用密钥用此命令：
   ```
   openssl genrsa -out profilerFQDN.key 1024
   ```
   (其中'profilerFQDN'用NP设备的完全限定域名替换，当部署的独立。对于HA系统，必须使用VIP的FQDN)。如果仿形铣床系统不在DNS，服务器(VIP)的IP地址可以使用而不是FQDN，但是证书附加对此IP地址，即要求使用在URL (避免证书警告的https://10.10.0.1/profiler)的IP。
5. 生成CA证书使用生成与此命令，创建一个3个年CA证书和在步骤生成的密钥的服务器证书#4：
   ```
   openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem
   ```
   提示对于合并到证书请求和一个特有名(DN)形成里CA证书的几个属性。对于一些此这些项目，默认值是建议的(在[])。输入DN的每个参数的所需的值或''。为了跳过项目，请务必记录下来用于此步骤的DN参数。他们一定是相同的与在证书签名请求的生成指定的那些服务器证书的在步骤#7。移动在最后一步创建的CA证书对需要的目录：
   ```
   mv cacert.pem /etc/pki/CA
   ```
   生成仿形铣床系统的一证书签名请求有新的专用密钥的：
   ```
   openssl req -new -key profilerFQDN.key -out profilerFQDN.csr
   ```
6. 正在步骤#5，提示您完成系统的DN服务器CSR的。保证您使用使用CA证书在步骤#5的同样值服务器CSR。如果有在参数上的任何变化， CSR没有顺利地创建。另外，提示您创建证书的一密码短语。请务必记录下来密码短语。
7. 生成与在上一个步骤和专用密钥的服务器证书生成的CSR。此步骤输出是在仿形铣床服务器的签名证书(或服务器安装，一旦HA对)。
   ```
   openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key
   ```
   提示您签署和做证书。输入**y**确认签署和做证书完成服务器证书生成。
8. 搬到证书文件内部安全策略指定的位置(如果适用)或请使用默认位置：如果位置没有由内部安全策略，指定在/etc/pki/tls/certs/必须安置证书。
   ```
   mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
   ```
9. 搬到专用密钥文件内部安全策略指定的位置(如果适用)或请使用默认位置：如果位置没有由内部安全策略，指定在/etc/pki/tls/private/必须安置专用密钥。使用下列命令：
   ```
   mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
   ```
10. 编辑**ssl.conf文件**用一台编辑器例如vi做必要的更改强制仿形铣床Web服务器使用新的专用密钥和证书(ssl.conf在/etc/httpd/conf.d/被找到)。在**ssl.conf中，**服务器证书部分在线路107开始。更改从出厂默认设置(/etc/pki/tls/certs/localhost.cert)的SSLCertificateFile配置项指向在步骤#8的系统创建的新证书文件。在**ssl.conf中，**服务器专用密钥部分在线路114开始。更改从出厂默认设置(等/私有pki/的tls//localhost.key)的服务器专用密钥配置项指向在系统安置的新的专用密钥文件在步骤#9。
11. 重新启动在设备的Apache Web服务器用此命令：
    ```
    apachectl -k restart
    ```
    注意： 如果系统是部署的独立，请跳过跨步#13。
12. 对于HA仅NP系统，请完成这些步骤安装专用密钥和CRT在另一个成员(当前第二) HA对。这保证，设备是主要的在对， UI的SSL安全机制相等地运行。a. 复制在步骤#3的主要的设备生成的专用密钥对附属设备。如果位置没有由内部安全策略，指定在/etc/pki/tls/private/必须安置专用密钥。请使用此命令(从在主要的/etc/pki/tls/private目录) ：
    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```
    复制从从主要的CA返回到附属设备的签字的CRT。如果位置没有由内部安全策略，指定在/etc/pki/tls/certs/必须安置证书。
    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```
    对附属设备的SSH和编辑其**ssl.conf文件**用一台编辑器例如vi做必要的更改强制在第二的Web服务器使用新的专用密钥和证书(ssl.conf在/etc/httpd/conf.d/被找到)在**ssl.conf中，**服务器证书部分在线路107开始。更改从出厂默认设置(/etc/pki/tls/certs/localhost.cert)的

SSLCertificateFile配置项指向在系统安置的新证书文件在步骤#11b。在**ssl.conf中，**服务器专用密钥部分在线路114开始。更改从出厂默认设置(等/私有pki/的tls//localhost.key)的服务器专用密钥配置项指向在系统安置的新的专用密钥文件在步骤#11a。重新启动在附属设备的Apache Web服务器用此命令：

```
apachectl -k restart
```

由于创建与这些步骤的服务器证书使用私有CA，访问仿形铣床UI的浏览器必须配置安装在可信的根认证机关信息库的证书在与IE 7.0的Windows PCs。执行下列步骤：复制已创建服务器证书对设备的/home/beacon目录：

```
cp profilerFQDN.crt /home/beacon
```

请使用WinSCP或一可比较的软件对SCP从设备的.crt文件到PC。双击**.crt文件**开始Windows认证管理器，并且点击**安装证书**，启动证书导入向导。选择**单选按钮**。在此存储安置所有证书激活**浏览按钮**。选择**浏览**，并且点击**可靠的根证书颁发机构**证书存储。点击OK键接受此证书。重复在用于管理仿形铣床系统的另一PCs的此进程。

13. 访问仿形铣床UI并且注意HTTPS会话开始没有浏览器生成的证书警告。

选项 2：生成/提交CSR对内部/外部CA

在您开始其次前略述的步骤，验证是重要的仿形铣床系统适当地配置使用企业名称服务，并且DNS条目被做这样系统有完全合格的域名(FQDN)。为了验证这是实际情形，请保证您能开始一UI会话用有一旦HA系统的系统(即而不是IP地址的https://beacon.bspruce.com/beacon)或VIP的FQDN的仿形铣床系统。

完成这些步骤生成系统的一新的专用密钥，生成CSR为内部或外部CA供槁，然后放置有效签名证书在NP ：

1. 启动SSH或控制台会话到NP设备，并且举起它对根访问权限。HA系统，对保证的VIP的启动SSH您是在主系统。
2. 去NP的默认PKI目录：

   ```
   cd /etc/pki/tls
   ```

3. 请使用此命令生成system:的一个新的专用密钥文件

   ```
   openssl genrsa ?des3 ?out profilerFQDN.key 1024
   ```

   那里‘profilerFQDN’用NP设备的完全限定域名替换，当部署的独立。对于HA系统，必须使用VIP的FQDN)。提示您输入和确认密码短语完成专用密钥的生成。使用专用密钥，此密码短语为将来操作要求。请务必记录下来用于专用密钥生成的密码短语。
4. 当专用密钥生成在最后一步，请生成证书签名请求(CSR)发送对证书(CRT)的生成的Certificate Authority (CA)此系统的。

   请使用此命令生成CSR

   ```
   openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr
   ```

   (用‘profilerFQDN’请替代系统的完全限定域名。)当您创建系统的时， CSR提示对于专用密钥的密码短语;输入它继续。然后提示对于合并到证书请求和特有名(DN)的形成里的几个属性。对于一些此这些项目，默认值是建议的(在[])。输入DN的每个参数的所需的值或‘’。跳过项目。
5. 验证CSR的内容用此命令：

   ```
   openssl req -noout -text -in profilerFQDN.csr
   ```

   (用‘profilerFQDN’请替代系统的完全限定域名。)在最后一步被输入的这返回关于CSR的信息和DN。如果在CSR的任何信息需要更改，请重复步骤#4全文
6. 提交CSR对选定的Certificate Authority (CA)符合内政。如果请求是成功的， CA退还数字式地签了字与CA的专用密钥的身份证书。当这您的选定的CA签字的新建的CRT用于替换在仿形铣床系统时的出厂默认设置CRT，访问仿形铣床UI的所有浏览器能验证站点的标识和在浏览器的警告消息被看到在对Web服务器的连接在NP服务器在用户认证之前不再显示为，只要CRT保

持有效。(这假设，浏览器有CA被添加到其可信的根证书权限。)

7. 从属在使用的CA，可能其他信息需要与CSR一起提交，例如或身份证明要求的其他凭证认证机关，和认证机关能欲知详情与申请人联系。一旦数字式地签字的CRT从CA回来，请继续进行下一步用在上面步骤创建的那些替换出厂专用密钥和证书。对于HA系统，同一个步骤使用安装专用密钥和证书在附属设备在对。
8. 搬到证书和专用密钥文件内部安全策略指定的位置，如果适用或者请使用默认位置：如果位置没有由内部安全策略，指定在/etc/pki/tls/private/必须安置专用密钥。使用以下命令：
   ```
   mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
   ```
   如果位置没有由内部安全策略，指定在/etc/pki/tls/certs/必须安置证书。
   ```
   mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
   ```
9. 编辑**ssl.conf文件**用一台编辑器例如维托做必要的更改强制Web服务器使用新的专用密钥和证书(ssl.conf在/etc/httpd/conf.d/被找到)。在**ssl.conf中，**服务器证书部分在线路107开始。更改从出厂默认设置(/etc/pki/tls/certs/localhost.cert)的SSLCertificateFile配置项指向在系统安置的新证书文件在步骤#8.b。在**ssl.conf中，**服务器专用密钥部分在线路114开始。更改从出厂默认设置(等/私有pki/的tls//localhost.key)的服务器专用密钥配置项指向在系统安置的新的专用密钥文件在步骤#8.a。
10. 重新启动在设备的Apache Web服务器用此命令：
    ```
    apachectl -k restart
    ```
    注意： 如果系统是部署的独立，请跳过跨步#12。
11. 对于HA仅NP系统，请完成这些步骤安装专用密钥和CRT在另一个成员(当前第二) HA对。这保证，设备是主要的在对， UI的SSL安全机制相等地运行。复制在步骤#3的主要的设备生成的专用密钥对附属设备。如果位置没有由内部安全策略，指定在/etc/pki/tls/private/必须安置专用密钥。请使用此命令(从在主要的/etc/pki/tls/private目录) ：
    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```
    .。复制从从主要的CA返回的签字的CRT到附属设备。如果位置没有由内部安全策略，指定在/etc/pki/tls/certs/必须安置证书。
    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```
    对附属设备的SSH和编辑其ssl.conf文件用一台编辑器例如vi做必要的更改强制在第二的Web服务器使用新的专用密钥和证书(ssl.conf在/etc/httpd/conf.d/被找到)。在**ssl.conf中，**服务器证书部分在线路107开始。更改从出厂默认设置(/etc/pki/tls/certs/localhost.cert)的SSLCertificateFile配置项指向在系统安置的新证书文件在步骤#11.b。在**ssl.conf中，**服务器专用密钥部分在线路114开始。更改从出厂默认设置(等/私有pki/的tls//localhost.key)的服务器专用密钥配置项指向在系统安置的新的专用密钥文件在步骤#11.a。重新启动在附属设备的Apache Web服务器用此命令：
    ```
    apachectl -k restart
    ```
12. 访问仿形铣床UI并且注意HTTPS会话开始，不用浏览器生成的证书警告。如果警告仍然存在，请验证使用的浏览器有发出的CA被添加到其可信的根证书权限。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco NAC Appliance (Clean Access)产品网页
- 技术支持和文档 - Cisco Systems