目录

简介

本文通过正确调整PKI事件计时器配置描述与大规模Cisco IOS证书服务器公共密钥基础设施(PKI)部署的一故障情况和其潜在的缓解。

问题

用户症状

此问题在Cisco IOS注册机关(RA)配置服务数百和有时千位PKI客户端设备的一个大规模PKI环境能被看到。当此特定的失败发生时，从PKI客户端的证书登记也许间歇地或一致发生故障。

在PKI客户端很可能这些日志消息也许被看到：

在您启用这些PKI调试后：

被看到客户端要求Certificate Authority (CA)服务器反转证书，反而收到从CA服务器的一“HTTP 404 Not Found”错误消息。

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message
```

```
Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

注意：此问题不是RA特定，并且能也发生，当没有使用时RA (仅CA)。

排除故障和问题识别

在失败里观察的其中一关键症状是有来自PKI客户端在RA的很多PKI请求。这能在Netflow或数据包捕获输出看到。相当数量PKI请求能淹没服务器，以便不能响应足够迅速。一种方式验证此情况将远程登录到在侦听的HTTP端口的CA服务器。当服务在端口侦听并且回应时，您应该看到开放的连接。在故障状态，表明的telnet尝试计时TCP没有均等完成三通的握手。

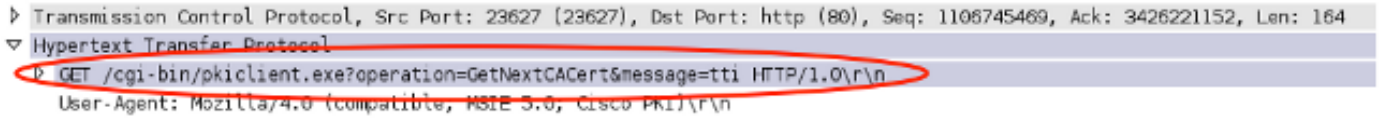
为了改善请知道TCP为什么发生故障，输入**debug ip tcp transactions地址<tcp_peer_address>** on命令服务器为了了解到TCP服务器的处理流到特定TCP源地址(指定地址过滤器是重要的，当您调试一个大规模环境)时。在故障状态，这些调试被观察：

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
```

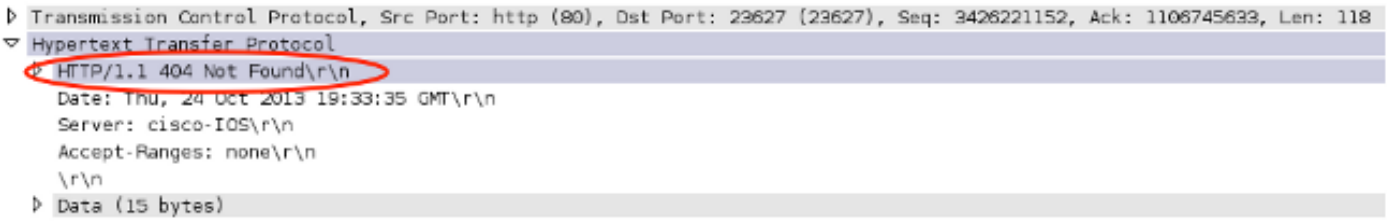
```
Host: 192.168.105.3


Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

提示： 在版本15.1和15.2 **debug ip tcp transactions命令没**有对此的地址选项。在此命令位置，如果连接队列限制达到，请输入**debug ip tcp packet地址<tcp_peer_address**为了也显示。

PKI请求的一数据包捕获可也帮助暴露关于什么的其他信息这些PKI请求是。从数据包捕获，您能看到请求大量类似于：



对于服务器能实际上回应的其中一些请求，您也看到"404不查找”答复：



根本原因

有造成此特定问题的一些个要素。首先， GetNextCACert显示这些PKI请求是从客户端的反转请求请求为反转/Shadow CA证书。欲了解更详细的信息在CA反转操作，请参阅IOS PKI自动注册、自动反转和计时器。"404没被找到的”答复表明RA/CA服务器也许没在请求时有Shadow证书。这可以验证与**显示crypto pki**在CA和RA服务器的**certificate命令**输出。问题归结于在PKI服务器和客户端找到的此证书计时器配置：

RA/CA服务器

```
CA-Server#show running | section pki server
crypto pki server ca-server
<snip>
```

```
lifetime certificate 600
lifetime ca-certificate 1825
auto-rolloverCA-Server#show crypto pki server | include Rollover
Auto-Rollover configured, overlap period 30 days
CA-Server#
```

PKI客户端

```
crypto pki trustpoint test enroll url http://enrollment_url.test.com:80
enrollment mode ra subject-name OU = TEST OU, OU = cisco auto-enroll 70
```

问题是CA证书正确性时候配置是5年(1825天)，但是反转/Shadow证书在直到30天的CA服务器不得到创建在当前证书终止之前。路由器证书有600天正确性时间，并且基于自动注册配置，路由器可能在70% 600天寿命以后请求反转/Shadow证书。这能是早在180天在当前CA证书有效期前。这些PKI事件的时期和说明的一个详细的计算，再参考的IOS PKI自动注册、自动反转和计时器。 这解释客户端为什么继续要求CA反转/Shadow，并且继续收到"404没被找到的”错误，因为他们在服务器没有创建。此情况仍然存在，直到CA反转/Shadow证书生成。

同时，由于进入RA服务器的很多请求， Cisco IOS RA服务器可以超出此HTTP连接阈值和开始下降传入的HTTP连接请求：

- 最大数量HTTP并发服务器连接限制。这可以更改到最多16个并发连接用**ip http max-connections 16**命令。
- 80连接内部HTTP服务器连接速度限制每分钟。当此阈值达到时， theCiscoIOS HTTP服务器节流孔返回和侦听新建的HTTP请求的终止15秒。目前，此速率限制阈值不是可配置的用户。结果， theTCP “连接队列限制被到达的”错误在theTCP处理调试看到。

> **注意**：目前上述阈值不可能用Cisco IOS命令监控。增强请求打开改进此，参见Cisco Bug ID CSCuj83430。

解决方案

对此问题的解决方案将更正在CA服务器的PKI事件计时器配置这样反转/Shadow证书在所有PKI客户端反转请求之前生成。这可以执行与这些步骤：

1. 输入**shutdown命令**在crypto pki server command.in命令禁用CA服务器下。
2. 增加根据证书寿命和重新注册配置的反转重叠时间：

```
CA-Server(config)#crypto pki server ca-server
CA-Server(cs-server)#auto-rollover ?
<0-1825> Overlap time between CA certificates during rollover, in days
<cr>
CA-Server(cs-server)#auto-rollover 365
```

3. 重新授权给CA服务器。
4. 如果有anRA，手工获取反转/Shadow证书的反转theRA。

> **提示**：为了手工强制CA到反转，无需启用自动反转，请输入**crypto pki server <server name>反转**命令。

并且，如以前讨论，推荐增加HTTP最大并发连接限制到16为了服务器能处理一高流入连接速率。