对从Cisco IOS CA收到的404个错误进行故障排除以进行大规模部署

目录

简介

本文档介绍大规模Cisco IOS®证书服务器公共密钥基础设施(PKI)部署的故障情况，以及通过正确调整PKI事件计时器配置来缓解其潜在问题。

问题

用户症状

在大型PKI环境中，Cisco IOS注册机构(RA)配置为为数百甚至数千台PKI客户端设备提供服务，就可以看到此问题。当出现此特定故障时，来自PKI客户端的证书注册可能会间歇性或一致性失败。

在PKI客户端上，可能会看到以下日志消息：

```
*Dec 30 15:37:46.996: CRYPTO_PKI: Socket timeout
*Dec 30 15:40:47.929: %PKI-3-SOCKETSEND: Failed to send out message to CA server.
```

启用以下PKI调试后：

```
debug crypto pki message
debug crypto pki validation
```

发现客户端请求证书颁发机构(CA)服务器全反证书，但从CA服务器接收“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：此问题不特定于RA，并且当未使用RA时（仅限CA）也可能发生。

故障排除和问题识别

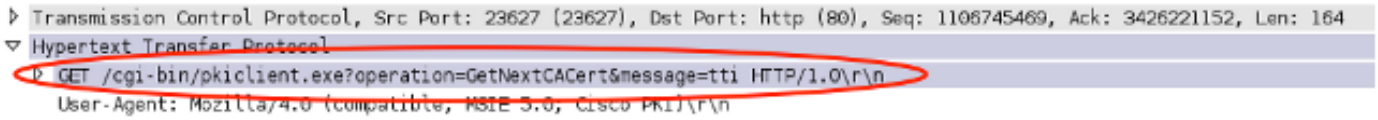
故障中观察到的一个关键症状是RA上有许多来自PKI客户端的PKI请求。NetFlow或数据包捕获输出都可以看到这一点。PKI请求的数量可能会使服务器不堪重负，使其无法足够快地响应。验证此情况的一种方法是通过telnet连接到它正在侦听的HTTP端口上的CA服务器。当服务在端口上侦听并响应时，您应该看到连接打开。在失败状态下，telnet尝试超时，表明TCP甚至无法完成三次握手。

为了更好地了解TCP失败的原因，请在服务器上输入**debug ip tcp transactions address <tcp_peer_address>**命令，以便了解服务器对特定TCP源地址的TCP流的处理（在调试大规模环境时指定地址过滤器非常重要）。 在失败状态下，会观察到以下调试：

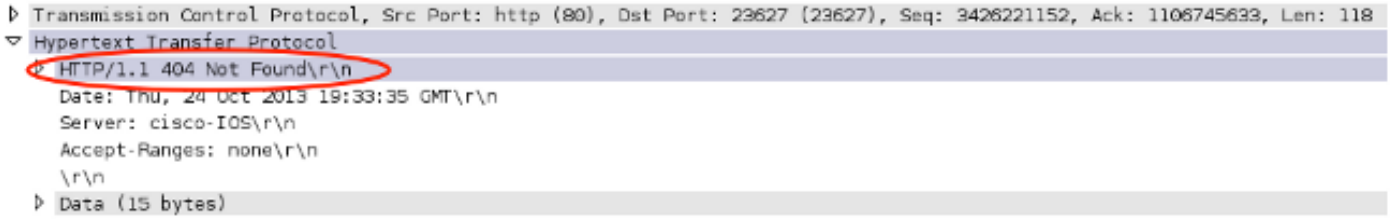
```
TCP0: bad seg from x.x.x.x -- connection queue limit reached:
port 80 seq 1276472961 ack 0 rcvnxt 0 rcvwnd 4128 len 0
TCP0: bad seg from x.x.x.x -- connection queue limit reached:
port 80 seq 1276472961 ack 0 rcvnxt 0 rcvwnd 4128 len 0
TCP0: bad seg from x.x.x.x -- connection queue limit reached:
port 80 seq 1276472961 ack 0 rcvnxt 0 rcvwnd 4128 len 0
```

提示：在版本15.1和15.2中，**debug ip tcp transactions命**令没有地址选项。替换此命令，输入**debug ip tcp packet address <tcp_peer_address**，以便同时显示是否达到连接队列限制。

PKI请求的数据包捕获也有助于揭示有关这些PKI请求的其他信息。从数据包捕获中，您可以看到大量请求，类似于：



对于服务器实际可以响应的其中一些请求，您还会看到“404未找到”响应：



根本原因

造成这一特定问题的因素有几个。首先，GetNextCACert显示这些PKI请求是来自客户端的滚动请求，以请求滚动/影子CA证书。有关CA全反操作的详细信息，请参阅IOS PKI Auto-Enroll、Auto-Rollover和Timers。“404 Not Found”响应表示RA/CA服务器在请求时可能没有影子证书。这可以通过CA和RA服**务器上的**show crypto pki certificate命令输出进行验证。问题是由于在PKI服务器和客户端上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-rollover

CA-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证书有效期配置为5年（1825天），但直到当前证书到期前30天，才会在CA服务器上创建滚动/影子证书。路由器证书的有效期为600天，根据自动注册配置，路由器可以在600天的有效期中70%后请求滚动/影子证书。这最早可能比当前CA证书过期时间早180天。有关这些时间的详细计算和PKI事件的说明，请再次参阅IOS PKI自动注册、自动滚动和计时器。这解释了为什么客户端继续请求CA滚动/阴影，并继续接收“404未找到”错误，因为这些错误尚未在服务器上创建。此情况持续存在，直到生成CA全反/影子证书。

同时，由于大量请求进入RA服务器，Cisco IOS RA服务器可能会超过此HTTP连接阈值并开始丢弃传入的HTTP连接请求：

- 最大HTTP并发服务器连接数限制。使用ip http max-connections 16命令，此连接最多可以更**改为16个并发连**接。
- 内部HTTP服务器连接速率限制为每分钟80次连接。达到此阈值后，CiscoIOS HTTP服务器将阻止并停止侦听新的HTTP请求15秒。目前，此速率限制阈值不可用户配置。因此，在TCP事务调试中出现TCP“连接队列限制已达”错误。

> **注意**：目前，无法使用Cisco IOS命令监控上述阈值。已打开增强请求以改进此，请参阅Cisco Bug ID CSCuj83430。

解决方案

此问题的解决方案是更正CA服务器上的PKI事件计时器配置，以便在任何PKI客户端滚动请求之前生成滚动/影子证书。这可通过以下步骤完成：

1. 在crypto PKI server命令下输入**shutdown**命令，以禁用CA服务器。
2. 根据证书有效期和重新注册配置延长滚动重叠时间：

```
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. 重新启用CA服务器。
4. 如果有RA，请手动将RA回滚以检索滚动/阴影证书。

> **提示**：要强制CA手动滚动而不启用自动滚动，请输入**crypto pki server <server-name> rollover**命令。

此外，如前所述，建议将HTTP最大并发连接限制增加到16，以便服务器处理高传入连接速率。