目次

この資料は正しく PKI イベント タイマーのコンフィギュレーションを調整することによって大規模 Cisco IOS ® 認証サーバ 公開鍵インフラストラクチャ （PKI）配備および潜在的な軽減を用いる障害状況を記述したものです。

問題

ユーザ現象

この問題は何百および時々桁をもの PKI クライアントデバイス保守するために Cisco IOS Registration Authority （RA）が設定される大規模 な PKI 環境で見られる場合があります。 この特定の失敗が発生するとき、PKI クライアントからの証明書登録は断続的にまたは一貫して失敗するかもしれません。

PKI クライアントでこれらの口グメッセージが見られるかもしれません可能性が高いといえます:

これらの PKI デバッグを有効に した後:

Client 要求が CA サーバから認証局 （CA） サーバ ロールオーバー 認証、代りに「HTTP 404 Not Found」エラーメッセージを受け取るがことが見られます。

```
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 この問題は RA が使用されないとき RA 仕様でし、また起こる場合があります (CA だけ) 。

問題識別解決すれば

失敗で観察されるキー現象の 1 つは PKI クライアントから来る RA に多くの PKI 要求があることです。 これは NetFlow またはパケットキャプチャ出力と見られる場合があります。 PKI 要求の量は十分にすぐに応答できないようにサーバを圧倒できます。 この条件を確認する 1 つの方法は HTTPポートの CA サーバに telnet にを受信していることです。 サービスがポートで受信し、対応されているとき、開いた接続を見るはずです。 FAILED 状態では、示す telnet TCP は三方ハンドシェイクを終えないことを試みは時間を計ります。

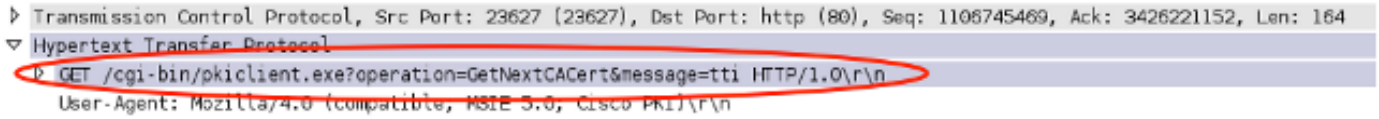
大規模 な 環境をデバッグするとき) よりよく TCP がなぜ失敗するか理解するために、サーバの特定の TCP 送信元アドレス (への TCP フローの処理に把握を規定 することは重要アドレスフィルタをです入力して下さい得るためにサーバの **debug ip tcp transactions アドレス <tcp_peer_address>** コマンドを。 FAILED 状態では、これらのデバッグは観察されます:

```
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
```

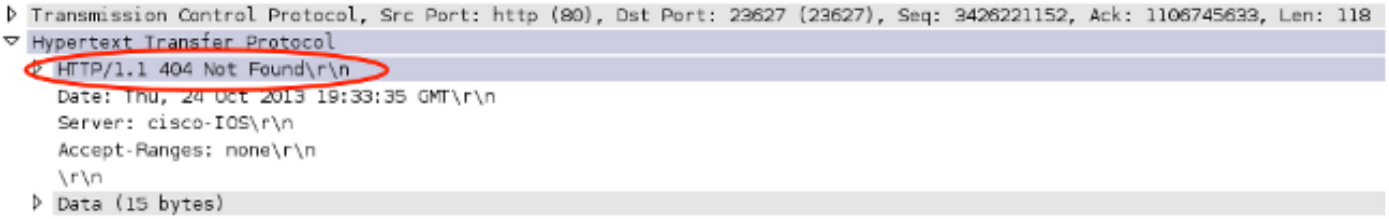
```
Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

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
```

> **ヒント**：バージョン 15.1 および 15.2 で **debug ip tcp transactions コマンドに**それのアドレスオプションがありません。 このコマンドの代わりに、接続キュー制限が達するかどうか示すためにまた **debug ip tcp packet アドレス <tcp_peer_address を**入力して下さい。

PKI 要求のためのパケットキャプチャはまた明らかにするのをこれらの PKI 要求がであるものについてのその他の情報を助けることができます。 パケットキャプチャから、に類似した 要求の大きな 番号を次のように表示できます:



いくつかのこれらの要求のためにサーバが実際にに応答できることまた "404 が」応答を見つけないのを見ます:



根本的原因

この特定の問題に貢献する少数のファクタがあります。 最初に、GetNextCACert はこれらの PKI 要求がロールオーバー/シャドウ CA 認証のために要求するクライアントからのロールオーバー 要

求であることを示します。 詳細については CA ロールオーバー オペレーションで、IOS PKI およびタイマーが、自動ロールオーバー自動登録するのを参照して下さい。 "404 見つけられなかった」応答は RA/CA サーバは要求の時にシャドウ 認証がないかもしれませんことを示します。 これは CA および RA サーバの**提示暗号 PKI certificate コマンド**出力と確認することができます。 問題は PKI サーバおよびクライアントで見つけられるこの認証 タイマーのコンフィギュレーションが原因です:

RA/CA サーバ

```
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 クライアント

```
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
```

問題は CA 認証有効性時間が 5 年（1825 日）であるために設定されるがロールオーバー/シャドウ 認証は現在の認証終止前の 30 日までの CA サーバで作成されませんことです。 ルータ認証は 600 日有効性時間があり、自動登録設定に基づいて、ルータは 600 日ライフタイムの 70% の後でロールオーバー/シャドウ 認証を要求する可能性があります。 これは現在の CA 認証 有効期限の前に 180 日には早くもある可能性があります。 これらの時の詳しい計算および PKI イベントの説明に関しては、再度 IOS PKI を自動登録します、自動ロールオーバーおよびタイマー参照して下さい。 これはサーバでまだ作成されていないのでクライアントが CA ロールオーバー/シャドウをなぜ要求し続ける説明し "404 検出されなかった」エラーをか受け取り続けます。 この条件は CA ロールオーバー/シャドウ 認証が生成されるまで持続します。

その間、RA サーバに入って来る多量の要求が原因で、Cisco IOS RA サーバはこの HTTP接続 しきい値を超過し、着信 HTTP接続 要求を廃棄し始めることができます:

- 最大 HTTP 同時サーバ接続制限。 これは最大 **ip http max-connections 16** コマンドで 16 同時接続に変更することができます。
- 分毎に 80 の接続の内部 HTTPサーバ 接続速度制限。 このしきい値が達するとき、theCiscoIOS HTTPサーバは絞り、15 秒を新しい HTTP 要求を聞き取ることを止めます。 現在、このレートリミット しきい値は設定可能なユーザではないです。 その結果、theTCP「接続キュー制限によって達される」エラーは theTCP トランザクション デバッグと見られます。

> **注** 現在上のしきい値は Cisco IOSコマンドで監視することができません。 機能拡張要求はこれを改善する見ます Cisco バグ ID CSCuj83430 を開きました。

解決策

この問題へのソリューションはロールオーバー/シャドウ 認証があらゆる PKI クライアント ロー

ルオーバー 要求前に生成されることそのような物 CA サーバの PKI イベント タイマーのコンフィギュレーションを訂正することです。 これはこれらのステップとすることができます:

1. CA サーバをディセーブルにする暗号 PKI サーバ command.in 順序の下で **shutdownコマンドを**入力して下さい。
2. 認証 ライフタイムおよび再登録 設定に基づいてロールオーバー オーバーラップ時間を増加して下さい:

```
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. CA サーバを再び有効に して下さい。
4. anRA がある場合、手動で ロールオーバー theRA ロールオーバー/シャドウ 認証を取得する。

> **ヒント**： CA を自動ロールオーバーを有効に しないでロールオーバーに手動で強制するために、**暗号 PKI サーバ <server-name> ロールオーバー** コマンドを入力して下さい。

またサーバが高い着信接続 比率を処理することができるように、以前に説明されている通り、16 への HTTP 最大同時接続制限を高めることを推奨します。