/etc/cron.daily/certwatch script runs following to find out which certificate file httpd uses –

```
# /usr/sbin/httpd -t -DDUMP_CERTS 2>/dev/null | /bin/sort -u
/etc/pki/tls/certs/localhost.crt
```

Here we issue the certwatch command manually to check -

```
root@lcls-dev3 ~]# certwatch /etc/pki/tls/certs/localhost.crt
To: root
Subject: The certificate for lcls-dev3.slac.stanford.edu will expire in 28 days

 ################# SSL Certificate Warning ################

  Certificate for hostname 'lcls-dev3.slac.stanford.edu', in file (or by
nickname):
     /etc/pki/tls/certs/localhost.crt
```

Here we create the new certificate which would expire after one year –

```
[root@lcls-dev3 certs]#  cd /etc/pki/tls/certs
[root@lcls-dev3 certs]# ./make-dummy-cert localhost.crt
[root@lcls-dev3 certs]# ls -lrt
total 1208
-rw-r--r--  1 root root 651075 Apr  7  2010 ca-bundle.trust.crt
-rw-r--r--  1 root root 571442 Apr  7  2010 ca-bundle.crt
-rwxr-xr-x  1 root root    610 May 15 03:00 make-dummy-cert
-rw-r--r--  1 root root   2242 May 15 03:00 Makefile
-rw-------. 1 root root   3254 Jul 13 11:22 localhost.crt
```

This is how we check the newly created certificate’s expiry date –

```
[root@lcls-dev3 certs]# openssl x509 -in ./localhost.crt -enddate -noout
notAfter=Jul 13 18:22:33 2013 GMT
```

+++

Email produced by cron job /etc/cron.daily/certwatch –

```
>  ################# SSL Certificate Warning ################
>
>   Certificate for hostname 'lcls-dev3.slac.stanford.edu', in file (or
> by nickname):
>      /etc/pki/tls/certs/localhost.crt
>
>   The certificate needs to be renewed; this can be done
>   using the 'genkey' program.
>
>   Browsers will not be able to correctly connect to this
>   web site using SSL until the certificate is renewed.
>
```

```
>  ##########################################################
>                                    Generated by certwatch(1)
```

The **certwatch** program is used to issue warning mail when an SSL certificate is about to expire.

The program has two modes of operation: normal mode and quiet mode. In normal mode, the certificate given by the *filename* argument is examined, and a warning email is issued to standard output if the certificate is outside its validity period, or approaching expiry. If the certificate cannot be found, or any errors occur whilst parsing the certificate, the certificate is ignored and no output is produced. In quiet mode, no output is given, but the exit status can still be used.

```
lcls-dev3 # /usr/sbin/httpd -t -DDUMP_CERTS 2>/dev/null | /bin/sort -u

/etc/pki/tls/certs/localhost.crt
```

Test certwatch from command line –

```
[root@lcls-dev3 ~]# certwatch /etc/pki/tls/certs/localhost.crt

To: root
Subject: The certificate for lcls-dev3.slac.stanford.edu will expire in 28 days

 ################# SSL Certificate Warning ################

  Certificate for hostname 'lcls-dev3.slac.stanford.edu', in file (or by nickname):
     /etc/pki/tls/certs/localhost.crt

  The certificate needs to be renewed; this can be done
  using the 'genkey' program.

  Browsers will not be able to correctly connect to this
  web site using SSL until the certificate is renewed.

 ##########################################################
                                  Generated by certwatch(1)

# cd /etc/pki/tls/certs
[root@lcls-dev3 certs]# ./make-dummy-cert localhost.crt
[root@lcls-dev3 certs]# ls -lrt
total 1208
```

```
-rw-r--r--  1 root root 651075 Apr  7  2010 ca-bundle.trust.crt
-rw-r--r--  1 root root 571442 Apr  7  2010 ca-bundle.crt
-rwxr-xr-x  1 root root    610 May 15 03:00 make-dummy-cert
-rw-r--r--  1 root root   2242 May 15 03:00 Makefile
-rw-------. 1 root root   3254 Jul 13 11:22 localhost.crt

[root@lcls-dev3 certs]# certwatch /etc/pki/tls/certs/localhost.crt


[root@lcls-dev3 certs]# openssl x509 -in ./localhost.crt -enddate -noout

notAfter=Jul 13 18:22:33 2013 GMT
```

++

How can I renew my Centos/Apache SSL certificate?

I got this question the other day from a Centos administrator: "*The `certwatch` tool has been sending the me an email warning me that I need to renew the SSL Certificate. What do I do*?"

The email message read like the following (names have been changed):

```
################# SSL Certificate Warning ################

Certificate for hostname 'www.yourlinuxguy.com', in file:
/etc/pki/tls/certs/www.yourlinuxguy.com.cert

The certificate needs to be renewed; this can be done
using the 'genkey' program.

Browsers will not be able to correctly connect to this
web site using SSL until the certificate is renewed.

##########################################################
Generated by certwatch(1)
```

First I want to clarify a couple things. When you run the `genkey` tool, you are actually doing what the name suggests; generating a new key pair (public/private), from which the certificate is formulated. Technically, you are not *renewing* the certificate as the `certwatch` warning message implies, but that's okay (it *is* possible in some situations to "renew" a certificate based on an existing key pair, but that's not important right now). The `genkey` tool makes it so easy and convenient that it is just easier this way. Remember that a certificate is nothing but a public key that is "stamped" with approval by a CA. In this case, the CA is you, too. Not exactly a trusted hierarchy, but there you go…

So to cut to the chase, it's really easy. Here's basically what you need to do: 1.) run the tool, and 2.) validate your SSL settings in your `httpd.conf`.

Run The Tool

At this point, you may or may not want to make a backup of your cert files… This is up to you… You can do that with something like this command (of course, your mileage may vary):

```
cp -av /etc/pki/tls /etc/pki/tls.bak
```

If you just run the `genkey` tool without specifying the certificate lifetime, it defaults to something like 30 days. Let’s try something a little longer; like 4 years. Now just specify your hostname on the command line:

```
genkey --days 1460 www.yourlinuxguy.com
```

…this will launch an interactive tool to do things like generate the random data, make the key pair, and walk you through specifying the content of the certificate (Country, Location, etc.). It will place the new stuff in some default location, and at the end of the process, tell you where it all is. You should take note of the location, but it will likely be what I mentioned above for the backup.

Validate Your SSL Settings

Now, theoretically, you should be able to restart your Apache daemon. However, you might have used custom names or locations for your certificate files in the past, so you might want to check to be sure they match the SSL settings in your Apache config files. Of course it’s hard for me to tell you where those settings are, since it’s so easy to customize Apache; but here’s a good way to find the two most important values:

```
cd /etc/httpd
egrep -R -e "SSLCertificateKeyFile" -e "SSLCertificateFile" *
```

…and that will likely return results from a file called “`ssl.conf`” or something like that. Edit the config file if necessary; just make sure the values match the place that the `genkey` tool placed the new private key and cert file, and you should be good.

Now, you can restart Apache…

```
/etc/init.d/httpd restart
```

…and you’re done!