Apache Server installation

Installation

We’re going to install apache 1.3 + modssl + ipv6 from the packages collection. you can do this directly from the command line with something like:

pkg_add ftp://[hostname]/[path]apache+mod_ssl+ipv6-1.3.31+2.8.19.tbz

You could also build it from the ports by going to:

/usr/ports/www/apache13-modssl+ipv6/

and typing make then make install.

Ok... Where did it go?

pkg_info -L apache+mod_ssl-1.3.31+2.8.19

looks like it’s in **/usr/local/**

the webpages are served from under **/usr/local/www/** the **httpd.conf** is in **/usr/local/etc/apache/** and the startup script is **/usr/local/etc/rc.d/apache.sh**.

Take a look at **/usr/local/etc/rc.d/apache.sh.**

Note that it provides instructions about what to put in **/etc/rc.conf**.

Edit **/etc/rc.conf**

Now you should able to start apache with the default config by running:

/usr/local/etc/rc.d/apache.sh start

Ok apache is now running, you should be able to connect to it on your machine. you’ll also notice that if you change the url from http://localhost to https://localhost that you have an ssl webserver running... Take a look at the certificate. You obviously don’t want to present a certificate to your customers that says snakeoil cert.

Lets create our own self signed cert.

cd to **/usr/local/etc/apache**, note that the certificate that the machine is using is located in this directory. rather than stomp on it, lets create a subdirectory called **mycert** and do our work in there.

To create a cert we use openssl. first we generate a key.

openssl genrsa -des3 -out server.key 1024

Lets remove the password from that key so that we have one that apache can use to start up without prompting us with the password.

openssl rsa -in server.key -out server.pem

In order generate a certificate we first need to generate a certificate signing request.

openssl req -new -key server.key -out server.csr

Follow the prompts, note that **common name** is the name of the server. If you were going to get a certificate signed by a certificate authority, you would take the csr an dsend it to them. We are going to sign our own cert with our private key.

openssl x509 -req -days 60 -in server.csr -signkey server.key -out server.crt

Ok now we have all the pieces to reconfigure apache to use our new cert.

Find the part of **/usr/local/etc/apache/httpd.conf** that deals with the **SSL Virtual Host Context** (note that the https server is just one instance of a virtual host). Scroll down and you'll see:

SSLCertificateFile /usr/local/etc/apache/ssl.crt/server.crt

comment that out and add:

SSLCertificateFile /usr/local/etc/apache/mycert/server.crt

and below, comment out:

SSLCertificateKeyFile /usr/local/etc/apache/ssl.key/server.key

and Replace it with:

SSLCertificateKeyFile /usr/local/etc/apache/mycert/server.pem

Now save the httpd.conf, then run **apachectl stop**, followed by **apachectl startssl**.

now connect to your webserver via ssl and examine your certificate.