Apache Web Server

Quick and Dirty
Chris Wilson
for AfNOG 2008

(Originally by Joel Jaeggli for AfNOG 2007)

About Apache

- Apache http server project
- http://httpd.apache.org
- Apache foundation started to support the web server project, but now extends to a multitude of other projects.

Install from Ports

- `cd /usr/ports/www/apache22/`
- `make install`

File System Layout

- config files are in `/usr/local/etc/apache22/`
- files the webserver will serve are in `/usr/local/www/apache22/data/`
- Startup script is `/usr/local/etc/rc.d/apache22`

Start Automatically

- Take a look in `/usr/local/etc/rc.d/apache22`
- Add `apache22_enable="YES"` to `/etc/rc.conf`
- Run `/usr/local/etc/rc.d/apache22 start`

Generating Certificates (1)

- Change to the Apache configuration directory:
  - `cd /usr/local/etc/apache22`
- Generate an RSA encryption key:
  - `openssl genrsa -des3 -out server.key.generate 1024`
- You will need to enter a password to encrypt the new key
- Unless we remove the password, you will have to enter it every time you start Apache

Generating Certificates (2)

- Use this command strip the password off the key:
  - `openssl rsa -in server.key.generate -out server.key`
- Enter the *same* password as before, to decrypt the key

Generating Certificates (3)

- Now create a certificate request:
  - `openssl req -new -key server.key -out server.csr`
- It will ask you for country, address, etc.
- These will appear in the certificate when you inspect it in the browser
- The Common Name must be the name that you use to access the website (e.g. `localhost`)

Generating Certificates (4)

- You can sign the certificate yourself, for testing:
  - `openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt`
- Your browser will not trust the certificate. It will show a warning when you view the page
- You can get a proper certificate from Verisign, Equifax etc. for about $50 by sending your certificate signing request (`.csr` file)

Installing your New Certificates

- Edit `extra/httpd-ssl.conf`
- Find the following lines:
  - `SSLCertificateKeyFile`
  - `SSLCertificateFile`
- Make sure they point to your certificate files:
  - `SSLCertificateKeyFile "…/server.key"`
  - `SSLCertificateFile "…/server.crt"`

Enabling SSL

- Edit `httpd.conf`
- Uncomment `#Include etc/apache22/extra/httpd-ssl.conf`

Start Apache!

- `/usr/local/etc/rc.d/apache22 start`
- Check that you can access `http://localhost` in your browser
- Check that you can access `https://localhost` in your browser, and that you get a certificate warning
- Click on the padlock icon in your browser and check that the certificate details are correct
- Profit!

Enable IPv6

- Default configuration listens on all addresses (IPv4 and IPv6) on port 80
- Nothing to do!
- If you bind to a specific V4 address, you can bind to V6 too, for example:
  - `Listen [2001:db8::a00:20ff:fea7:ccea]:80`
  - `<VirtualHost [2001:db8::a00:20ff:fea7:ccea]>`