



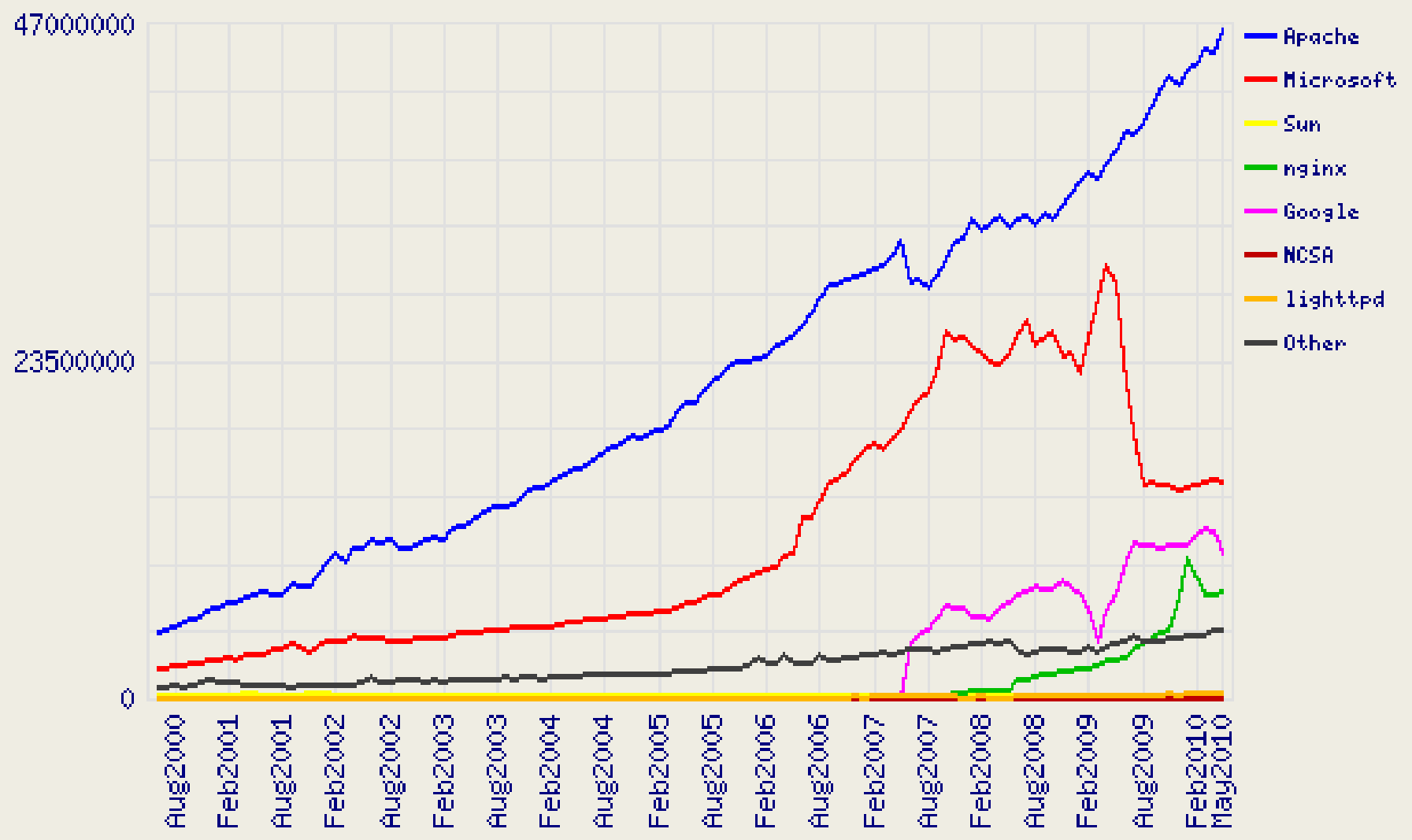
APACHE HTTP SERVER

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.

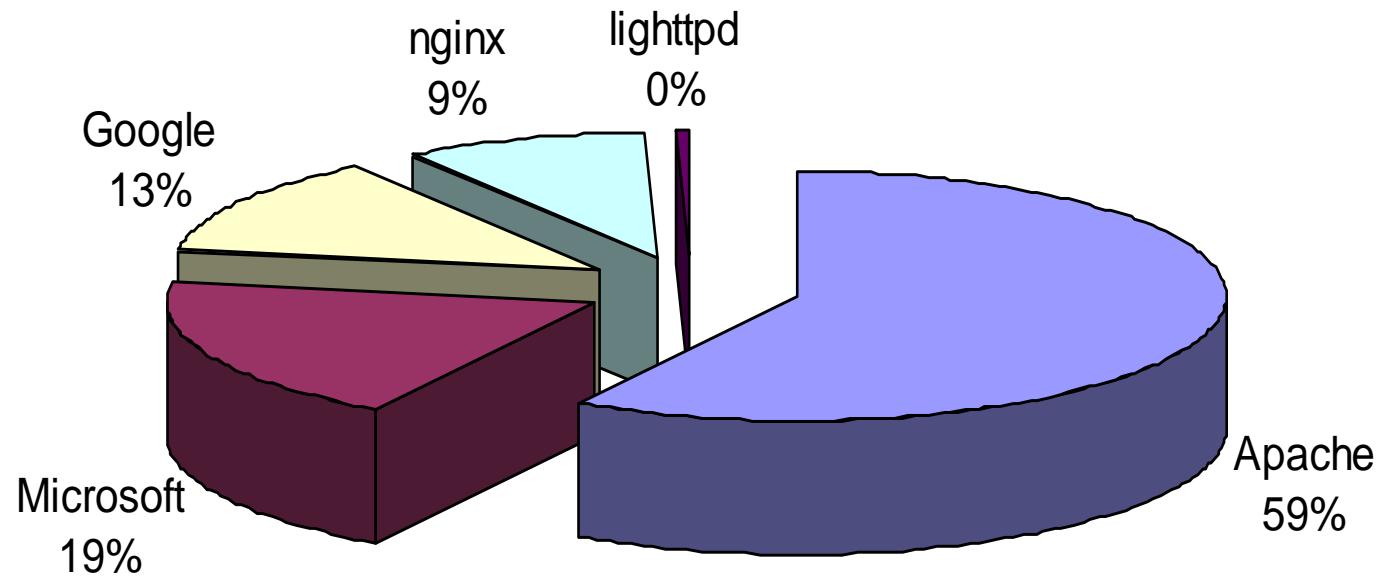


Stats of Web Server types



What the Busiest 1M Websites use

Totals for Active Servers Across All Domains - May 2010



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`
- **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`
- **Restart**
`$ apachectl restart`

Apache SSL

- Secure Socket Layer (SSL) port is 443
- SSL is important to protect communication between browser and web-server
- Requires the creation of SSL certificates and Certificate Signing Requests (CSR)
- For integrity SSL certificates are signed by a Certificate Authority's (CA) such as Verisign
- Self signed Certificates will also work but your browser will not trust it and will give a warning to users (which most don't read)
- *Refer to the Creating SSL Certificate Exercise Section*

How SSL Works

- Each SSL certificate has a Public and Private key
- The Public Key is used to encrypt the information
- The Public Key is accessible to everyone
- The private Key is used to decipher the information
- The private should be not be disclosed

Role of Certificate Authority

- There are a number of CA that certify certificates
- Most browsers have pre-included public Keys from the CA's
- A CA certified certificate will have validation information signed by the CA's private key
- The browser will decrypt the validation information using the public key and verify that the certificate is certified by the CA
- If this fails a warning is given

Virtual Hosting

- Apache Provides multiple options of virtual hosting and scales
 - *Name Based virtual hosts*
 - *IP Based Virtual Hosts*
 - *Aliases*
- Its recommended to use an IP address over hostnames in virtual hosting configuration
- *Refer to virtual hosting Exercise section*

Apache and IPv6

- Apache supports IPv4 and IPv6 by default
- Set the listen option to port 80 will listen for both IPv4 and IPv6
- listen option with IPv4 and IPv6 specific addresses will invoke different sockets for each protocol

Listen 196.200.219.xx:80

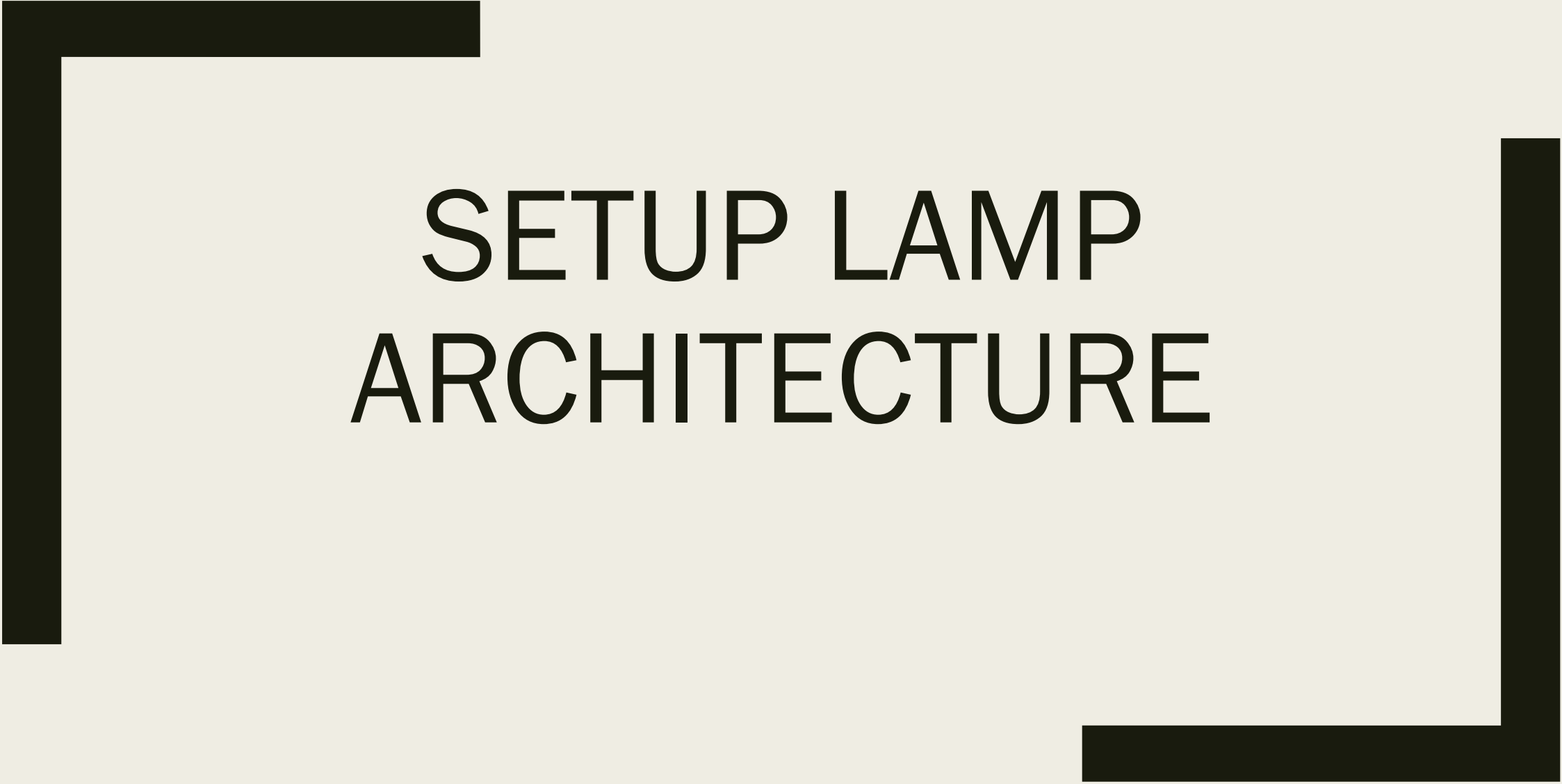
Listen [2001:4348:0:219:196.200.219:xx]:80

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!

Apache implementations

- Apache is widely used to serve many content applications
- Webmail, Blogs, Wiki's, CMS etc
- Attempt to install wordpress and configure it



SETUP LAMP
ARCHITECTURE

Setup the software

- `# sudo apt-get install apache2 mysql-server php5-mysql libapache2-mod-php5`
- Rule for the the FIREWALL
- `# ufw allow www`
 - *Necessary to authorized HTTP requests*

PHP Test Page

- Create the file
- `/var/www/test.php`

With the command

```
# echo '<? phpinfo() ? >' > /var/www/test.php
```

Acced to the page : `http://<adresse_IP_of_server>/test.php`

Create a SSL certificate

- `/etc/ssl`
- `# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ssl/certs/www.monsite.ro.crt`

Activate the ssl module on Apache

- By default Apache configured to use the HTTPS protocole
- `# a2enmod ssl`

Serve an website in ssl

- Create a new file `/etc/apache2/site-available/www.monsite.fr-ssl`
- `<VirtualHost_default_:443>`
 - `ServerAdmin webmaster@monsite.ro` (replaced by your address)
 - `DocumentRoot /srv/www.monsite.ro-ssl/error.log`
 - `ErrorLog ${APACHE_LOG_DIR}/www.monsite.ro-ssl/error.log`
 - `LogLevel warn`
 - `CustomLog ${APACHE_LOG_DIR}/www.monsite.ro-ssl/access.log combined`

 - `SSLEngine on`
 - `SSLCertificateFile /etc/ssl/certs/www.monsite.ro.crt`
 - `BrowserMatch "MSIE [2-6]" \
 - nokeepalive ssl-unclean-shutdown \
 - downgrade-1.0 force-response-1.0`
 - `BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown`
- `</VirtualHost>`

Serve Several website

- Activate virtual hosts on the 443 port by adding the ligne :
- NameVirtualHost *:443
- In the file /etc/apache2/ports.conf
- And modify
- /etc/apache2/sites-vailable/monsite.ro-ssl
- ????

■ Create :

- # mkdir /srv/www.monsite.fr-ssl
- # mkdir /var/log/apache2/www.monsite.ro-ssl

To activate restart Apache

a2ensite www.monsite.ro-ssl

service apache2 restart

If the FireWall is activated you need to add :

ufw allow "WWW Secure"



AN WEBSERVER IN PYTHON

Setup Cherrypy

- <http://cherrypy.org>
- On Linux
 - *Python3 setup.py install*

Put on ligne of the first page

Create in your directory a small text file : tutorial.conf

```
[global]
```

```
server.socket_host="127.0.0.1"    ????
```

```
server.socket_port=8080
```

```
server.thread_pool=5
```

```
tools.session.on=TRUE
```

```
tools.encode.encoding="Utf-8"
```

```
[/annexe]
```

```
tools.staticdir.on=TRUE
```

```
tools.staticdir.dir="annexes"
```

- Create your Python Script

- Import cherrypy

- class MonSiteWeb(object):

- *def index(self) :*

- return "<h1>Bonjour à vous !</h1>"

- *Index.exposed=TRUE*

- # Main Program

- cherrypy.quickstart(MonSiteWeb(),config="tutorial.conf")

Setup your website

- <http://localhost:8080/index>