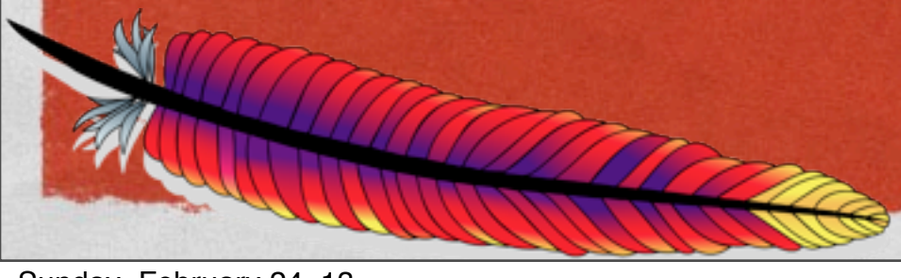
APACHE HTTPD BASICS

Rich Bowen
rbowen@apache.org

Slides are at: **tm3.org/httpd-ac2013**

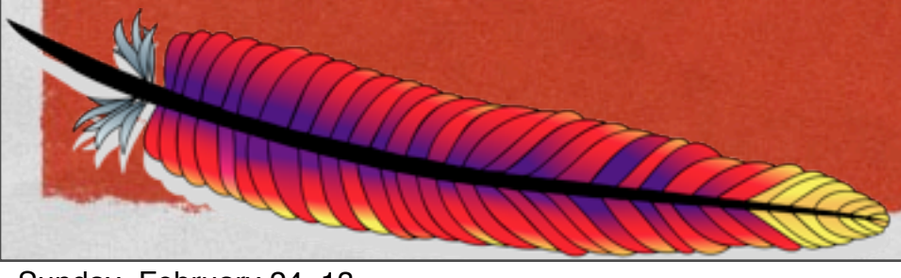
OVERVIEW

- Architecture
- Installation
- Configuration
- Modules
- Community/Development



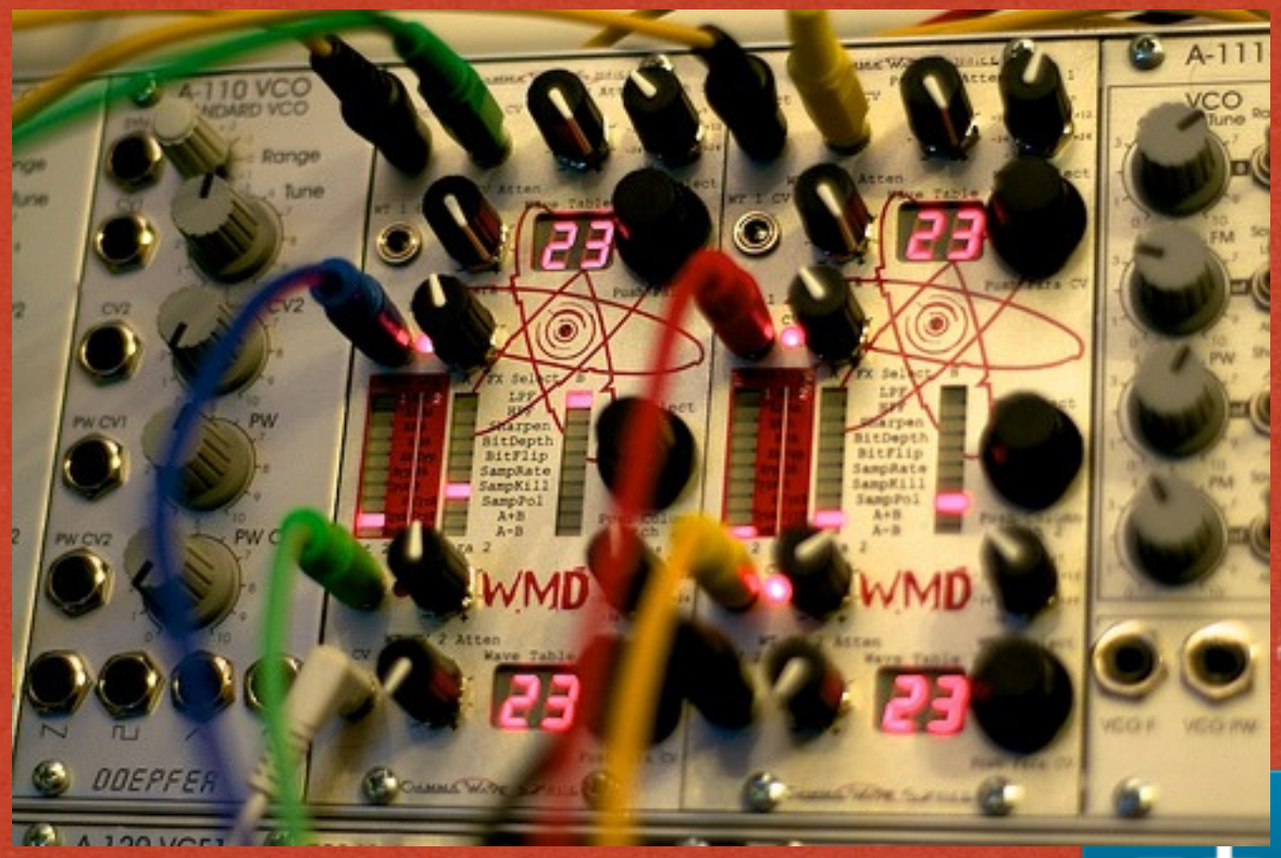
TL;DR

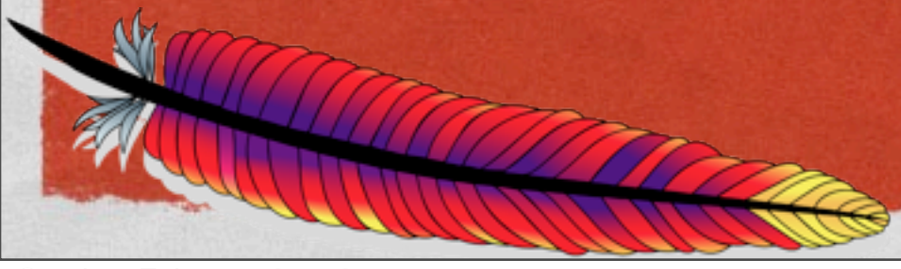
- http://httpd.apache.org/docs/current



ARCHITECTURE

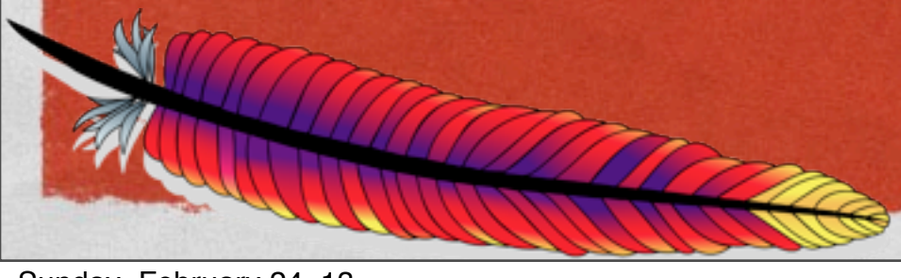
- Modular "plugin" architecture
- Small core
- Everything in optional modules
- MPMs





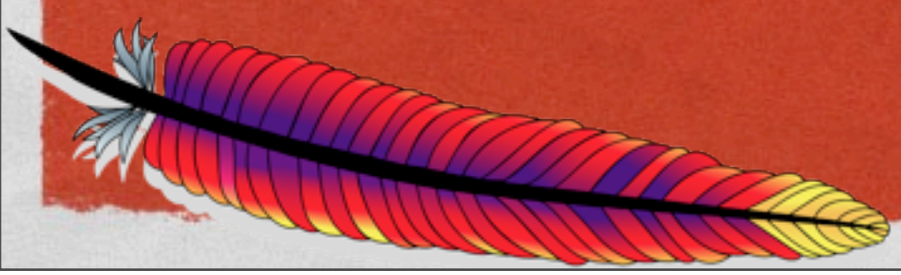
MPM

- Multi-Processing Modules
- Your server receives multiple requests at the same time. MPMs provide different ways of handling that concurrency

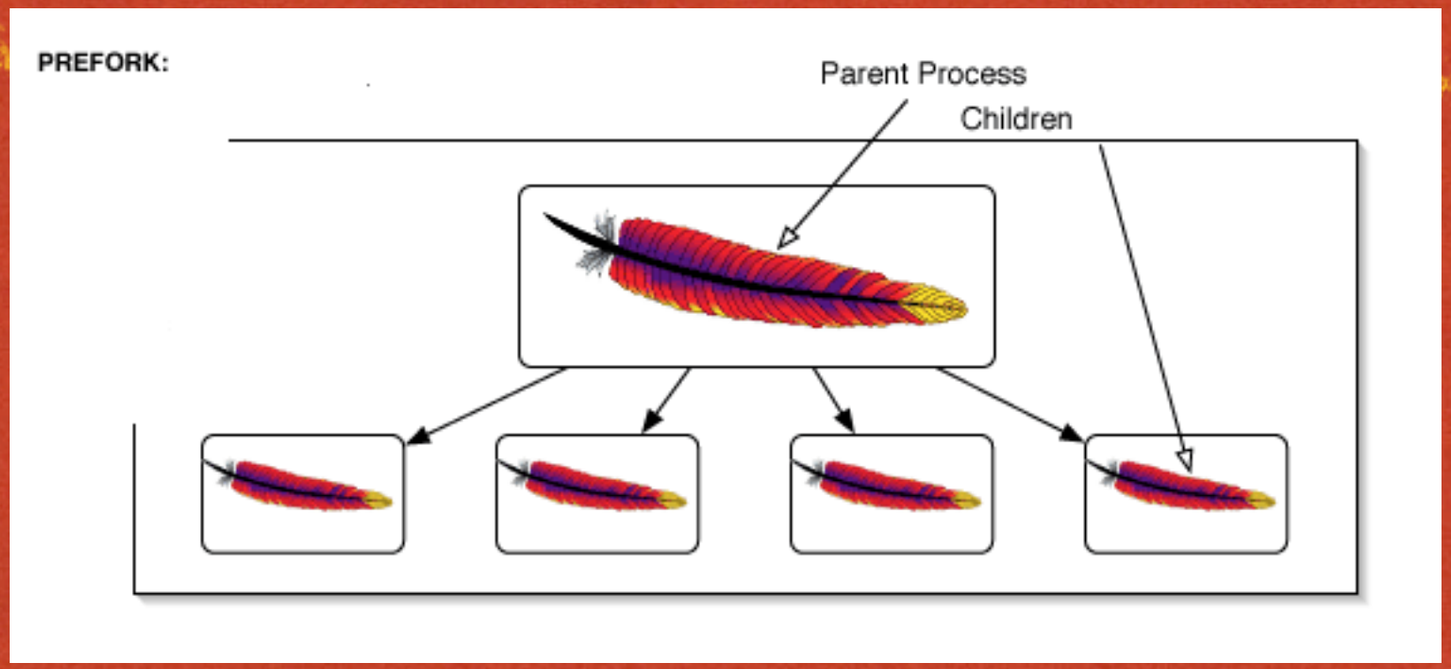


PREFORK

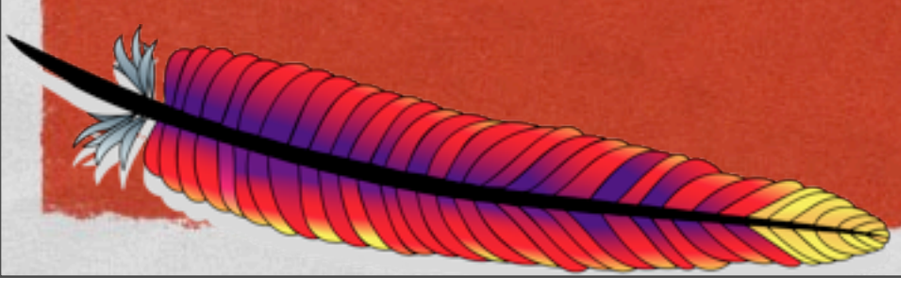
- Default for 2.2 and earlier
- One parent, multiple forked child processes
- Each child process can answer a single request
- Create/Destroy child processes as load dictates



PREFORK

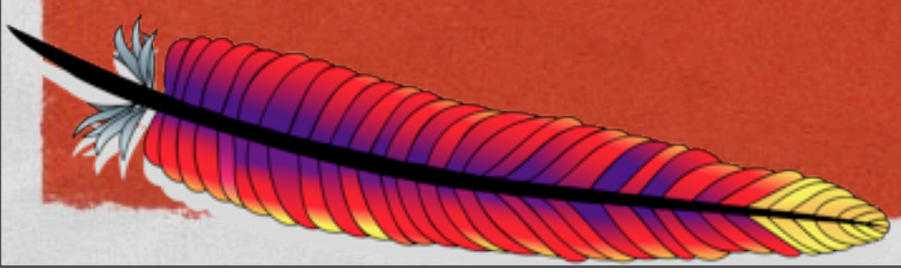


- Advantages: Very stable
- Disadvantages: Not very scalable, perhaps a little slow

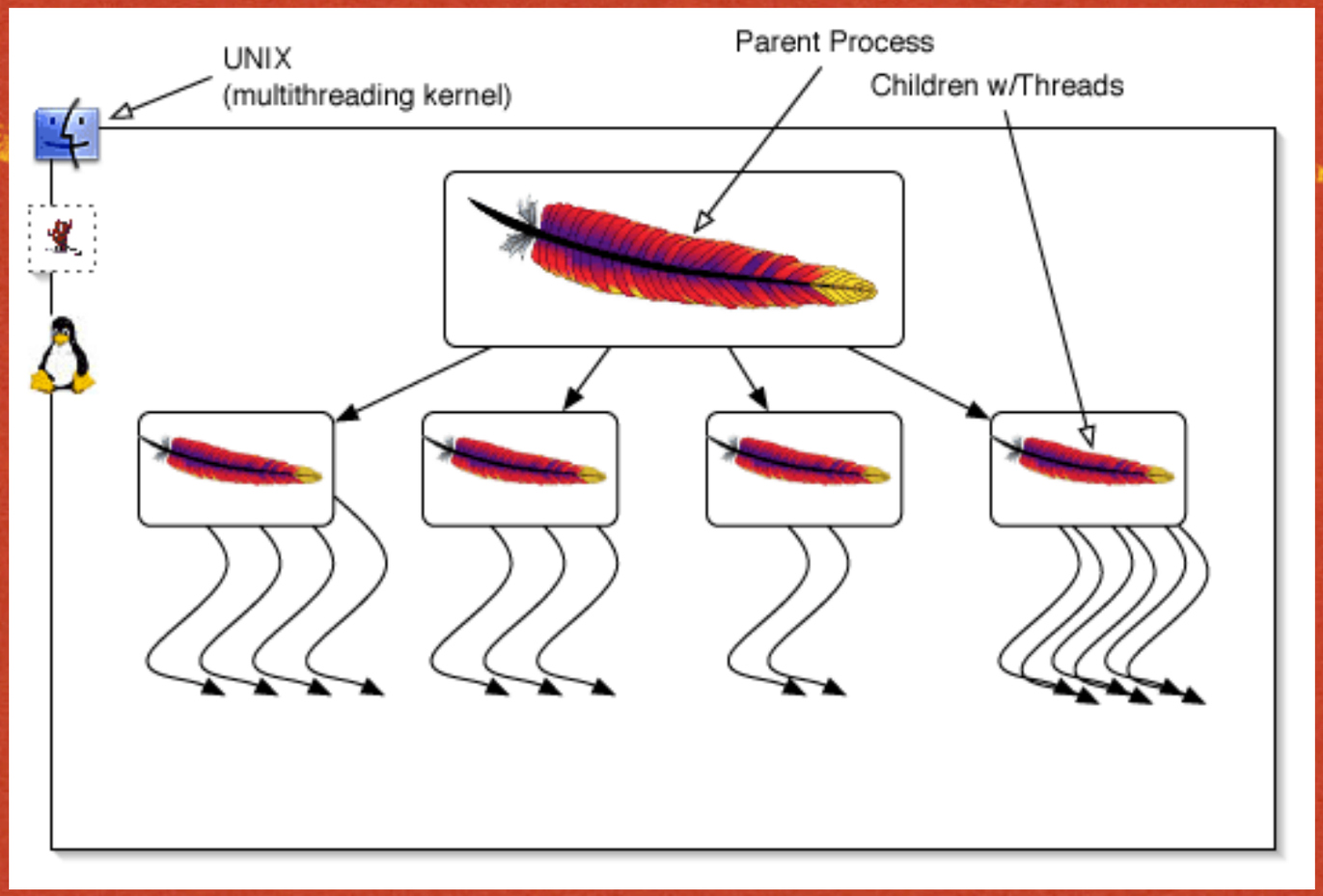


CHILD PROCESSES

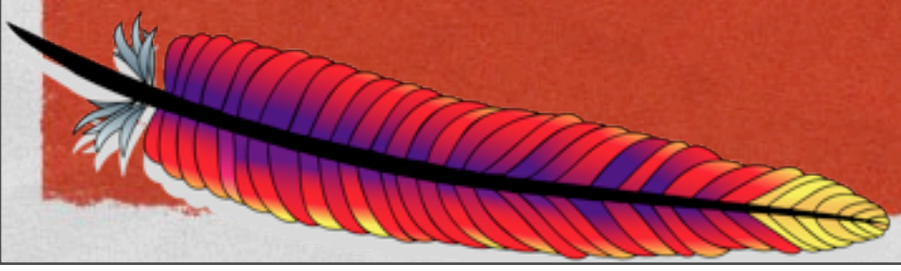
- Processes created, reaped, as required by server load
- MinSpareServers
- MaxSpareServers
- MaxClients (MaxRequestWorkers on 2.4)



WORKER

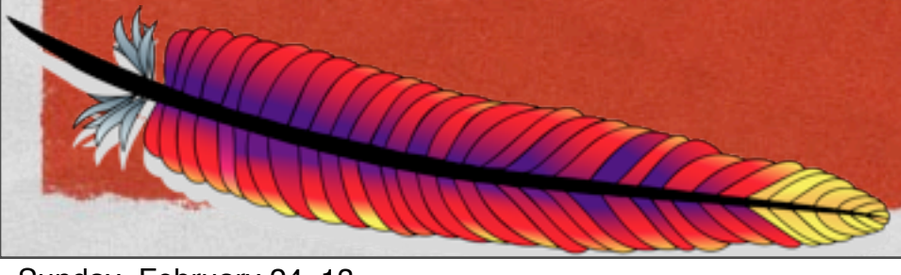


- Advantage: Fast and very scalable
- Disadvantage: Need to think about thread safety



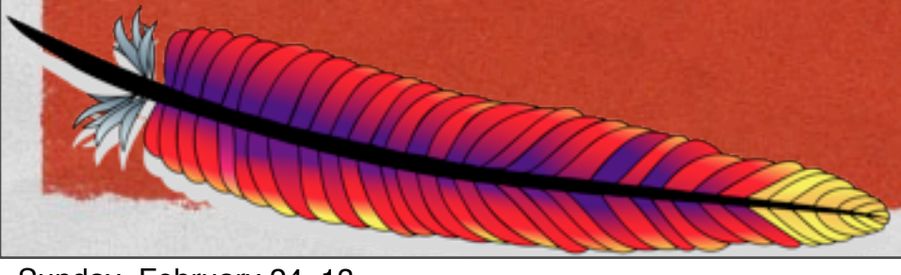
THREAD MANAGEMENT

- Similar to prefork:
  - ThreadsPerChild
  - MinSpareThreads
  - MaxSpareThreads
  - MaxRequestWorkers

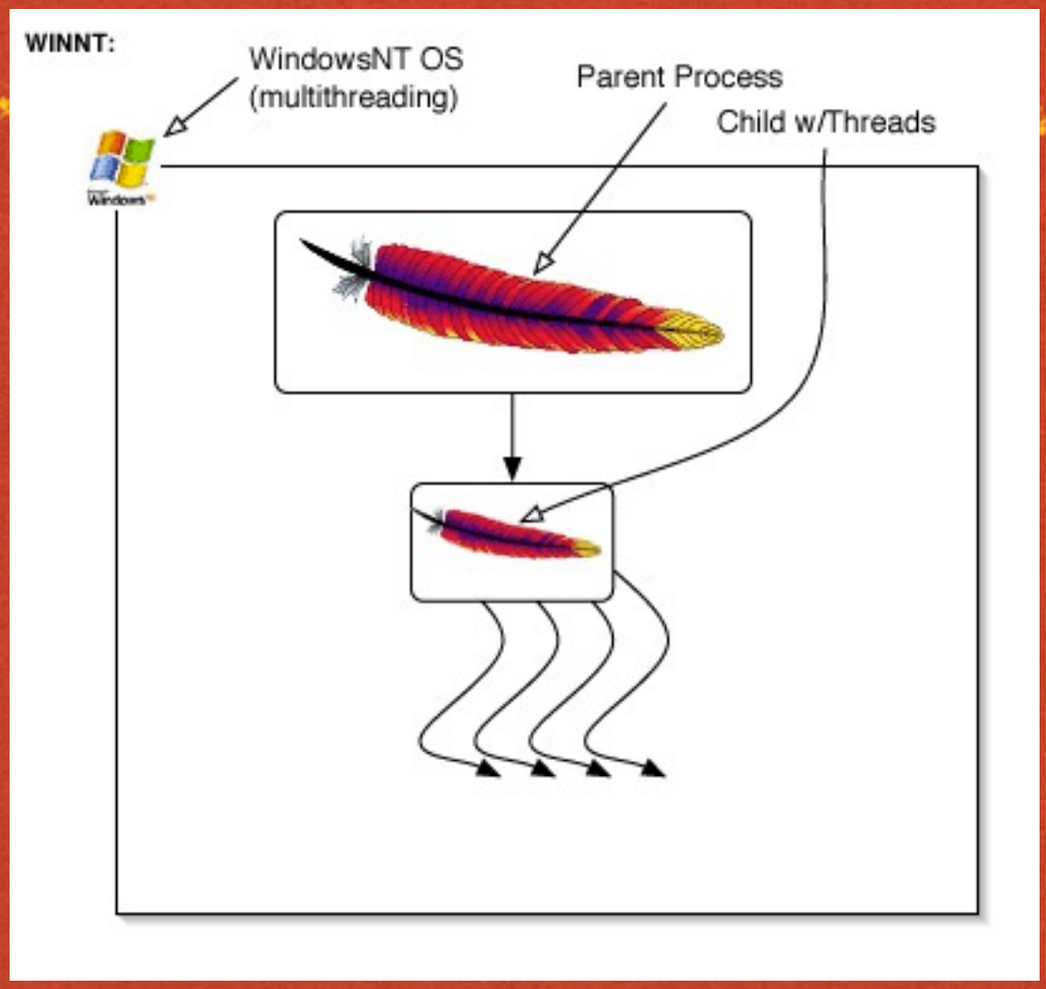


EVENT

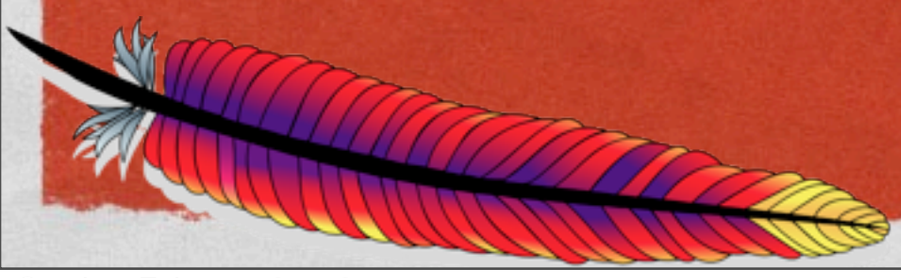
- Like worker, but with some added shinyness
- Default on most modern Unix operating systems



WINNT

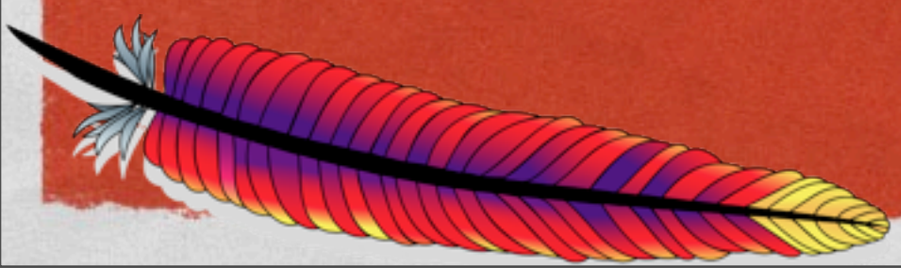


- Like worker, but only one child process



CHOOSING AN MPM

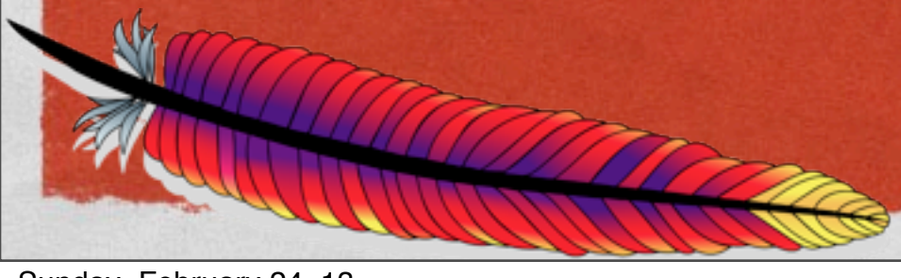
- Prior to 2.4, you choose the MPM at build or install time. Changing MPM requires rebuild/reinstall
- `./configure --with-mpm=worker`
- See configure section in a moment



2.4

- With 2.4, you can (and should) build the MPMs as loadable modules, and select in configuration

```
--enable-mpms-shared=MPM-LIST
                        Space-separated list of MPM modules to enable for
                        dynamic loading. MPM-LIST=list | "all"
```

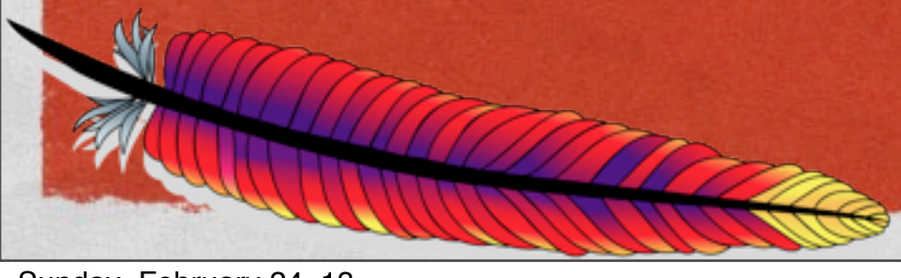


2.4

- With 2.4, you can (and should) build the MPMs as loadable modules, and select in configuration

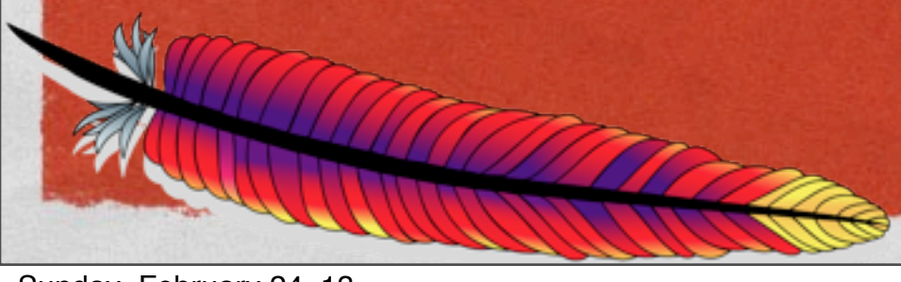
```
--enable-mpms-shared=MPM-LIST
                        Space-separated list of MPM modules to enable for
                        dynamic loading. MPM-LIST=list | "all"
```

```
LoadModule mpm_event_module modules/mod_mpm_event.so
```



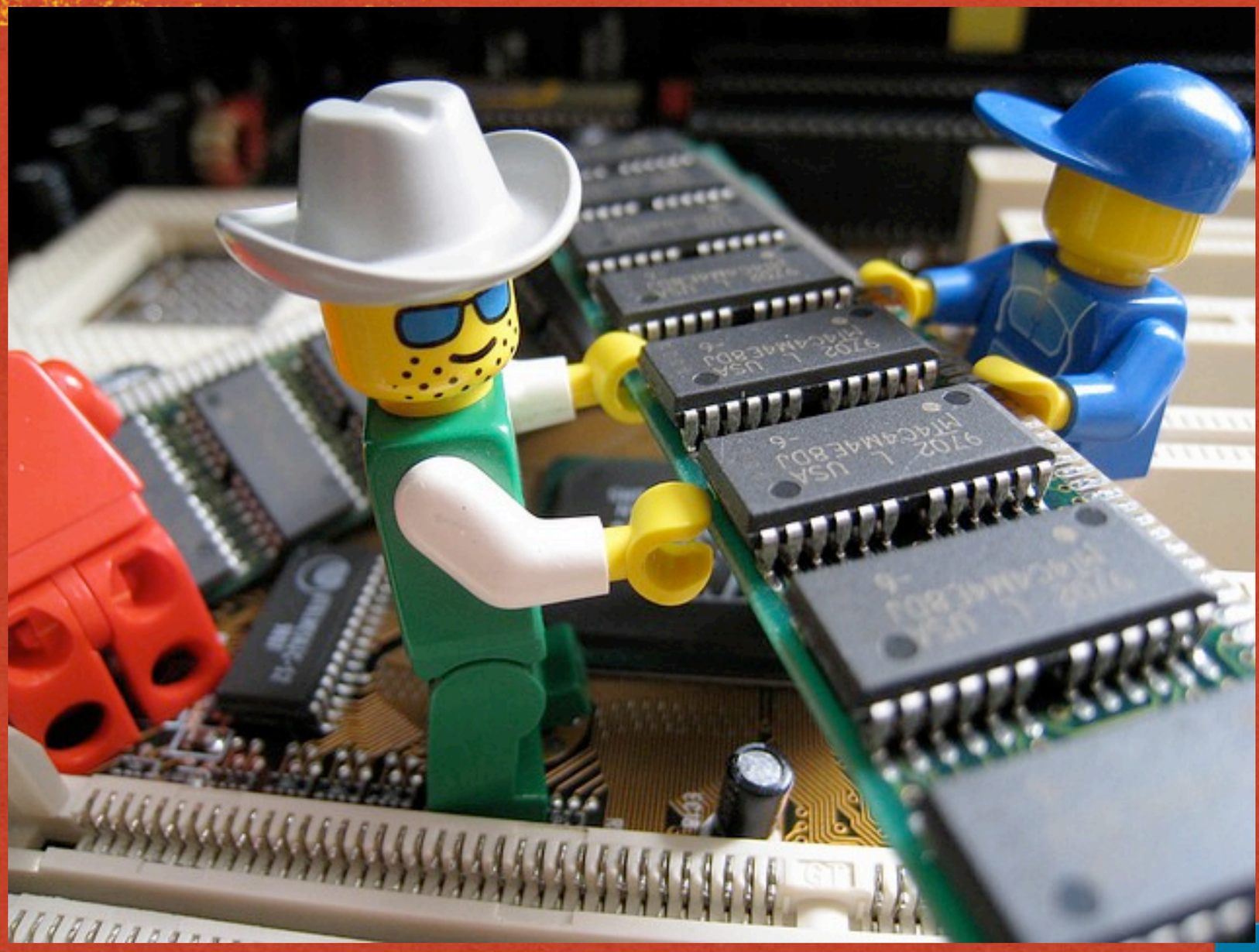
WHICH MPM?

- If possible, go with the default, which will most likely be Event
- Use Prefork if you're doing something that might not be threadsafe



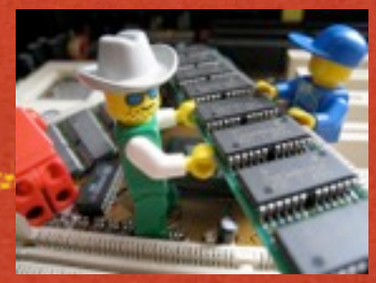
INSTALLATION

- Packages
- Source

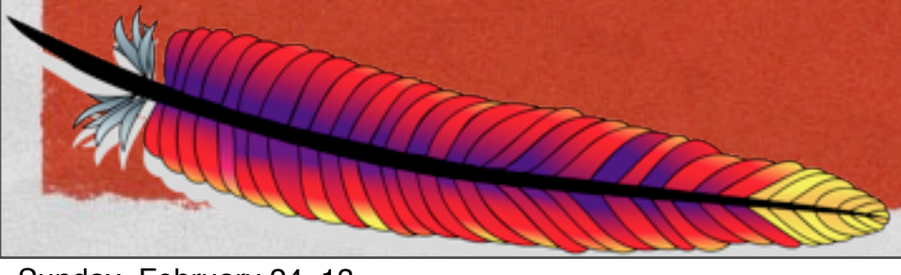


by Daniel Dionne on Flickr

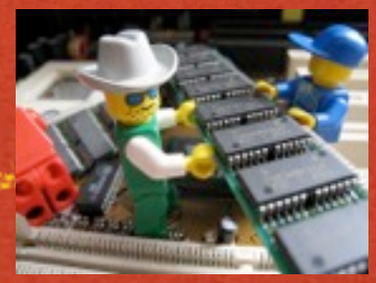
INSTALLATION - PACKAGES



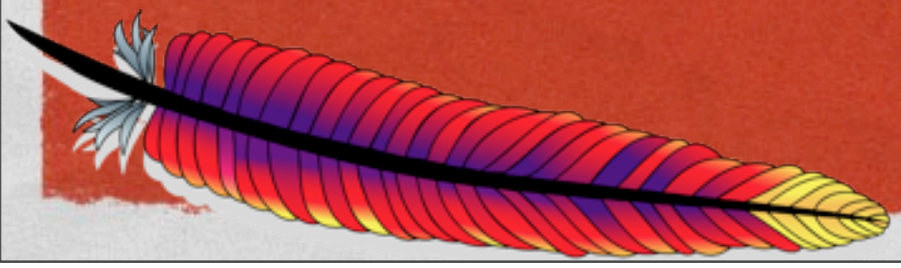
- Most of you will install from a package
- This used to be something of a debate - those days are thankfully past



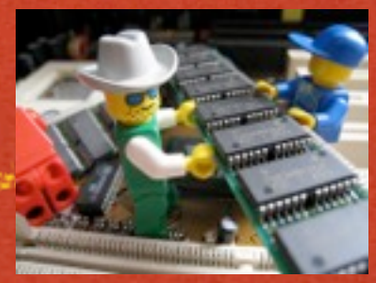
PACKAGE INSTALL



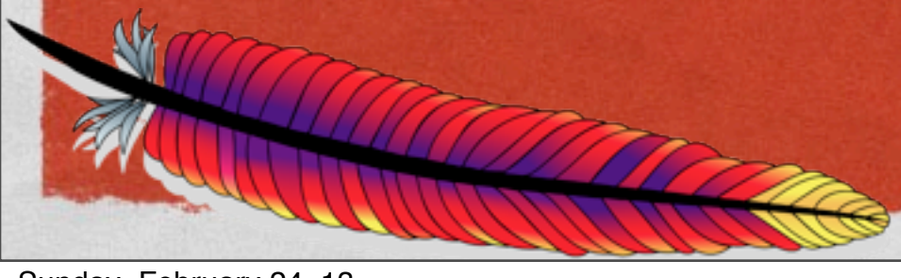
- apt-get install apache2 apache2-dev
- yum install apache2 apache2-dev
- Download installer from
  www.apachelounge.com/download



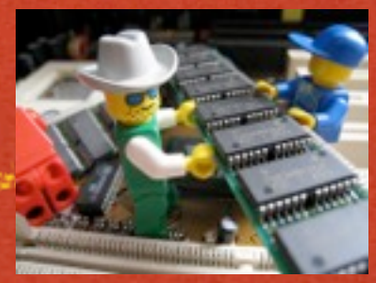
BUILDING FROM SOURCE



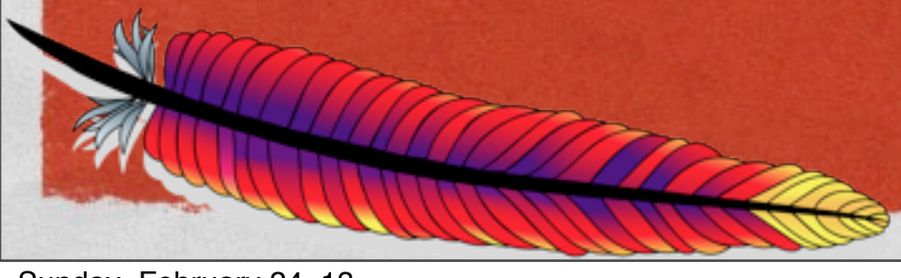
- There are still many reasons to build from source
- It helps you be more familiar with how httpd fits together



CONFIGURE



- The ./configure script sets up how httpd will be built
- Options include:
  - File locations
  - Modules to be built
  - Other settings

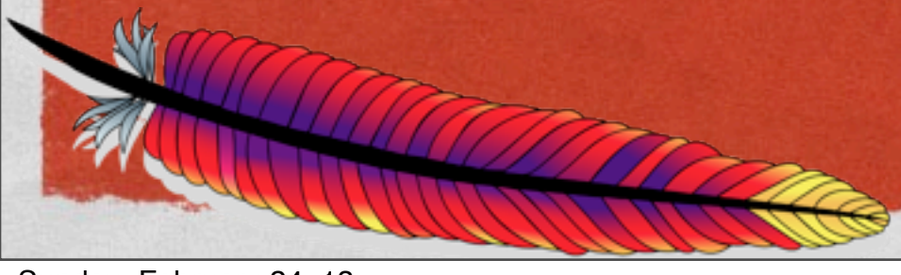


```
[rbowen@NCC1701:apache/httpd-trunk]$ ./configure --help
(02-14 19:56)
`configure' configures this package to adapt to many kinds of systems.

Usage: ./configure [OPTION]... [VAR=VALUE]...

To assign environment variables (e.g., CC, CFLAGS...), specify them as
VAR=VALUE.  See below for descriptions of some of the useful variables.

Defaults for the options are specified in brackets.

Configuration:
  -h, --help              display this help and exit
      --help=short        display options specific to this package
      --help=recursive    display the short help of all the included packages
  -V, --version           display version information and exit
  -q, --quiet, --silent   do not print `checking...' messages
      --cache-file=FILE   cache test results in FILE [disabled]
  -C, --config-cache      alias for `--cache-file=config.cache'
  -n, --no-create         do not create output files
      --srcdir=DIR        find the sources in DIR [configure dir or `..']

Installation directories:
  --prefix=PREFIX         install architecture-independent files in PREFIX
                          [/usr/local/apache2]
  --exec-prefix=EPREFIX   install architecture-dependent files in EPREFIX
                          [PREFIX]

By default, `make install' will install all the files in
`/usr/local/apache2/bin', `/usr/local/apache2/lib' etc. You can specify
```

```
[rbowen@NCC1701:apache/httpd-trunk]$ ./configure --help
(02-14 19:56)
`configure' configures this package to adapt to many kinds of systems.

Usage: ./configure [OPTION]... [VAR=VALUE]...

To assign environment variables (e.g., CC, CFLAGS...), specify them as
VAR=VALUE.  See below for descriptions of some of the useful variables.

Defaults for the options are specified in brackets.

Configuration:
  -h, --help              display this help and exit
      --help=short        display options specific to this package
      --help=recursive    display the short help of all the included packages
  -V, --version           display version information and exit
  -q, --quiet, --silent   do not print `checking...' messages
      --cache-file=FILE   cache test results in FILE [disabled]
  -C, --config-cache      alias for `--cache-file=config.cache'
  -n, --no-create         do not create output files
      --srcdir=DIR        find the sources in DIR [configure dir or `..']

Installation directories:
  --prefix=PREFIX         install architecture-independent files in PREFIX
                          [/usr/local/apache2]
  --exec-prefix=EPREFIX   install architecture-dependent files in EPREFIX
                          [PREFIX]

By default, `make install' will install all the files in
`/usr/local/apache2/bin', `/usr/local/apache2/lib' etc. You can specify
```

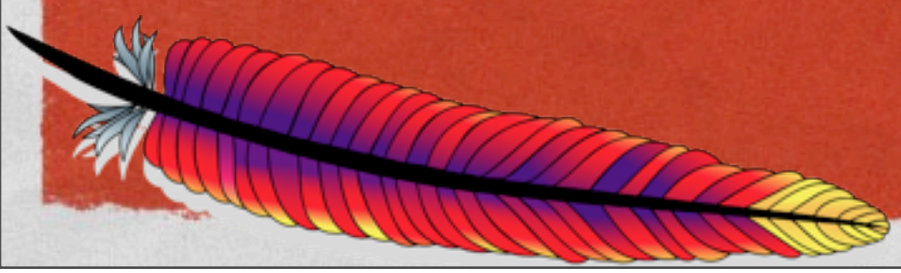
Where does it go?

```
--enable-modules=MODULE-LIST
                    Space-separated list of modules to enable | "all" |
                    "most" | "few" | "none"| "reallyall"
--enable-mods-shared=MODULE-LIST
                    Space-separated list of shared modules to enable |
                    "all" | "most" | "few"| "reallyall"
--enable-mods-static=MODULE-LIST
                    Space-separated list of static modules to enable |
                    "all" | "most" | "few"
--disable-authn-file    file-based authentication control
--enable-authn-dbm      DBM-based authentication control
--enable-authn-anon     anonymous user authentication control
--enable-authn-dbd      SQL-based authentication control
--disable-authn-core    core authentication module
--disable-authz-host    host-based authorization control
--disable-authz-groupfile
                    'require group' authorization control
```



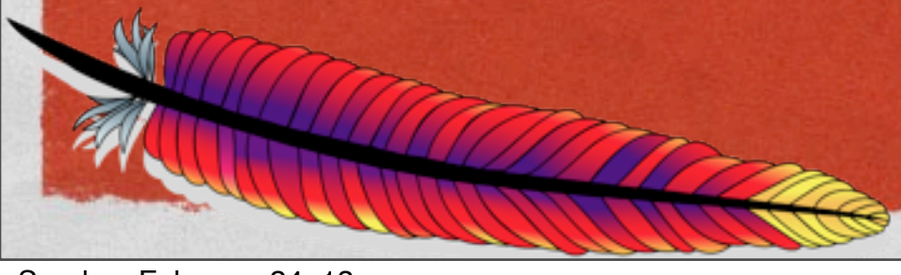
Specific modules

```
--enable-modules=MODULE-LIST
                    Space-separated list of modules to enable | "all" |
                    "most" | "few" | "none" | "reallyall"
--enable-mods-shared=MODULE-LIST
                    Space-separated list of shared modules to enable |
                    "all" | "most" | "few" | "reallyall"
--enable-mods-static=MODULE-LIST
                    Space-separated list of static modules to enable |
                    "all" | "most" | "few"
--disable-authn-file    file-based authentication control
--enable-authn-dbm      DBM-based authentication control
--enable-authn-anon     anonymous user authentication control
--enable-authn-dbd      SQL-based authentication control
--disable-authn-core    core authentication module
--disable-authz-host    host-based authorization control
--disable-authz-groupfile
                    'require group' authorization control
```



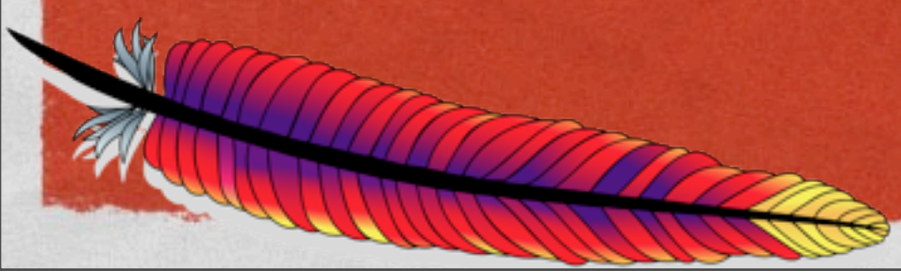
Or just install everything and decide later

```
--enable-modules=MODULE-LIST
                    Space-separated list of modules to enable | "all" |
                    "most" | "few" | "none"| "reallyall"
--enable-mods-shared=MODULE-LIST
                    Space-separated list of shared modules to enable |
                    "all" | "most" | "few"| "reallyall"
--enable-mods-static=MODULE-LIST
                    Space-separated list of static modules to enable |
                    "all" | "most" | "few"
--disable-authn-file    file-based authentication control
--enable-authn-dbm      DBM-based authentication control
--enable-authn-anon     anonymous user authentication control
--enable-authn-dbd      SQL-based authentication control
--disable-authn-core    core authentication module
--disable-authz-host    host-based authorization control
--disable-authz-groupfile
                    'require group' authorization control
```



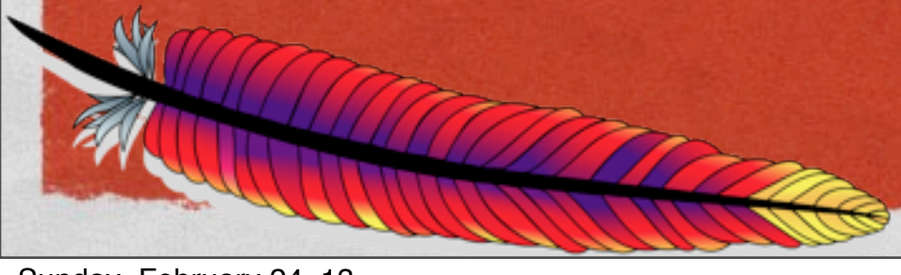
LOADMODULE

```
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule mpm_event_module modules/mod_mpm_event.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule heartbeat_module modules/mod_heartbeat.so
#LoadModule heartmonitor_module modules/mod_heartmonitor.so
#LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
#LoadModule asis_module modules/mod_asis.so
```



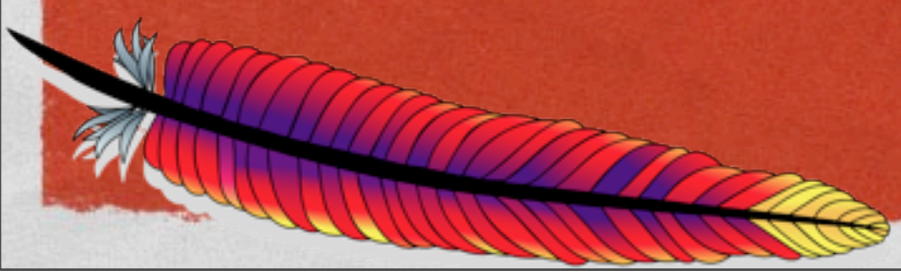
DEMO GOES HERE

...



CONFIG.NICE

- When you run ./configure, the options you selected are saved in a file called config.nice which you can then run again later to get the same options
- Or add additional options
- ./config.nice --prefix=/usr/local/apache-alt

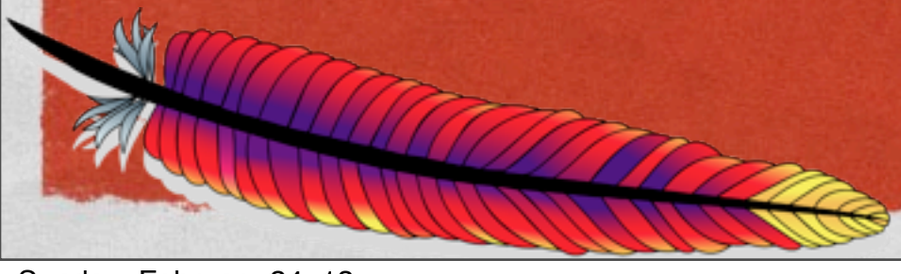


MODULES

- aaa
- cache
- dav
- debugging
- filters
- generators
- loggers
- mappers
- metadata
- proxy
- session
- ssl

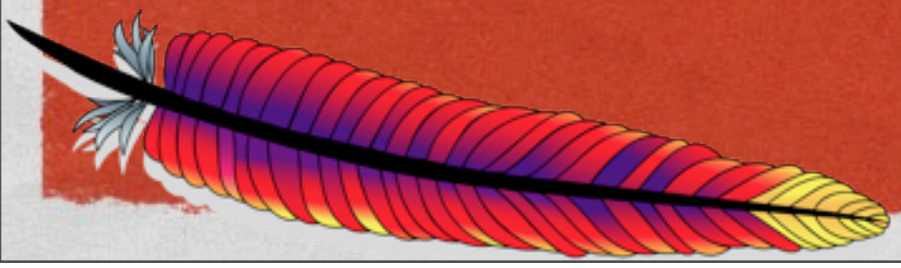
CONFIGURATION FILES

by oliverchesler on Flickr



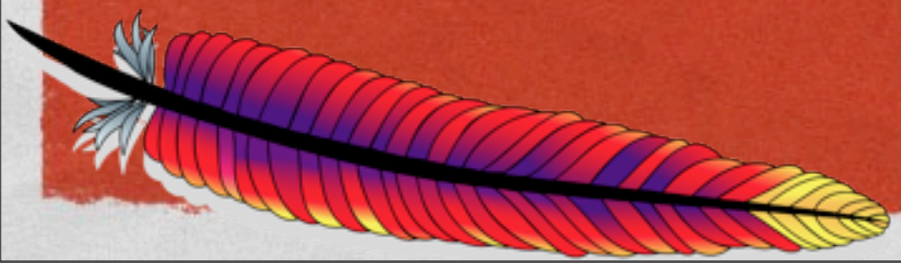
CONFIGURATION

- Plain text configuration files loaded at server start/ restart
- Edit with your favorite configuration file
- No, there's no GUI configuration manager tool



HTTPD.CONF

- The main configuration file is usually called httpd.conf
- By default, located in /usr/local/apache2/conf but this varies from one distribution to another
- httpd -V will tell you where it is



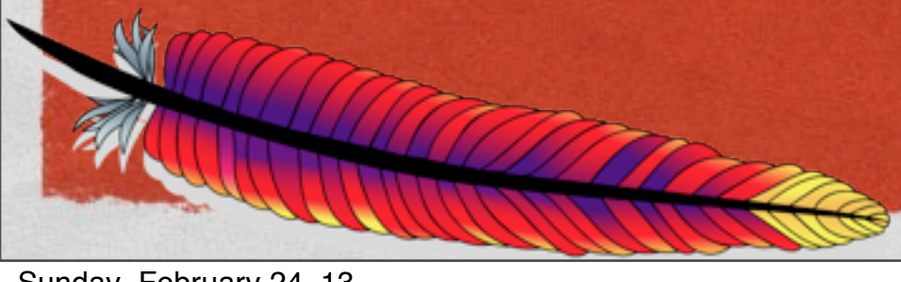
```
[rbowen@NCC1701:apache/httpd-trunk]$ /usr/local/apache2/bin/httpd -V
(02-14 20:38)
Server version: Apache/2.5.0-dev (Unix)
Server built:   Mar  8 2012 11:17:43
Server's Module Magic Number: 20120211:1
Server loaded:  APR 1.4.6, APR-UTIL 1.4.1
Compiled using: APR 1.4.6, APR-UTIL 1.4.1
Architecture:   64-bit
Server MPM:     event
  threaded:     yes (fixed thread count)
    forked:     yes (variable process count)
Server compiled with....
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D APR_USE_PTHREAD_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D DYNAMIC_MODULE_LIMIT=256
 -D HTTPD_ROOT="/usr/local/apache2"
 -D SUEXEC_BIN="/usr/local/apache2/bin/suexec"
 -D DEFAULT_PIDLOG="logs/httpd.pid"
 -D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="conf/mime.types"
 -D SERVER_CONFIG_FILE="conf/httpd.conf"
```

```
[rbowen@NCC1701:apache/httpd-trunk]$ /usr/local/apache2/bin/httpd -V
(02-14 20:38)
Server version: Apache/2.5.0-dev (Unix)
Server built:   Mar  8 2012 11:17:43
Server's Module Magic Number: 20120211:1
Server loaded:  APR 1.4.6, APR-UTIL 1.4.1
Compiled using: APR 1.4.6, APR-UTIL 1.4.1
Architecture:   64-bit
Server MPM:     event
  threaded:     yes (fixed thread count)
    forked:     yes (variable process count)
Server compiled with....
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D APR_USE_PTHREAD_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D DYNAMIC_MODULE_LIMIT=256
 -D HTTPD_ROOT="/usr/local/apache2"
 -D SUEXEC_BIN="/usr/local/apache2/bin/suexec"
 -D DEFAULT_PIDLOG="logs/httpd.pid"
 -D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="conf/mime.types"
 -D SERVER_CONFIG_FILE="conf/httpd.conf"
```

COMMENTS

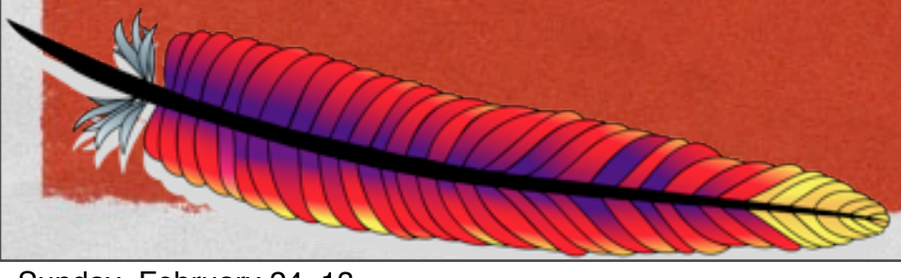
- Line starts with #
- Comments can't start mid-line
- No block comment characters

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName localhost:80
```



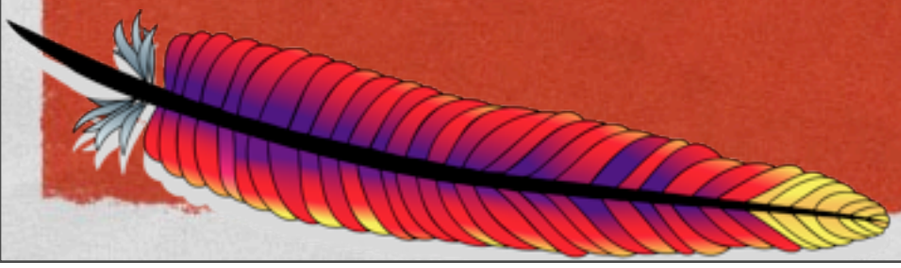
DIRECTIVES

- Keyword followed by one or more arguments
- Directives are permitted in various contexts:
  - server config
  - virtual host
  - directory
  - .htaccess



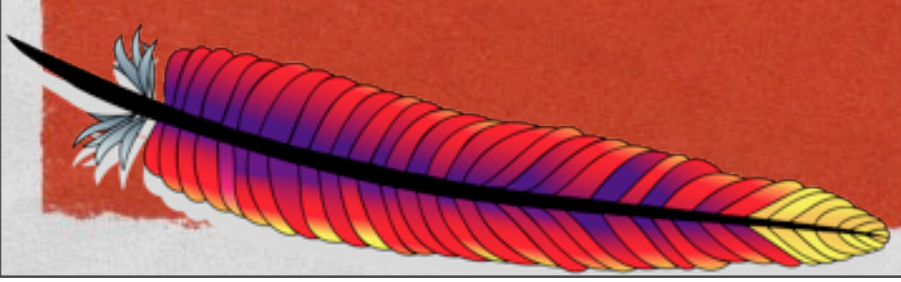
SECTIONS/CONTAINERS

- Encloses one or more directives
- Designates the scope in which those directives are active.
- Look like XML containers



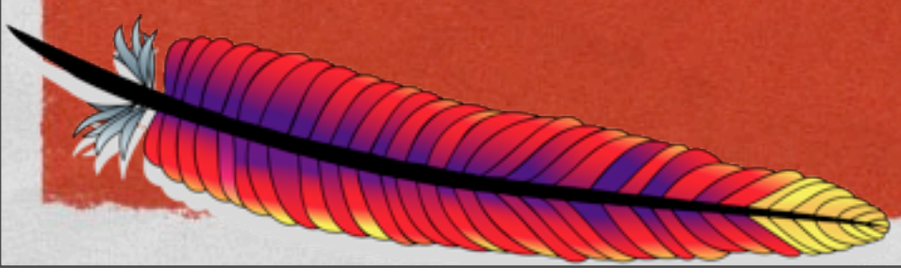
CONTAINER

```
<Directory "/usr/local/apache2/htdocs">
    Options Indexes FollowSymLinks Includes
    XBitHack On

    AllowOverride None

    Require all granted
</Directory>
```



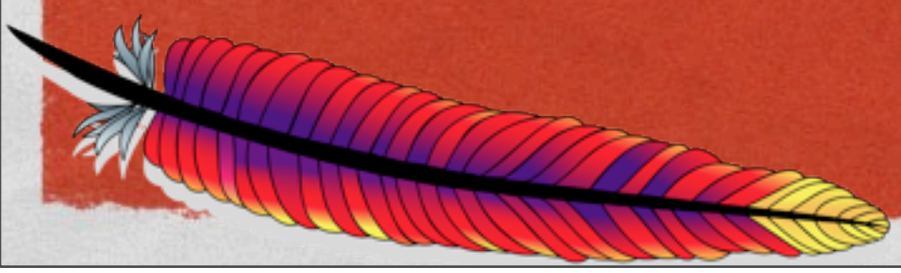
.HTACCESS FILES

- Per-directory configuration files
- Override server-wide configuration
- Applied at request time when a request is mapped to a particular directory



ALLOWOVERRIDE

- AllowOverride specifies what is permitted in .htaccess files
- 'None' is default in 2.4 and later
- 'All' is default in 2.2 and earlier



ALLOWOVERRIDE

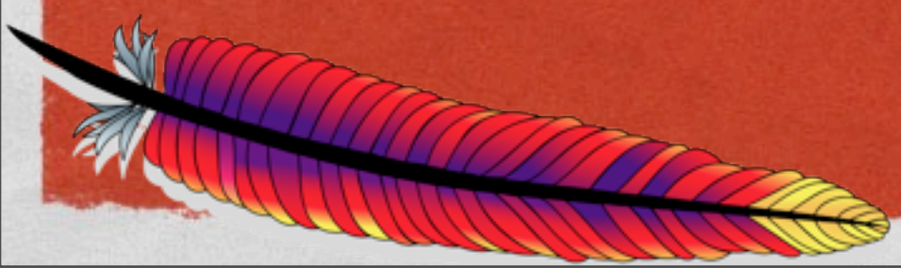
If you want to use it you need at least ...

CGIMapExtension Directive

Description:	Technique for locating the interpreter for CGI scripts
Syntax:	`CGIMapExtension cgi-path .extension`
Context:	directory, .htaccess
Override:	FileInfo
Status:	Core
Module:	core
Compatibility:	NetWare only

HTACCESS USE

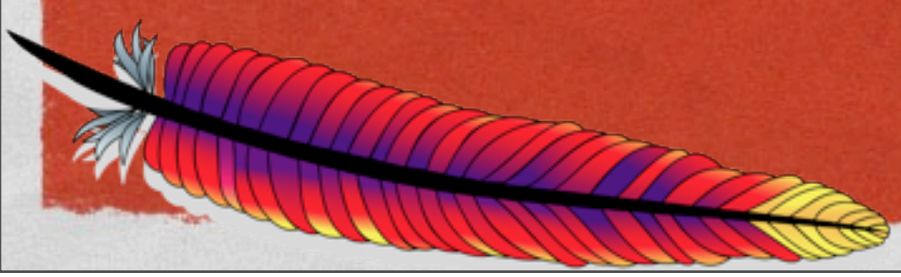
- For people who don't have access to the main config
- Rapid prototyping without restarting httpd
- Significant performance impact of using them
- Each directory in patch checked



DON'T DO THIS:

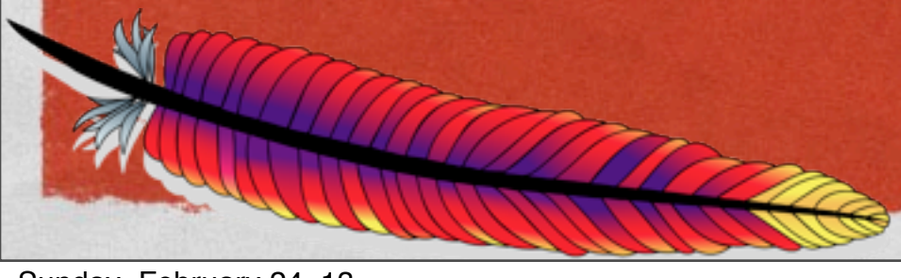
```
<Directory />
  AllowOverride All
</Directory>
```

```
/.htaccess
/www/.htaccess
/www/htdocs/.htaccess
/www/htdocs/example/.htaccess
```



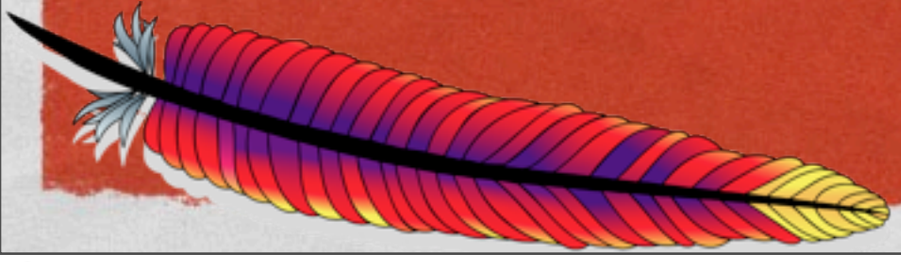
REWRITERULES

- RewriteRule syntax can vary greatly from main-config context to .htaccess context



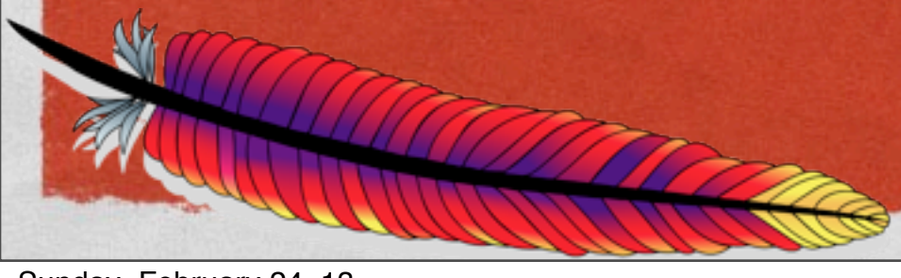
MIME

By photography.andreas, on Flickr



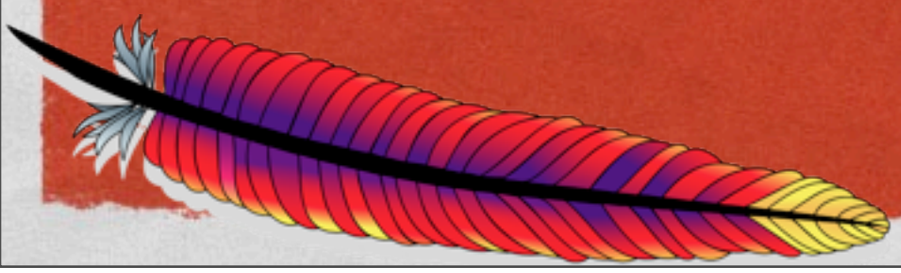
MIME

- Multipart Internet Mail Extension
- Headers that tell what's coming in the body



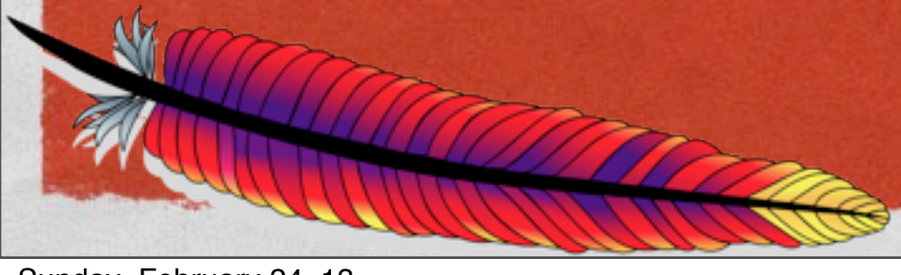
HEADERS

- Content-type: text/html
- Content-length: 34248
- Content-language: en_UK
- Headers ended with a newline



CONTENT-TYPE

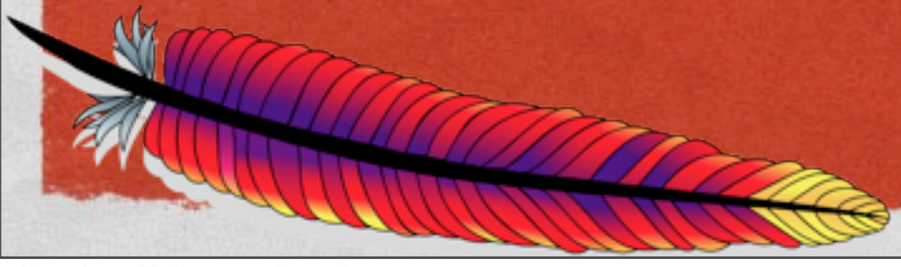
- Content-type: image/gif



CONTENT-TYPE

Major type

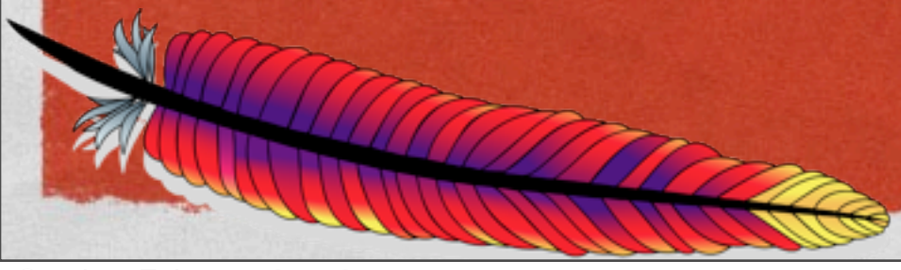
- Content-type: image/gif



CONTENT-TYPE

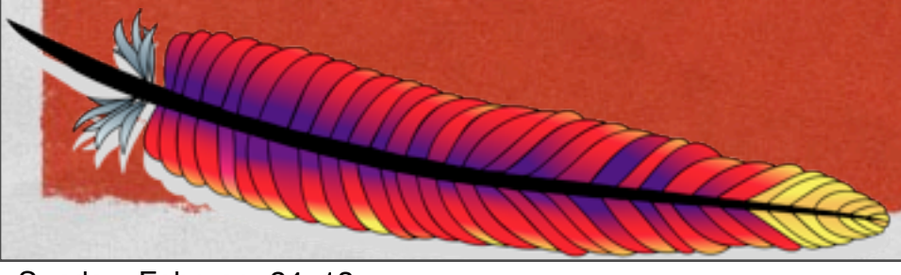
Minor type

- Content-type: image/gif



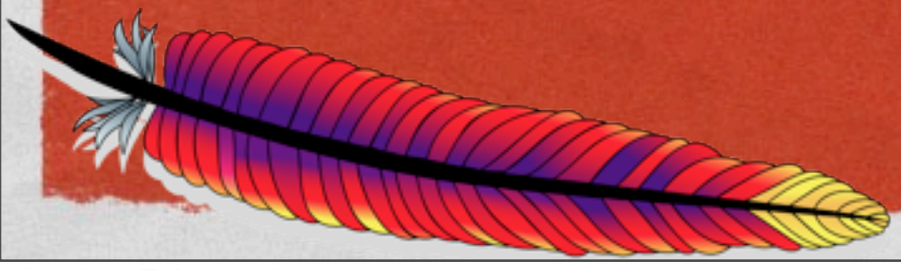
MOD_MIME

- mod_mime sets MIME headers for resources
- Also associates resources with handlers, which then produce output



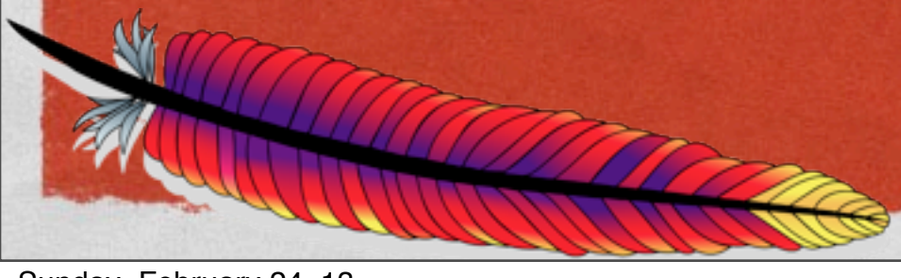
ADDTYPE

- AddType image/gif .gif
- Associates a mime type with a file extension

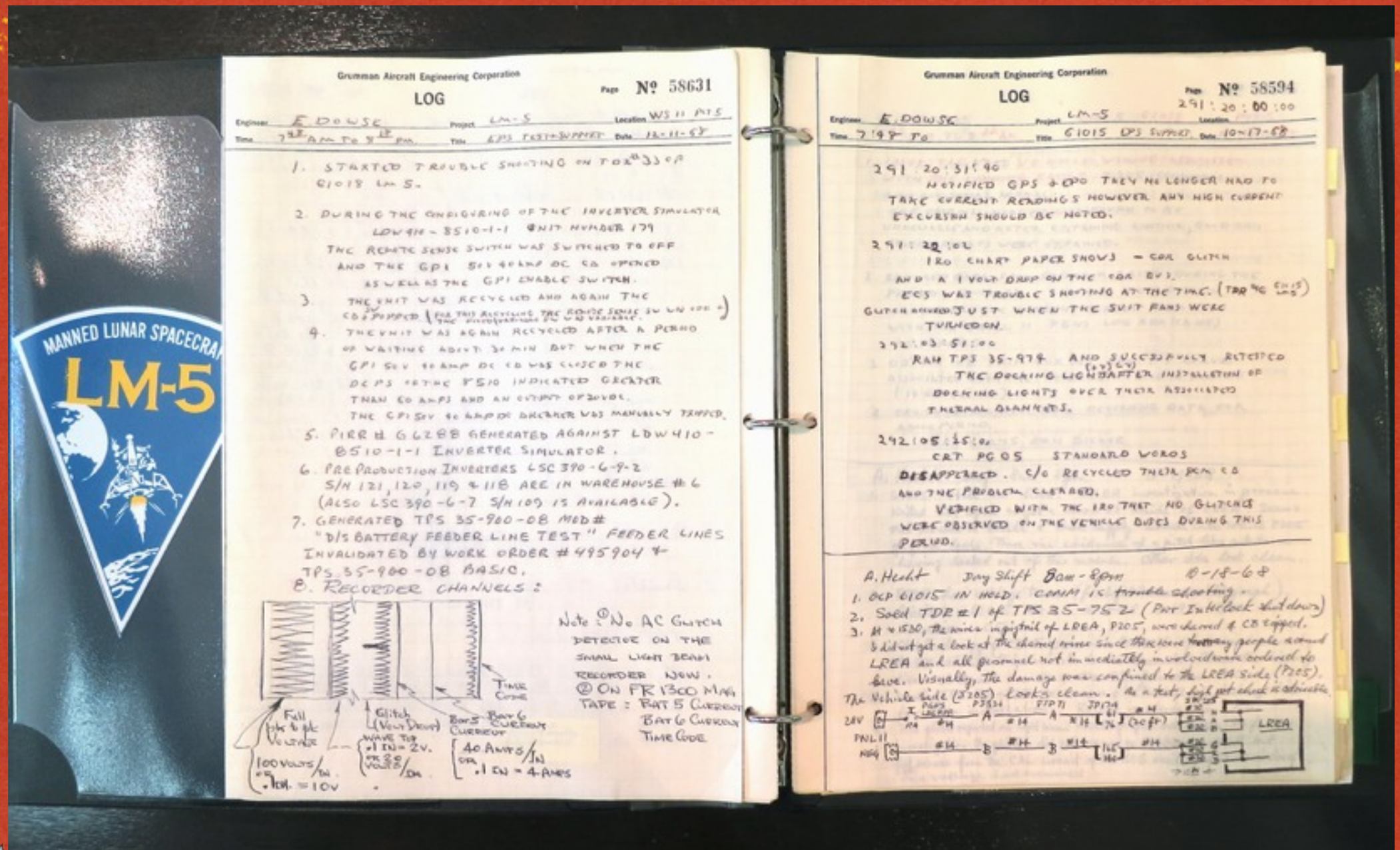


ADDHANDLER

- AddHandler cgi-script .cgi
- Associates a handler to a file extension
- A handler processes a resource to produce content



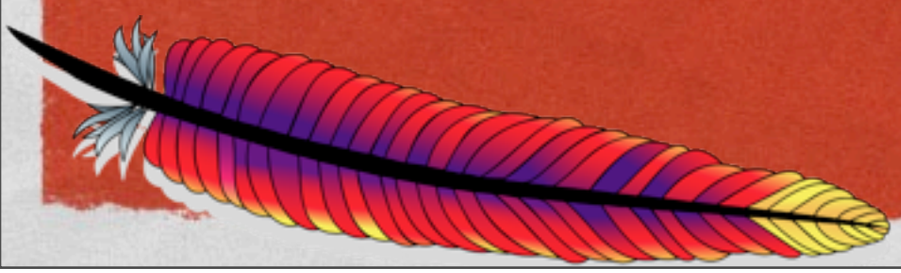
LOGGING



By jurvetson, on Flickr

ACCESS LOG

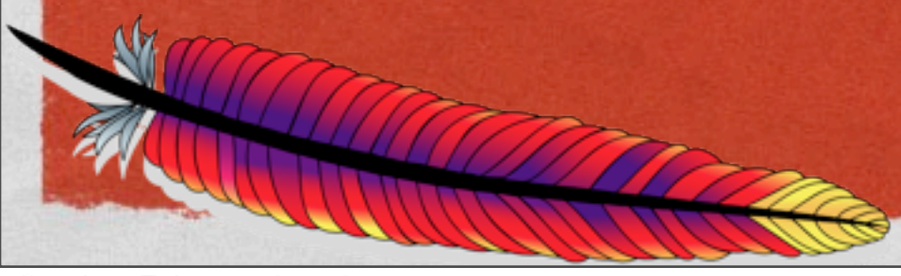
- Each request to the server is logged to the server access log files
- Log files are configurable
  - Location
  - Format



LOGFORMAT

- Defines the format of the log file

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

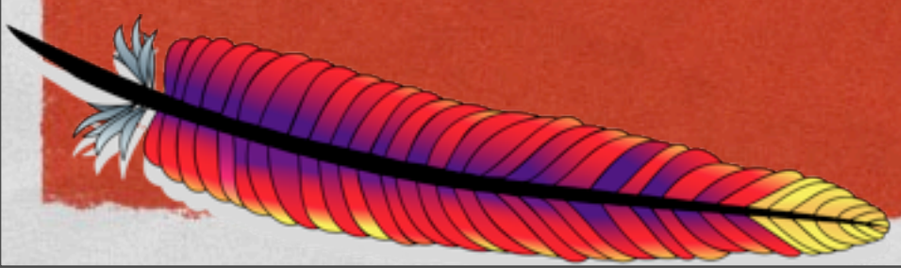


CUSTOMLOG

- Defines where the log goes, and which format to use

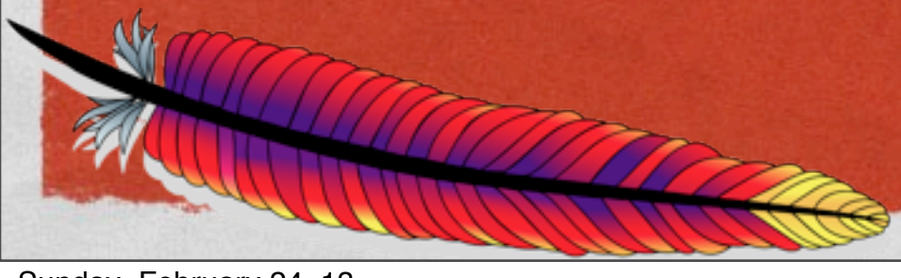
```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

```
CustomLog /var/log/httpd/access_log common
```



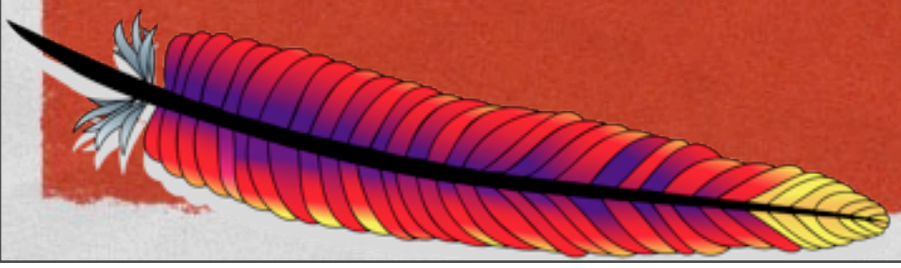
PIPED LOGS

```
CustomLog |/usr/loca/bin/log_process common
```



COMMON LOG FORMATS

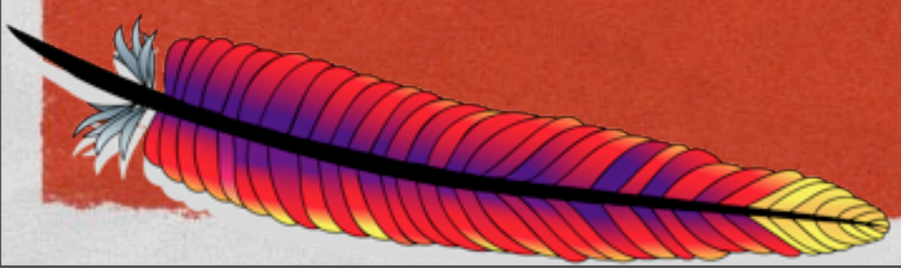
```
# Common Log Format (CLF)
LogFormat "%h %l %u %t \"%r\" %>s %b" common

# Common Log Format with Virtual Host
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost

# NCSA extended/combined log format
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" \
          combined
```



ERRORLOG

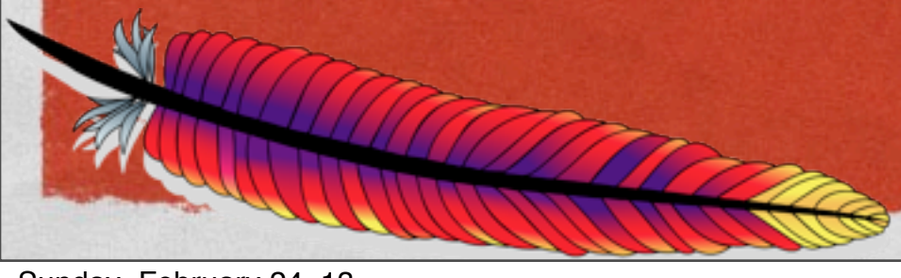
- The ErrorLog directive specifies where the error log should be placed

```
ErrorLog /var/log/httpd/error_log
```

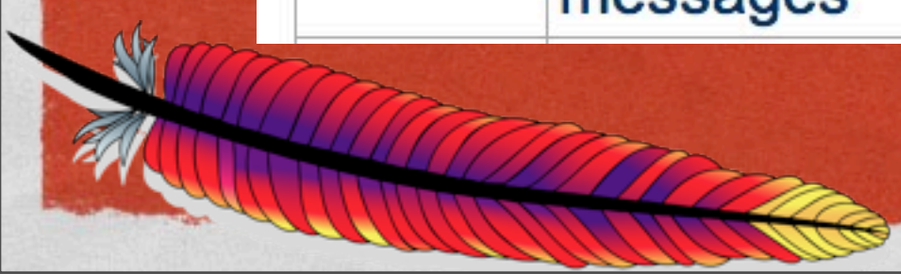


LOGLEVEL

- Specifies how loud the error log should be



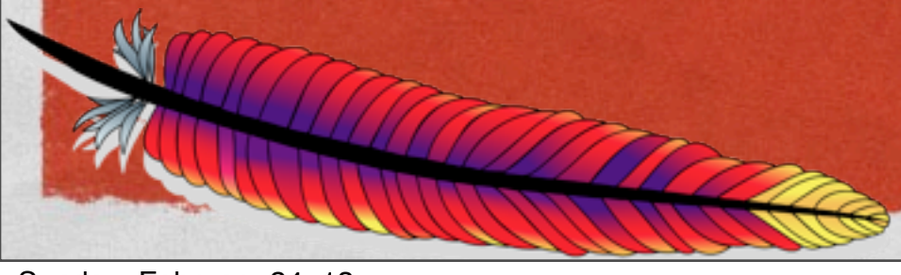
Level	Description	Example
`emerg`	Emergencies - system is unusable.	"Child cannot open lock file. Exiting"
`alert`	Action must be taken immediately.	"getpwuid: couldn't determine user name from uid"
`crit`	Critical Conditions.	"socket: Failed to get a socket, exiting child"
`error`	Error conditions.	"Premature end of script headers"
`warn`	Warning conditions.	"child process 1234 did not exit, sending another SIGHUP"
`notice`	Normal but significant condition.	"httpd: caught SIGBUS, attempting to dump core in ..."
`info`	Informational.	"Server seems busy, (you may need to increase StartServers, or Min/MaxSpareServers)..."
`debug`	Debug-level messages	"Opening config file ..."



LOGLEVEL (2.4)

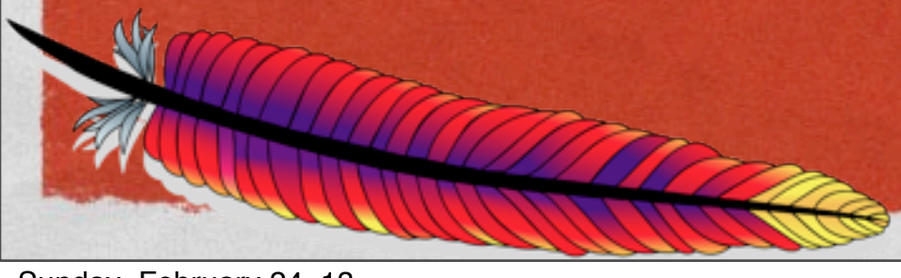
- In 2.4 you can specify LogLevel per directory (ie, in <Directory> blocks
- Also, can specify LogLevel per module

```
LogLevel info ssl:warn
```



LOGLEVEL (2.4)

- 2.4 adds several new log levels
- This functionality eliminates the need for a separate RewriteLog

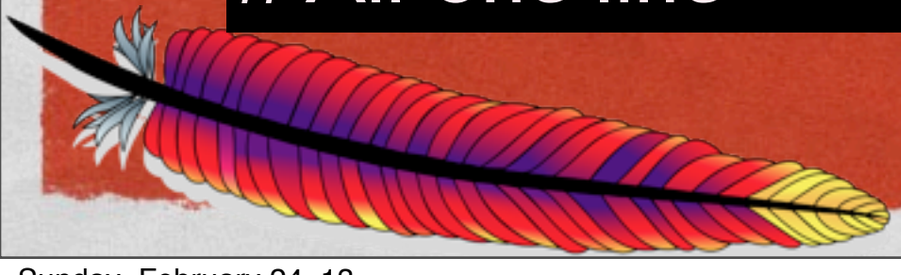


`trace1`	Trace messages	"proxy: FTP: control connection complete"
`trace2`	Trace messages	"proxy: CONNECT: sending the CONNECT request to the remote proxy"
`trace3`	Trace messages	"openssl: Handshake: start"
`trace4`	Trace messages	"read from buffered SSL brigade, mode 0, 17 bytes"
`trace5`	Trace messages	"map lookup FAILED: map=rewritemap key=keyname"
`trace6`	Trace messages	"cache lookup FAILED, forcing new map lookup"
`trace7`	Trace messages, dumping large amounts of data	"| 0000: 02 23 44 30 13 40 ac 34 df 3d bf 9a 19 49 39 15 |"
`trace8`	Trace messages, dumping large amounts of data	"| 0000: 02 23 44 30 13 40 ac 34 df 3d bf 9a 19 49 39 15 |"

ERRORLOGFORMAT (2.4)

- 2.4 also adds a configurable error log format (format is fixed in 2.2 and earlier)

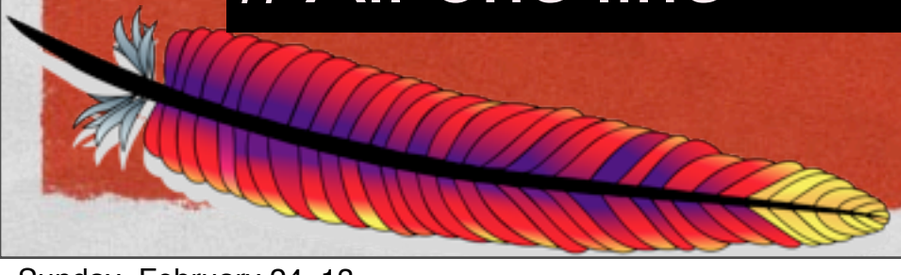
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T]
        %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
# All one line
```



ERRORLOGFORMAT (2.4)

Module

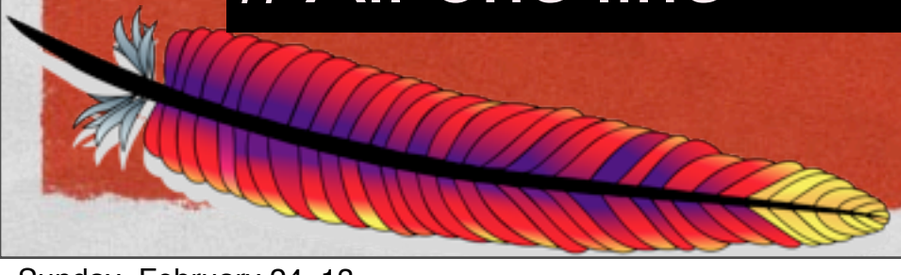
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T]
        %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
# All one line
```



ERRORLOGFORMAT (2.4)

Process ID, Thread ID

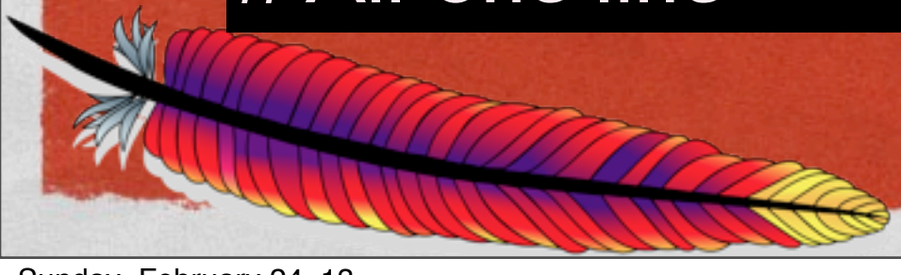
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T]
        %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
# All one line
```



ERRORLOGFORMAT (2.4)

The error message

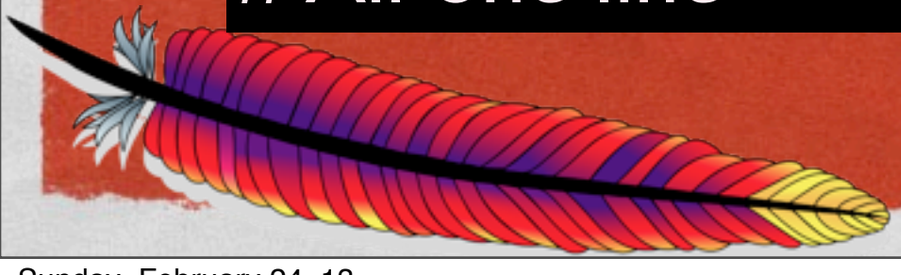
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T]
        %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
# All one line
```



ERRORLOGFORMAT (2.4)

Process ID, Thread ID

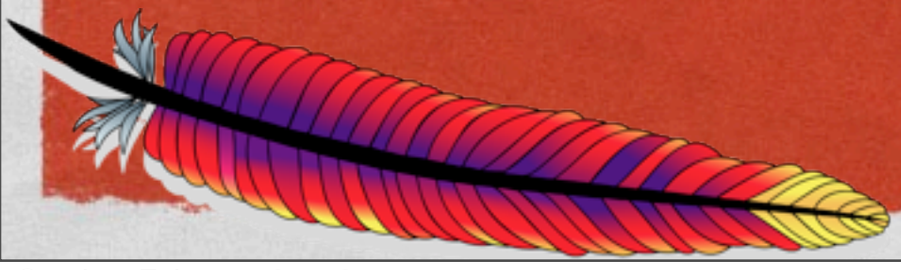
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T]
        %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
# All one line
```



ERRORLOGFORMAT (2.4)

Log ID

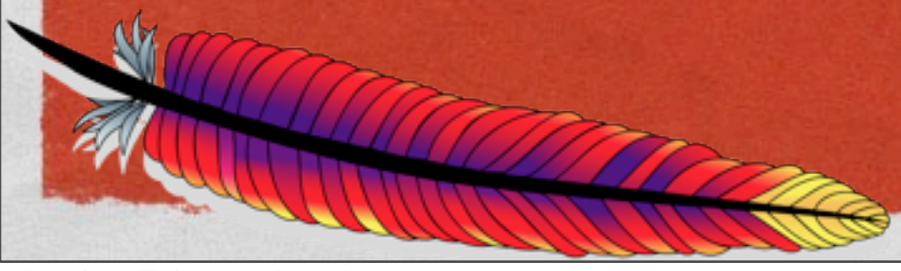
```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T ]
      %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i %L"
# All one line
```



TAIL -F

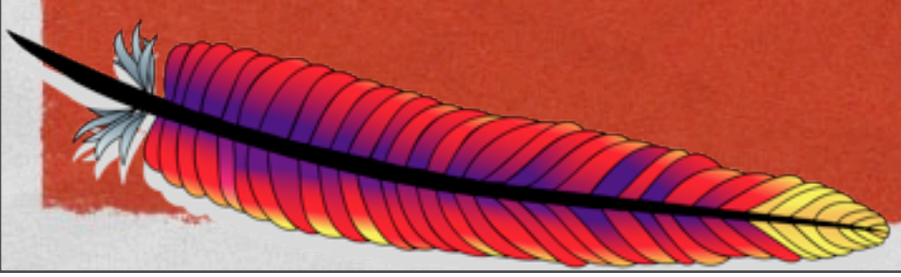
- Because the module name is right there in the log file:

```
tail -f /var/log/httpd/error_log | grep rewrite
```



MOD_LOG_FORENSIC

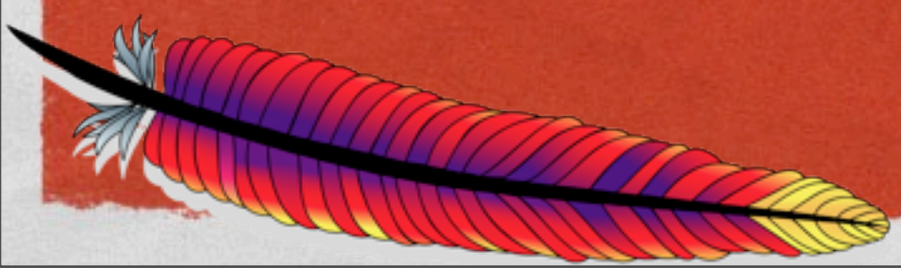
```
+yQtJf8CoAB4AAFNXBIEAAAAA|GET /manual/de/
images/down.gif HTTP/1.1|Host:localhost%3a8080|User-
Agent:Mozilla/5.0 (X11; U; Linux i686; en-US; rv%3a1.6)

...

-yQtJf8CoAB4AAFNXBIEAAAAA
```



MOD_LOGIO

- Adds a %I, %O log format variables to LogFormat

- %I = Input
- %O = Output
- Logs total bytes in/out, including headers



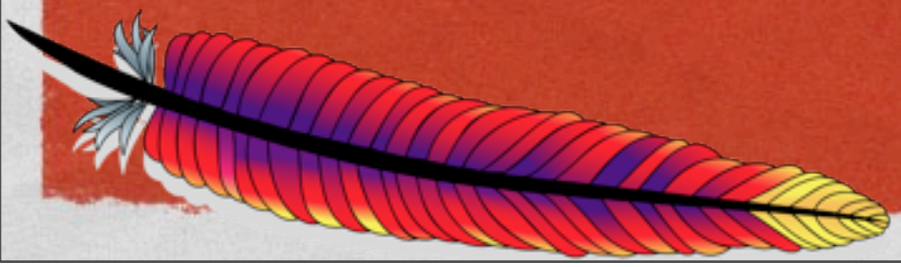
LOG ROTATION

- Logs get big

by nickandnora on Flickr

LOG ROTATION

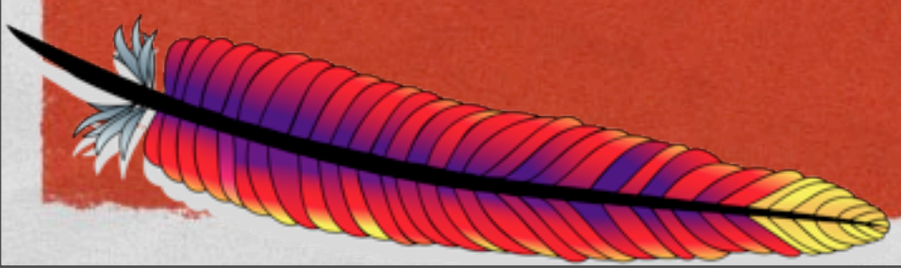
- Archive them off periodically, or when they reach a particular size
- Most OSes provide some kind of log rotation utility
- Requires a restart of the httpd process



ROTATELOGS

- rotatelogs script is a piped log handler that handles log rotation
- Can rotate by time (eg every day or week) or by size (eg when it reached 500M)

```
CustomLog "|bin/rotatelogs /var/logs/logfile 5M" common
```

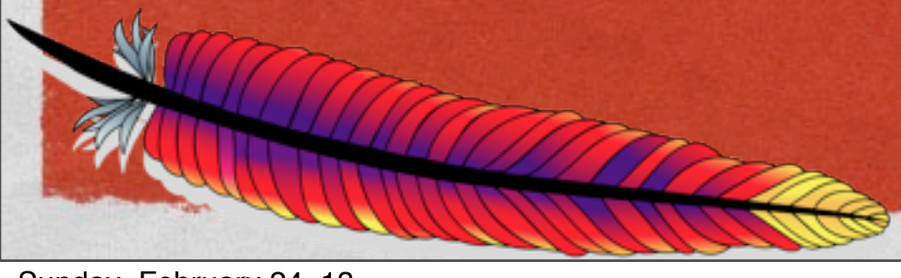


ROTATELOGS

```
CustomLog "|bin/rotatelogs /var/logs/logfile 86400" common
```

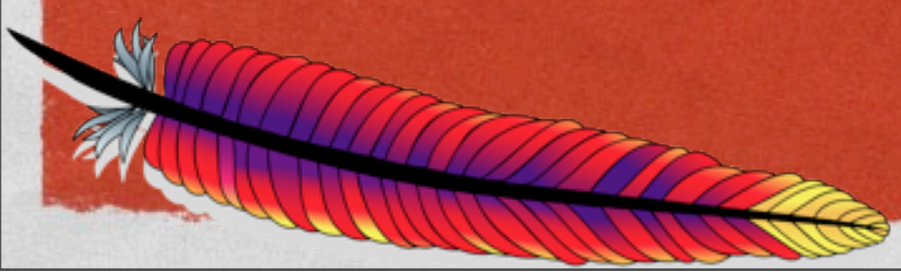
```
CustomLog "|bin/rotatelogs /var/logs/logfile.%Y.%m.%d 86400" common
```

```
ErrorLog "|bin/rotatelogs /var/logs/errorlog.%Y-%m-%d-%H_%M_%S 5M"
```



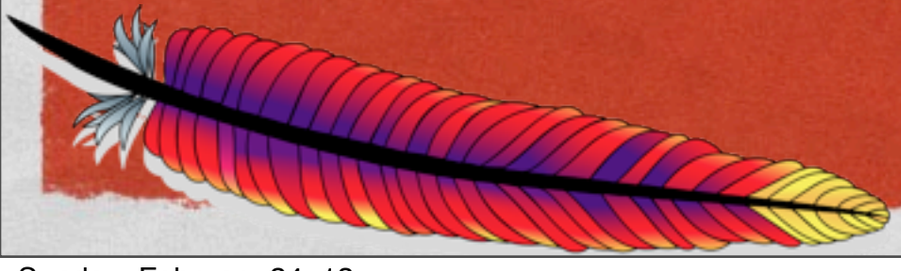
ROTATELOGS (2.4)

- -p program -- Run a program post-rotate
- -L linkname -- Creates a hard link to a consistently-named file so that you can `tail -F` that filename
- -f -- Create the file immediately, even if no request has been received yet



AUTHENTICATION

By DJ Empirical, on Flickr

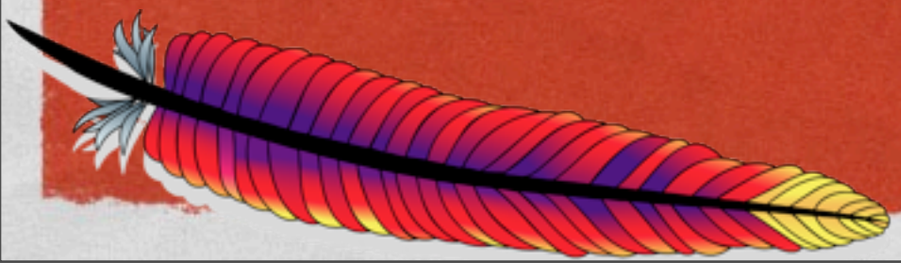


WHO ARE YOU?

- Passport or driver's license
- Retinal scan
- Username/password

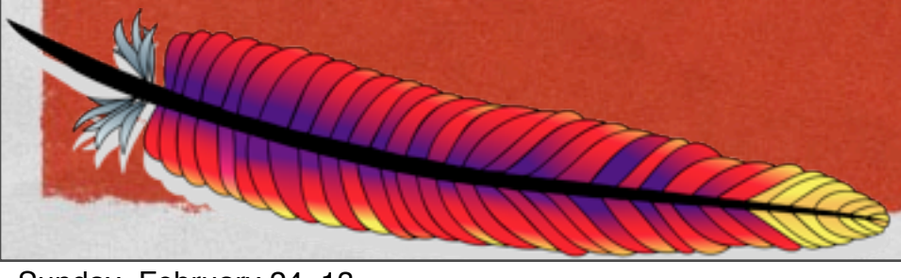
AUTHORIZATION

- Separate from *Authentication*
- Are you allowed to be here?
- Security clearance
- Invitation list
- Can be revoked, and this doesn't change your authentication



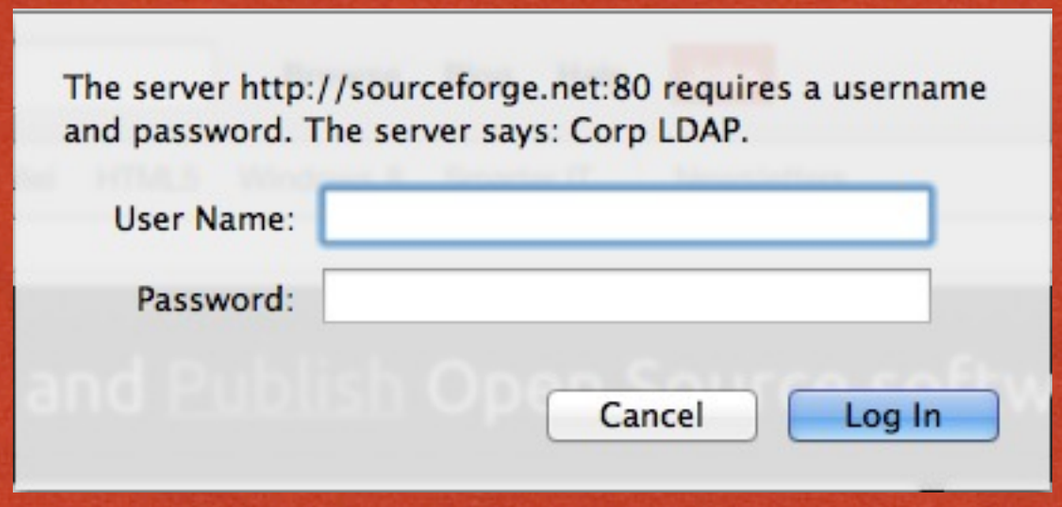
ACCESS CONTROL

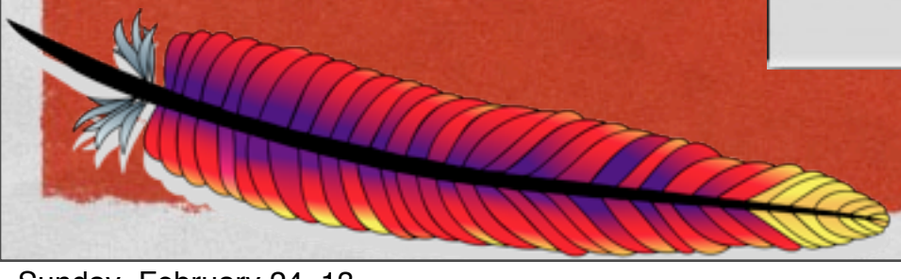
- Access control can be a separate thing
- Do you have a key?
- Is it during business hours?
- Do you know the secret handshake (overlap with Authentication)



BASIC AUTH

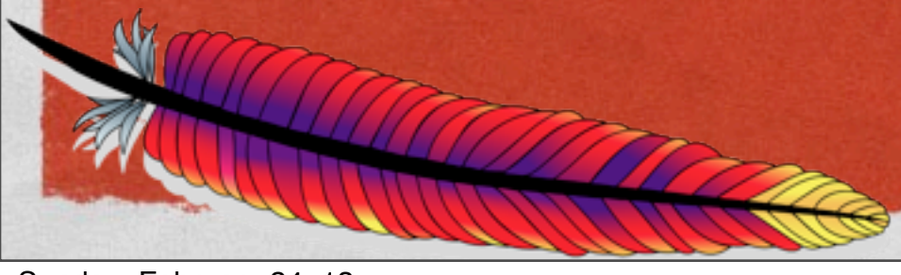
- Apache httpd implements HTTP Basic Authentication, which is a simple username/password protocol
- Browser challenges you for a username and password





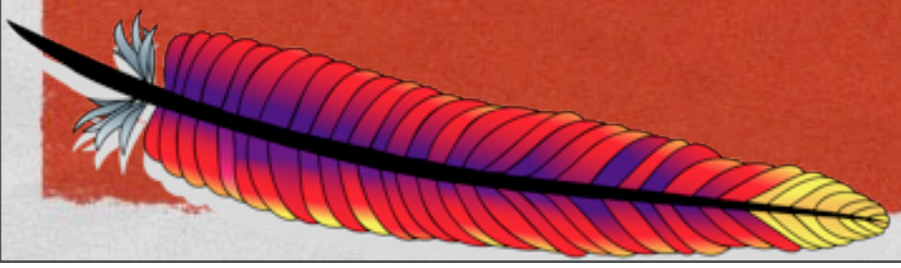
BASIC

- Credentials then passed plaintext with each subsequent request
- Not terribly secure



DIGEST AUTH

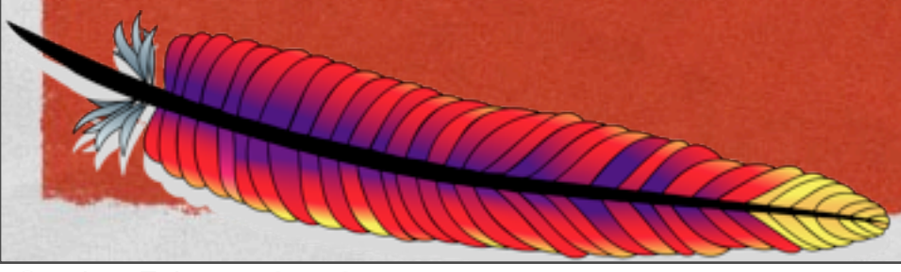
- Digest auth improves things by passing credentials hashed
- If you use HTTP auth, this is the preferred one
- Either one over SSL is a zillion times better



REQUIRE

- You can then Require a particular user or group

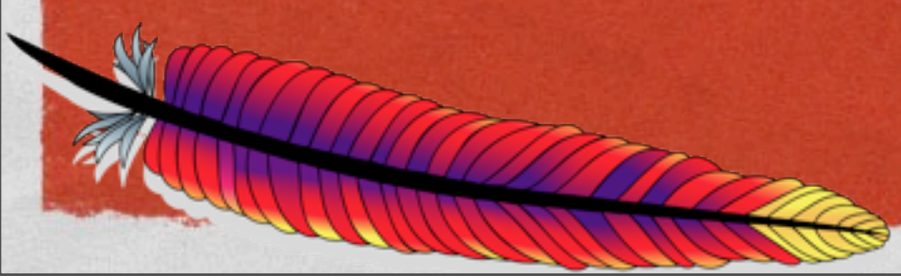
```
AuthType Basic
AuthName "Restricted Files"
# (Following line optional)
AuthBasicProvider file
AuthUserFile /usr/local/apache/passwd/passwords
Require user rbowen
```



HTPASSWD

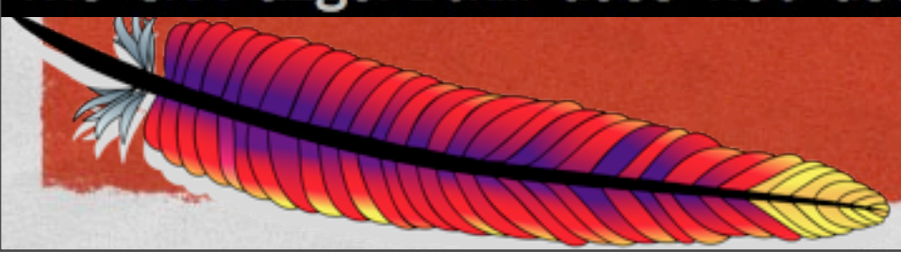
- Password file created using the htpasswd utility

```
# htpasswd -c /usr/local/apache/passwd/passwords
rbowen
New password: mypassword
Re-type new password: mypassword
Adding password for user rbowen
```



HTPASSWD

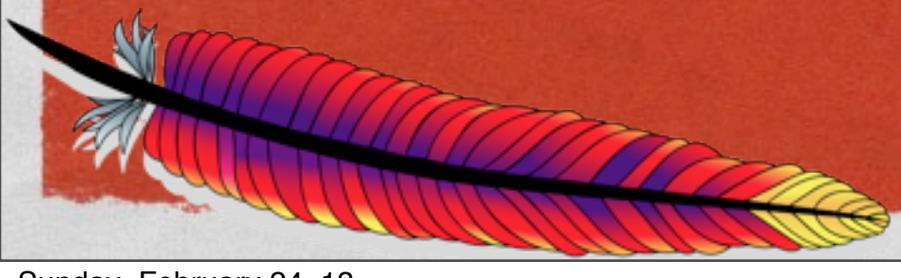
```
[rbowen@NCC1701:~]$ htpasswd -h
Usage:
        htpasswd [-cmdpsD] passwordfile username
        htpasswd -b[cmdpsD] passwordfile username password

        htpasswd -n[mdps] username
        htpasswd -nb[mdps] username password
 -c  Create a new file.
 -n  Don't update file; display results on stdout.
 -m  Force MD5 encryption of the password (default).
 -d  Force CRYPT encryption of the password.
 -p  Do not encrypt the password (plaintext).
 -s  Force SHA encryption of the password.
 -b  Use the password from the command line rather than prompting for it.
 -D  Delete the specified user.
On other systems than Windows, NetWare and TPF the '-p' flag will probably not work.
The SHA algorithm does not use a salt and is less secure than the MD5 algorithm.
```



LDAP

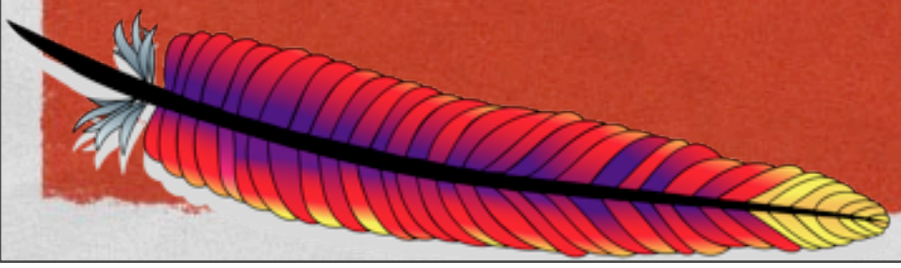
- Authn can also be against LDAP

```
AuthLDAPURL ldap://ldap.example.com/o=Example?uid
Require ldap-group cn=Administrators, o=Example
```



ROLL YOUR OWN

- These days most people do application-based authentication
- Username and password requested in web form, and processed by some back-end logic
- Often done very poorly, and the source of many security breaches

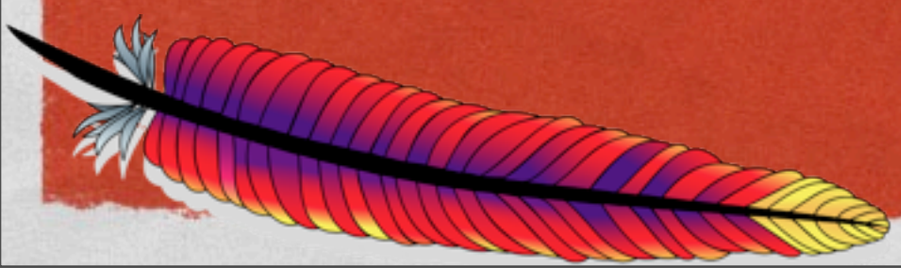


ACCESS CONTROL

By ~Brenda-Starr~, on Flickr

ACCESS CONTROL

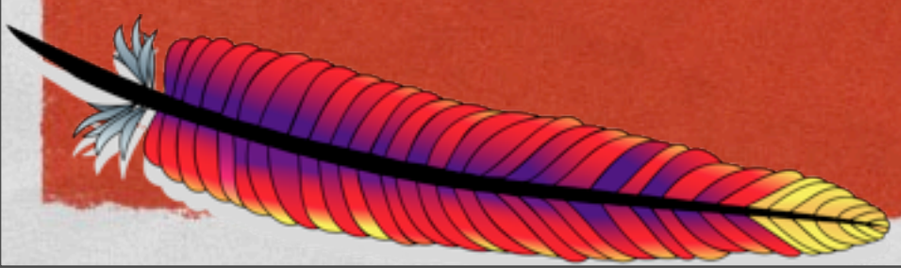
- Can be based on anything
- Can be related to authentication, but doesn't need to be
- Often related to client attributes, such as address



2.2 AND EARLIER

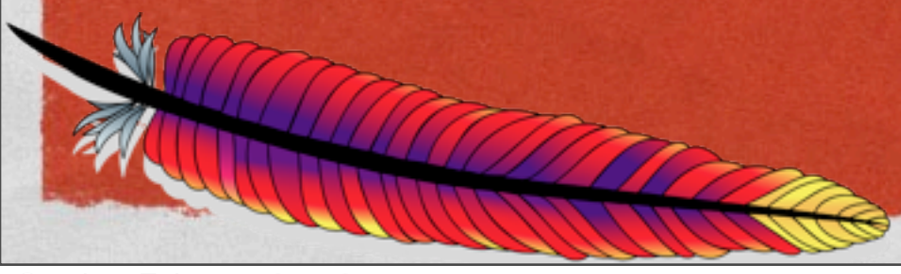
- Order, Allow and Deny
- Order specifes the order in which restrictions will be applied - allow,deny or deny,allow
- Then you can allow or deny requests

```
Order deny,allow
Order allow,deny
```



ALLOW

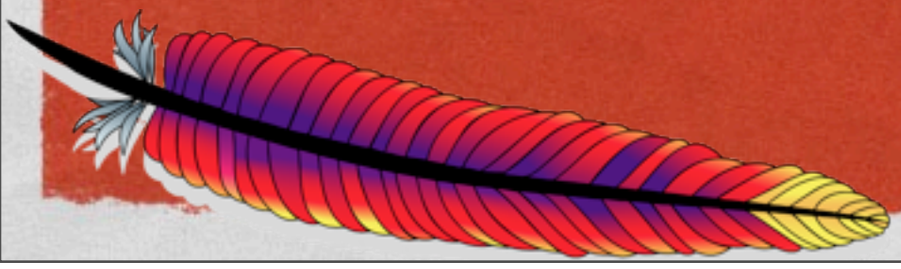
```
Allow from .example.com
Allow from 192.168
Allow from 10.0.4.12
Allow from 10.1.0.0/255.255.0.0
Allow from 2001:db8::a00:20ff:fea7:ccea/10
Allow from env=let_me_in
Allow from all
```



DENY

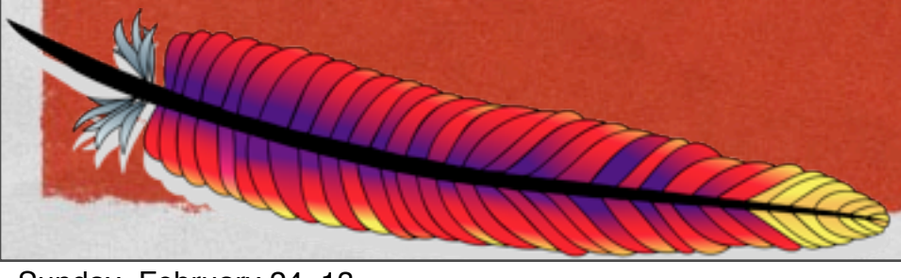
- Ditto

```
Deny from .example.com
Deny from 192.168
Deny from 10.0.4.12
Deny from 10.1.0.0/255.255.0.0
Deny from 2001:db8::a00:20ff:fea7:ccea/10
Deny from env=let_me_in
Deny from all
```



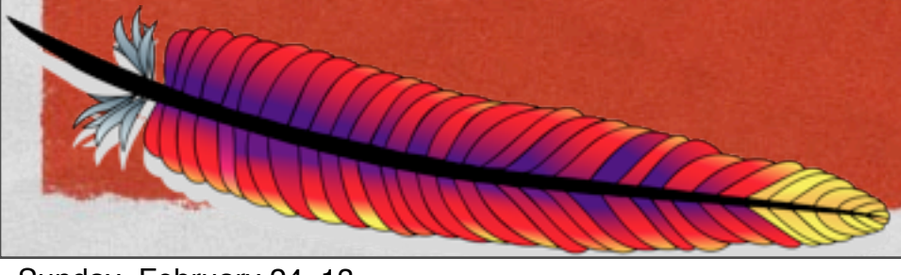
2.4 AND LATER

- Tuesday 4 p.m.–5 p.m.
- Access control in Apache httpd 2.4
- Be there



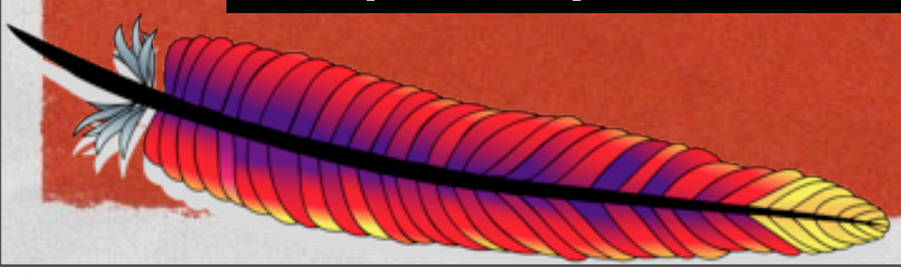
SIMPLER, YET MORE FLEXIBLE

- Order, Deny, and Allow go away
- Require does everything

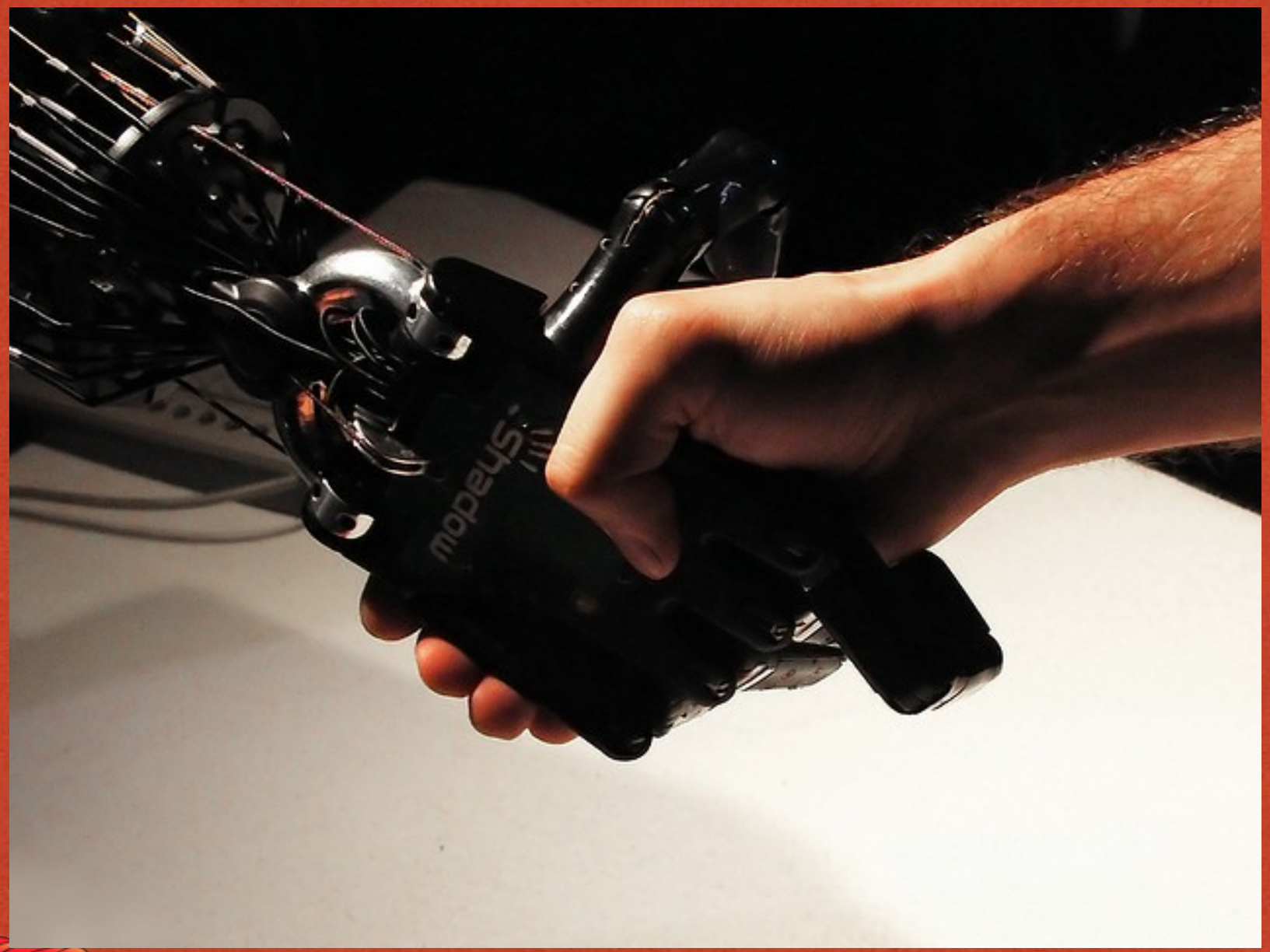


REQUIRE

```
Require all granted
Require all denied

Require env env-var [env-var] ...
Require method http-method [http-method] ...
Require expr expression

Require user userid [userid] ...
Require group group-name [group-name] ...
Require valid-user

Require ip 10 172.20 192.168.2
```



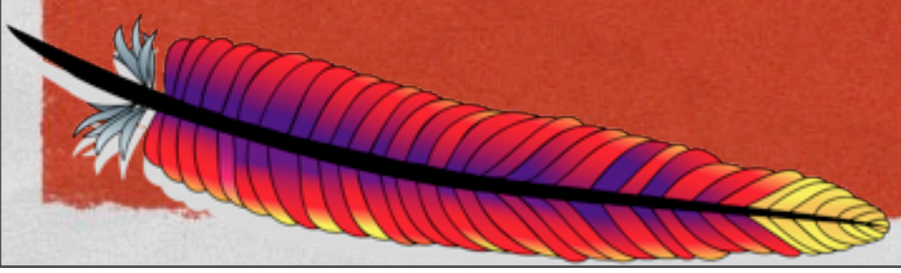
NEGOTIATION



By -sel on Flickr

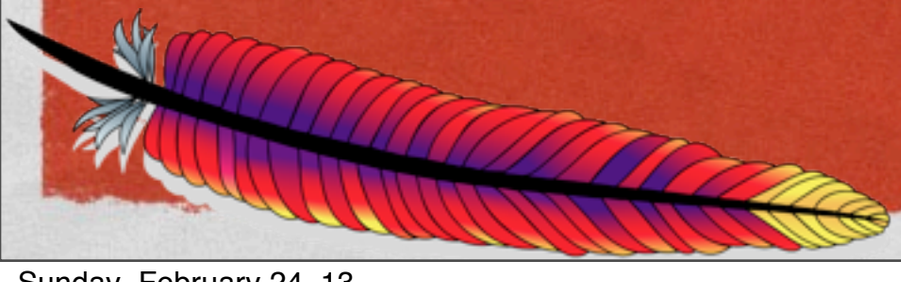
CONTENT NEGOTIATION

- Serve different content based on request (client) attributes
- Language
- File type



TYPE MAPS

- Defines:
  - what resource to negotiate
  - what to negotiate on
  - what files (or other content) represent that resource



```
# File: document.html.var
URI: document.html

Content-language: en
Content-type: text/html
URI: document.html.en

Content-language: fr
Content-type: text/html
URI: document.html.fr

Content-language: de
Content-type: text/html
URI: document.html.de
```

```
# File: document.html.var
URI: document.html

Content-language: en
Content-type: text/html
URI: document.html.en

Content-language: fr
Content-type: text/html
URI: document.html.fr

Content-language: de
Content-type: text/html
URI: document.html.de
```

Requested URI

```
# File: document.html.var
URI: document.html

Content-language: en
Content-type: text/html
URI: document.html.en

Content-language: fr
Content-type: text/html
URI: document.html.fr

Content-language: de
Content-type: text/html
URI: document.html.de
```

Request header on which to negotiate

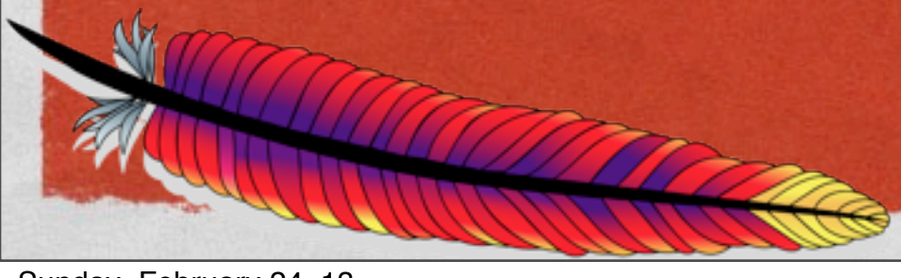
```
# File: document.html.var
URI: document.html

Content-language: en
Content-type: text/html
URI: document.html.en

Content-language: fr
Content-type: text/html
URI: document.html.fr

Content-language: de
Content-type: text/html
URI: document.html.de
```

Variant of resource to deliver

CONFIGURATION

AddHandler type-map .var

- Then the map file in this case would be called document.html.var (ie, the name of the resouce, plus .var)

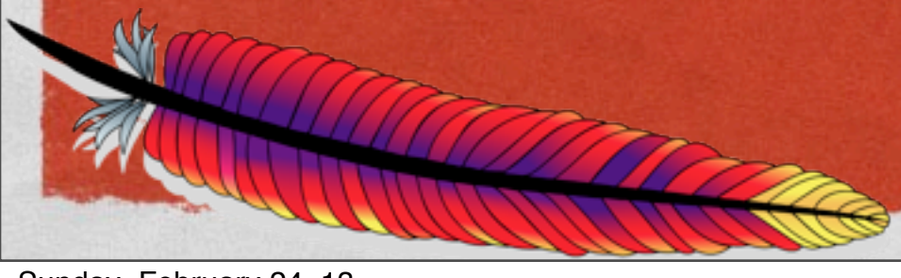


```
# File: document.html.var
URI: document.html

Content-language: en
Content-type: text/html
# Note that this is a relative URI:
URI: en/document.html.en

Content-language: fr
Content-type: text/html
URI: fr/document.html.fr

Content-language: de
Content-type: text/html
URI: de/document.html.de
```

```
Content-language: cs
Content-type: text/html; charset=UTF-8
Body:----------cs--
<!--#set var="CONTENT_LANGUAGE" value="cs"
--><!--#set var="TITLE" value="Objekt nenalezen!"
--><!--#include virtual="include/top.html" -->

    Požadované URL nebylo na tomto serveru nalezeno.

  <!--#if expr="-n v('HTTP_REFERER')" -->

    Zdá se, že odkaz na
    <a href="<!--#echo encoding="url" var="HTTP_REFERER" -->">odkazující
    stránce</a> je chybný nebo zastaralý. Informujte, prosím, autora
    <a href="<!--#echo encoding="url" var="HTTP_REFERER" -->">této stránky</a>
    o chybě.

  <!--#else -->

    Pokud jste zadal(a) URL ručně, zkontrolujte, prosím,
    zda jste zadal(a) URL správně, a zkuste to znovu.

  <!--#endif -->

<!--#include virtual="include/bottom.html" -->
----------cs--

Content-language: de
Content-type: text/html; charset=UTF-8
Body:----------de--
<!--#set var="CONTENT_LANGUAGE" value="de"
--><!--#set var="TITLE" value="Objekt nicht gefunden!"
--><!--#include virtual="include/top.html" -->

    Der angeforderte URL konnte auf dem Server nicht gefunden werden.

  <!--#if expr="-n v('HTTP_REFERER')" -->

    Der Link auf der
    <a href="<!--#echo encoding="url" var="HTTP_REFERER" -->">verweisenden
```

INLINE NEGOTIATED CONTENT

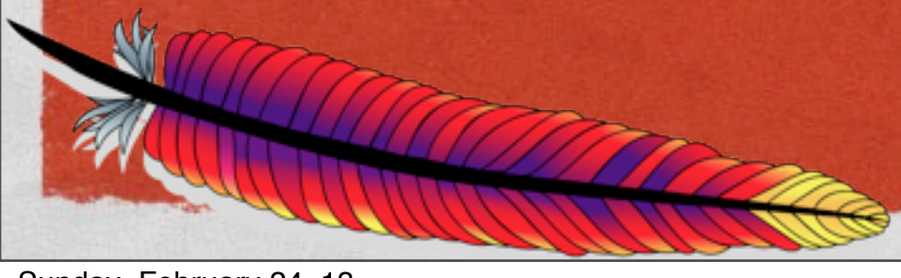
- Rather than pointing to a URI, the Body: line specifies the actual content to be served



MULTIVIEWS

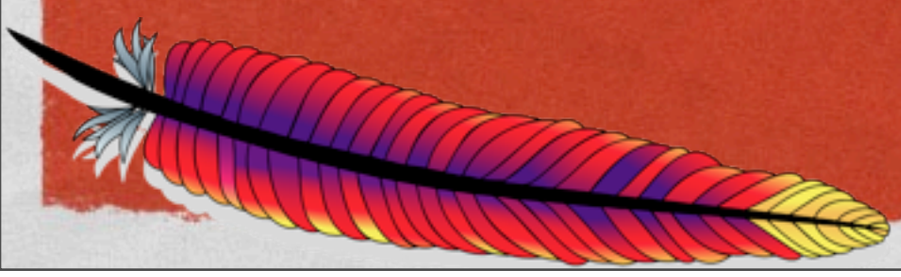
Options +MultiViews

- Instead of a typemap, the mapping is dynamic
- Directory is scanned for matching resources



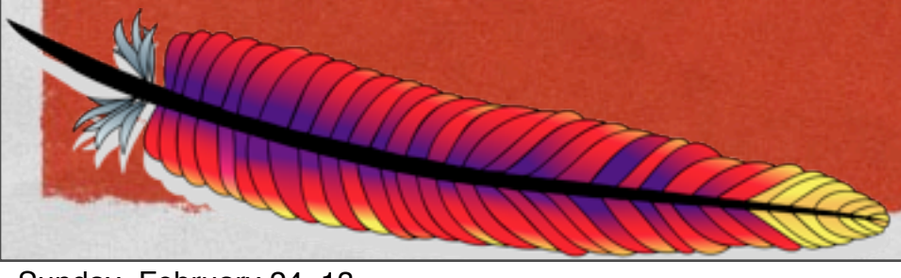
MULTIVIEWS

- A resource 'foo' is requested
- The directory is scanned for foo.* and a type-map is faked up with appropriate media types and content encoding information
- The resource is then negotiated



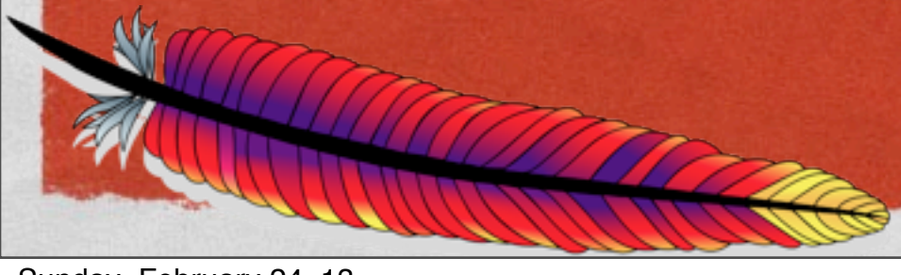
TYPE MAPS VS MULTIVIEWS

- Type maps is more hassle to set up
- Multiviews is much slower at request time



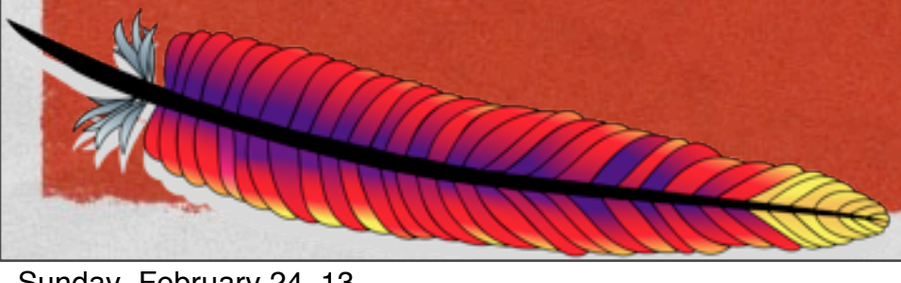
CLIENT CONFIGURATION

- Demo here

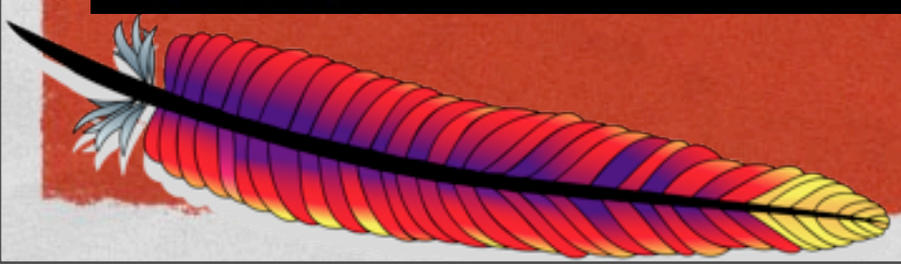


NEGOTIATED MANUAL

- httpd manual is provided in several languages
- Requests are negotiated by client language configuration

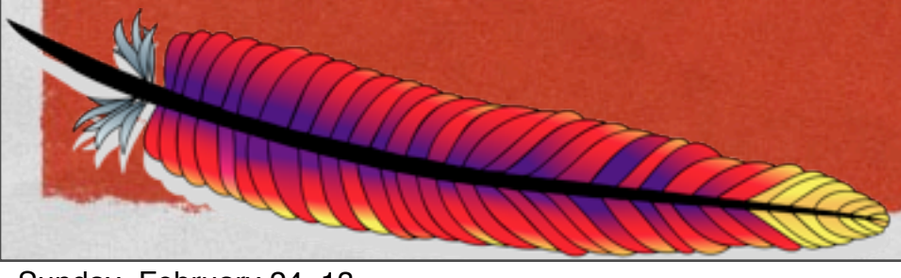


```
AliasMatch ^/manual(?:/(?:da|de|en|es|fr|ja|ko|pt-br|ru|tr|zh-cn))?(/.*)?$ "/usr/local/apache2/manual$1"
<Directory "/usr/local/apache2/manual">
    Options Indexes FollowSymlinks
    AllowOverride None
    Require all granted

    <Files *.html>
        SetHandler type-map
    </Files>
    # .tr is text/troff in mime.types!
    <Files *.html.tr.utf8>
        ForceType text/html
    </Files>

    AddLanguage da .da

    SetEnvIf Request_URI ^/manual/(da|de|en|es|fr|ja|ko|pt-br|ru|tr|zh-cn)/ prefer-language=$1
    RedirectMatch 301 ^/manual(?:/(da|de|en|es|fr|ja|ko|pt-br|ru|tr|zh-cn)){2,}(/.*)?$ /manual/$1$2

    LanguagePriority en da de es fr ja ko pt-br ru tr
    ForceLanguagePriority Prefer Fallback
</Directory>
```



NEGOTIATED ERROR DOCS

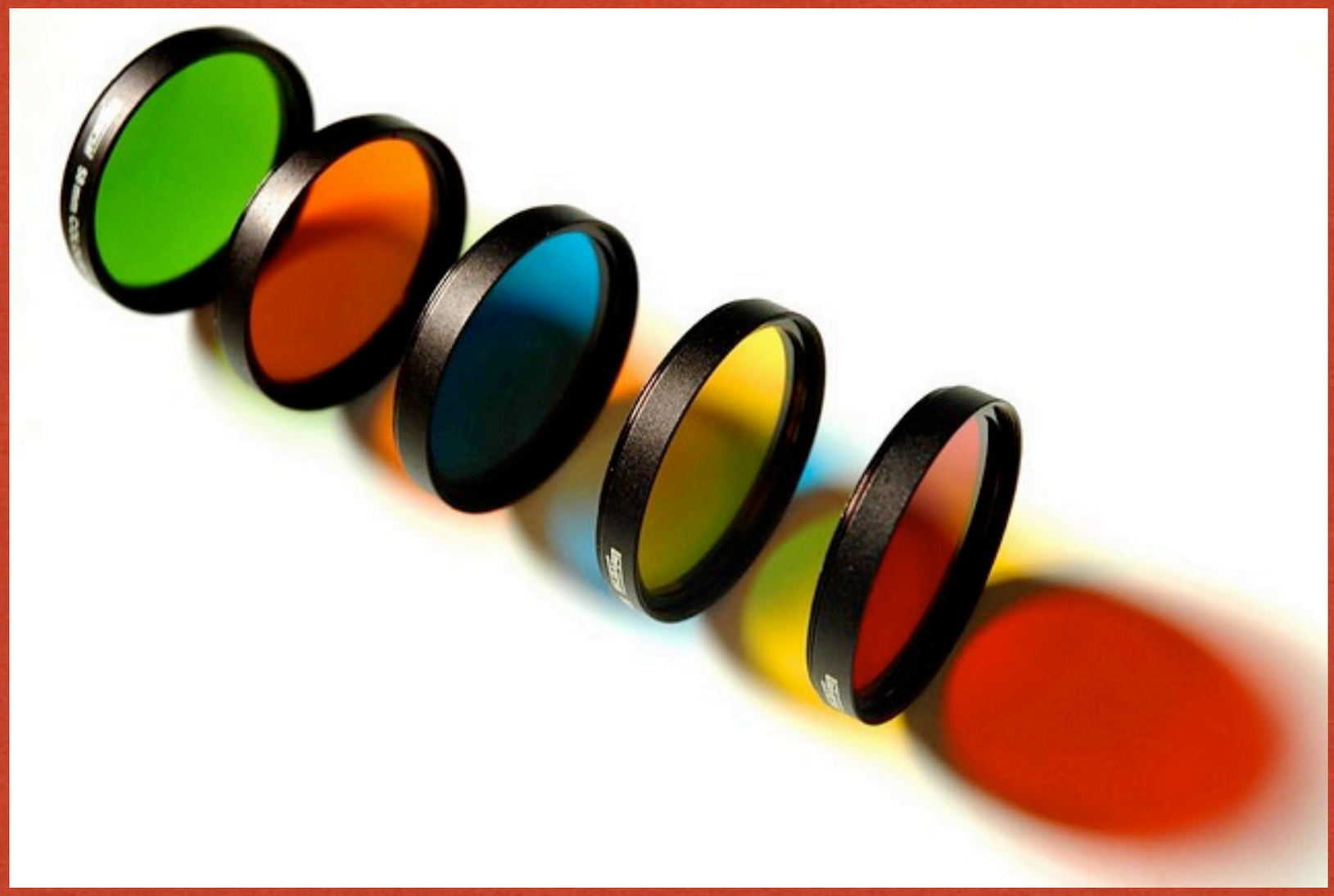
- Error messages are served in the language configured in the requesting client
- Messages are negotiated in-line content



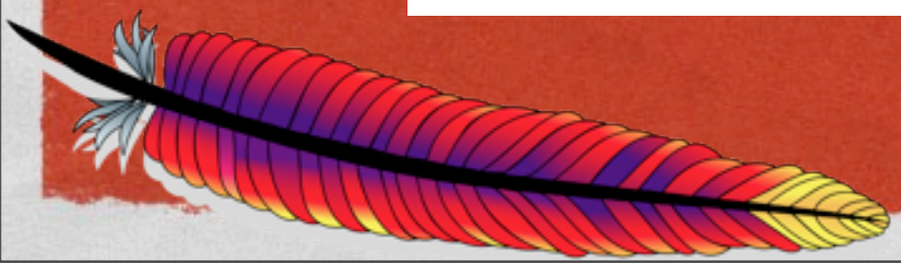
```
Alias /error/ "/usr/local/apache2/error/"

<Directory "/usr/local/apache2/error">
    AllowOverride None
    Options IncludesNoExec
    AddOutputFilter Includes html
    AddHandler type-map var
    Require all granted
    LanguagePriority en cs de es fr it ja ko nl pl pt-br ro sv tr
    ForceLanguagePriority Prefer Fallback
</Directory>

ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
```

```
Content-language: sv
Content-type: text/html; charset=UTF-8
Body:----------sv--
<!--#set var="CONTENT_LANGUAGE" value="sv"
--><!--#set var="TITLE" value="Tj&auml;nsten ej tillg&auml;nglig!"
--><!--#include virtual="include/top.html" -->

    Servern &auml;r f&ouml;r tillf&auml;llet of&ouml;rm&ouml;gen att
    utf&ouml;ra din f&ouml;rfr&aring;gan p&aring; grund av underh&aring;ll
    eller kapacitetsbegr&auml;nsningar. V&auml;nligen f&ouml;rs&ouml;k
    igen senare.

<!--#include virtual="include/bottom.html" -->
----------sv--

Content-language: tr
Content-type: text/html; charset=UTF-8
Body:----------tr--
<!--#set var="CONTENT_LANGUAGE" value="tr"
--><!--#set var="TITLE" value="Hizmet sunulamıyor!"
--><!--#include virtual="include/top.html" -->

    Sunucu, bakım gerektiren çeşitli sorunlardan ötürü,
    bir süreliğine taleplerinize yanıt veremiyor.
    Lütfen daha sonra tekrar deneyin.

<!--#include virtual="include/bottom.html" -->
HTTP_SERVICE_UNAVAILABLE.html.var
```

FILTERS

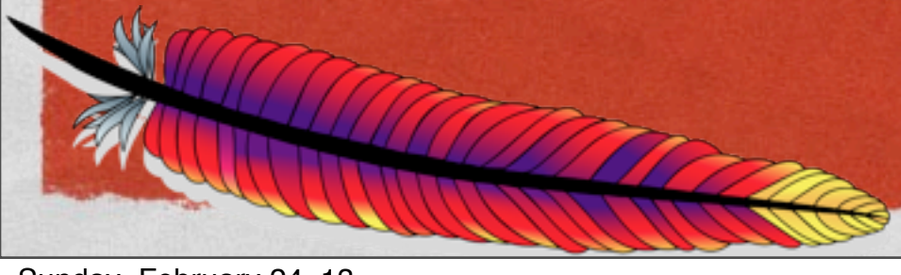


By Ramm Balmur, on Flickr



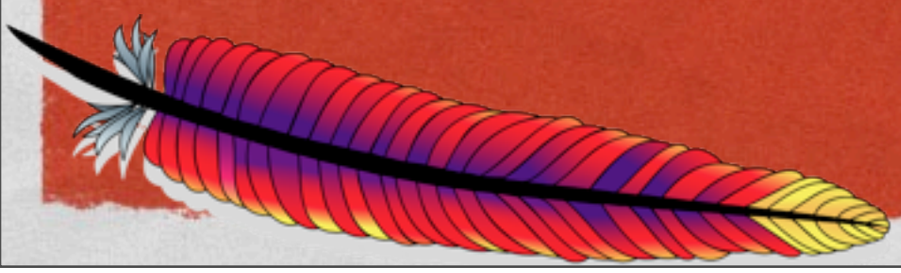
FILTERS

- Modify content as it passes through
- Can stack multiple filters to produce an aggregate result



MOD_SPELING

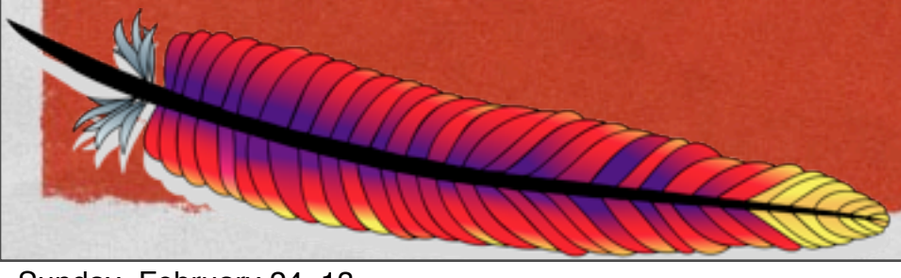
- Corrects simple URL typos
- Letter transposition
- Upper/Lower case
- o/0, 1/i/l, 3/E, etc



MOD_SPELING

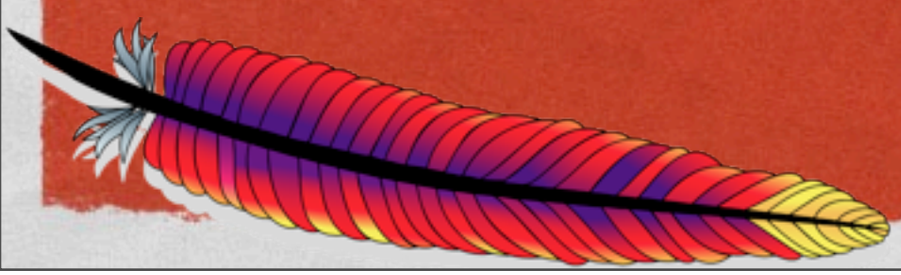
```
LoadModule speling_module modules/mod_speling.so

CheckSpelling On
```

```
CheckCaseOnly on
```



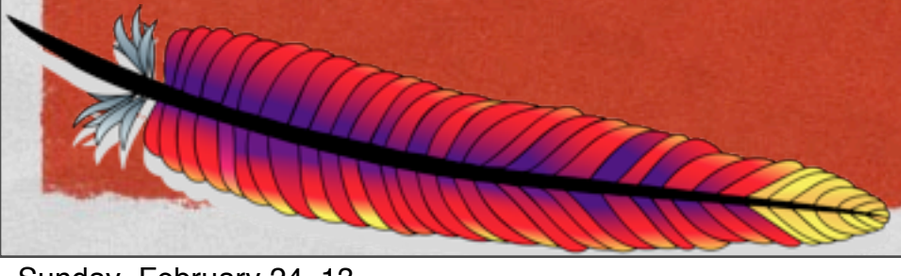
DEFLATE

- gzip content compression
- Client decompresses on arrival
- Much faster delivery, and so results in lower server load, in spite of computational effort required to compress



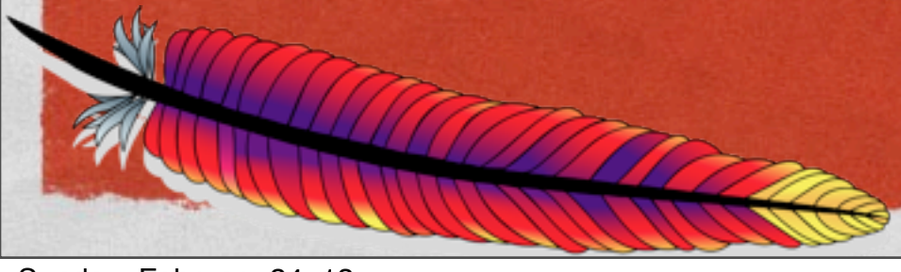
DEFLATE

```
AddOutputFilterByType DEFLATE \
                      text/html text/plain text/xml
```



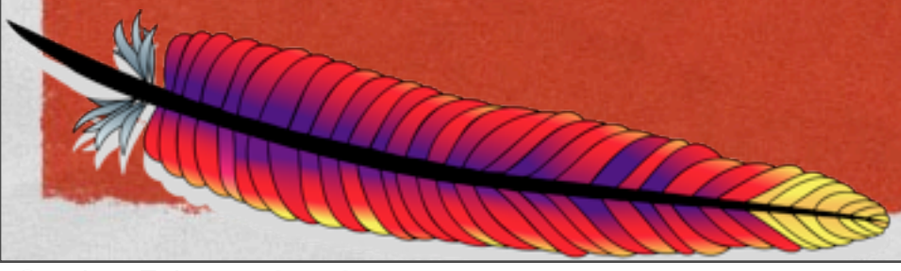
LOGGING

```
DeflateFilterNote ratio

LogFormat '"%r" %b (%{ratio}n) "%{User-agent}i"' deflate
CustomLog logs/deflate_log deflate
```



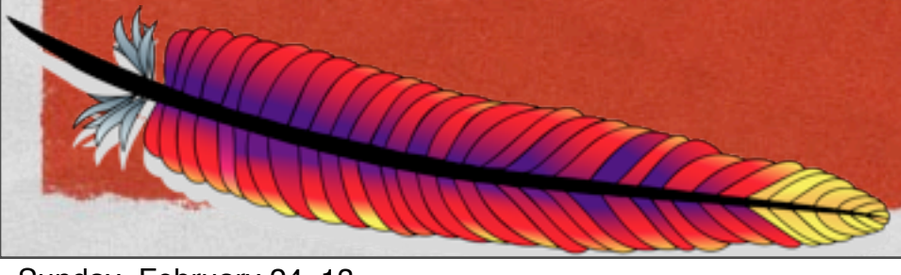
LOGGING

```
DeflateFilterNote Input instream
DeflateFilterNote Output outstream
DeflateFilterNote Ratio ratio

LogFormat \
    '"%r" %{outstream}n/%{instream}n (%{ratio}n%%)' deflate
CustomLog logs/deflate_log deflate
```



INCLUDE

- Server-side includes
- Macros placed inline in HTML pages which are evaluated at request time

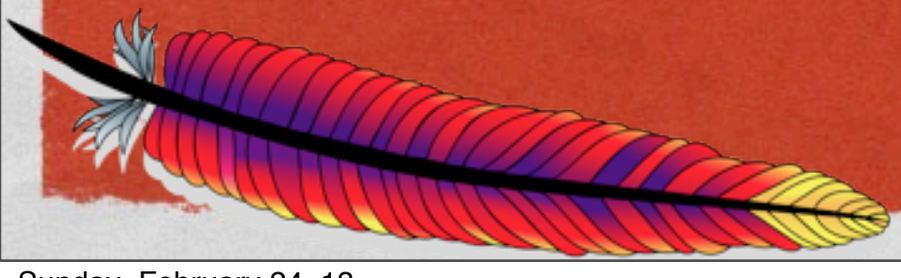


<!--# -->

```
<!--#echo var="DATE_LOCAL" -->
```

- Replaced at request time with:

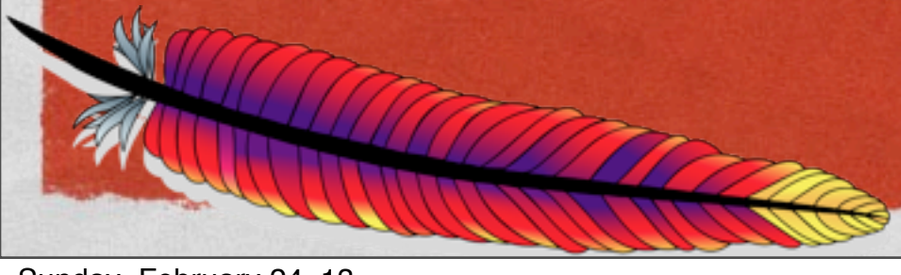
```
Tuesday, 15-Jan-2013 19:28:54 EST
```



CONFIG

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

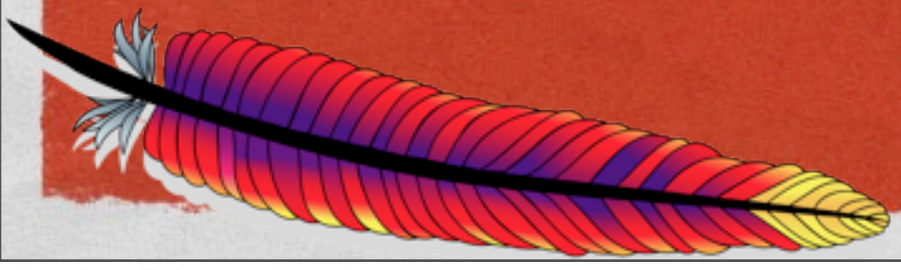
XBitHack on



INCLUDE

```
<!--#include virtual="/footer.html" -->
```

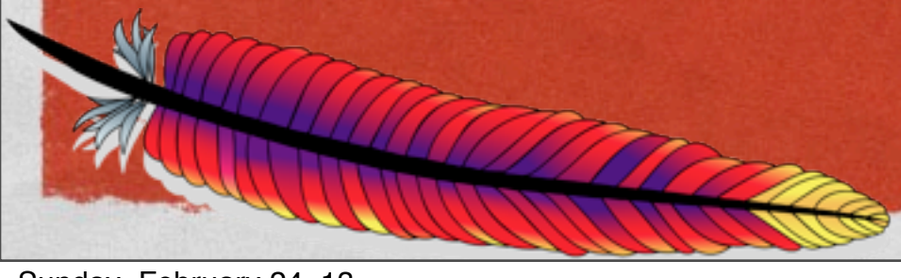
```
<pre>
<!--#exec cmd="ls" -->
</pre>
```



RATELIMIT

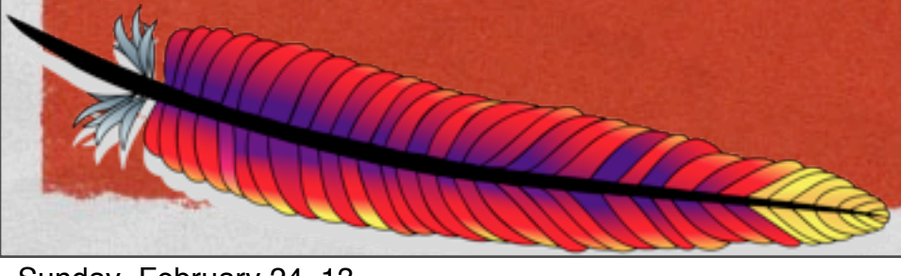
- Slow down a particular directory resource so that it doesn't overwhelm your available bandwidth.

```
<Location /downloads>
    SetOutputFilter RATE_LIMIT
    SetEnv rate-limit 400
    # KB/s
</Location>
```



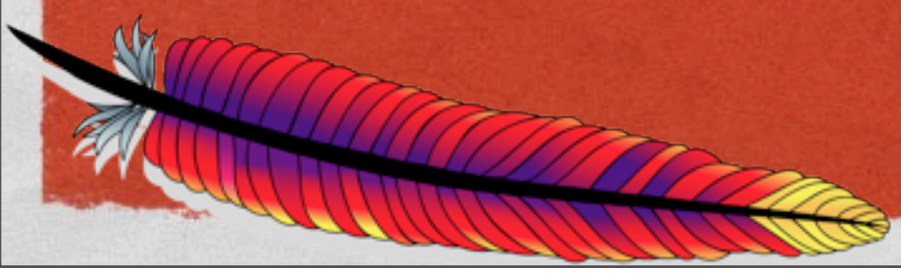
SUBSTITUTE

```
<Location />
    AddOutputFilterByType SUBSTITUTE text/html
    Substitute s/foo/bar/ni
</Location>
```



SUBSTITUTE

```
ProxyPass /blog/ http://internal.blog.example.com
ProxyPassReverse /blog/ http://internal.blog.example.com/

Substitute \
  "s|http://internal.blog.example.com/|http://www.example.com/blog/|i"
```

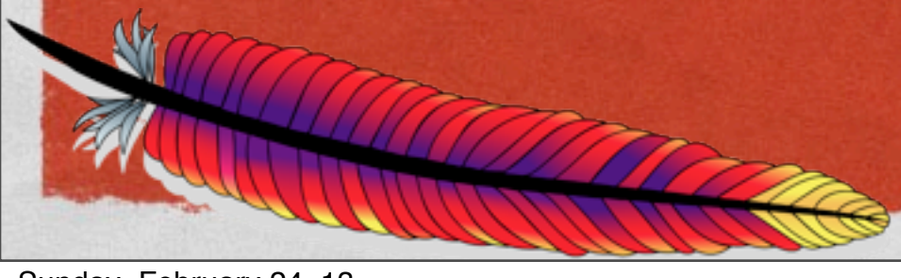


SECURITY ISSUES

By ~Brenda-Starr~ on Flickr

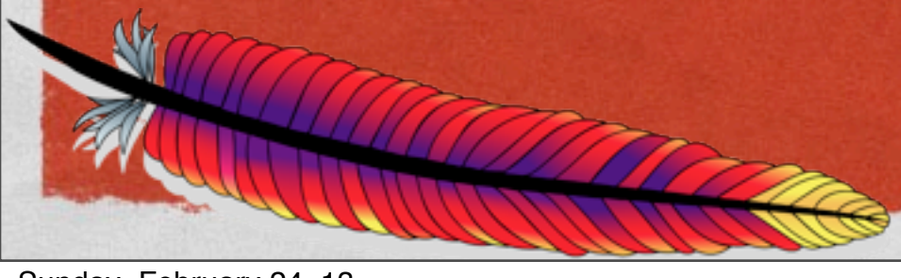
USER/GROUP

- The User and Group directive define what permissions the server process has
- Ensure that that user, and that group, is impotent to do harm



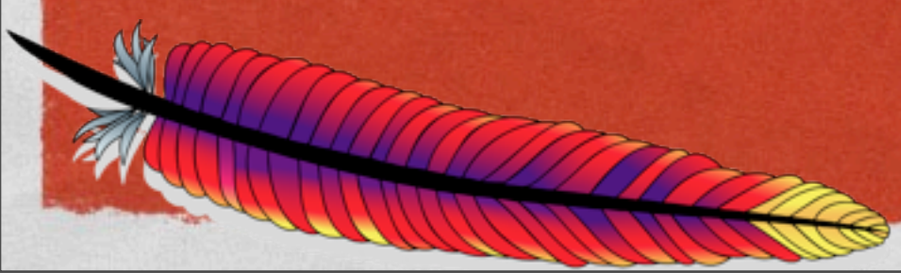
FILE PERMISSIONS

- NO FILES SHOULD BE OWNED BY THE SERVER USER
- Content files owned by the server user are vulnerable to be overwritten by any compromised php/cgi/whatever
- Correct file permissions don't guarantee safety, but they are a required first line of defence



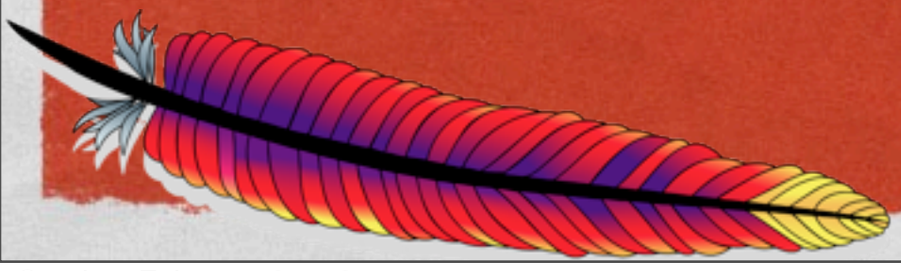
SO, WHO SHOULD OWN FILES?

- Config files should be owned by root, and only readable/writable by root
- Content files should be owned by the content author (you?) or by root
- Files should be 644. Directories should be 755.



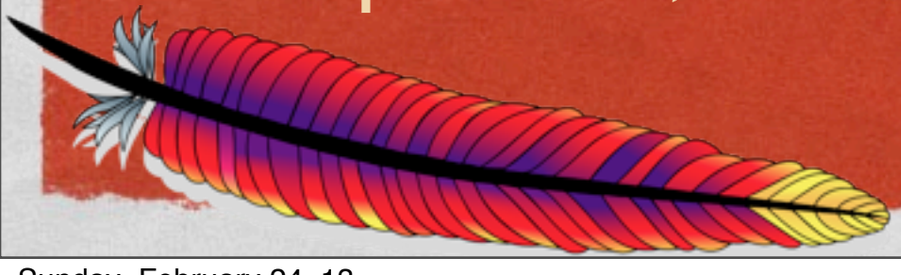
WHAT ABOUT ...

- Sometimes, files must be writable by the server
- Try to find a way around it
- If you can't, find the minimal number of files, and the minimal permissions



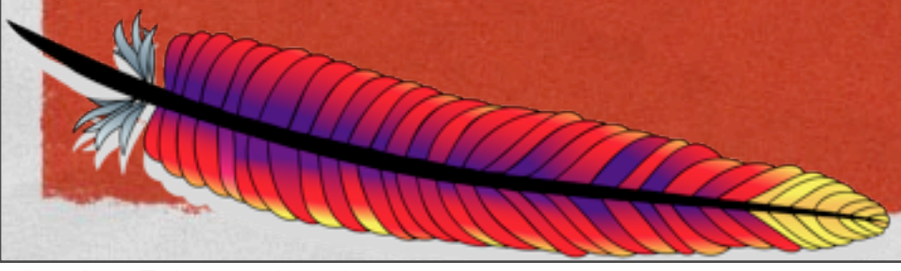
PREVENTING DOS ATTACKS

- KeepAliveTimeout should be set as low as possible, or KeepAlive turned off entirely
- In 2.4, you can set KeepAliveTimeout in ms
- Set MaxRequestWorkers to balance between maximum number of workers without exhausting server resources
- If possible, use a threaded MPM

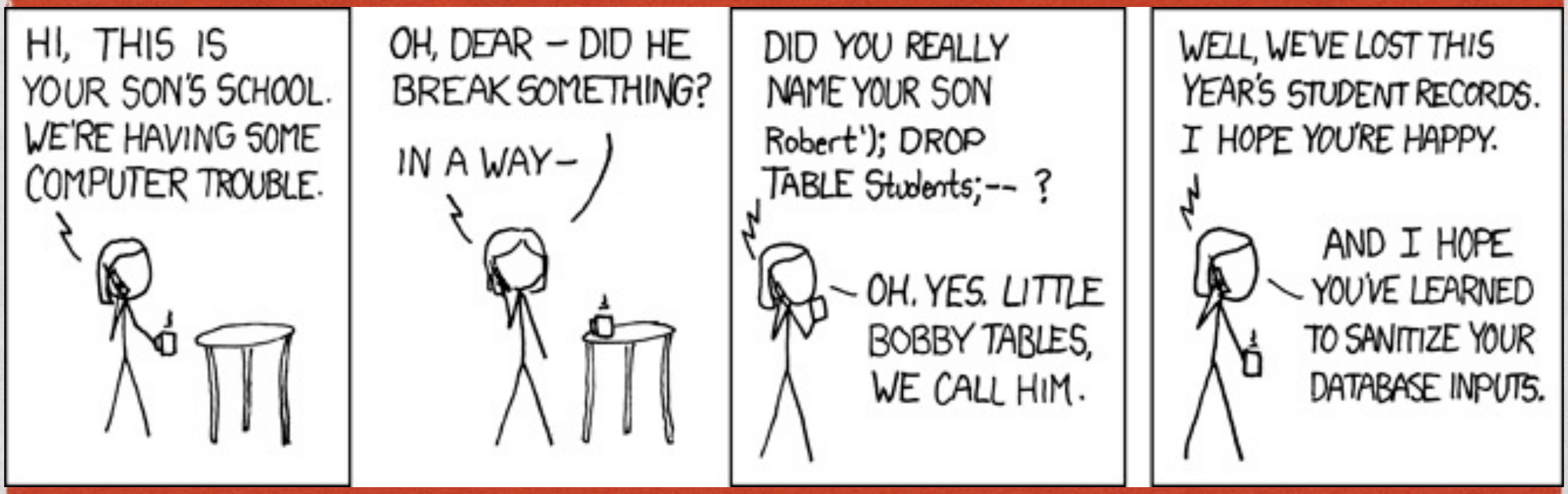


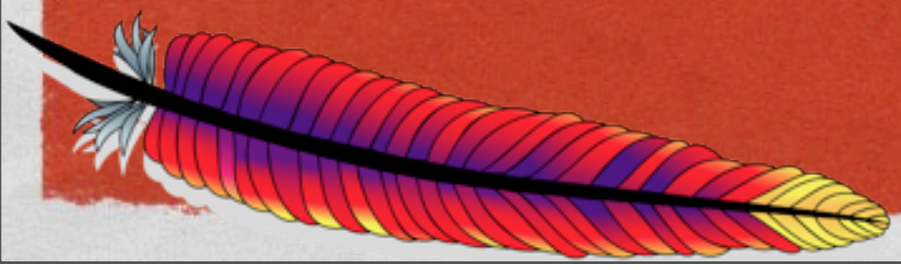
DYNAMIC CONTENT SECURITY

- Third party web apps the #1 source of server exploits
- Keep up on security reports and update immediately
- Be aware of common security exploits



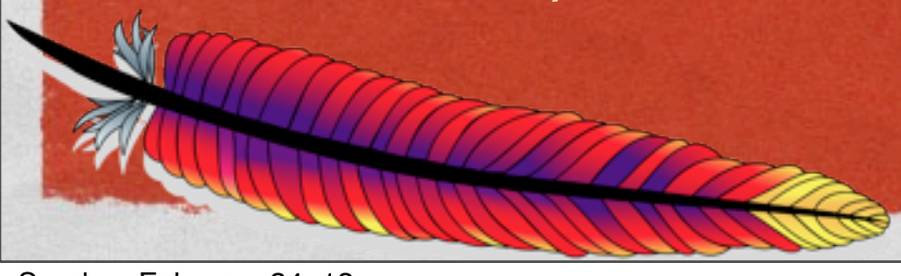
SQL INJECTION





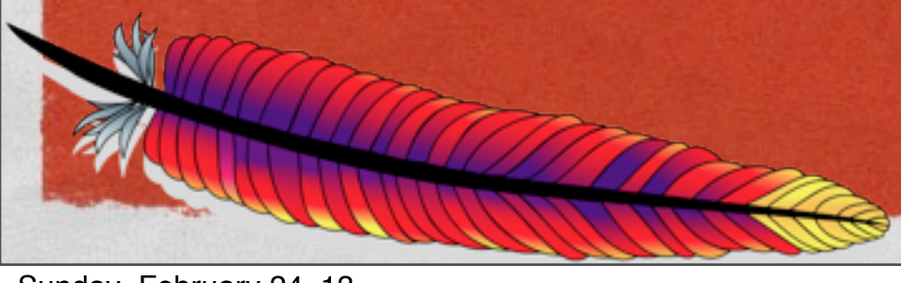
BOOKS

- There are *lots* of books about this
- Most of them are outdated, because they focus on specific techniques
- Recommended: Essential PHP Security by Chris Shiflett. Focuses on PHP, but covers concepts rather than specific code
- Also: Simson Garfinkel's web security book (2012 edition)



ATTEND IGOR'S TALK

- Wednesday 11:45 a.m.–12:30 p.m.
- SSL: "Securing" the Web with Apache

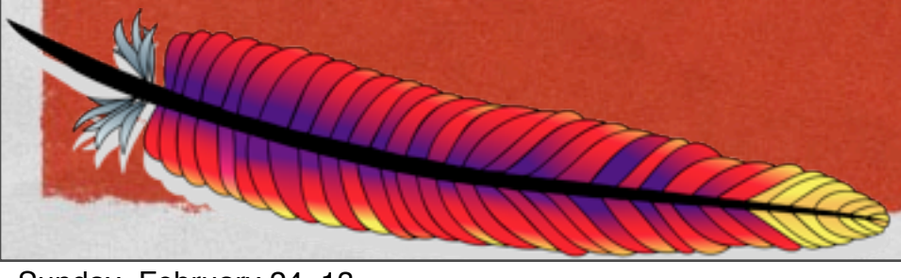


PERFORMANCE

By Armchair Aviator on Flickr

DEFAULTS

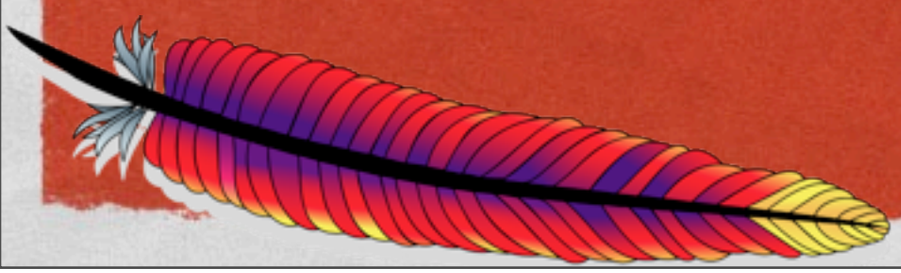
- We try to have sane defaults
- There's a lot you can do to make it slower



DNS

- Try to avoid DNS lookups
- HostNameLookups Off
- Name-based access control

```
Deny from example.com
# Or, in 2.4
# Require not example.com
```



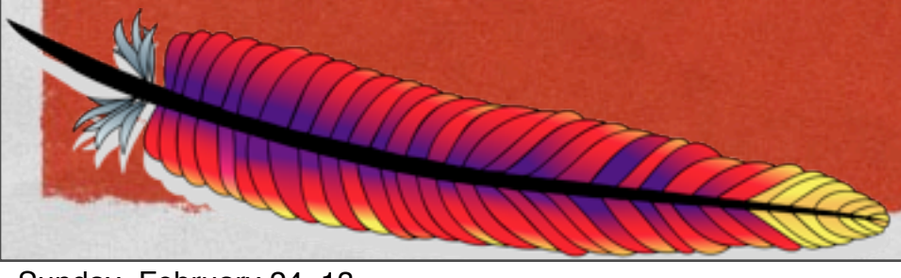
SYMLINKS

```
Options -FollowSymlinks
```

OR

```
Option SymlinksIfOwnerMatch
```

- Has to stat each directory in the path to the file, and the file itself, to see if it's a symlink
- stat isn't cached, so occurs with every request

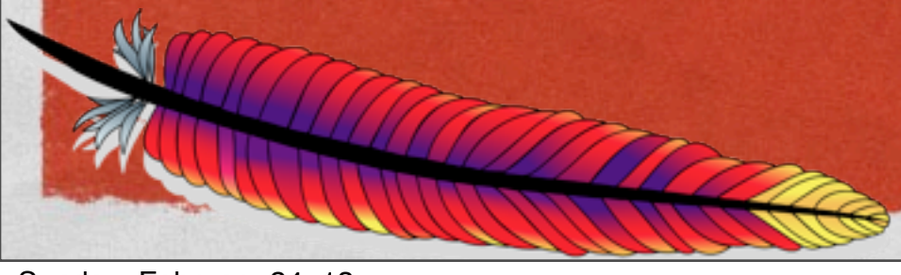


ALLOWOVERRIDE

- .htaccess files are the performance killer

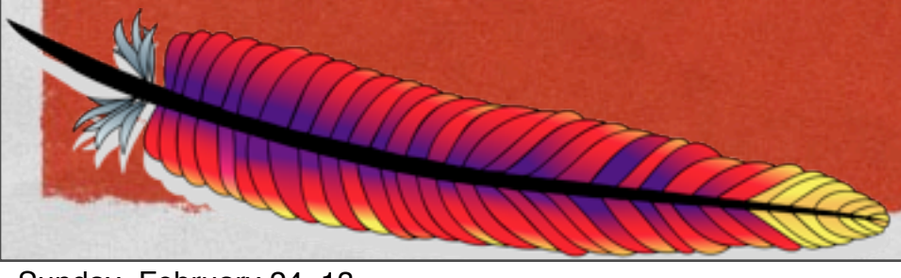
- If AllowOverride is on, httpd will have to `stat .htaccess` in each directory in the path to any requested resource, for every request. (Even if there's no .htaccess file there - it has to check.)

- This is not cached. Happens every request.



ALLOWOVERRIDE

- Disable .htaccess files wherever and whenever possible
- AllowOverride None
- Move configurations to <Directory> blocks in the main config instead of in .htaccess files



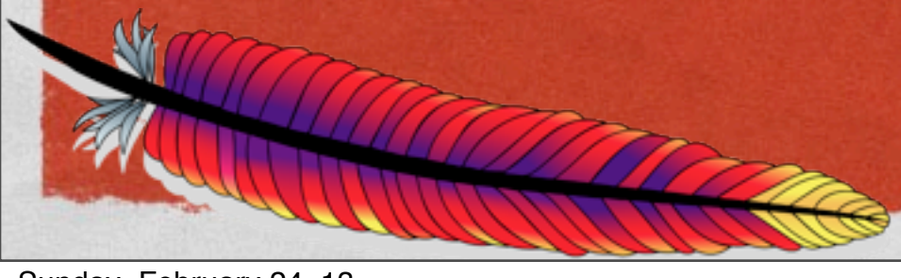
DIRECTIVE ORDERING

- Put stuff in the most likely order, so that you can avoid unnecessary processing

```
RewriteRule ^/products/widgets/grobnit.html /out_of_stock.html [R]
RewriteRule ^/index.html /index.php [R]
```

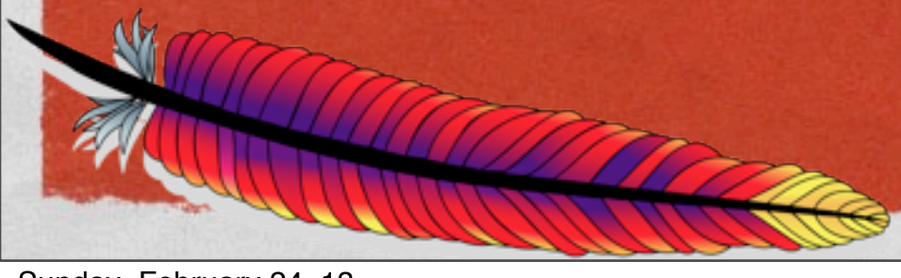
vs

```
RewriteRule ^/index.html /index.php [R]
RewriteRule ^/products/widgets/grobnit.html /out_of_stock.html [R]
```



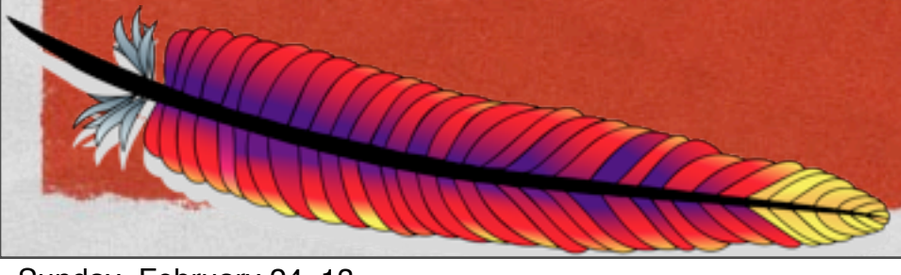
CONTENT NEGOTIATIO

- Very cool feature
- Avoid it if you don't actually need it
- Use a Type map rather than MultiViews if possible



MODULES

- You probably have modules loaded that you're not using
- They're taking up memory space, and may be taking processing time, unecessarily



```
[rbowen@NCC1701:local/apache2]$ ./bin/httpd -M
Loaded Modules:
 core_module (static)
 so_module (static)
 http_module (static)
 authn_file_module (shared)
 authn_dbm_module (shared)
 authn_anon_module (shared)
 authn_dbd_module (shared)
 authn_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 authz_dbm_module (shared)
 authz_owner_module (shared)
 authz_dbd_module (shared)
 authz_core_module (shared)
 auth_digest_module (shared)
 allowmethods_module (shared)
 file_cache_module (shared)
 socache_shmcb_module (shared)
 socache_dbm_module (shared)
 socache_memcache_module (shared)
 watchdog_module (shared)
 dbd_module (shared)
 dumpio_module (shared)
 buffer_module (shared)
 ratelimit_module (shared)
 reqtimeout_module (shared)
 request_module (shared)
 include_module (shared)
 filter_module (shared)
```

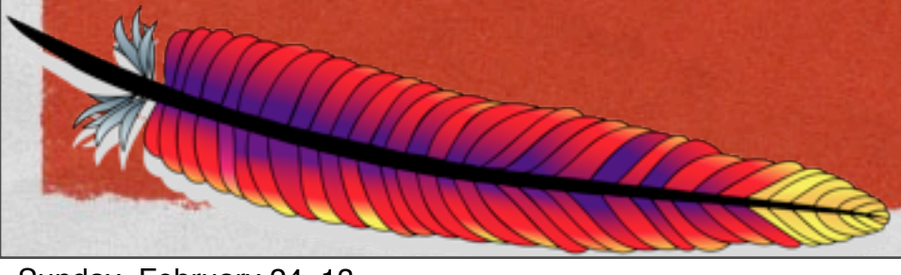
```
[rbowen@NCC1701:local/apache2]$ ./bin/httpd -M
Loaded Modules:
 core_module (static)
 so_module (static)
 http_module (static)
 authn_core_module (shared)
 authz_host_module (shared)
 authz_core_module (shared)
 request_module (shared)
 include_module (shared)
 filter_module (shared)
 deflate_module (shared)
 [illegible]e_module (shared)
 log_config_module (shared)
 env_module (shared)
 setenvif_module (shared)
 mpm_event_module (shared)
 unixd_module (shared)
 status_module (shared)
 autoindex_module (shared)
 info_module (shared)
 cgid_module (shared)
 negotiation_module (shared)
 dir_module (shared)
 alias_module (shared)
 rewrite_module (shared)
```

URL MAPPING

By Dunechaser on Flickr

URL MAPPING

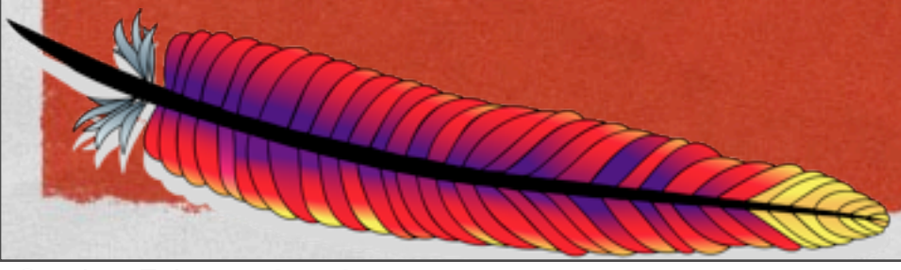
- The process of translating a request URL into an actual resource location



DOCUMENTROOT

DocumentRoot /usr/local/apache/htdocs

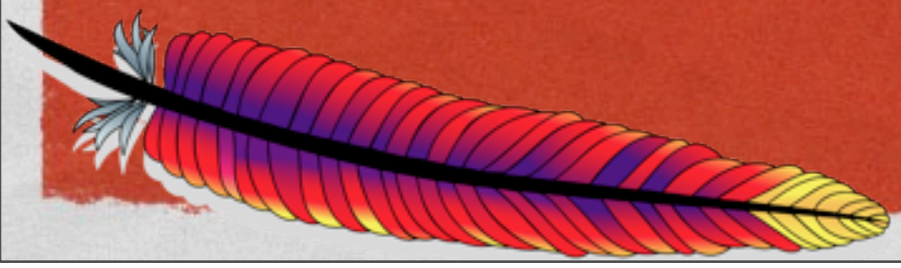
- Maps a request for http://example.com/ to a directory path
- Other requests are then mapped to subdirectories of that path



ALIAS

```
Alias /errors /usr/local/apache/errors
```

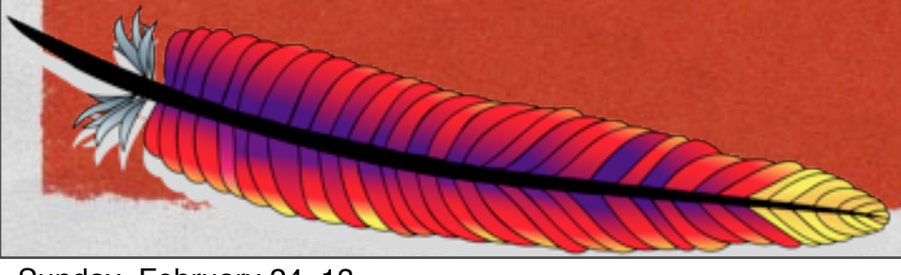
- Maps a URL path to a directory, usually outside of the DocumentRoot
- Don't use 'Alias /' - that's what DocumentRoot is for
- Don't use Aliases that overlap, or httpd will scold you



ALIASMATCH

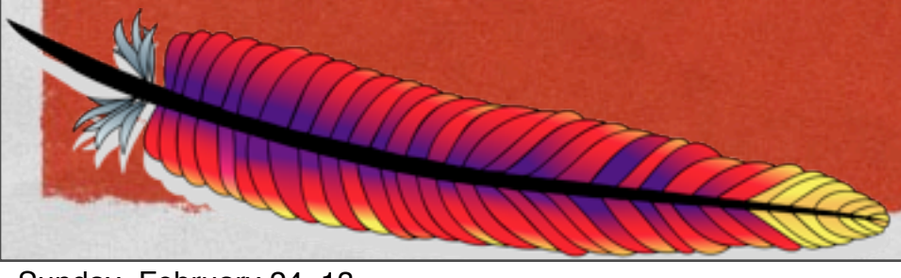
- Like Alias, but with super powers

```
AliasMatch /(image|pic)s? /usr/local/apache/img
```



SCRIPTALIAS

- Like Alias, but also implies that everything in the target directory is a CGI program
- See CGI, in a few minutes

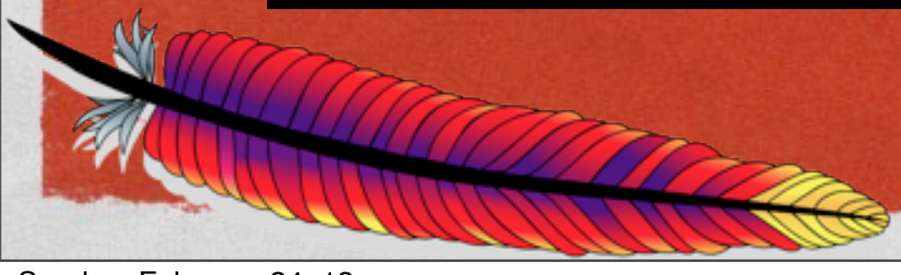


REDIRECT

Redirect /fish/ http://aquarium.com/here/

- Redirects a request somewhere else - usually a fully-qualified URL.
- The client receives a Location: header, and then makes a second HTTP request
- Sub-paths are also redirected, so the trailing slash is important

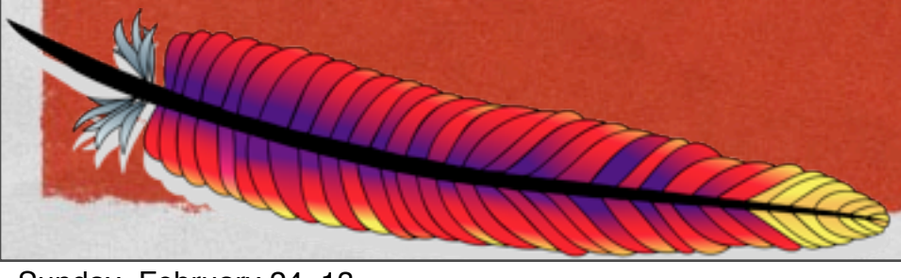
```
/fish/guppy.html --> http://aquarium.com/here/guppy.html
                    without the trailing slash ...
/fish/guppy.html --> http://aquarium.com/hereguppy.html
```



REDIRECTMATCH

- Like Redirect, but with super powers

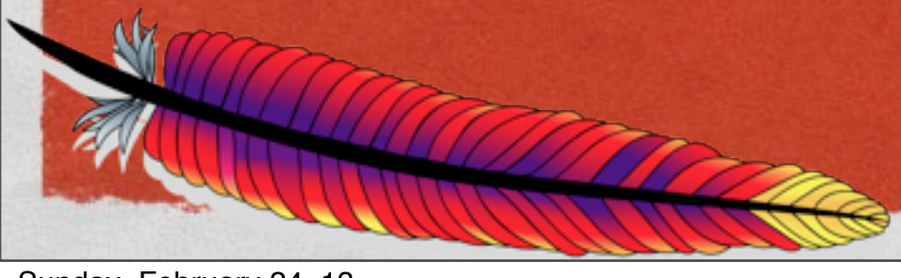
```
RedirectMatch (.*)\.gif$ http://other.example.com$1.jpg
```



REDIRECTMATCH

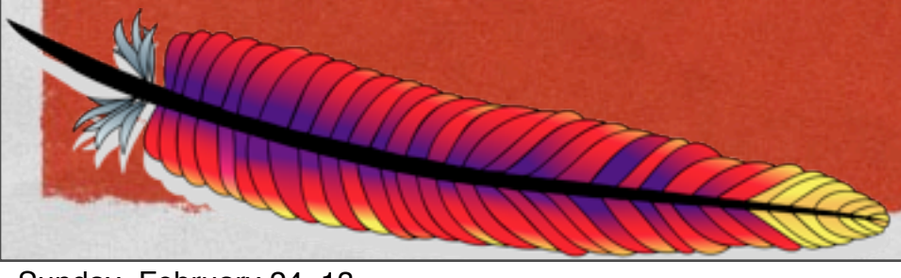
- Like Redirect, but with super powers

```
RedirectMatch (.*)\.gif$ http://other.example.com$1.jpg
```



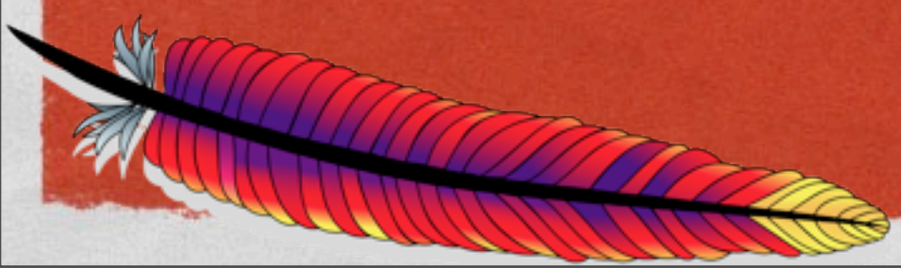
PROXYPASS

- Makes a request, transparently, to another server, and then returns the response to the client
- See Proxy section in a moment



USERDIR

- Maps a request for /~username to that user's home directory, or some other user-controlled space
- Easy way to give web-site hosting to users on your system without giving them access to the server DocumentRoot



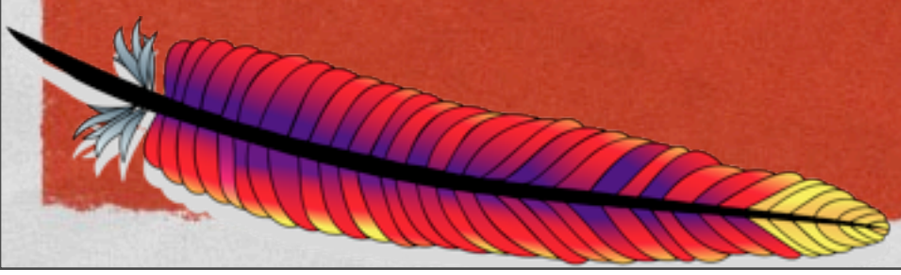
USERDIR

`http://www.example.com/~bob/one/two.html` will be translated to:

UserDir directive used	Translated path
UserDir public_html	~bob/public_html/one/two.html
UserDir /usr/web	/usr/web/bob/one/two.html
UserDir /home/*/www	/home/bob/www/one/two.html

The following directives will send redirects to the client:

UserDir directive used	Translated path
UserDir http://www.example.com/users	http://www.example.com/users/bob/one/two.html
UserDir http://www.example.com/*/usr	http://www.example.com/bob/usr/one/two.html
UserDir http://www.example.com/~*/	http://www.example.com/~bob/one/two.html

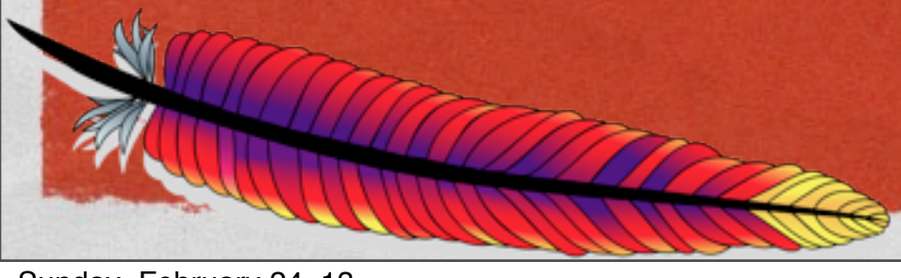


<LOCATION>

- Maps a URL space to something - often a handler

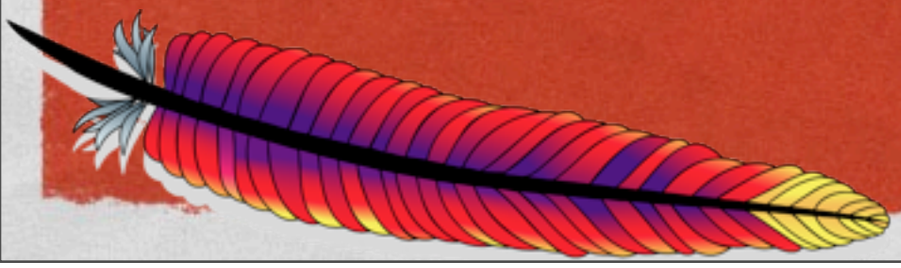
```
<Location /server-info>
    SetHandler server-info
</Location>
```

- Requests starting with "/server-info" will be handled by the server-info handler, even if there's a directory called /server-info. (More about this later.)



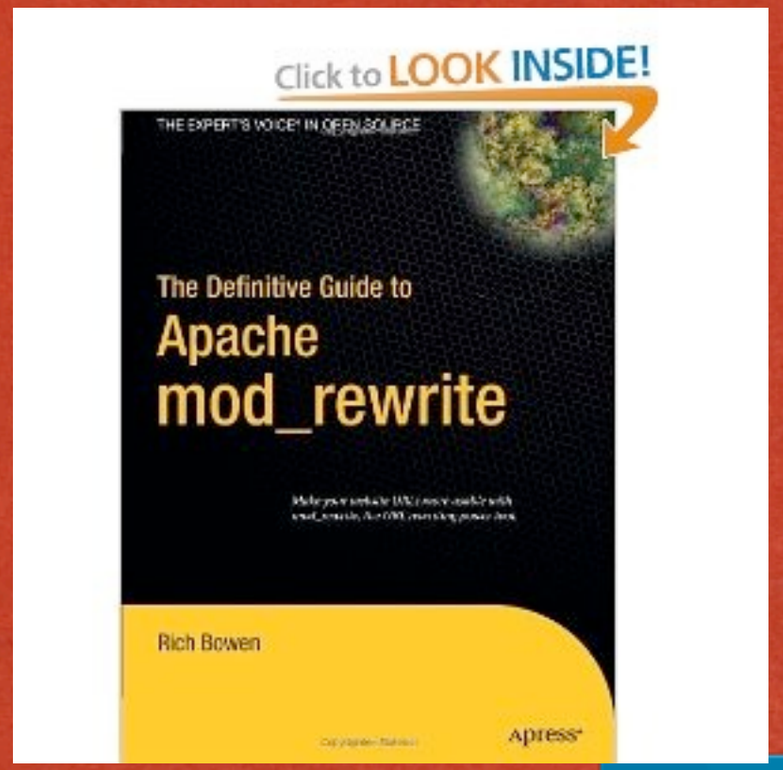
REWRITE

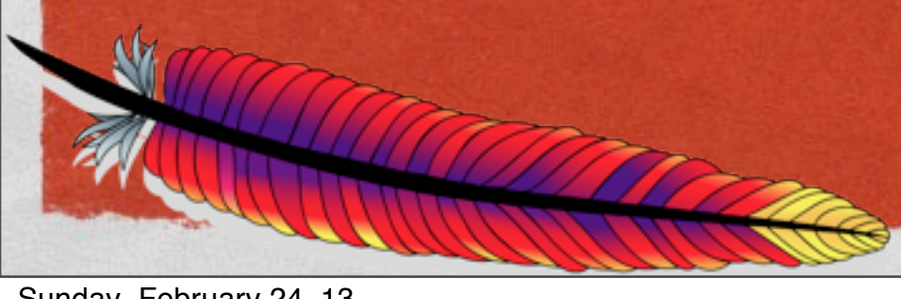
- All super powers
- Applies the powers of regular expressions to your URLs, and does anything you want
- Comes with a side of fries



MOD_REWRITE

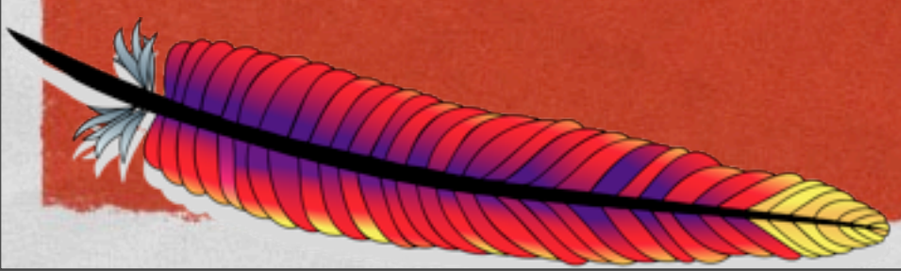
- Tomorrow: mod_rewrite boot camp
- How many of you will be there?





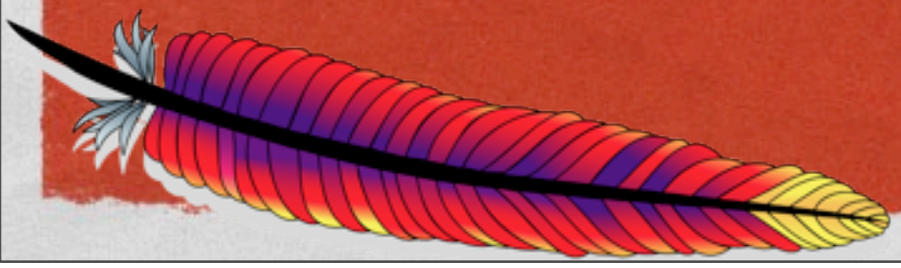
REWRITERULE

```
RewriteBase /
RewriteCond %{REQUEST_URI} !=/index.php
RewriteRule ^(.*) /index.php?req=$1  [L,PT]
```

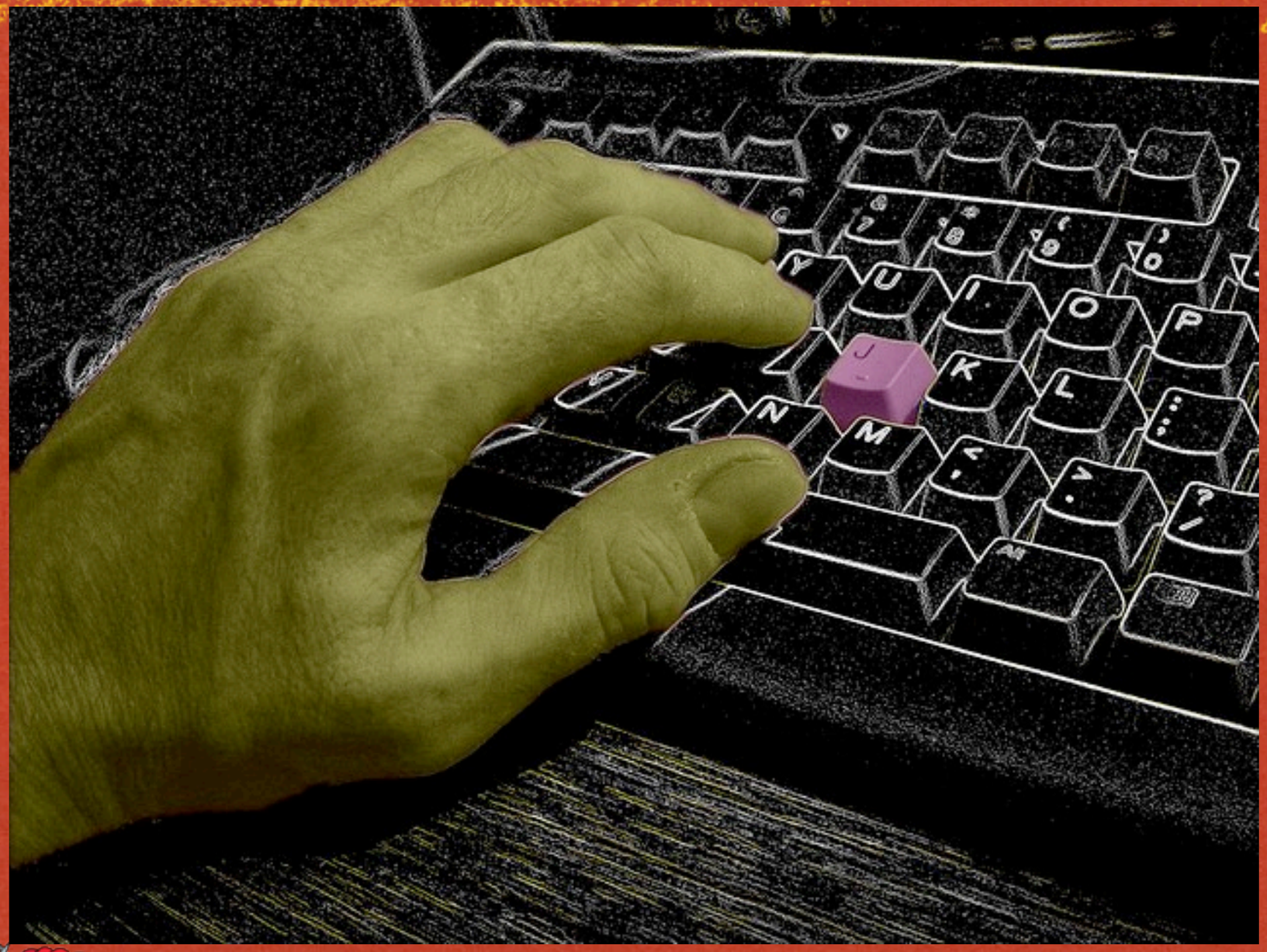


REWRITERULE

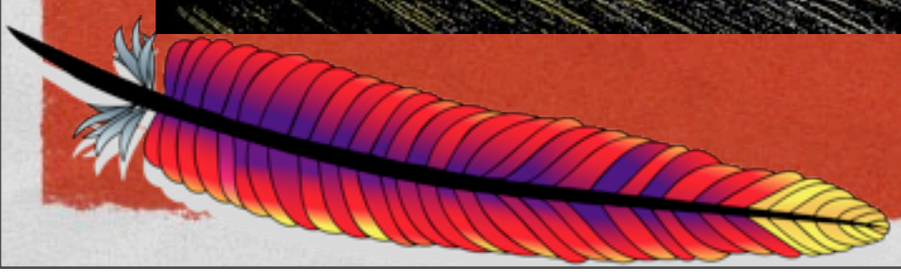
- Can also map requests to resources using external programs, database queries, or plain-text one-to-one mappings
- And can have side-effects such as cookies, proxy requests, handlers, HTTP status codes, and so on



CGI

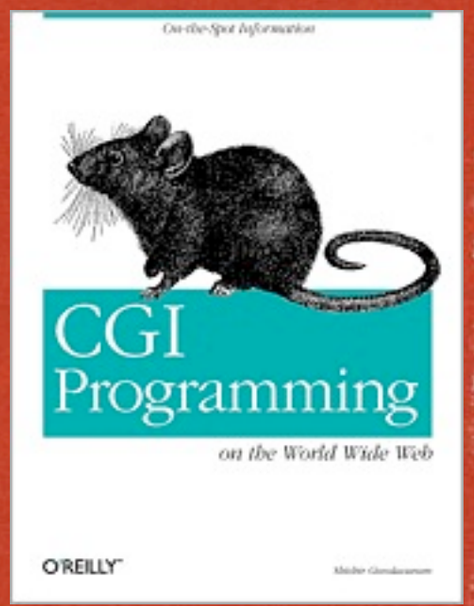


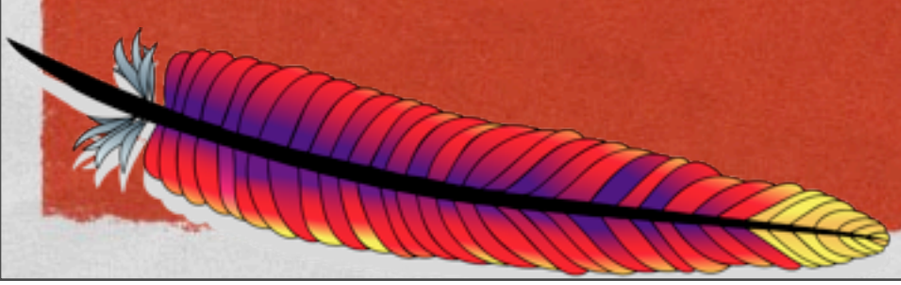
By josef.stuefer on Flickr



CGI

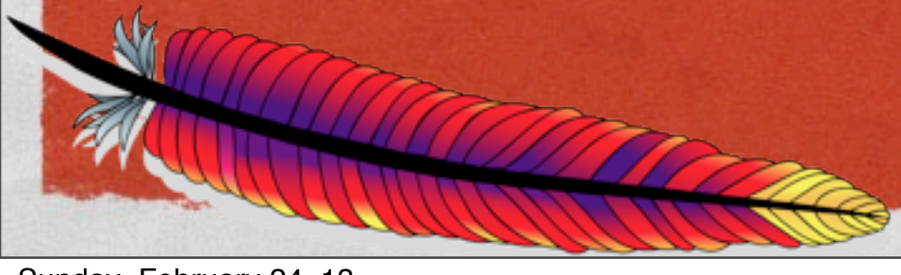
- Common Gateway Interface
- Defines how programs should behave in order to send their output through a server and back to the client





CGI

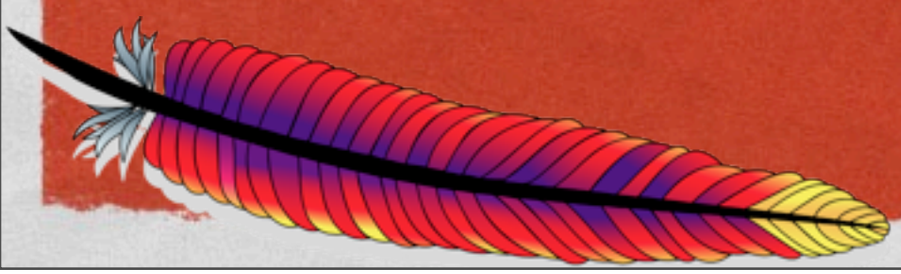
- Simplest way to provide dynamic content on your website
- Just need to know a few rules



HEADERS

- A CGI program needs to send valid HTTP headers before it sends any content

```
#!/usr/bin/perl

print "Content-type: text/html\n\n";
print "Hello, World!<br />";
```

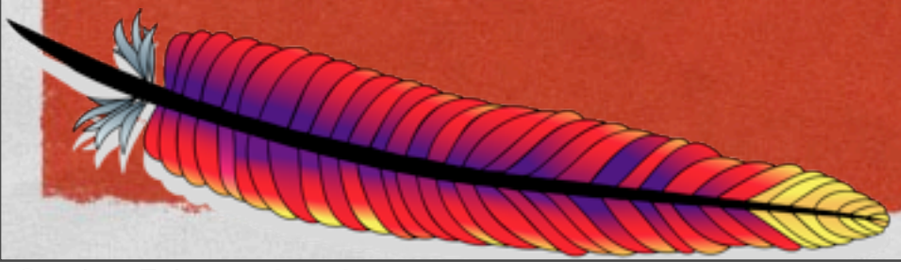


CONFIGURATION

- ScriptAlias:

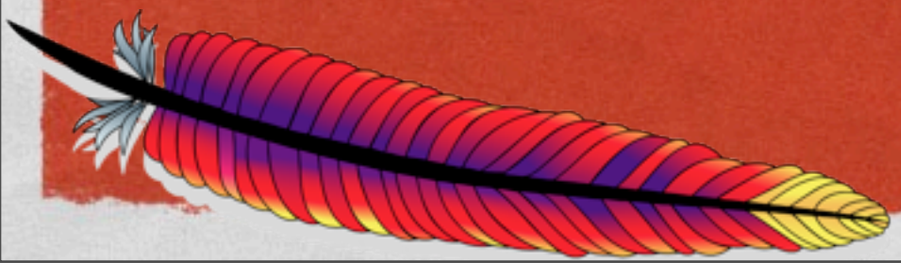
```
ScriptAlias /cgi-bin/  /var/www/cgi/
```

- Anything in that directory is now assumed to be a CGI program, and httpd will attempt to execute it



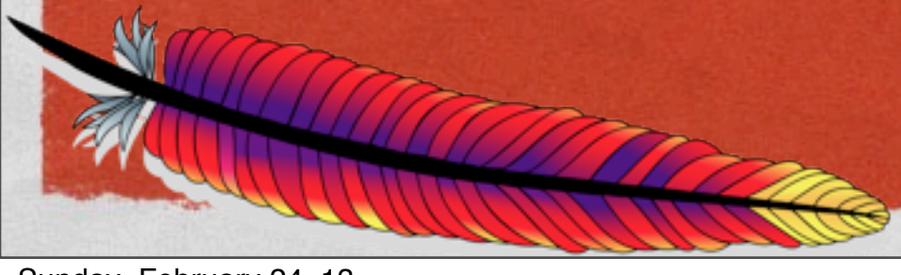
AND ...

- The script/program file must be executable by the server User
- CGI programs are executed with the privileges of the server user. This is why you don't want content files owned by that user, or writable by that user



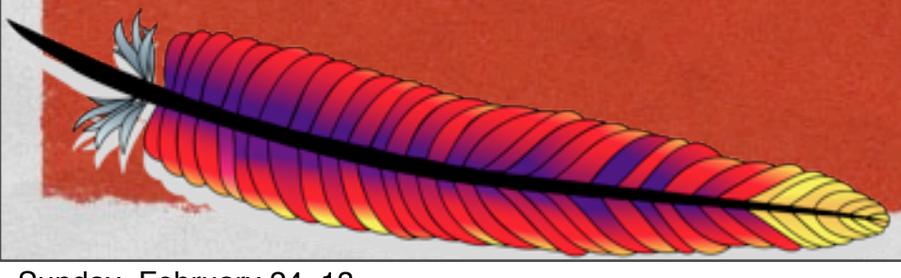
LANGUAGE

- CGI programs may be written in any language



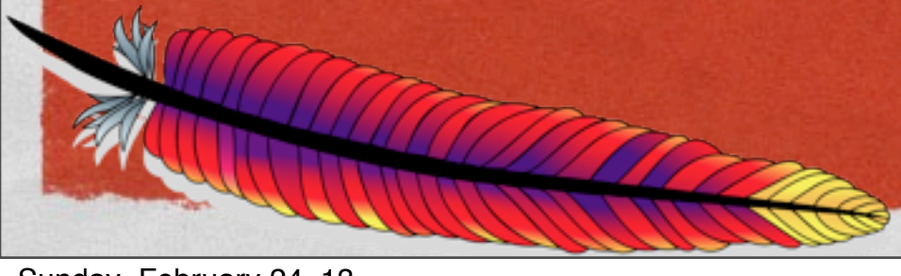
DEBUGGING CGI

- 500 Internal Server Error
- Means something bad happened
- Details are in the error log



DEMO GOES HERE

- CGI program demo here



AUTOINDEX

By kyz on Flickr

MOD_AUTOINDEX

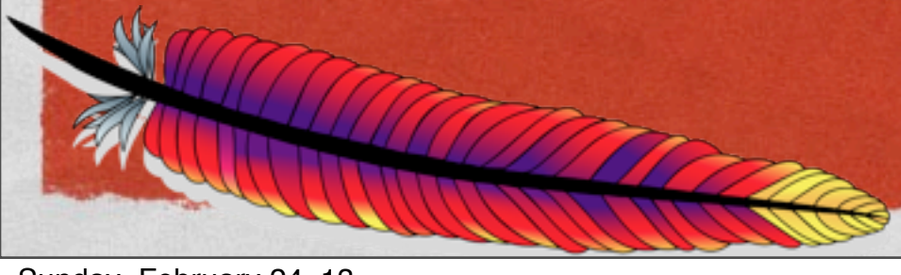
HEADER GOES HERE

Name	Last modified	Size	Description
Parent Directory		-	
one.gif	2013-02-20 22:29	32	
three.png	2013-02-20 22:29	1.4K	
two.jpg	2013-02-20 22:29	1.0K	

FOOTER GOES HERE

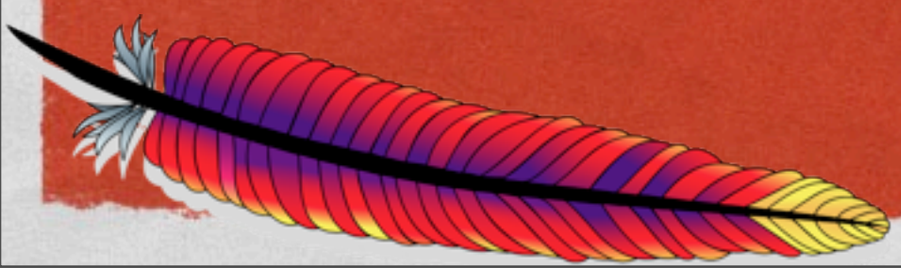
AUTOINDEX

- Provides a directory listing with a few simple features
- Sorting. Searching. Links. Icons.



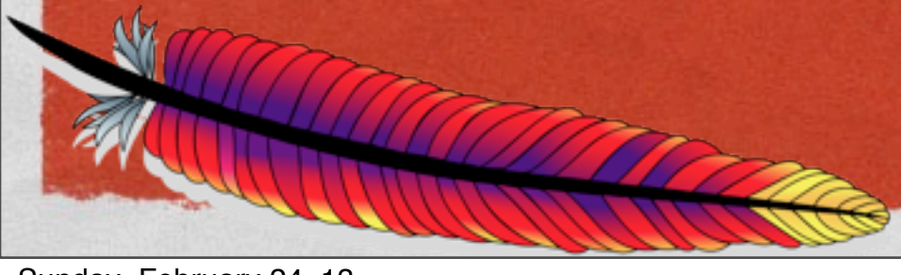
OPTIONS

- http://localhost/upload/?C=S;O=A - Order by size, ascending
- http://localhost/upload/?C=D;O=D - Order by description, decending
- http://localhost/upload/?P=t* - Just the files starting with t

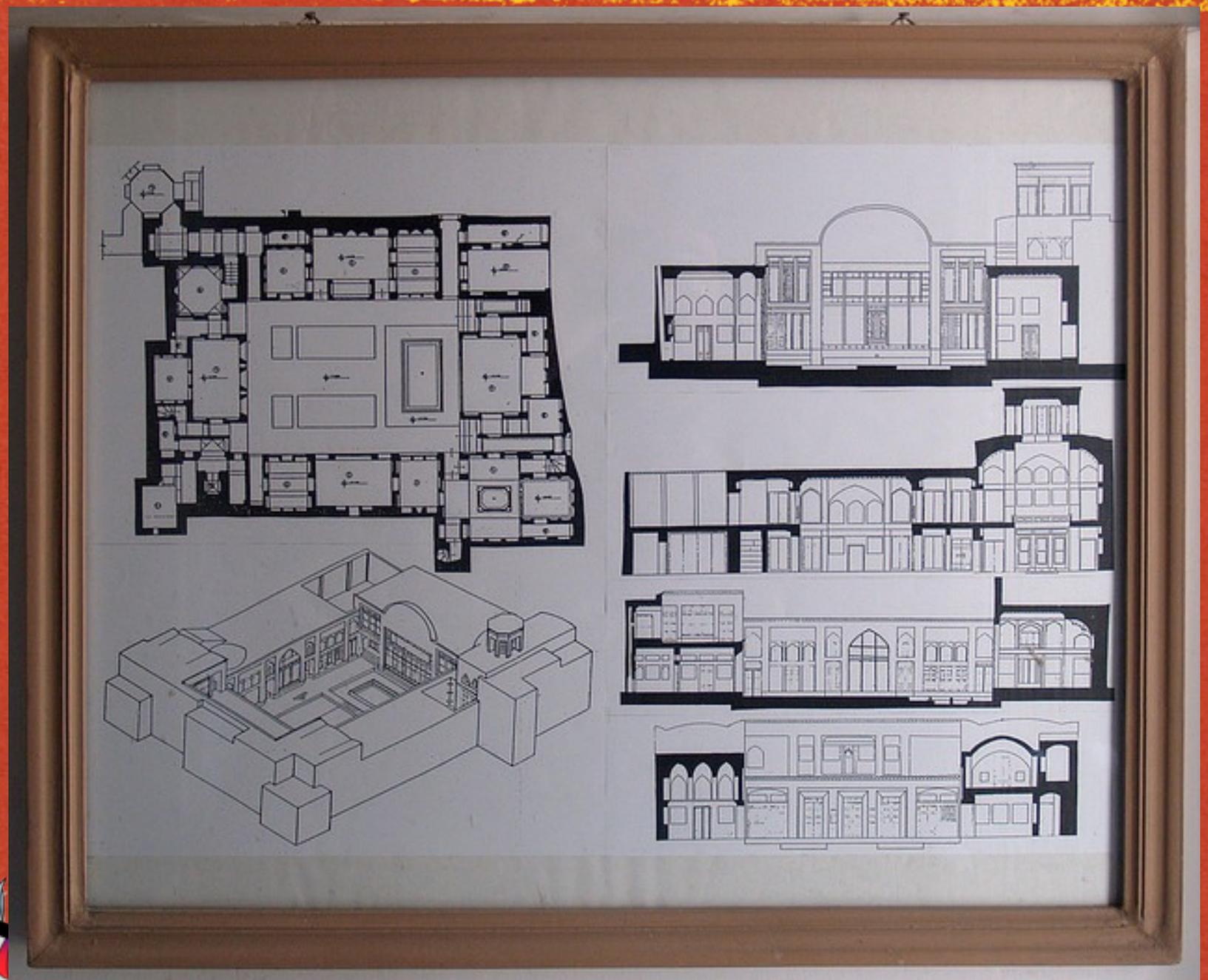


DEMO

- Demo goes here



MOD_INFO

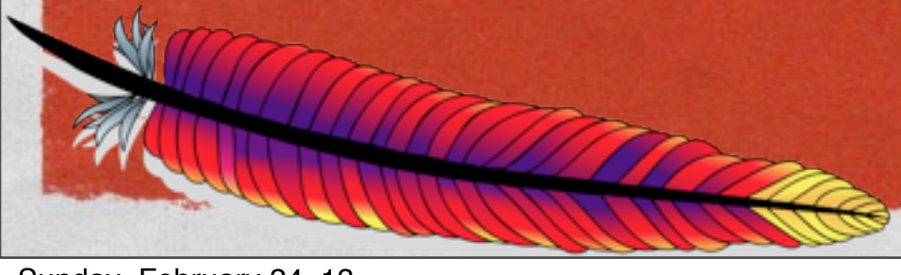


by seier+seier on Flickr

MOD_INFO

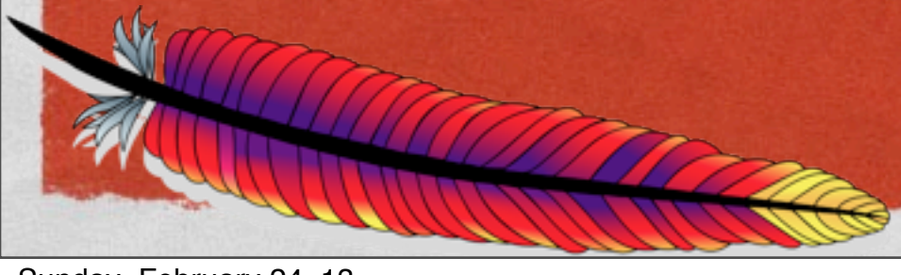
- Dump configuration information about your server

```
<Location /server-info>
    SetHandler server-info
    Require host example.com
</Location>
```



EASIER TO SHOW YOU ...

- Demo Goes Here



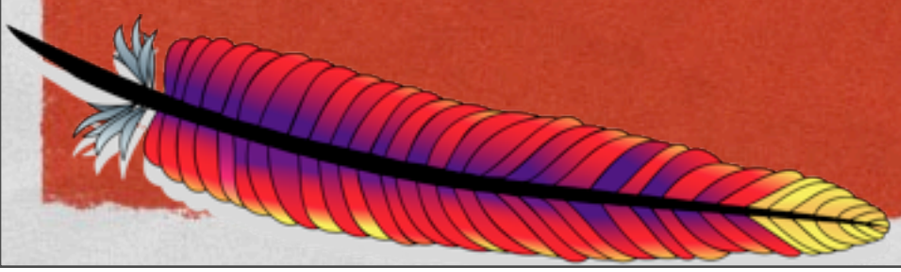
MOD_STATUS

by storem on Flickr

STATUS SNAPSHOT

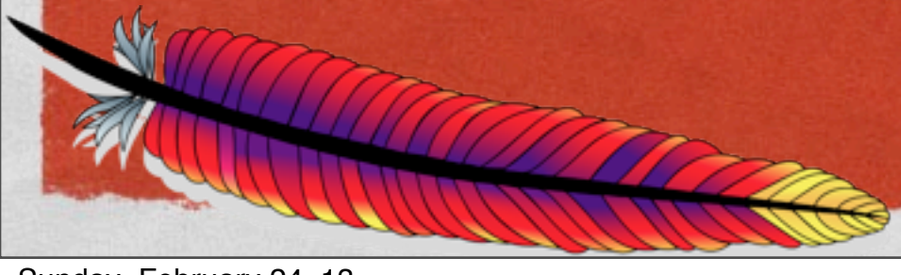
```
<Location /server-status>
    SetHandler server-statis
    Require host example.com
</Location>
```

- Shows current activity on your server



EASIER TO SHOW YOU ...

- Demo Here (http://httpd.apache.org/server-status)

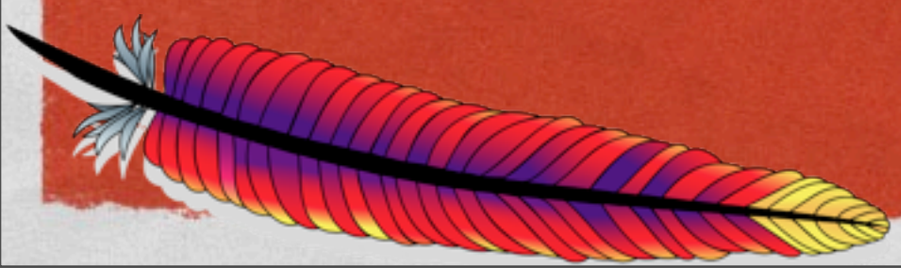


SSL

by david.nikonvscanon on Flickr

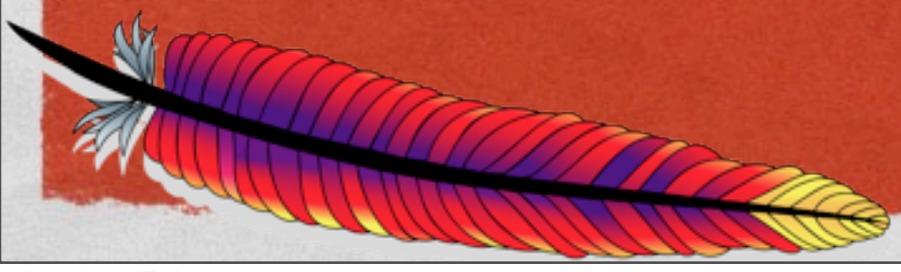
PURPOSE

- Secure the connection: Client and Server negotiate an encrypted connection, rendering all traffic between them secure
- Authenticate the request: A certificate ensures that you are talking with the server that you expect to be



CONFIG

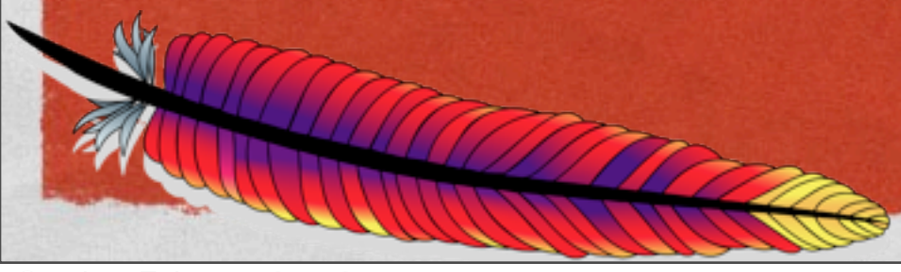
```
Listen 443
<VirtualHost *:443>
    ServerName www.example.com
    SSLEngine on
   SSLCertificateKeyFile /path/to/www.example.com.key
    SSLCertificateFile /path/to/www.example.com.cert
</VirtualHost>
```



CONFIG

Make yourself

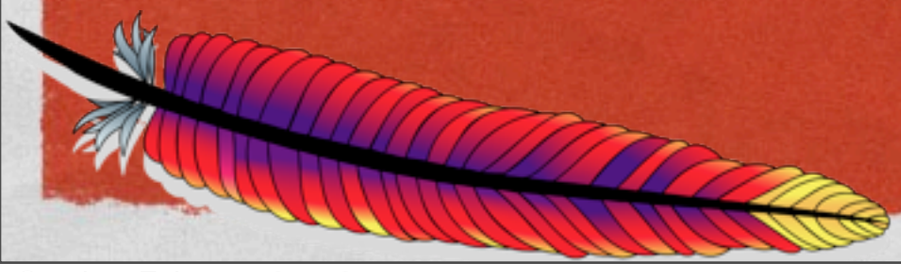
```
Listen 443
<VirtualHost *:443>
    ServerName www.example.com
    SSLEngine on
   SSLCertificateKeyFile /path/to/www.example.com.key
    SSLCertificateFile /path/to/www.example.com.cert
</VirtualHost>
```



CONFIG

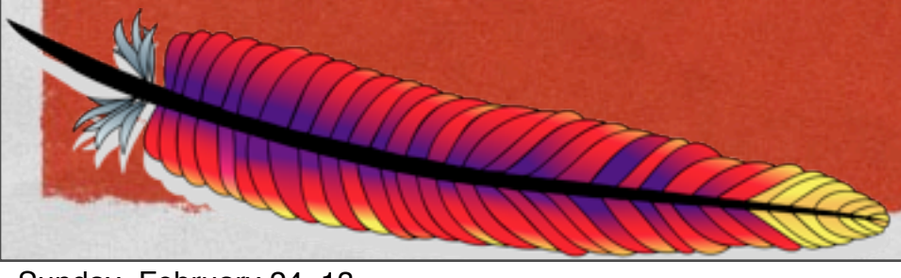
Usually, purchase from third-party vendor

```
Listen 443
<VirtualHost *:443>
    ServerName www.example.com
    SSLEngine on
   SSLCertificateKeyFile /path/to/www.example.com.key
    SSLCertificateFile /path/to/www.example.com.cert
</VirtualHost>
```



HTTPS://

- Requests to https://example.com will connect to :443 by default, expecting an SSL connection

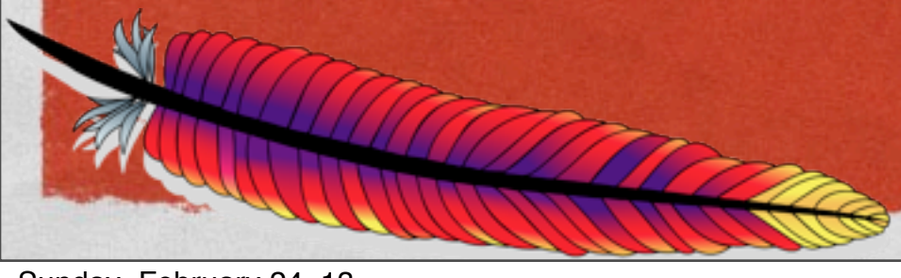


PROXYING

by Travis S. on Flickr

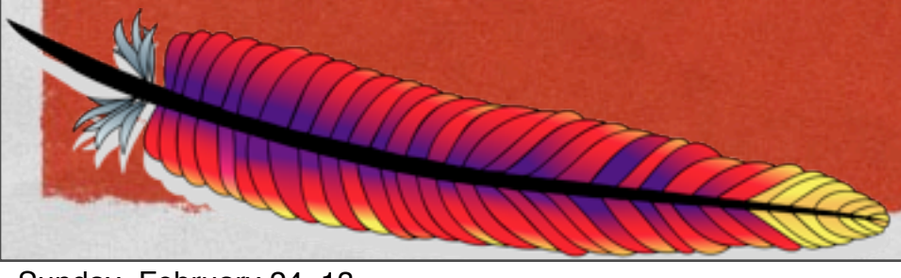
PROXYPASS

- A request received by the server results in a proxy request to another server. The response is then returned to the client
- The client is (usually) unaware that this is going on



REASONS

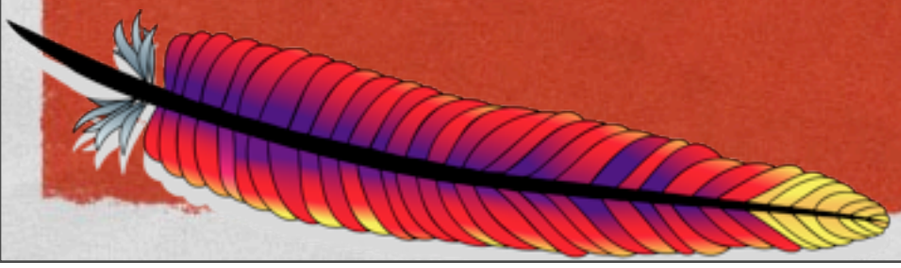
- Single front-end to multiple back-end servers
- Load balancing
- Infrastructure hiding



CONFIGURATION

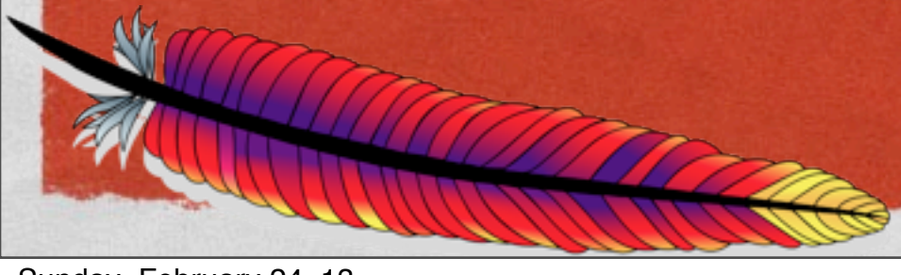
```
ProxyPass /images http://images.example.com/img
ProxyPassReverse /images http://foo.example.com/img
```

- Image requests are sent to a back-end image server
- ProxyPassReverse ensures that any Location (redirect) headers sent from the back-end are rewritten to refer to the front-end server, keeping the client unaware that proxying is going on



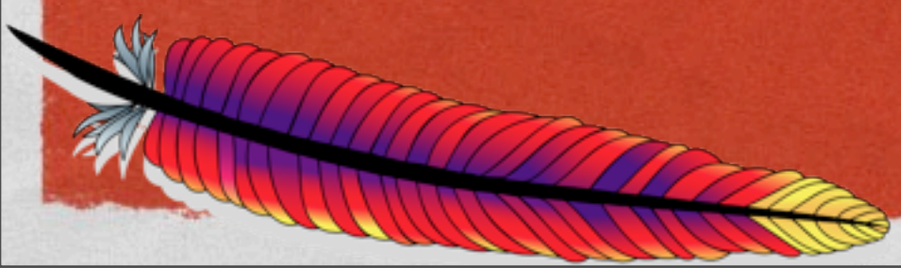
LOOKING BACK ...

- Remember this slide from earlier:



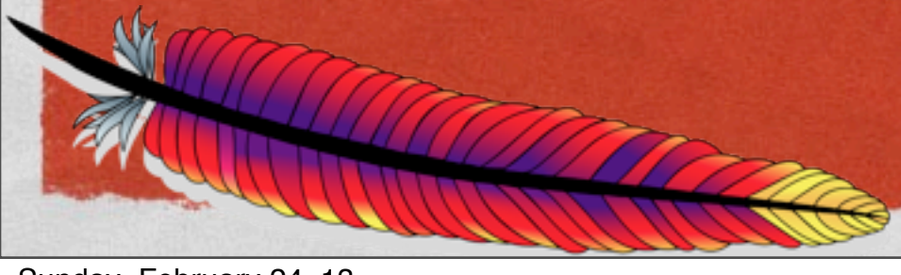
SUBSTITUTE

```
ProxyPass /blog/ http://internal.blog.example.com/
ProxyPassReverse /blog/ http://internal.blog.example.com/

Substitute \
  "s|http://internal.blog.example.com/|http://www.example.com/blog/|i"
```



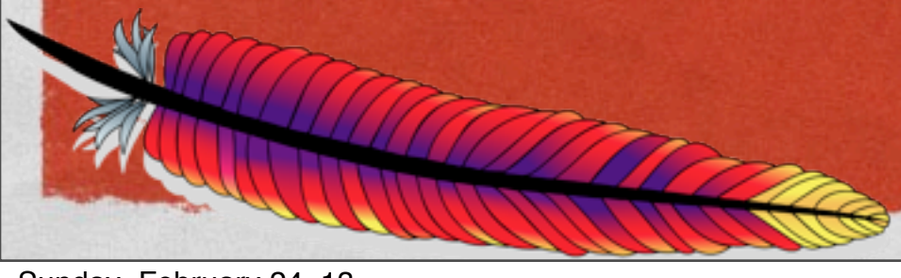
FIXUP HTML

- Do that if the content contains hard-coded links including the back-end server name



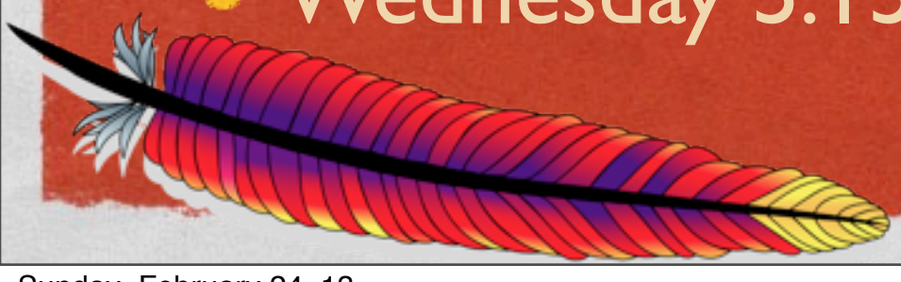
MOD_PROXY_HTML

- More sophisticated rewriting of response, including headers, cookies, javascript obfuscation, and CSS



COMING SOON TO A CONFERENCE NEAR YOU

- Tomorrow: mod_rewrite boot camp
- Tuesday 10:15 am: New in 2.4
- Tuesday 4pm: Access Control
- Wednesday 11:45am: Securing the web (Igor Galic)
- Wednesday 1:45pm: N things you didn't know httpd could do
- Wednesday 5:15pm: mod_lua (Daniel Gruno)



FIN

by Horia Varlan on Flickr

Rich Bowen
rbowen@apache.org

Slides are at: **tm3.org/httpd-ac2013**