Basic Apache

By

Kenneth Power

Training Seminar 2006

Location, Location, Location

/usr/local/apache

- **bin/**
- **conf/**
- **sites/**
- **domlogs/**
- **logs/**
- **modules/**

Your httpd.conf file and You

Could You Tell Me How to Act, Please?

What's My Name Again?

Names vs. IP

Account Examples

```
<VirtualHost 192.168.90.197>
ServerAlias freedom.com
ServerAdmin webmaster@freedom.com
DocumentRoot /home/freedom/public_html
BytesLog domlogs/freedom.com-bytes_log
ServerName www.freedom.com

User freedom
Group freedom
CustomLog /usr/local/apache/domlogs/freedom.com combined
ScriptAlias /cgi-bin/ /home/freedom/public_html/cgi-bin/
</VirtualHost>
```

```
<VirtualHost 192.168.90.197:443>
ServerAdmin webmaster@freedom.com
DocumentRoot /home/freedom/public_html
ServerName freedom.com
UserDir public_html

User freedom
Group freedom
ScriptAlias /cgi-bin/ /home/freedom/public_html/cgi-bin/

SSLEnable
SSLCertificateFile /usr/share/ssl/certs/freedom.com.crt
SSLCertificateKeyFile /usr/share/ssl/private/freedom.com.key
SSLLogFile /usr/local/apache/domlogs/freedom.com-ssl_data_log
CustomLog /usr/local/apache/domlogs/freedom.com-ssl_log combined
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
</VirtualHost>
```

AllowOverride

All	Enables all overrides
None	Disables all overrides
Authconfig	user/group authorization
FileInfo	Control document types
Indexes	Control directory indexing
Limit	Control network/host access
Options	Use special directives

The End Run: .htaccess

mod_rewrite
http://www.example.com/article/32
http://www.example.com/index.php?s=article&id=32

.htaccess – The Dangers

Directory Traversal

php_*

The Cookie Cutter Approach

/usr/local/cpanel/etc/httptemplates

- **default**
- **ssldefault**

Default

```
<VirtualHost %ip%>
ServerAlias %serveralias%
ServerAdmin %serveradmin%
DocumentRoot %docroot%
ServerName %servername%
!usecannameoff=1!
UseCanonicalName off
!usecannameoff!
!dirprotect=1!
...
@ADDONS@
</VirtualHost>
```

Just Addon

Tomcat, Resin, Mono, more

The Many Versions of Apache

Basic differences

2: Worker and Prefork

Why does it matter?

“We do not recommend using a threaded MPM in production with Apache2. Use the prefork MPM instead, or use Apache1.”

Source: http://www.php.net/manual/en/install.unix.apache2.php

PHP

Face Off! 4 vs 5.1

MySQL

Training Seminar 2006

PHP Security

Catching a Greased Pig;
or How to Secure Your PHP Installation

Training Seminar 2006

Modules and Multi-User

Pardon me while I read your file

One Solution: CGI

CGI Strategy

she-bang, not a Ricky Martin song

#!/usr/local/bin/php

suExec

- **PHPsuExec**
- **suPHP**

Basic Apache

PHP Specifics:

- **Safe Mode ***
- **open_basedir**
- **display_errors**
- **disable_functions ***
- **register_globals**

Caveats

- 6.0: Goodbye Safe Mode
- .htaccess
- Web application breakage

Performance

Why do you need Zend Optimizer?

mod_security

What is it?

How do I enable it?

Enabling mod_security

mod_security Configuration

/usr/local/apache/conf

- **modsec.conf**
- **modsec.user.conf**

modsec.conf Example

```
<IfModule mod_security.c>
SecFilterEngine On
SecFilterCheckURLEncoding On
SecFilterForceByteRange 0 255
SecAuditEngine RelevantOnly
SecAuditLog logs/audit_log
SecFilterDebugLog logs/modsec_debug_log
SecFilterDebugLevel 0
SecFilterDefaultAction "deny,log,status:406"
SecFilterSelective REMOTE_ADDR "^127.0.0.1$" nolog,allow
Include "/usr/local/apache/conf/modsec.user.conf"
</IfModule>
```

mode_security - Rules

Occur on every incoming Request

Get: first line only

Post: body included

Rule Syntax

SecFilter KEYWORD [ACTIONS]

KEYWORD: What to Match

ACTIONS: What to do

Rules: What Do We Match?

Normalized data

GET /bin/./sh -> /bin/sh

Action: Now What Do I Do?

1. Primary – *deny, pass, redirect*
2. Seconday
3. Flow – *chain, skip*

Action Parameters

Colon (:) separated

White space single quoted (')

```
SecFilterDefaultAction “deny,log,status:'Hello World!'”
```

mod_security Examples

Parameter Checking

```
SecFilterSelective ARG_parameter “!^[0-9]{1,5}$”
```

mod_security Examples

File Upload

Deny all, selective

```
SecFilterSelective HTTP_CONTENT_TYPE multipart/form-
  data

<Location /upload.php>
   SecFilterInheritance Off
</Location>
```

mod_security Examples

Securing FormMail

```
<Location /cgi-bin/FormMail>
   SecFilterSelective ARG_recipient “![a-zA-Z0-9]
     +@example\.com$”
</Location>
```

mod_security and Multi-User

.htaccess
- Users can define rules
- Users can invalidate your rules

Mandatory
- Global
- Per rule

mod_security and Performance

Apache 1.3 and Memory

Testing

/usr/src/modsecurity-apache-{$version}/util
run-test.pl

Speed

mod_security Future

Apache 2.2 unsupported

New version

Problems & Troubleshooting

- **Configuration**
- **Upgrades**
- **Tools**

Configuration Problems

- **MaxClients**
- **VirtualHost:**
  - **NameVirtualHost directive**
  - **ServerName directive**
- **Redirects**

Upgrade Problems

- **Module Recompile**
- **Library Mismatch**

Tools

- **Error Messages**
  - **400 Series**
    - **400**
    - **401**
    - **403**
    - **404**
  - **500 Series**

The Log Files

/usr/local/apache/logs

- ***access_log***
- ***error_log***

Log File Example

access_log:
127.0.0.1 - - [02/Jun/2006:12:16:50 -0500]
"GET /~kpower/test.php HTTP/1.1" 500
697 "-" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.8.0.
3) Gecko/20060523 Ubuntu/dapper
Firefox/1.5.0.3"

Log File Example

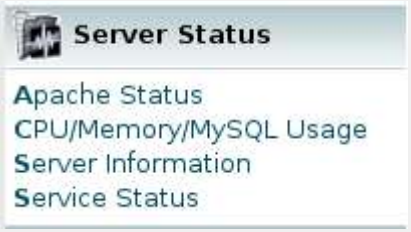
error_log:
[Fri Jun 02 12:16:50 2006] [alert] [client 127.0.0.1] / home/kpower/public_html/.htaccess: php_flag not allowed here

Configuration Testing

/usr/local/apache/bin

httpd -t -f *file*

Server Info



- **Status**
- **Information**

Server Status

Current Time: Tuesday, 06-Jun-2006 14:30:32 CDT
Restart Time: Thursday, 01-Jun-2006 14:02:13 CDT
Parent Server Generation: 0
Server uptime: 5 days 28 minutes 19 seconds
Total accesses: 1457 - Total Traffic: 11.2 MB
CPU Usage: u2.48438 s.75 cu0 cs0 - .000746% CPU load
.00336 requests/sec - 27 B/second - 7.9 kB/request
1 requests currently being processed, 7 idle servers

Server Status

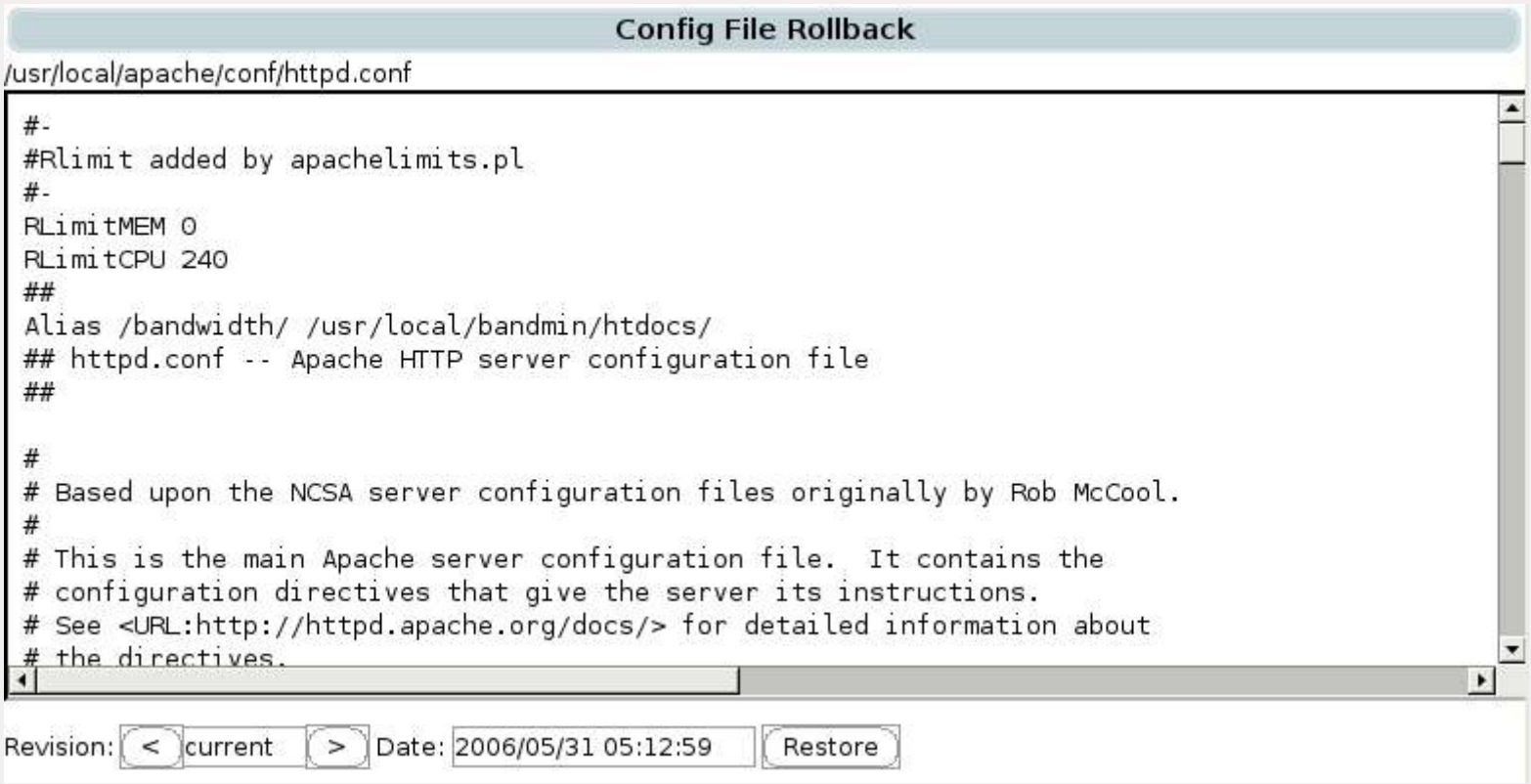
Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Host	VHost	Request
0-0	41687	0/181/181	W	0.41	330639	0	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status/ HTTP/1.0
1-0	41688	0/182/182	_	0.41	433308	2	0.0	1.39	1.39	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0
2-0	41689	0/182/182	_	0.41	434006	2	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0
3-0	41690	0/186/186	_	0.41	433585	2	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status/ HTTP/1.0
4-0	41691	0/185/185	_	0.41	290139	2	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0
5-0	41724	0/181/181	_	0.41	156939	2	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0
6-0	41725	0/181/181	_	0.40	433584	2	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0
7-0	41726	0/181/181	_	0.40	180339	10	0.0	1.40	1.40	127.0.0.1	miracle54.cpanel.net	GET /whm-server-status HTTP/1.0

Srv Child Server number - generation
PID OS process ID
Acc Number of accesses this connection / this child / this slot
M Mode of operation
CPU CPU usage, number of seconds
SS Seconds since beginning of most recent request
Req Milliseconds required to process most recent request
Conn Kilobytes transferred this connection
Child Megabytes transferred this child
Slot Total megabytes transferred this slot

Configuration Roll-back

Revision Control

Configuration Roll-back



Conclusion

Question
&
Answer