**Web Server:**

1. What OS model are we using?
   1. Cat /etc/issue OR cat /etc/version
      1. This will tell you if you are utilizing Ubuntu, or CentOS
2. Make appropriate updates to OS:
   1. Sudo yum update OR sudo apt-get update
3. What type of web server do you have?
   1. Cd /etc
      1. Locate apache2 OR httpd folders
   2. Service apache2|httpd status
      1. This will inform you if service is running
4. Make appropriate changes to .conf files **(from now on i will utilize httpd)**
   1. Cd /etc/httpd/httpd.conf
      1. Locate following:
         1. ServerAdmin
            1. Who will be notified if needed?

[name@ide.com](mailto:name@ide.com)

* + - 1. ServerName
         1. Change to your server name and port

[www.myserver.edu:80](about:blank)

* + - 1. DirectoryIndex
         1. File server can access only with directory name

Index.html

* + - 1. KeepAlive
         1. Turn on
      2. DocumentRoot
         1. **Where are all your files located?**

/var/www/

**This can depend on how you develop virtual hosts**

**Verify .html documents in directory**

* + - 1. AllowOverride
         1. **Do not allow. This disables .htaccess**
      2. Options
         1. Remove ‘indexes’ from options. **This will disable CGI-Bin and other scripts**
      3. AddHandler
         1. Remove all scripts

1. **Validate DocumentRoot with Virtual Hosts:**
   1. Cd /etc/httpd/conf.d/vhost.conf
      1. Verify document root location
      2. Cd ‘documentRoot’
         1. Verify .html files in each directory
2. Disable userdir
   1. Vim /etc/httpd/conf.d/userdir.conf
      1. UserDir disabled
3. If using LDAP:
   1. Vim /etc/httpd/conf.d/auth\_ldap.conf
      1. Add to end:
         1. <Directory /var/www/html/auth-ldap>  
            SSLRequireSSL  
            AuthName “LDAP Authentication”  
            AuthType Basic  
            AuthBasicProvider ldap  
            AuthLDAPURL ldap://dlp.srv.world/dc=srv,dc=world,?uid?sub?(objectClass=\*)  
            Require ldap-filter objectClass=posixAccount  
            </Directory>
4. Disable proxy capabilities:
   1. Vim /etc/httpd/conf.d/f\_proxy.conf
      1. module is enabled by default so create new
         1. <IfModule mod\_proxy.c>

ProxyRequests off

<Proxy \*>

# access permission

Require ip 127.0.0.1 10.0.0.0/24

</Proxy>

# specify the way of load balancing with "lbmethod". it's also possible to set "bytraffic".

ProxyPass / balancer://cluster lbmethod=byrequests

<proxy balancer://cluster>

BalancerMember http://node01.srv.world/ loadfactor=1

BalancerMember http://node02.srv.world/ loadfactor=1

</proxy>

</IfModule>

**Additional Services:**

1. Access Log Analyzer: AWstats
   1. Install: sudo yum --enablerepo=epel -y install awstats
      1. awstats.(hostname).conf created. Modify with:
         1. Sudo vim /etc/awstats/awstats.(hostname).conf
            1. # line 122: change

# if your config for log format in httpd.conf is 'combined' Set here '1'

# If log-config is 'common' set here '4', but in this case, some info unavailable (browser info etc.)

LogFormat=1

# line 153: specify your hostname

SiteDomain="[www.srv.world](http://www.srv.world)"

# line 168: set IP address you'd like to exclude

HostAliases="localhost 127.0.0.1 REGEX[server\.world$] REGEX[^10\.0\.0\.]"

1. vi /etc/httpd/conf.d/awstats.conf
   1. # line 30: IP address you permit to access

Require ip 10.0.0.0/24

1. Set cron to update log every hour:

/usr/share/awstats/wwwroot/cgi-bin/awstats.pl -config+[www.srv.world](http://www.srv.world) -update

1. Access at “[http://(hostname)/awstats/awstats.pl](about:blank)

**Harden against DDoS:**

1. Install: sudo yum --enablerepo=epel install mod\_evasive
2. Vim /etc/httpd/conf.d/mod\_evasive.conf

# line 18: threshhold for the number of requests for the same page per page interval

DOSPageCount 5

# line 24: threshhold for the total number of requests for any object by the same client on the same listener per site interval

DOSSiteCount 50

# line 28: The interval for the page count threshhold

DOSPageInterval 1

# line 32: The interval for the site count threshhold

DOSSiteInterval 1

# line 41: amount of time (in seconds) that a client will be blocked for if they are added to the blocking list

DOSBlockingPeriod 300

# line 48: notification address if IP address becomes blacklisted

DOSEmailNotify root@localhost

# line 66: specify log directory

DOSLogDir "/var/log/mod\_evasive"

1. Mkdir /var/log/mod\_evasive
2. Chown apache. /var/log/mod\_evasive
3. Systemctl restart httpd
4. Use to test:

Perl /usr/share/doc/mod\_evasive-\*/test.pl

\*\*\*should get 40 forbidden in a bit

ll /var/log/mod\_evasive

\*\*logs are saved

Mail

\*\*shows email to ServerAdmin stating what IP was blacklisted

**Utilize mod\_security:**

1. Sudo yum install mod\_security
2. Add rules only to SecRuleEngine!!!

Vim /etc/httpd/conf.d/mod\_security.conf

\*\*\*note, default rules are set.

1. Test rules and verify:

Vim /etc/httpd/modsecurity.d/activated\_rules/rules-01.conf

# default action when matching rules

SecDefaultAction "phase:2,deny,log,status:406"

# "etc/passwd" is included in request URI

SecRule REQUEST\_URI "etc/passwd" "id:'500001'"

# "../" is included in request URI

SecRule REQUEST\_URI "\.\./" "id:'500002'"

# "<SCRIPT" is included in arguments

SecRule ARGS "<[Ss][Cc][Rr][Ii][Pp][Tt]" "id:'500003'"

# "SELECT FROM" is included in arguments

SecRule ARGS "[Ss][Ee][Ll][Ee][Cc][Tt][[:space:]]+[Ff][Rr][Oo][Mm]" "id:'500004'"

systemctl restart httpd

1. Logs are stored in directory:

Cat /var/lg/httpd/modsec\_audit.log

1. General rules are provided from official repository

Sudo yum install mod\_security\_crs

# rules are placed like follows

# they are linked into the directory /etc/httpd/modsecurity.d/activated\_rules

ll /usr/lib/modsecurity.d/base\_rules