Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Apache

Red Hat / CentOS Install mod_security Apache Intrusion Detection And Prevention Engine

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

How do I install ModSecurity - an open source intrusion detection and prevention engine for web applications under CentOS / RHEL / Red Hat Enterprise Linux 5.x server?

ModSecurity operates embedded into the web server (httpd), acting as a powerful umbrella - shielding web applications from attacks. In order to use mod_security, you need to turn on EPEL repo under CentOS / RHEL [3] Linux. Once repo is turned on, type the following command to install ModSecurity: [2]

```
# yum install mod_security
```

Sample output:

```
Loaded plugins: downloadonly, fastestmirror, priorities, protectbase
Loading mirror speeds from cached hostfile
 * epel: www.gtlib.gatech.edu
 * base: mirror.skiplink.com
 * updates: centos.aol.com
 * addons: mirror.cs.vt.edu
 * extras: mirror.trouble-free.net
0 packages excluded due to repository protections
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package mod_security.x86_64 0:2.5.9-1.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

===========================================================================================
 Package                                  Arch                               Version
===========================================================================================
Installing:
 mod_security                             x86_64                             2.5.9-1.el5

Transaction Summary
===========================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 935 k
Is this ok [y/N]: y
Downloading Packages:
mod_security-2.5.9-1.el5.x86_64.rpm
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : mod_security                                   [1/1]

Installed: mod_security.x86_64 0:2.5.9-1.el5
Complete!
```

mod_security configuration files

1. **/etc/httpd/conf.d/mod_security.conf** - main configuration file for the mod_security Apache module.
2. **/etc/httpd/modsecurity.d/** - all other configuration files for the mod_security Apache.
3. **/etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf** - Configuration contained in this file should be customized for your specific requirements before deployment.
4. **/var/log/httpd/modsec_debug.log** - Use debug messages for debugging mod_security rules and other problems.
5. **/var/log/httpd/modsec_audit.log** - All requests that trigger a ModSecurity events (as detected) or a serer error are logged ("RelevantOnly") are logged into this file.

Open /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf file, enter:

```
# vi /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf
```

Make sure SecRuleEngine set to "On" to protect webserver for the attacks:

```
SecRuleEngine On
```

Turn on other required options and policies as per your requirements. Finally, restart httpd:

```
# service httpd restart
```

Make sure everything is working:

```
# tail -f /var/log/httpd/error_log
```

Sample output:

```
[Sat May 09 23:18:31 2009] [notice] caught SIGTERM, shutting down
[Sat May 09 23:18:33 2009] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat May 09 23:18:34 2009] [notice] ModSecurity for Apache/2.5.9 (http://www.modsecurity.o
[Sat May 09 23:18:34 2009] [notice] Original server signature: Apache/2.2.3 (CentOS)
[Sat May 09 23:18:34 2009] [notice] Digest: generating secret for digest authentication ..
[Sat May 09 23:18:34 2009] [notice] Digest: done
[Sat May 09 23:18:35 2009] [notice] Apache/2.2.0 (Fedora) configured -- resuming normal ope
```

Refer mod_security [4] documentations to understand security policies.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/rhel-fedora-centos-httpd-mod_security-configuration/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/apache/**
[2] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[3] EPEL repo under CentOS / RHEL: **http://www.cyberciti.biz/faq/rhel-fedora-centos-linux-enable-epel-repo/**
[4] mod_security: **http://www.modsecurity.org/documentation/**