Integrating Mod_Security With Nagios XI 5

Purpose

This document describes how to install Mod_Security with the Apache webserver and Nagios XI.

If you are configuring Mod_Security with Nagios XI 2024, see How To Configure Apache ModSecurity In Nagios XI 2024

Still need installation help? We'll do it for free.

Schedule a free Quickstart session with our support team or contact sales at sales@nagios.com.

Visit Nagios Support Forum Visit Nagios Knowledge Base Schedule a Quickstart

Terminal Access

The steps in this document require you to establish a terminal session to your Nagios XI server as a user with root privileges.

Install Mod_Security

Begin by installing the needed packages for Mod_Security. Establish a terminal session to your Nagios XI server and execute the following command:

RHEL | CentOS | Oracle Linux

```
yum install -y mod_security mod_security_crs
```

Debian | Ubuntu

```
apt-get install -y modsecurity-crs libapache2-mod-security2
```

Configure Mod_Security

Some operating systems require additional steps to enable Mod_Security.

Debian | Ubuntu

Steps to enable Mod_Security.

```
cd /etc/modsecurity/
mv modsecurity.conf-recommended modsecurity.conf
```

Open the *modsecurity.conf* file in the vi-text editor with the following command:

```
vi modsecurity.conf
```

When using the vi editor, to make changes press **i** on the keyboard first to enter insert mode. Press **Esc** to exit insert mode.

The *modsecurity.conf* file requires the following line to be changed from:

```
#SecRuleEngine DetectionOnly
```

To:

```
SecRuleEngine on
```

When you have finished, save the changes in vi by typing:

```
:wq
```

and press **Enter**.

Download Rules File

Download the mod_security_excluded_rules.conf file for inclusion. This excludes all present rules that cause issues within the Nagios XI interface.

RHEL | CentOS | Oracle Linux

```
cd /etc/httpd/conf.d/
wget https://assets.nagios.com/downloads/nagiosxi/misc/mod_security_excluded_rules.conf
```

Debian | Ubuntu

```
cd /etc/modsecurity/
wget https://assets.nagios.com/downloads/nagiosxi/misc/mod_security_excluded_rules.conf
```

Restart Apache

Restart the Apache service to complete the integration using the following command:

RHEL 7+ | CentOS 7| Oracle Linux 7+

```
systemctl restart httpd.service
```

Debian | Ubuntu 16/18/20

```
systemctl restart apache2.service
```

Test

You should now open your Nagios XI interface and test that everything appears to be working as expected.

See the Troubleshooting section of this document if Nagios XI is not working as expected.

Troubleshooting

As the mod_security rules are updated and added to by OWASP, Trustwave, and other third parties, rules may occasionally cause Nagios XI to behave strangely or various functionality to stop working at all. The httpd error_log contains all Mod_Security related errors as well. These can be easily grepped for and added to the excluded rules configuration file.

The following command will list to screen what errors are being caused by Mod_Security rules. You can then attempt to use the same functionality that was causing issues, and ideally see the rule displayed.

```
tail -f /var/log/httpd/error_log | grep -o "/etc/httpd/modsecurity.d/activated_rules/.\{0,75\}"
```

The output will look like this:

```
/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"]
[line "77"] [id "950901"]
```

The **[id "...."]** is what we are looking for, to add to the excluded rules. Simply modify the file

```
/etc/modsecurity/mod_security_excluded_rules.conf
```

or

```
/etc/httpd/conf.d/mod_security_excluded_rules.conf
```

and add the new rule between <IfModule> statements like below:

```
<LocationMatch .*>
     <IfModule mod_security2.c>
          SecRuleRemoveById 981203
          SecRuleRemoveById 981204
          SecRuleRemoveById [ID Number]
     </IfModule>
</LocationMatch>
```

Restart Apache to finalize the changes (refer to the commands earlier in this document). Nagios XI should now function normally.

If you are experiencing many issues, it may be easier to output the error log searches to a temporary file and search it for unique rules after doing a few separate tasks within Nagios XI.

```
tail -f /var/log/httpd/error_log | grep -o "/etc/httpd/modsecurity.d/activated_rules/.\{0,75\}" >
/tmp/mod_sec.errors sort -u /tmp/mod_sec.errors
```

Finishing Up

Mod_Security will now be installed on your system, ready to start.

Still need installation help? We'll do it for free.

Schedule a free Quickstart session with our support team or contact sales at sales@nagios.com.

Visit Nagios Support Forum Visit Nagios Knowledge Base Schedule a Quickstart