How to Install Linux Malware Detect (LMD) and ClamAV on CentOS 7

Linux Malware Detect (LMD) is malware detector and scanner for Linux, designed for shared hosting environments. LMD is released under GNU GPLV2 license, it can be installed on cPanel WHM and Linux environments with together other detection tools such as ClamAV.

Clam AntiVirus (ClamAV) is an open source antivirus solution to detect trojans, malware, viruses and other malicious software. ClamAV supports multiple platforms including Linux, Windows, and MacOS.

On this page

In this tutorial,
I will show you how to install Linux Malware Detect (LMD) with Clam AntiVirus (ClamAV). I will use CentOS 7 as the operating system.

Prerequisite

- CentOS 7
- Root privileges

Step 1 - Install Epel repository and Mailx

Install the Epel (Extra Packages for Enterprise Linux) repository and the mailx command with yum. We need mailx installed on the system so that LMD can send the scan reports to your email address.

```
yum -y install epel-release
```

Install mailx so we can use the mail command on CentOS 7:

```
yum -y install mailx
```

Step 2 - Install Linux Malware Detect (LMD)

Linux Malware Detect is not available in CentOS or Epel repository, we need to install it manually from source.

Download LMD and extract it:

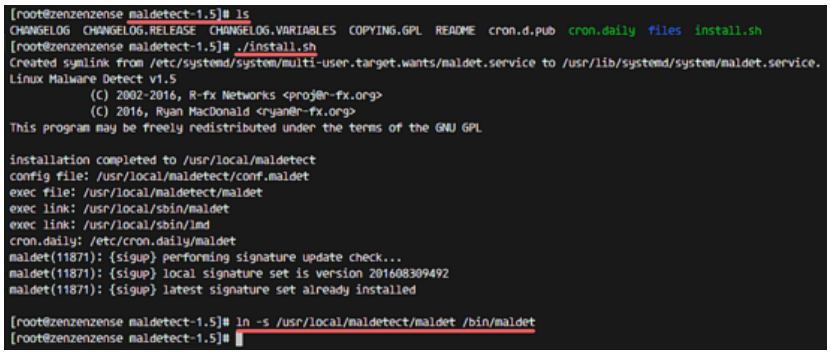
```
cd /tmp
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
tar -xzvf maldetect-current.tar.gz
```

Go to the maldetect directory and run the installer script 'install.sh' as root:

```
cd maldetect-1.5
./install.sh
```

Next, make a symlink to the maldet command in the /bin/ directory:

```
ln -s /usr/local/maldetect/maldet /bin/maldet
hash -r
```



Step 3 - Configure Linux Malware Detect (LMD)

LMD has benn installed into the '/usr/local/maldet/' directory. Go to that directory and edit the configuration file 'conf.maldet' with vim:

```
cd /usr/local/maldetect/
vim conf.maldet
```

Enable email alert by changing the value to '**1**' on line 16.

```
email_alert="1"
```

Type in your email address on line 21.

```
email_addr="root@zenzenzense.localdomain"
```

We will use the ClamAV clamscan binary as default scan engine because it provides a high-performance scan on large file sets. Change value to '**1**' on line 114.

```
scan_clamscan="1"
```

Next, enable quarantining to move malware to the quarantine automatically during the scan process. Change value to '**1**' on line 180.

```
quarantine_hits="1"
```

Change value to 1 on line 185 to enable clean based malware injections.

```
quarantine_clean="1"
```

Save and exit.

Step 4 - Install ClamAV

In this step, we will install Clam AntiVirus or ClamAV to get the best scanning results of LMD. ClamAV is available in the Epel repository (that we've installed in the first step).

Install ClamAV and ClamAV devel with yum:

```
yum -y install clamav clamav-devel
```

After ClamAV has been installed, update the ClamAV virus databases with the freshclam command:

```
freshclam
```

```
[root@zenzenzense ~]# freshclam
ClamAV update process started at Thu Oct  6 21:49:28 2016
main.cvd is up to date (version: 57, sigs: 4218790, f-level: 60, builder: amishhammer)
Downloading daily-22312.cdiff [100%]
Downloading daily-22313.cdiff [100%]
Downloading daily-22314.cdiff [100%]
Downloading daily-22315.cdiff [100%]
Downloading daily-22316.cdiff [100%]
daily.cld updated (version: 22316, sigs: 667069, f-level: 63, builder: neo)
bytecode.cld is up to date (version: 283, sigs: 53, f-level: 63, builder: neo)
Database updated (4885912 signatures) from database.clamav.net (IP: 155.98.64.87)
[root@zenzenzense ~]#
```

Step 5 - Testing LMD and ClamAV

We will test an LMD manual scan with the maldet command. We will use the maldet command to scan the web directory '/var/www/html/'.

Go to the web root directory and download some sample malware (eicar) with wget:

```
cd /var/www/html
wget http://www.eicar.org/download/eicar.com.txt
wget http://www.eicar.org/download/eicar_com.zip
wget http://www.eicar.org/download/eicarcom2.zip
```

Next, scan the web root directory with the maldet command below:

```
maldet -a /var/www/html
```

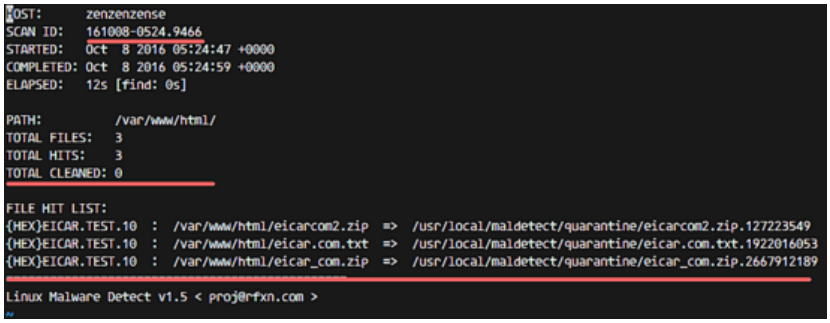
```
[root@zenzenzense html]# ll
total 16
-rw-r--r--. 1 nginx nginx  68 Oct  8 05:24 eicar.com.txt
-rw-r--r--. 1 nginx nginx 184 Oct  8 05:24 eicar_com.zip
-rw-r--r--. 1 nginx nginx 308 Oct  8 05:24 eicarcom2.zip
-rw-r--r--. 1 nginx nginx   6 Oct  6 21:37 index.html
[root@zenzenzense html]# maldet -a /var/www/html/
Linux Malware Detect v1.5
           (C) 2002-2016, R-fx Networks <proj@rfxn.com>
           (C) 2016, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(9466): {scan} signatures loaded: 10906 (8988 MD5 / 1918 HEX / 0 USER)
maldet(9466): {scan} building file list for /var/www/html/, this might take awhile...
maldet(9466): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
maldet(9466): {scan} file list completed in 0s, found 3 files...
maldet(9466): {scan} found clamav binary at /bin/clamscan, using clamav scanner engine...
maldet(9466): {scan} scan of /var/www/html/ (3 files) in progress...
maldet(9466): {scan} processing scan results for hits: 3 hits 0 cleaned
maldet(9466): {scan} scan completed on /var/www/html/: files 3, malware hits 3, cleaned hits 0, time 12s
maldet(9466): {scan} scan report saved, to view run: maldet --report 161008-0524.9466
maldet(9466): {alert} sent scan report to root@zenzenzense.localdomain
[root@zenzenzense html]# ll
total 4
-rw-r--r--. 1 nginx nginx 6 Oct  6 21:37 index.html
[root@zenzenzense html]#
```

You can see that LMD is using the ClamAV scanner engine to perform the scan, and there are 'malware hits 3' and the malware files were automatically moved to the quarantine directory.

Check the scan report with the command below:

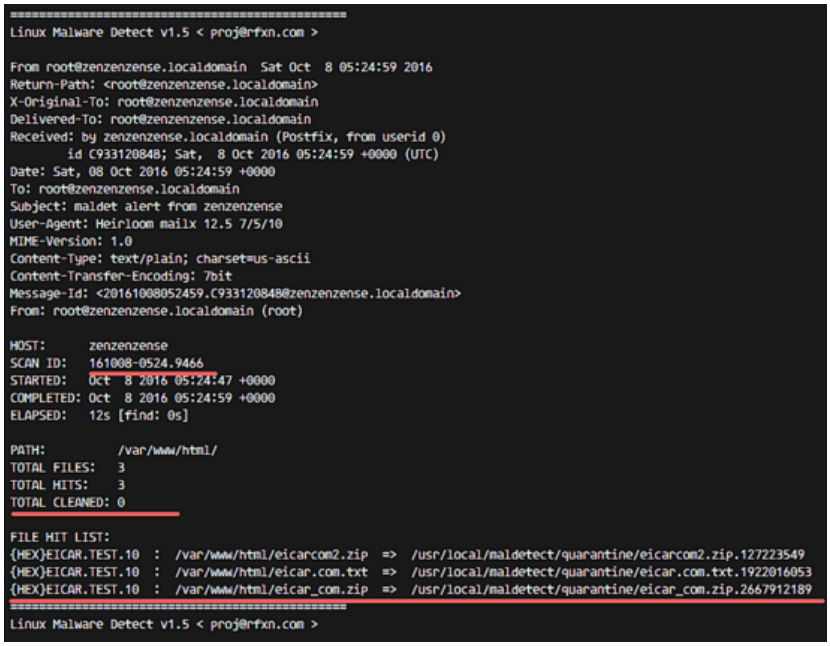
```
maldet --report 161008-0524.9466
```

SCANID = 161008-0524.9466 is found in the Maldet output.



Now check the email report from LMD:

```
tail -f /var/mail/root
```



As you can see, the scan report has been sent to the destination email address.

Step 6 - Other LMD Commands

Perform a scan for specific file extention only:

```
maldet -a /var/www/html/*.php
```

Get a list of all reports:

```
maldet -e list
```

```
[root@zenzenzense html]# maldet -e list
Linux Malware Detect v1.5
           (C) 2002-2016, R-fx Networks <proj@rfxn.com>
           (C) 2016, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

Oct  8 2016  05:40:22  |  SCAN  ID:  161008-0540.10366  |  FILES:  1  |  HITS:  1  |  CLEANED:  0
Oct  8 2016  05:38:59  |  SCAN  ID:  161008-0538.10039  |  FILES:  1  |  HITS:  1  |  CLEANED:  0
Oct  8 2016  05:24:47  |  SCAN  ID:  161008-0524.9466   |  FILES:  3  |  HITS:  3  |  CLEANED:  0
Oct  8 2016  05:19:33  |  SCAN  ID:  161008-0519.8900   |  FILES:  4  |  HITS:  4  |  CLEANED:  0
```

Scan files that have been created/modified in the last X days.

```
maldet -r /var/www/html/ 5
```

5 = the last days.

Restore files from the quarantine directory.

```
maldet -s SCANID
```

```
[root@zenzenzense html]# ll
total 4
-rw-r--r--. 1 nginx nginx 6 Oct  6 21:37 index.html
[root@zenzenzense html]# maldet -e list
Linux Malware Detect v1.5
           (C) 2002-2016, R-fx Networks <proj@rfxn.com>
           (C) 2016, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

Oct  8 2016  05:40:22  |  SCAN  ID:  161008-0540.10366  |  FILES:  1  |  HITS:  1  |  CLEANED:  0
Oct  8 2016  05:38:59  |  SCAN  ID:  161008-0538.10039  |  FILES:  1  |  HITS:  1  |  CLEANED:  0
Oct  8 2016  05:24:47  |  SCAN  ID:  161008-0524.9466   |  FILES:  3  |  HITS:  3  |  CLEANED:  0
Oct  8 2016  05:19:33  |  SCAN  ID:  161008-0519.8900   |  FILES:  4  |  HITS:  4  |  CLEANED:  0
[root@zenzenzense html]# maldet -s 161008-0524.9466
Linux Malware Detect v1.5
           (C) 2002-2016, R-fx Networks <proj@rfxn.com>
           (C) 2016, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(11481): {restore} quarantined file /usr/local/maldetect/quarantine/eicarcom2.zip.127223549 restored to /var/www/html/eicarcom2.zip
maldet(11481): {restore} quarantined file /usr/local/maldetect/quarantine/eicar.com.txt.1922016053 restored to /var/www/html/eicar.com.txt
maldet(11481): {restore} quarantined file /usr/local/maldetect/quarantine/eicar_com.zip.2667912189 restored to /var/www/html/eicar_com.zip
[root@zenzenzense html]# ll
total 16
-rw-r--r--. 1 nginx nginx  68 Oct  8 05:24 eicar.com.txt
-rw-r--r--. 1 nginx nginx 184 Oct  8 05:24 eicar_com.zip
-rw-r--r--. 1 nginx nginx 308 Oct  8 05:24 eicarcom2.zip
-rw-r--r--. 1 nginx nginx   6 Oct  6 21:37 index.html
[root@zenzenzense html]#
```

Enable monitoring of a directory.

```
maldet -m /var/www/html/
```

Check the monitor log file:

```
tail -f /usr/local/maldetect/logs/inotify_log
```

```
[root@zenzenzense ~]# maldet -m /var/www/html/
Linux Malware Detect v1.5
            (C) 2002-2016, R-fx Networks <proj@rfxn.com>
            (C) 2016, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(11878): {mon} added /var/www/html/ to inotify monitoring array
maldet(11878): {mon} starting inotify process on 1 paths, this might take awhile...
maldet(11878): {mon} inotify startup successful (pid: 11972)
maldet(11878): {mon} inotify monitoring log: /usr/local/maldetect/logs/inotify_log
[root@zenzenzense ~]# tail -f /usr/local/maldetect/logs/inotify_log
/usr/share/nginx/html/eicar_com.zip CREATE 08 Oct 05:09:01
/usr/share/nginx/html/eicar_com.zip MODIFY 08 Oct 05:09:01
Setting up watches.  Beware: since -r was given, this may take a while!
Watches established.
/usr/share/nginx/html/yuuki.txt CREATE 08 Oct 05:11:33
/usr/share/nginx/html/eicarcom2.zip CREATE 08 Oct 05:12:34
/usr/share/nginx/html/eicarcom2.zip MODIFY 08 Oct 05:12:34
/usr/share/nginx/html/eicarcom2.zip MOVED_FROM 08 Oct 05:13:12
Setting up watches.  Beware: since -r was given, this may take a while!
Watches established.
/var/www/html/eicarcom2.zip MOVED_FROM 08 Oct 06:10:28
/var/www/html/eicar.com.txt MOVED_FROM 08 Oct 06:10:28
/var/www/html/eicar_com.zip MOVED_FROM 08 Oct 06:10:28
/var/www/html/index.html MOVED_FROM 08 Oct 06:11:15
/var/www/html/haru.txt MOVED_TO 08 Oct 06:11:15
/var/www/html/haru.txt MOVED_FROM 08 Oct 06:11:35
/var/www/html/index.html MOVED_TO 08 Oct 06:11:35
```

Reference

- https://github.com/andrewelkins/Linux-Malware-Detect

Suggested articles

1 Comment(s)

Add comment

Name * Email *

p

Comments

From: Jack **at:** *2016-12-15 21:49:41* Reply

Hi, many thanks for this great document.
With standard install of ISPConfig on CentOS 7, mailx and epel are already installed, as well as clam but inotify is not, also you might add:
yum install -y inotify-tools
And another issue is that maldet does not find clamd:
[root@websrv logrotate.d]# tail -f /usr/local/maldetect/logs/event_logDec 15 22:22:13 websrv maldet(7136): {mon} warning clamd service not running; force-set monitor mode file scanning to every 120sDec 15 22:22:23 websrv maldet(7136): {mon} scanned 108 new/changed files with clamav engineDec 15 22:24:23 websrv maldet(7136): {mon} warning clamd service not running; force-set monitor mode file scanning to every 120sDec 15 22:24:32 websrv maldet(7136): {mon} scanned 127 new/changed files with clamav engineDec 15 22:26:32 websrv maldet(7136): {mon} warning clamd service not running; force-set monitor mode file scanning to every 120sDec 15 22:26:41 websrv maldet(7136): {mon} scanned 186 new/changed files with clamav engineDec 15 22:28:41 websrv maldet(7136): {mon} warning clamd service not running; force-set monitor mode file scanning to every 120sDec 15 22:28:50 websrv maldet(7136): {mon} scanned 128 new/changed files with clamav engine
But it works:
[root@websrv maldetect]# ps -afe | grep clamamavis 1641 1 1 21:35 ? 00:00:58 /usr/sbin/clamd -c /etc/clamd.d/amavisd.conf --foreground=yesroot 7767 1 0 22:11 pts/1 00:00:01 /usr/bin/inotifywait -r --fromfile /usr/local/maldetect/sess/inotify.paths.7136 --exclude (^/var/tmp/mysql.sock$|^/tmp/mysql.sock$|^/var/cache/buagent/md0.cache.data$|^/var/tmp/#sql_.*\.MYD$|^/tmp/#sql_.*\.MYD$|^/var/tmp/clamav-.*|^/tmp/clamav-.*|^/usr/local/maldetect*|^/dev/pts*|^/dev/null) --timefmt %d %b %H:%M:%S --format %w%f %e %T -m -e create,move,modify
But in our case amavis is the owner of the process, maybe we should change that somewhere but I don't know.
Do you have an idea?

Tutorial Info

Author:	Muhammad Arul
Published:	Oct 31, 2016
Tags:	centos, linux, security