KB Category:	**Internal**		
Author:	Jan Francis Lictao	Date:	**May 25, 2019**

Problem Description:	Installation of AntiVirus (ClamAV) to our Linux servers.
Symptoms and Cause of the issue:	No AntiVirus installed and it's required in PCIDSS Compliance.

Servers:
172.22.9.3 - GL2-VLIN-FIM01
172.17.0.124 - JKA-VLIN-FNP01
172.17.0.125 - JKA-VLIN-FIM01
172.17.0.3 - OSTicket
172.22.9.4 - GL2-VLIN-NMS01

Procedures:
Step 1: Login to the server via SSH and switch to super user.

Step 2: Install ClamAV dependencies and developer tools as prerequisites.

[root@osticket ~]# yum groupinstall "Development Tools"

[root@osticket ~]#yum install openssl openssl-devel libcurl-devel zlib-devel libpng-devel libxml2-devel json-c-devel bzip2-devel pcre2-devel ncurses-devel

[root@osticket ~]#yum install sendmail sendmail-devel

Step 3: Download the latest and stable installer of ClamAV using wget command.

[root@osticket ~]# wget https://www.clamav.net/downloads/production/clamav-0.101.2.tar.gz

Step 4: Extract now the downloaded installer file.
Note: Installer has been downloaded in /root/ directory

[root@osticket ~]# ls -ltrh clamav-0.101.2.tar.gz
-rw-r--r-- 1 root root 21M Mar 27 04:30 clamav-0.101.2.tar.gz

[root@osticket ~]# tar -xzf clamav-0.101.2.tar.gz

Step 5: After extracting, navigate to the extracted directory.

[root@osticket ~]# cd /root/clamav-0.101.2

Step 6: Configure the build so that ClamAV script should detect each of above dependencies automatically. Once configure is done, it will print a summary

[root@osticket clamav-0.101.2]# ./configure --enable-check

```
configure: Summary of detected features follows
        OS        : linux-gnu
        pthreads    : yes (-lpthread)
  configure: Summary of miscellaneous features
        check      : -lcheck_pic -pthread -lrt -lm -lsubunit
        fanotify    : yes
        fdpassing   : 1
        IPv6       : yes
  configure: Summary of optional tools
        clamdtop    : -lncurses (auto)
        milter      : yes (disabled)
        clamsubmit  : yes (libjson-c-dev found at /usr), libcurl-devel found at /usr)
  configure: Summary of engine performance features
        release mode: yes
        llvm       : no (disabled)
        mempool     : yes
  configure: Summary of engine detection features
        bzip2      : ok
        zlib       : /usr
        unrar      : yes
        preclass    : yes (libjson-c-dev found at /usr)
        pcre       : /usr
        libmspack   : yes (Internal)
        libxml2     : yes, from /usr
        yara       : yes
        fts        : yes (libc)
```

Step 7: Additional configuration.

Install the clamav even without root privileges
./configure --with-systemdsystemunitdir=no

Install the clamav configuration to /etc instead of /usr/local/etc
./configure -–sysconfdir=/etc

Install ClamAV to a directory other than /usr/local
./configure --prefix=`pwd`/install

freshclam and clamd will run with root privileges
./configure --disable-clamav

Step 8: Compile and install the ClamAV.

[root@osticket ~]#make -j2
[root@osticket ~]#make check
[root@osticket ~]#make install

Step 9: Once installation is successfully; we need to configure the freshclam to download updates and enable some options.

[root@osticket clamav-0.101.2]# cp /usr/local/etc/freshclam.conf.sample /usr/local/etc/freshclam.conf

Options to enable include:
LogTime
LogRotate
NotifyClamd
DatabaseOwner

Step 10: Create the database directory.

[root@osticket ~]#mkdir /usr/local/share/clamav

Step 11: Create clamav group and clamav user account to run clamd, clamscan and freshclam. Then set ownership of the database directory.

*[root@osticket ~]#*groupadd clamav
*[root@osticket ~]#*useradd -g clamav -s /bin/false -c “Clam Antivirus” clamav
[root@osticket ~]#sudo chown -R clamav:clamav /usr/local/share/clamav

Step 11: Create script to run scan every day and send email if infected file is detected.

clamscan_daily.sh

Step 12: Enable ClamAV database updates by adding freshclam command at crontab to run every 12 AM of the day.

[root@osticket ~]# crontab -e

*0 0 * * * /usr/local/bin/freshclam*

Verification Steps:
Step 1: Run **freshclam** to check if the clamav database is updated.

[root@osticket ~]# freshclam
Thu May 30 21:40:18 2019 -> ClamAV update process started at Thu May 30 21:40:18 2019
Thu May 30 21:40:18 2019 -> main.cvd is up to date (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Thu May 30 21:40:18 2019 -> daily.cld is up to date (version: 25465, sigs: 1584853, f-level: 63, builder: raynman)
Thu May 30 21:40:18 2019 -> bytecode.cvd is up to date (version: 328, sigs: 94, f-level: 63, builder: neo)

Step 2: Try scan a directory using clamscan command and result will display.

[root@osticket ~]# clamscan /home/jlictao

---------- SCAN SUMMARY ----------
Known viruses: 6142017
Engine version: 0.101.2
Scanned directories: 1
Scanned files: 7
Infected files: 0
Data scanned: 0.14 MB
Data read: 0.07 MB (ratio 2.00:1)
Time: 50.507 sec (0 m 50 s)