

Anti-Virus

Considerations

- Install And Enable Anti-Virus Software
- Configure Daily Scans

Install And Enable Anti-Virus Software

Clamav installation

Preparation for ClamAV installation

1. Ensure that the EPEL repository has been installed

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

```
yum clean all
```

ClamAV installation

1. Run the command below to install ClamAV

```
yum -y install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd
```

Configuring ClamAV

1. Remove "Example" string from the configuration file

```
sed -i -e "s/^Example/#Example/" /etc/clamd.d/scan.conf
```

2. Edit scan.conf

```
Open scan.conf for editing
```

```
=====
```

```
vi /etc/clamd.d/scan.conf
```

Look for and the change line from

```
=====
```

```
#LocalSocket /var/run/clamd.scan/clamd.sock
```

to

```
LocalSocket /var/run/clamd.scan/clamd.sock
```

Configure FreshClam

1. Remove "Example" string from ClamAV's freshclam update engine configuration file

```
sed -i -e "s/^Example/#Example/" /etc/freshclam.conf
```

2. Run the virus definition database update

```
freshclam
```

Start and enable Clamd services

1. Use the following commands to start and enable Clamd services

```
systemctl start clamd@scan
```

```
systemctl enable clamd@scan
```

Configure Daily Scans

Configure ClamAV for daily scans

1. Create and edit the file clamscan_daily in the folder /etc/cron.daily

```
Create clamscan_daily
=====

vi /etc/cron.daily

=====

Add below to file changing the option

EMAIL_FROM="from email address";
EMAIL_TO="to email address";
DIRTOSCAN="list of directories";

as required
=====

#!/bin/bash
LOGFILE="/var/log/clamav/clamav-$(date +%Y-%m-%d).log";
EMAIL_MSG="Please see the log file attached.";
EMAIL_FROM="from email address";
EMAIL_TO="to email address";
DIRTOSCAN="list of directories";

for S in ${DIRTOSCAN}; do
    DIRSIZE=$(du -sh "$S" 2>/dev/null | cut -f1);

    echo "Starting a daily scan of "$S" directory.
    Amount of data to be scanned is "$DIRSIZE".";

    clamscan -ri "$S" >> "$LOGFILE";

    # get the value of "Infected lines"
```

```
MALWARE=$(tail "$LOGFILE"| grep Infected| cut -d" " -f3);

# if the value is not equal to zero, send an email with the log file attached
if [ "$MALWARE" -ne "0" ];then
# using heirloom-mailx below
echo "$EMAIL_MSG"| mail -a "$LOGFILE" -s "Malware Found" -r "$EMAIL_FROM" "$EMAIL_TO";
fi
done

exit 0
```