# 01_Linuxサーバデータベース -
# サーバのウイルススキャン。(ClamAVとinotifyによる指定ディレクトリの自動スキャン)

## 概要

Redmineの稼働サーバにウィルス対策ソフトClam-AVをインストールし、不審なファイルのアップロードを防ぎます。

### 動作要件

- スキャン対象はRedmineの添付ファイル格納ディレクトリです。
    - それ以外にも転用できるようにスクリプトを変数で定義しています。
- inotifyサービスを利用して、スキャン対象を絞ります。
- スキャンするタイミングは上記格納ディレクトリにファイルがアップロードされたときです。これによってCPU消費を節約します。
- ClamAVによって不審なファイルと判断された場合、そのファイルを削除します。その後、詳細はログに出力されます。

## 動作確認環境

- Ubuntu 20.04
- ClamAV 0.103.8

## 手順

- サーバのターミナルからコマンドラインで設定を行います。
- パッケージ管理はaptitudeを利用しています。好みに合わせてaptに置き換えてください。

### さっくりとした手順

1. ClamAVをインストールします。
2. 最新のウィルス定義ファイルがダウンロードできることを確認します。
3. ClamAVの動作を確認します。
4. inotifyサービスをインストールします。
5. チェックスクリプトを作成します。
6. スクリプトをサービス化します。
7. サービスの動作を確認します。

### ClamAVの設定と確認

#### ClamAVのインストール

```
sudo aptitude update

sudo aptitude install clamav clamav-daemon
```

#### ウィルス定義ファイルの更新

```
sudo freshclam
```

で定義ファイルを更新しようとしたところ、以下のエラーが出ました。

```
sudo freshclam

ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
```

対処を行います。

```
sudo lsof /var/log/clamav/freshclam.log

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
freshclam 7001 clamav 3wW REG 202,1 2161 2319263 /var/log/clamav/freshclam.log
# この時に出てきたPIDを控えておきます。
```

このプロセスを停止します。

```
sudo ki -9 7001
# 出てきたPIDを指定します
```

ログファイルのパーミッション変更

```
sudo chmo -R 777 /var/log/clamav/
```

上記を実施後、

```
sudo freshclam
```

定義ファイルが更新されることを確認しました。

**ウイルス定義ファイル自動更新**

```
sudo systemctl start clamav-freshclam.service

sudo systemctl enable clamav-freshclam.service

systemctl status clamav-freshclam.service
# active (running)を確認します
```

**ClamAVの動作確認**

- バージョン確認

```
clamscan --version
ClamAV 0.103.8/26829/Thu Mar 2 20:16:49 2023
# 2023/03/03、aptでインストールした際のバージョン
```

- eicarテストファイルによる確認

```
cd ~

wget http://www.eicar.org/download/eicar.com

clamscan eicar.com
```

- テスト結果

```
Win.Test.EICAR_HDB-1 FOUND

---------- SCAN SUMMARY ----------
Known viruses: 8654357
Engine version: 0.103.8
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
```

が表示されたので、機能していることを確認です。

```
rm eicar.com
```

でテストファイルを削除します。（スキャンしただけなのでファイルの自動削除は行われません）

## スクリプト作成

**inotifyのインストール**

```
sudo aptitude install inotify-tools
```

**スクリプト生成**

- 以下のスクリプトを教義・信仰に沿ったエディタで作成します。
    - スクリプト名:clamav-inotify.sh

```
#!/bin/bash

##　変数ここから
#　監視対象のディレクトリを指定してください。
WATCH_DIR="/var/lib/redmine/files"

#　スキャン対象の最大サイズを指定してください。
#　Redmineのようにアップロード上限をWeb画面から設定できる場合、そのサイズに合わせます。
MAX_FILE_SIZE="10240M"

#　スキャンログのパスを定義します。
SCAN_LOG="/var/log/redmine/redmine-scan.log"
##　変数ここまで


#　監視対象のディレクトリ（およびサブディレクトリ）に新しいファイルが作成されたときに、そのファイルをスキャンする処理を行います
inotifywait -m -r -e　create--format '%f' "$WATCH_DIR"　|
while read FILE
do
　#　新しいファイルがディレクトリでなく、かつ隠しファイルでないことを確認します。
　if [ ! -d "$FILE" ] && [ "$(echo "$FILE"　cut -c1)" != "." ]; then
　　#　ClamAVを使用して新しいファイルをスキャンします。
　　RESULT=$(clamscan --recursive --max-filesize="$MAX_FILE_SIZE" "$WATCH_DIR/$FILE")
　　if echo "$RESULT"　grep -q "　FOUND; then
　　　echo "ウイルスが検出されました: $FILE" >> "$SCAN_LOG"
　　　rm "$WATCH_DIR/$FILE"
　　else
　　　echo "スキャンが完了しました: $FILE" >> "$SCAN_LOG"
　　fi
　　fi
done
```

- 実行権付与

```
sudo　chmo　+x　clamav-inotify.sh
```

**スクリプトのサービス化**

- 以下のスクリプトを教義・信仰に沿ったエディタで作成します。
    - 配置ディレクトリ:/etc/systemd/system/
    - サービス名:clamav-inotify.service

- ファイル内容

```
[Unit]
Description=ClamAV　Inotify　Service
After=network.target

[Service]
Type=simple
ExecStart=/usr/bin/bash　/home/hoge/clamav-inotify.sh
#　上記のスクリプトをフルパスで指定します
Restart=always
User=root

[Install]
WantedBy=multi-user.target
```

- サービスの有効化

sudo systemctl enable clamav-inotify.service

sudo systemctl start clamav-inotify.service

systemctl status clamav-inotify.service
# active (runnning)を確認します

## 動作確認

### テストウィルスを配置→削除確認

cd /var/lib/redmine/files
# スクリプトで指定したスキャン対象ディレクトリに移動します。

sudo wget http://www.eicar.org/download/eicar.com
# eicarテストウィルスをダウンロードします。

ls -l eicar.com
# ファイルがある状態から削除されていることを確認します。

### ログ確認

cat /var/log/redmine/redmine-scan.log
# スクリプトで指定したログ

以下のようにログに出れば成功です。

/mnt/wasabi/redmine/files/eicar.com: Win.Test.EICAR_HDB-1 FOUND

---------- SCAN SUMMARY ----------
Known viruses: 8654357
Engine version: 0.103.8
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 34.852 sec (0 m 34 s)
Start Date: 2023:19:03 11:50:39
End Date: 2023:19:03 11:51:14
ウイルスが検出されました: eicar.com

# 動作確認日

2023/03/03

### ファイル

| | | | |
|---|---|---|---|
| 0_春節でパソコンを使うお姉さん2024010507(ftmm).jpg | 225 KB | 2024/01/05 | 手動人形 |