01_Linuxサーバデータベース - Apacheで特定のアクセス元からの通常アクセスをログに残さない設定。

概要

Webサービスの運用時、「誰がいつどこにアクセスしたか」を判別するアクセスログはとても重要なものです。
ではありますが、Webアクセス解析時に自分のアクセスログが邪魔になるケースがありました。

そこで、Apacheの設定ファイルで特定のアクセス元からのログを残さないようにしました。

確認環境

- OS : Ubuntu 20.04 LTS
- Apache 2.4.55

前提

- 大本のコンフィグ(httpd.conf)ではなくバーチャルサイトで設定していること。
- Apache設定ファイルに管理者権限で設定ができること。
- 除外するIP/NWに対し、合意が取れていること。

注意事項

- この方法でエラーログの除外設定はできません。

実施した手順

ほぼ全てSSHクライアントターミナルからの操作です。

さっくりとした手順

1. コンフィグのバックアップを取ります。
2. ログを残さない除外IP/NWを加えます。
3. コンフィグの整合性を確認し、設定を反映します。
4. 除外したIP/NWからのアクセスログが出ないことを確認します。

コンフィグ設定

コンフィグのバックアップを取ります。

```
sudo  c -pi  /etc/apache2/sites-available/sites.conf  /path/to/backup/directory/sites.co$(date  +%Y%m%)l
#  自分が設定しているバーチャルサイトのコンフィグ  /  バックアップディレクトリに合わせます。

diff -u  /etc/apache2/sites-available/sites.conf  /path/to/backup/directory/sites.co$(date  +%Y%m%)l
#  差分が無いことでバックアップが取れていることを確認します。
```

コンフィグファイルを編集します。

```
sudo vi  /etc/apache2/sites-available/sites.conf
#  教義・信仰に従ったエディタで編集してください。
```

編集例

ここでは、以下の設定とします。

- 除外IP: 192.168.1.11
- 除外NW: 192.168.2.0/24
- アクセスログの格納場所: /var/log/redmine/access.log

```
#  以下のIP/NWはアクセスログに記録させません
SetEnvIf Remote_Addr  "192.168.1.11"  dontlog
SetEnvIf Remote_Addr  "^192\.168\.2\."  dontlog
CustomLog  /var/log/redmine/access.log  combined  env=!dontlog
```

保存後、以下のような差分を確認します。

```
diff -u  /path/to/backup/directory/sites.con$(date  +%Y%m%)  /etc/apache2/sites-available/sites.conf
```

- ●差分

```
+          #  以下のIP/NWはアクセスログに記録させません
+          SetEnvIf  Remote_Addr  "192.168.1.11"  dontlog
+          SetEnvIf  Remote_Addr  "^192\.168\.2\."  dontlog
-          CustomLog  /var/log/redmine/access.log  combined
+          CustomLog  /var/log/redmine/access.log  combined  env=!dontlog
```

設定反映

コンフィグの整合性を確認後に設定を反映します。

```
sudo apache2ctl  configtest
#  Syntax  OKを確認します。

systemctl  status  apache2.service
#  active  (running)を確認します。

sudo systemctl  restart  apache2.service

systemctl  status  apache2.service
#  active  (running)を確認します。
```

動作確認

設定後の動作を確認します。

- ●アクセスログ確認コマンド発行

```
tail -f  /var/log/redmine/access.log
#  自分の環境(設定したアクセスログ)に合わせます。
```

- ●エラーログ確認コマンド発行

※別ターミナルで開きます。

```
tail -f  /var/log/redmine/error.log
#  自分の環境(設定したエラーログ)に合わせます。
```

●ブラウザで以下を実施

1. 設定したIP / NWから設定対象のWebサイトにアクセスする。
    - 設定したIP / NWからのアクセスログが出ないこと。
2. 設定していないIP / NWから設定対象のWebサイトにアクセスする。
    - 設定していないIP / NWからのアクセスログが出ること。
3. 設定したIP / NWから設定対象のWebサイトにアクセスするがエラーを起こす。(404/403エラーなど)
    - 設定したIP / NWからのエラーログが出ること。
4. 設定していないIP / NWから設定対象のWebサイトにアクセスするがエラーを起こす。(404/403エラーなど)
    - 設定していないIP / NWからのエラーログが出ること。

ファイル

apache_logo.jpg	153 KB	2023/11/14	手動人形