Lsctl による Linux Security 64 の設定方法

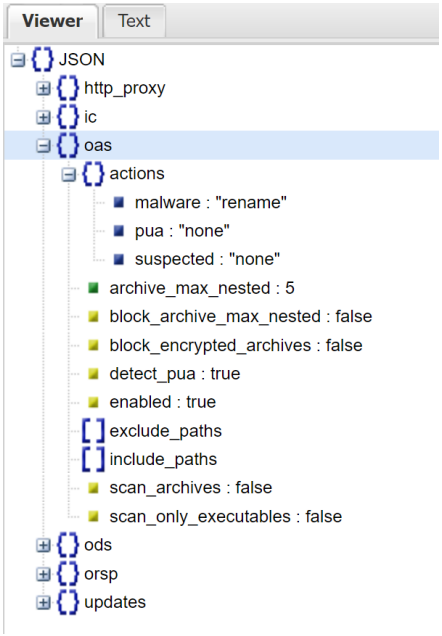
このナレッジでは Policy Manager(PM)を利用せずスタンアロン運用されている Linux Security 64(LS64) に対し、Lsctl コマンドを使用して設定を反映させる手法を解説いたします。

シナリオ 1(単一の Key:機能オン・オフ等)

リアルタイムスキャン(On Access Scan:oas)の Malware(ウイルス)検知時の処理を”rename”から”remove”に変更する。

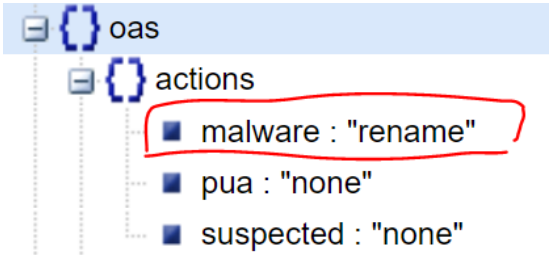
1. LS64 の現在の設定を確認します。

   /opt/f-secure/linuxsecurity/bin/lsctl get　を実行



※JSON 形式のテキストデータが表示されます。この例では JSON ビューワを利用し、見やすい形に整形しています。外部サイト: http://jsonviewer.stack.hu/

※JSON は“Key: Value”形式で形成されるツリー階層構造のデータ集合体です。この例では“oas”に“actions”→“malware”という順で Key がネストされています。コロン(:)右側の”rename”が Value です。



2. 下記コマンドで Key “malware” の Value を” remove” に変更します。

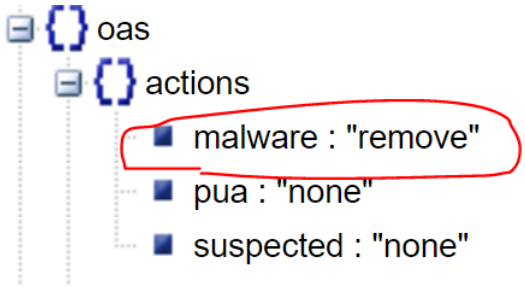
   /opt/f-secure/linuxsecurity/bin/lsctl set oas actions malware remove

   ※コマンドフォーマット解説

```
# /opt/f-secure/linuxsecurity/bin/lsctl set oas actions malware remove
                                          対象keyまでのツリー構造を羅列 Valueを記述
```

3. 設定が変更された事を確認します。

   /opt/f-secure/linuxsecurity/bin/lsctl get　を実行



   ※malware の value が remove に設定されています。

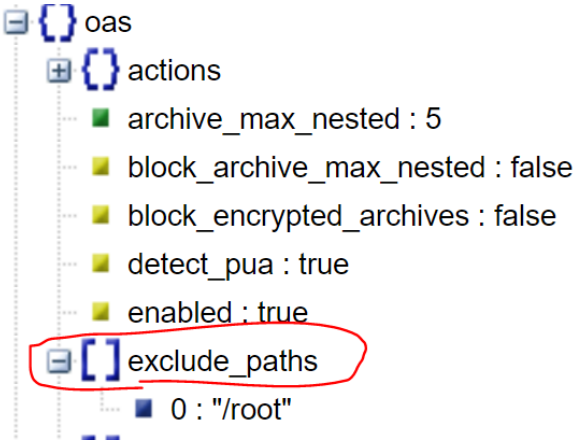
4. 以上

シナリオ 2(配列の Key:スキャン対象/除外/URL の入力等)

リアルタイムスキャン(On Access Scan:oas)の除外フォルダを追加する。

1. LS64 の現在の設定を取得します。

   /opt/f-secure/linuxsecurity/bin/lsctl get を実行します。



※“exclude_paths“が Key となりますが、数列形式の Value を必要とします。
※この例では既に/root を除外フォルダとして登録しています。

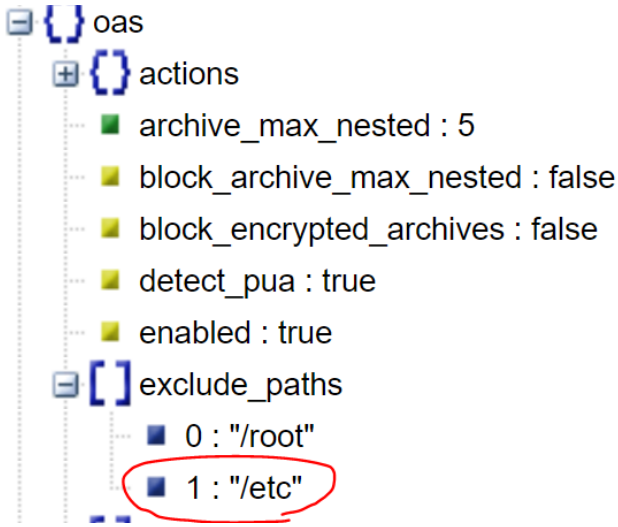
2. 下記コマンドで/etc を除外フォルダの配列に追加します。

   /opt/f-secure/linuxsecurity/bin/lsctl add oas exclude_paths /etc

   ※add を delete に変更すると配列からの削除が可能です。

3. 設定が変更された事を確認します。

   /opt/f-secure/linuxsecurity/bin/lsctl get　を実行します。



※/etc が除外フォルダとして追加されました。

4. 以上

JSON データ操作の詳細については専門的知識を必要とする分野となります。LS64 の設定を簡単に実施したい場合、Policy Manager のご利用をお勧めいたします。

Lsctl で設定可能な Key の一覧は下記の URL でご確認ください。
https://help.f-secure.com/product.html#business/linux-security-64/latest/ja/concept_61A4E8E64D5B4402B2E1B3616075EDC9-latest-ja