

Suricata IDS Rule-Set Manager

Rule-manager is a set of CLI scripts in python which were integrated into Flowmon in order to help users better navigate Flowmon IDS Probe rulesets they are using. This tool enables user to gain insight into the structure of rules and rule groups creating a given ruleset as well as control which rule categories to enable or disable [1].

This document contains basic instructions for using rule-manager set of CLI scripts integrated to the Flowmon Platform. It includes the description of basic rule-manager commands that can be executed from the command-line of the Flowmon appliance [1].

Table of Contents

<i>Suricata IDS Rule-Set Manager.....</i>	<i>1</i>
<i>Introduction.....</i>	<i>1</i>
<i>Purpose of rule-manager</i>	<i>3</i>
<i>Usage in the command line.....</i>	<i>4</i>
Ruleset statistics	5
Rule-trigger statistics	6
Generate suppress or threshold command.....	7
Enable and Disable rules.....	8
List ruleset groups.....	10
Check ruleset for validity	11
<i>References</i>	<i>12</i>

Introduction

Suricata is an Intrusion detection system (IDS) that detects potential threats in the network traffic. For the detection of these threats, it uses so-called signatures. A signature represents a structured list of rules that describes a threat based on the content of packets. An IDS system then inspects network traffic and applies these rules to each packet that comes through the IDS system. If rules stated in the signature are satisfied for the inspected packet, the IDS system generates an alert to notify the user [1].

For management of the rules, Flowmon IDS Probe uses preconfigured Suricata-Update tool. The tool gathers rules from multiple sources combining them into one suricata.rules file [1].

By default, the tool is configured to gather rules from two sources [1]:

1. **Flowmon Services** (Remote Rule Source)
 - a. Flowmon copy of [Emerging Threats Open Rules](#).
 - b. If the services.flowmon.com is not reachable, offline backup is used.
2. **/data/idsp/user-config/rules** (Local Rule Source)
 - a. All files ending in .rules inside this folder are loaded.
 - b. The directory is empty after a new installation. The folder is intended to be used for the user-defined rules.

The rules sources can be adjusted via configuration files [1]:

1. **/data/idsp/user-config/update.yaml**

- a. Attributes sources and local can be used to add additional remote or local sources. Default sources provided by the Flowmon IDS Probe are not visible in this configuration file.
- b. Examples for sources attribute:

```
# Remote rule sources. Simply a list of URLs.
sources:
# Emerging Threats Open with the Suricata version dynamically replaced.
# -
https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.tar.gz
# The SSL blacklist, which is just a standalone rule file
# - https://sslbl.abuse.ch/blacklist/sslblacklist.rules
```

2. **/data/idsp/user-config/flowmon-idsp-suricata-update.yaml**

- a. Attribute enable_flowmon_rules_feed allows you to disable the default rules from Flowmon Services feed. Deactivation is useful for completely replacing default rules with your own rules source.

Suricata-Update tool allows users to customize rulesets via separated configuration files. The order of application of configuration files and their meaning is following [1]:

1. **/data/idsp/user-config/disable.conf** (deactivate rules)
2. **/data/idsp/user-config/enable.conf** (activate deactivated rules)
3. **/data/idsp/user-config/drop.conf** (convert rules action to “drop”, not usable for IDSP)
4. **/data/idsp/user-config/modify.conf** (rewrite rules definition)

Configuration files inside /data/idsp/user-config/ folder can be recreated (if they are missing or invalid) by copying their original version in the following way:

```
cp /data/components/flowmon-idsp-suricata-update/etc/suricata/* /data/idsp/user-config/
```

The configuration will be applied during the next execution of the Suricata-Update tool. The tool is scheduled to be executed every hour. If you want to speed up the process, you can manually restart the service by executing command:

```
sudo systemctl restart flowmon-idsp-suricata-update
```

For more information about suricata-update tool configuration files and rule matching please visit [the official documentation](#) [1].

Please note that Flowmon IDS Probe uses own service for executing suricata-update tool. **Do not run suricata-update command** directly [1].

Purpose of rule-manager

Rule-manager was created in order to help IDS administrators navigate rule sources they are using for their Suricata IDS. For instance [Emerging Threats Open Rules](#) rule source contains thousands of rules in more than 50 rule groups.

Since not all rule groups or all rules within a given rule group from this rule source are suitable for given application of Flowmon IDS Probe, disabling these unnecessary rules can reduce the amount of generated alerts with little informational value from security perspective or even false positive alerts and help improve performance of Flowmon IDS Probe.

Rule-manager allows administrator to identify all local and remote rule sources applied for Flowmon IDS Probe on a given Flowmon Appliance instance. As well as show rule groups which belong to a given rule source as well as their description.

Furthermore it allows for administrator to calculate statistical data about rules in a given ruleset file based on the metadata attribute. This data can then be used by administrator to disable or re-enable rule categories with specified metadata attributes to tailor the ruleset used by his Flowmon IDS Probe instance according to his needs.

In addition to that the program allows the administrator to check rule trigger statistics for specified metadata *keyword* and *value* from detected events which are stored in **/data/idsp/outputs/eve.json** file. This data can then be combined to suppress or threshold generating alerts from uninteresting events detected. Rule-manager can generate suppress or threshold command for a given signature which can then be saved in configuration file **/data/idsp/user-config/threshold.config**. After that the events specified by suppress or threshold will be displayed accordingly.

Usage in the command line

Rule-manager can be run as a command from the command-line of the Flowmon appliance. Bellow we provide a list of program functionalities along with their example usage:

```
-h, --help                show this help message and exit

-s ['<keyword>' or '<keyword> <keyword_value>' ...], --stats ['<keyword>' or
'<keyword> <keyword_value>' ...]
    Shows statistical data about number of rules with given keyword.If
    none are provided lists all
    keywords

-r <keyword> <value> <N>, --rule-trigger-stats <keyword> <value> <N>
    Shows statistical data about first N number of rule hits with
    matching key value pair, sorted
    descending by number of rule hits.

-t <gid> <sid> <type> <track> count seconds, --generate-threshold <gid> <sid>
<type> <track> count seconds
    Generates threshold command to create threshold for a given rule.
    You can add the command to
    threshold config - threshold.conf

-sp <gid> <sid> <track> <ip>, --generate-supress <gid> <sid> <track> <ip>
    Generates supress command to supress alerts for a given rule. You
    can add the command to
    threshold config - threshold.conf

-f <path>, --file <path>
    File to calculate stats on, use with -s, -r. Default -s file
    /data/idsp/rules/suricata.rules,
    Default -r file /data/idsp/outputs/eve.json

-e <keyword> <value>, --enable-category <keyword> <value>
    Enable rules with matching key-value.

-d <keyword> <value>, --disable-category <keyword> <value>
    Disable rules with matching key-value.

-g, --list-used-groups
    Return a list of all used rule groups (.rules files).

-u, --update-used-groups
    Updates the list of used rule groups in (sourceList.json) based on
    used rule sources.

-l [<groupname>], --list-used-groups-long [<groupname>]
    Return a list of all used rule groups (.rules files) with
    descriptions from (sourceList.json)

--set-group-description <groupname> <description>
    Sets group description in sourceList.json

-ldc, --list-disabled-categories
    Return a list of all disabled rule categories

-c <path>, --check-rules-syntax <path>
    Checks the syntax of rules in .rules file.

-o <filename>, --output <filename>
    Write output to a specified file.
```

Ruleset statistics

```
[flowmon@flowmon ~]$ rule-manager -s
```

Statistics option of the program can be used to display metadata keywords used in a given ruleset along with the amount of enabled and disabled rules with a given metadata keyword.

```
[flowmon@localhost ~]$ rule-manager -s
All Signatures:
Total Signatures: 52347
Enabled Signatures: 24854 (47.48 %)
Disabled Signatures: 27493 (52.52 %)

KEYWORD: SID Total: 52347; Enabled: 24854 (47.48 %); Disabled: 27493 (52.52 %)
KEYWORD: AFFECTED_PRODUCT Total: 21404; Enabled: 12276 (57.35 %); Disabled: 9128 (42.65 %)
KEYWORD: ATTACK_TARGET Total: 36714; Enabled: 18492 (50.37 %); Disabled: 18222 (49.63 %)
KEYWORD: CREATED_AT Total: 51973; Enabled: 24851 (47.82 %); Disabled: 27122 (52.18 %)
KEYWORD: DEPLOYMENT Total: 37014; Enabled: 18761 (50.69 %); Disabled: 18253 (49.31 %)
KEYWORD: SIGNATURE_SEVERITY Total: 36847; Enabled: 18594 (50.46 %); Disabled: 18253 (49.54 %)
KEYWORD: TAG Total: 17293; Enabled: 7784 (45.01 %); Disabled: 9509 (54.99 %)
KEYWORD: UPDATED_AT Total: 51973; Enabled: 24851 (47.82 %); Disabled: 27122 (52.18 %)
KEYWORD: CLASSTYPE Total: 52322; Enabled: 24854 (47.5 %); Disabled: 27468 (52.5 %)
KEYWORD: FORMER_CATEGORY Total: 29620; Enabled: 16961 (57.26 %); Disabled: 12659 (42.74 %)
KEYWORD: PERFORMANCE_IMPACT Total: 14915; Enabled: 7138 (47.86 %); Disabled: 7777 (52.14 %)
KEYWORD: CONFIDENCE Total: 5635; Enabled: 2900 (51.46 %); Disabled: 2735 (48.54 %)
KEYWORD: REVIEWED_AT Total: 4704; Enabled: 1726 (36.69 %); Disabled: 2978 (63.31 %)
KEYWORD: CVE Total: 1850; Enabled: 1437 (77.68 %); Disabled: 413 (22.32 %)
KEYWORD: MITRE_TACTIC_ID Total: 8662; Enabled: 3391 (39.15 %); Disabled: 5271 (60.85 %)
KEYWORD: MITRE_TACTIC_NAME Total: 8662; Enabled: 3391 (39.15 %); Disabled: 5271 (60.85 %)
KEYWORD: MITRE_TECHNIQUE_ID Total: 8662; Enabled: 3391 (39.15 %); Disabled: 5271 (60.85 %)
KEYWORD: MITRE_TECHNIQUE_NAME Total: 8662; Enabled: 3391 (39.15 %); Disabled: 5271 (60.85 %)
KEYWORD: MALWARE_FAMILY Total: 7632; Enabled: 5921 (77.58 %); Disabled: 1711 (22.42 %)
KEYWORD: DEPRECATION_REASON Total: 2581; Enabled: 6 (0.23 %); Disabled: 2575 (99.77 %)
KEYWORD: FORMER_SID Total: 138; Enabled: 90 (65.22 %); Disabled: 48 (34.78 %)
KEYWORD: TLS_STATE Total: 183; Enabled: 148 (80.87 %); Disabled: 35 (19.13 %)
```

```
[flowmon@flowmon ~]$ rule-manager -s deployment signature_severity
```

When additional metadata keywords are supplied to the statistics options it will display values of specified metadata keywords present in a given ruleset along with the amount of enabled and disabled rules with a given metadata keyword.

```
[flowmon@localhost ~]$ rule-manager -s deployment signature_severity
All Signatures:
Total Signatures: 52347
Enabled Signatures: 24854 (47.48 %)
Disabled Signatures: 27493 (52.52 %)

KEYWORD: DEPLOYMENT Total: 37014; Enabled: 18761 (50.69 %); Disabled: 18253 (49.31 %)
VALUES:
  alert_only Total: 48; Enabled: 38 (79.17 %); Disabled: 10 (20.83 %)
  datacenter Total: 5397; Enabled: 370 (6.86 %); Disabled: 5027 (93.14 %)
  internal Total: 1189; Enabled: 802 (67.45 %); Disabled: 387 (32.55 %)
  internet Total: 156; Enabled: 48 (30.77 %); Disabled: 108 (69.23 %)
  perimeter Total: 31655; Enabled: 18342 (57.94 %); Disabled: 13313 (42.06 %)
  ssldecrypt Total: 1486; Enabled: 1173 (78.94 %); Disabled: 313 (21.06 %)

KEYWORD: SIGNATURE_SEVERITY Total: 36847; Enabled: 18594 (50.46 %); Disabled: 18253 (49.54 %)
VALUES:
  critical Total: 2777; Enabled: 2013 (72.49 %); Disabled: 764 (27.51 %)
  informational Total: 8000; Enabled: 1611 (20.14 %); Disabled: 6389 (79.86 %)
  major Total: 24131; Enabled: 13641 (56.53 %); Disabled: 10490 (43.47 %)
  minor Total: 1939; Enabled: 1329 (68.54 %); Disabled: 610 (31.46 %)
```



```
[flowmon@flowmon ~]$ rule-manager -s -f '/data/idsp/default_rules/emerging-ftp.rules'
```

Input ruleset file option can be supplied with `-f` to calculate statistics on a given ruleset file. By default statistics are calculated on `suricata.rules` file used by Flowmon IDS probe.

```
[flowmon@localhost ~]$ rule-manager -s -f '/data/idsp/default_rules/emerging-ftp.rules'
All Signatures:
  Total Signatures: 58
  Enabled Signatures: 58 (100.0 %)
  Disabled Signatures: 0 (0.0 %)

KEYWORD: SID Total: 58; Enabled: 58 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: AFFECTED_PRODUCT Total: 7; Enabled: 7 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: ATTACK_TARGET Total: 7; Enabled: 7 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: CREATED_AT Total: 58; Enabled: 58 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: DEPLOYMENT Total: 7; Enabled: 7 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: SIGNATURE_SEVERITY Total: 7; Enabled: 7 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: TAG Total: 6; Enabled: 6 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: UPDATED_AT Total: 58; Enabled: 58 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: CLASSTYPE Total: 58; Enabled: 58 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: CVE Total: 31; Enabled: 31 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: FORMER_CATEGORY Total: 1; Enabled: 1 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: PERFORMANCE_IMPACT Total: 1; Enabled: 1 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: CONFIDENCE Total: 1; Enabled: 1 (100.0 %); Disabled: 0 (0.0 %)
KEYWORD: REVIEWED_AT Total: 1; Enabled: 1 (100.0 %); Disabled: 0 (0.0 %)
```

Rule-trigger statistics

```
[flowmon@flowmon ~]$ rule-manager -r signature_severity Informational 10
```

Rule-trigger stats option allows user to display first N rules ordered by the number of rule triggers among detected events in `eve.json` specified by given metadata *keyword* and *value*.

Visualized data such as GID and SID of a given rule can then be used to generate suppress or threshold command for a given rule in order to reduce the amount of alerts generated for this rule.

```
[flowmon@localhost ~]$ rule-manager -r signature_severity Informational 10
COUNT | SID | GID | SIGNATURE MESSAGE | CATEGORY |
96 "2024364:1:ET SCAN Possible Nmap User-Agent Observed: Web Application Attack"
89 "2019401:1:ET POLICY Vulnerable Java Version 1.8.x Detected: Potentially Bad Traffic"
83 "2024364:1:ET SCAN Possible Nmap User-Agent Observed: Web Application Attack"
68 "2024364:1:ET SCAN Possible Nmap User-Agent Observed: Web Application Attack"
65 "2024364:1:ET SCAN Possible Nmap User-Agent Observed: Web Application Attack"
29 "3115336:1:SN MS-SRVS service - NetShareEnum: "
28 "2019401:1:ET POLICY Vulnerable Java Version 1.8.x Detected: Potentially Bad Traffic"
23 "2019401:1:ET POLICY Vulnerable Java Version 1.8.x Detected: Potentially Bad Traffic"
20 "2019401:1:ET POLICY Vulnerable Java Version 1.8.x Detected: Potentially Bad Traffic"
17 "2019401:1:ET POLICY Vulnerable Java Version 1.8.x Detected: Potentially Bad Traffic"

Threshold a given rule with the following command:
  threshold gen_id <gid>, sig_id <sid>, type <threshold|limit|both>, track <by_src|by_dst|by_rule|by_both>

To apply append this command to threshold.config
For more information see https://docs.suricata.io/en/latest/configuration/global-thresholds.html

Suppress an alert for a given rule with the following command:
  suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst|by_either>, ip <ip|subnet|addressvar>

To apply append this command to threshold.config
For more information see https://blog.inliniac.net/2012/03/07/f-secure-av-updates-and-suricata-ips/
```

```
[flowmon@flowmon ~]$ rule-manager -r signature_severity Informational 10 -f /data/idsp/outputs/eve.json.2.gz
```

Rule trigger stats can also be calculated on archived eve.json logs from Flowmon IDS Probe.

```
[flowmon@localhost ~]$ rule-manager -r signature_severity Informational 10 -f /data/idsp/outputs/eve.json.2.gz
COUNT | SID | GID | SIGNATURE MESSAGE | CATEGORY |
36 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
28 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
16 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
14 "3115336:1:SN MS-SRVS service - NetShareEnum: "
13 "3115336:1:SN MS-SRVS service - NetShareEnum: "
12 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
12 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
10 "3115336:1:SN MS-SRVS service - NetShareEnum: "
8 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"
8 "2027390:1:ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent: Misc activity"

Threshold a given rule with the following command:
threshold gen_id <gid>, sig_id <sid>, type <threshold|limit|both>, track <by_src|by_dst|by_rule|by_both>

To apply append this command to threshold.config
For more information see https://docs.suricata.io/en/latest/configuration/global-thresholds.html

Suppress an alert for a given rule with the following command:
suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst|by_either>, ip <ip|subnet|addressvar>

To apply append this command to threshold.config
For more information see https://blog.inliniac.net/2012/03/07/f-secure-av-updates-and-suricata-ips/
```

Generate suppress or threshold command

```
[flowmon@flowmon ~]$ rule-manager -t 1 2024364 threshold both 10 60
```

Rule-manager can be used to generate threshold command for a given rule. Generated command can then be added to threshold.config.

```
[flowmon@localhost ~]$ rule-manager -t 1 2024364 threshold both 10 60
Generated threshold command:
threshold gen_id 1, sig_id 2024364, type threshold, track both, count 10, seconds 60
```

```
[flowmon@flowmon ~]$ rule-manager -sp 1 2024364 by_src 192.168.10.1/24
```

Rule-manager can be used to generate suppress command for a given rule. Generated command can then be added to threshold.config.

```
[flowmon@localhost ~]$ rule-manager -sp 1 2024364 by_src 192.168.10.1/24
Suppress an alert for a given rule with the following command:
suppress gen_id 1, sig_id 2024364, track by_src, ip 192.168.10.1/24
```

Enable and Disable rules

```
[flowmon@flowmon ~]$ rule-manager -d deployment perimeter
```

Disabling given rule category based on metadata keyword and value.

Metadata keywords identified when running statistical module of rule-manager can be used to disable or re-enable disabled rules according to a specific deployment scenario of Flowmon IDS Probe in order to improve the used ruleset.

```
[flowmon@flowmon ~]$ rule-manager -e deployment perimeter
```

Enabling given rule category based on metadata keyword and value.

```
[flowmon@flowmon ~]$ rule-manager -e group emerging-info.rules
```

Enabling given rule group based on group name. *Group names are equivalent to .rules files used by Flowmon IDS Probe.*

```
[flowmon@localhost ~]$ rule-manager -e deployment perimeter
Rule Category: deployment perimeter was not disabled. No change.
[flowmon@localhost ~]$
[flowmon@localhost ~]$ rule-manager -d deployment perimeter
Disabling rule category deployment perimeter.
To see changes wait until Suricata-Updates runs or apply:
'sudo systemctl restart flowmon-idsp-suricata-update'
[flowmon@localhost ~]$
[flowmon@localhost ~]$ rule-manager -d deployment perimeter
Rule Category: deployment perimeter was already disabled.
[flowmon@localhost ~]$
[flowmon@localhost ~]$ rule-manager -e deployment perimeter
Enabling rule category deployment perimeter.
To see changes wait until Suricata-Updates runs or apply:
'sudo systemctl restart flowmon-idsp-suricata-update'
[flowmon@localhost ~]$
```



```
[flowmon@flowmon ~]$ rule-manager -ldc
```

Listing all disabled rule categories based on group name, metadata attributes or regular expressions.

```
[[flowmon@localhost ~]$ rule-manager -ldc
Listing disabled rule categories:
  Disabled Groups:
    group:app-layer-events.rules
    group:botcc.portgrouped.rules
    group:decoder-events.rules
    group:dhcp-events.rules
    group:dnp3-events.rules
    group:emerging-activex.rules
    group:emerging-deleted.rules
    group:emerging-games.rules
    group:emerging-icmp_info.rules
    group:emerging-icmp.rules
    group:emerging-inappropriate.rules
    group:emerging-info.rules
    group:emerging-scada.rules
    group:emerging-scada_special.rules
    group:emerging-shellcode.rules
    group:emerging-web_specific_apps.rules
    group:files.rules
    group:ipsec-events.rules
    group:kerberos-events.rules
    group:modbus-events.rules
    group:ntp-events.rules
    group:nfs-events.rules
    group:stream-events.rules

  Disabled Metadata:

  Disabled Classtypes:
    re:classtype:not-suspicious
    re:classtype:protocol-command-decode
    re:classtype:misc-activity
    re:classtype:tcp-connection
    re:classtype:icmp-event

  Other disabled rule categories:
    2230010
    2230003
    2230002
    2230009
    2230015
    2221010
```

List ruleset groups

```
[flowmon@flowmon ~]$ rule-manager -g
```

To be able to identify all rule groups which are used on a given Flowmon Appliance by Flowmon IDS Probe rule-manager provides an option to list all used local and remote rule sources along with all rule groups from a given rule source.

```
[[flowmon@localhost ~]$ rule-manager -g

Rule Sources:
-----
- Rule Source: emerging.rules.tar
  * Group: tor.rules
  * Group: emerging-web_client-optional.rules
  * Group: emerging-policy.rules
  * Group: dshield.rules
  * Group: botcc.rules
  * Group: emerging-deleted-optional.rules
  * Group: emerging-inappropriate.rules
  * Group: emerging-hunting-optional.rules
  * Group: emerging-adware_pup-optional.rules
  * Group: emerging-user_agents.rules
  * Group: emerging-malware-optional.rules
  * Group: emerging-malware.rules
  * Group: emerging-activex.rules
  * Group: emerging-smtp-optional.rules
  * Group: emerging-exploit-optional.rules
  * Group: emerging-mobile_malware-optional.rules
  * Group: compromised-optional.rules
  * Group: emerging-info.rules
  * Group: 3coresec.rules
  * Group: emerging-pop3.rules
  * Group: emerging-sql.rules
-----
- Rule Source: Local
  * Group: /data/idsp/user-config/rules/local1.rules
  * Group: /data/idsp/user-config/rules/local2.rules
```

```
[flowmon@flowmon ~]$ rule-manager -l emerging-pop3
```

For rules groups from the default Flowmon copy of of [Emerging Threats Open Rules](#) description of rules in each rule group is also provided.

```
[[flowmon@localhost ~]$ rule-manager -l emerging-pop3

Rule Sources:
-----
- Rule Source: emerging.rules.tar
  * Group: emerging-pop3.rules - Description: This category is for signatures related to attacks that detect nonmalicious POP3 activity for logging purposes.
```

```
[flowmon@flowmon ~]$ rule-manager --set-group-description emerging-pop3 "New description for category."
```

Description for all listed rule groups used on a given Flowmon Appliance can be updated and changed by the user at any time. This is especially handy for setting up custom descriptions for local rules groups added.

```
[flowmon@localhost ~]$ rule-manager --set-group-description emerging-pop3 "New description for category."
- Rule Source: emerging.rules.tar
* Group: emerging-pop3.rules - Description: New description for category.
Description for Group 'emerging-pop3.rules' successfully updated.
```

```
[flowmon@flowmon ~]$ rule-manager -l emerging-pop3
```

```
[flowmon@localhost ~]$ rule-manager -l emerging-pop3

Rule Sources:
-----
- Rule Source: emerging.rules.tar
* Group: emerging-pop3.rules - Description: New description for category.
```

Check ruleset for validity

```
[flowmon@flowmon ~]$ rule-manager -c /data/idsp/user-config/rules/local2.rules
```

Rule-manager provides an option to check syntax of any given rules file, in order to be able to determine if the file is a valid .rules file and can be used by Flowmon IDS Probe.

```
[flowmon@localhost ~]$ rule-manager -c /data/idsp/user-config/rules/local1.rules
Rule Syntax Errors:

Rule file is correct!

Rules summary:

b'2/5/2024 -- 13:42:04 - <Notice> - Configuration provided was successfully loaded. Exiting.'
```

```
[flowmon@flowmon ~]$ rule-manager -c /data/idsp/user-config/rules/local2.rules
-o output.txt
[flowmon@flowmon ~]$ cat output.txt
```

Output of all commands of rule-manager can also be redirected to a file as shown bellow.

```
[flowmon@localhost ~]$ rule-manager -c /data/idsp/user-config/rules/local2.rules -o output.txt
[flowmon@localhost ~]$ cat output.txt
Rule Syntax Errors:

Rule file is correct!

Rules summary:

b'2/5/2024 -- 13:43:41 - <Notice> - Configuration provided was successfully loaded. Exiting.'
```

References

1. (1.4.2024) *Suricata IDS Configuration and Tuning*. Available at:
https://support.kemptechnologies.com/hc/article_attachments/11439506157965.