## Suricata-Update - Optimization #3250

### Check if the options listed common for all commands are still valid

10/16/2019 05:49 AM - Shivani Bhardwaj

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Low</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tharushi Jayasekara</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Beginner, Outreachy, Python</td>
</tr>
</tbody>
</table>

### Description

Bring our any options that are not common to all the commands to their respective commands.

### Related issues:

- Related to Optimization #3248: Make list-enabled-sources command as an option...

### History

**#1 - 12/15/2019 06:53 AM - Shivani Bhardwaj**
- Status changed from New to Assigned

**#2 - 12/15/2019 06:54 AM - Shivani Bhardwaj**
- Related to Optimization #3248: Make list-enabled-sources command as an option for list-sources added

**#3 - 09/28/2020 07:26 AM - Shivani Bhardwaj**
- Assignee changed from Shivani Bhardwaj to Community Ticket
- Label Beginner, Outreachy, Python added

**#4 - 10/07/2020 03:54 PM - Shivani Bhardwaj**
- Status changed from Assigned to New

**#5 - 10/08/2020 11:38 AM - Tharushi Jayasekara**
- Assignee changed from Community Ticket to Tharushi Jayasekara

**#6 - 10/08/2020 11:58 AM - Shivani Bhardwaj**
- Assignee changed from Tharushi Jayasekara to Community Ticket

**#7 - 10/08/2020 08:20 PM - Tharushi Jayasekara**
- Assignee changed from Community Ticket to Tharushi Jayasekara

**#8 - 10/09/2020 02:08 PM - Tharushi Jayasekara**

Shivani Bhardwaj wrote:

> Bring our any options that are not common to all the commands to their respective commands.

Hi Shivani,
Can I know whether this is referring to the global arguments in parsers.py as 'options listed common for all commands'?

**#9 - 10/09/2020 04:54 PM - Shivani Bhardwaj**

Tharushi Jayasekara wrote in #note-8:

Shivani Bhardwaj wrote:

> Bring our any options that are not common to all the commands to their respective commands.
Hi Shivani,
Can I know whether this is referring to the global arguments in parsers.py as 'options listed common for all commands'?

Hi, Tharushi!

Sorry about the missing information in this issue. This is in regards to the "commands" of suricata-update. If you do `suricata-update -h`, in the end you'll see a list of commands under the title "other commands:". Let's take for example the `list-sources` command. If you do `suricata-update list-sources -h`, you'll see a list of arguments that can be used with `list-sources` and if you try any other command, say `update-sources` and do `suricata-update update-sources -h`, you'll again see a similar list. Now some options are indeed common to all the commands (e.g. `-h`, `-v`, `-q`) but others might not be. This task is about finding out which options (if any) are redundant for each of these commands.

You can restrict your work to researching and finding these redundant options for all the commands. If there are any, we can go about making a separate ticket for code changes required to only show the relevant options for any particular command.

You can find what each of the command means and is used for here: https://suricata-update.readthedocs.io/en/latest/ [there is a dedicated section for each of these commands].

Does this help?

#10 - 10/09/2020 05:30 PM - Tharushi Jayasekara

Shivani Bhardwaj wrote in #note-9:

Tharushi Jayasekara wrote in #note-8:

Shivani Bhardwaj wrote:

Bring our any options that are not common to all the commands to their respective commands.

Hi Shivani,
Can I know whether this is referring to the global arguments in parsers.py as 'options listed common for all commands'?

Hi, Tharushi!

Sorry about the missing information in this issue. This is in regards to the "commands" of suricata-update. If you do `suricata-update -h`, in the end you'll see a list of commands under the title "other commands:". Let's take for example the `list-sources` command. If you do `suricata-update list-sources -h`, you'll see a list of arguments that can be used with `list-sources` and if you try any other command, say `update-sources` and do `suricata-update update-sources -h`, you'll again see a similar list. Now some options are indeed common to all the commands (e.g. `-h`, `-v`, `-q`) but others might not be. This task is about finding out which options (if any) are redundant for each of these commands.

You can restrict your work to researching and finding these redundant options for all the commands. If there are any, we can go about making a separate ticket for code changes required to only show the relevant options for any particular command.

You can find what each of the command means and is used for here: https://suricata-update.readthedocs.io/en/latest/ [there is a dedicated section for each of these commands].

Does this help?

Thanks Shivani. That's indeed very helpful!
Would you recommend running each command with every option to check whether the options are valid?
I would also like to know where I could present the findings once the redundant options are found.

#11 - 10/09/2020 05:54 PM - Shivani Bhardwaj

Thanks Shivani. That's indeed very helpful!
Would you recommend running each command with every option to check whether the options are valid?

Not sure if that would be helpful. If the command does not use a certain option, it'll probably simply avoid it. (I'd recommend trying this though :) )
Maybe the command implementation would give you a better idea. I would probably start by looking at what the common options are and finding out where are they used in the code. If an option is obviously useless for a command and is used in an unrelated scenario in the code elsewhere, note that down and; if any option is way too confusing, reach out and ask to clarify.
You do not need to ask or inform for every particular option for every command separately.

I would also like to know where I could present the findings once the redundant options are found.

I think we could keep the conversation here itself to maintain the history and avoid any confusion.
Bring our any options that are not common to all the commands to their respective commands.

You do not need to ask or inform for every particular option for every command separately.

I would also like to know where I could present the findings once the redundant options are found.

I think we could keep the conversation here itself to maintain the history and avoid any confusion.

Hi Shivani,

Thanks to your helpful guidelines, I believe I was able to figure out some redundant options in the commands. My findings are as follows -

The options that are declared common for all commands (declared as global arguments in parsers.py) are: -h, -v, -q, --version, --data-dir, --config, --suricata-conf, --suricata, --suricata-version, --user-agent, --no-check-certificate.

According to my understanding, the 2 options --user-agent and --no-check-certificate seem to be valid only for the command update-sources and are redundant options for all the other commands.

Please correct me if I'm wrong!

@jasonish, do the following options (except suricata-version for check-versions) affect the working of commands in any way?

--suricata-conf <filename>
configuration file (default: /etc/suricata/suricata.yaml)

--suricata <path>
Path to Suricata program

--suricata-version <version>
Override Suricata version

I tried to put garbage for these values with all commands. Did not see anything jump up there. Am I overlooking something?

Hi Shivani,

Thanks to your helpful guidelines, I believe I was able to figure out some redundant options in the commands.

My findings are as follows -

The options that are declared common for all commands (declared as global arguments in parsers.py) are: -h, -v, -q, --version, --data-dir, --config, --suricata-conf, --suricata, --suricata-version, --user-agent, --no-check-certificate.

According to my understanding, the 2 options --user-agent and --no-check-certificate seem to be valid only for the command update-sources and are redundant options for all the other commands.

Please correct me if I'm wrong!

I think that --suricata-conf and --suricata-version are only used for the default command "update".

The --suricata option is used by nearly all commands. As Suricata-Update attempts to run the Suricata binary to find out where the data directory is located. It parses out the "--localstatedir" from the output of "suricata --build-info".
According to my understanding, the 2 options --user-agent and --no-check-certificate seem to be valid only for the command update-sources and are redundant options for all the other commands.

These arguments are also used to the "update" subcommand. The "update" subcommand is what is defaulted to if no subcommand is provided on the command line. For example, the following to commands are identical:

`.bin/suricata-update -D ./data --no-test --no-check-certificate

`.bin/suricata-update update -D ./data --no-test --no-check-certificate

This might make this task a little harder than it seems on the surface.

Tharushi Jayasekara wrote in #note-12:

Shivani Bhardwaj you can go ahead and claim another ticket while we figure if this one can be for contribution period. Please make sure to mention this ticket as a part of your contributions when you submit your final application. Thanks for all your work!

Tharushi Jayasekara you can go ahead and claim another ticket while we figure if this one can be for contribution period. Please make sure to mention this ticket as a part of your contributions when you submit your final application. Thanks for all your work!

Thank you Shivani!

While I was working on it, I also noticed some inconsistencies with the suricata-update docs at https://suricata-update.readthedocs.io/en/latest/. For example, I could not find --no-check-certificate in the documentation as an option under any of the commands mentioned above. Not sure if it's relevant, but keeping you updated on it.