EVE DNS logger defaults to version 2 instead of version when version not specified.

10/10/2019 09:47 PM - Jason Ish

Status: Closed
Priority: Normal
Assignee: Jason Ish
Category: 
Target version: 5.0.0
Affected Versions: 4.1.5, 5.0rc1
Effort: 

Description
To support backward configuration file compatibility, the EVE DNS logger should default to v1 style logging if the version parameter is not supplied.

This is true for 4.1.5 when compiled without Rust. But when compiled with Rust (and including 5.0rc1), it will default to v2 output. This is due to the Rust implementation not initially having v1 output support.

History

#1 - 10/11/2019 02:18 PM - Victor Julien
So this only shows in 4.1.x+rust (experimental) and 5.0rc (experimental)? Asking because if it already is in a supported version / build config, then changing it may have too many side effects.

#2 - 10/11/2019 02:27 PM - Jason Ish
Victor Julien wrote:

So this only shows in 4.1.x+rust (experimental) and 5.0rc (experimental)? Asking because if it already is in a supported version / build config, then changing it may have too many side effects.

Probably a game of numbers then.

Will we have more people who are on an upgrade path of 4.0, 4.1 (with Rust) to 5.0? These are the people that will be affected, if they didn't noticed already and haven't tweaked their config. They will silently drop back to v1. If they skipped 4.1, they won't notice.

Or will there be more people upgrading from 4.1.x w/Rust to 5.0? These people will be less affected. If they did a fresh install, they will have the version set and will never see this issue. Or they did not have the version set and didn't noticed.

It's tricky to balance, but defaulting to v2 should probably be considered a real bug. I'm just surprised it went unnoticed (unreported) for this long.

#3 - 10/11/2019 02:34 PM - Victor Julien
I'm lost now about who would be affected and in which case. Maybe its good to have a little table in here that maps between: old version, config version, new version, dns version in use as a result.

#4 - 10/11/2019 02:47 PM - Jason Ish
Hmm.. Its a bit of a matrix.

4.1.5 configuration users should NOT be affected. The version was explicitly set there, and v1 section removed from the default configuration.

4.0 configuration users who upgraded to 4.1 w/Rust --> affected, forced to v2 logging.
4.0 configuration users who upgraded to 4.1 wo/Rust -> not affected, stayed on v1 logging.

5.0 has the same result as 4.1 w/Rust.

Basically,

```python
if version == 1:
    set_log_version(1)
elif version == 2:
    set_log_version(2)
else (undefined):
```
if rust:
    set_log_version(2)
else:
    set_log_version(1)

#5 - 10/12/2019 02:46 PM - Jason Ish
I think it's worth keeping in mind that the original plan was to deprecate v1 output style when we dropped the non-Rust DNS implementation. But we added v1 logging to the Rust implementation to satisfy Debian packaging requirements.

#6 - 10/13/2019 08:04 AM - Victor Julien
- Tracker changed from Bug to Documentation
- Target version set to 5.0.0

#7 - 10/13/2019 09:14 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/pull/4297