Putting a place holder for discussion following up an IRC discussion with Jason Ish.

It seems DNS v2 logging differs than v1 in the way that if you would like to specify a custom type logging - https://github.com/OISF/suricata/blob/master/suricata.yaml.in#L188 it is done per type of request not the answer. It could also be a bit misleading as a user might expect to be able to log in just a or aaaa answers but that is not the case in v2.

Related issues:
Related to Task #4137: deprecate: eve.dns v1 record support

I don't understand what this ticket is about. Can you add more info? Also, what action is required?

So in v1, if you selected to log types of "cname", and a request for an "a" came in, you would not see the request logged, but if a cname was part of the resolution, you'd see the one "cname" response record. It does lack any context of why its logged though.

In v2, setting the type to cname will only log DNS transactions when the request is for a cname. This was intentional, from the commit log, and I believe it was discussed in Jabber or something, but I didn't relay that discussion into the Github pull request.

With v2 logging we could do similar, its a little more complex. If you just selected "cname", you wouldn't get the request for the "a" that created the "cname" response, and the response would only contain the "cname" portion, and not the full response. OR, it could mean only log records with a "cname" entry, then it would get the full response, but still no discrete request object, which is fine, as the full response does have the query in it.

I think in v1 logging this feature primarily existed to cut back on the number of records. v2 logging cuts back on the number of records logged by design, and changes things enough that this feature is not straight forward to implement without some discussion on how it should be done.

Ideally I think we should have deprecated it in v6, and removal in 7. But I guess that would now be deprecate in 7 and remove in 8?

This issue of the types in the response may not be that important anymore. I don't think anyone else has brought it up. It may have been important in v1 to reduce the number of events logged. But as v2 logs the response as a single event, logging all response values is not that much of an issue
anymore.

#7 - 11/12/2020 02:31 PM - Victor Julien
- Related to Task #4137: deprecate: eve.dns v1 record support added

#8 - 05/06/2022 05:16 PM - Jason Ish
- Status changed from New to Closed

Closing, v1 has been removed. V2 is the current reference.