syslog-protocol

Rainer Gerhards
Adiscon
rgerhards@hq.adiscon.com

2005-11-04

Current Status

- Being worked on since late 2003
- Implements layered architecture
- has been in last call in summer, but AD review by Sam Hartman brought up some important issues
- Issues have been worked on, new ID (-15) published 2005-10
- Some questions remain

Versioning

- Sam Hartman pointed out that there might be an issue with versioning.
- I replied that backward compatibility is described in the appendix - see
  http://www.mail-archive.com/syslog-sec%40www.employees.org/msg00295.html
- I think versioning is sufficiently covered.
- **Question: does the WG agree? If not, what should be added?**

IANA Policy

- Currently
  - Version Numbers require Standards Action
  - SD-ID and PARAM-NAMEs relaxed to “IETF Concensus”
- **Questions**
  - **Do we really require “Standards Action” for the Version?**
  - **Is “IETF Concensus” sufficient for SD-ID and PARAM-NAMEs (I strongly think so)?**

Use of Unicode

- Unicode necessary for international needs
- Supported in all fields that may contain locale-specific data
- Disallowed in header and identifiers
- Shall address visual spoofing issues
- See mailing list:
  http://www.mail-archive.com/syslog%40lists.ietf.org/msg00013.html
- **Question: is this model acceptable?**

SD-IDs

- SD-IDs uniquely identify data elements
- Extensions are now in the format extension@enterpriseid, preventing namespace collisions (but requiring some more space)
- Experimental PARAM-NAMEs can not be added to standard SD-IDs, they need to be added in extension SD-IDs
- **Question: is this model acceptable?**

Will it be implemented?

- Of course, that's up to the implementors, BUT
  - Do we think there are some things in it that makes it hard to implement?
  - If so, which ones and are these things absolutely necessary?
  - Do we address the syslog community needs, including the end-user needs?

Any other Issues?

- Question: Are there any other issues that I have not brought up?
- If so, which?