59th IETF

syslog WG

Chair: Chris Lonvick <clonvick@cisco.com>

mailing list: syslog-sec@employees.org

Agenda

I.	Review of Scope and Charter (Chris)	10 min.
II.	Update of "syslog Protocol" ID (Rainer or proxy)	30 min.
III.	Introduction of "syslog Transport" ID (Anton or proxy)	15 min.
IV.	Update of "syslog-sign" ID (Jon or proxy)	15 min.
V.	Update of "syslog-device-mib" ID (Glenn)	30 min.
VI.	Wrap-up and review of decisions made (Chris)	10 min.

Discussion Items for This Meeting

syslog-protocol

- Are we on the Right Track by splitting “syslog-protocol” out from syslog-sign?
- Should the description of a “relay” be separated from the “syslog-protocol document?
- Should a separate “syslog-transport-udp” document be created?
- Specific Issues raised in Rainer's slides.

syslog-transport-udp

- No specific items for discussion at this time.

Discussion Items for This Meeting

syslog-sign

- (again) Are we on the Right Track by splitting “syslog-protocol” out from syslog-sign?
- Should syslog-sign apply to “classical” syslog, or be written specifically to work with syslog-protocol?

syslog-device-mib

- Specific items from Glenn's slides.

Syslog WG Charter (1/3)

- Syslog is a de-facto standard for logging system events. However, the protocol component of this event logging system has not been formally documented. While the protocol has been very useful and scaleable, it has some known but undocumented security problems. For instance, the messages are unauthenticated and there is no mechanism to provide verified delivery and message integrity.

Syslog WG Charter (2/3)

- The goal of this working group is to document and address the security and integrity problems of the existing Syslog mechanism. In order to accomplish this task we will document the existing protocol. The working group will also explore and develop a standard to address the security problems.

Syslog WG Charter (3/3)

- Beyond documenting the Syslog protocol and its problems, the working group will work on ways to secure the Syslog protocol. At a minimum this group will address providing authenticity, integrity and confidentiality of Syslog messages as they traverse the network. The belief being that we can provide mechanisms that can be utilized in existing programs with few modifications to the protocol while providing significant security enhancements.

WG Status

- “The BSD syslog Protocol” - RFC 3164 produced August 2001.
- “Reliable Delivery for syslog” - RFC 3195 produced November 2001.
- draft-ietf-syslog-protocol-03.txt - wip
- draft-ietf-syslog-transport-udp-00.txt – nearly wip
- draft-ietf-syslog-sign-13.txt - wip
- draft-ietf-syslog-device-mib-05.txt - wip
- draft-ietf-syslog-international-00.txt - wip

Recent Progress 1/2

- syslog-sign was developing the syslog protocol for its own use – better timestamp, definition of "cookies", length, etc.
- Rainer Gerhards volunteered to pull the "protocol" out of syslog-sign and establish the definitions in its own ID.
- Anton Okmianski has volunteered to pull out the udp transport mapping into a separate ID.
- These will be submitted together to the IESG for consideration as RFCs when they are ready.

Recent Progress 2/2

- Once syslog-protocol and syslog-transport are submitted,
  - Jon Callas can incorporate these features into syslog-sign
  - syslog-international can progress
  - RFC 3195 may be revised as necessary

syslog-sign

- Slightly “on hold” while we make sure syslog-protocol is the right direction.
  - The parts of the protocol and transport will need to be removed from the syslog-sign ID.
  - IANA Considerations look appropriate but some parts will need to be removed since they belong in syslog-protocol.
  - Security Considerations will need to be moved to syslog-protocol and syslog-transport.
  - “cookies” will need to be reworked in the format of the “tags” defined in syslog-protocol.

syslog-sign

- Currently the document is “transport agnostic”. Should it be kept that way?
  - By keeping it loose, it may be used in “classical” syslog, which may get more people to implement it sooner. The alternative is to restrict it to syslog-protocol and Reliable Delivery of Syslog (3195) which may delay its acceptance.

Other Reference

- loganalysis@lists.shmoo.com
- discussion of formatting the contents of the messages (which is outside the scope of this WG)
- Great discussion of the interpretation of event messages.