Mapping SNMP Notifications to SYSLOG

Jürgen Schönwälder

Jacobs University Bremen

71st IETF Meeting in Philadelphia
Motivation and Goals

Motivation

- Some operators prefer SNMP notifications, some operators prefer SYSLOG messages
- Some devices generate SNMP notifications, some devices generate SYSLOG messages
- Latest SYSLOG can carry structured data elements

Goals

- Mapping SNMP notifications to SYSLOG messages
  - without losing machine readable information
  - focusing on the structured data elements
  - leaving the free text message to implementations
- Based on RFC3416 notification format, RFC1157 traps can be dealt with by applying RFC3584
Example: SNMP Notification (linkUp)

BER Encoding

30:7C
04:08:80:00:02:B8:04:61:62:63
04:04:63:74:78:31
A7:6A
02:03:6D:08:67
02:01:00
02:01:00
30:5D
30:0F
06:08:2B:06:01:02:01:01:03:00
43:03:01:72:8C
30:17
06:0A:2B:06:01:06:03:01:01:04:01:00
06:09:2B:06:01:06:03:01:01:05:04
30:0F
06:0A:2B:06:01:02:01:02:02:01:01:03
02:01:03
30:0F
06:0A:2B:06:01:02:01:02:02:01:01:07:03
02:01:01
30:0F
06:0A:2B:06:01:02:01:02:02:01:08:03
02:01:01

ASN.1 Interpretation

SEQUENCE {
  800002b804616263
  "ctx1"
  SNMPv2-Trap-PDU {
    INTEGER 7145575
    INTEGER 0
    INTEGER 0
    SEQUENCE OF {
      SEQUENCE {
        sysUpTime.0
        94860
      }
      SEQUENCE {
        snmpTrapOID.0
        linkUp
      }
      SEQUENCE {
        ifIndex.3
        3
      }
      SEQUENCE {
        ifAdminStatus.3
        up(1)
      }
      SEQUENCE {
        ifOperStatus.3
        up(1)
      }
    }
  }
}
Example: SYSLOG Message (linkUp)

Example message:

```
<29>1 2003-10-11T22:14:15.003Z mymachine.example.com
  snmptrapd - ID47
  [snmp ctxEngine="800002b804616263"
    ctxName="ctx1"
    sysUpTime="94860"
    snmpTrapOID="1.3.6.1.6.3.1.1.5.4"
    o="1.3.6.1.2.1.2.2.1.1.3" d="3"
    o="1.3.6.1.2.1.2.2.1.7.3" d="1"
    o="1.3.6.1.2.1.2.2.1.8.3" d="1"]
  linkUp on interface #3
```

- All SNMP data is kept in the `snmp` SD element.
- Most varbinds are represented by two SD params; one SD param for the OID and one SD param for the value.
- The two special varbinds `sysUpTime.0` and `snmpTrapOID.0` are dealt with using special rules.
Open Issues

1. Is it a good idea to special case the first two RFC3416 notification varbinds?
2. Should MIB aware implementations be allowed to include an optional label (descriptor)?
   \[o="1.3.6.1.2.1.2.2.1.1.3" \ l="ifIndex.3" \ d="3"\]
3. Descriptors are not guaranteed to be unique; what about module names? This might be getting too big.
4. Should the facility and priority be fixed or implementation or configuration specific?
5. Do we fake a HOSTNAME or is the SNMP context a workable solution?
6. Security considerations?
Standardization?

**SNMP ⇒ SYSLOG**

- Is there interest in a standard mapping of SNMP notifications to structured data elements carried in SYSLOG messages?
- If yes, where should this work be entertained?
  - OPSAWG?

**SYSLOG ⇒ SNMP**

- Is there also interest in a standard mapping of (structured data elements carried in) SYSLOG messages to SNMP notifications?
- If yes, where should this work be entertained?
  - OPSAWG?
References

R. Presuhn.

J. Case, M. Fedor, M. Schoffstall, and J. Davin.
RFC 1157, SNMP Research, PSI, MIT, May 1990.


R. Gerhards.
The syslog Protocol.