YANG Data Model for Monitoring I2NSF Network Security Functions
(draft-hong-i2nsf-nsf-monitoring-data-model-03)

IETF 101, London
March 21, 2018

Dongjin Hong, Jaehoon (Paul) Jeong, Jinyong (Tim) Kim,
Susan Hares, Liang Xia, and Henk Birkholz [Presenter]
Updates from the Previous Versions

• The Previous Drafts:
  – draft-hong-i2nsf-nsf-monitoring-data-model-02

• Changes from the previous versions
  – The YANG data model is refactored by parts of the comments from Henk Birkholz.
    • The structures with identities for reuse are reflected.
    • The notification feature is included.
  – Typos and grammatical errors are corrected.
Monitoring Information Model

- draft-zhang-i2nsf-info-model-monitoring-05
Updated YANG Data Model

• OLD

- Monitoring Information (Container)
  - message_id
  - message_version
  - message_type
  - time_stamp
  - Severity
  - message
    - Event
    - Log
    - Counter
    - Alarm (Alert)

• NEW

- Monitoring Information
  - container
  - Counter
    - Alarm
    - Event
    - Log
  - notification
Comment from Info-Model Author

- OLD

```yaml
container access-mode
  description
  "User access mode. e.g., PPP, SVN, LOCAL";
leaf ppp{
  type boolean;
  description
  "Access-mode : ppp";
}
leaf svn{
  type boolean;
  description
  "Access-mode : svn";
}
leaf local{
  type boolean;
  description
  "Access-mode : local";
}
```

- NEW

```yaml
identity access-mode {
  description
  "TBD";
}
identity ppp {
  base access-mode;
  description
  "Access-mode : ppp";
}
identity svn {
  base access-mode;
  description
  "Access-mode : svn";
}
identity local {
  base access-mode;
  description
  "Access-mode : local";
}
```

```yaml
container access-violation{
  description
  "If the system event is access violation;
  uses i2nss-system-event-type-content;"
}
container config-change{
  description
  "If the system event is
  config change violation";
  uses i2nss-system-event-type-content;
}
```

```yaml
notification system-detection-access-violation{
  description
  "This notification is sent, when a security-sensitive
  authentication action fails.";
  uses i2nss-system-event-type-content;
  uses common-notification-content;
}
```
Support of Identity

• For reuse, identity is used instead of grouping.
Next Steps

• **Complete Refactoring**
  – We will improve the YANG Data Model with both comments and discussion.

• **Verification of the YANG Data Model in the next Hackathon**

• **Configuration and manipulation for monitoring**
  – Using NSF-Facing Interface

• **WG Adoption Call after IETF 101**