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]

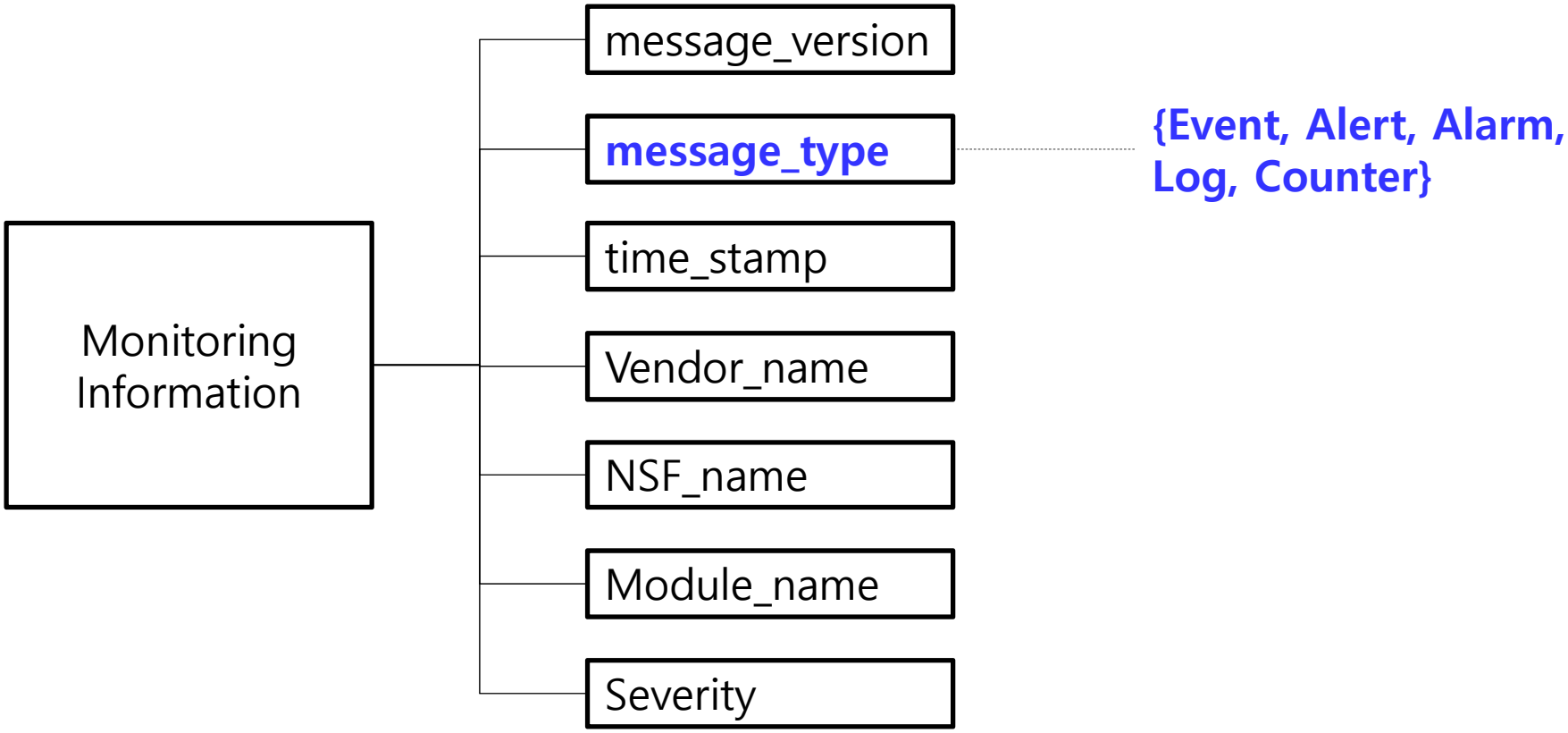
Updates from the Previous Versions

- The Previous Drafts:
  - draft-hong-i2nsf-nsf-monitoring-data-model-01
  - 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.

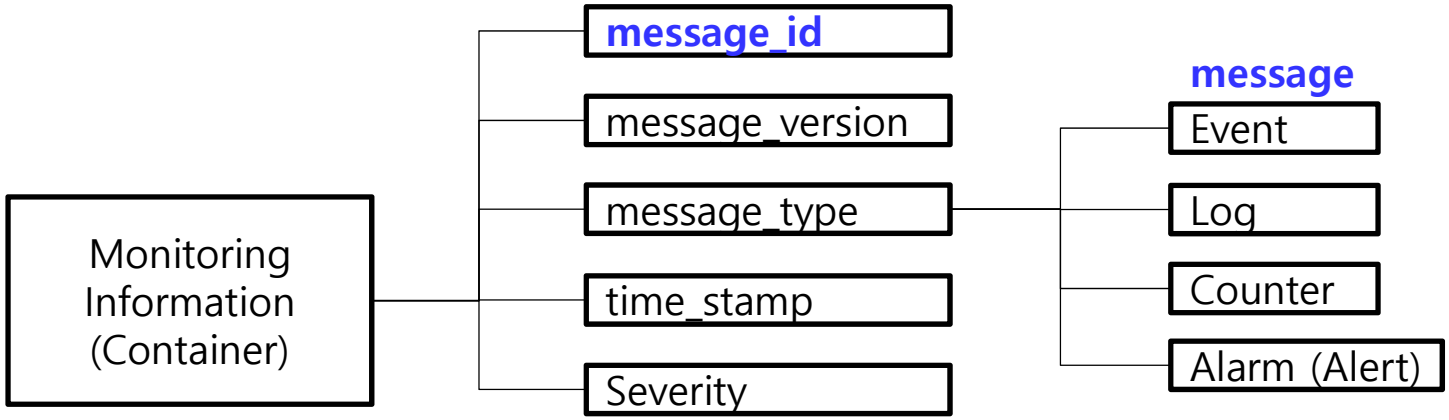
Monitoring Information Model

- draft-zhang-i2nsf-info-model-monitoring-05

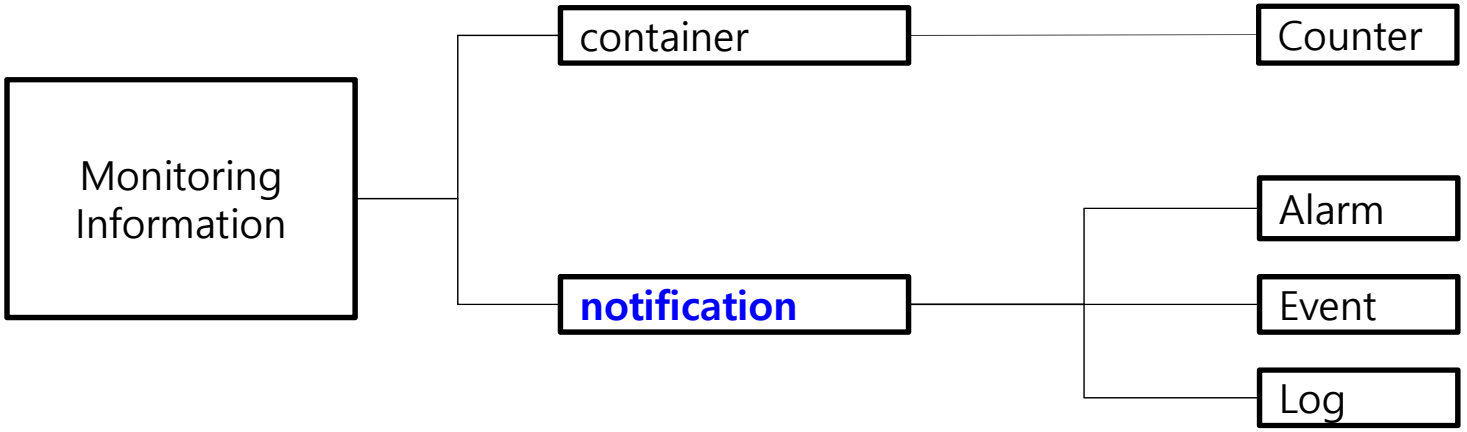


Updated YANG Data Model

- OLD



- NEW



Comment from Info-Model Author

- OLD

```
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

```
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";
}
```

```
container access-violation {
    description
      "If the system event is
      access violation";
    uses i2nsf-system-event-type-content;
  }
  container config-change {
    description
      "If the system event is
      config change violation";
    uses i2nsf-system-event-type-content;
  }
}
```

```
notification system-detection-access-violation {
  description
    "This notification is sent, when a security-sensitive
     authentication action fails.";
  uses i2nsf-system-event-type-content;
  uses common-notification-content;
}
```

Support of Identity

- For reuse, identity is used instead of grouping.

```
identity protocol-type {
    description
        "An identity used to enable type choices in leafs
        and leaflists wrt protocol metadata.";
}
identity ip {
    base protocol-type;
    description
        "General IP protocol type.";
}
identity ipv4 {
    base ip;
    description
        "IPv4 protocol type.";
}
identity ipv6 {
    base ip;
    description
        "IPv6 protocol type.";
}
identity tcp {
    base ipv4;
    base ipv6;
    description
        "TCP protocol type.";
}
identity udp {
    base ipv4;
    base ipv6;
    description
    "UDP protocol type.";
}
identity icmp {
    base ipv4;
    base ipv6;
    description
        "General ICMP protocol type.";
}
```


```
grouping protocol {
    description
        "A set of protocols";
    container protocol {
        description
        "Protocol types:
         TCP, UDP, ICMP, ICMPv6, IP, HTTP, FTP and etc.";
        leaf tcp {
            type boolean;
            description
                "TCP protocol type.";
        }
        leaf udp {
            type boolean;
            description
                "UDP protocol type.";
        }
        leaf icmp {
            type boolean;
            description
                "ICMP protocol type.";
        }
        leaf icmpv6 {
            type boolean;
            description
                "ICMPv6 protocol type.";
        }
        leaf ip {
            type boolean;
            description
                "IP protocol type.";
        }
        leaf http {
            type boolean;
            description
                "HTTP protocol type.";
        }
        leaf ftp {
            type boolean;
            description
                "ftp protocol type.";
        }
    }
}
```

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**