

Semantic Metadata **Annotation** for Network **Anomaly** Detection

draft-netana-nmop-network-anomaly-semantics-03

Helps to annotate operational data, refine outlier detection, supports supervised and semi-supervised machine learning development, enables data exchange among network operators, vendors and academia, and make anomalies for humans apprehensible

thomas.graf@swisscom.com
wanting.du@swisscom.com
alex.huang-feng@insa-lyon.fr
vincenzo.riccobene@huawei-partners.com
antonio.roberto@huawei.com

06. September 2024

Semantic Metadata Annotation for Network Anomaly Detection

draft-netana-nmop-network-anomaly-semantics

Goal: Enable the exchange of labelled dataset for network anomaly detection between operators, vendors and academia

```
module: ietf-symptom-semantic-metadata
```

```
  +--rw symptom* [event-id]
```

```
    +--rw id?                yang:uuid
    +--rw event-id           yang:uuid
    +--rw description?       string
    +--rw start-time?        yang:date-and-time
    +--rw end-time?          yang:date-and-time
    +--rw confidence-score?  score
    +--rw concern-score?    score
```

```
    +--rw tags* [key]
      | +--rw key      string
      | +--rw value?   string
```

```
    +--rw (pattern)?
      | +--:(drop)
      | | +--rw drop?          empty
      | +--:(spike)
      | | +--rw spike?         empty
      | +--:(mean-shift)
      | | +--rw mean-shift?    empty
      | +--:(seasonality-shift)
      | | +--rw seasonality-shift? empty
      | +--:(trend)
      | | +--rw trend?         empty
      | +--:(other)
      | | +--rw other?         string
```

```
    +--rw annotator* [name]
      +--rw (annotator-type)?
        | +--:(human)
        | | +--rw human?      empty
        | +--:(algorithm)
        | | +--rw algorithm?  empty
        +--rw name            string
```

- **Symptom ID and description** uniquely identifies the detected symptom with its start and end time, how confident the system identified the anomaly and how concerned an operator should be.
- **Tags** describe the semantic metadata of the symptom).
- **Pattern** describes the identified pattern of the anomaly.
- **Annotator Name, Type**, describes wherever the anomaly was detected by a human or algorithm and uniquely identifies the entity who/which detected.

Semantic Metadata Annotation

Status, Summary and Next steps

Status

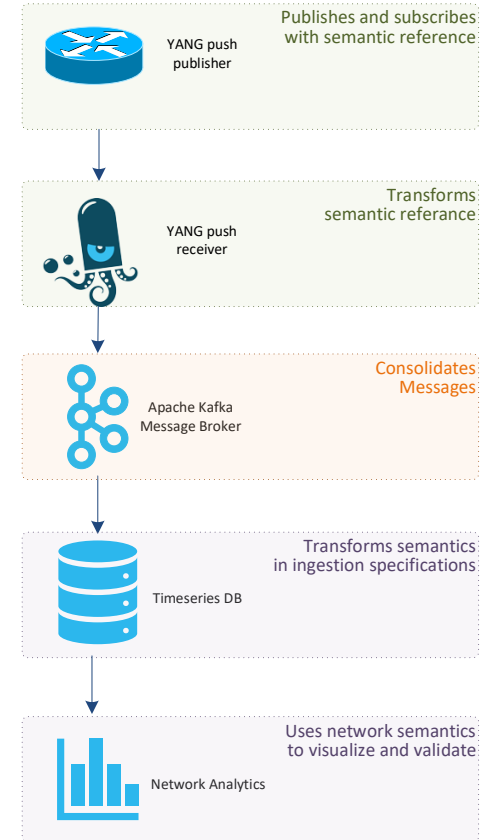
- Addressed comment from Reshad Rahman.

Summary

- Symptom and annotator is now a list instead of a container.
- ietf-interfaces-with-symptoms example only augments "/if:interfaces/if:interface" to be NMDA compliant.
- **Do you realize the benefit of having standardized semantic metadata annotation for Network Anomaly Detection and how it helps network operators, vendor and academia to collaborate?**
- **-> What are your thoughts and comments?**

Next Steps

- **-> We request NMOP working group adoption.**
- **-> Work on example implementation in IETF 121 hackathon.**



thomas.graf@swisscom.com
wanting.du@swisscom.com
alex.huang-feng@insa-lyon.fr
vincenzo.riccobene@huawei-partners.com
antonio.roberto@huawei.com

06. September 2024