Self Describing Data Object Tags

draft-ietf-netmod-node-tags-06

Qin WU (Huawei)

Benoit Claise(Huawei)

Peng Liu (CMCC)

Zongpeng Du (CMCC)

Mohamed Boucadair (Orange)

Recap

- Self describing Data Object Tags classify data objects from different YANG modules and identify characteristics data
  - Model Tag at the module level defined inRFC8819 while object tags provide node level tags
- Self describing data object tags can be used in the streaming telemetry to reduce the amount of data exported to the destination.
- This draft has passed through YANG Doctor Last Call Review and also received review from Adrian Farrell.
  - Many thanks to Adrian and Mahesh.

Change 04 - 06

- Add user tag formatting clarification;
- Provide guidance to the Designated Expert for evaluation of YANG Data Object Tag registry and YANG Data Object Tag prefix registry.
- Update the figure 1 and figure 2 with additional tags.
- Security section enhancement for user tag management.
- Change data object name into name in the module.
- Use the folding defined in [RFC8792].
- Other Editorial changes to address Adrian's comments and comments during YANG doctor review.

Update figure 1 with additional tags

draft-ietf-netmod-node-tags-04

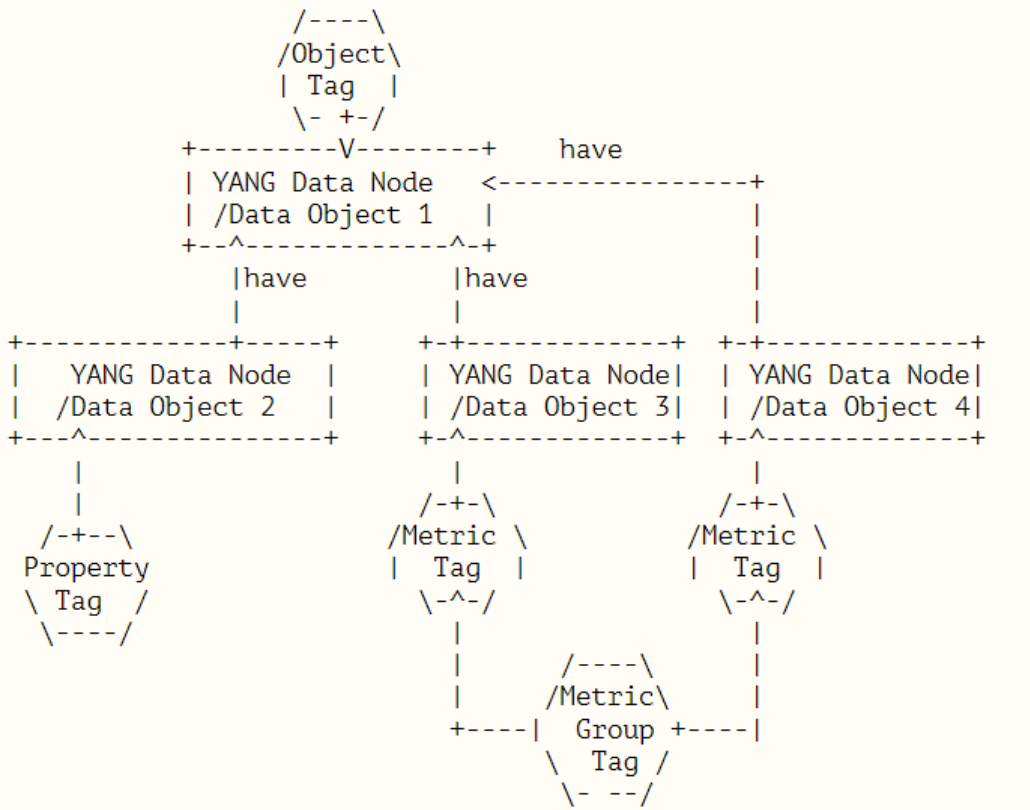


Figure 1: The Relation between Object, Property and Metric

draft-ietf-netmod-node-tags-06

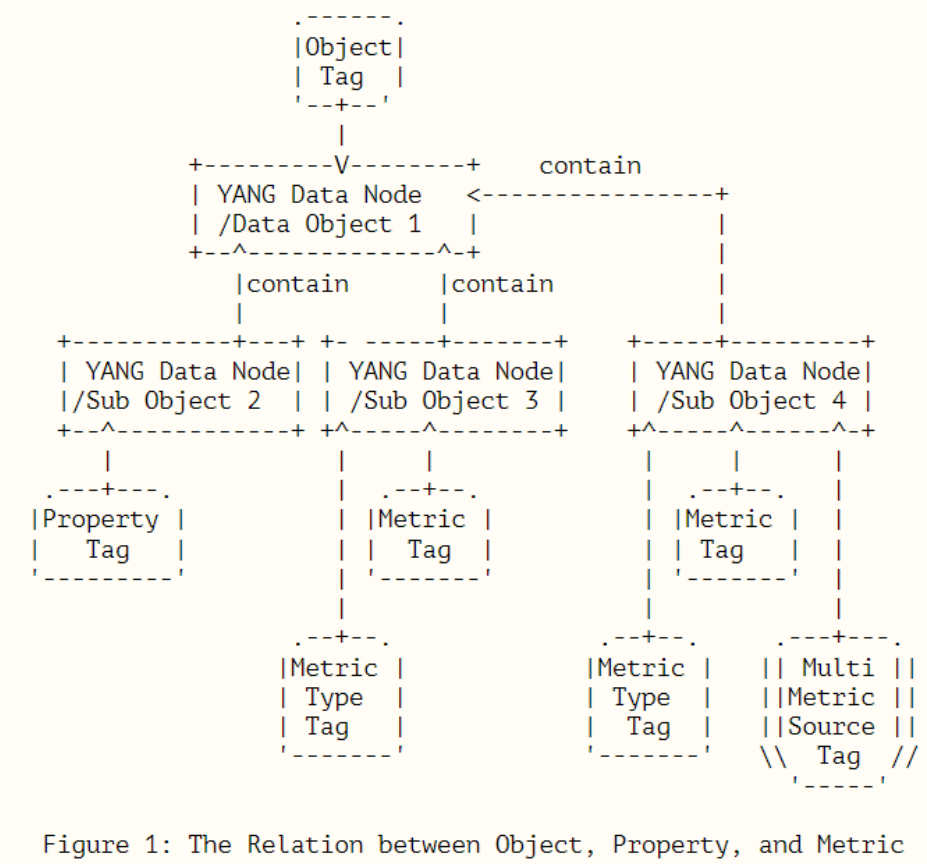


Figure 1: The Relation between Object, Property, and Metric

Add Metric type tag, Multi-source tag

"Specification Required" assignment policy

9.1. YANG Data Object Tag Prefixes Registry

This document requests IANA to create a new registry entitled "YANG Data Object Tag Prefixes" grouped under a new "Protocol" category named "YANG Data Object Tag Prefixes".

This registry allocates tag prefixes. All YANG Data Object Tags should begin with one of the prefixes in this registry.

Prefix entries in this registry should be short strings consisting of lowercase ASCII alpha-numeric characters and a final ":" character.

The allocation policy for this registry is Specification Required [RFC8126]. The Reference and Assignee values should be sufficient to identify and contact the organization that has been allocated the prefix.

9.2. IETF YANG Data Object Tags Registry

This document requests IANA to create three new registries "IETF OPM Tags","IETF Metric Type Tags","IETF Multiple Source Tags" grouped under a new "Protocol" category. These 3 registries should be included below "YANG Data Object Tag Prefixes" when listed on the same page.

Three registries are used to allocate tags that have the registered prefix "ietf:". New values should be well considered and not achievable through a combination of already existing IETF tags.

The allocation policy for these three registries is IETF Review [RFC8126].

9.1. YANG Data Object Tag Prefixes Registry

This document requests IANA to create "YANG Data Object Tag Prefixes" subregistry in "YANG Data Object Tag" registry.

This registry allocates tag prefixes. All YANG Data Object Tags should begin with one of the prefixes in this registry.

Prefix entries in this registry should be short strings consisting of lowercase ASCII alpha-numeric characters and a final ":" character.

The allocation policy for this registry is Specification Required [RFC8126]. The Reference and Assignee values should be sufficient to identify and contact the organization that has been allocated the prefix. There is no specific guidance for the Designated Expert and there is a presumption that a code point should be granted unless there is a compelling reason to the contrary.

9.2. IETF YANG Data Object Tags Registry

This document requests IANA to create "IETF OPM Tags","IETF Metric Type Tags","IETF Multiple Source Tags" three subregistries in "YANG Data Object Tag" registry. These 3 subregistries appear below "YANG Data Object Tag Prefixes" registry.

Three subregistries allocate tags that have the registered prefix "ietf:". New values should be well considered and not achievable through a combination of already existing IETF tags.

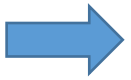
The allocation policy for these three subregistries is IETF Review [RFC8126]. The Designated Expert is expected to verify that IANA assigned tags conform to Net-Unicode as defined in [RFC5198], and shall not need normalization.

User Tags Format Clarification

If a user tag is defined as any tag that has the prefix "user:" how can you then know that users are not required to use the "user:" prefix? That would mean that a user tag is any tag that does or does not have the prefix "user:"

4.3. User Tags Prefix

A user tag is any tag that has the prefix "user:".



4.3. User Tags

A user tag is any tag that has the prefix "user:". For the avoidance of confusion, the colon (":") when it appears for the first time, is always assumed to be the separator between a prefix and the rest of the tag. And so, when a user tag does not have a prefix, it MUST NOT contain a colon.

4. Data Object Tag Values

All data object tags SHOULD begin with a prefix indicating who owns their definition. An IANA registry (Section 9.1) is used to register data object tag prefixes. Initially, three prefixes are defined.

No further structure is imposed by this document on the value following the registered prefix, and the value can contain any YANG type 'string' characters except carriage returns, newlines, tabs, and spaces.

Except for the conflict-avoiding prefix, this document is purposefully not specifying any structure on (i.e., restricting) the tag values. The intent is to avoid arbitrarily restricting the values that designers, implementers, and users can use. As a result of this choice, designers, implementers, and users are free to add or not add any structure they may require to their own tag values.

Tag management conflict resolving

Issue: Are there any risks associated with an attacker adding or removing tags so that a requester gets the wrong data?

10. Security Considerations

The YANG module specified in this document defines schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446].

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

This document adds the ability to associate data object tag meta-data with data object within the YANG modules. This document does not define any actions based on these associations, and none are yet defined, and therefore it does not by itself introduce any new security considerations.

Users of the data object tag meta-data may define various actions to be taken based on the data object tag meta-data. These actions and their definitions are outside the scope of this document. Users will need to consider the security implications of any actions they choose to define.

10. Security Considerations

The YANG module specified in this document defines schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446].

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content, e.g., the presence of tags may reveal information about the way in which data objects are used and therefore providing access to private information or revealing an attack vector should be restricted. Note that appropriate privilege and security levels need to be applied to the addition and removal of user tags to ensure that a user receives the correct data.

This document adds the ability to associate data object tag meta-data with data object within the YANG modules. This document does not define any actions based on these associations, and none are yet defined, and therefore it does not by itself introduce any new security considerations.

Users of the data object tag meta-data may define various actions to be taken based on the data object tag meta-data. These actions and their definitions are outside the scope of this document. Users will need to consider the security implications of any actions they choose to define, including the potential for a tag to get 'masked' by another user.

Next Step

- All open issues have been addressed.
- WGLC?