IETF NETMOD Virtual Interim

YANG Metadata Annotation for Immutable Flag

draft-ma-netmod-immutable-flag-09

February 6, 2024
Where is this “immutable” concept from?

Derived from the discussion of “system-config” draft

• Related, because a lot of system config is immutable

• But independent, hence why factored out
Motivation

• Understanding that servers do this already
  • Proprietary documentation
  • Errors already returned when violations occur

• Desire to formally flag which nodes a server considers immutable
  • So clients can know beforehand when violations may occur

• This work merely provides more visibility for the clients to know which configuration is immutable.
The Current Solution

Define a YANG metadata annotation called “immutable” and an ability to retrieve it with a query parameter “with-immutable”

• The “immutable” metadata annotation (RFC 7952)
  • A boolean type
    • Either a node is immutable or not
    • Hierarchically applies to descendants, until overridden
      • Reduces response size

• The “with-immutable” query parameter
  • New metadata not returned unless explicitly requested
  • Avoid breaking legacy clients
Example

```xml
<rpc message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
              xmlns:im="urn:ietf:params:xml:ns:yang:ietf-immutable">
        <datastore ds:operation="operational"></datastore>
        <subtree-filter>
            <applications xmlns="http://example.com/schema/1.2/config"/>
        </subtree-filter>
        <with-origin/>
        <im:with-immutable/>
    </get-data>
</rpc>

<rpc-reply message-id="101"
            xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-nmda">
        <applications xmlns="http://example.com/schema/1.2/config"
                       xmlns:or="urn:ietf:params:xml:ns:yang:ietf-origin"
                       xmlns:im="urn:ietf:params:xml:ns:yang:ietf-immutable">
            <application or:origin="system" im:immutable="true">
                <name>ssh</name>
                <protocol>tcp</protocol>
                <port>22</port>
            </application>
            <application or:origin="intended" im:immutable="false">
                <name>my-ssh</name>
                <protocol>tcp</protocol>
                <port>10022</port>
            </application>
        </applications>
    </data>
</rpc-reply>
```
Why not NACM

NACM refers to Network Configuration Access Control Model (RFC 8341)

- can be disabled by setting the “enable-nacm” leaf to “false”
- can be bypassed by emergency recovery session
- can be overridden by adding new rules before existing rules are matched
  - While NACM rules declaring the immutability should also be immutable themselves
Why not node-tags

Node-tags refer to the solution defined in I-D. ietf-netmod-node-tags

• Not preferred as immutable tag is returned by reading a separate “node-tags” module

• Tags can be removed from the operational state by adding a masked-tag entry
  • While immutability cannot be controlled by the client
Why not YANG deviation statement

The “deviation” statement defines the way a server deviates from a standard.

• Not preferred for immutability which is not an implementation limitation caused by server software/hardware ability

• Cannot deviate mutability property of the system-provided node
Is this draft ready for adoption?