NETCONF Access Control

draft-bierman-netconf-rfc6536bis-00

NETCONF WG
IETF #97 Seoul

Andy Bierman <andy@yumaworks.com>
Martin Björklund <mbj@tail-f.com>

v0.3

Agenda

- Problem Overview

- Solution Overview

- Next Steps

Problem Overview

- NACM does not support YANG 1.1

  – Actions and nested notifications are new

- NACM does not support RESTCONF

  – RESTCONF methods need to be mapped

- NETCONF WG Charter:

  – 5. Update RFC 6536 (NETCONF Access Control Model) to introduce access control rights associated with actions.

Solution Overview: YANG 1.1

- YANG Actions
  - must have read permission to all ancestor nodes of the action-stmt
  - must have execute permission for the action node
- Nested Notifications
  - must have read permission to all ancestor nodes of the notification-stmt
  - must have read permission for the notification node

Solution Overview: RESTCONF

- RESTCONF Methods (section 3.2.2)
  - Maps RESTCONF [method, resource class] to NETCONF [RPC, edit-operation]

```
+----------+-------------------+----------------------+------------------+
| method   | resource class    | NETCONF operation    | Edit operation   |
+----------+-------------------+----------------------+------------------+
| OPTIONS  | all               | none                 | N/A              |
| HEAD     | all               | <get>                | N/A              |
| GET      | all               | <get>                | N/A              |
| POST     | datastore, data   | <edit-config>        | create           |
| POST     | operation         | specified operation  | N/A              |
| PUT      | data              | <edit-config>        | create, replace  |
| PUT      | datastore         | <copy-config>        | replace          |
| PATCH    | data, datastore   | <edit-config>        | merge            |
| DELETE   | data              | <edit-config>        | delete           |
+----------+-------------------+----------------------+------------------+
```

Solution Overview: YANG Module

- Update the node-instance-identifier to support actions and notifications
  - Use data rules to select instances of a specific action or notification
    - Can select /foo/bar/reset or /foo/baz/reset, not all actions named 'reset'
    - Can select all instances /foo/bar/reset or just a subset of instances /foo/bar[name='system']/reset

Next Steps

- Determine if scope of work is correct

- Determine if the the solution proposal is correct

- Update the draft

- Start a WG Last Call review cycle