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]

<table>
<thead>
<tr>
<th>method</th>
<th>resource class</th>
<th>NETCONF operation</th>
<th>Edit operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONS</td>
<td>all</td>
<td>none</td>
<td>N/A</td>
</tr>
<tr>
<td>HEAD</td>
<td>all</td>
<td>&lt;get&gt;</td>
<td>N/A</td>
</tr>
<tr>
<td>GET</td>
<td>all</td>
<td>&lt;get&gt;</td>
<td>N/A</td>
</tr>
<tr>
<td>POST</td>
<td>datastore, data</td>
<td>&lt;edit-config&gt;</td>
<td>create</td>
</tr>
<tr>
<td>POST</td>
<td>operation</td>
<td>specified operation</td>
<td>N/A</td>
</tr>
<tr>
<td>PUT</td>
<td>data</td>
<td>&lt;edit-config&gt;</td>
<td>create, replace</td>
</tr>
<tr>
<td>PUT</td>
<td>datastore</td>
<td>&lt;copy-config&gt;</td>
<td>replace</td>
</tr>
<tr>
<td>PATCH</td>
<td>data, datastore</td>
<td>&lt;edit-config&gt;</td>
<td>merge</td>
</tr>
<tr>
<td>DELETE</td>
<td>data</td>
<td>&lt;edit-config&gt;</td>
<td>delete</td>
</tr>
</tbody>
</table>
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 solution proposal is correct
- Update the draft
- Start a WG Last Call review cycle