An Autonomic Control Plane

draft-ietf-anima-autonomic-control-plane-03.txt

96th IETF, 18 July 2016
Michael Behringer (editor), Toerless Eckert, Steinthor Bjarnason
## Using the Adjacency Table

<table>
<thead>
<tr>
<th>Node-ID</th>
<th>i/f</th>
<th>Link address</th>
<th>ACP address</th>
<th>Domain</th>
<th>Certificate</th>
<th>Validity</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;UDI-1&gt;</td>
<td>Eth0</td>
<td>FE80:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>Full (In domain)</td>
</tr>
<tr>
<td>&lt;UDI-2&gt;</td>
<td>Eth1</td>
<td>FE80:...</td>
<td>-</td>
<td>Example1.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>No</td>
</tr>
<tr>
<td>&lt;UDI-3&gt;</td>
<td>-</td>
<td>2000:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>Valid</td>
<td>Full (in domain)</td>
</tr>
<tr>
<td>&lt;UDI-4&gt;</td>
<td>Eth2</td>
<td>FE80:...</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- **Node has no domain**
  - And I have domain
    - Be a proxy to bootstrap that node

- **Node has domain**
  - And I don’t have domain
    - I bootstrap
      - If response = “redirect”
        - Enter the redirect target into adjacency table; use this node to bootstrap.

- **Intent driven behaviour (tbd)**

### Outside scope for now.

- If response = "redirect"
  - Enter the redirect target into adjacency table; use this node to bootstrap.

- **ACP based functions, e.g., Intent distribution, negotiation, Synchronisation, etc.**
Changes from -02: Insecure Adjacency Discovery: mDNS

- Text in ACP draft
  - Normative, cannot be in reference model
- Reasons for mDNS:
  - Bootstrap should also work outside ANIMA
  - Should introduce few new elements
  - mDNS assumed well known and likely pre-existing, even in IoT devices
  - Using GRASP insecure and secure seen as a security risk
- in GRASP section, removed “insecure GRASP”

Needs Discussion
Changes from -02:
Certificate Requirements (5.1.1)

• Goal: As simple as possible
• Do not use the common fields (ou, etc)
  • They may be used by the operator
  • Avoid potential conflicts; allow for maximum parallelism
• But: Use a standard field (!)
  • Otherwise, in practice integration problems on CA / RA side.
• Should include ACP address (in zone 0)
• Suggestion: subjectAltName / rfc822Name
  • anima.acp+<ACP address>@<domain>
  • An example: anima.acp+FD99:B02D:8EC3:0:200:0:6400:1@example.com
Changes from -02:
Focus on a single addressing scheme

• Proposed addressing scheme:

<table>
<thead>
<tr>
<th>8</th>
<th>40</th>
<th>3</th>
<th>13</th>
<th>63</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD</td>
<td>hash(domain)</td>
<td>Type</td>
<td>Zone ID</td>
<td>Device ID</td>
<td>V</td>
</tr>
</tbody>
</table>

• Add “Virtualisation” bit at the end
  • Allow addressing a virtual machine on a single node

• Keep routing simpler:
  • Node announces not a /128, but /127
Why the “V” bit?

<table>
<thead>
<tr>
<th>(base scheme)</th>
<th>Zone ID</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>V</td>
</tr>
</tbody>
</table>

containers →

- AN controller element
- xxxx::1

physical node

- xxxx::0/127
- xxxx::0
- xxxx::0/127
Changes from -02

• Deleted appendix on “ACP without separation”
  • As previously decided
• Editorial changes, references, etc.