

A YANG Data Model and RADIUS Extension for Policy-based Network Access Control

draft-ietf-opsawg-ucl-acl-01

Qiufang Ma (Huawei) Presenter

Qin Wu (Huawei)

Mohamed Boucadair (Orange)

Daniel King (Lancaster University)

Document Status

- Adopted after IETF 117, RADEXT WG helped review the new RADIUS attribute (User-Access-Group-ID) definition part
 - A lot of good review comments – Thank you all!
- Issues tracked in <https://github.com/boucadair/policy-based-network-acl>
 - Should we specify any mechanism for the endpoint group string to be mapped as ID?
<https://github.com/boucadair/policy-based-network-acl/issues/25>
 - Consider to add some text about what hardware ramifications might exist and what operational trade-offs implementations would consider.
<https://github.com/boucadair/policy-based-network-acl/issues/14>
- Everyone is welcome to report issues or propose changes on the GitHub repo

High-level Document Updates since IETF 117

- Move the definition of schedule YANG data model into a separate document (draft-ma-opsawg-schedule-yang), and use groupings defined in draft-ma-opsawg-schedule-yang
 - <https://mailarchive.ietf.org/arch/msg/opsawg/fKx-pFULtWbc56TN8SgoC5kVK24/>
 - See next slide
- Change the document title and add a reference to "policy"
 - A Policy-based Network Access Control -> A YANG Data Model and RADIUS Extension for Policy-based Network Access
- Change endpoint group-id as a string, and fix related examples accordingly
 - allows for some hierarchy that might be useful to ease coordination of different endpoint groups
- Tweaks to the RADIUS section and add a restriction to the length based on comments from RADEXT
- Add informative reference to I-D. dekok-radext-deprecating-radius for authentication method recommendations
- Use typedef to ease leafref of the node
- Add IPv6 examples besides IPv4

Separation of the schedule YANG model from draft-ietf-opsawg-ucl-acl

- draft-ma-opsawg-schedule-yang-00 is posted
 - A new I-D but borrows heavily from draft-ietf-opsawg-ucl-acl-00 (95% of the contents)
 - Remaining 5% add reference to some on-going efforts related to scheduling, e.g.,
 - I-D.contreras-opsawg-scheduling-oam-tests (schedule on-demand OAM tests)
 - I-D.ietf-opsawg-ucl-acl (ACL policy activation based date and time conditions)
 - I-D.united-tvr-schedule-yang (manage network resources with time scheduled changes)
 - Two groupings (period and recurrence) are defined in the ietf-schedule.yang
 - Conform to the definition of “period of time” and “recurrence rule” formats in RFC5545, one wheel we don’t really want to reinvent
 - Designed to be applicable for common scheduling information such as event, policy, scheduled services or resources based on date and time
- A side meeting (Thursday afternoon, 3PM~4PM, Karlin 4) has be planned to
 - Seek coordination among authors of different documents
 - Explore whether a common framework for scheduled service is needed

Next Steps

- Bring the side meeting achievement back to the WG
- Continuously work on the common schedule YANG data model which this document normatively depends on
- Resolve open issues
 - Comments and suggestions are welcome
- Request the WG to review the document updates and provide the feedback

Comments, Questions, Concerns?