NETCONF Access Control

draft-ietf-netconf-access-control-03
IETF 80, March 2011

Andy Bierman
andy.bierman@brocade.com

Martin Bjorklund
mbj@tail-f.com

Agenda

- Changes to NACM Draft
- Open Issues

Changes to NACM draft

- RFC 2119 terminology cleanup
  - Added many MUST/SHOULD/MAY clarifications
- Clarifications
  - Procedures updated to account for nacm-enabled flag == false
  - Changed term usage of 'database' to 'datastore'

Changes to NACM draft (2)

- Removed authentication text and objects.
- Changed module name from ietf-nacm to ietf-netconf-acm.
- Removed open issues section.

Open Issues

- Superuser
  - Need to word smith this text so the term superuser is avoided;
    - Emergency recovery user
- What to do about <copy-config> leaving out unauthorized data?
  - Should backup/restore only be done by a user with full access, or should the server violate the NETCONF operation and pretend the unauthorized data was not removed?
- How much rationale text needs to be added?

Open Issues (2)

- Should we reorganize rule specification to make it easier to manage the control of specific device features
  - All rules together is not reusable; too hard to understand when all rules mixed together
- Are debugging features needed
  - RPC to trace rule matching logic for real or 'dummy' access requests

Open Issues (3)

- What to do with authentication objects that were removed?
  - Leave as proprietary
  - Start new standard module in NETMOD WG