VACM Extensions for use with RADIUS

draft-nelson-isms-extended-vacm-00.txt

Background

- Usage of RADIUS for SNMP Secure Transport models addresses user authentication and authorization of the transport protocol.
- User authorization is still expected to use View based Access Control (VACM) model described in RFC3415.
- This split model will result in sub-optimal operational models with the need to replicate users from the RADIUS server to every SNMP engine.
- This draft describes an approach to use a policy identifier from the RADIUS server to bind the authenticated user to specific authorization delivered by VACM.

Solution Approach

- Separation of concerns
  - RADIUS deals with mapping of users to groups.
  - VACM manages the rules for access control to specific SNMP operations and MIB objects.
- Maintain SNMPv3 modularity
  - Leverage “tmStateReference” cache.
- Dynamic vs Static policy
  - RADIUS leveraged to update dynamic user to group mapping. VACM Access rules are managed using existing methods

VACM Extensions

- tmStateReference cache updated to add tmAccessPolicy to store User Group.
- Extension requires VACM MIB to be updated based on User properties received in RADIUS.
  - tmSecurityName copied to vacmSecurityName.
  - tmAccessPolicy copied to vacmSecurityToGroupTable
- No updates required to ASI or Elements of Procedure for VACM.

RADIUS specifics

- draft-ietf-isms-radius-usage-07 is a pre-requisite
- Leverages Management-Policy-ID attribute described in draft-ietf-radext-management-authorization-07.

Discussion Items

- Name collision issues
  - Existing user to group mapping exists in the VACM MIB.
  - Which entity is authoritative (RADIUS server or local SNMP engine).
- VACM entries created by RADIUS server need to purged at the end of the session.
- One possible method to avoid collision and represent appropriate temporal semantics is to define new MIB module to store mappings of user to group for RADIUS solution.
- VACM can be extended to look up new MIB.