Extensions to the View-based Access Control Model for use with RADIUS
draft-ietf-isms-radius-vacm-04.txt

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols. In particular, it describes a backward-compatible supplement to the View-based Access Control Model (VACM) for version 3 of the Simple Network Management Protocol (SNMPv3) for use with the Remote Authentication Dial-In User Service (RADIUS) and other Authentication, Authorization, and Accounting (AAA) services to provide authorization of MIB database access, and defines objects for managing this supplement. It is intended to be used in conjunction with session-oriented secure SNMP Transport Models that facilitate RADIUS authentication, such as the Secure Shell Transport Model.

Comments are solicited and should be addressed to the working group’s mailing list at isms@ietf.org.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at

This Internet-Draft will expire on August 30, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.
1. Introduction

This memo specifies an integration of several protocols to operationally simplify the administration of the access rights granted to users of network management data. In this environment:

- The View-Based Access Control Model (VACM) [RFC3415] provides a means to manage users’ access rights to management information accessed using SNMP.

It is possible to authenticate SNMPv3 messages via a RADIUS when those messages are sent over the SSH transport. As originally envisioned, VACM authorizes a given SNMP transaction using on-device, pre-existing authorization configuration. In order to leverage a centralized RADIUS service to its full extent, the access control decision in the Access Control Subsystem needs to be able to make use of authorization information received from RADIUS as well. This document defines an extension to the View-based Access Control Model to obtain authorization information for an authenticated principal, from RADIUS or equivalent AAA service supporting a Transport Security Model.

Additional introductory material on the RADIUS operational model and RADIUS usage with SNMP may be found in Sections 1.3 and 1.5 of [RFC5608].

It is important to understand the SNMP architecture and the terminology of the architecture to understand where the Extended View-based Access Control Model described in this memo fits into the
architecture and how it interacts with other subsystems and models within the architecture. It is expected that reader will have also read and understood RFC3411 [RFC3411], RFC3412 [RFC3412], RFC3413 [RFC3413], RFC3415 [RFC3415]and RFC3418 [RFC3418]. As this document describes an extension to VACM, a thorough understanding of RFC3415 [RFC3415] is assumed.

2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIV2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

4. Overview

4.1. System Block Diagram

A block diagram of the major system components referenced in this document may be useful to understanding the text that follows.
This diagram illustrates that a network management application communicates with a network device, the managed entity, using, for example, SNMP over SSH. The network device uses RADIUS to communicate with a RADIUS Server to authenticate the network management application (or the user whose credentials that application provides) and to obtain authorization information related to access via SNMP for purpose of device management. Other secure transport protocols might be used instead of SSH, and other AAA services might be used instead of RADIUS.

4.2. Using RADIUS with SNMP

There are two use cases for RADIUS support of management access via SNMP. These are (a) service authorization and (b) access control authorization. The former is discussed in detail in [RFC5608]. The second use case is the subject of this document. This document describes how RADIUS attributes and messages are applied to the specific application area of SNMP Access Control Models, and VACM in particular.

The RFC 3411 SNMP architecture maintains strong modularity and separation of concerns, extending to separating user identity (authentication) from user database access rights (authorization). The former is the business of the Security Subsystem and the latter is the business of the Access Control Subsystem. RADIUS, on the other hand, allows for no such separation of authorization from authentication. In order to use RADIUS with SNMP, binding of user authentication to user authorization must be achieved, without violating the modularity of the RFC 3411 SNMP architecture.
RADIUS does support a limited form of Authorize-Only operations. The RADIUS "Authorize Only" Service-Type Attribute can be specified in an Access-Request message, but only when accompanied by a RADIUS State Attribute, which contains an implementation specific "cookie" representing the successful outcome of a previous authentication transaction. For that reason, it is not possible to completely separate the use of RADIUS by the Access Control Subsystem from the use of RADIUS by other subsystems. This suggests that the most straightforward approach is to leverage the existing RADIUS usage, as documented in [RFC5608], and the tmStateReference cache, as documented in Section 5.2 of [RFC5590].

The operative use case assumption here is that roles within an organization, which are reflected in VACM as groups and rules, change infrequently, while the users assigned to those roles change much more frequently. This memo describes how the user-to-role (group) mapping can be outsourced to the RADIUS server, avoiding the need to re-provision managed devices as users are added, deleted, or assigned new roles in an organization.

This memo assumes that the detailed access control policies are pre-configured in VACM, and does not attempt to address the question of how the policy associated with a given role is put in place.

The only additional information obtained from the AAA service is the mapping of the authenticated user’s identifier to a specific role (or "group" in VACM terminology) in the access control policy. Dynamic user authorization for MIB database access control, as defined herein, is limited to mapping the authenticated user to a group, which in turn is mapped to the pre-existing rules.

4.3. Applicability

Though this memo was motivated to support the use of specific Transport Security Models, it MAY be used with other Transport Security Models whose implementations satisfy these requirements:

- the model has a notion of "session";
- the model uses an AAA service for sign-on service authorization;
- the model provides an indication of the beginning session for a particular user, identified using a SecurityName, and provides the corresponding value of vacmGroupName to be used, based on information provided by the AAA service in use;
o the model provides an indication of the end of a session, whether
due to disconnection, termination due to timeout, or any other
reason.

Likewise, although this memo specifically refers to RADIUS, it MAY be
used with other AAA services satisfying these requirements:

o the service provides information semantically equivalent to the
  RADIUS Management-Policy-ID attribute, which has been mapped
  (perhaps trivially) into a GroupName;

o the service provides information semantically equivalent to the
  RADIUS User-Name Attribute, which has been mapped (perhaps
  trivially) into a SecurityName.

5. Structure of the MIB Module

5.1. Textual Conventions

This MIB module makes use of the SnmpAdminString and
SnmpSecurityModel textual conventions.

5.2. The Table Structures

This MIB module defines a single table, the
extVacmSecurityToGroupTable. This table is indexed by the integer
assigned to each security model, the protocol-independent
SecurityName corresponding to a principal, and the unique identifier
of a transport session. This index structure was chosen to support
use cases in which a given user could potentially have multiple
concurrent sessions, and to support environments in which multiple
security models might find concurrent usage.

6. Relationship to Other MIB Modules

6.1. Relationship to the VACM MIB

The extVacmSecurityToGroupTable has a close relationship to the VACM
MIB’s vacmSecurityToGroupTable.

6.1.1. Extended VACM for RADIUS Authorization

This memo relies on implementation-specific integration of the RADIUS
client for user authentication and authorization. In particular, the
implementation MUST make the RADIUS Management-Policy-Id [RFC5607]
and User-Name Attributes (or equivalent) from the RADIUS Access-Accept message (or equivalent) available to Extended VACM.

The design of VACM ensures that if an unknown policy (group name) is used in the VacmSecurityToGroupTable, no access is granted.

The intended use of the content of the Management-Policy-Id attribute is to provision a mapping between the authenticated user, associated with the secure transport session, and an access control group pre-provisioned in the VACM MIB module. Details of this mapping are described in following sections.

6.1.2. VACM Extension for RADIUS Authorization

This memo describes a method by which selected MIB objects associated with VACM [RFC3415] are dynamically provisioned based on information received from RADIUS, or another AAA service. This method requires no changes to the Abstract Service Interface (ASI) for the Access Control Subsystem, nor any changes in the Elements of Procedure (EOP) for VACM. A new MIB module that reflects the information received from the AAA service to update the vacmSecurityToGroupTable is defined in this document, as well as the elements of procedure for creating, updating, and deleting entries in this module’s table. Its implementation does require that code somewhere in the NAS be able to access (read and write) the VACM MIB module and Extended VACM MIB Module, in immediate response to access control policy information received from RADIUS.

6.1.2.1. Dynamic Update of VACM and Extended VACM MIB Module Objects

The implementation-dependent interface between the RADIUS Client function and the SNMP Engine is responsible for updating the extVacmSecurityToGroupTable and the corresponding rows of the vacmSecurityToGroupTable table within the VACM MIB Module [RFC3415]. Specifically, the RADIUS User-Name Attribute is used as the vacmSecurityName and the RADIUS Management-Policy-Id Attribute is used as the vacmGroupName. The value used for vacmSecurityModel is the registered value for the security model in use. Note that the security model SHOULD be one which binds principal identity to access control policy via an external AAA server, such as the Transport Security Model. To do otherwise potentially creates a security risk.

Whenever a new session begins, a new entry is created in the extVacmSecurityToGroupTable, indexed by the identifier of the Security Model itself, the SecurityName (derived from, e.g., the RADIUS User-Name Attribute), and a unique transport session identifier.
If no corresponding entry exists in the `vacmSecurityToGroupTable`, nothing has been pre-provisioned for this particular user, so an entry is created, with a `StorageType` of "volatile", and with using the `vacmGroupName` supplied by the RADIUS server.

If a corresponding entry already exists in the `vacmSecurityToGroupTable`, and the row’s `StorageType` is "volatile", the operational assumption is that this entry was probably dynamically created by this function, since an entry created by a security administrator would not normally be given a `StorageType` of "volatile". The value being provided by RADIUS will either be the same as what is already there, or, if it is different, the new information is understood as a more recent role (group) assignment for the user, which should supersede the one currently held there. Consequently, `vacmGroupName` is updated with the whatever value is supplied by the RADIUS server.

If a corresponding entry already exists in the `vacmSecurityToGroupTable`, and the row’s `StorageType` is anything other than "volatile", a role (group) mapping for this principal has already been administratively explicitly provisioned on this system, and will not be overridden.

### 6.1.2.2. Purging Entries in the Extended VACM MIB Module

Entries in the `vacmSecurityToGroupTable` MUST NOT persist across system reboots.

When the corresponding secure transport session has been terminated for any reason, the corresponding `extVacmSecurityToGroupEntry` is deleted. When no rows remain having corresponding values for `extVacmSecurityName` and `extVacmSecurityModel`, then, if the corresponding row in the in the `vacmSecurityToGroup` has a `StorageType` of "volatile", that row MUST be deleted as well. The mechanism to accomplish this task is implementation specific.

### 6.1.3. Elements of Procedure for Extended VACM

This section describes the Elements of Procedure for Extended VACM. The function of the VACM extension is to manage the creation and deletion of rows in the `vacmSecurityToGroupTable`, based on the outcome of RADIUS authorization. All access control decision functions are taken by VACM, as defined in [RFC3415]. The elements of procedure for VACM are unchanged.

When a RADIUS (or other AAA service) authorizes SNMP data access control for a user-authenticated secure transport session, the NAS causes the RADIUS provisioning information to be made available to
the Extended VACM facility, which populates the vacmSecurityToGroupTable, as follows:

1. If the the RADIUS Management-Policy-Id Attribute is not available, no action is taken.

2. If an existing row has a vacmSecurityName matching the RADIUS User-Name Attribute, a vacmSecurityModel corresponding to the security model, and an extVacmTransportSessionID matching the ID provided by the Secure Transport, an internal logic error of some kind has may have occurred. Recovery is implementation-specific.

3. If no additional table rows could be created, e.g. because of resource constraints, this is an internal error. Recovery is implementation-specific.

4. Create a new row with the columns populated as follows:
   A. extVacmSecurityModel = value of SnmpSecurityModel registered with the security model in use
   B. extVacmSecurityName = RADIUS User-Name Attribute or equivalent
   C. extVacmTransportSessionID = ID provided by the Secure Transport Model
   D. extVacmGroupName = RADIUS Management-Policy-Id Attribute

5. Using the value of extVacmSecurityModel for vacmSecurityModel, and the value of extVacmSecurityName for vacmSecurityName, if no corresponding entry exists in the vacmSecurityToGroupTable, create one, using extVacmGroupName to fill in vacmGroupName, using a value of "volatile" for vacmSecurityToGroupStorageType, and "active" for vacmSecurityToGroupStatus.

6. Otherwise (that is, if corresponding entry already exists in the vacmSecurityToGroupTable), if vacmSecurityToGroupStorageType is "volatile" and vacmSecurityToGroupStatus is "active", update the value of vacmGroupName with the value from extVacmGroupName.

When a RADIUS-authenticated secure transport session is disconnected by the remote peer, the NAS causes the Extended VACM to remove the corresponding table row from the vacmSecurityToGroupTable. The NAS provides an implementation dependent identifier of the session in question to Extended VACM.
1. Search for a row with a matching extVacmSecurityModel and extVacmTransportSessionID.

2. If a table row exists with a matching value of extVACMTransportSessionID, that row is deleted.

When the last row bearing a particular (extVacmSecurityModel, extVacmSecurityName) pair is deleted from the extVacmSecurityToGroupTable, the vacmSecurityToGroupTable is examined for a corresponding row. If one exists, and if its StorageType is "volatile" and its RowStatus is "active", that row is deleted as well.

6.2. MIB modules required for IMPORTS

The MIB module employs definitions from [RFC2578], [RFC2579] and [RFC3411].

7. Definitions

SNMP-EXT-VACM-MIB DEFINITIONS ::= BEGIN

IMPORTS
   MODULE-COMPLIANCE, OBJECT-GROUP FROM SNMPv2-CONF
   MODULE-IDENTITY, OBJECT-TYPE, mib-2,
      Unsigned32, Counter32 FROM SNMPv2-SMI
   SnmpAdminString, SnmpSecurityModel FROM SNMP-FRAMEWORK-MIB;

snmpExtVacmMIB MODULE-IDENTITY
   LAST-UPDATED "201002250000Z" -- 25 February, 2010
   ORGANIZATION "ISMS Working Group"
   CONTACT-INFO "WG-email: isms@ietf.org"

   DESCRIPTION "The management and local datastore information
definitions for the Extended View-based Access
Control Model for SNMP.

   Copyright (c) 2010 IETF Trust and the persons
identified as the document authors. All rights
reserved.

   Redistribution and use in source and binary forms,
with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in Section 4.c of the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info).

This version of this MIB module is part of RFC XXXX; see the RFC itself for full legal notices.

REVISION "201002250000Z"
DESCRIPTION "Initial version, published as RFC XXXX."
::= { mib-2 XXX }

extVacmMIBObjects OBJECT IDENTIFIER ::= { snmpExtVacmMIB 1 }

extVacmMIBConformance OBJECT IDENTIFIER ::= {snmpExtVacmMIB 2 }

extVacmSecurityToGroupTable OBJECT-TYPE
SYNTAX SEQUENCE OF ExtVacmSecurityToGroupEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "This table maps a combination of securityModel and securityName into a groupName which is used to define an access control policy for a group of principals."
::= { extVacmMIBObjects 1 }

extVacmSecurityToGroupEntry OBJECT-TYPE
SYNTAX ExtVacmSecurityToGroupEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry in this table maps the combination of a securityModel and securityName into a groupName. An entry corresponds to a secure transport session. Entries do not persist across reboots. When the secure transport session is torn down, disconnected, timed out (e.g. following the RADIUS Session-Timeout Attribute), or otherwise terminated for any reason, the corresponding extVacmSecurityToGroupEntry is deleted."
INDEX
::= { extVacmSecurityModel, extVacmSecurityName, extVacmTransportSessionID }

ExtVacmSecurityToGroupEntry ::= SEQUENCE
{
  extVacmSecurityModel      SnmpSecurityModel,
  extVacmSecurityName      SnmpAdminString,
  extVacmTransportSessionID Unsigned32,
  extVacmGroupName         SnmpAdminString
}

extVacmSecurityModel OBJECT-TYPE
SYNTAX      SnmpSecurityModel(1..2147483647)
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION "The Security Model to which the session referred to by this entry belongs. This object cannot take the 'any' (0) value."
::= { extVacmSecurityToGroupEntry 1 }

extVacmSecurityName OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE(1..32))
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION "The Security Name of the principal associated with this session, provided by the Transport Model, and represented in a Security Model independent format. Transport model which is mapped by this entry to a groupName."
::= { extVacmSecurityToGroupEntry 2 }

extVacmTransportSessionID OBJECT-TYPE
SYNTAX      Unsigned32
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION "A transport model-specific identifier of the session. This value MUST be unique among all of a given transport model’s currently open sessions. The value has no particular significance other to distinguish sessions. An example of a suitable value would be tlstmSessionID."
::= { extVacmSecurityToGroupEntry 3 }

extVacmGroupName OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE(1..32))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "The name of the group to which this entry is to belong. This information would have come from, for example, the RADIUS Management-Policy-ID attribute."
This group name is used to set the vacmGroupName in the corresponding vacmSecurityToGroupEntry.

```plaintext
::= { extVacmSecurityToGroupEntry 4 }
```

-- Conformance information

```plaintext
extVacmMIBCompliances
OBJECT IDENTIFIER ::= {extVacmMIBConformance 1}

extVacmMIBGroups
OBJECT IDENTIFIER ::= {extVacmMIBConformance 2}
```

-- compliance statements

```plaintext
extVacmMIBBasicCompliance MODULE-COMPLIANCE
   STATUS       current
   DESCRIPTION "The compliance statement for SNMP engines which implement the Extensions to the View-based Access Control Model for use with RADIUS."

   MODULE -- this module
      MANDATORY-GROUPS { extVacmGroup }

   ::= { extVacmMIBCompliances 1 }
```

-- units of conformance

```plaintext
extVacmGroup OBJECT-GROUP
   OBJECTS {
      extVacmGroupName
   }
   STATUS       current
   DESCRIPTION "A collection of objects for supporting the use of RADIUS to provide user / group mappings for VACM."

   ::= { extVacmMIBGroups 1 }
```

END

8. Security Considerations

This integration strongly assumes that RADIUS (or some other AAA service) is at least as trusted as the security administrator with access rights to the vacmSecurityToGroupTable. It assumes that the transport security model can be trusted to pass through the users’ security name and the group name provided by the AAA service. It
also trusts the transport security model to enforce any session timeouts imposed by the RADIUS server, and to provide an indicate whenever a session ends.

The algorithms in this memo make heuristic use of the StorageType of entries in the vacmSecurityToGroupTable to distinguish those which have been provisioned by a security administrator (which would presumably not be configured as "volatile") and those dynamically generated. In making this distinction, it assumes that those entries explicitly provisioned by a security administrator and given a non-"volatile" status are not to be dynamically over-ridden. Users of this memo need to be aware of this operational assumption, which, while reasonable, is not necessarily universal.

There are no management objects defined in this MIB module that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB module is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB module via direct SNMP SET operations.

Some of the readable objects in this MIB module (including some objects with a MAX-ACCESS of not-accessible, whose values are exposed as a result access to indexed objects) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

- extVacmSecurityToGroupTable - the entire table is potentially sensitive, since walking the table will reveal user names, security models in use, transport session identifiers, and group names.
- extVacmSecurityModel - though not-accessible, this is exposed as an index of extVacmGroupName
- extVacmSecurityName - though not-accessible, this is exposed as an index of extVacmGroupName
- extVacmTransportSessionID - though not-accessible, this is exposed as an index of extVacmGroupName
- extVacmGroupName - since this identifies a security policy and associates it with a particular user, this is potentially sensitive.
SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

9. IANA Considerations

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER values recorded in the SMI Numbers registry:

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>OBJECT IDENTIFIER value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmpExtVacmMIB</td>
<td>{ mib-2 XXX }</td>
</tr>
</tbody>
</table>

Editor’s Note (to be removed prior to publication): the IANA is requested to assign a value for "XXX" under the ‘mib-2’ subtree and to record the assignment in the SMI Numbers registry. When the assignment has been made, the RFC Editor is asked to replace "XXX" (here and in the MIB module) with the assigned value and to remove this note.

10. Contributors

The following participants from the isms working group contributed to the development of this document:

- David Harrington
11. References

11.1. Normative References


11.2. Informative References


Appendix A. Open Issues

This section identifies questions and issues that have not been addressed in this version of this document. This section will probably be removed prior to publication, since there will be no questions left to address.

1. Make sure that the new Elements of Procedure make sense and cover all the corner cases correctly.

2. Security considerations need to be filled in, specifically concerning trust relationships to RADIUS and the interaction with statically configured policy.

3. There’s a lot of repetition / redundancy.
Authors’ Addresses

Kaushik Narayan
Cisco Systems, Inc.
10 West Tasman Drive
San Jose, CA  95134
USA

Phone: +1.408.526.8168
Email: kaushik_narayan@yahoo.com

David Nelson
Elbrys Networks, Inc.
282 Corporate Drive, Unit #1,
Portsmouth, NH  03801
USA

Phone: +1.603.570.2636
Email: d.b.nelson@comcast.net

Randy Presuhn (editor)
None
San Jose, CA  95120
USA

Email: randy_presuhn@mindspring.com