RADIUS Accounting Server MIB

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This memo defines a set of extensions which instrument RADIUS accounting server functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS accounting servers.

1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing RADIUS accounting servers.

RADIUS accounting servers are today widely deployed by dialup Internet Service Providers, in order to provide accounting services. As a result, the effective management of RADIUS accounting servers is of considerable importance.

2. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- An overall architecture, described in RFC 2571 [1].
- Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIv1 and described in...
The second version, called SMIv2, is described in STD 58, RFC 2578 [5], RFC 2579 [6] and RFC 2580 [7].

- **Message protocols for transferring management information.** The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, RFC 1157 [8]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [9] and RFC 1906 [10]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [10], RFC 2572 [11] and RFC 2574 [12].

- **Protocol operations for accessing management information.** The first set of protocol operations and associated PDU formats is described in STD 15, RFC 1157 [8]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [13].

- **A set of fundamental applications described in RFC 2573 [14] and the view-based access control mechanism described in RFC 2575 [15].**

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIv2. A MIB conforming to the SMIv1 can be produced through the appropriate translations. The resulting translated MIB must be semantically equivalent, except where objects or events are omitted because no translation is possible (use of Counter64). Some machine readable information in SMIv2 will be converted into textual descriptions in SMIv1 during the translation process. However, this loss of machine readable information is not considered to change the semantics of the MIB.

### 3. Overview

The RADIUS accounting protocol, described in [16], distinguishes between the client function and the server function. In RADIUS accounting, clients send Accounting-Requests, and servers reply with Accounting-Responses. Typically NAS devices implement the client function, and thus would be expected to implement the RADIUS accounting client MIB, while RADIUS accounting servers implement the server function, and thus would be expected to implement the RADIUS accounting server MIB.
However, it is possible for a RADIUS accounting entity to perform both client and server functions. For example, a RADIUS proxy may act as a server to one or more RADIUS accounting clients, while simultaneously acting as an accounting client to one or more accounting servers. In such situations, it is expected that RADIUS entities combining client and server functionality will support both the client and server MIBs.

3.1. Selected objects

This MIB module contains thirteen scalars as well as a single table:

(1) the RADIUS Accounting Client Table contains one row for each RADIUS accounting client that the server shares a secret with.

Each entry in the RADIUS Accounting Client Table includes eleven columns presenting a view of the activity of the RADIUS accounting server.

4. Definitions

RADIUS-ACC-SERVER-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY,
Counter32, Integer32,
IpAddress, TimeTicks, mib-2 FROM SNMPv2-SMI
SnmpAdminString FROM SNMP-FRAMEWORK-MIB

MODULE-COMPLIANCE, OBJECT-GROUP FROM SNMPv2-CONF;

radiusAccServMIB MODULE-IDENTITY
LAST-UPDATED "9906110000Z" -- 11 Jun 1999
ORGANIZATION "IETF RADIUS Working Group."
CONTACT-INFO
" Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA  98052
US

Phone: +1 425 936 6605
EMail: bernarda@microsoft.com"
DESCRIPTION
"The MIB module for entities implementing the server side of the Remote Access Dialin User Service (RADIUS) accounting protocol."
REVISION "9906110000Z" -- 11 Jun 1999
DESCRIPTION "Initial version as published in RFC 2621"
::= { radiusAccounting 1 }

radiusMIB OBJECT-IDENTITY
  STATUS current
  DESCRIPTION
    "The OID assigned to RADIUS MIB work by the IANA."
  ::= { mib-2 67 }

radiusAccounting OBJECT IDENTIFIER ::= {radiusMIB 2}

radiusAccServMIBObjects OBJECT IDENTIFIER ::= { radiusAccServMIBObjects 1 }

radiusAccServ OBJECT IDENTIFIER ::= { radiusAccServMIBObjects 1 }

radiusAccServIdent OBJECT-TYPE
  SYNTAX     SnmpAdminString
  MAX-ACCESS read-only
  STATUS     current
  DESCRIPTION
    "The implementation identification string for the
    RADIUS accounting server software in use on the
    system, for example; ‘FNS-2.1’"
  ::= {radiusAccServ 1}

radiusAccServUpTime OBJECT-TYPE
  SYNTAX     TimeTicks
  MAX-ACCESS read-only
  STATUS     current
  DESCRIPTION
    "If the server has a persistent state (e.g., a process),
    this value will be the time elapsed (in hundredths of a
    second) since the server process was started.
    For software without persistent state, this value will
    be zero."
  ::= {radiusAccServ 2}

radiusAccServResetTime OBJECT-TYPE
  SYNTAX     TimeTicks
  MAX-ACCESS read-only
  STATUS     current
  DESCRIPTION
    "If the server has a persistent state (e.g., a process)
    and supports a ‘reset’ operation (e.g., can be told to
    re-read configuration files), this value will be the
    time elapsed (in hundredths of a second) since the
    server was ‘reset.’ For software that does not
    have persistence or does not support a ‘reset’ operation,
this value will be zero."
::= {radiusAccServ 3}

radiusAccServConfigReset OBJECT-TYPE
SYNTAX INTEGER { other(1),
    reset(2),
    initializing(3),
    running(4) }
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Status/action object to reinitialize any persistent
server state. When set to reset(2), any persistent
server state (such as a process) is reinitialized as if
the server had just been started. This value will
never be returned by a read operation. When read, one
of the following values will be returned:
    other(1) - server in some unknown state;
    initializing(3) - server (re)initializing;
    running(4) - server currently running."
::= {radiusAccServ 4}

-- New Stats proposed by Dale E. Reed Jr (daler@iea.com)

radiusAccServTotalRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of packets received on the
accounting port."
::= {radiusAccServ 5}

radiusAccServTotalInvalidRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Accounting-Request packets
received from unknown addresses."
::= {radiusAccServ 6}

radiusAccServTotalDupRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of duplicate RADIUS Accounting-Request
packets received."
::= { radiusAccServ 7 }

radiusAccServTotalResponses OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Response packets sent."
::= { radiusAccServ 8 }

radiusAccServTotalMalformedRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of malformed RADIUS Accounting-Request packets received. Bad authenticators or unknown types are not included as malformed Access-Requests."
::= { radiusAccServ 9 }

radiusAccServTotalBadAuthenticators OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Request packets which contained invalid Signature attributes."
::= { radiusAccServ 10 }

radiusAccServTotalPacketsDropped OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of incoming packets silently discarded for a reason other than malformed, bad authenticators, or unknown types."
::= { radiusAccServ 11 }

radiusAccServTotalNoRecords OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Request packets which were received and responded to but not recorded."
radiusAccServTotalUnknownTypes OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS packets of unknown type which were received."
::= { radiusAccServ 13 }

-- End of new

radiusAccClientTable OBJECT-TYPE
SYNTAX SEQUENCE OF RadiusAccClientEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The (conceptual) table listing the RADIUS accounting clients with which the server shares a secret."
::= { radiusAccServ 14 }

radiusAccClientEntry OBJECT-TYPE
SYNTAX RadiusAccClientEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry (conceptual row) representing a RADIUS accounting client with which the server shares a secret."
INDEX { radiusAccClientIndex }
::= { radiusAccClientTable 1 }

RadiusAccClientEntry ::= SEQUENCE {
  radiusAccClientIndex                           Integer32,
  radiusAccClientAddress                         IpAddress,
  radiusAccClientID                        SnmpAdminString,
  radiusAccServPacketsDropped                    Counter32,
  radiusAccServRequests                          Counter32,
  radiusAccServDupRequests                       Counter32,
  radiusAccServResponses                         Counter32,
  radiusAccServBadAuthenticators                 Counter32,
  radiusAccServMalformedRequests                 Counter32,
  radiusAccServNoRecords                         Counter32,
  radiusAccServUnknownTypes                      Counter32
}

radiusAccClientIndex OBJECT-TYPE
SYNTAX Integer32 (1..2147483647)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A number uniquely identifying each RADIUS accounting client with which this server communicates."
::= \{ radiusAccClientEntry 1 \}

radiusAccClientAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The NAS-IP-Address of the RADIUS accounting client referred to in this table entry."
::= \{ radiusAccClientEntry 2 \}

radiusAccClientID OBJECT-TYPE
SYNTAX SnmpAdminString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The NAS-Identifier of the RADIUS accounting client referred to in this table entry. This is not necessarily the same as sysName in MIB II."
::= \{ radiusAccClientEntry 3 \}

-- Server Counters
--
-- Requests - DupRequests - BadAuthentication - MalformedRequests -
-- UnknownTypes - PacketsDropped - Responses = Pending
--
-- Requests - DupRequests - BadAuthentication - MalformedRequests -
-- UnknownTypes - PacketsDropped - NoRecords = entries logged

radiusAccServPacketsDropped OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of incoming packets received from this client and silently discarded for a reason other than malformed, bad authenticators, or unknown types."
::= \{ radiusAccClientEntry 4 \}

radiusAccServRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of packets received from this
client on the accounting port."
::= { radiusAccClientEntry 5 }

radiusAccServDupRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of duplicate RADIUS Accounting-Request
packets received from this client."
::= { radiusAccClientEntry 6 }

radiusAccServResponses OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Response packets
sent to this client."
::= { radiusAccClientEntry 7 }

radiusAccServBadAuthenticators OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Request packets
which contained invalid authenticators received
from this client."
::= { radiusAccClientEntry 8 }

radiusAccServMalformedRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of malformed RADIUS Accounting-Request
packets which were received from this client.
Bad authenticators and unknown types
are not included as malformed Accounting-Requests."
::= { radiusAccClientEntry 9 }

radiusAccServNoRecords OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Accounting-Request packets which were received and responded to but not recorded."
 ::= { radiusAccClientEntry 10 }

radiusAccServUnknownTypes OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS packets of unknown type which were received from this client."
 ::= { radiusAccClientEntry 11 }

-- conformance information

radiusAccServMIBConformance
OBJECT IDENTIFIER ::= { radiusAccServMIB 2 }

radiusAccServMIBCompliances
OBJECT IDENTIFIER ::= { radiusAccServMIBConformance 1 }

radiusAccServMIBGroups
OBJECT IDENTIFIER ::= { radiusAccServMIBConformance 2 }

-- compliance statements

radiusAccServMIBCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement for accounting servers implementing the RADIUS Accounting Server MIB."
MODULE -- this module
MANDATORY-GROUPS { radiusAccServMIBGroup }

OBJECT radiusAccServConfigReset
WRITE-SYNTAX INTEGER { reset(2) }
DESCRIPTION "The only SETable value is 'reset' (2)."
 ::= { radiusAccServMIBCompliances 1 }

-- units of conformance

radiusAccServMIBGroup OBJECT-GROUP
OBJECTS {radiusAccServIdent,
radiusAccServUpTime,
radiusAccServResetTime,
radiusAccServConfigReset,
radiusAccServTotalRequests,
radiusAccServTotalInvalidRequests,
radiusAccServTotalDupRequests,
radiusAccServTotalResponses,
radiusAccServTotalMalformedRequests,
radiusAccServTotalBadAuthenticators,
radiusAccServTotalPacketsDropped,
radiusAccServTotalNoRecords,
radiusAccServTotalUnknownTypes,
radiusAccClientAddress,
radiusAccClientID,
radiusAccServPacketsDropped,
radiusAccServRequests,
radiusAccServDupRequests,
radiusAccServResponses,
radiusAccServBadAuthenticators,
radiusAccServMalformedRequests,
radiusAccServNoRecords,
radiusAccServUnknownTypes
}

STATUS current
DESCRIPTION
"The collection of objects providing management of
a RADIUS Accounting Server."
 ::= { radiusAccServMIBGroups 1 }

END

5. References


6. Security Considerations

There are management objects (radiusAccServConfigReset) defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations.

There are a number of managed objects in this MIB that may contain sensitive information. These are:

radiusAccClientAddress
This can be used to determine the address of the RADIUS accounting client with which the server is communicating. This information could be useful in impersonating the client.

radiusAccClientID
This can be used to determine the client ID for the accounting client with which the server is communicating. This information could be useful in impersonating the client.

It is thus important to control even GET access to these objects and possibly to even encrypt the values of these object when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment.

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPSec), 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.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2574 [12] and the View-based Access Control Model RFC 2575 [15] is recommended. Using these security features, customer/users can give access to the objects only to those principals (users) that have legitimate rights to GET or SET (change/create/delete) them.

7. Acknowledgments

The authors acknowledge the contributions of the RADIUS Working Group in the development of this MIB. Thanks to Narendra Gidwani of Microsoft, Allan C. Rubens of MERIT, Carl Rigney of Livingston and Peter Heitman of American Internet Corporation for useful discussions of this problem space.
8. Authors’ Addresses

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Phone: 425-936-6605  
EMail: bernarda@microsoft.com

Glen Zorn  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Phone: 425-703-1559  
EMail: glennz@microsoft.com
9. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.