Yang data model for TACACS+
draft-zheng-opsawg-tacacs-yang-02

Abstract

This document defines a YANG modules that augment the System data model defined in the RFC 7317 with TACACS+ client model. The data model of Terminal Access Controller Access Control System Plus (TACACS+) client allows the configuration of TACACS+ servers for centralized Authentication, Authorization and Accounting.

The YANG modules in this document conforms to the Network Management Datastore Architecture (NMDA) defined in RFC 8342.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 22, 2019.

Copyright Notice

Copyright (c) 2019 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 (https://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
This document defines a YANG modules that augment the System data model defined in the [RFC7317] with TACACS+ client model.

TACACS+ provides Device Administration for routers, network access servers and other networked computing devices via one or more centralized servers which is defined in the TACACS+ Protocol. [I-D.ietf-opsawg-tacacs]

The System Management Model [RFC7317] defines two YANG features to support local or RADIUS authentication:

- User Authentication Model: Define a list of usernames and passwords and control the order in which local or RADIUS authentication is used.
- RADIUS Client Model: Defines a list of RADIUS server that a device used.

Since TACACS+ is also used for device management and the feature is not contained in the system model, this document defines a YANG data model that allows users to configure TACACS+ client functions on a device for centralized Authentication, Authorization and Accounting provided by TACACS+ servers.
The YANG models can be used with network management protocols such as NETCONF [RFC6241] to install, manipulate, and delete the configuration of network devices.

The YANG data model in this document conforms to the Network Management Datastore Architecture (NMDA) defined in [RFC8342].

2. Conventions used in this document

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP14, [RFC2119], [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are defined in [RFC6241] and are used in this specification:

- client
- configuration data
- server
- state data

The following terms are defined in [RFC7950] and are used in this specification:

- augment
- data model
- data node

The terminology for describing YANG data models is found in [RFC7950].

2.1. Tree Diagrams

Tree diagrams used in this document follow the notation defined in [RFC8340].

3. TACACS+ Client Model

This model is used to configure TACACS+ client on the device to support deployment scenarios with centralized authentication, authorization, and accounting servers. Authentication is used to
validates a user’s name and password, authorization allows the user to access and execute commands at various command levels assigned to the user and accounting keeps track of the activity of a user who has accessed the device.

The ietf-system-tacacsplus module is intended to augment the "/sys:system" path defined in the ietf-system module with "tacacsplus" grouping. Therefore, a device can use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) to validate users who attempt to access the router by several mechanisms, e.g. a command line interface or a web-based user interface.

The "server" list is directly under the "tacacsplus" container, which is to hold a list of different TACACS+ server and use server-type to distinguish the three protocols. The list of servers is for redundancy purpose.

Most of the parameters in the "server" list are taken directly from the TACACS+ protocol [I-D.ietf-opsawg-tacacs], and some are derived from the wide implementation of network equipment manufacturers. For example, when there are multiple interfaces connected to the TACACS+ server, the source address of outgoing TACACS+ packets could be specified, or the source address could be specified through the interface setting. For the TACACS+ server located in a private network, a VRF instance needs to be specified.

The "statistics" container under the "server list" is to record session statistics and usage information during user access which include the amount of data a user has sent and/or received during a session.

The data model for TACACS+ client has the following structure:
module ietf-system-tacacsplus
    augment /sys:system:
        +++rw tacacsplus {tacacsplus}?
        +++rw server* [name]
            +++rw name            string
            +++rw server-type?    enumeration
            +++rw address         inet:host
            +++rw port?           inet:port-number
            +++rw shared-secret   string
            +++rw (source-type)?
            |   |   +++rw source-ip?    inet:ip-address
            |   ||  +++rw source-interface? if:interface-ref
            +++rw single-connection? boolean
            +++rw timeout?         uint16
            +++rw vrf-instance?
            |   -> /ni:network-instances/network-instance/name
            +++ro statistics
                +++ro connection-opens?  yang:counter64
                +++ro connection-closes?  yang:counter64
                +++ro connection-aborts?  yang:counter64
                +++ro connection-failures?  yang:counter64
                +++ro connection-timeouts?  yang:counter64
                +++ro messages-sent?      yang:counter64
                +++ro messages-received?   yang:counter64
                +++ro errors-received?     yang:counter64

4. TACACS+ Client Module

<CODE BEGINS> file "ietf-system-tacacsplus@2019-06-20.yang"

module ietf-system-tacacsplus {
    yang-version 1.1;
    namespace "urn:ietf:params:xml:ns:yang:ietf-system-tacacsplus";
    prefix sys-tcsplus;

    import ietf-inet-types {
        prefix inet;
        reference "RFC 6991: Common YANG Data Types";
    }
    import ietf-yang-types {
        prefix yang;
        reference "RFC 6991: Common YANG Data Types";
    }
    import ietf-network-instance {
        prefix ni;
        reference
    }

"RFC 8529: YANG Data Model for Network Instances";
}
import ietf-interfaces {
  prefix if;
  reference
    "RFC 8343: A YANG Data Model for Interface Management";
}
import ietf-system {
  prefix sys;
  reference "RFC 7317: A YANG Data Model for System Management";
}
import ietf-netconf-acm {
  prefix nacm;
  reference "RFC 8341: Network Configuration Access Control Model";
}
organization
  "IETF Opsawg (Operations and Management Area Working Group)";
contact
  "WG Web:  <http://tools.ietf.org/wg/opsawg/>
     WG List:  <mailto:opsawg@ietf.org>
     Editor:  Guangying Zheng
     <mailto:zhengguangying@huawei.com>"
description
  "This module provides configuration of TACACS+ client.

Copyright (c) 2018 IETF Trust and the persons identified as
authors of the code.  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 YANG module is part of RFC XXXX; see the RFC
itself for full legal notices."

revision 2019-06-20 {
  description
    "Initial revision.";
  reference "foo";
}

feature tacacsplus {
  description
"Indicates that the device can be configured as a TACACS+ client.";
reference "draft-ietf-opsawg-tacacs-11: The TACACS+ Protocol";

grouping statistics {
  description
  "Grouping for TACACS+ packets statistics attributes";
  container statistics {
    config false;
    description
      "A collection of server-related statistics objects";
    leaf connection-opens {
      type yang:counter64;
      description
        "Number of new connection requests sent to the server, e.g.
         socket open";
    }
    leaf connection-closes {
      type yang:counter64;
      description
        "Number of connection close requests sent to the server, e.g.
         socket close";
    }
    leaf connection-aborts {
      type yang:counter64;
      description
        "Number of aborted connections to the server. These do
         not include connections that are close gracefully.";
    }
    leaf connection-failures {
      type yang:counter64;
      description
        "Number of connection failures to the server";
    }
    leaf connection-timeouts {
      type yang:counter64;
      description
        "Number of connection timeouts to the server";
    }
    leaf messages-sent {
      type yang:counter64;
      description
        "Number of messages sent to the server";
    }
    leaf messages-received {
      type yang:counter64;
      description
        "Number of messages received from the server";
    }
  }
}
"Number of messages received by the server";
)
leaf errors-received {
  type yang:counter64;
  description
   "Number of error messages received from the server";
}
}
}
grouping tacacsplus {
  description
   "Grouping for TACACS+ attributes";
  container tacacsplus {
    if-feature "tacacsplus";
    description
     "Container for TACACS+ configurations and operations.";
    list server {
      key "name";
      ordered-by user;
      description
       "List of TACACS+ servers used by the device"

       When the TACACS+ client is invoked by a calling
       application, it sends the query to the first server in
       this list. If no response has been received within
       'timeout' seconds, the client continues with the next
       server in the list. If no response is received from any
       server, the client continues with the first server again.
       When the client has traversed the list 'attempts' times
       without receiving any response, it gives up and returns an
       error to the calling application.";
    }
    leaf name {
      type string;
      description
       "An arbitrary name for the TACACS+ server.";
    }
    leaf server-type {
      type enumeration {
        enum authentication {
          description
           "The server is an authentication server.";
        }
        enum authorization {
          description
           "The server is an authorization server.";
        }
        enum accounting {

description
   "The server is an accounting server.";
}
)
description
   "Server type: authentication/authorization/accounting.";
)
leaf address {
    type inet:host;
    mandatory true;
    description
       "The address of the TACACS+ server.";
}
leaf port {
    type inet:port-number;
    default "49";
    description
       "The port number of TACACS+ Server port.";
}
leaf shared-secret {
    type string;
    mandatory true;
    nacm:default-deny-all;
    description
       "The shared secret, which is known to both the
       TACACS+ client and server. TACACS+ server administrators
       SHOULD configure secret keys of minimum
       16 characters length.";
    reference "TACACS+ protocol:";
}
choice source-type {
    description
       "The source address type for outbound TACACS+ packets.";
    case source-ip {
        leaf source-ip {
            type inet:ip-address;
            description
               "Specifies source IP address for TACACS+ outbound
               packets.";
        }
    }
    case source-interface {
        leaf source-interface {
            type if:interface-ref;
            description
               "Specifies the interface from which the IP address is
               derived for use as the source for the outbound TACACS+
               packet";
        }
    }
}
leaf single-connection {
    type boolean;
    default "false";
    description
        "Whether the single connection mode is enabled for the
         server. By default, the single connection mode is
disabled.";
}
leaf timeout {
    type uint16 {
        range "1..300";
    }
    units "seconds";
    default "5";
    description
        "The number of seconds the device will wait for a
         response from each TACACS+ server before trying with a
different server.";
}
leaf vrf-instance {
    type leafref {
        path "/ni:network-instances/ni:network-instance/ni:name";
    }
    description
        "Specifies the VPN Routing and Forwarding (VRF) instance to
         use to communicate with the TACACS+ server.";
}

uses statistics;
}

augment "/sys:system" {
    description
        "Augment the system model with authorization and accounting
         attributes
         Augment the system model with the tacacsplus model";
    uses tacacsplus;
}

<CODE ENDS>
5. Security Considerations

The YANG module defined in this document is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446].

The NETCONF access control model [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations.

This document describes the use of TACACS+ for purposes of authentication, authorization and accounting, it is vulnerable to all of the threats that are present in TACACS+ applications. For a discussion of such threats, see Section 9 of the TACACS+ Protocol [I-D.ietf-opsawg-tacacs].

6. IANA Considerations

This document registers a URI in the IETF XML registry [RFC3688]. Following the format in [RFC3688], the following registration is requested to be made:

   Registrant Contact: The IESG.
   XML: N/A, the requested URI is an XML namespace.

This document registers a YANG module in the YANG Module Names registry [RFC7950].

   Name: ietf-system-tacacsplus
   Prefix: sys-tacsplus
   Reference: RFC XXXX
7. Acknowledgments

The authors wish to thank Alex Campbell and Ebben Aries, Alan DeKok, Joe Clarke, many others for their helpful comments.

8. References

8.1. Normative References


8.2. Informative References

[I-D.ietf-opsawg-tacacs]

Authors' Addresses

Guangying Zheng
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: zhengguangying@huawei.com

Michael Wang
Huawei Technologies, Co., Ltd
101 Software Avenue, Yuhua District
Nanjing 210012
China

Email: wangzitao@huawei.com
Bo Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: lana.wubo@huawei.com