Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 11, 2019

G. Zheng
M. Wang
B. Wu
Huawei

March 10, 2019

Yang data model for Terminal Access Controller Access Control System Plus
draft-zheng-opsawg-tacacs-yang-01

Abstract

This document defines two YANG modules that augment the System data model defined in the [RFC 7317] with TACACS+ client model and additional AAA 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 Accouting. While the current system model only supports authentication configuration, the additional AAA model allows system authorization and accouting configuration.

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

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 September 11, 2019.

Table of Contents

1. Introduction

This document defines two YANG modules that augment the System data model defined in the [RFC 7317] with TACACS+ client model and additional AAA 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 Accouting. While the current system model only supports authentication configuration, the additional AAA model allows system authorization and accouting configuration.

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

A YANG Data Model for System Management [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.

Additionally, to support full AAA feature, the "ietf-aaa" YANG module defined in this document provides user authorization model and user accouting model. The additional AAA model is intended to be used together with the authentication feature of the System model, to authorize what services that a user is allowed to use, and to maintain a record of the actions performed when a user logging on.

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

o 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. TACACSPLUS 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-tacacs module is intended to augment the "/sys:system" path defined in the ietf-system module with "tacacs" 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 "tacacs" container, which is 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.

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 has the following structure:

```
module: ietf-aaa-tacacs
  augment /sys:system:
    +--rw tacacs {tacacs}?
       +--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-ip?           inet:ip-address
       |  +--rw single-connection?   boolean
       |  +--rw network-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
       +--rw options
          +--rw timeout?   uint16
```

4. AAA Model Augmentation

This document augments the system model with authorization model and accouting model to support full AAA feature.

For the authentication model, if the NETCONF server advertises the "tacacs" feature, the device also supports user authentication using TACACSPLUS. For NETCONF transport protocols that support password authentication, the leaf-list "user-authentication-order" is used to control if TACACSPLUS password authentication should be used.

For the authorization model and accouting model, the extended AAA data model has the following structure:

```
module: ietf-system-aaa
  augment /sys:system:
    +--rw authorization {authorization}?
    |  +--rw user-authorization-order*   identityref
    |  +--rw events
    |     +--rw event* [event-type]
    |        +--rw event-type    identityref
    +--rw accouting {accouting}?
       +--rw user-accouting-order*   identityref
       +--rw events
          +--rw event* [event-type]
             +--rw event-type    identityref
             +--rw record?       enumeration
```

4.1. User Authorization Model

Following authentication, a user must gain authorization for doing certain tasks. For instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands.

This document defines two optional authorization YANG features: "local-users" and "tacacs", which the server advertises to indicate support for configuring local users on the device and support for using TACACSPLUS for authorization, respectively.

In addition, an authorization parameter is defined to indicate a specific authorization event, and an event can be added by defining other event identifiers. Currently, "aaa_authorization_event_command" is used to determine whether the user is allowed to run commands.

4.2. User Accounting Model

Accounting is used to record the authorization information and accouting specific information such as start and stop times and resource usage information.

This document defines two optional accouting YANG features: "local-users" and "tacacs", which the server advertises to indicate support for configuring local users on the device and support for using TACACSPLUS for accouting, respectively.

Two accouting parameters are defined to indicate specific accouting event and also the record type.

- "event type": "aaa_accounting_event_command" is defined to record commands issued by the user.

- "record": Start records indicate that a accouting service is about to begin. Stop records indicate that a service has just terminated.

5. TACACS+ Module

<CODE BEGINS> file "ietf-aaa-tacacs@2019-03-06.yang"

```
module ietf-aaa-tacacs {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-aaa-tacacs";
  prefix aaa-tcs;

  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 "draft-ietf-rtgwg-ni-model-12: YANG Model for
    Network Instances";
  }
  import ietf-system {
    prefix sys;
    reference "RFC 7317: A YANG Data Model for System Management";
  }
  import ietf-netconf-acm {
    prefix nacm;
  }

  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 2019-03-06 {
     description
       "Initial revision.";
     reference "foo";
   }

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



   grouping statistics {
     description
       "Grouping for 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 by the server";
        }
        leaf errors-received {
          type yang:counter64;
          description
            "Number of error messages received from the server";
        }
      }
    }

    grouping tacacs {
      description
        "Grouping for tacacs attributes";
      container tacacs {
        if-feature "tacacs";
        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 TACACSPLUS 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:";
        }
        leaf source-ip {
          type inet:ip-address;
          description
            "Source IP address for a TACACS+ server.";
        }
        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 network-instance {
          type leafref {
            path "/ni:network-instances/ni:network-instance/ni:name";
          }
          description
            "Configure the vpn-instance name.";
        }
        uses statistics;
      }
      container options {
        description
          "TACACS+ client options.";
        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.";
        }
      }
    }
  }

  augment "/sys:system" {
    description
      "Augment the system model with authorization and accounting
         attribuets
       Augment the system model with the tacacs model";
    uses tacacs;
```

```
    }
  }

    <CODE ENDS>
```

6. AAA Module

```
    <CODE BEGINS> file "ietf-system-aaa@2019-03-06.yang"

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


    import ietf-system {
      prefix sys;
      reference "RFC 7317: A YANG Data Model for System Management";
    }
    import ietf-netconf-acm {
      prefix nacm;
    }

    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 system AAA.

       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 2019-03-06 {
```

```
    description
      "Initial revision.";
    reference "foo";
  }

  feature authorization {
    description
      "Indicates that the device supports configuration of
       user authorization.";
  }

  feature accouting {
    description
      "Indicates that the device supports configuration of
       user accouting.";
  }

  identity authorization-method {
    description
      "Base identity for user authorization methods.";
  }

  identity accouting-method {
    description
      "Base identity for user accouting methods.";
  }

  identity tacacs {
    base sys:authentication-method;
    base authorization-method;
    base accouting-method;
    description
      "Indicates AAA operation using TACACS+.";
    reference "draft-ietf-opsawg-tacacs-11: The TACACS+ Protocol";
  }

  identity local-users {
    base sys:authentication-method;
    base authorization-method;
    base accouting-method;
    description
      "Indicates accouting of locally
       configured users.";
  }

  identity aaa_accounting_event_type {
    description
      "Base identity for specifying events types that should be
```

```
        sent to AAA server for accounting";
    }

    identity aaa_accounting_event_command {
      base aaa_accounting_event_type;
      description
        "Specifies interactive command events for AAA accounting";
    }

    identity aaa_authorization_event_type {
      description
        "Base identity for specifying activities that should be
         sent to AAA server for authorization";
    }

    identity aaa_authorization_event_command {
      base aaa_authorization_event_type;
      description
        "Specifies interactive command events for AAA authorization";
    }

    augment "/sys:system" {
      description
        "Augment the system model with authorization and accounting
           attribuets
         Augment the system model with the tacacs model";
      container authorization {
        nacm:default-deny-write;
        if-feature "authorization";
        description
          "The authorization configuration subtree.";
        leaf-list user-authorization-order {
          type identityref {
            base authorization-method;
          }
          ordered-by user;
          description
            "When the device authorize a user, it tries the authorization
             methods in this leaf-list in order.  If authorization with
             one method fails, the next method is used. If no method
             succeeds, the user is denied access.

             If the 'tacacs-authentication' feature is advertised by
             the NETCONF server, the 'tacacs' identity can be added to
             this list.
             If the 'local-users' feature is advertised by the
             NETCONF server, the 'local-users' identity can be
             added to this list.";
```

```
      }
      container events {
        description
          "The container contains an set of authorization events";
        list event {
          key "event-type";
          description
            "List of events of AAA authorization";
          leaf event-type {
            type identityref {
              base aaa_authorization_event_type;
            }
            description
              "The type of event to record at the AAA authorization
               server";
          }
        }
      }
    }
    container accouting {
      nacm:default-deny-write;
      if-feature "accouting";
      description
        "The accouting configuration subtree.";
      leaf-list user-accouting-order {
        type identityref {
          base accouting-method;
        }
        ordered-by user;
        description
          "When the device audit a user with a password,
           it tries the accouting methods in this leaf-list in
           order. The accouting method may be specified as TACACS+
           servers, or the local.";
      }
      container events {
        description
          "The container contains an set of accouting events";
        list event {
          key "event-type";
          description
            "List of events of accounting";
          leaf event-type {
            type identityref {
              base aaa_accounting_event_type;
            }
            description
              "The type of activity to record at the AAA accounting
```

```
                server";
            }
            leaf record {
              type enumeration {
                enum start_stop {
                  description
                    "Send START record to the accounting server at the
                     beginning of the activity, and STOP record at the
                     end of the activity.";
                }
                enum stop {
                  description
                    "Send STOP record to the accounting server when the
                     user activity completes";
                }
              }
              description
                "Type of record to send to the accounting server for this
                 activity type";
            }
          }
        }
      }
    }
  }
```

<CODE ENDS>

7. 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 [RFC6536] 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 accouting, 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].

8. 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:

URI: urn:ietf:params:xml:ns:yang:ietf-tacacs
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-tacacs
Namespace: urn:ietf:params:xml:ns:yang: ietf-tacacs
Prefix: tcs
Reference: RFC XXXX

9. Normative References

[I-D.ietf-opsawg-tacacs]
Dahm, T., Ota, A., dcmgash@cisco.com, d., Carrel, D., and L. Grant, "The TACACS+ Protocol", draft-ietf-opsawg-tacacs-12 (work in progress), December 2018.

[RFC1492] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, DOI 10.17487/RFC1492, July 1993, <https://www.rfc-editor.org/info/rfc1492>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6021] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6021, DOI 10.17487/RFC6021, October 2010, <https://www.rfc-editor.org/info/rfc6021>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <https://www.rfc-editor.org/info/rfc6536>.

[RFC7317] Bierman, A. and M. Bjorklund, "A YANG Data Model for System Management", RFC 7317, DOI 10.17487/RFC7317, August 2014, <https://www.rfc-editor.org/info/rfc7317>.

[RFC792] Postel, J., "Internet Control Message Protocol", RFC 792, September 1981.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

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