Yang data model for Terminal Access Controller Access Control System Plus

draft-zheng-netmod-tacacs-yang

Guangying Zheng
Zitao Wang
Bo Wu
Huawei Technologies
Why this draft

• **Motivations**
  - Existing ietf-system.yang [RFC 8344] covers basic user authentication properties on system management. But it does not cover:
    - TACACS+ authentication method which is widely used;
    - the authorization and accounting properties.
  - Vendors develop their private TACACS+ YANG, which may cause some problems:
    - Service provider may need to implement several TACACS+ YANG modules to manipulate massive devices.

• **Objective**
  - Defines a data model of Terminal Access Controller Access Control System Plus (TACACS+).
    - extract some common properties including with common configuration properties and operational state data.
Solution Overview

• Augments RFC 7317 (system management)
• The data model for configuration of the TACACS+ client has the following structure:

TACACS+ template is used to configure a set of TACACS+ server with the defined domain. Each domain defined maintains a user list in the "user@domain" format. When a TACACS+ client receives a request from a user, the TACACS+ template is selected based on the domain carried with the user.
Comments

- Thanks Alex Campbell valuable comments
  - Comments to the structure:
    - TACACS+ template
    - Separate lists for ipv4 and ipv6 servers
    - Primary/secondary server
    - Operational statistic leaves
  - Comments to server attributes
    - Server IP use ipv4-address-no-zone
    - Public net attribute
    - Ietf-network-instance attribute
Next steps

• The authors appreciate thoughts, feedback, and text on the content of the documents.
• And then prepare another version.
Thanks