Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

M. Jethanandani
Cisco Systems, Inc

March 13, 2017

Accounting in NETCONF and RESTCONF
draft-mahesh-netconf-accounting-01

Abstract

This document defines an accounting record for NETCONF and RESTCONF.

Requirements Language

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].

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 http://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 14, 2017.

Copyright Notice

Table of Contents

1. Introduction

NETCONF [RFC6241] and RESTCONF [RFC8040] protocol operations are authenticated and authorized as part of the Authentication, Authorization and Accounting (AAA) framework. An accounting record needs to be created as part of the same framework for each of these operations to satisfy the accounting part of AAA. Having an accounting record that is consistent across vendors allows for the operator to compare operations across devices from different vendors. This document defines such a record and a corresponding YANG data model (ietf-netconf-am.yang).

The rest of this document will use NETCONF to imply both NETCONF and RESTCONF, but where applicable will call out each protocol specifically.

1.1. Terminology

The following terms are defined in NETCONF [RFC6241] and are not redefined here:

- client
- server
- session
- user

2. Accounting Record

An accounting record for NETCONF consists of the following fields.

acct-code	date-time	src-ip	session-id	task-id	user	groups	path	action	rule	status

where:

acct-code: START indicates a start of a new record, NONE a continuation, and STOP the end of the record.

date-time: The date and time when the operation was performed (UTC Timezone)

src-ip: The source IP address that was used to request the operation

session-id: The session-id in case of NETCONF and would be blank in case of RESTCONF

task-id: Used to track a accounting record in case it needs to split for uploading or storing. The id is a monotonically increasing number assigned by the server.

user: The NETCONF user that requesed this operation.

groups: The group the user belongs to.

path: The path in the NACM rule on which the operations is being performed

action: The action in the NACM rule

rule: The rule in the NACM that was used to authorize the action.

status: Whether the operations was permitted or denied.

3. Data Model Definitions

3.1. Data Organization

The following diagram highlights the contents and structure of the Accounting YANG module.

```
   module: ietf-netconf-am
      +--ro nam
         +--ro accounting-record* [task-id]
            +--ro task-id       uint32
            +--ro session-id?   nc:session-id-type
            +--ro acct-code     enumeration
            +--ro date-time     yang:date-and-time
            +--ro src-ip        inet:ip-address
            +--ro group         nacm:group-name-type
            +--ro user?         nacm:user-name-type
            +--ro path          nacm:node-instance-identifier
            +--ro action        nacm:access-operations-type
            +--ro rule?         string
            +--ro status?       nacm:action-type
```

3.2. YANG Module

The following YANG module specifies the normative NETCONF content that MUST be supported by the server.

The "ietf-netconf-am" YANG module imports typedefs from YANG-TYPES [RFC6991], from NETCONF [RFC6241] and from NACM [RFC6536].

<CODE BEGINS> file "ietf-netconf-am@2017-03-13.yang"

```
module ietf-netconf-am {
    yang-version 1.1;
    namespace "urn:ietf:params:xml:ns:yang:ietf-netconf-am";
    prefix "nam";

    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-netconf {
        prefix nc;
        //reference
        //    "RFC 6241: NETCONF Protocol";
    }
```

```
    import ietf-netconf-acm {
        prefix nacm;
        //reference
        //    "RFC 6536: NACM";
    }

    organization
        "IETF NETCONF (Network Configuration) Working Group";

    contact
        "WG Web:   <http://tools.ietf.org/wg/netconf/>
         WG List:  <mailto:netconf@ietf.org>

         WG Chair: Mehmet Ersue
                   <mailto:mehmet.ersue@nsn.com>

         WG Chair: Mahesh Jethanandani
                   <mailto:mjethanandani@gmail.com>

         Editor:   Mahesh Jethanandani
                   <mailto:mjethanandani@gmail.com>";


    description
        "This module defines an accounting record for NETCONF operations
         performed on the server. If these operations are authorized
         using rules defined by NACM [RFC6536], then that information is
         also captured by this module.

         Copyright (c) 2014 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 "2017-03-13" {
         description
             "Initial version";
         reference
             "RFC XXXX: NETCONF and RESTCONF Accounting";
     }
```

```
     /*
      * Data definition statements.
      */

     container nam {
         config false;
         description
             "Parameters for NETCONF Accounting Model.";

         list accounting-record {
             key "task-id";
             description
                 "A list of accounting records generated by the server";

             leaf task-id {
                 type uint32;
                 description
                     "The task-id is a monotonically increasing number
                      assigned by the server to capture a single
                      transaction.";
             }

             leaf session-id {
                 type nc:session-id-type;
                 description
                     "If this operation happened over NETCONF, this
                      field captures the NETCONF session-id. In case
                      of RESTCONF this field can be left blank.";
             }

             leaf acct-code {
                 type enumeration {
                     enum start {
                         description
                             "Start of an accounting record";
                     }
                     enum stop {
                         description
                             "Indicates the end of an accounting
                              record";
                     }
                     enum none {
                         description
                             "Indicates a single payload or a
                              continuation of an accounting record.";
                     }
                 }
                 mandatory true;
```

```
                description
                    "Some of the AAA server place a limit on the size
                     of the payload that can be transmitted at any
                     particular time.

                     This field indicates what constitues a complete
                     accounting record by setting up the boundaries. If
                     the accounting record fits within the payload
                     boundary the field should be set to none.";
            }

            leaf date-time {
                type yang:date-and-time;
                mandatory true;
                description
                    "The date and time when the operation was
                     requested.";
            }

            leaf src-ip {
                type inet:ip-address;
                mandatory true;
                description
                    "The source IP address where the request was made
                     from.";
            }

            leaf group {
                type nacm:group-name-type;
                mandatory true;
                description
                    "The name of the group that the user who requested
                     the operation belongs to.";
            }

            leaf user {
                type nacm:user-name-type;
                description
                    "The user within the group that is requesting this
                     operation.";
            }

            leaf path {
                type nacm:node-instance-identifier;
                mandatory true;
                description
                    "Data Node Instance Identifier associated with the
                     data node that the request is being made on.
```

```
                        Instance identifiers start with the top-level
                        data node, and a complete identifier is required
                        for this value.";
                }

                leaf action {
                    type nacm:access-operations-type;
                    mandatory true;
                    description
                        "The type of NETCONF operation being requested.";
                }

                leaf rule {
                    type string {
                        length "1..max";
                    }
                    description
                        "The name assigned to the rule that was used to
                         authorize the action, if authorization was
                         enabled.";
                }

                leaf status {
                    type nacm:action-type;
                    description
                        "Action taken by the server when the above
                         mentioned rule matched, if authorization was
                         enable.";
                }
            }
        }
}
```

<CODE ENDS>

4. IANA Considerations

This document makes two requests of IANA.

The first request is to register one URI in "The IETF XML Registry". Following the format in The IETF XML Registry [RFC3688], the following needs to be registered.

URI: urn:ietf:params:xml:ns:yang:ietf-netconf-am

Registrant Contact: The IESG

XML: N/A, the requested URI is an XML namespace

The second request is to register one module in the "YANG Module Names" registry. Following the format in YANG [RFC7950], the following needs to be registered.

Name: ietf-netconf-am

Namespace: urn:ietf:params:xml:ns:yang:ietf-netconf-am

Prefix: nam

Reference: RFC XXXX

Note to RFC Editor - Please replace XXXX with the RFC id assigned to this draft.

5. Security Considerations

The YANG module defined in this memo is designed to be accessed using the NETCONF protocol. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH.

Most of the data nodes defined in this YANG module are readonly, i.e. config false, and are therefore not vulnerable in network environments. However, they might contain data that might be sensitive and should be protected with the right NACM [RFC6536] rules.

6. Acknowledgements

7. Normative References

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

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

[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, <http://www.rfc-editor.org/info/rfc6241>.

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

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <http://www.rfc-editor.org/info/rfc6991>.

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

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

Author’s Address

Mahesh Jethanandani
Cisco Systems, Inc
170 West Tasman Drive
San Jose, CA 95070
USA

Email: mjethanandani@gmail.com