Abstract

This document defines an extension to the Netconf Access Control Model (NACM) to support notification authorization per event stream.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on April 30, 2009.

Copyright Notice

Copyright (c) 2017 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 (http://trustee.ietf.org/license-info) in effect on the date of
The publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................................ 2
   1.1. Terminology ............................................ 3
2. Yang Model Extension........................................ 3
   2.1. The extended Yang Model data node .................... 3
   2.2. Outgoing <notification> Authorization ................... 4
   2.3. Tree Diagrams ........................................ 4
3. Security Considerations ...................................... 5
4. IANA Considerations ........................................ 5
5. Normative References........................................ 5

1. Introduction

RFC5277 (NETCONF Event Notifications) defines the event stream. An event stream is defined as a set of event notifications matching some forwarding criteria. At some point after the NETCONF server receives the internal event from a stream, it is converted to an appropriate XML encoding by the server, and a <notification> element is ready to send to all NETCONF sessions subscribed to that stream. In some case, same event type of notification may be part of multiple event streams.

RFC6536 (Network Configuration Protocol (NETCONF) Access Control Model) defines the NACM rule for notification, however it only allows user to define notification-name. No stream name can be defined in the NACM rule.

As NACM rule can not limit user to only subscriber certain stream, So there is no obvious solution if one user is only allowed to see some events from certain stream, like system-monitor stream and security-monitor stream. So this document is to extend NACM protocol to support such use case.
1.1. Terminology

The key words "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 BCP 14 [RFC2119].

The following terms are defined used within this document:

- NACM

The following terms are defined in [RFC6536] and are not redefined here:

- NACM

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

- Netconf
- client
- configuration data
- server
- state data

The following terms are defined in [RFC6020] and are not redefined here:

- augment
- data model
- data node
- presence container

2. Yang Model Extension

2.1. The extended Yang Model data node

A new leaf, termed as "stream-name", is specified which stream will be checked during NACM notification rule authorization.
The type of "stream-name" is an Union, it can be "matchall-string-type", or string. Type "matchall-string-type" is defined in RFC6536

leaf stream-name {
    type union {
        type matchall-string-type;
        type string;
    }

description
"This leaf matches if it has the value '*' or if its value equals the requested stream name."
}

2.2. Outgoing <notification> Authorization

For each rule-list entry found, process all rules, in order, until a rule that matches the requested access operation is found. A rule matches if all the following criteria are met:

* The rule’s "module-name" leaf is "*" or equals the name of the YANG module where the notification is defined.

* The rule’s "access-operations" leaf has the "read" bit set or has the special value "*".

* The rule does not have a "rule-type" defined or the "ruletype" is "notification" and all the following criteria are met:
    * the "notification-name" is "*" or equals the name of the notification.
    * the "stream-name" is "*" or equals the name of the stream.

2.3. Tree Diagrams

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams is as follows:

- Brackets "[" and "]" enclose list keys.

- Abbreviations before data node names: "rw" means configuration (read-write), and "ro" means state data (read-only).

- Symbols after data node names: "?" means an optional node, "!" means a presence container, and "*" denotes a list and leaf-list.
module: ietf-netconf-acm
augment /nacm:nacm/nacm:rule-list/nacm:rule/nacm:rule-type/nacm:notification
   +--rw stream-name? union

3. Security Considerations

The data model defined does not create any security implications.

4. IANA Considerations

This draft does not request any IANA action.

5. Normative References


Authors’ Addresses

Qifeng Zhang
Ericsson (China) Communications Company Ltd.
Ericsson Tower, No. 5 Lize East Street,
Chaoyang District Beijing 100102, P.R. China

Email: qifeng.zhang@ericsson.com