NETCONF Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2018

Q. Wu
X. Ding
Huawei
March 3, 2018

NETCONF Base Notifications for NMDA
draft-wu-netconf-base-notification-nmda-00

Abstract

NMDA introduces additional datastores for systems that support more advanced processing chains converting configuration to operational state. Support the monitoring of the base system events pertaining to these datastores hasn’t been discussed in Network Configuration Protocol (NETCONF) Base Notifications [RFC6470]. This document updates [RFC6470] to support the Network Management Datastore Architecture (NMDA) defined in [I-D.ietf-netmod-revised-datastores].

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 4, 2018.

Copyright Notice

Copyright (c) 2018 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 to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of...
1. Introduction

[RFC6470] provides standard mechanisms to support the monitoring of the base system events within the NETCONF server. Such mechanism allows a NETCONF client to receive notifications for some common system events (e.g., a change in NETCONF server capabilities, that may impact management applications).

This document updates Network Configuration Protocol (NETCONF) Base Notifications [RFC6470] to support the Network Management Datastore Architecture (NMDA) defined in [I-D.ietf-netmod-revised-datastores]. Specifically, with NMDA, there are several additional datastores that are subject to system events. Extensions are needed to indicate the affected datastore and affected phase (because it is no longer simply about <running>; there are now also (for example) <intended> and <operational>).

The solution presented in this document is backwards compatible with [RFC6470]. This is achieved by only adding new top-level resources, and thereby leaving the semantics of all existing resources alone.

Note that "push-change-update" notification and "push-update" notification defined in [I-D.ietf-netconf-yang-push] are not general purpose notifications. and used to send to the receivers of a subscription entire or a portion of datastore contents. The solution presented in this document can work together with "push-change-update" notification and "push-update" notification defined in [I-D.ietf-netconf-yang-push] to indicate to yang push client fine granularity of data change metadata properties (e.g. who made
configuration changes, identify specific location of configuration changes or phase of configuration changes) pertaining to multiple subscriptions of the same receivers.

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] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are defined in [I-D.ietf-netmod-revised-datastores] and are not redefined here:

- operational state datastore
- running configuration datastore
- intended configuration datastore

2. Summary of Updates to RFC 6470

This document is intended to provide an extension of notifications initially defined within [RFC6470], with the development of NMDA architecture and data model. Key relationships between these two documents include:

- the existing notifications defined in [RFC6470] are remain unchanged, no additional information is added.
- an extra event notification is defined in this document to overcome the shortcoming of [RFC6470] for supporting NMDA.

3. NETCONF Base Notifications YANG Model extension for NMDA

3.1. Overview

The YANG module in NETCONF Base Notifications [RFC6470] specifies the following 5 event notifications for the 'NETCONF' stream to notify a client application that the NETCONF server state has changed:

- netconf-config-change
- netconf-capability-change
- netconf-session-start
These event notifications used within the ‘NETCONF’ stream are accessible to clients via the subscription mechanism described in [RFC5277].

This document extends the YANG module defined in [RFC6470] to include NMDA specific extension which allows a NETCONF client to receive notifications for additional common system event as follows:

**netconf-data-change:**
Generated when the NETCONF server detects that the conventional configuration datastore or ‘config true’ objects in the operational state datastore has been changed by a management session. The notification summarizes the edits that have been detected.

The following is an example of a netconf-data-change notification message:

```xml
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2017-06-16T16:30:59.137045+09:00</eventTime>
    <changed-by>
      <username>admin</username>
      <session-id>0</session-id>
      <source-host>10.251.93.83</source-host>
    </changed-by>
    <datastore>operational</datastore>
    <edit>
      <target>/ietf-interfaces:interfaces/ietf-interfaces:statistics</target>
      <operation>create</operation>
      <origin>default</origin>
      <current-phase>inactive</current-phase>
    </edit>
    <edit>
      <operation>merge</operation>
      <origin>system</origin>
      <current-phase>in-use</current-phase>
    </edit>
  </netconf-data-change>
</notification>
```
3.2. Definitions

This section presents the YANG module defined in this document.

```yml
<CODE BEGINS> file "ietf-netconf-notifications-nmda@2018-02-01.yang"
module ietf-netconf-notifications-nmda {  
  prefix ncdn;

  import ietf-netconf {  
    prefix nc;
  }

  import ietf-datastores {  
    prefix ds;
  }

  import ietf-origin {  
    prefix or;
  }

  import ietf-netconf-notifications {  
    prefix ncn;
  }
}

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

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

  WG Chair: Kent Watsen  
  <mailto:kwatsen@juniper.net>

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

  Editor: Qin Wu  
  <mailto:bill.wu@huawei.com>

  Editor: Xiaojian Ding  
  <mailto:dingxiaojian1@huawei.com>";

description  
"This module defines a YANG data model for use with the NETCONF protocol that allows the NETCONF client to receive additional common NETCONF base event notifications related to NMDA.

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. 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 2018-02-01 {
  description
    "Initial version.";
  reference "RFC xxx: NETCONF Base Notifications for NMDA";
}

identity change-phase {
  description
    "Base identity for change phase.";
}

identity inactive {
  base change-phase;
  description
    "Identity for inactive data. It is referred to as configuration that is not currently used.";
}

identity in-use {
  base change-phase;
  description
    "Identity for the in use data. It is referred to as configuration that is actively used.";
}

identity Remnant {
  base in-use;
  description
    "Identity for the remnant configuration. It indicates that both the previous and current configuration coexist.";
}

identity miss-resource {
  base in-use;
  description
    "Identity for the missing resource. It indicates that Configuration in <intended> can refer to resources that are not available or otherwise not physically present and parts of <intended> are not applied.";
}
identity sys-resource {
  base in-use;
  description
    "Identity for the system conctrolled resource. It indicates that
     a system controlled resource has matching configuration in
     <intended>."
}

notification netconf-data-change {
  description
    "Generated when the NETCONF server detects that the
     <operational> datastore or conventional configuration datastore
     has been changed by a management session.  The notification summarizes
     the edits that have been detected.

     The server MAY choose to also generate this notification while loading
     a datastore during the boot process for the device.";
  uses ncn:changed-by-parms;
  leaf datastore {
    type identityref {
      base ds:datastore;
    }
    default "ds:operational";
    description
      "Indicates which datastore has changed or which datastore is
       target of edit-data operation."
  }
}

list edit {
  description
    "An edit record SHOULD be present for each distinct
     edit operation that the server has detected on
     the target datastore.  This list MAY be omitted
     if the detailed edit operations are not known.
     The server MAY report entries in this list for
     changes not made by a NETCONF session (e.g., CLI).";
  leaf target {
    type instance-identifier;
    description
      "Topmost node associated with the configuration change.
       A server SHOULD set this object to the node within
       the datastore that is being altered.  A server MAY
       set this object to one of the ancestors of the actual
       node that was changed, or omit this object, if the
       exact node is not known.";
  }
4. Security Considerations

The YANG module defined in this memo is designed to be accessed via the NETCONF protocol [RFC6241]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH, defined in [RFC6242].

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, get-data or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

/netconf-data-change:
Event type itself indicates that the system configuration has changed. This event could alert an attacker that specific configuration data nodes have been altered.

/netconf-data-change/changed-by:

Indicates whether the server or a specific user management session made the configuration change. Identifies the user name, session-id, and source host address associated with the configuration change, if any.

/netconf-data-change/datastore:

Indicates which datastore has been changed. This data can be used to determine if the running configuration data, the intended configuration data or the operational state datastore data has been changed.

/netconf-data-change/edit:

Identifies the specific edit operations and specific datastore subtree(s), specific source of configuration that have changed. the current stage of the datastore change(e.g., inactive, in use or remnant). This data could be used to determine if specific server vulnerabilities may now be present.

5. IANA Considerations

This document registers one XML namespace URN in the ’IETF XML registry’, following the format defined in [RFC3688]:


Registrant Contact: The IESG.

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

This document registers one module name in the ‘YANG Module Names’ registry, defined in [RFC7950]:

name: ietf-netconf-notifications-nmda

cprefix: ncdn


RFC: xxxx
6. Acknowledgements

Thanks to Juergen Schoenwaelder and Alex Clemm to review this draft and provide important input to this document.

7. Normative References

[I-D.ietf-netconf-yang-push]

[I-D.ietf-netmod-revised-datastores]


Appendix A. Appendix

A.1. Tree diagram

module: ietf-netconf-notifications

notifications:
  +---n netconf-data-change
    +---ro changed-by
      |   +---ro (server-or-user)
      |     |   +---:(server)
      |     |     |   +---ro server?   empty
      |     |     +---:(by-user)
      |     |       +---ro username   string
      |     |       +---ro session-id  nc:session-id-or-zero-type
      |     |       +---ro source-host? inet:ip-address
    +---ro datastore?  identityref
    +---ro edit*
      |   +---ro target?   instance-identifier
      |   +---ro origin?   
      |   +---ro current-phase?
      |   +---ro operation? nc:edit-operation-type

Authors’ Addresses

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu  210012
China

Email: bill.wu@huawei.com

Xiaojian Ding
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu  210012
China

Email: dingxiaojian1@huawei.com