NETCONF
Internet-Draft
Intended status: Standards Track
Expires: December 28, 2019

M. Jethanandani
VMware
K. Watsen
Watsen Networks

June 26, 2019

An HTTPS-based Transport for Configured Subscriptions
draft-mahesh-netconf-https-notif-00

Abstract

This document defines a YANG data module for configuring HTTPS based configured subscription, as defined I-D.ietf-netconf-subscribed-notifications. The use of HTTPS maximizes transport-level interoperability, while allowing for encoding selection from text, e.g. XML or JSON, to binary.

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 December 28, 2019.

Table of Contents

1. Introduction

Subscribed Notifications [I-D.ietf-netconf-subscribed-notifications] defines a YANG data module for configuring subscribed notifications. It even defines a subscriptions container that contains a list of receivers. But it defers the configuration and management of those receivers to other documents. This document defines a YANG [RFC7950] data module for configuring and managing HTTPS based receivers for the notifications. Such a configured receiver can be a third party collector, collecting events on behalf of receivers that want to co-relate events from different publishers. Configured subscriptions enable a server, acting as a publisher of notifications, to proactively push notifications to external receivers without the receivers needing to first connect to the server, as is the case with dynamic subscriptions.

This document describes how to enable the transmission of YANG modeled notifications, in the configured encoding (i.e., XML, JSON) over HTTPS. The use of HTTPS maximizes transport-level

interoperability, while the encoding selection pivots between implementation simplicity (XML, JSON) and throughput (text versus binary).

1.1. Note to RFC Editor

This document uses several placeholder values throughout the document. Please replace them as follows and remove this section before publication.

RFC XXXX, where XXXX is the number assigned to this document at the time of publication.

2019-06-26 with the actual date of the publication of this document.

1.2. Abbreviations

Acronym	Expansion
HTTP	Hyper Text Transport Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security

1.3. 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 [RFC2119] RFC8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.3.1. Subscribed Notifications

The following terms are defined in Subscribed Notifications [I-D.ietf-netconf-subscribed-notifications].

o Subscribed Notifications

2. YANG module

2.1. Overview

The YANG module is a definition of a set of receivers that are interested in the notifications published by the publisher. The module contains the TCP, TLS and HTTPS parameters that are needed to communicate with the receiver. The module augments the Subscribed Notifications [I-D.ietf-netconf-subscribed-notifications] receiver

container to create a reference to a receiver defined by the YANG module.

An abridged tree diagram representing the module is shown below.

```
module: ietf-https-notif
  +--rw receivers
     +--rw receiver* [name]
        +--rw name            string
        +--rw tcp-params
        |  +--rw remote-address    inet:host
        |  +--rw remote-port?      inet:port-number
        |  +--rw local-address?    inet:ip-address
        |  +--rw local-port?       inet:port-number
        |  +--rw keepalives!
        |         ...
        +--rw tls-params
        |  +--rw client-identity
        |  |     ...
        |  +--rw server-authentication
        |  |     ...
        |  +--rw hello-params {tls-client-hello-params-config}?
        |  |     ...
        |  +--rw keepalives! {tls-client-keepalives}?
        |         ...
        +--rw http-params
           +--rw protocol-version?   enumeration
           +--rw client-identity
           |     ...
```

```
              +--rw proxy-server! {proxy-connect}?
                    ...

     augment /sn:subscriptions/sn:subscription/sn:receivers/sn:receiver:
       +--rw receiver-ref?   -> /receivers/receiver/name
```

2.2. YANG module

The YANG module is shown below.

```
<CODE BEGINS> file "ietf-https-notif@2019-06-26.yang"
module ietf-https-notif {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-https-notif";
  prefix "hsn";

  import ietf-subscribed-notifications {
    prefix sn;
```



```
    reference
      "I-D.ietf-netconf-subscribed-notifications";
  }

  import ietf-tcp-client {
    prefix tcpc;
  }

  import ietf-tls-client {
    prefix tlsc;
  }

  import ietf-http-client {
    prefix httpc;
  }

  organization
    "IETF NETCONF Working Group";

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

```
     Authors: Mahesh Jethanandani (mjethanandani at gmail dot com)
              Kent Watsen (kent plus ietf at watsen dot net)";
  description
    "YANG module for configuring HTTPS base configuration.

     Copyright (c) 2018 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 "2019-06-26" {
    description
      "Initial Version.";
    reference
      "RFC XXXX, YANG Data Module for HTTPS Notifications.";
  }

  identity https {
```



```
    base sn:transport;
    description
      "HTTPS transport for notifications.";
  }

  container receivers {
    list receiver {
      key "name";

      leaf name {
        type string;
        description
          "";
      }
```

```
      container tcp-params {
        uses tcpc:tcp-client-grouping;
        description
          "TCP client parameters.";
      }

      container tls-params {
        uses tlsc:tls-client-grouping;
        description
          "TLS client parameters.";
      }

      container http-params {
        uses httpc:http-client-grouping;
        description
          "HTTP client parameters.";
      }
      description
        "All receivers interested in this notification.";
    }
    description
      "HTTPS based notifications.";
  }

  augment "/sn:subscriptions/sn:subscription/sn:receivers/sn:receiver" {
    leaf receiver-ref {
      type leafref {
        path "/receivers/receiver/name";
      }
      description
        "Reference to a receiver.";
    }
    description
```



```
      "Augment the subscriptions container to define the receiver.";
  }
}
<CODE ENDS>
```

3. Security Considerations

The YANG module specified in this document defines a schema for data that 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 (NACM) [RFC8341] 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. These are the subtrees and data nodes and their sensitivity/vulnerability:

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, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

Some of the RPC operations in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control access to these operations. These are the operations and their sensitivity/vulnerability:

4. IANA Considerations

This document registers one URI and one YANG module.

4.1. URI Registration

in the IETF XML registry [RFC3688] [RFC3688]. Following the format in RFC 3688, the following registration is requested to be made:

URI: urn:ietf:params:xml:ns:yang:ietf-http-notif

Registrant Contact: The IESG. XML: N/A, the requested URI is an XML

namespace.

4.2. YANG Module Name Registration

This document registers three YANG module in the YANG Module Names registry YANG [RFC6020].

```
name: ietf-https-notif
namespace: urn:ietf:params:xml:ns:yang:ietf-https-notif
prefix: hn
reference: RFC XXXX
```

5. Examples

This section tries to show some examples in how the model can be used.

5.1. HTTPS Configured Subscription

This example shows how a HTTPS client can be configured to send notifications to a receiver at address 192.0.2.1, port 443 with server certificates, and the corresponding trust store that is used to authenticate a connection.

[note: '\' line wrapping for formatting only]

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <receivers
      xmlns="urn:ietf:params:xml:ns:yang:ietf-https-notif">
      <receiver>
        <name>foo</name>
        <tcp-params>
          <remote-address>192.0.2.1</remote-address>
          <remote-port>443</remote-port>
          <local-address>192.0.3.1</local-address>
          <local-port>63001</local-port>
        </tcp-params>
        <tls-params>
          <server-authentication>
            <ca-certs>explicitly-trusted-server-ca-certs</ca-certs>
            <server-certs>explicitly-trusted-server-certs</server-ce\
rts>
          </server-authentication>
        </tls-params>
      </receiver>
  </receivers>
```

```
  <subscriptions
      xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notificatio\
ns">
    <subscription>
      <id>6666</id>
      <stream-subtree-filter>foo</stream-subtree-filter>
      <stream>some-stream</stream>
        <receivers>
          <receiver>
            <name>my-receiver</name>
            <receiver-ref
                xmlns="urn:ietf:params:xml:ns:yang:ietf-https-notif">foo</recei
-ref>
          </receiver>
        </receivers>
      </subscription>
  </subscriptions>

  <truststore xmlns="urn:ietf:params:xml:ns:yang:ietf-truststore">
    <certificates>
       <name>explicitly-trusted-server-certs</name>
       <description>
         Specific server authentication certificates for explicitly
         trusted servers.  These are needed for server certificates
         that are not signed by a pinned CA.
       </description>
       <certificate>
         <name>Fred Flintstone</name>
         <cert>base64encodedvalue==</cert>
       </certificate>
     </certificates>
     <certificates>
       <name>explicitly-trusted-server-ca-certs</name>
       <description>
         Trust anchors (i.e. CA certs) that are used to authenticate\

         server connections.  Servers are authenticated if their
         certificate has a chain of trust to one of these CA
         certificates.
       </description>
       <certificate>
         <name>ca.example.com</name>
         <cert>base64encodedvalue==</cert>
       </certificate>
     </certificates>
  </truststore>
```

```
</config>
```


6. Contributors

7. Acknowledgements

8. Normative references

[I-D.ietf-netconf-subscribed-notifications]
Voit, E., Clemm, A., Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Event Notifications", draft-ietf-netconf-subscribed-notifications-26 (work in progress), May 2019.

[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>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[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>.

[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>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[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

Mahesh Jethanandani
VMware

Email: mjethanandani@gmail.com

Kent Watsen
Watsen Networks
USA

Email: kent+ietf@watsen.net