ï»¿

Internet Engineering Task Force (IETF)
Request for Comments: 8808
Category: Standards Track
ISSN: 2070-1721

Q. Wu
Huawei
B. Lengyel
Ericsson Hungary
Y. Niu
Huawei

August 2020

A YANG Data Model for Factory Default Settings

Abstract

This document defines a YANG data model with the "factory-reset" RPC to allow clients to reset a server back to its factory default condition. It also defines an optional "factory-default" datastore to allow clients to read the factory default configuration for the device.

The YANG data model in this document conforms to the Network Management Datastore Architecture (NMDA) defined in RFC 8342.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8808.

Table of Contents

1. Introduction

This document defines a YANG data model and associated mechanism to reset a server to its factory default contents. This mechanism may be used, for example, when the existing configuration has major errors and so restarting the configuration process from scratch is the best option.

A "factory-reset" remote procedure call (RPC) is defined within the YANG data model. When resetting a device, all previous configuration settings will be lost and replaced by the factory default contents.

In addition, an optional "factory-default" read-only datastore is defined within the YANG data model. This datastore contains the data to replace the contents of implemented read-write conventional configuration datastores at reset and can also be used in the <get-data> operation.

The YANG data model in this document conforms to the Network Management Datastore Architecture defined in [RFC8342].

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 [RFC8342] and [RFC7950] and are not redefined here:

* server
* startup configuration datastore
* candidate configuration datastore
* running configuration datastore
* intended configuration datastore
* operational state datastore
* conventional configuration datastore
* datastore schema
* RPC operation

This document defines the following term:

"factory-default" datastore: A read-only configuration datastore holding a preset initial configuration that is used to initialize the configuration of a server. This datastore is referred to as "<factory-default>".

2. "Factory-Reset" RPC

This document introduces a new "factory-reset" RPC. Upon receiving the RPC:

* All supported conventional read-write configuration datastores (i.e., <running>, <startup>, and <candidate>) are reset to the contents of <factory-default>.
* Read-only datastores receive their contents from other datastores (e.g., <intended> gets its contents from <running>).
* All data in any dynamic configuration datastores MUST be discarded.

* The contents of the <operational> datastore MUST reflect the operational state of the device after applying the factory default configuration.

In addition, the "factory-reset" RPC MUST restore nonvolatile storage to factory condition. Depending on the system, this may entail deleting dynamically generated files, such as those containing keys (e.g., /etc/ssl/private), certificates (e.g., /etc/ssl), logs (e.g., /var/log), and temporary files (e.g., /tmp/*). Any other cryptographic keys that are part of the factory-installed image will be retained (such as an Initial Device Identifier (IDevID) certificate [BRSKI]). When this process includes security-sensitive data such as cryptographic keys or passwords, it is RECOMMENDED to perform the deletion in as thorough a manner as possible (e.g., overwriting the physical storage medium with zeros and/or random bits for repurposing or end-of-life (EOL) disposal) to reduce the risk of the sensitive material being recoverable. The "factory-reset" RPC MAY also be used to trigger some other resetting tasks such as restarting the node or some of the software processes.

Note that operators should be aware that since all read-write datastores are immediately reset to factory default, the device may become unreachable as a host on the network. It is important to understand how a given vendor's device will behave after the RPC is executed. Implementors SHOULD reboot the device and get it properly configured or otherwise restart processes needed to bootstrap it.

3. "Factory-Default" Datastore

Following the guidelines for defining datastores in Appendix A of [RFC8342], this document introduces a new optional datastore resource named "factory-default" that represents a preset initial configuration that can be used to initialize the configuration of a server. A device MAY implement the "factory-reset" RPC without implementing the "factory-default" datastore, which would only eliminate the ability to programmatically determine the factory default configuration.

Name: "factory-default".

YANG modules: The "factory-default" datastore schema MUST be either (1) the same as the conventional configuration datastores or (2) a subset of the datastore schema for the conventional configuration datastores.

YANG nodes: All "config true" data nodes.

Management operations: The contents of the datastore is set by the server in an implementation-dependent manner. The contents cannot be changed by management operations via the Network Configuration Protocol (NETCONF), RESTCONF, the CLI, etc., unless specialized, dedicated operations are provided. The datastore can be read using the standard NETCONF/RESTCONF protocol operations. The "factory-reset" operation copies the factory default contents to <running> and, if present, <startup> and/or <candidate>. The contents of these datastores is then propagated automatically to any other read-only datastores, e.g., <intended> and <operational>.

Origin: This document does not define a new origin identity, as it does not interact with the <operational> datastore.

Protocols: RESTCONF, NETCONF, and other management protocols.

Defining YANG module: "ietf-factory-default".

The contents of <factory-default> are defined by the device vendor and MUST persist across device restarts. If supported, the "factory-default" datastore MUST be included in the list of datastores in the YANG library [RFC8525].

4. YANG Module

This module uses the "datastore" identity [RFC8342] and the "default-deny-all" extension statement from [RFC8341].

<CODE BEGINS> file "ietf-factory-default@2020-08-31.yang"

```
module ietf-factory-default {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-factory-default";
  prefix fd;

  import ietf-datastores {
    prefix ds;
    reference
      "RFC 8342: Network Management Datastore Architecture
       (NMDA)";
  }
  import ietf-netconf-acm {
    prefix nacm;
    reference
      "RFC 8341: Network Configuration Access Control Model";
  }

  organization
    "IETF Network Modeling (netmod) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

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

     Editor:   Balazs Lengyel
               <mailto:balazs.lengyel@ericsson.com>

     Editor:   Ye Niu
               <mailto:niuye@huawei.com>";
  description
    "This module provides functionality to reset a server to its
     factory default configuration and, when supported, to
     discover the factory default configuration contents
     independently of resetting the server.

     Copyright (c) 2020 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
     (https://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC 8808; see the
     RFC itself for full legal notices.";

  revision 2020-08-31 {
    description
      "Initial revision.";
    reference
      "RFC 8808: A YANG Data Model for Factory Default Settings";
  }

  feature factory-default-datastore {
    description
      "Indicates that the factory default configuration is
       available as a datastore.";
  }

  rpc factory-reset {
```

```
        nacm:default-deny-all;
        description
          "The server resets all datastores to their factory
           default contents and any nonvolatile storage back to
           factory condition, deleting all dynamically
           generated files, including those containing keys,
           certificates, logs, and other temporary files.

           Depending on the factory default configuration, after
           being reset, the device may become unreachable on the
           network.";
      }

      identity factory-default {
        if-feature "factory-default-datastore";
        base ds:datastore;
        description
          "This read-only datastore contains the factory default
           configuration for the device that will be used to replace
           the contents of the read-write conventional configuration
           datastores during a 'factory-reset' RPC operation.";
      }
    }
<CODE ENDS>
```

5. IANA Considerations

IANA has registered the following URI in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-factory-default
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.

IANA has registered the following YANG module in the "YANG Module Names" subregistry [RFC6020] within the "YANG Parameters" registry:

Name: ietf-factory-default
Namespace: urn:ietf:params:xml:ns:yang:ietf-factory-default
Prefix: fd
Reference: 8808

6. 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 Network Configuration 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.

Access to the "factory-reset" RPC operation and factory default values of all configuration data nodes within the "factory-default" datastore is considered sensitive and therefore has been restricted by using the "default-deny-all" access control statement defined in [RFC8341].

The "factory-reset" RPC can prevent any further management of the device when the server is reset back to its factory default condition, e.g., the session and client configurations are included in the factory default contents or treated as dynamic files in nonvolatile storage and overwritten by the "factory-reset" RPC.

The operational disruption caused by setting the configuration to factory default contents or the lack of appropriate security control

on the factory default configuration varies greatly, depending on the implementation and current configuration.

The nonvolatile storage is expected to be wiped clean and reset back to the factory default state, but there is no guarantee that the data is wiped clean according to any particular data-cleansing standard, and the owner of the device MUST NOT rely on any sensitive data (e.g., private keys) being forensically unrecoverable from the device's nonvolatile storage after a "factory-reset" RPC has been invoked.

7. References

7.1. 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, <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>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[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>.

[RFC8525] Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K., and R. Wilton, "YANG Library", RFC 8525, DOI 10.17487/RFC8525, March 2019, <https://www.rfc-editor.org/info/rfc8525>.

7.2. Informative References

[BRSKI] Pritikin, M., Richardson, M. C., Eckert, T., Behringer, M. H., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-bootstrapping-keyinfra-43, 7 August 2020, <https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-43>.

Acknowledgements

Thanks to Juergen Schoenwaelder, Ladislav Lhotka, Alex Campbell, Joe Clarke, Robert Wilton, Kent Watsen, Joel Jaeggli, Lou Berger, Andy Bierman, Susan Hares, Benjamin Kaduk, Stephen Kent, Stewart Bryant, Ã\211ric Vyncke, Murray Kucherawy, Roman Danyliw, Tony Przygienda, and John Heasley for reviewing, and providing important input to, this document.

Contributors

Rohit R Ranade
Huawei

Email: rohitrranade@huawei.com

Authors' Addresses

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

Email: bill.wu@huawei.com

Balazs Lengyel
Ericsson Hungary
Budapest
Magyar Tudosok korutja 11
1117
Hungary

Phone: +36-70-330-7909
Email: balazs.lengyel@ericsson.com

Ye Niu
Huawei

Email: niuye@huawei.com