Factory Default Setting
draft-ietf-netmod-factory-default-09

Abstract

This document defines a method to reset a server to its factory-default content. The reset operation may be used, e.g., when the existing configuration has major errors so re-starting the configuration process from scratch is the best option.

A new factory-reset RPC is defined. When resetting a datastore, all previous configuration settings will be lost and replaced by the factory-default content.

A new optional "factory-default" read-only datastore is defined, that contains the data that will be copied over to the running datastore at reset.

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 June 8, 2020.
1. Introduction

This document defines a method to reset a server to its factory-default content. The reset operation may be used, e.g., when the existing configuration has major errors so re-starting the configuration process from scratch is the best option.

A factory-reset RPC is defined. When resetting a datastore, all previous configuration settings will be lost and replaced by the factory-default content.

A "factory-default" read-only datastore is defined, that contains the data to replace the contents of implemented read-write conventional configuration datastores at reset. This datastore can also be used in <get-data> operation.
NETCONF defines the <delete-config> RPC operation, but that only acts on the <startup-datastore>, whereas the <factory-reset> RPC operation can perform additional changes to the device to fully reset the device back to a factory-default state.

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] [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
- RPC operation

The following terms are defined in this document as follows:

- factory-default datastore: A read-only configuration datastore holding a preconfigured minimal initial configuration that can be used to initialize the configuration of a server. The content of the datastore is usually static, but MAY depend on external factors like available HW.

2. Factory-Reset RPC

A new "factory-reset" RPC is introduced. Upon receiving the RPC
All supported conventional read-write configuration datastores (i.e. <running>, <startup>, and <candidate>) are all reset to the contents of <factory-default>.

Read-only datastores receive their content from other datastores (e.g. <intended> getts its content from <running>).

All data in any ephemeral datastores MUST be discarded.

The contents of the <operational> datastore MUST be reset back to an appropriate factory-default state.

In addition, the "factory-reset" RPC MUST restore storage to factory condition, including remove log files, remove temporary files (from datastore or elsewhere). It MUST also remove security credentials and restoring default security settings including remove certificates, keys, zero passwords, etc. The process invoked by the "factory-reset" RPC SHOULD zero/pattern-write than remove sensitive files such as the TLS keys, configuration stores, etc. 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 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 or otherwise restart processes needed to bootstrap it.

### 3. Factory-Default Datastore

Following guidelines for defining Datastores in the appendix A of [RFC8342], this document introduces a new optional datastore resource named ‘factory-default’ that represents a preconfigured minimal initial configuration that can be used to initialize the configuration of a server. A device MAY only implement the <factory-reset> RPC without implementing the 'factory-default' datastore, which make it lose the ability to see what configuration the device would be reset back to.

- **Name**: "factory-default"
- **YANG modules**: all
- **YANG nodes**: all "config true" data nodes
- **Management operations**: The content of the datastore is set by the server in an implementation dependent manner. The content can not
be changed by management operations via 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 content to `<running>` and, if present, `<startup>` and then the content of these datastores is 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 `<operational>` datastore.
- **Protocols:** RESTCONF, NETCONF and other management protocol.
- **Defining YANG module:** "ietf-factory-default".

The datastore content is usually defined by the device vendor. It is usually static, but MAY change e.g., depending on external factors like HW available or during device upgrade.

The contents of `<factory-default>` MUST persist across device restarts.

### 4. YANG Module

This module imports typedefs from [RFC8342], and it references [RFC6421],[RFC8341].

```yml
<CODE BEGINS> file "ietf-factory-default@2019-11-27.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;
  }

  import ietf-netconf-acm {
    prefix nacm;
  }

  organization 
    "IETF NETMOD (Network Modeling) Working Group";
  contact
    "WG Web:  <https://tools.ietf.org/wg/netconf/>
    WG List:  <mailto:netconf@ietf.org>
    Editor:   Qin Wu
    <mailto:bill.wu@huawei.com>
```

This module defines the
  - factory-reset RPC
  - factory-default datastore

It provides functionality to reset a server to its
factory-default content.

Copyright (c) 2019 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 2019-11-27 {
  description
    "Initial revision."
  reference
    "RFC XXXX: Factory default Setting"
}

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 the content of all read-write
     configuration datastores (i.e.,<running>,<startup>,and
     <candidate>) to their factory default content."
}

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

5. IANA Considerations

This document registers one URI in the IETF XML Registry [RFC3688].
The following registration has been made:


Registrant Contact: The IESG.

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

This document registers one YANG module in the YANG Module Names Registry [RFC6020]. The following registration has been made:

name: ietf-factory-default


prefix: fd

RFC: xxxx

6. Security Considerations

The YANG module defined in this document extends the base operations for NETCONF [RFC6241] and 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 <factory-reset> RPC operation may be considered sensitive in some network environments, e.g., remote access to reset the device or
overwrite security sensitive information in one of the other
datastores, e.g. running, therefore it is important to restrict
access to this RPC using the standard access control methods.
[RFC8341]

The ‘factory-reset’ RPC can prevent any further management of the
device if the session and client config is included in the factory-
reset contents.

The operational disruption caused by setting the config to factory-
reset contents varies greatly depending on the implementation and
current config.

7. Acknowledgements

Thanks to Juergen Schoenwaelder, Ladislav Lhotka, Alex Campbell, Joe
Clarke, Robert Wilton, Kent Watsen, Joel Jaeggli, Lou Berger, Andy
Bierman, Susan Hares to review this draft and provide important input
to this document.

8. Contributors

Rohit R Ranade
Huawei
Email: rohitrranade@huawei.com

9. References

9.1. 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,

RFC 7950, DOI 10.17487/RFC7950, August 2016,

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,

Access Control Model", STD 91, RFC 8341,
DOI 10.17487/RFC8341, March 2018,
9.2. Informative References

[I-D.ietf-netmod-yang-instance-file-format]

Appendix A. Changes between revisions

Editorial Note (To be removed by RFC Editor)

v08 - 09
- Provide some guideline for operators and implementor who implement factory default method.

v07 - 08
- Provide clarification and recommendation on the relationship between factory-reset RPC and reboot.
- Nits fixed based on YANG Doctor Review.

v06 - 07
- Remove Factory-default content specification;
- Remove reference to YANG instance data file format and zero touch provision [RFC8573];
- Remove copy-config operation extension on factory-default datastore

v05 - 06
- Additional text to enhance security section.
- Add nacm:default-deny-all on "factory-reset" RPC.
- A few clarification on Factory-default content specification.

v03 - 04
o Additional text to clarify factory-reset RPC usage.

v02 - 03

o Update security consideration section.

v01 - v02

o Address security issue in the security consideration section.

o Remove an extension to the NETCONF <copy-config> operation which allows it to operate on the factory-default datastore.

o Add an extension to the NETCONF <get-config> operation which allows it to operate on the factory-default datastore.

v00 - v01

o Change YANG server into server defined in NMDA architecture based on discussion.

o Allow reset the content of all read-write configuration datastores to its factory-default content except <candidate>.

o Add clarification text on factory-reset protocol operation behavior.

v03 - v00

o Change draft name from draft-wu to draft-ietf-netmod-factory-default-00 without content changes.

v02 - v03

o Change reset-datastore RPC into factory-reset RPC to allow reset the whole device with factory default content.

o Remove target datastore parameter from factory-reset RPC.

o Other editorial changes.

v01 - v02

o Add copy-config based on Rob’s comment.

o Reference Update.

v03 - v00 - v01
- Changed name from draft-wu-netconf-restconf-factory-restore to draft-wu-netmod-factory-default
- Removed copy-config; reset-datastore is enough
- v02 - v03
- Restructured
- Made new datastore optional
- Removed Netconf capability
- Listed Open issues
- v01 - v02
- -
- v00 - v01
- -

Authors’ Addresses

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

Email: bill.wu@huawei.com

Balazs Lengyel
Ericsson Hungary
Magyar Tudosok korutja 11
1117 Budapest
Hungary

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

Ye Niu
Huawei

Email: niuye@huawei.com