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

Модель данных YANG для заводских установок

Аннотация

Этот документ задаёт модель данных YANG для вызова RPC factory-reset, позволяющего клиентам сбросить сервер к заводским настройкам, заданным по умолчанию. Модуль также определяет необязательное хранилище factory-default, позволяющее клиентам считывать с устройства принятые по умолчанию заводские настройки.

Модель данных YANG в этом документе соответствует архитектуре хранилищ данных управления сетью (Network Management Datastore Architecture или NMDA), определённой в RFC 8342.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8808.

Оглавление

1. Введение

Этот документ задаёт модель данных YANG и связанный с ней механизм для сброса сервера к заводским настройкам. Этот механизм может применяться, например, при наличии в имеющейся конфигурации серьёзных ошибок, когда лучшим решением является «настройка с нуля» (factory default).

Вызов удалённой процедуры (remote procedure call или RPC) factory-reset определён в модели данных YANG. При сбросе устройства все предыдущие настройки теряются с заменой установленными на заводе параметрами.

Кроме того, в модули YANG определено необязательное хранилище factory-default с доступом лишь для чтения. Это хранилище содержит данные для замены содержимого доступных для чтения и записи традиционных хранилищ конфигурации при сбросе устройства и может использоваться также в операции <get-data>.

Модель данных YANG в этом документе соответствует архитектуре NMDA, определённой в RFC 8342.

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1.1. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

Перечисленные ниже термины определены в [RFC8342], [RFC7950] и не переопределяются здесь.

- server - сервер;
- startup configuration datastore - хранилище стартовой конфигурации;
- candidate configuration datastore - хранилище будущей конфигурации, хранилище-кандидат;
- running configuration datastore - хранилище рабочей конфигурации;
- intended configuration datastore - хранилище предполагаемой конфигурации;
- operational state datastore - хранилище рабочего состояния;
- conventional configuration datastore - традиционное (обычное) хранилище данных конфигурации;
- datastore schema - схема хранилища данных;
- RPC operation — операция RPC.

Этот документ определяет один термин.

factory-default datastore - хранилище заводский настроек
: Доступное лишь для чтения хранилище данных конфигурации, используемое для инициализации настройки сервера. Это хранилище называют также <factory-default>.

2. RPC factory-reset

Этот документ добавляет RPC factory-reset. При получении такого вызова выполняются указанные ниже действия.

- Все поддерживаемые традиционные хранилища конфигурации с доступом для чтения и записи (т. е., <running>, <startup>, <candidate>) сбрасываются в состояние хранилища <factory-default>.
- Доступные лишь для чтения хранилища получают своё содержимое из других хранилищ (например, <intended> берет содержимое <running>).
- Все данных в любых хранилищах динамической конфигурации **должны** отбрасываться.
- Содержимое хранилища <operational> **должно** отражать рабочее состояние устройства после применения заводских настроек.

В дополнение к этому вызов RPC factory-reset **должен** возвращать энергонезависимое хранилище в исходное (заводское) состояние. В зависимости от системы это может повлечь удаление созданных динамически файлов, таких как файлы с ключами (например, /etc/ssl/private), сертификатами (например, /etc/ssl), системными журналами (например, /var/log) и временные файлы (например, /tmp/*). Все криптографические ключи, относящиеся к заводским настройкам, такие как исходный сертификат идентификатор устройства (Initial Device Identifier или IDevID [BRSKI]) будут сохранены. Если этот процесс включает чувствительные к безопасности данные, такие как криптографические ключи или пароли, **рекомендуется** удалять их как можно тщательней (например, перезаписывая физический носитель нулями и/или случайными битами для перепрофилируемых или выводимых из эксплуатации носителей) для снижения риска утечки конфиденциальных сведений. Вызов RPC factory-reset **можно** также применять для запуска некоторых других задач сброса, таких как перезапуск устройства или некоторых программных процессов.

Отметим, что операторам следует учитывать возможность недоступности устройства через сеть в результате сброса всех доступных для чтения и записи хранилищ к заданным на заводе настройкам. Важно понимать, как будет вести себя устройство данного производителя после выполнения RPC. Оператору **следует** перезагрузить устройство и настроить его должным образом или запустить процесс начальной настройки (bootstrap).

3. Хранилище данных factory-default

Следуя руководствам по определению хранилищ данных из Приложения A к [RFC8342], этот документ вводит необязательное хранилище factory-default, представляющее исходную конфигурацию, которая позволяет инициализировать сервер. Устройство **может** реализовать RPC factory-reset без реализации хранилища factory-default, что будет лишь препятствовать возможности программными средствами определить заводскую конфигурацию.

Имя
: factory-default.

Модули YANG
: Схема хранилища данных factory-default **должна** (1) совпадать со схемой традиционных хранилищ конфигурации или (2) быть частью такой схемы.

Узлы YANG
: Все узлы данных config true.

Операции управления
: Содержимое хранилища устанавливается сервером в зависимости от реализации и не может быть изменено через протокол управления сетью (Network Configuration Protocol или NETCONF), RESTCONF, интерфейс CLI и т. п. без использования специализированных операций. Хранилище можно читать с использованием стандартных операций протоколов NETCONF и RESTCONF. Операция factory-reset копирует содержимое заданного на заводе хранилища в хранилище <running>, а также (при наличии) в <startup> и <candidate>. Содержимое обновлённых хранилищ автоматически распространяется в доступные лишь для чтения хранилища, такие как <intended> и <operational>.

Источник
: Этот документ не задаёт новый идентификатор источника, поскольку он не связан с хранилищем <operational>.

Протоколы
: RESTCONF, NETCONF и другие протоколы управления.

Модуль YANG сопределением
: ietf-factory-default.

Содержимое <factory-default> определяет производитель устройства и оно **должно** сохраняться при перезапуске. Если поддерживается хранилище factory-default, оно **должно** включаться в список хранилищ библиотеки YANG [RFC8525].

4. Модуль YANG

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
       "Этот модуль обеспечивает функцию сброса устройства к заданным
        на заводе настройкам и (при поддержке) раскрытия содержимого
        принятой по умолчанию заводской конфигурации независимо от
        сброса сервера.

        Авторские права (Copyright (c) 2020) принадлежат IETF Trust
        и лицам, указанным в качестве авторов кода. Все права защищены.

        Распространение и использование в исходной или двоичной форме с
        изменениями или без таковых разрешено в соответствии с лицензией
        Simplified BSD, изложенной в разделе 4  IETF Trust's Legal
        Provisions применительно к документам IETF
        (http://trustee.ietf.org/license-info).

        Эта версия данного модуля YANG является частью RFC 8808, где
        правовые вопросы рассмотрены более полно.";

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

     feature factory-default-datastore {
       description
         "Указывает доступность хранилища заводских настроек.";
     }

     rpc factory-reset {
       nacm:default-deny-all;
       description
         "Сервер сбрасывает все хранилища и энергонезависимую память
          к заданным на заводе настройкам, удаляя все динамически
          созданные файлы, в том числе файлы с ключами, сертификатами
          и системными журналами (log), а также временные файлы.

          В зависимости от заданной на заводе конфигурации устройство
          после сброса может стать недоступным из сети.";
     }

     identity factory-default {
       if-feature "factory-default-datastore";
       base ds:datastore;
       description
         "Доступная лишь для чтения заводская конфигурация
```

```
            устройства, используемая для замены содержимого доступных
            для чтения и записи традиционных хранилищ данных
            конфигурации с помощью RPC factory-reset.";
        }
      }
    <CODE ENDS>
```

5. Взаимодействие с IANA

Агентство IANA зарегистрировало URI в субреестре ns реестра 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.
```

Агентство IANA зарегистрировало модуль YANG в субреестре YANG Module Names [RFC6020] реестра YANG Parameters.

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

6. Вопросы безопасности

Заданные в этом документе модули YANG определяют схемы для данных, которые разработаны для доступа через протоколы управления сетью, такие как NETCONF [RFC6241] и RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый транспорт с обязательной реализацией Secure Shell (SSH) [RFC6242]. Нижним уровнем RESTCONF служит HTTPS с обязательной реализацией защищённого транспорта TLS [RFC8446].

Модель управления доступом NETCONF [RFC8341] обеспечивает средства, позволяющие предоставить доступ лишь конкретным пользователям NETCONF и RESTCONF к предопределённому подмножеству доступных в NETCONF или RESTCONF протокольных операций и содержимого.

Доступ к операции RPC factory-reset и заводским значениям всех узлов данных конфигурации в хранилище factory-default считается чувствительным и поэтому его следует ограничивать с использованием оператора контроля доступа default-deny-all, определённого в [RFC8341].

RPC factory-reset может препятствовать управлению настройками устройства при сбросе сервера к заводским установкам. Например, конфигурация сессий и клиентов, включённая в принятые по умолчанию настройки или обрабатываемая как динамические файлы в энергонезависимой памяти, будет перезаписана RPC factory-reset.

Нарушение работы, вызванное сбросом в заводскую конфигурацию или отсутствием надлежащего контроля безопасности в заводской конфигурации, сильно зависит от реализации и текущей конфигурации.

Предполагается, что энергонезависимое хранилище будет очищено и возвращено в заводское состояние, но нет гарантии очистки данные в соответствии с каким-либо стандартом очистки и владельцу устройства **недопустимо** полагаться на надёжное удаление конфиденциальных сведений (например, секретных ключей) из энергонезависимой памяти после вызова RPC factory-reset.

7. Литература

7.1. Нормативные документы

[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. Дополнительная литература

[BRSKI] Pritikin, M., Richardson, M. C., Eckert, T., Behringer, M. H., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", Work in Progress[1], Internet-Draft, draft-ietf-anima-bootstrapping-keyinfra-43, 7 August 2020, <https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-43>.

Благодарности

Спасибо 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, Éric Vyncke, Murray Kucherawy, Roman Danyliw, Tony Przygienda, John Heasley за рецензии и существенный вклад в этот документ.

Участник работы

Rohit R Ranade
Huawei
Email: rohitrranade@huawei.com

Адреса авторов

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 8995. *Прим. перев.*