

Internet Engineering Task Force (IETF)
Request for Comments: 7895
Category: Standards Track
ISSN: 2070-1721

A. Bierman
YumaWorks
M. Bjorklund
Tail-f Systems
K. Watsen
Juniper Networks
June 2016

Библиотека модуля YANG

YANG Module Library

Тезисы

Этот документ описывает библиотеку YANG, которая обеспечивает информацию обо всех модулях YANG, используемых сервером управления сетью (например, NETCONF¹). Обеспечиваемые простые механизмы кэширования позволяют клиентам минимизировать усилия при поиске информации.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF² и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG³. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc7895>.

Авторские права

Авторские права (Copyright (c) 2017) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

Этот документ является субъектом прав и ограничений, перечисленных в BCP 78 и IETF Trust Legal Provisions и относящихся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно, поскольку в них описаны права и ограничения, относящиеся к данному документу. Фрагменты программного кода, включенные в этот документ, распространяются в соответствии с упрощенной лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение.....	1
1.1. Термины.....	2
1.2. Диаграммы деревьев.....	2
2. Библиотека модуля YANG.....	2
2.1. Контейнер modules-state.....	2
2.1.1. Лист modules-state/module-set-id.....	3
2.1.2. Лист modules-state/module.....	3
2.2. Модуль библиотеки YANG.....	3
3. Взаимодействие с IANA.....	6
3.1. Реестр модулей YANG.....	6
4. Вопросы безопасности.....	6
5. Литература.....	7
5.1. Нормативные документы.....	7
5.2. Дополнительная литература.....	7
Благодарности.....	7
Адреса авторов.....	7

1. Введение

Нужны стандартные механизмы для идентификации модулей и submodule YANG, используемых сервером, который реализует модели данных YANG. При использовании на сервер большого числа модулей YANG содержимое библиотеки YANG может оказаться достаточно большим. Эта информация изменяется не часто, поэтому для клиентов важно обеспечить возможность кэшировать содержимое библиотеки YANG и легко идентифицировать устаревшие компоненты кэша.

Информация библиотеки YANG может быть разной на каждом сервере и может меняться в процессе работы или после перезагрузки сервера.

¹Network Configuration Protocol - протокол настройки сети.

²Internet Engineering Task Force.

³Internet Engineering Steering Group.

Если сервер реализует множество протоколов доступа к определенным в YANG данным, каждый из этих протоколов должен иметь свой концептуальный экземпляр библиотеки YANG.

Ниже перечислена информация, требуемая клиентским приложениям (для каждого модуля YANG в библиотеке) для полного использования языка моделирования данных YANG.

- Name - имя модуля YANG.
- Revision - каждый модуль и submodule YANG в библиотеке имеет номер выпуска, который определяется оператором revision в модуле или submodule. Если такого оператора revision нет, строка выпуска для модуля или submodule будет пустой (размер 0).
- Submodule list - **должны** быть указаны имя и выпуск каждого submodule.
- Feature list - **должны** быть указаны все возможности YANG, поддерживаемые сервером.
- Deviation list - **должны** быть указаны имена каждого модуля YANG, приведенного в операторах deviation.

1.1. Термины

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14 [RFC2119].

Приведенные ниже термины определены в [RFC6241]:

- client - клиент;
- server - сервер.

Приведенные ниже термины определены в [YANG1.1]:

- module - модуль;
- submodule - submodule.

Этот документ определяет один термин.

YANG library – библиотека YANG

Набор модулей и submodule YANG, используемых сервером.

1.2. Диаграммы деревьев

В этом документе применяется упрощенное графическое представление модели данных. Значение символов на диаграммах описано ниже.

- Квадратные скобки [и] служат для указания ключей списка.
- Сокращение rw используется для конфигурационных данных (read-write - чтение и запись), а ro - для данных состояния (read-only - только чтение).
- Символ ? после имени узла указывает необязательный узел, ! Означает контейнер присутствия, а * - list и leaf-list.
- В скобках указываются узлы choice и case, а узлы case дополнительно помечаются двоеточием (:).
- Три точки (...) служат для обозначения содержимого subtree, которое не показано.

2. Библиотека модуля YANG

Модуль ietf-yang-library предоставляет информацию о библиотеке YANG, используемой сервером. Этот модуль определен с использованием YANG версии 1, но поддерживает описания модулей YANG, написанные в любой версии YANG.

Ниже приведена диаграмма дерева YANG для модуля ietf-yang-library.

```
+--ro modules-state
  +--ro module-set-id      string
  +--ro module* [name revision]
    +--ro name              yang:yang-identifier
    +--ro revision          union
    +--ro schema?           inet:uri
    +--ro namespace         inet:uri
    +--ro feature*          yang:yang-identifier
    +--ro deviation* [name revision]
      | +--ro name          yang:yang-identifier
      | +--ro revision      union
    +--ro conformance-type  enumeration
    +--ro submodule* [name revision]
      +--ro name            yang:yang-identifier
      +--ro revision        union
      +--ro schema?         inet:uri
```

2.1. Контейнер modules-state

В этом обязательном контейнере содержатся идентификаторы модулей модели данных YANG, поддерживаемых сервером.

2.1.1. *Lucm modules-state/module-set-id*

Этот обязательный лист содержит уникальный идентификатор, который связан с конкретной реализацией и представляет текущий набор модулей и submodule на конкретном сервере. Значение этого листа **должно** меняться при изменении набора модулей и submodule в библиотеке YANG. Не требуется совпадения значений module-set-id во всех случаях для одного и того же набора.

Этот лист позволяет клиенту считать набор модулей, кэшировать его и обновлять лишь при смене значения листа.

Если значение этого листа меняется, сервер также генерирует уведомление yang-library-change с новым значением module-set-id.

Отметим, что для сервера NETCONF, реализующего YANG 1.1 [YANG1.1], смена значения module-set-id будет приводить к новому значению для возможности :yang-library, определенной в [YANG1.1]. Таким образом, если такой сервер реализует уведомления NETCONF [RFC5277] и генерирует уведомление netconf-capability-change [RFC6470], это уведомление будет создаваться при каждом изменении module-set-id.

2.1.2. *Lucm modules-state/module*

Этот обязательный лист содержит одну запись для каждого модуля модели данных YANG, поддерживаемого сервером. В этом списке **должна** присутствовать запись для каждого выпуска каждого модуля YANG, который используется сервером. Может импортироваться несколько выпусков одного модуля в дополнение к записи для выпуска, реализованного сервером.

2.2. Модуль библиотеки YANG

Модуль ietf-yang-library определяет информацию мониторинга для модулей YANG, используемых сервером.

Модули ietf-yang-types и ietf-inet-types из [RFC6991] используются этим модулем для некоторых определений типов.

```
<CODE BEGINS> file "ietf-yang-library@2016-06-21.yang"

module ietf-yang-library {
  namespace "urn:ietf:params:xml:ns:yang:ietf-yang-library";
  prefix "yanglib";

  import ietf-yang-types {
    prefix yang;
  }
  import ietf-inet-types {
    prefix inet;
  }

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

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

    WG Chair: Mehmet Ersue
              <mailto:mehmet.ersue@nsn.com>

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

    Editor: Andy Bierman
            <mailto:andy@yumaworks.com>

    Editor: Martin Bjorklund
            <mailto:mbj@tail-f.com>

    Editor: Kent Watsen
            <mailto:kwatsen@juniper.net>";

  description
    "Этот модуль содержит информацию мониторинга для модулей и
    submodule YANG, используемых в сервере на базе YANG.

    Авторские права (Copyright (c) 2016) 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 7895, где
    правовые вопросы рассмотрены более полно.";
```

```
revision 2016-06-21 {
  description
    "Первоначальный выпуск.";
  reference
    "RFC 7895: YANG Module Library.";
}

/*
 * Определения типов
 */

typedef revision-identifier {
  type string {
    pattern '\d{4}-\d{2}-\d{2}';
  }
  description
    "Представляет конкретную дату в формате ГГГГ-ММ-ЧЧ.";
}

/*
 * Группировки
 */

grouping module-list {
  description
    "Структура данных модуля представлена в виде группировки и
    может использоваться многократно в конфигурационных или
    иных структурах данных мониторинга.";

  grouping common-leafs {
    description
      "Общие параметры модулей и submodule YANG.";

    leaf name {
      type yang:yang-identifier;
      description
        "Имя модуля или submodule YANG.";
    }
    leaf revision {
      type union {
        type revision-identifier;
        type string { length 0; }
      }
      description
        "Дата выпуска модуля или submodule YANG. Если в модуле
        или submodule YANG нет оператора revision, используется
        пустая строка.";
    }
  }
}

grouping schema-leaf {
  description
    "Общий параметр листа schema для модулей и submodule.";

  leaf schema {
    type inet:uri;
    description
      "Содержит URL, представляющий ресурс со схемой YANG для
      этого модуля или submodule.

      Этот лист будет присутствовать лишь при наличии URL
      доступного для извлечения схемы для данной записи.";
  }
}

list module {
  key "name revision";
  description
    "Каждая запись представляет один выпуск одного модуля,
    поддерживаемого в данный момент сервером.";

  uses common-leafs;
  uses schema-leaf;

  leaf namespace {
```

```

    type inet:uri;
    mandatory true;
    description
        "Идентификатор пространства имен XML для этого модуля.";
}
leaf-list feature {
    type yang:yang-identifier;
    description
        "Список имен свойств YANG из данного модуля, которые
        поддерживаются сервером, независимо от их определения
        в модуле или любом из включенных submodule.";
}
list deviation {
    key "name revision";
    description
        "Список имен отклонений модулей YANG и выпусков,
        используемых этим сервером для изменения соответствия
        модуля, связанного с этой записью. Отметим, что один
        и тот же модуль может использоваться для указания
        отклонений множества модулей, поэтому запись МОЖЕТ
        появляться во множестве записей module.

        Модуль отклонений ДОЛЖЕН присутствовать в списке
        module с тем же именем и выпуском. Значением
        conformance-type для модуля deviation будет implement.";
    uses common-leafs;
}
leaf conformance-type {
    type enumeration {
        enum implement {
            description
                "Показывает, что сервер реализует один или множество
                доступных протоколу объектов, определенных в модуле
                YANG, указанном этой записью. Это включает операторы
                deviation, определенные в модуле.

                Для модулей YANG версии 1.1 имеется не более одной
                записи с типом соответствия implement для конкретного
                имени модуля, поскольку YANG 1.1 требует реализации
                не более одного выпуска модуля.

                Для модулей YANG версии 1 НЕ СЛЕДУЕТ включать более
                одной записи module для конкретного имени модуля.";
        }
        enum import {
            description
                "Показывает, что сервер импортирует повторно используемые
                определения из указанного выпуска модуля, но не реализует
                каких-либо доступных протоколу объектов из этого выпуска.

                МОЖЕТ существовать множество записей module для одного
                имени модуля. Это может возникать в случаях импорта одного
                модуля множеством других модулей с разными датами выпуска
                в операторах import.";
        }
    }
    mandatory true;
    description
        "Указывает тип соответствия, заявленного сервером для модуля
        YANG, указанного этой записью.";
}
list submodule {
    key "name revision";
    description
        "Каждая запись представляет 1 submodule в родительском модуле.";
    uses common-leafs;
    uses schema-leaf;
}
}
}
/*
 * Узлы данных рабочего состояния
 */
container modules-state {

```

```

config false;
description
  "Содержит информацию мониторинга модуля YANG.";

leaf module-set-id {
  type string;
  mandatory true;
  description
    "Содержит специфический для сервера идентификатор, который
    представляет текущий набор модулей и submodule. Сервер
    ДОЛЖЕН менять значение этого листа при изменении данных,
    представленных экземплярами списков module.";
}

uses module-list;
}

/*
 * Уведомления
 */

notification yang-library-change {
  description
    "Генерируется при изменении набора модулей и submodule,
    поддерживаемых сервером.";
  leaf module-set-id {
    type leafref {
      path "/yanglib:modules-state/yanglib:module-set-id";
    }
    mandatory true;
    description
      "Содержит значение module-set-id, которое представляет
      набор модулей и submodule, которые сервер поддерживал в
      момент генерации уведомления.";
  }
}
}

}

<CODE ENDS>

```

3. Взаимодействие с IANA

3.1. Реестр модулей YANG

Этот документ регистрирует один идентификатор URI в реестре IETF XML Registry [RFC3688]. В соответствии с форматом RFC 3688, регистрация имеет вид

```

URI: urn:ietf:params:xml:ns:yang:ietf-yang-library
Registrant Contact: The NETCONF WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

```

Этот документ регистрирует также один модуль YANG в реестре YANG Module Names [RFC6020].

```

name:          ietf-yang-library
namespace:    urn:ietf:params:xml:ns:yang:ietf-yang-library
prefix:       yanglib
reference:    RFC 7895

```

4. Вопросы безопасности

Определенный здесь модуль YANG предназначен для доступа по протоколу NETCONF [RFC6241]. Нижним уровнем NETCONF является защищенный транспортный уровень и обязательным для реализации является транспорт SSH [RFC6242]. Модель управления доступом NETCONF [RFC6536] обеспечивает пути предоставления доступа лишь определенному набору пользователей NETCONF к заранее заданному подмножеству всех операций и содержимого протокола NETCONF.

Некоторые из доступных для чтения узлов данных этого модуля YANG могут оказаться чувствительными или уязвимыми в отдельных сетевых средах. Поэтому важно ограничить возможность чтения (например, с помощью get, get-config или notification) таких данных. Ниже указаны деликатные/уязвимые поддеревья и узлы данных.

/modules-state/module. Список модулей, используемых реализацией сервера, может помочь атакующему при определении возможностей сервера и известных ошибок реализации. Хотя часть такой информации доступна всем пользователям через сообщения NETCONF <hello> (или похожие сообщения других протоколов управления), этот модуль YANG может раскрывать дополнительные детали, способные помочь атакующему. Уязвимости сервера могут относиться к конкретным модулям, версиям возможностям или отклонениям. Эта информация включается в каждую запись module. Например, если конкретная операция с определенным узлом данных может приводить к аварии на сервере или значительно снижать его производительность, информация из списка модулей будет помогать атакующему обнаружить серверы с таким дефектом для организации атаки на службы.

5. Литература

5.1. 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, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, [RFC 3688](#), DOI 10.17487/RFC3688, January 2004, <<http://www.rfc-editor.org/info/rfc3688>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#)¹, DOI 10.17487/RFC6020, October 2010, <<http://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, <<http://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, <<http://www.rfc-editor.org/info/rfc6242>>.
- [RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", [RFC 6536](#), DOI 10.17487/RFC6536, March 2012, <<http://www.rfc-editor.org/info/rfc6536>>.
- [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", [RFC 6991](#), DOI 10.17487/RFC6991, July 2013, <<http://www.rfc-editor.org/info/rfc6991>>.

5.2. Дополнительная литература

- [RFC5277] Chisholm, S. and H. Trevino, "NETCONF Event Notifications", RFC 5277, DOI 10.17487/RFC5277, July 2008, <<http://www.rfc-editor.org/info/rfc5277>>.
- [RFC6470] Bierman, A., "Network Configuration Protocol (NETCONF) Base Notifications", RFC 6470, DOI 10.17487/RFC6470, February 2012, <<http://www.rfc-editor.org/info/rfc6470>>.
- [YANG1.1] Bjorklund, M., "The YANG 1.1 Data Modeling Language", Work in Progress², draft-ietf-netmod-rfc6020bis-12, April 2016.

Благодарности

Вклад Andy Bierman в этот материал основан на поддержке со стороны Space & Terrestrial Communications Directorate (S&TCD) по контракту № W15P7T-13-C-A616. Любые мнения, выводы, заключения или рекомендации, выраженные в этом материале, принадлежат авторам и не обязательно отражают точку зрения Space & Terrestrial Communications Directorate (S&TCD).

Адреса авторов

Andy Bierman

YumaWorks

Email: andy@yumaworks.com

Martin Bjorklund

Tail-f Systems

Email: mbj@tail-f.com

Kent Watsen

Juniper Networks

Email: kwatsen@juniper.net

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

¹В [RFC 7950](#) содержится спецификация YANG версии 1.1. *Прим. перев.*

²Документ опубликован в [RFC 7950](#). *Прим. перев.*