Internet Engineering Task Force (IETF)
Request for Comments: 7317
Category: Standards Track
ISSN: 2070-1721

A. Bierman
YumaWorks
M. Bjorklund
Tail-f Systems

August 2014

A YANG Data Model for System Management

Модель данных YANG для управления системой

Аннотация

Этот документ задаёт модель YANG для идентификации и настройки некоторых базовых свойств системы в устройстве, содержащем сервер протокола настроки сети NETCONF (Network Configuration Protocol). Документ также включает определения узлов данных для идентификации системы, управления временем суток time-of-day) и пользователями, настройки распознавателя DNS и некоторых протокольных операций для управления системой.

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 в RFC 5741.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке http://www.rfc-editor.org/info/rfc7317.

Оглавление

1. Введение

Этот документ задаёт модель данных YANG [RFC6020] для настройки и идентификации некоторых базовых свойств устройства, содержащего сервер NETCONF.

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

Устройства, управляемые NETCONF и, возможно, иными механизмами, имеют общие свойства, которые нужно настраивать и отслеживать стандартными способами. Модуль YANG ietf-system, определённый в этом документе, обеспечивает:

- настройку и мониторинг идентификации системы;
- настройку и мониторинг времени суток;
- настройку аутентификации пользователей;
- настройку конфигурации локальных пользователей;
- настройку распознавателя DNS;
- операции управления системой (выключение, перезапуск, установка времени).

1.1. Терминология

Ключевые слова **должно** (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].

Ниже указаны термины, определённые в [RFC6241] и не переопределяемые здесь.

- client - клиент;
- configuration data - данные конфигурации;
- server - сервер;
- state data - данные состояния.

Ниже указаны термины, определённые в [RFC6020] и не переопределяемые здесь.

- augment - дополнение;
- data model - модель данных.

1.2. Диаграммы деревьев

В этом документе применяется упрощённое графическое представление модели данных, обозначения в котором описаны ниже.

- Квадратные скобки [и] содержат в себе ключи.
- В сокращениях перед именами узлов rw указывает данные конфигурации (read-write), ro - данные состояния (read-only), -x - операции RPC или действия, -n - уведомления.
- После имени узла символ ? указывает необязательный узел, ! - контейнер с присутствием, * - list или leaf-list.
- Круглые скобки включают узлы choice и case, а узлы case помечаются также двоеточием (:).
- Три точки (...) указывают пропущенное содержимое субдерева (ветви).

2. Цели

2.1. Идентификация системы

Есть много общих свойств, применяемых для идентификации устройств, опреационных систем, версий программ и пр., что требуется поддерживать в модулей данных системы. Эти объекты определены как данные рабочего состояния, а возвращаемая сервером информация может зависеть от производителя устройства.

Представлены также некоторые настраиваемые пользователем административные строки, такие как местоположение и описание системы.

2.2. Управление системным временем

Требуется поддерживать управление датой и временем, используемыми в системе. Требуется возможность установки системной даты и времени с использованием одного или нескольких серверов NTP, а также поддержка базы часовых поясов (Time Zone Database) [RFC6557]. Следует обеспечивать возможность настройки в системе применения NTP.

2.3. Аутентификация пользователей

Механизм проверки подлинности должен поддерживать парольную аутентификацию по протоколу RADIUS для вариантов развёртывания с централизованными серверами аутентификации. Для развёртываний без такой централизациии или при недоступности центрального сервера аутентификации требуется поддержка локальных пользователей.

Поскольку для протокола NETCONF обязательна поддержка SSH (Secure Shell) [RFC6242], модель аутентификации должна поддерживать методы SSH publickey и password [RFC4252].

Модели настройки аутентификации следует быть достаточно гибкой для поддержки методов проверки подлинности, заданных другими стандартами или производителями. Следует обеспечивать возможность настройки аутентификации в системе.

2.4. Распознаватель DNS

В системе с сервером NETCONF требуется настройка распознавателя DNS для управления способом распознавания доменных имён.

2.5. Управление системой

Необходимы несколько операций для поддержки таких задач, как перезапуск устройства и установка времени системы.

3. Модель данных системы

3.1. Идентификация системы

Ниже показана структура модели данных для идентификации системы.

```
+--rw system
|  +--rw contact?          string
|  +--rw hostname?         inet:domain-name
|  +--rw location?         string
+--ro system-state
   +--ro platform
      +--ro os-name?       string
      +--ro os-release?    string
      +--ro os-version?    string
      +--ro machine?       string
```

3.2. Управление системным временем

Ниже показана структура модели данных для управления системным временем.

```
+--rw system
|  +--rw clock
|  |  +--rw (timezone)?
|  |     +--:(timezone-name)
|  |     |  +--rw timezone-name?     timezone-name
|  |     +--:(timezone-utc-offset)
|  |        +--rw timezone-utc-offset?   int16
|  +--rw ntp!
|     +--rw enabled?   boolean
|     +--rw server* [name]
|        +--rw name                 string
|        +--rw (transport)
|        |  +--:(udp)
|        |     +--rw udp
|        |        +--rw address    inet:host
|        |        +--rw port?      inet:port-number
|        +--rw association-type?   enumeration
|        +--rw iburst?             boolean
|        +--rw prefer?             boolean
+--ro system-state
   +--ro clock
      +--ro current-datetime?      yang:date-and-time
      +--ro boot-datetime?         yang:date-and-time
```

В будущих версиях могут добавляться операторы case или задаваться дополнения в других моделях данных.

3.3. Модель для распознавателя DNS

Ниже показана структура модели данных для настройки распознавателя DNS.

```
+--rw system
   +--rw dns-resolver
      +--rw search*    inet:domain-name
      +--rw server* [name]
      |  +--rw name    string
      |  +--rw (transport)
      |     +--:(udp-and-tcp)
      |        +--udp-and-tcp
      |           +--rw address    inet:ip-address
      |           +--rw port?      inet:port-number
      +--rw options
         +--rw timeout?    uint8
         +--rw attempts?   uint8
```

В будущих версиях могут добавляться операторы case или задаваться дополнения в других моделях данных.

3.4. Модель для клиента RADIUS

Ниже показана структура модели данных для настройки клиента RADIUS.

```
+--rw system
   +--rw radius
      +--rw server* [name]
      |  +--rw name                    string
      |  +--rw (transport)
      |  |  +--:(udp)
      |  |     +--rw udp
      |  |        +--rw address                inet:host
      |  |        +--rw authentication-port?   inet:port-number
      |  |        +--rw shared-secret          string
      |  +--rw authentication-type?   identityref
      +--rw options
         +--rw timeout?    uint8
         +--rw attempts?   uint8
```

В будущих версиях могут добавляться операторы case или задаваться дополнения в других моделях данных.

3.5. Модель аутентификации пользователей

В этом документе заданы 3 метода аутентификации для использования с NETCONF:

- открытый ключ (publickey) для локальных пользователей через SSH;
- пароль для локальных пользователей через любой защищённый транспорт;
- пароль для пользователей RADIUS через любой защищённый транспорт.

Другие стандарты и производители могут определять дополнительные методы.

В документе заданы два необязательных свойства YANG - local-users и radius-authentication, которые сервер анонсирует для индикации поддержки настройки локальных пользователей на устройстве и аутентификации RADIUS.

Заданные в этом документе параметры аутентификации служат в основном для проверки подлинности пользователей NETCONF, но могут применяться и другими интерфейсами, например, консольным (CLI) или WEB.

Ниже показана структура модели данных для аутентификации пользователей.

```
+--rw system
   +--rw authentication
      +--rw user-authentication-order*   identityref
      +--rw user* [name]
         +--rw name         string
         +--rw password?    ianach:crypt-hash
         +--rw authorized-key* [name]
            +--rw name          string
            +--rw algorithm     string
            +--rw key-data      binary
```

3.5.1. Аутентификация с открытым ключом через SSH

Если сервер NETCONF анонсирует свойство local-users, это говорит о поддержке локальных пользователей и их открытых ключей SSH в списке /system/authentication/user.

Аутентификацию по открытому ключу запрашивает клиент SSH. Если сервер поддерживает функцию local-users, при организации SSH сессии между клиентом NETCONF и сервером с использованием метода publickey [RFC4252], сервер SSH ищет имя из запроса SSH в списке /system/authentication/user и проверяет ключ, как указано в [RFC4253].

3.5.2. Парольная аутентификация локальных пользователей

Если сервер NETCONF анонсирует свойство local-users, конфигурация и пароли локальных пользователей поддерживаются в списке /system/authentication/user.

Для транспортных протоколов NETCONF, поддеживающих парольную аутентификацию, лист-список (leaf-list) user-authentication-order служит для решения вопроса о применении парольной аутентификации локальных пользователей.

В SSH парольную аутентификацию запрашивает клиент, другой транспорт NETCONF также **может** поддерживать аутентификацию по паролю.

При запросе парольной аутентификации локального пользователя транспорт NETCONF ищет представленное клиентом имя пользователя в списке /system/authentication/user и проверяет его пароль.

3.5.3. Парольная аутентификация с RADIUS

Если сервер NETCONF анонсирует свойство radius-authentication, устройство поддерживает аутентификацию пользователей с применением протокола RADIUS.

Для транспортных протоколов NETCONF с поддержкой аутентификации по паролю лист-список user-authentication-order применяется для управления использованием парольной аутентификации RADIUS.

В SSH парольную аутентификацию запрашивает клиент, другой транспорт NETCONF также **может** поддерживать аутентификацию по паролю.

3.6. Управление системой

Для управления системой заданы три операции:

```
set-current-datetime
system-restart
system-shutdown
```

Операция system-restart служит для перезапуска системы в целом (не только сервера NETCONF), а system-shutdown - для выключения питания системы.

4. Связи с SNMPv2-MIB

Если устройство реализует SNMPv2-MIB [RFC3418], реализация может сопоставить два объекта (см. 6. Модуль YANG System). В таблице показано соответствие узлов данных YANG объектам SNMPv2-MIB.

Узлы данных конфигурации интерфейса и связанные объекты SNMPv2-MIB.

Узел данных YANG	***Объект SNMPv2-MIB***
contact	sysContact
location	sysLocation

5. Модуль YANG IANA Crypt Hash

Этот модуль YANG ссылается на [RFC1321], [IEEE-1003.1-2008] и [FIPS.180-4.2012].

```
<CODE BEGINS> file "iana-crypt-hash@2014-08-06.yang"

module iana-crypt-hash {
  namespace "urn:ietf:params:xml:ns:yang:iana-crypt-hash";
  prefix ianach;

  organization "IANA";
  contact
    "        Internet Assigned Numbers Authority

     Postal: ICANN
             12025 Waterfront Drive, Suite 300
             Los Angeles, CA  90094-2536
             United States

     Tel:    +1 310 301 5800
     E-Mail: iana@iana.org>";
  description
    "Этот модуль YANG задаёт тип для хранения паролей с помощью
     хэш-функции и способы идентификации хэш-функциии, поддерживаемой
     реализацией.

     Свежую версию модуля можно загрузить с web-сайта IANA.

     Запросы для новых значений следует направлять в IANA по адресу
     iana@iana.org.

     Авторские права (Copyright (c) 2014) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Исходный выпуск этого модуля YANG является частью RFC 7137,
     где правовые аспекты приведены более полно.";

  revision 2014-08-06 {
    description
      "исходный выпуск.";
    reference
      "RFC 7317: A YANG Data Model for System Management";
  }

  typedef crypt-hash {
    type string {
      pattern
        '$0$.*'
      + '|$1$[a-zA-Z0-9./]{1,8}$[a-zA-Z0-9./]{22}'
      + '|$5$(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{43}'
      + '|$6$(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{86}';
    }
    description
      "Тип crypt-служит для хранения паролей с использованием
       хэш-функции. Алгоритмы применения хэш-функции и кодирования
       результата реализованы в системах UNIX функцией crypt(3).

       Значение этого типа соответствует 1 из показанных ниже форм:

         $0$<открытый текст пароля>
         $<id>$<salt>$<хэш пароля>
         $<id>$<parameter>$<salt>$<хэш пароля>

       Префикс $0$ указывает, что значение является открытым текстом.
       При получении сервером такого значения рассчитывается его хэш
       и строка $<id>$<salt>$ или $<id>$<parameter>$<salt>$
       добавляется перед ним. Результат помещается в хранилище данных
       конфигурации.

       Если значение начинается с $<id>$, где <id> отличается от 0,
       это говорит принявшему серверу, что значение уже хэшировано и
       оно помещается неизменным в хранилище данных.

       Когда серверу нужно проверить указанный пользователем пароль,
       он ищет сохраненную хэш-строку, извлекает из неё затрафку
       (salt) и заново вычисляет хэш полученного на входе пароля. Если
       результат совпадает с сохранённым, пароль воспринимается.

       Этот тип определяет указанные ниже функции хэширования.
```

```
           id | Функция       | Свойство (feature)
           ---+---------------+-------------------
            1 | MD5           | crypt-hash-md5
            5 | SHA-256       | crypt-hash-sha-256
            6 | SHA-512       | crypt-hash-sha-512

         Сервер указывает поддержку хэш-функций, анонсируя
         соответствующие значения.";
       reference
         "IEEE Std 1003.1-2008 - crypt() function
          RFC 1321: The MD5 Message-Digest Algorithm
          FIPS.180-4.2012: Secure Hash Standard (SHS)";
     }

     feature crypt-hash-md5 {
       description
         "Устройство поддерживает хэш-функцию MD5 в crypt-hash.";
       reference "RFC 1321: The MD5 Message-Digest Algorithm";
     }

     feature crypt-hash-sha-256 {
       description
         "Устройство поддерживает хэш-функцию SHA-256 в crypt-hash.";
       reference "FIPS.180-4.2012: Secure Hash Standard (SHS)";
     }

     feature crypt-hash-sha-512 {
       description
         "Устройство поддерживает хэш-функцию SHA-512 в crypt-hash.";
       reference "FIPS.180-4.2012: Secure Hash Standard (SHS)";
     }

   }
   <CODE ENDS>
```

6. Модуль YANG System

Этот модуль YANG импортирует расширения YANG из [RFC6536] и типы YANG из [RFC6991], а также ссылается на [RFC1035], [RFC2865], [RFC3418], [RFC5607], [RFC5966], [RFC6557].

```
   <CODE BEGINS> file "ietf-system@2014-08-06.yang"

  module ietf-system {
    namespace "urn:ietf:params:xml:ns:yang:ietf-system";
    prefix "sys";

    import ietf-yang-types {
      prefix yang;
    }

    import ietf-inet-types {
      prefix inet;
    }

    import ietf-netconf-acm {
      prefix nacm;
    }

    import iana-crypt-hash {
      prefix ianach;
    }

    organization
      "IETF NETMOD (NETCONF Data Modeling Language) Working Group";

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

       WG Chair: Thomas Nadeau
                 <mailto:tnadeau@lucidvision.com>

       WG Chair: Juergen Schoenwaelder
                 <mailto:j.schoenwaelder@jacobs-university.de>

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

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

    description
      "Этот модуль содержит определения YANG для идентификации и
       настройки некоторых базовых свойств системы в устройстве с
       сервером NETCONF. Это включает определения узлов данных для
       идентификации системы, управления временем и пользователями,
```

```
      настройки распознавателя DNS и некоторых протокольных
      операций для управления системой.

      Авторские права (Copyright (c) 2014) принадлежат IETF Trust и
      лицам, указанным как авторы. Все права защищены.

      Распространение и применение модуля в исходной или двоичной
      форме с изменениями или без таковых разрешено в соответствии с
      лицензией Simplified BSD License, изложенной в параграфе 4.c
      IETF Trust's Legal Provisions Relating to IETF Documents
      (https://trustee.ietf.org/license-info).

      Эта версия модуля YANG является частью RFC 7137, где правовые
      аспекты приведены более полно.";

    revision 2014-08-06 {
      description
        "Исходный выпуск.";
      reference
        "RFC 7317: A YANG Data Model for System Management";
    }

  /*
   * Определения типов
   */

    typedef timezone-name {
      type string;
      description
        "Имя часового пояса изи Time Zone Database, иногда называемой
         Olson Database.

         Точный набор пригодных значений зависит от реализации.
         Определение пригодных значений клиентом выходит за рамки
         документа.";
      reference
        "RFC 6557: Procedures for Maintaining the Time Zone Database";
     }

    /*
     * Свойства (функции)
     */

    feature radius {
      description
        "Указывает, что устройство настроено как клиент RADIUS.";
      reference
        "RFC 2865: Remote Authentication Dial In User Service (RADIUS)";
    }

    feature authentication {
      description
        "Устройство разрешает настройку аутентификации пользователей.";
    }

    feature local-users {
      if-feature authentication;
      description
        "Устройство разрешает настройку локальной аутентификации
         пользователей.";
    }

    feature radius-authentication {
      if-feature radius;
      if-feature authentication;
      description
        "Устройство поддерживает настройку аутентификации пользователей
         по протоколу RADIUS.";
      reference
        "RFC 2865: Remote Authentication Dial In User Service (RADIUS)
         RFC 5607: Remote Authentication Dial-In User Service (RADIUS)
                   Authorization for Network Access Server (NAS)
                   Management";
    }

    feature ntp {
      description
        "На устройстве может бать указан 1 или несколько серверов NTP
         для установки системной даты и времени.";
    }

    feature ntp-udp-port {
      if-feature ntp;
      description
        "Устройство поддерживает настройку порта UDP для серверов NTP.
```

```
      Это является свойством (feature), поскольку многие реализации
      не поддерживают изменение номера порта.";
  }

  feature timezone-name {
    description
      "Указывает возможность настроить на устройстве локальный часовой
       пояс с использованием базы данных TZ для установки часового
       пояса и сезонного времени.";
    reference
      "RFC 6557: Procedures for Maintaining the Time Zone Database";
  }

  feature dns-udp-tcp-port {
    description
      "Устройство поддерживает настройку порта UDP и TCP для серверов
       DNS.

       Это является свойством (feature), поскольку многие реализации
       не поддерживают изменение номера порта.";
  }

  /*
   * Идентификаторы (отождествления)
   */

  identity authentication-method {
    description
      "Базовый идентификатор методов аутентификации пользователей.";
  }

  identity radius {
    base authentication-method;
    description
      "Аутентификация пользователей с применением протокола RADIUS.";
    reference
      "RFC 2865: Remote Authentication Dial In User Service (RADIUS)
       RFC 5607: Remote Authentication Dial-In User Service (RADIUS)
                 Authorization for Network Access Server (NAS)
                 Management";
  }

  identity local-users {
    base authentication-method;
    description
      "Парольная аутентификация заданных локально пользователей.";
  }

  identity radius-authentication-type {
    description
      "Базовый идентификатор для типов аутентификации RADIUS.";
  }

  identity radius-pap {
    base radius-authentication-type;
    description
      "Устройство поддерживает аутентификацию PAP через RADIUS.";
    reference
      "RFC 2865: Remote Authentication Dial In User Service (RADIUS)";
  }

  identity radius-chap {
    base radius-authentication-type;
    description
      "Устройство поддерживает аутентификацию CHAP через RADIUS.";
    reference
      "RFC 2865: Remote Authentication Dial In User Service (RADIUS)";
  }

  /*
   * Узлы данных конфигурации
   */

  container system {
    description
      "Конфигурация системной группы.";

    leaf contact {
      type string;
      description
        "Контактные данные администратора системы.

         Реализация сервера МОЖЕТ отображать этот лист на объект MIB
         sysContact. Такая реализация должна применять тот или иной
         механизм для обработки различий в размере и наборе символов
         для этого листа и sysContact, выходящий за рамки документа.";
```

```
      reference
        "RFC 3418: Management Information Base (MIB) for the
                   Simple Network Management Protocol (SNMP)
                   SNMPv2-MIB.sysContact";
    }
    leaf hostname {
      type inet:domain-name;
     description
       "Имя хоста - одна метка или полное доменное имя хоста.";
    }
    leaf location {
      type string;
      description
        "Местоположение системы.

         Реализация сервера МОЖЕТ отображать этот лист на объект MIB
         sysLocation. Такая реализация должна применять тот или иной
         механизм для обработки различий в размере и наборе символов
         для этого листа и sysContact, выходящий за рамки документа.";

      reference
        "RFC 3418: Management Information Base (MIB) for the
                   Simple Network Management Protocol (SNMP)
                   SNMPv2-MIB.sysLocation";
    }

    container clock {
      description
        "Конфигурация системной даты и свойств времени.";

      choice timezone {
        description
          "Сведения о часовом поясе системы.";

        case timezone-name {
          if-feature timezone-name;
          leaf timezone-name {
            type timezone-name;
            description
              "Имя в базе данных TZ, применяемое в системе, такое как
               Europe/Stockholm.";
          }
        }
        case timezone-utc-offset {
          leaf timezone-utc-offset {
            type int16 {
              range "-1500 .. 1500";
            }
            units "minutes";
            description
              "Число минут, добавляемых к времени UTC для указания
               часового пояса системы. Например, UTC - 8:00 hours
               будет представлено в форме -480. Отметим, что при
               использовании этого объекта сезонное время не
               применяется.";
          }
        }
      }
    }

    container ntp {
      if-feature ntp;
      presence
        "Включает клиента NTP, если для листа enabled не задано
         значение false (по умолчанию true).";
      description
        "Конфигурация клиента NTP.";

      leaf enabled {
        type boolean;
        default true;
        description
          "Указывает, что системе следует пытаться синхронизировать
           свои часы с сервером NTP из списка ntp/server.";
      }
      list server {
        key name;
        description
          "Список серверов NTP для синхронизации часов системы. Если
           /system/ntp/enabled имеет значение true, система будет
           пытаться подключится и использовать эти серверы NTP.";

        leaf name {
          type string;
          description
            "Произвольное имя для сервера NTP.";
```

```
        }
        choice transport {
          mandatory true;
          description
            "Зависящие от транспорта параметры для сервера.";

          case udp {
            container udp {
              description
                "Параметры NTP, связанные с транспортом UDP.";
              leaf address {
                type inet:host;
                mandatory true;
                description
                  "Адрес сервера NTP.";
              }
              leaf port {
                if-feature ntp-udp-port;
                type inet:port-number;
                default 123;
                description
                  "Номер порта на сервере NTP.";
              }
            }
          }
        }

        leaf association-type {
          type enumeration {
            enum server {
              description
                "Используется клиентский режим ассоциации и устройство
                 не будет синхронизировать заданный сервер NTP.";
            }
            enum peer {
              description
                "Используется симметричный активный режим ассоциации и
                 устройство может синхронизировать этот сервер NTP.";
            }
            enum pool {
              description
                "Используется клиентский режим ассоциации с одним или
                 несколькими серверами NTP, найденными распознаванием
                 DNS по имени домена в листе address. Устройство не
                 будет синхронизировать серверы.";
            }
          }
          default server;
          description
            "Желаемый тип ассоциации с этим сервером NTP.";
        }
        leaf iburst {
          type boolean;
          default false;
          description
            "Указывает, включать ли серверу burst-синхронизацию.";
        }
        leaf prefer {
          type boolean;
          default false;
          description
            "Указывает, следует ли предпочитать этот сервер.";
        }
      }
    }

    container dns-resolver {
      description
        "Конфигурация для распознавателя DNS.";
      leaf-list search {
        type inet:domain-name;
        ordered-by user;
        description
          "Упорядоченный список доменов для поиска при распознавании
           имени хоста.";
      }
      list server {
        key name;
        ordered-by user;
        description
          "Серверы DNS, которые распознавателю следует опрашивать.

           Когда распознаватель вызвается запрашивающим приложением,
           он передаёт запрос первому серверу имён из списка. При
           отсутствии ответа в течение timeout секунд распознаватель
           обращается к следующему серверу из списка, а если ответа
```

```
          нет ни от одного, он возвращается к первому. После
          прохождения по списку attempts раз без получения какого-
          либо ответа вызвавшему приложению возвращается ошибка и
          попытки прекращаются.

          Реализация МОЖЕТ ограничивать число записей в списке.";

        leaf name {
          type string;
          description
            "Произвольное имя для сервера DNS.";
        }
        choice transport {
          mandatory true;
          description
            "Зависящие от транспорта параметры для сервера.";

          case udp-and-tcp {
            container udp-and-tcp {
              description
                "Параметры сервера DNS для транспорта UDP и TCP.";
              reference
                "RFC 1035: Domain Names - Implementation and
                           Specification
                 RFC 5966: DNS Transport over TCP - Implementation
                           Requirements";
              leaf address {
                type inet:ip-address;
                mandatory true;
                description
                  "Адрес сервера DNS.";
              }
              leaf port {
                if-feature dns-udp-tcp-port;
                type inet:port-number;
                default 53;
                description
                  "Номер порта UDP и TCP на сервере DNS.";
              }
            }
          }
        }
      }
      container options {
        description
          "Опции распознавателя, набор которых ограничен доступными в
           разных реализациях распознавателей и сочтённых полезными.";
        leaf timeout {
          type uint8 {
            range "1..max";
          }
          units "seconds";
          default "5";
          description
            "Продолжительность ожидания распознавателем ответа от
             сервера перед попыткой воспользоваться следующим.";
        }
        leaf attempts {
          type uint8 {
            range "1..max";
          }
          default "2";
          description
            "Число попыток откравки запроса по всему списку серверов
             имён перед возвратом ошибки вызвавшему приложению.";
        }
      }
    }

    container radius {
      if-feature radius;

      description
        "Конфигурация клиента RADIUS.";

      list server {
        key name;
        ordered-by user;
        description
          "Список применяемых устройством серверов RADIUS.

          При вызове клиента RADIUS запрашивающим приложением, он
          передаёт запрос первому серверу из списка. При отсутствии
          ответа в течение timeout секунд клиент обращается к
          следующему серверу из списка, а если ответа нет ни от
          одного, он возвращается к первому. После прохождения по
```

```
           списку attempts раз без получения ответа вызвавшему
           приложению возвращается ошибка и попытки прекращаются.";

        leaf name {
          type string;
          description
            "Произвольное имя для сервера RADIUS.";
        }
        choice transport {
          mandatory true;
          description
            "Зависящие от транспорта параметры для сервера.";

          case udp {
            container udp {
              description
                "Зависящие от транспорта UDP параметры для сервера.";
              leaf address {
                type inet:host;
                mandatory true;
                description
                  "Адрес сервера RADIUS.";
              }
              leaf authentication-port {
                type inet:port-number;
                default "1812";
                description
                  "Номер порта на сервере RADIUS.";
              }
              leaf shared-secret {
                type string;
                mandatory true;
                nacm:default-deny-all;
                description
                  "Общий секрет, известный клиенты и серверу RADIUS.";
                reference
                  "RFC 2865: Remote Authentication Dial In User
                              Service (RADIUS)";
              }
            }
          }
        }
        leaf authentication-type {
          type identityref {
            base radius-authentication-type;
          }
          default radius-pap;
          description
            "Тип аутентификации, запрошенный у сервера RADIUS.";
        }
      }
      container options {
        description
          "Опции клиента RADIUS.";

        leaf timeout {
          type uint8 {
            range "1..max";
          }
          units "seconds";
          default "5";
          description
            "Число секунд ожидания устройством ответа от сервера
             RADIUS перед переходом к другому серверу.";
        }
        leaf attempts {
          type uint8 {
            range "1..max";
          }
          default "2";
          description
            "Число попыток отправик запроса каждому серверу RADIUS
             перед прекращением попыток.";
        }
      }
    }

    container authentication {
      nacm:default-deny-write;
      if-feature authentication;

       description
         "Субдерево настроек аутентификации.";

       leaf-list user-authentication-order {
         type identityref {
```

```
        base authentication-method;
      }
      must '(. != "sys:radius" or ../../radius/server)' {
        error-message
          "При использовании radius должен быть настроен"
        + " сервер RADIUS.";
        description
          "При использовании метода акутентификации radius
           должен быть настроен сервер RADIUS.";
      }
      ordered-by user;

      description
        "Когда устройство проверяет подлинность пользователя по
         паролю, оно применяет методы аутентификации из этого
         leaf-list в заданном порядке. При отказе одно метода
         применяется слудующий. Если ни один метод не дал
         результата, доступ пользователя отвергается.

         Пустой leaf-list user-authentication-order позволяет
         проверять подлинность пользователя с применением
         беспарольных механизмов.

         Если сервер NETCONF анонсирует свойство
         radius-authentication, в список может добавляться
         отождествление radius.

         Если сервер NETCONF анонсирует свойство local-users,
         в список может добавляться идентификатор local-users.";
    }

    list user {
      if-feature local-users;
      key name;
      description
        "Список локальных пользователей, заданный на устройстве.";

      leaf name {
        type string;
        description
          "Строка имени пользователя для этой записи.";
      }
      leaf password {
        type ianach:crypt-hash;
        description
          "Пароль для этой записи.";
      }
      list authorized-key {
        key name;
        description
          "Список открытх ключей SSH для этого пользователя. Ключи
           разрешены для аутентификации SSH в соответствии с
           RFC 4253.";
        reference
          "RFC 4253: The Secure Shell (SSH) Transport Layer
                     Protocol";

        leaf name {
          type string;
          description
            "Произвольное имя для ключа SSH.";
        }
        leaf algorithm {
          type string;
          mandatory true;
          description
            "Алгоритм с открытым ключом для этого ключа SSH.

             Пригодны значения из реестра IANA Secure Shell
             (SSH) Protocol Parameters, Public Key
             Algorithm Names.";
          reference
            "IANA 'Secure Shell (SSH) Protocol Parameters'
             registry, Public Key Algorithm Names";
        }
        leaf key-data {
          type binary;
          mandatory true;
          description
            "Двоичные данные открытого ключа для этого ключа SSH,
             как указано в параграфе 6.6 RFC 4253, например,

               string    идентификатор сертификата или формата
                         открытого ключа
               byte[n]   данные ключа или сертификата.";
          reference
```

```
                "RFC 4253: The Secure Shell (SSH) Transport Layer
                           Protocol";
            }
          }
        }
      }
    }

    /*
     * Узлы данных рабочего состояния
     */

    container system-state {
      config false;
      description
        "Рабочее состояние системной группы.";

      container platform {
        description
          "Зависящие от производителя сведения для идентификации
           платформы и операционной системы.";
        reference
          "IEEE Std 1003.1-2008 - sys/utsname.h";
        leaf os-name {
          type string;
          description
            "Имя применяемой ОС, например, Linux.";
          reference
            "IEEE Std 1003.1-2008 - utsname.sysname";
        }
        leaf os-release {
          type string;
          description
            "Текущий выпуск используемой ОС. Эта строка МОЖЕТ указывать
             номер выпуска исходного кода ОС.";
          reference
            "IEEE Std 1003.1-2008 - utsname.release";
        }
        leaf os-version {
          type string;
          description
            "Текущая версия используемой ОС. Эта строка МОЖЕТ указывать
             дату сборки ОС и сведения о целевом варианте.";
          reference
            "IEEE Std 1003.1-2008 - utsname.version";
        }
        leaf machine {
          type string;
          description
            "Зависящая от производителя строка аппаратной платформы.";
          reference
            "IEEE Std 1003.1-2008 - utsname.machine";
        }
      }

      container clock {
        description
          "Свойства мониторинга системной даты и времени.";

        leaf current-datetime {
          type yang:date-and-time;
          description
            "Текущая дата и время системы.";
        }

        leaf boot-datetime {
          type yang:date-and-time;
          description
            "Дата и время при перезапуске системы.";
        }
      }
    }

    rpc set-current-datetime {
      nacm:default-deny-all;
      description
        "Установить для листа /system-state/clock/current-datetime
         заданное значение.

         Если система использует NTP (/system/ntp/enabled true),
         эта операция приведёт к ошибке с error-tag operation-failed
         и error-app-tag ntp-active.";
      input {
        leaf current-datetime {
          type yang:date-and-time;
          mandatory true;
```

```
          description
            "Текущая дата и время системы.";
        }
      }
    }

    rpc system-restart {
      nacm:default-deny-all;
      description
        "Запрос незамедлительного перезапуска всей системы. Серверу
         СЛЕДУЕТ передать клиенту отклик rpc до перезапуска.";
    }

    rpc system-shutdown {
      nacm:default-deny-all;
      description
        "Запрос незамедлительного выключения всей системы. Серверу
         СЛЕДУЕТ передать клиенту отклик rpc до выключения.";
    }

  }
  <CODE ENDS>
```

7. Взаимодействие с IANA

Агентство IANA создало на основе раздела 5 поддерживаемый им (IANA-maintained) модуль YANG iana-crypt-hash, который позволяет добавлять алгоритмы хэширования в тип crypt-hash. Регистрация выполняется по процедуре Expert Review, заданной в [RFC5226].

Этот документ регистрирует два идентификатора URI в реестре IETF XML Registry [RFC3688] с использованием формата RFC 3688.

```
URI: urn:ietf:params:xml:ns:yang:iana-crypt-hash
Registrant Contact: The IESG.
XML: N/A; запрошенный URI является пространством имён XML.

URI: urn:ietf:params:xml:ns:yang:ietf-system
Registrant Contact: The IESG.
XML: N/A; запрошенный URI является пространством имён XML.
```

Этот документ регистрирует два модуля YANG в ррестре YANG Module Names [RFC6020].

```
name: iana-crypt-hash
namespace: urn:ietf:params:xml:ns:yang:iana-crypt-hash
prefix: ianach
reference: RFC 7317

name: ietf-system
namespace: urn:ietf:params:xml:ns:yang:ietf-system
prefix: sys
reference: RFC 7317
```

8. Вопросы безопасности

Заданные этим документом модули YANG определяют схему для данных, предназначенную для доступа через сеть с использованием протоколов управления, таких как NETCONF [RFC6241]. Нижним уровнем NETCONF служит защищённый транспорт с обязательной поддержкой SSH (Secure Shell) [RFC6242]. Модель управления доступом NETCONF [RFC6536] обеспечивает возможность разрешить доступ лишь определённых пользователей NETCONF к заранее заданному подмножеству операций и содержимого NETCONF.

В модуле YANG ietf-system определено множество узлов данных, которые разрешают запись, создание и удаление (т. е. config true, как принято по умолчанию). Эти узлы могут быть конфиденциальными или уязвимыми в некоторых сетевых средах. Запись в такие узлы (например, edit-config) без должной защиты может негативно влиять на работу сети. Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

/system/clock/timezone
Этот выбор (choice) включает объекты, служащие для управления часовым поясом на устройстве.

/system/ntp
Этот контейнер содержит объекты, применяемые для контроля используемых устройством серверов NTP.

/system/dns-resolver
Этот контейнер содержит объекты, применяемые для контроля используемых устройством серверов DNS.

/system/radius
Этот контейнер содержит объекты, применяемые для контроля используемых устройством серверов RADIUS.

/system/authentication/user-authentication-order
Этот лист определяет способ аутентификации попыток регистрации пользователя в системе (login).

/system/authentication/user
Этот список указывает локальных пользователей, разрешённых в системе.

Некоторые из доступных для чтения узлов модуля YANG ietf-system могут быть конфиденциальны или уязвимы в той или иной сетевой среде. Важно контролировать доступ к таким объектам (например, get, get-config, notification). Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

/system/platform
Этот контейнер включает объекты, которые могут помочь в определении конкретного сервера NETCONF и версии ОС на устройстве.

/system/authentication/user
Этот контейнер включает объекты, которые могут помочь в определении имён пользователей и паролей, применяемых в системе.

Некоторые из операций RPC в модуле YANG ietf-system могут быть чувствительны или уязвимы в той или иной сетевой среде. Важно контролировать доступ к таким операциям. Ниже указаны такие операции.

set-current-datetime
Меняет текущую дату и время на устройстве.

system-restart
Перезагружает устройство.

system-shutdown
Выключает устроство.

Поскольку документ описывает применение протокола RADIUS для аутентификации, к нему применимы все угрозы, имеющиеся для приложений RADIUS. Эти угрозы рассмотрены в [RFC2865], [RFC3162] и разделе 4 [RFC3579].

Документ содержит параметры конфигурации для механизмов аутентификации SSH publickey и password. В параграфе 9.4 [RFC4251] и разделе 11 [RFC4252] рассмотрены соображения безопасности для этих механизмов.

Модуль YANG iana-crypt-hash определяет тип crypt-hash, который может служить для хранения хэш-значений MD5. Вопросы безопасности для MD5 рассмотрены в [RFC6151]. Применение MD5 **не рекомендуется**.

9. Литература

9.1. Нормативные документы

[FIPS.180-4.2012] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>.

[IEEE-1003.1-2008] Institute of Electrical and Electronics Engineers, "POSIX.1-2008", IEEE Standard 1003.1, March 2008.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4252] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol", RFC 4252, January 2006.

[RFC4253] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5607] Nelson, D. and G. Weber, "Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management", RFC 5607, July 2009.

[RFC5966] Bellis, R., "DNS Transport over TCP - Implementation Requirements", RFC 5966, August 2010.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, June 2011.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, March 2012.

[RFC6991] Schoenwaelder, J., "Common YANG Data Types", RFC 6991, July 2013.

9.2. Дополнительная литература

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC6557] Lear, E. and P. Eggert, "Procedures for Maintaining the Time Zone Database", BCP 175, RFC 6557, February 2012.

Адреса авторов

Andy Bierman
YumaWorks
EMail: andy@yumaworks.com

Martin Bjorklund
Tail-f Systems
EMail: mbj@tail-f.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru