Network Working Group
Request for Comments: 5427
Category: Standards Track

G. Keeni
Cyber Solutions Inc.

March 2009

Текстовые соглашения для управления Syslog

Textual Conventions for Syslog Management

Статус документа

Этот документ является проектом стандарта Internet (Internet Standards Track) и служит приглашением к дискуссии и внесению предложений с целью совершенствования протокола. Информацию о состоянии стандартизации и статусе протокола можно найти в текущей редакции документа «Internet Official Protocol Standards» (STD 1). Документ может распространяться свободно.

Авторские права

Аннотация

Этот модуль MIB определяет текстовые соглашения для представления информации Facility и Severity, обычно используемой в сообщениях syslog. Цель заключается в том, чтобы сделать эти текстовые соглашения импортируемыми и применимыми в других модулях MIB, которым иначе пришлось бы определять своё представление.

Оглавление

1. Стандартная модель управления Internet

Подробный обзор документов, описывающих современную схему стандартного управления в Internet (Internet-Standard Management Framework), приведён в разделе 7 документа RFC 3410 [RFC3410].

Доступ к объектам управления выполняется через виртуальное информационное хранилище, называемое базой данных управления или MIB[3]. Доступ к объектам MIB обычно осуществляется по протоколу SNMP[4]. Объекты в MIB определяются с использованием механизмов, описанных в структуре SMI[5]. В этом документе описан модуль MIB, соответствующий спецификации SMIv2, описанной в STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] и STD 58, RFC 2580 [RFC2580].

2. Основы

Операционные системы, процесс и приложения, совокупно называемые далее «источники» (Facilities), генерируют сообщения, показывающие их состояние или происходящие события. Эти сообщения называют сообщениями syslog. В общем случае сообщения syslog наряду с другой информацией включают код, представляющий источник сообщения (Facility), и код, представляющий уровень важности сообщения (Severity). Коды Facility и Severity обычно используются для классификации и отбора полученных сообщений при их обработке и отображении. Коды Facility полезны для отбора инициатора содержимого сообщений, но не всегда достаточно конкретны для чёткой идентификации инициатора. Реализациям протокола syslog [RFC5424], содержащим структурированные элементы данных (SDE[6]), следует использовать эти SDE для определения элемента, служащего источником содержимого сообщения.

---

[1] В оригинале - IETF Contributions. *Прим. перев.*
[2] В оригинале - IETF Standards Process. *Прим. перев.*
[3] Management Information Base.
[4] Simple Network Management Protocol - простой протокол сетевого управления.
[5] Structure of Management Information - структура данных управления.
[6] Structured data element.

В этом документе определён набор текстовых соглашений (TC[1]), которые могут применяться для представления кодов Facility и Severity, обычно используемых в сообщениях syslog.

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

3. MIB для текстовых соглашений Syslog

```
SYSLOG-TC-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, mib-2
              FROM SNMPv2-SMI        -- [RFC2578]
    TEXTUAL-CONVENTION
              FROM SNMPv2-TC;        -- [RFC2579]

syslogTCMIB  MODULE-IDENTITY
    LAST-UPDATED "200903300000Z"     --  30 марта 2009 г.
    ORGANIZATION "IETF Syslog Working Group"
    CONTACT-INFO
    "                    Glenn Mansfield Keeni
                 Postal: Cyber Solutions Inc.
                         6-6-3, Minami Yoshinari
                         Aoba-ku, Sendai, Japan 989-3204.
                    Tel: +81-22-303-4012
                    Fax: +81-22-303-4015
                 EMail: glenn@cysols.com

      Support Group EMail: syslog@ietf.org
      "

    DESCRIPTION
        "Модуль MIB, содержащий текстовые соглашения для сообщений syslog.

         Copyright (c) 2009 IETF Trust и лица, указанные в качестве авторов
         кода. Все права защищены.

         Распространение и использование в исходном и двоичном формате с
         внесением изменений или без таковых допускается при выполнении
         перечисленных ниже условий.

         - При распространении исходного кода должен сохраняться приведённый
           выше текст об авторских правах, данный список условий и приведённый
           ниже отказ от ответственности.

         - При распространении в двоичном формате в документации и/или других
           сопроводительных документах должен сохраняться приведённый выше
           текст об авторских правах, данный список условий и приведённый
           ниже отказ от ответственности.

         - Названия Internet Society, IETF, IETF a также названия других
           конкретных участников не могут использоваться для одобрения или
           продвижения продукции, основанной на этой программе, без
           предварительного письменного разрешения.

         THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
         CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED
         WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
         WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
         PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
         OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
         INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
         (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
         GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
         BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
         LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
         (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
         OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
         POSSIBILITY OF SUCH DAMAGE.

         Эта версия данного модуля MIB является частью 5427;
         правовые аспекты полностью приведены в этом RFC.
        "

    REVISION "200903300000Z"     --  30 марта 2009
    DESCRIPTION
        "Исходная версия, опубликованная в RFC 5427."

    ::= { mib-2 173 }

-- ------------------------------------------------------------
-- Текстовые соглашения
-- ------------------------------------------------------------
```

[1]Textual convention.

```
SyslogFacility  ::=  TEXTUAL-CONVENTION
    STATUS  current
    DESCRIPTION
        "В этих текстовых соглашениях перечислены объекты (Facility),
         являющиеся источниками сообщений syslog.

         Значения Facility в сообщениях syslog задаются кодами в форме
         десятичных чисел. Для взаимодействия и совместимости с
         более ранними версиями данный документ задаёт нормативное отображение
         между метками, представляющими значения Facility, и соответствующими
         числовыми кодами. Метки могут применяться, например, в пользовательских
         интерфейсах приложений SNMP.

         Метка зачастую семантически бессмысленна, поскольку неразумно пытаться
         перечислить все возможные варианты Facility, а для многих демонов и
         процессов нет явно выделенного кода или метки Facility. Например, нет
         метки Facility, соответствующей сервису HTTP. Реализации служб HTTP
         могут генерировать сообщения, например, с метками local7 или uucp.
         Это обычная практика, поскольку инициаторы, трансляторы и коллекторы
         могут настраиваться на подобающую обработку таких ситуаций. Для повышения
         точности приложение может также включать структурированные данные APP-NAME.

         Отметим, что механизмы операционной системы для настройки syslog
         (например, файл syslog.conf) ещё не стандартизованы и могут применять
         разные наборы меток Facility и/или их отображений на коды Facility.

         В частности, метки, соответствующие кодам Facility 4, 10, 13 и 14,
         и коду для метки cron, существенно различаются в разных операционных
         системах. Для того, чтобы различать метки, соответствующие кодам 9 и 15,
         метке cron2 был присвоен код 15. Приведённый список не является полным
         и могут существовать другие отличия, которые могут появляться и впредь.

         Указанное здесь отображение ДОЛЖНО использоваться в интерфейсе MIB, хотя
         для конкретных реализаций syslog могут применяться иные отображения в других
         интерфейсах сетевого управления.
        "
    REFERENCE "Протокол Syslog (RFC5424), таблица 1"
    SYNTAX  INTEGER
         {

           kern             (0), -- сообщения ядра
           user             (1), -- сообщения пользовательского уровня
           mail             (2), -- сообщения почтовой системы
           daemon           (3), -- сообщения системных демонов
           auth             (4), -- проверка полномочий
           syslog           (5), -- внутренние сообщения syslogd
           lpr              (6), -- сообщения подсистемы печати
           news             (7), -- сообщения подсистемы сетевых новостей
           uucp             (8), -- сообщения подсистемы UUCP
           cron             (9), -- сообщения демона часов
           authpriv         (10),-- сообщения системы защиты и проверки полномочий
           ftp              (11),-- сообщения демона ftp
           ntp              (12),-- сообщения подсистемы NTP
           audit            (13),-- сообщения аудита
           console          (14),-- консольные сообщения
           cron2            (15),-- сообщения демона часов
           local0           (16),
           local1           (17),
           local2           (18),
           local3           (19),
           local4           (20),
           local5           (21),
           local6           (22),
           local7           (23)
         }

SyslogSeverity  ::=  TEXTUAL-CONVENTION
    STATUS  current
    DESCRIPTION
        "В этих текстовых соглашениях перечислены уровни важности (Severity)
         сообщений syslog.

         Уровни Severity в сообщениях syslog указываются десятичными числами.
         Для взаимодействия и совместимости си совместимости с более
         ранними версиями данный документ задаёт нормативное отображение
         между метками, представляющими значения Severity и соответствующими
         числовыми кодами. Метки могут применяться, например, в пользовательских
         интерфейсах приложений SNMP.

         Метка зачастую семантически бессмысленна, поскольку неразумно пытаться
         перечислить все возможные варианты Severity, а критерии, используемые
         инициаторами syslog, исторически зависят от реализации.

         Отметим, что механизмы операционной системы для настройки syslog
         (например, файл syslog.conf) ещё не стандартизованы и могут применять
```

```
            разные наборы меток Severity  и/или их отображений на коды Severity.

            Например, приложение foobar может помечать сообщения как crit на
            основе некого субъективного критерия. Оператор может настроить syslog на
            пересылку сообщений, несмотря на то, что трактовка crit может различаться
            у разных инициаторов. Это обычная практика, поскольку инициаторы,
            трансляторы и коллекторы могут настраиваться на подобающую обработку
            таких ситуаций.
          "
        REFERENCE "Протокол Syslog (RFC5424): Таблица 2"
        SYNTAX  INTEGER
            {
              emerg           (0),  -- чрезвычайная ситуация, система не может использоваться
              alert           (1),  -- тревога, требуются незамедлительные действия
              crit            (2),  -- критическая ситуация
              err             (3),  -- ошибка
              warning         (4),  -- предупреждение
              notice          (5),  -- нормальная но важная ситуация (состояние)
              info            (6),  -- информационное сообщение
              debug           (7)   -- отладочное сообщение
            }
    END
```

4. Вопросы безопасности

Модуль не определяет каких-либо элементов управления, определены лишь текстовые соглашения, которые могут применяться другими модулями MIB для определения объектов управления. Значимые проблемы безопасности могут быть вызваны только модулями MIB, определяющими объекты управления. Следовательно, этот документ не оказывает влияния на безопасность Internet. Поскольку объекты, определённые с использованием описанных здесь TC, могут создавать проблемы безопасности, пользователям этих TC следует прочесть раздел «Вопросы безопасности» в [RFC5424].

5. Взаимодействие с IANA

Модули MIB в этом документе используют приведённое в таблице значение OBJECT IDENTIFIER, выделенное IANA и включённое в реестр SMI Numbers.

Дескриптор	*Значение OBJECT IDENTIFIER*
syslogTCMIB	{ mib-2 173 }

6. Литература

6.1. Нормативные документы

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

[RFC2578] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

6.2. Дополнительная литература

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

7. Благодарности

Этот документ является результатом работы группы Syslog. Автор благодарит Chris Lonvick, David Harrington, Juergen Schoenwaelder и Pasi Eronen за их комментарии и предложения.

Адрес автора

Glenn Mansfield Keeni
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-3204
Japan
Phone: +81-22-303-4012
EMail: glenn@cysols.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru