Network Working Group
Request for Comments: 5424
Obsoletes: 3164
Category: Standards Track

R. Gerhards
Adiscon GmbH

March 2009

Протокол Syslog

The Syslog Protocol

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

Тезисы

Этот документ описывает протокол syslog, который служит для передачи уведомлений о событиях. Протокол использует многоуровневую архитектуру, которая позволяет передавать сообщения syslog на основе разных транспортных протоколов. Обеспечивается формат сообщений, поддерживающий производителям добавлять фирменные расширения в структурированном виде.

Этот документ разрабатывался с учетом устройства традиционной системы syslog. Необходимость создания многоуровневой спецификации связана с тем, что для стандартизации надежных и безопасных расширения syslog остро не хватало документов типа Standards-Track и независимых от транспорта RFC. Без этого документа все прочие стандарты должны были бы определять свой формат пакетов syslog и механизм их доставки, что обязательно привело бы к проблемам совместимости. Многоуровневая архитектура обеспечивает прочную основу и позволяет за один раз создавать код для каждой функции syslog и вида транспорта.

Этот документ отменяет RFC 3164.

Оглавление

[1] В оригинале - IETF Contributions. *Прим. перев.*
[2] В оригинале - IETF Standards Process. *Прим. перев.*

1. Введение

Этот документ описывает многоуровневую архитектуру для службы syslog. Цель создания такой архитектуры заключается в том, чтобы отделить содержимое сообщений от их транспортировки и обеспечить возможность простого расширения для каждого уровня.

Документ описывает стандартный формат сообщений syslog и излагает концепция транспортных отображений. Описаны также структурированные элементы данных, которые могут применяться для передачи структурированной и простой для анализа информации, что позволяет производителям добавлять свои расширения.

Документ не описывает форматов хранения сообщений syslog, поскольку это выходит за рамки протокола syslog и не требуется для интероперабельности.

При разработке документа принимались во внимание исходные цели традиционного протокола syslog. Потребность в разработке новой многоуровневой модели обусловлена тем, что для стандартизации надежных и безопасных расширения syslog остро не хватало документов типа Standards-Track и независимых от транспорта RFC. Без этого документа все прочие стандарты должны были бы определять свой формат пакетов syslog и механизм их доставки, что обязательно привело бы к проблемам совместимости. Многоуровневая архитектура обеспечивает прочную основу и позволяет за один раз создавать код для каждой функции syslog и вида транспорта.

Документ отменяет RFC 3164, который включал информацию о некоторых имеющихся реализациях протокола.

2. Уровни требований

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 RFC 2119 [RFC2119].

3. Определения

Syslog использует три уровня, перечисленных ниже.

- «содержимое» (syslog content) — информация в сообщениях syslog;
- «приложение» (syslog application) — генерация, интерпретация, маршрутизация и хранение сообщений syslog;
- «транспорт» (syslog transport) — передача сообщений в «канал» и считывание из «канала».

На каждом концептуальном уровне выполняются некоторые функции, разделенные по ролям.

- «инициатор» (originator) генерирует содержимое для передачи в сообщениях syslog;
- «коллектор» (collector) собирает содержимое сообщений syslog для дальнейшего анализа;
- «транслятор» (relay) пересылает сообщения, воспринимает сообщения от инициатора или других трансляторов и передает их коллекторам или другим трансляторам;
- «транспортный отправитель» (transport sender) передает сообщения syslog заданному транспортному протоколу;
- «транспортный получатель» (transport receiver) принимает сообщения syslog от заданного транспортного протокола.

На рисунке 1 показаны уровни и роли.

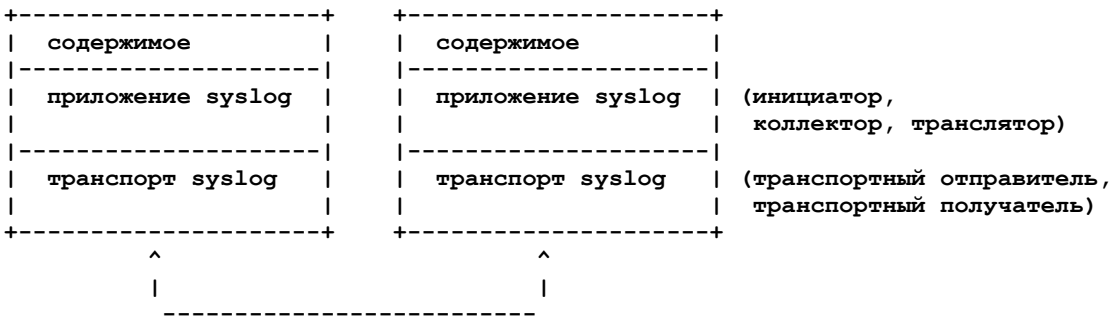

Рисунок 1. Уровни Syslog

4. Базовые принципы

Ниже перечислены принципы, применяемые к коммуникациям syslog.

- Протокол syslog не обеспечивает подтверждения доставки сообщений. Хотя некоторые виды транспорта могут сообщать о состоянии передачи, концептуально протокол syslog является симплексным (односторонним).
- Инициаторы и трансляторы можно настроить на передачу одного и того же сообщения множеству коллекторов и/или трансляторов.
- Инициатор, транслятор и коллектор могут функционально размещаться в одной системе.

4.1. Примеры развертывания

Примеры вариантов применения протокола показаны на рисунке 2, но возможны и другие варианты развертывания. Как видно из рисунка, трансляторы могут передавать все или некоторые сообщения, которые они получают, а также сообщения, которые они создают сами. Прямоугольниками на рисунке показаны поддерживающие syslog приложения.

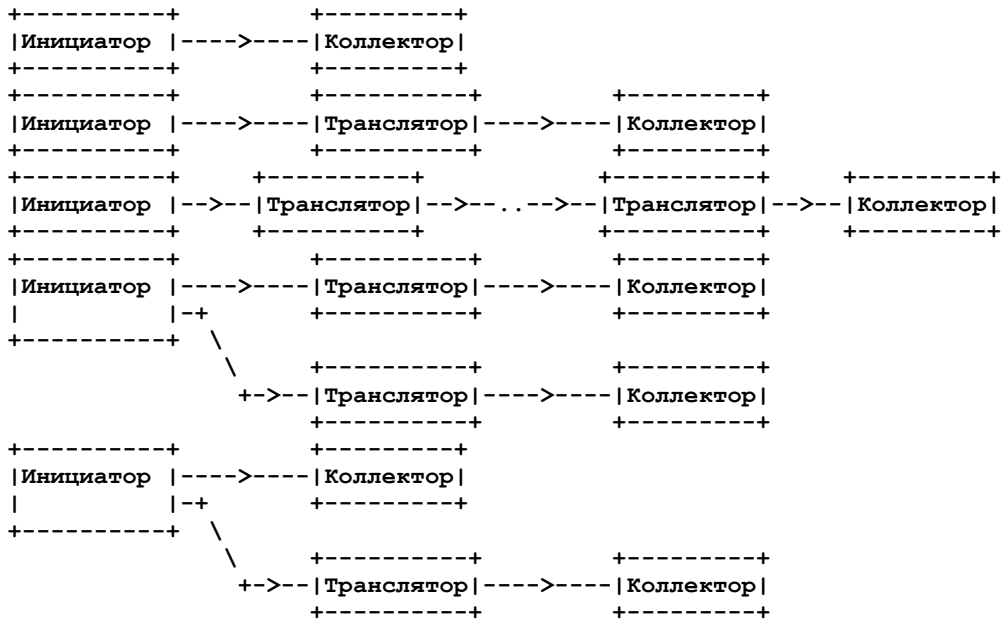

Рисунок 2. Некоторые варианты развертывания syslog.

5. Протокол транспортного уровня

Этот документ не задает какой-либо протокол транспортного уровня. Вместо этого описывается формат сообщений syslog, независимый от транспорта. Транспортные протоколы syslog определяются в других документах. Один из вариантов транспорта определен в [RFC5426] и согласуется с традиционным транспортом UDP. Этот транспорт нужен для поддержки интероперабельности, поскольку протокол UDP исторически применялся для передачи сообщений syslog.

Для любых транспортных протоколов syslog **недопустимо** преднамеренное изменение сообщений syslog. Если транспортному протоколу требуется выполнить временные преобразования у транспортного отправителя, эти преобразования **должны** быть обращены транспортным протоколом у транспортного получателя, чтобы коллектор или транслятор видел точную копию сообщения, созданного инициатором или транслятором. В противном случае будет нарушаться работа криптографических средств сквозной проверки (например, цифровых подписей). Изменение сообщений может происходить также в результате ошибок при передаче или иных проблем. Защита от таких изменений выходит за рамки этого документа.

5.1. Минимальные требования к транспортному отображению

Все реализации данной спецификации **должны** поддерживать транспорт на основе TLS, как описано в [RFC5425].

Все реализациям также **следует** поддерживать основанный на протоколе UDP транспорт, как описано в [RFC5426].

Реализациям **рекомендуется** использовать транспорт на базе TLS.

6. Формат сообщений Syslog

В сообщениях syslog используются определения ABNF [RFC5234], перечисленные ниже.

```
SYSLOG-MSG      = HEADER SP STRUCTURED-DATA [SP MSG]

HEADER          = PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID
PRI             = "<" PRIVAL ">"
PRIVAL          = 1*3DIGIT ; диапазон 0 .. 191
VERSION         = NONZERO-DIGIT 0*2DIGIT
HOSTNAME        = NILVALUE / 1*255PRINTUSASCII

APP-NAME        = NILVALUE / 1*48PRINTUSASCII
PROCID          = NILVALUE / 1*128PRINTUSASCII
MSGID           = NILVALUE / 1*32PRINTUSASCII

TIMESTAMP       = NILVALUE / FULL-DATE "T" FULL-TIME
FULL-DATE       = DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR   = 4DIGIT
DATE-MONTH      = 2DIGIT  ; 01-12
DATE-MDAY       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 в зависимости от месяца и года

FULL-TIME       = PARTIAL-TIME TIME-OFFSET
PARTIAL-TIME    = TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND [TIME-SECFRAC]
TIME-HOUR       = 2DIGIT  ; 00-23
TIME-MINUTE     = 2DIGIT  ; 00-59
TIME-SECOND     = 2DIGIT  ; 00-59
TIME-SECFRAC    = "." 1*6DIGIT
TIME-OFFSET     = "Z" / TIME-NUMOFFSET
TIME-NUMOFFSET  = ("+" / "-") TIME-HOUR ":" TIME-MINUTE

STRUCTURED-DATA = NILVALUE / 1*SD-ELEMENT
SD-ELEMENT      = "[" SD-ID *(SP SD-PARAM) "]"
SD-PARAM        = PARAM-NAME "=" %d34 PARAM-VALUE %d34
```

```
SD-ID           = SD-NAME
PARAM-NAME      = SD-NAME
PARAM-VALUE     = UTF-8-STRING ; для символов '"', '\' и ']' ДОЛЖНО использоваться
                               ; специальное представление
SD-NAME         = 1*32PRINTUSASCII ; кроме '=', SP, ']', %d34 (")

MSG             = MSG-ANY / MSG-UTF8
MSG-ANY         = *OCTET ; не начинается с BOM
MSG-UTF8        = BOM UTF-8-STRING
BOM             = %xEF.BB.BF
UTF-8-STRING    = *OCTET ; строка UTF-8 в соответствии с RFC 3629

OCTET           = %d00-255
SP              = %d32
PRINTUSASCII    = %d33-126
NONZERO-DIGIT   = %d49-57
DIGIT           = %d48 / NONZERO-DIGIT
NILVALUE        = "-"
```

6.1. Размер сообщения

Ограничения на размер сообщений syslog диктуются используемым для syslog транспортным отображением. Сам по себе верхний предел не существует. Каждое транспортное отображение определяет нижний предел поддерживаемого максимального размера сообщений и это значение **должно** быть не менее 480 октетов.

Любой транспортный получатель **должен** обеспечивать восприятие сообщений размером до 480 октетов, включительно. Всем реализациям транспортных получателей **следует** воспринимать сообщения размером до 2048 октетов, включительно. Транспортные получатели **могут** принимать сообщения размером более 2048 октетов. Если транспортный получатель принимает сообщение, размер которого превышает поддерживаемое им значение, получателю **следует** отсечь часть данных в этом сообщении до приемлемого размера. **Возможно** также отбрасывание таких сообщений.

Если транспортный получатель отсекает часть сообщения, отбрасываться **должна** последняя часть сообщения (конец). Отсечка сообщения **может** вызвать повреждение кодировки UTF-8 или данных STRUCTURED-DATA. Транспортный получатель **может** отбросить такое сообщение или попытаться его обработать.

6.2. HEADER

В заголовке (HEADER) **должен** использоваться 7-битовый набор символов ASCII в 8-битовых полях, как описано в [RFC5234]. Код ASCII определен в USA Standard Code for Information Interchange [ANSI.X3-4.1968].

Формат заголовка должен обеспечивать некоторую совместимость со старыми системами BSD syslog (см. Приложение A.1).

6.2.1. PRI

В PRI **должно** быть от 3 до 5 символов, первый и последний из которых являются угловыми скобками. PRI начинается с левой скобки < (знак «меньше», %d60), за которым следует число и правая угловая скобка > (знак «больше», %d62). Число в угловых скобках называют приоритетом (Priority, PRIVAL) и представляет как источник (Facility), так и важность (Severity). Priority может включать от одной до трех десятичных цифр (ABNF DIGITS), которые могут принимать значения от %d48 (для 0) до %d57 (для 9).

Значения Facility и Severity не являются нормативными, но используются часто. Эти значения приведены ниже в таблице только для справки. Значения Facility должны относиться к диапазону от 0 до 23, включительно.

Таблица 1. Источники сообщений syslog

Код	***Источник (значимость)***
0	Сообщения ядра
1	Сообщения пользовательского уровня
2	Почтовая система
3	Системные службы (демоны)
4	Сообщения, связанные с защитой и предоставлением полномочий
5	Внутренние сообщения syslogd
6	Подсистема печати (line printer)
7	Подсистема сетевых новостей (network news)
8	Подсистема UUCP
9	Часы (демон)
10	Сообщения, связанные с защитой и предоставлением полномочий
11	Демон FTP
12	Подсистема NTP
13	Аудит (log audit)

14	Сигнал (log alert)
15	Часы (демон)
16	Локальное (local0)
17	Локальное (local1)
18	Локальное (local2)
19	Локальное (local3)
20	Локальное (local4)
21	Локальное (local5)
22	Локальное (local6)
23	Локальное (local7)

В каждом сообщении Priority также включает десятичные индикатор уровня важности (Severity). Значения важности и описания приведены в таблице. Severity **должны** относиться к диапазону от 0 до 7, включительно.

Таблица 2. Уровни важности сообщений syslog

Код	***Уровень важности***
0	Emergency - чрезвычайная ситуация, система не может использоваться
1	Alert - тревога, требуются незамедлительные действия
2	Critical - критическая ситуация
3	Error - ошибка
4	Warning - предупреждение
5	Замечание, нормальная но важная ситуация (состояние)
6	Informational - информационное сообщение
7	Debug — отладочное сообщение

Значение Priority рассчитывается по формуле 8 * Facility + Severity. Например, для сообщения ядра (Facility=0) с уровнем важности Emergency (Severity=0) будет Priority = 0. А для сообщения local4 (Facility=20) с уровнем важности Notice (Severity=5) мы получим Priority = 165. В PRI сообщения syslog эти значения будут указываться в виде <0> и <165>, соответственно. За угловой скобкой число 0 указывается только для случая Priority = 0, а в остальных случаях использовать символ в начале поля **недопустимо**.

6.2.2. VERSION

Поле VERSION указывает версию спецификации протокола syslog. Номер версии **должен** увеличиваться для любой новой спецификации, меняющей любую часть формата HEADER. К таким изменениям относятся добавление или удаление полей, а также изменение синтаксиса или семантики имеющихся полей. Данный документ устанавливает VERSION = 1. Значения VERSION выделяются агентством IANA (параграф 9.1) по процедуре Standards Action, описанной в [RFC5226].

6.2.3. TIMESTAMP

Поле TIMESTAMP содержит формализованную временную метку [RFC3339].

Хотя [RFC3339] разрешает множество вариантов синтаксиса, данный документ вносит дополнительные ограничения. Поле TIMESTAMP **должно** соответствовать приведенным ниже требованиям:

- символы T и Z **должны** использовать верхний регистр (заглавные буквы);
- использование символа T **обязательно**;
- **недопустимо** использовать високосные секунды.

Инициатору **следует** включать TIME-SECFRAC, если это позволяют точность часов и производительность. Параметр timeQuality SD-ID, описанный в параграфе 7.1, позволяет инициатору задать точность и достоверность временных меток.

Приложения syslog **должны** использовать NILVALUE в качестве TIMESTAMP при неспособности syslog получить системное время.

6.2.3.1. Примеры

Пример 1

```
1985-04-12T23:20:50.52Z
```

Это значение представляет время 20 минут 50,52 сек. после 23 часов 12 апреля 1985 года для часового пояса UTC.

Пример 2

```
1985-04-12T19:20:50.52-04:00
```

Здесь представлен тот же момент, что в примере 1, но время указно для часового пояса US Eastern Standard Time (с учетом летнего времени).

Пример 3

```
2003-10-11T22:14:15.003Z
```

Это значение представляет 11 октября 2003 года, 10:14:15 после полудня и 3 мсек. следующей секунды для часового пояса UTC. Временная метка обеспечивает миллисекундное разрешение. Создатель метки может иметь более высокое разрешение, но ограничение дробной части секунд тремя цифрами не позволяет задать время с большей точностью.

Пример 4

```
2003-08-24T05:14:15.000003-07:00
```

Это значение представляет 24 августа 2003 года, 05:14:15 до полудня и 3 мксек. Следующей секунды. Микросекундное разрешение указывается дополнительными цифрами в TIME-SECFRAC. Метка относится к часовому поясу -7 по отношению к UTC. Такая метка может быть создана для часового пояса US Pacific в период действия летнего времени.

Пример 5 — неприемлемая метка TIMESTAMP

```
2003-08-24T05:14:15.000000003-07:00
```

Эта метка похожа на показанную в примере 4, но TIME-SECFRAC указывает время в наносекундах. В результате размер TIME-SECFRAC превышает дозволенные 6 цифр, что делает метку неприемлемой.

6.2.4. HOSTNAME

Поле HOSTNAME указывает машину, котоая была исходным отправителем сообщения syslog.

В поле HOSTNAME **следует** включать имя хоста или полное доменное имя инициатора в формате, заданном STD 13 [RFC1034]. Этот формат в данном документе называется FQDN[1].

На практике не все приложения syslog способны предоставлять FQDN. По этой причине в полях HOSTNAME **могут** указываться другие значения. В данном документе содержатся предложения по использованию других значений в таких ситуациях. Приложению syslog **следует** выбирать наиболее конкретное (специфичное) значение из числа представленных ниже в порядке снижения предпочтений (специфичности):

1. FQDN;
2. статический адрес IP;
3. имя хоста (hostname);
4. динамический адрес IP;
5. NILVALUE.

При использовании адреса IPv4 он **должен** указываться в форме десятичных чисел, разделенных точками, как указано в STD 13 [RFC1035]. Если используется адрес IPv6, он **должен** указываться в корректном текстовом представлении, как описано в параграфе 2.2 [RFC4291].

Приложениям syslog **следует** использовать в поле HOSTNAME одно и то же имя, пока это возможно.

Значение NILVALUE **следует** применять только в тех случаях, когда приложение syslog не имеет возможности получить реальное имя хоста. Такие ситуации считаются крайне нежелательными.

6.2.5. APP-NAME

В полях APP-NAME **следует** указывать устройство или приложение, создавшее это сообщение. Поле представляет собой строку без дополнительной семантики и предназначено для фильтрации сообщений на трансляторах и коллекторах.

Если приложение syslog не знает своего имени для APP-NAME или не может предоставить такую информацию, **можно** использовать NILVALUE. Устройство может оказаться не способным предоставить эту информацию в силу ограничений локальной политики, а также в результате недоступности информации или ее неприменимости к данному устройству.

Это поле **может** присваиваться оператором.

6.2.6. PROCID

Значения PROCID, включаемые в сообщения, не имеют переносимого (за пределы локальной системы) смысла и могут лишь в некоторых случаях показывать прерывание работы syslog. Поле не имеет какого-либо конкретного синтаксиса и семантики — оно зависит от реализации и/или оператора. При отсутствии идентификатора **может** указываться значение NILVALUE.

Поле PROCID часто применяется для указания имени или идентификатора процесса, связанного с системой syslog. При недоступности имени и идентификатора может указываться значение NILVALUE. На встраиваемых системах без идентификаторов процесса в ОС в качестве PROCID может служить идентификатор перезагрузки.

PROCID может обеспечивать анализаторам возможность зафиксировать перерывы в работе syslog по изменению идентификатора процесса syslog. Однако PROCID не обеспечивает надежной идентификации перезагрузки, поскольку в таких случаях процесс syslog может получить такой же идентификаторв, который был у предыдущего экземпляра syslog.

PROCID может также применяться для идентификации сообщений, относящихся к той или иной группе. Например, агент SMTP MTA[2] может помещать идентификатор транзакции SMTP в поле PROCID, что позволит коллекторам и трансляторам группировать сообщения по идентификатору транзакции SMTP.

[1]Fully Qualified Domain Name — полное доменное имя.
[2]Mail transfer agent – агент передачи электронной почты.

6.2.7. MSGID

В поле MSGID **следует** указывать тип сообщения. Например, межсетевой экран может указывать в поле MSGID значение TCPIN для входящего трафика TCP и TCPOUT для исходящего. Сообщения с одинаковыми полями MSGID должны отражать события с одинаковой семантикой. Само поле MSGID является текстовой строкой без дополнительной семантики и предназначено для фильтрации сообщений на трансляторах и коллекторах.

Если приложение syslog не может предоставить какого-либо значения для этого поля, **следует** использовать NILVALUE.

Это поле **может** присваиваться оператором.

6.3. STRUCTURED-DATA

Механизм STRUCTURED-DATA обеспечивает представление информации в четко определенном, легко читаемом и интерпретируемом формате. Имеется множество вариантов использования этого механизма. Например, с его помощью можно указать метаданные о сообщении syslog или специфическую для приложения информацию типа счетчиков трафика или адресов IP.

Структура STRUCTURED-DATA может содержать множество структурированных элементов данных, которые обозначаются далее SD-ELEMENT.

Если структура не содержит структурированных элементов данных, в поле STRUCTURED-DATA **должно** помещаться значение NILVALUE.

Данные в STRUCTURED-DATA **должны** представляться в 7-битовой кодировке ASCII, как описано в [RFC5234]. Коды ASCII определены с USA Standard Code for Information Interchange [ANSI.X3-4.1968]. Исключением является поле PARAM-VALUE (параграф 6.3.3), в котором **должна** использоваться кодировка UTF-8.

Коллектор **может** игнорировать некорректно сформированные элементы STRUCTURED-DATA, транслятор **должен** пересылать такие поля STRUCTURED-DATA в неизменном виде.

6.3.1. SD-ELEMENT

Элемент данных SD-ELEMENT состоит из имени и пар «имя - значение». Имя обозначается SD-ID, пары «имя — значение» - SD-PARAM.

6.3.2. SD-ID

Регистр символов в SD-ID принимается во внимание и эти поля служат уникальными идентификаторами типа и назначения SD-ELEMENT. В одном сообщении **недопустимо** наличие одинаковых SD-ID.

Для имен SD-ID используются два формата, описанных ниже.

- Имена, не содержащие символа @ (ABNF %d64), зарезервированы для распределения по процедуре IETF Review, описанной в BCP26 [RFC5226]. Определенные к настоящему моменту имена описаны в разделе 7. Имена такого формата применимы лишь после регистрации в IANA. В зарегистрированных именах **недопустимо** наличие символов @ (ABNF %d64), = (ABNF %d61),] (ABNF %d93), " (ABNF %d34), пробелов и символов управления (символы ASCII с кодами 127 и от 0 до 32).
- Кто угодно может определить дополнительные SD-ID, используя формат name@<private enterprise number> (например, ourSDID@32473). Формат имени слева от символа @ не задается, однако эти имена **должны** представлять строки печатных символов US-ASCII и в них **недопустимо** включать символы @ (ABNF %d64), = (ABNF %d61),] (ABNF %d93), " (ABNF %d34), пробелов и символы управления. Справа от символа @ **должен** указываться фирменный номер (private enterprise number), как описано в параграфе 7.2.2. В этом документе в качестве такого номера используется строка 32473. Это значение было выделено IANA для использования в качестве примеров в документации. Разработчики должны использовать выделенное им значение номера при создании локально расширяемых имен SD-ID.

6.3.3. SD-PARAM

Каждая структура SD-PARAM состоит из имени (PARAM-NAME) и значения (PARAM-VALUE).

Регистр символов в PARAM-NAME принимается во внимание. Агентство IANA контролирует выделение значений PARAM-NAME, за исключением имен в SD-ID, содержащих символ @. Область действия PARAM-NAME находится внутри конкретного SD-ID. Таким образом, одинаковые имена PARAM-NAME в разных SD-ID не совпадают.

Для поддержки разных языков в поле PARAM-VALUE **должна** применяться кодировка UTF-8. Приложение syslog **может** ввести любую корректную последовательность UTF-8. Приложения syslog **должны** воспринимать любые корректные последовательности UTF-8 в «кратчайшей форме». **Недопустимы** отказы по причине наличия в PARAM-VALUE управляющих символов. Приложение syslog **может** менять сообщения с управляющими символами (например, заменяя октеты со значением 0 (USASCII NUL) четырьмя символами #000). По причинам, описанным в параграфе 3.1 UNICODE TR36 [UNICODE-TR36], инициатор **должен** представлять сообщения в «кратчайшей форме» (shortest form), а коллекторам **недопустимо** интерпретировать сообщения, не имеющие «кратчайшей формы» (non-shortest form).

В PARAM-VALUE для символов " (ABNF %d34), \ (ABNF %d92) и] (ABNF %d93) **должно** использоваться escape-представление, требуемое для предотвращения ошибок при разборе. Использование escape-представления для символа] не является строго обязательным, но данная спецификация **требует** это для предотвращения ошибок при реализации приложений syslog. Для из этих трех символов **должно** использоваться представление \", \\ и \], соответственно. Escape-представление символа \ применяется для согласованности с другими частями сообщений syslog, а также с традиционными приложениями syslog.

Символ \, за которым не следует ни одного из указанных выше трех символов, рассматривается, как неприемлемая escape-последовательность. В таких случаях этот и следующий за ним символ **должны** трактоваться, как обычные символы. Таким образом, некорректная последовательность не изменяется.

SD-PARAM **может** неоднократно повторяться в одном SD-ELEMENT.

6.3.4. Контроль изменений

После определения SD-ID и PARAM-NAME менять синтаксис и семантику этих объектов **недопустимо**. Если нужно изменить существующий объект, **должны** создаваться новые SD-ID или PARAM-NAME , а старые сохраняться неизменными. К существующим SD-ID **можно** добавить **необязательные** (опциональные) PARAM-NAME.

6.3.5. Примеры

Во всех примерах этого параграфа показана лишь структурированная часть сообщений. Каждый пример следует рассматривать как одну строку, которая в документе может быть разбита на несколько с целью удобочитаемости. Пояснения даны после примеров.

Пример 1 - корректно

```
[exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"]
```

Этот пример показывает структурированный элемент данных с неконтролируемым IANA SD-ID типа exampleSDID@32473, имеющим три параметра.

Пример 2 - корректно

```
[exampleSDID@32473 iut="3" eventSource="Application"
eventID="1011"][examplePriority@32473 class="high"]
```

Аналогично примеру 1, но включает второй структурированный элемент данных, который следует сразу же за первым (без SP между ними).

Пример 3 - некорректно

```
[exampleSDID@32473 iut="3" eventSource="Application"
eventID="1011"] [examplePriority@32473 class="high"]
```

Этот пример похож на предыдущий, но включает небольшую ошибку — между двумя структрированными элементами данных имеется пропуск (]SP[). Это некорректно и приводит к тому, что поле STRUCTURED-DATA будет заканчиваться после первого элемента, а второй будет интерпретироваться, как часть поля MSG.

Пример 4 - некорректно

```
[ exampleSDID@32473 iut="3" eventSource="Application"
eventID="1011"][examplePriority@32473 class="high"]
```

Этот пример почти совпадает с примером 2, но включает другую ошибку — символ SP после начальной скобки. Структурированный элемент SD-ID **должен** следовать сразу же после открывающей скобки, поэтому наличие пропуска (SP) делает поле STRUCTURED-DATA неприемлемым. Приложение syslog **может** отбросить такое сообщение.

Пример 5 - корректно

```
[sigSig ver="1" rsID="1234" ... signature="..."]
```

Пример 5 является корректным и показывает гипотетический SD-ID, выделенный IANA. Точки в этом примере применены для сокращения.

6.4. MSG

Компонента MSG содержит сообщение в свободной форме с информацией о событии.

В MSG **следует** использовать кодировку UNICODE в варианте UTF-8, как описано в [RFC3629]. Если приложение syslog не может представить MSG в Unicode, оно **может** воспользоваться любой другой кодировкой.

Приложениям syslog **следует** избегать включения октетов со значениями меньше 32 (диапазон символов управления традиционной кодировки US-ASCII за исключением DEL). Эти значения разрешены, но приложения syslog **могут** менять такие символы при получении. Например, они могут быть заменены escape-последовательностями (т. е., 0 может смениться на \0). Приложениям syslog **не следует** менять значения каких-либо иных октетов.

Если приложение syslog представляет MSG в кодировке UTF-8, строка **должна** начинаться с маски BOM[1], которая для UTF-8 представляет собой ABNF %xEF.BB.BF. Приложение syslog **должно** использовать «кратчайшую форму» (shortest form) и **может** применять любые корректные последовательности UTF-8.

Если приложение syslog обрабатывает строку MSG, начинающуюся с BOM и MSG содержит UTF-8 не в кратчайшей форме, **недопустимо** интерпретировать MSG, как строку в кодировке UTF-8 по причинам, указанным в параграфе 3.1 [UNICODE-TR36]. Рекомендации для таких случаев приведены в Приложении A.8.

В соответствии с UNICODE TR36 [UNICODE-TR36] приложению syslog **недопустимо** интерпретировать сообщения, которые не имеют кратчай1шей формы. Им **недопустимо** также интерпретировать некорректные последовательности UTF-8.

6.5. Примеры

Ниже приведены примеры корректных сообщений syslog, сопровожденные описаниями. Примеры основаны на похожих примерах из [RFC3164] и могут быть знакомы читателям. Непечатаемая маска Unicode BOM в примерах обозначена последовательностью BOM.

Пример 1 — без STRUCTURED-DATA

[1]Unicode byte order mask – маска порядка байтов Unicode.

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47
- BOM'su root' failed for lonvick on /dev/pts/8
```

В этом примере VERSION имеет значение 1, Facility — 4, а Severity - 2. Сообщение было создано 11 октября 2003 года в 10:14:15 после полудня по времени UTC, плюс 3 мсек следующей секунды. Сообщение исходит от хоста, который идентифицирует себя именем mymachine.example.com. Поле APP-NAME имеет значение su, PROCID не известно, а MSGID - ID47. Компонента MSG является строкой **su root' failed for lonvick...** в кодировке UTF-8, указанной BOM. Структурированных данных в сообщении нет, это показано символом «-» в поле STRUCTURED-DATA.

Пример 2 - без STRUCTURED-DATA

```
<165>1 2003-08-24T05:14:15.000003-07:00 192.0.2.1
myproc 8710 - - %% It's time to make the do-nuts.
```

В этом примере VERSION снова имеет значение 1, Facility - 20, а Severity 5. Сообщение было создано 24 августа 2003 года в 5:14:15 до полудня по времени -7 часов относительно UTC, плюс 3 мксек следующей секунды. Поле HOSTNAME содержит адрес 192.0.2.1, поскольку приложение syslog не знает имени FQDN и указало вместо него один из адресов IPv4. Поле APP-NAME имеет значение myproc, а PROCID = 8710 (это может быть, например, UNIX PID). STRUCTURED-DATA нет в сообщении, что показано символом «-» в поле STRUCTURED-DATA. Идентификатора сообщения (MSGID) нет и это показано символом «-» в поле MSGID.

Текст сообщения **%% It's time to make the do-nuts.** Не включает Unicode BOM и приложение syslog не знает кодировки компоненты MSG.

Пример 3 - со STRUCTURED-DATA

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog - ID47 [exampleSDID@32473 iut="3" eventSource=
"Application" eventID="1011"] BOMAn application event log entry...
```

Этот пример создан на основе примера 1, однако в нем содержится структура STRUCTURED-DATA с одним элементом [exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"]. Само сообщение (MSG) является строкой **An application event log entry...** в кодировке UTF-8, указанной BOM.

Пример 4 — только STRUCTURED-DATA

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog - ID47 [exampleSDID@32473 iut="3" eventSource=
"Application" eventID="1011"][examplePriority@32473 class="high"]
```

Этот пример показывает сообщение со STRUCTURED-DATA, но без MSG. Такие сообщения допускаются.

7. Идентификаторы структурированных данных

В этом разделе описаны изначально зарегистрированные IANA значения SD-ID. Определение структурированных элементов данных приведено в параграфе 6.3. Все определенные здесь SD-ID являются **необязательными** (OPTIONAL).

Для некоторых из этих параметров указан максимальный размер значения в символах. В каждом из таких случаев приложение syslog **должно** быть готово получить указанное число символов в любом корректном варианте UTF-8. Поскольку один символ может занимать до 6 октетов, приложениям syslog **рекомендуется** быть готовыми принять до 6 октетов на символ.

7.1. timeQuality

Элемент timeQuality в SD-ID **может** использоваться инициатором для описания своего понимания системного времени. Этот SD-ID **следует** включать, если инициатор не имеет должной синхронизации с надежным внешним источником точного времени или не знает корректного часового пояса. Основным применением этого элемента структурированных данных является предоставления сведений об уровне доверия к значению TIMESTAMP (см. параграф 6.2.3). Все параметры этого элемента являются **необязательными**.

7.1.1. tzKnown

Параметр tzKnown показывает, известен ли инициатору часовой пояс. При известном часовом поясе **должно** указываться значение 1. Если информация о часовом поясе сомнительна, **должно** указываться значение 0. Если инициатор знает часовой пояс, но хочет указывать время в формате UTC, он **должен** указать значение 1 (часовой пояс известен).

7.1.2. isSynced

Параметр isSynced говорит о наличии синхронизации с надежным внешним источником синхронизации (например, по протоколу NTP). Если время инициатора синхронизировано, он **должен** указывать значение 1, в противном случае **должно** указываться значение 0.

7.1.3. syncAccuracy

Параметр syncAccuracy показывает представление инициатора о точности синхронизации его часов. Этот параметр указывается целым числом, показывающим максимальное число микросекунд, на которое может отклоняться системное время за интервал между двумя последовательными синхронизациями.

При isSynced = 0 **недопустимо** указывать этот параметр. Если isSynced = 1, но параметр syncAccuracy не указан, коллектор или транслятор будет предполагать точность синхронизации достаточной. Параметр syncAccuracy **должен** указываться только в тех случаях, когда инициатор имеет данные о надежности внешнего источника точного времени. В большинстве случаев такую информацию извлекают из конфигурации оператора.

7.1.4. Примеры

Приведенный ниже пример отражает ситуацию, когда инициатор не знает часового пояса и не использует синхронизацию.

```
[timeQuality tzKnown="0" isSynced="0"]
```

Таким образом инициатор показывает неточность своих временных меток. Это может служить рекомендацией для коллекторов и трансляторов по использованию своего локального времени взамен TIMESTAMP из сообщения, если нужно сопоставление сообщений от различных инициаторов.

Ниже приведен пример сообщений от инициатора, знающего часовой пояс и синхронизированного от надежного внешнего источника.

```
[timeQuality tzKnown="1" isSynced="1"]
```

В следующем примере инициатор также знает часовой пояс и надежно синхронизирован, а также знает точность своей синхронизации.

```
[timeQuality tzKnown="1" isSynced="1" syncAccuracy="60000000"]
```

Разница между двумя предыдущими примерами заключается в том, что во втором случае инициатор предполагает, что его локальное время отклоняется от «истинного» не более, чем на 60 секунд. Таким образом, если инициатор указывает 9:00:00, это говорит, событие произошло не ранее 8:59:00 и не позднее 9:01:00.

7.2. origin

Элемент origin в SD-ID **может** служить для индикации инициатора сообщения syslog. Ниже описаны параметры элемента. Все эти параметры являются **необязательными**.

Указание любого из описанных ниже параметров предназначено прежде всего для анализаторов журналов событий и аналогичных приложений.

7.2.1. ip

Параметр ip указывает IP-адрес, известный инициатору в момент создания сообщения. Этот параметр **должен** содержать текстовое представление адреса IP, как описано в параграфе 6.2.4.

Параметр может использоваться для предоставления идентификационных сведений, дополняющих данные поля HOSTNAME. Особенно полезен этот параметр в тех случаях, когда адрес IP включен в сообщение, но поле HOSTNAME содержит имя FQDN. Полезен этот параметр и для описания адресов IP на многодомных хостах.

Если у инициатора множество адресов IP, он **может** включить в параметр ip один из таких адресов и **может** также указать множество параметров ip в одном элементе структурированных данных origin.

7.2.2. enterpriseId

Параметр enterpriseId **должен** содержать код SMI Network Management Private Enterprise Code, поддерживаемый IANA, с префиксом iso.org.dod.internet.private.enterprise (1.3.6.1.4.1). Следующее за префиксом значение **должно** быть уникальным, а также **должно** быть зарегистрировано в IANA в соответствии с RFC 2578 [RFC2578]. Предприятия имеют полномочия выделять значения только в субдереве iso.org.dod.internet.private.enterprise.<private enterprise number>, выделенном IANA этому предприятию. Параметр enterpriseId **должен** содержать только значение из субдерева iso.org.dod.internet.private.enterprise.<private enterprise number>. В общем случае требуется лишь выделенный IANA номер (одно значение). Предприятие может использовать дополнительные субидентификаторы после выделенного предприятию номера. Такие субидентификаторы **должны** разделяться точками и представляться в десятичном формате. Примерм может служить номер 32473.1.2. Следует отметить, что идентификатор 32473.1.2 служит примером и применять его на практике **недопустимо**. Полный список актуальных номеров PEN[1] поддерживается IANA.

Указывая идентификатор предприятия можно дополнительно конкретизировать обработку сообщения.

7.2.3. software

Параметр software служит уникальным идентификатором программы, создавшей сообщение. При использовании этого параметра **следует** указывать также enterpriseId для идентификации производителя программы. Параметр software не совпадает с полем заголовка APP-NAME и всегда **должен** содержать имя создавшей сообщение программы, тогда как в APP-NAME может включаться любое имя, включая заданное оператором значение.

Параметр software представляет собой строку. **Недопустимо** использовать в этой строке более 48 символов.

7.2.4. swVersion

Параметр swVersion уникально идентифицирует версию программы, создавшей сообщение. Если этот параметр используется, **следует** также указывать параметры software и enterpriseId.

Параметр swVersion представляет собой строку. **Недопустимо** использовать в этой строке более 32 символов.

7.2.5. Пример

Ниже приведен пример с указанием двух адресов IP.

```
[origin ip="192.0.2.1" ip="192.0.2.129"]
```

В этом примере инициатор указывает наличие у него двух адресов IP - 192.0.2.1 и 192.0.2.129.

[1]Private Enterprise Numbers.

7.3. meta

Элемент meta в SD-ID **может** служить для предоставления мета-данных о сообщении. Параметры этого элемента описаны ниже, все параметры являются **необязательными** (OPTIONAL). При использовании элемента meta в SD-ID **следует** включить хотя бы один параметр.

7.3.1. sequenceId

Параметр sequenceId служит для отслеживания порядка, в котором инициатор отправляет сообщения транспорту syslog для передачи. Этот параметр является целым числом, для которого **должно** устанавливаться значение 1 при запуске функции syslog. Значение параметра **должно** увеличиваться для каждого последующего сообщения. Максимальное значение номера составляет 2147483647 и при достижении максимума следующее сообщение **должно** получать номер 1.

7.3.2. sysUpTime

Параметр sysUpTime **может** использоваться для включения в параметр SNMP sysUpTime в сообщении. Синтаксис и семантика параметра определены в [RFC3418].

Протокол syslog не поддерживает напрямую синтаксис SNMP INTEGER и значение **должно** представляться в десятичном формате (без десятичной точки) с использованием только символов 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9.

Смысл параметра указан в RFC 3418, как «время (в сотых долях секунды) с момента, когда связанная с сетевым управленим часть системы была в последний раз реинициализирована». Это, естественно, относится к связанной с SNMP частью управления системой, которая **может** не совпадать с той частью системы управления, которая связана с syslog.

7.3.3. language

Параметр language **может** использоваться инициатором для указания естественного языка, применяемого в поле MSG. Если параметр используется, он **должен** содержать идентификатор языка, определенный в BCP 47 [RFC4646].

8. Вопросы безопасности

8.1. Кодировка UNICODE

Этот документ задает использование кодировки UTFдля полей PARAM-VALUE и MSG. С кодировкой UNICODE связано множество проблем безопасности. Всем разработчикам и операторам следует внимательно прочесть документ UNICODE TR36 [UNICODE-TR36] (UTR36), в котором рассмотрены эти проблемы. Данный документ защищает от технических проблем, описанных в UTR36, **требуя** применять «кратчайшую форму» (shortest form) кодирования для приложений syslog. Однако возможность путаницы, связанной с одинаковым изображением разных символов, сохраняется. Этот документ пытается минимизировать влияние данной проблемы, разрешая использовать UNICODE только там, где ожидаются и требуются локальные сценарии (script). Во всех прочих полях **требуется** использовать кодировку US-ASCII. Кроме того, поля PARAM-VALUE и MSG не следует рассматривать в качестве основного источника идентификационной информации и это позволит дополнительно снизить риск, связанный с одинаковым изображением разных символов.

8.2. Управляющие символы

Этот документ не вносит каких-либо обязательных для исполнения ограничений на содержимое MSG и PARAM-VALUE. Поэтому данные поля **могут** содержать символы управления, включая NUL.

В некоторых языках программирования (прежде всего, C и C++) символ NUL (ABNF %d00) традиционно применяется в качестве завершения строки. Большинство реализаций этих языков предполагают, что строка завершается первым NUL-символом. Это ограничение отражается прежде всего на использовании библиотек. Данное ограничение часто переносится на прикладные программы и языки сценариев, написанные с использованием упомянутых языков. Таким образом, символы NUL требуют внимательного отношения и аккуратной обработки. Атакующий может преднамеренно включить символы NUL для сокрытия расположенной после них информации. Некорректная обработка NUL-символов может также приводить к искажению контрольных сумм, передаваемых внутри сообщений.

Многие популярные текстовые редакторы также написаны на языках с упомянутым ограничением. Целесообразно кодировать NUL-символы при записи текстовых файлов. Если записывать эти символы без специального представления, файл может оказаться непригодным для чтения.

Другие символы управления также могут создавать проблемы. Например, атакующий может преднамеренно включать символы «забоя» (backspace), чтобы сделать часть сообщения не читаемой. Подобные проблемы возникают почти для всех управляющих символов.

Кроме того, атакующий может использовать недопустимые последовательности UTF-8 для вставки управляющих символов ASCII.

Данная спецификация разрешает приложениям syslog переформатировать полученные управляющие символы. Это обусловлено, в частности, значительными рисками, связанными с управляющими символами. Инициаторам следует принимать во внимание, что при использовании ими кодировок, отличных от ASCII и UTF8, получатель может «повредить» сообщение при попытке отфильтровать управляющие символы ASCII.

8.3. Отсечка сообщений

Отсечка (укорачивание) сообщений может быть использовано злоумышленниками для сокрытия важной информации. Сообщения, размер которых превышает поддерживаемый минимум, могут отбрасываться или укорачиваться транспортными получателями. Это может вести к потере информации.

Для предотвращения потерь информации следует делать размер сообщений не превышающим минимальное значение разрешенного максимального размера сообщений, указанное в параграфе 6.1. Для повышения эффективности и надежности размер сообщений следует сокращать до приемлемого минимума. Важную информацию следует размещать в начале сообщения, поскольку вероятность ее утраты при отсечке на транспортых получателях с ограничениями по размеру в этом случае будет меньше.

Инициаторам следует ограничивать размер представленных пользователем данных в сообщении syslog. Если этого не сделать, атакующий сможет передавать большие объемы данных в надежде воспользоваться возможной слабостью.

8.4. Повторное использование сообщений

В протоколе syslog нет механизмов детектирования повторного применения сообщений (replay). Атакующий может записать набор сообщений, показывающих нормальную работу машины. Позднее он может удалить данную машину из сети и отправить собранные сообщения syslog транслятору или коллектору. Даже с учетом поля TIMESTAMP в заголовке (HEADER) атакующий может записать пакеты и просто изменить временные метки в соответствии с текущим временем, а потом повторно передать сообщения. Администраторы могут не заметить ничего необычного в полученных сообщениях и ошибочно трактовать их получение как признак нормальной работы машины.

Криптографические подписи в сообщениях могут предотвратить изменение полей TIMESTAMP и атак с повторным использованием пакетов.

8.5. Гарантии доставки

Поскольку в этом документе не описан механизм гарантированной доставки, а нижележащий транспорт (например, UDP) может быть ненадежным, часть сообщений может теряться. Сообщения могут отбрасываться в сети в результате перегрузки, а также злонамеренно перехватываться и отбрасываться. Последствия отбрасывания одного или множества сообщений syslog определить невозможно. Если сообщение говорит лишь о малозначимой смене состояния, его пропуск может просто остаться не замеченным, а может вызвать некоторое раздражение оператора. С другой стороны, если сообщение содержало более важную информацию, администраторы могут остаться в неведении относительно развития ситуации и возможных проблемах. Сообщения могут также перехватываться и отбрасываться атакующим с целью сокрытия своих действий.

Может оказаться целесообразным включение ограничений по скорости отправки на инициаторах и трансляторах syslog. Это позволит предотвратить перегрузки в результате всплеска активности.

Гарантированная доставка сообщений желательна не всегда. Гарантированная доставка означает необходимость блокировки инициатора или транслятора когда коллектор или транслятор не способен больше воспринимать сообщения. В некоторых операционных системах (Unix/Linux) инициатор или транслятор syslog работает в рамках системного процесса с высоким приоритетом (syslogd). Если это процесс блокируется, система в целом «зависает». То же самое будет наблюдаться при взаимной блокировке между syslogd и, например, сервером DNS.

Для предотвращения таких проблем надежную доставку можно реализовать так, чтобы сообщения осознанно отбрасывались в тех случаях, когда они приводят к блокировке приложения syslog. Преимущество в таких случаях заключается в том, инициатор или транслятор осознанно отбрасывают сообщения и могут уведомить об этом коллектор или транслятор. При отсутствии надежной доставки сообщения будут просто теряться, а их адресаты об этом даже не узнают.

8.6. Контроль перегрузок

Поскольку syslog может генерировать неограниченный объем данных, передача этих данных по протоколу UDP в общем случае проблематична по причине слабого контроля перегрузок в UDP. Механизмы контроля насыщения, которые реагируют на перегрузку снижением скорости передачи и обеспечивают беспристрастное распределение пропускной способности между потоками одного пути, играют важную роль в обеспечении стабильной работы Internet [RFC2914]. Этим объясняется то, что транспорт TLS для syslog **требуется** реализовать и этот траспорт **рекомендуется** для общего применения.

Единственным случаем, где транспорт UDP для syslog **может** служить альтернативно для транспорта TLS, являются управляемые сети в которых могут быть явно обеспечены пути для трафика UDP syslog с помощью механизмов организации трафика (traffic engineering) типа ограничения скорости или резервирования пропускной способности. Во всех других следах **следует** применять транспорт TLS.

В любой реализации возможны случаи, когда инициатору или транслятору приходится блокировать отправку сообщений. Одним из наиболее распространенных случаев является переполнение внутренней очереди. Это может происходить в результате ограничения скорости или низкой производительности приложения syslog. В любом случае **рекомендуется** не отбрасывать сообщения, а временно сохранять их до появления возможности передачи. Однако, если сообщения приходится отбрасывать, инициаторам и трансляторам **рекомендуется** выбирать для отбрасывания менее важные сообщения, сохраняя более важные.

Сообщения с меньшими значениями SEVERITY имеют более высокий уровень важности. В такой ситуации сообщения, которые придется отбрасывать, следует просто отвергать. Приложение syslog может уведомлять коллекторы и трансляторы о фактах отбрасывания сообщений.

8.7. Целостность сообщений

Помимо того, что сообщения syslog могут быть отвергнуты, они могут повреждаться при передаче или изменяться атакующими. В таких случаях исходное содержимое сообщения не попадет к коллекторам и трансляторам. Кроме того при расположении атакующего между транспортным отправителем и транспортным получателем сообщений syslog этот атакующий может перехватывать и изменять сообщения «на лету» для сокрытия несанкционированных действий.

8.8. Просмотр сообщений

Несмотря на отсутствие строгих рекомендаций по формату MSG, большинство сообщений syslog создается в понятной человеку форме с расчетом на то, что способные администраторы смогут читать и понимать эти сообщения. В

протоколе syslog нет механизмов защиты конфиденциальности передаваемых сообщений. В большинстве случаев передача сообщений в форме открытого текста обеспечивает преимущества для сотрудников оператора, если они собирают пакеты из линии. Сотрудники оператора могут читать сообщения и сопоставлять их с другими событиями, которые видны из проходящих в линии пакетов, для отслеживания и решения проблем. К сожалению, атакующие также могут видеть содержимое понятных человеку сообщений syslog. Злоумышленники могут использовать полученную информацию для компрометации машины или других нарушений работы.

Для предотвращения этой проблемы операторам рекомендуется использовать защищенное транспортное отображение.

8.9. Неприемлемая конфигурация

Поскольку в протоколе нет какой-либо распространяемой управляющей информации о сообщениях или конфигурации, ответственность за отправку сообщений нужным получателям полностью ложится на администраторов сетей. Были отмечены случаи, когда некорректно настроенные приложения syslog отправляли свои сообщения не тем трансляторам или коллекторам. Во многих случаях непредусмотренные трансляторы и коллекторы могут оказаться не настроенными на прием сообщений syslog и будут просто отбрасывать их. Однако в отдельных случаях получение сообщений syslog вызывало проблему у таких непредусмотренных получателей. Если сообщение пришло непредусмотренному получателю, оно может остаться не рассмотренным и не обработанным.

Использование надежного транспортного отображения может помочь в обнаружении некоторых из отмеченных проблем. Например, это может помочь с обнаружением проблемы, когда сообщения передаются системе, не настроенной на их прием. Однако это не поможет при обнаружении проблем, связанных с отправкой сообщений не тому адресату, если последний настроен на восприятие сообщений.

8.10. Петли в пересылке

Как показано на рисунке 2, машины могут быть настроены на пересылку сообщений syslog последующим трансляторам с целью доставки коллектору. В одной реальной ситуации администратор обнаружил, что он ошибочно настроил два транслятора на пересылку сообщений с некоторыми значениями SEVERITY от одного к другому и обратно. Когда любая из этих машин получит или создаст сообщение соответствующего типа, она будет пересылать его другому транслятору. Тот, в свою очередь, перешлет его обратно. Этот (бесконечный) цикл пересылки будет перегружать промежуточную сеть и сами машины. Администраторам следует соблюдать осторожность, чтобы таких петель не возникало.

8.11. Вопросы загрузки

Сетевые администраторы должны найти время для оценки емкости коллектора syslog. Атакующий может организовать DoS-атаку[1], заполняя дисковое пространство коллектора ложными сообщениями. Организация циклической перезаписи позволяет решить эту проблемы, но при этом администратор утратит возможность видеть достаточно старые[2] записи.Транспортный получатель должен иметь сетевой интерфейс, способный принимать отправленные ему сообщения.

Администраторы и специалисты по планированию сетей должны внимательно рассмотреть пути между инициаторами, трансляторами и коллекторами. Сообщения syslog не должны приводить к перегрузке сетевых каналов.

Для снижения остроты отмеченных здесь проблем рекомендуется использовать транспорт с гарантированной доставкой.

8.12. Отказ в обслуживании

Как и в любой системе, злоумышленник может просто перегрузить транспортного получателя, отправляя ему сообщения в объеме, превышающем возможности обработки инфраструктуры или самого устройства. Разработчикам следует предпринять попытки минимизации таких угроз (например, принимая сообщения syslog только с известных адресов IP).

9. Согласование с IANA

9.1. VERSION

Агентство IANA создало реестр syslog Version Values значений VERSION, описанных в параграфе 6.2.2. Номера версий **должны** увеличиваться для каждой новой спецификации протокола syslog, в которой меняется какая-либо из частей заголовка (HEADER). Изменения включают добавление или удаление полей, а также смену синтаксиса или семантики имеющихся полей.

Значения VERSION должны регистрироваться в соответствии с процедурой Standards Action, как описано в [RFC5226]. Зарегистрированное IANA значение VERSION приведено в таблице 3.

Таблица 3. Зарегистрированное IANA значение VERSION

Версия	***Формат***
1	Определен в [RFC5424]

9.2. SD-ID

Агентство IANA создало реестр syslog Structured Data ID Values для идентификаторов структурированных данных (SD-ID) и связанных с ними значений PARAM-NAME, описанных в разделе 7.

[1]Denial of Service — отказ в обслуживании.
[2]Больше продолжительности цикла. *Прим. перев.*

Новые значения SD-ID и PARAM-NAME должны регистрироваться в соответствии с процедурой IETF Review, описанной в [RFC5226].

После определения SD-ID и SD-PARAM синтаксис и семантику этих объектов **недопустимо** менять. Если желательно изменить имеющиеся объекты, **должны** создаваться новые SD-ID или SD-PARAM, а прежние сохраняться неизменными.

Здесь даны предложения по локально расширяемым именам. Агентство IANA не будет регистрировать и контролировать имена, содержащие символ @ (ABNF %d64).

Зарегистрированные IANA значения SD-ID и PARAM-NAME приведены в таблице 4.

Таблица 4. Зарегистрированные IANA значения SD-ID и их PARAM-NAME

SD-ID	***PARAM-NAME***	***Тип***
timeQuality		OPTIONAL
	tzKnown	OPTIONAL
	isSynced	OPTIONAL
	syncAccuracy	OPTIONAL
origin		OPTIONAL
	ip	OPTIONAL
	enterpriseId	OPTIONAL
	software	OPTIONAL
	swVersion	OPTIONAL
meta		OPTIONAL
	sequenceId	OPTIONAL
	sysUpTime	OPTIONAL
	language	OPTIONAL

10. Рабочая группа

С рабочей группой можно связаться по адресу списка рассылок

syslog@ietf.org

С текущим руководителем рабочей группы можно связаться через:

Chris Lonvick

Cisco Systems

EMail: clonvick@cisco.com

David Harrington

Huawei Technologies USA

EMail: dbharrington@comcast.net

11. Благодарности

Авторы благодарят Chris Lonvick, Jon Callas, Andrew Ross, Albert Mietus, Anton Okmianski, Tina Bird, Devin Kowatch, David Harrington, Sharon Chisholm, Richard Graveman, Tom Petch, Dado Colussi, Clement Mathieu, Didier Dalmasso и всех других людей, предоставивших свои комментарии к разным версиям этого предложения.

12. Литература

12.1. Нормативные документы

[ANSI.X3-4.1968] American National Standards Institute, "USA Code for Information Interchange", ANSI X3.4, 1968.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

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

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

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

[RFC2914] Floyd, S., "Congestion Control Principles", BCP 41, RFC 2914, September 2000.

[RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

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

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4646] Phillips, A. and M. Davis, "Tags for Identifying Languages", BCP 47, RFC 4646, September 2006.

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

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5425] Fuyou, M., Yuzhi, M., and J. Salowey, "TLS Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, March 2009.

[UNICODE-TR36] Davis, M. and M. Suignard, "UNICODE Security Considerations", July 2005.

12.2. Дополнительная литература

[RFC3164] Lonvick, C., "The BSD Syslog Protocol", RFC 3164, August 2001.

Приложение A. Рекомендации для разработчиков

В это разделе представлена информация, адресованная разработчикам. Эти сведения считаются полезными, но не относятся к нормативным. В силу этого от реализаций **не требуется** следовать им для обеспечения соответствия данной спецификации.

A.1. Отношения с BSD Syslog

Хотя приложения BSD syslog используются весьма широко, формат этой системы никогда не был стандартизован формально. Наблюдаемые форматы описаны в [RFC3164], относящемся к серии информационных (Informational RFC), и практика показывает наличие множества разных реализаций. Исследования в процессе создания этого документа показали, что у разных реализаций syslog на различных платформах очень мало общего. Единственное, на что все реализации согласны, - начинать сообщения с "<" PRIVAL ">". Во всем остальном унаследованные сообщения syslog не используют согласованного формата. По этой причине в RFC 3164 не описаны конкретные элементы сообщений syslog. В документе сказано, что любые сообщения, адресованные в порт syslog UDP, должны трактоваться как сообщения syslog, независимо от их формата и содержимого.

Данный документ сохраняет синтаксис и семантику значения PRI. Это позволит унаследованным реализациям syslog сохранить совместимость генерируемых сообщений syslog с данной спецификацией .

Многие существующие реализации используют UDP в качестве транспортного протокола для syslog. Данные спецификация поддерживает транспорт UDP, но не рекомендует его. Рекомендуется развертывание обязательной поддержки TLS. Могут применяться также дополнительные транспортные протоколы.

RFC 3164 описывает поведение трансляторов, а данный документ не задает этого поведения. Оно может быть описано в отдельном документе.

Поле TIMESTAMP, описанное в RFC 3164, обеспечивает меньшую точность по сравнению с метками, описанными в данном документе. В нем также не хватает информации о годе и часовом поясе. Если соответствующий этому документу формат нужно преобразовать в формат RFC 3164, предлагается использовать локальный часовой пояс отправителя, отбрасывая информацию о часовом поясе и годе. Если нужно преобразовать полученное сообщение RFC 3164 в заданный этим документом формат, следует добавить текущий год и часовой пояс, который **может** использоваться транслятором или коллектором.

Поле HOSTNAME в RFC 3164 менее конкретно, но его формат поддерживается данным документом в качестве одного из дополнительных представления HOSTNAME.

Часть MSG описана как TAG и CONTENT в RFC 3164. В данном документе MSG представляет собой то, что обозначено CONTENT в RFC 3164. TAG сейчас является частью заголовка, не представляя собой отдельного поля. Значение TAG разделено между полями APP-NAME, PROCID и MSGID. Это несколько отличается отличается от использования TAG, но в большинстве случаев обеспечивает ту же функциональность.

В RFC 3164 структурированные данные (STRUCTURED-DATA) не описаны. Если соответствующее этому документу сообщение, содержащее STRUCTURED-DATA, нужно преобразовать в соответствии с RFC 3164, STRUCTURED-DATA просто становится частью текста в свободном формате RFC 3164 CONTENT.

В общем случае этот документ пытается обеспечить простоту анализа заголовка с четким разделением полей, тогда как традиционный BSD syslog зависит от исторически сложившихся правил, осложняющих анализа и разделение полей.

A.2. Размер сообщений

Разработчикам следует помнить об ограничениях размера сообщений, отмеченных в параграфе 6.1, и пытаться разместить наиболее важные детали сообщения в его начале (в пределах минимально гарантируемого размера). Это обеспечит доступ к таким данных трансляторов и коллекторов даже в тех случаях, когда транспортный получатель на трансляторе по пути доставки использует отсечку для сообщения.

Причина того, что от транспортных получателей syslog требуется поддержка приема сообщений размером лишь до 480 октетов (включительно), заключается, наряду с другими причинами, в сложностях проблемы доставки в старых сетях. Сообщения syslog могут использовать транспортное отображение UDP с ограничением в 480 октетов для предотвращения сеансовых издержек и фрагментации сообщений. В сетях с проблемами вероятность успешной доставки однопакетного сообщения выше, нежели вероятность доставки фрагментов сообщения в двух пакетах. Следовательно, увеличение размера сообщений может лишить оператора части критически важной информации при возникновении проблемы тогда, как использование мелких сообщений обеспечит доставку этой информации.

Рекомендуется для сообщений, связанных с поиском неполадок ограничивать размер 480 октетами. Следует также отметить, что некоторые реализации UDP не поддерживают сообщений размером более 480 октетов. Такое поведение встречается весьма редко и может уже не создавать проблемы.

Имеются случаи, когда сообщения syslog используются для передачи заведомо большого объема информации (например, данных аудита). Отсутствие верхнего предела размера сообщений позволяет создавать приложения syslog с поддержкой сообщений любого размера, которые будут совместимы с данной спецификацией. В таких случаях оператор принимает на себя ответственность за поддержку требуемого размера сообщений всеми компонентами инфраструктуры syslog. Транспортное отображение может рекомендовать свои ограничения на размер сообщений, которые должны быть реализованы в соответствии со спецификацией транспорта.

Разработчикам следует помнить о том, что размеры сообщений задаются в октетах. Может возникать весьма большая разница между числом символов в кодировке UTF-8 и числом соответствующих им октетов.

Следует отметить, что IPv6 MTU примерно в 2,5 раза превышает 480. Реализации, предназначенные для применения исключительно в средах IPv6, могут учесть этот факт при ограничении размера сообщений.

A.3. Значения важности

В этом разделе приведены рекомендации по использованию значений важности (Severity) описанных в параграфе 6.2.1.

Все реализациям следует пытаться выделять наиболее подходящие значения важности для их сообщений. Наиболее важно присваивать сообщениям, предназначенным для включения отладки или тестирования программ присваивать значение Severity = 7. Severity 0 следует резервировать для сообщение критически высокой важности (типа отказов оборудования или предстоящего отключения питания). По усмотрению администратора реализации могут использовать значения 0 и 7 для других целей.

Поскольку понятие важности весьма субъективно, трансляторам и коллекторам не следует предполагать одинаковой трактовки этих значений всеми инициаторами сообщений.

A.4. Точность TIME-SECFRAC

Значение TIMESTAMP, описанное в параграфе 6.2.3, поддерживает доли секунд. Это служит основой для очень распространенной ошибки кодирования, когда удаляются начальные нули из дробной части секунд. Например, TIMESTAMP "2003-10-11T22:13:14.003" можно ошибочно записать в виде "2003-10-11T22:13:14.3". Это будет давать дробную часть в 300 мсек вместо исходных 3 мсек.

A.5. Регистр символов в именах

Имена используются в различных частях этого документа (например, для SD-ID и PARAM-NAME). В документе используется правило lower camel case[1]. Каждое имя начинается с маленькой буквы (нижний регистр), а каждое новое слово, встроенное в имя, начинается с заглавной буквы без использования дефиса или другого разделителя. Примером этого может служить timeQuality.

Хотя разработчики свободны при выборе регистра символов в экспериментальных именах, предполагается, что они будут следовать принятому здесь соглашению.

A.6. Приложения Syslog, не знающие времени

В параграфе 6.2.3 разрешено использование значения NILVALUE в качестве временной метки инициаторами, не имеющими часов. Можно возразить, что таких приложений уже не найти в современных инфраструктурах IT. Однако обсуждение этого вопроса показывает, что такие устройства еще могут встречаться на практике и поэтому следует обеспечить возможность работы с ними.

Однако реализациям **следует** указывать действительное время в TIMESTAMP, если операционная система, программа или оборудование включают часы. Действительное время в TIMESTAMP следует указывать даже в тех случаях, когда сложно получить системное время. Значение NILVALUE следует указывать лишь в тех случаях, когда просто нет возможности определить текущее время. Это разрешение не следует использовать в качестве оправдания для ленивых разработчиков.

A.7. Замечания по timeQuality SD-ID

Рекомендуется по умолчанию использовать значение 0 для параметра tzKnown (параграф 7.1.1). Следует указывать значение 1 лишь в тех случаях, когда администратор указал в конфигурации конкретный часовой пояс. Можно использовать значение 1 по умолчанию, если операционная система предоставляет точную информацию о часовом поясе. Однако и в таких случаях администратору следует убедиться в корректности данных о часовом поясе.

Важно не порождать заблуждений о точности временных меток в timeQuality SD-ID (параграф 7.1). Инициатору следует указывать только такую точность, в которой он уверен. В общем случае предполагается, что администратор может выяснить точность часов по конфигурации оператора. По умолчанию точность часов указывать не следует.

A.8. Кодировка UTF-8 и BOM

В этом документе указано, что информация SD-PARAMS всегда должна представляться в кодировке UTF-8. Использование других кодировок в разделе MSG (включая кодировку ASCIIPRINT) не разрешается для устройств, соответствующих данной спецификации. Здесь нужно рассмотреть два особых случая. Во-первых, соответствующие данной спецификации приложения syslog, могут оказаться не способны убедиться в том, что представленная инициатором информация использует кодировку UTF-8. Если нет возможности с уверенностью определить это, приложение syslog может выбрать отказ от включения BOM в MSG. Если приложение syslog имеет достоверное указание того, что содержимое сообщения представлено в кодировке UTF-8, ему следует включать BOM. В другом случае транслятор syslog может пересылать сообщения от устройств, которые не соответствуют данной спецификации.

[1]Стиль верблюда.

В этой ситуации устройство явно не будет включать BOM, пока не будет уверенности в том, что полученное сообщение использует кодировку UTF-8.

Адрес автора

Rainer Gerhards

Adiscon GmbH

Mozartstrasse 21

Grossrinderfeld, BW 97950

Germany

EMail: rgerhards@adiscon.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com