Network Working Group
Request for Comments: 5426
Category: Standards Track

A. Okmianski
Cisco Systems, Inc.

March 2009

Передача сообщений Syslog по протоколу UDP

Transmission of Syslog Messages over UDP

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

Авторские права (Copyright (c) 2009) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К этому документу применимы права и ограничения, перечисленные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно.

Этот документ может содержать материалы из документов IETF или участников IETF[1], опубликованных или публично доступных до 10 ноября 2008 г. Лица, контролирующие авторские права на некоторые из таких материалов, могли не предоставить IETF Trust прав на изменение материалов вне контекста стандартизации IETF[2]. Без получения соответствующей лицензии от лиц, контролирующих авторские права на такие материалы, этот документ не может быть изменен вне контекста стандартизации IETF, а также не могут создаваться производные работы вне контекста стандартизации. Исключением является лишь форматирование документа для публикации в качестве RFC или перевод на другие языки.

Аннотация

Этот документ описывает транспортировку сообщений syslog на основе протоколов UDP/IPv4 и UDP/IPv6. Многоуровневая архитектура syslog обеспечивает поддержку любого числа транспортных протоколов. Однако для обеспечения взаимодействия реализации протокола syslog должны поддерживать описанное здесь транспортное отображение.

Оглавление

1. Введение

В информационном RFC 3164 [8] описаны имеющиеся реализации протокола syslog. Там описан как формат сообщений syslog, так и их передача по протоколу UDP [1]. В последствии был предложен проект стандарта (Standards-Track) для протокола syslog в RFC 5424 [2].

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

RFC 5424 задаёт многоуровневую архитектуру, обеспечивающую поддержку любого числа транспортных отображений для передачи сообщений syslog. Данный документ описывает транспортное отображение UDP для протокола syslog.

Описанный в этом документе транспорт может применяться для передачи сообщений как через IPv4 [3], так и через IPv6 [4].

Сетевые администраторы и архитекторы должны быть осведомлены о важных проблемах надёжности и безопасности данного вида транспорта, связанных с использованием протокола UDP. Эти проблемы указаны в данной спецификации. Однако этот транспорт является облегчённым и основан на популярном использовании UDP для syslog.

2. Соглашения об уровнях 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 [5].

3. Транспортный протокол

3.1. Одно сообщение на дейтаграмму

Каждая дейтаграмма UDP **должна** содержать только одно сообщение syslog, которое **может** быть полным или усечённым. Форматирование и отсечка сообщений **должны** соответствовать RFC 5424 [2]. Включать в дейтаграммы дополнительные данные **недопустимо**.

3.2. Размер сообщения

Это транспортное отображение поддерживает передачу сообщений syslog размером до 65535 октетов минус размер заголовка UDP. Этот предел основан на максимальном размере дейтаграмм UDP в 65535 октетов, заданном в RFC 768 [1]. Для IPv4 максимальный размер данных (payload) составляет 65535 минус размер заголовков UDP и IP, поскольку IPv4 имеет 16-битовое поле размера, которое учитывает и размер заголовков.

В IPv4 получатели syslog **должны** быть способны принимать дейтаграммы размером до 480 октетов, включительно, а в IPv6 получатели syslog **должны** быть способны принимать дейтаграммы размером до 1180, включительно. Всем получателям syslog **следует** поддерживать возможность приёма дейтаграмм размером до 2048, включительно. Рекомендуется принимать и более крупные сообщения.

Приведённые выше ограничения и рекомендации создают базу для взаимодействия. Минимальный поддерживаемый размер определён на основе минимального значения MTU, которое должны поддерживать хосты Internet - 576 октетов для IPv4 [3] и 1280 октетов для IPv6 [4]. Дейтаграммы, соответствующие этим ограничениям, имеют наилучшие шансы доставки, поскольку для них заведомо не требуется фрагментирования.

Отправителям сообщений syslog **рекомендуется** ограничивать размер сообщений так, чтобы размер дейтаграмм IP не превышал минимальное значение MTU в используемой сети. Это позволяет избежать фрагментации дейтаграмм и возникновения связанных с ней проблем типа некорректного определения MTU.

Фрагментация может быть нежелательной, поскольку она повышает риск потери сообщения в результате потери единственного фрагмента. Протокол syslog не имеет механизма подтверждений и, следовательно, - эффективного способа организации повторной передачи. Это не позволяет использовать в syslog средства определения MTU для пути на уровне пакетизации [9]. если значение MTU в сети неизвестно заранее, лучшим выходом будет предположить минимальное значение в 480 октетов для IPv4 b 1180 для IPv6.

3.3. Порты источника и адресата

Получатели syslog **должны** поддерживать приём дейтаграмм через общеизвестный порт UDP 514, но **могут** настраиваться на другой порт-получатель. Отправители syslog должны адресовать дейтаграммы с сообщениями syslog в порт UDP 514, но **могут** быть настроены на работу через иной порт. Отправители syslog **могут** использовать любой порт отправителя UDP для передачи сообщений.

3.4. IP-адрес источника

IP-адрес отправителя в дейтаграммах UDP **не следует** трактовать как адрес хоста-инициатора сообщения syslog. Отправителем сообщения syslog может оказаться транслятор. Адрес инициатора содержится в самом сообщении syslog.

3.5. Структура UDP/IP

Каждая дейтаграмма UDP/IP, передаваемая транспортным отправителем, **должна** полностью соответствовать структуре, указанной в UDP RFC 768 [1] и IPv4 RFC 791 [3] или IPv6 RFC 2460 [4] в зависимости от используемого протокола.

3.6. Контрольные суммы UDP

Отправителям syslog **недопустимо** отключать контрольные суммы UDP. Отправителям IPv4 syslog **следует** использовать контрольные суммы UDP при передаче сообщений. Отметим, что RFC 2460 [4] требует использования контрольных сумм UDP при передаче дейтаграмм UDP по протоколу IPv6.

Получателям syslog **недопустимо** отключать контрольные суммы UDP. Получателям IPv4 syslog **следует** проверять контрольные суммы UDP, а также **следует** воспринимать сообщения syslog с нулевой контрольной суммой. Отметим, что RFC 2460 [4] требует использования контрольных сумм UDP при передаче по протоколу IPv6.

4. Вопросы надёжности

UDP представляет собой протокол с малыми издержками и без гарантии доставки. В этом разделе рассмотрены вопросы надёжности UDP, которые следует принимать во внимание разработчикам и пользователям.

4.1. Потеря дейтаграмм

Это транспортное отображение не поддерживает каких-либо механизмов обнаружения и корректировки потери дейтаграмм. Такие потери в процессе доставки могут быть обусловлены перегрузками, повреждением пакетов или иными проблемами в промежуточных сетях. Фрагментация IP усугубляет эту проблему, поскольку потеря единственного фрагмента приводит к отбрасыванию всего сообщения.

4.2. Повреждение сообщений

Дейтаграммы UDP/IP могут повреждаться в процессе доставки в результате программных, аппаратных или сетевых ошибок. Это транспортное отображение задаёт использование контрольных сумм UDP, позволяющие обнаружить повреждённые дейтаграммы, в дополнение к контрольным суммам, применяемым в IP и протоколах канального уровня (Layer 2). Однако контрольная сумма не гарантирует обнаружения ошибок, а данное транспортное отображение не поддерживает механизмов подтверждения или повторной передачи.

4.3. Контроль перегрузок

Поскольку syslog может создавать неограниченный объем данных, передача этих данных по протоколу UDP в общем случае проблематична, поскольку в UDP нет механизмов контроля перегрузок. Механизмы, реагирующие на перегрузки снижением скорости передачи трафика и обеспечивающее беспристрастное разделение ресурсов между потоками, использующими общий путь, имеют очень важное значение для стабильной работы Internet [6]. Именно по этой причине транспорт TLS для syslog [7] **требуется** от всех реализаций и **рекомендуется** для общего применения.

Единственным вариантом, где для syslog **может** использоваться транспорт UDP в качестве альтернативы транспорту TLS, являются управляемые сети, в которых явно обеспечиваются пути для трафика UDP syslog с использованием механизмов организации трафика типа ограничения скорости или резервирования пропускной способности. Во всех прочих средах **следует** использовать транспорт TLS [7].

4.4. Порядок доставки

Транспорт IP, используемый протоколом UDP, не гарантирует упорядоченной доставки дейтаграмм. Временные метки в каждом сообщении syslog могут применяться для восстановления порядка. Однако это не поможет в тех случаях, когда в одном интервале отсчёта времени создаётся множество сообщений, отправитель не может создавать временные метки или сообщения приходят от разных хостов, часы которых не синхронизированы. Порядок доставки сообщений syslog с использованием данного транспорта **не следует** использовать в качестве основы для восстановления абсолютного или относительного порядка событий на создавших сообщения syslog хостах.

5. Вопросы безопасности

Использовать данную спецификацию в незащищённых сетях **не рекомендуется**. Некоторые вопросы безопасности syslog рассмотрены в RFC 5424 [2]. В этом разделе рассмотрены конкретные вопросы безопасности при доставке сообщений syslog по протоколу UDP. Некоторые из отмеченных ниже проблем безопасности можно смягчить за счёт применения IPsec в соответствии с RFC 4301 [10].

5.1. Проверка подлинности отправителя и подмена сообщений

Это транспортное отображение не обеспечивает строгой проверки подлинности отправителя. Получатель сообщения syslog не имеет возможности удостовериться, что сообщение было действительно отправлено указанным в нем хостом, а не другим устройством. Возможны также ошибки, когда некорректно настроенная машина отправляет свои сообщения syslog получателю, который представил себя другой машиной.

Это транспортное отображение не обеспечивает защиты от обманных сообщений syslog. Атакующий может передавать получателю обманные сообщения syslog (с той же или другой машины).

Злоумышленник может скрыть истинную природу своей атаки среди среди множества других сообщений. Например, атакующий может начать создание обманных сообщений, говорящих о проблемах на некой машине. На это может обратить внимание системный администратор, который будет тратить время на исследование предполагаемой проблемы. За это время злоумышленник может организовать атаку на другую машину или другой процесс на той же машине.

Кроме того, злоумышленник может генерировать ложные сообщений syslog для создания некорректного представления о состоянии системы. Например, злоумышленник может остановить на машине критичный процесс, который при завершении генерирует уведомление. После этого атакующий может создать ложное сообщение о перезапуске этого процесса. Системный администратор может воспринять эту дезинформацию и не проверить реальное состояние процесса.

5.2. Раскрытие сообщений

Это транспортное отображение не обеспечивает конфиденциальности передаваемых сообщений. Если сообщения syslog представляют собой открытый текст, они будут переданы в такой же форме. В большинстве случаев передача открытых и в понятной человеку форме сообщений удобна для администраторов. К сожалению злоумышленники тоже могут получить доступ к содержимому таких сообщений syslog. Полученную из этих сообщений информацию злоумышленник может применить для организации атаки на машину. **Рекомендуется** не передавать «деликатную» информацию с использованием этого отображения или ограничивать её распространение лишь хорошо защищёнными сетями.

5.3. Повторное использование сообщений

Подмена и просмотр сообщений могут использоваться совместно в replay-атаках. Злоумышленник может записать набор сообщений, показывающих нормальную работу машины. Позднее атакующий может исключить эту машину из сети и заново передать записанные сообщения, изменив в них временные метки. Администраторы могут не увидеть ничего особенного в полученных сообщениях и примут их за индикацию нормального поведения машины.

5.4. Ненадёжность доставки

Как было отмечено в разделе 4. Вопросы надёжности, транспорт UDP не является надёжным и пакеты с дейтаграммами сообщений syslog могут теряться в процессе передачи без уведомления об этом. Потеря одного или множества сообщений syslog может иметь последствия для безопасности. Администраторы могут не узнать о возникновении и развитии той или иной потенциально серьёзной проблемы. Сообщения могут также перехватываться и отбрасываться злоумышленниками для сокрытия своей деятельности.

5.5. Приоритизация и дифференцирование сообщений

Это транспортное отображение не предусматривает приоритизации сообщений syslog в процессе их передачи и обработки. Если у отправителя, получателя и/или в сети не реализован некий механизм приоритизации, можно перегрузить получателя или сетевые устройства маловажными сообщениями, что может привести к отбрасыванию потенциально важных сообщений.

5.6. Отказ служб

Атакующий может вызвать перегрузку получателя, передавая большое число сообщений, которые не могут быть обработаны инфраструктурой или самим устройством. Разработчикам **следует** предпринимать попытки минимизации таких угроз (например, принимая сообщения лишь с заданного набора адресов IP).

6. Взаимодействие с IANA

Этот транспорт использует порт UDP 514 для syslog, как указано в реестре IANA для номеров портов.

7. Благодарности

Автор благодарит участников работы над документом: Chris Lonvick, Rainer Gerhards, David Harrington, Andrew Ross, Albert Mietus, Bernie Volz, Mickael Graham, Greg Morris, Alexandra Fedorova, Devin Kowatch, Richard Graveman и все другие люди, приславшие комментарии к разным версиям этого предложения.

8. Литература

8.1. Нормативные документы

[1] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

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

[3] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[4] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

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

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

[7] Miao, F. and Y. Ma, "TLS Transport Mapping for Syslog", RFC 5425, March 2009.

8.2. Дополнительная литература

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

[9] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[10] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

Адрес автора

Anton Okmianski

Cisco Systems, Inc.

595 Burrard St., Suite 2123

Vancouver, BC V7X 1J1

Canada

Phone: +1-978-936-1612

EMail: aokmians@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com