

Interface to the Routing System (I2RS) Traceability: Framework and Information Model

Интерфейс для отслеживания системы маршрутизации (I2RS) - схема и информационная модель

Аннотация

Этот документ описывает схему для отслеживания в интерфейсе с системой маршрутизации (Interface to the Routing System или I2RS) и информационную модель для этой схемы. Документ описывает мотивацию, требования и примеры использования, а также задаёт информационную модель для записи взаимодействий между элементами, реализующими протокол I2RS. Схема обеспечивает согласованный интерфейс отслеживания для компонентов, реализующих архитектуру I2RS, для записи сделанного, участников действий и времени. Документ нацелен на улучшение управления реализациями I2RS и может служить для устранения неполадок, аудита, прогнозов и учёта.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется лишь для информации.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Не все документы, одобренные IESG, претендуют на статус стандартов. Дополнительную информацию о стандартах Internet можно найти в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc7922>.

Авторские права

Copyright (c) 2016. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные 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. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение.....	1
2. Соглашения и термины.....	2
3. Мотивация.....	2
4. Применение.....	2
5. Информационная модель.....	2
5.1. Схема отслеживания I2RS.....	2
5.2. Поля журнала отслеживания I2RS.....	3
5.3. Маркер конца сообщения.....	5
6. Примеры.....	5
7. Эксплуатационные рекомендации.....	5
7.1. Создание журнала отслеживания.....	5
7.2. Временное хранилище для журнала.....	5
7.3. Ротация файлов журнала.....	5
7.4. Поиск журналов.....	5
7.4.1. Поиск через Syslog.....	6
7.4.2. Извлечение через сбор информации I2RS.....	6
7.4.3. Извлечение через подписку и публикацию I2RS.....	6
8. Вопросы безопасности.....	6
9. Литература.....	6
9.1. Нормативные документы.....	6
9.2. Дополнительная литература.....	6
Благодарности.....	7
Адреса авторов.....	7

1. Введение

Архитектура I2RS [RFC7921] указывает, что клиенты I2RS, желающие получить или изменить состояние маршрутизации, **должны** пройти проверку подлинности у агента I2RS. У клиентов I2RS имеются уникальные идентификаторы, которые они предоставляют для аутентификации и им следует иметь другой неанализируемый

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

(opaque) идентификатор для взаимодействующих через них приложений. Программирование состояния маршрутизации будет возвращать код результата конкретной операции и связанные с кодом причины. Эти сведения очень важны для понимания истории взаимодействий I2RS.

Этот документ определяет схему, требуемую для отслеживания взаимодействия между клиентом и агентом I2RS. Описаны также варианты применения трассировки в I2RS, на основе которых документ предлагает информационную модель и требования к отчётам для эффективной записи взаимодействий I2RS. В этом контексте эффективное устранение неполадок означает возможность определить, какая операция была выполнена конкретным клиентом I2RS через агент I2RS, каковы её результаты и когда операция происходила.

2. Соглашения и термины

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

В спецификации архитектуры I2RS [RFC7921] определены термины, используемые в этом документе, которые относятся к I2RS, такие как агент I2RS, клиент I2RS и т. п. Предполагается знакомство читателя с терминами и концепциями [RFC7921].

3. Мотивация

По мере расширения сети и правила становятся все более важной частью плоскости управления, которая создаёт и поддерживает состояние пересылки, а эксплуатационная сложность возрастает. I2RS предлагает детализированный и согласованный контроль над правилами и состоянием плоскости управления, а также удаляет или сокращает область действия политики, которая была применена к плоскости управления на любом отдельном устройстве пересылки. Возможность автоматизировать и абстрагировать даже сложные элементы управления на основе правил подчёркивает потребность в одинаково масштабируемой функции отслеживания для записи на уровне событий деталей изменения системы маршрутизации, соответствующей требованиям I2RS (раздел 5 в [RFC7920]).

4. Применение

Очевидны мотивом для отслеживания I2RS является необходимость устранения неполадок и поиска причин, вызывающих проблемы во все более сложных системах маршрутизации. Например, благодаря наличию в I2RS многоканального полнодуплексного интерфейса с высокой пропускной способностью и скоростью отклика клиенты I2RS могут выполнять большое число операций с агентами I2RS почти одновременно и, вполне возможно, в очень быстрой серии. При внесении многочисленных изменений сеть реагирует соответствующим образом. Эти изменения могут приводить к состязанию (race), проблемам производительности, потере данных или нарушению работы служб. Для поиска первопричины проблем очень важно, чтобы сетевой оператор или администратор видел изменения, внесённые через I2RS в конкретный момент времени.

Некоторые сетевые среды предъявляют строгие требования к аудиту конфигурации и изменений в процессе работы. В других средах могут быть требования по сохранению журнальной информации из соображений эксплуатационного или нормативного соответствия. Это требует от I2RS учёта изменений, внесённых в системы маршрутизации элементов сети.

По мере распространения I2RS в средах маршрутизации модель отслеживания, поддерживающая контролируемое хранение журналов трассировки с использованием стандартизованного структурированного формата, обеспечивает преимущества, такие как возможность создания базовых инструментов, поддерживающих автоматизированное тестирование, и облегчает указанные ниже варианты применения.

- Мониторинг и устранение неполадок в реальном масштабе времени.
- Автоматизированное сопоставление ошибок, анализ тенденций и обнаружение аномалий.
- Автономный (вручную или с помощью инструментов) анализ изменений состояния маршрутизатора по сохранённым журналам отслеживания.
- Расширенные возможности сетевого аудита, управления и прогнозирования.
- Улучшенный учёт операций системы маршрутизации.
- Обеспечение стандартизованного формата отчётов об инцидентах и журналов испытаний.

5. Информационная модель

В этом разделе рассматривается информационная модель трассировки I2RS и детали каждого из сохраняемых полей.

5.1. Схема отслеживания I2RS

В этом разделе описана схема отслеживания I2RS на основе архитектуры I2RS.

Взаимодействие между необязательным сетевым приложением, управляющим действиями клиента, клиентом и агентом I2RS, системой маршрутизации и данными, собранными в журнале трассировки I2RS, показано на рисунке 1.

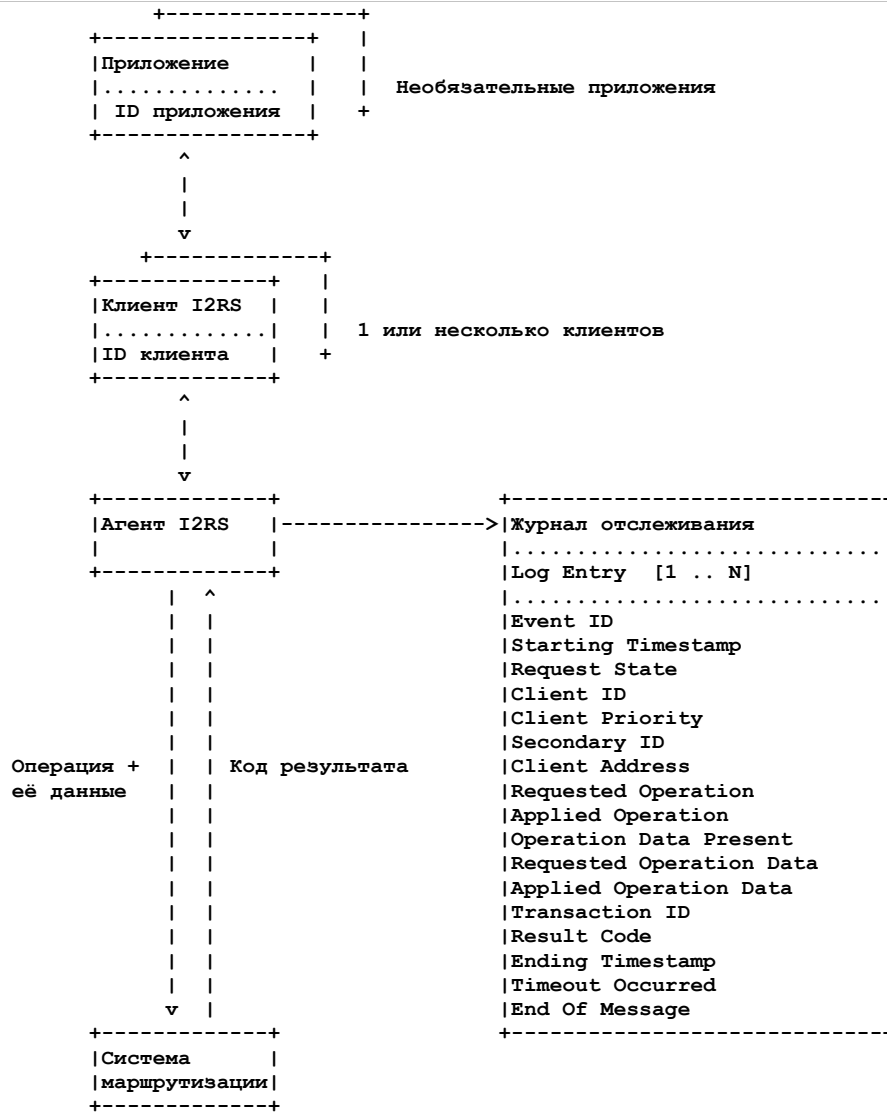


Рисунок 1. Запись журнала трассировки взаимодействия I2RS.

5.2. Поля журнала отслеживания I2RS

Ниже перечислены поля журнала трассировки I2RS. Эти поля обеспечивают для каждого взаимодействия I2RS возможность отслеживания до клиента, который сделал запрос в определённый момент времени.

Приведённый ниже список содержит поля, фиксируемые в журнале трассировки I2RS. Список представляет базовый набор полей, которые **должны** присутствовать во всех журналах трассировки I2RS. В дополнение к этому реализации агентов I2RS **могут** записывать другие поля, такие как производитель клиента I2RS или статистика агента (например, расход памяти, параметры производительности и т. п.).

Event ID - идентификатор события

Уникальный идентификатор для каждого события в журнале трассировки I2RS. Событием может быть аутентификация клиента агентом, операция клиента с агентом, отключение клиента от агента. События операций могут записываться неделимо (atomically) по завершению (в этом случае запись имеет обе временных метки Starting и Ending) или в начале каждой смены Request State. Поскольку операции могут происходить от одного клиента в одно время, важно иметь идентификатор, который можно однозначно связать с конкретной записью. Если для операции записывается каждая смена состояния, для каждой записи Request State **должен** использоваться один идентификатор. За счёт этого запрос легко отследить в журнале трассировки I2RS. Помимо требования уникальности Event ID, конкретный тип и значение задаёт реализация.

Starting Timestamp - временная метка начала

Время, когда операция I2RS вошла в указанное состояние запроса в агенте. Если запись журнала охватывает всю продолжительность запроса, это будет время получения запроса агентом. Это поле **должно** присутствовать во всех записях, задающих начало смены состояния, а также в записях, сохраняющих всю продолжительность запроса. Время указывается в полном формате временной метки [RFC3339], включая дату и часовой пояс (смещение от UTC¹). С учётом того, что многие операции I2RS могут происходить в быстрой серии, **должна** использоваться дробная часть метки для обеспечения адекватной детализации. Доли секунд **следует** указывать 3 цифрами после точки (second.microsecond).

Request State - состояние запроса

Состояние данной операции в конечном автомате I2RS в момент, указанные метками начала и завершения. Агенту I2RS **следует** генерировать запись в момент входа в состояние и выхода из него. При входе в новое состояние запись журнала будет иметь в поле Starting Timestamp время входа а поля Ending Timestamp не будет. При выходе из состояния запись будет иметь в поле Ending Timestamp время выхода и не будет включать поля Starting Timestamp. Прохождение через различные состояние можно привязать с помощью Event ID. Возможные состояния указаны ниже.

¹Coordinated Universal Time - универсальное координатное время.

PENDING

Запрос получен и помещён в очередь на обработку.

IN PROCESS

Запрос в данный момент обрабатывается агентом I2RS.

COMPLETED

Запрос достиг точки завершения.

Каждое изменение состояния **следует** записывать, если это не перегружает агента I2RS. Однако записи с Request State COMPLETED **должны** вноситься для всех операций. Если состояние COMPLETED является единственной записью для данного запроса, оно **должно** иметь временные метки начала и завершения, указывающие весь период запроса от поступления к агенту до завершения.

Client Identity - идентификатор клиента

Идентификатор клиента I2RS, используемый для проверки его подлинности агентом I2RS.

Client Priority - приоритет клиента

Приоритет клиента I2RS назначенный ему моделью контроля доступа, аутентифицировавшей клиента. Например, это может установить модель управления доступом (Access Control Model или NACM) протокола управления сетью (Network Configuration Protocol или NETCONF), как описано в [RFC6536].

Secondary Identity - второй идентификатор

Необрабатываемый идентификатор, который может быть известен клиенту от управляющего сетевого приложения. Этот идентификатор служит для трассировки сетевого приложения в течение действий клиента. Клиент может не предоставлять этот идентификатор агенту при отсутствии внешнего сетевого приложения, направляющего клиента. Однако это поле **должно** записываться, даже если клиент его не предоставляет. В этом случае указывается пустое значение.

Client Address - адрес клиента

Сетевой адрес клиента, подключённого к агенту, например, адрес IPv4 или IPv6.

Requested Operation - запрошенная операция

Операция I2RS, выполнение которой запрошено. Например, это может быть операция добавления маршрута, если маршрут вставляется в таблицу. Это не обязательно операция, фактически применённая к агенту.

В случае аутентификации клиента агентом запрошенной операцией **должна** быть CLIENT AUTHENTICATE. При отсоединении клиента от агента запрошенной операцией **должна** быть CLIENT DISCONNECT.

Applied Operation - примененная операция

Операция I2RS, выполненная фактически. Это может отличаться от Requested Operation в случаях, когда агент не может выполнить Requested Operation. Это поле может не записываться, если Request State имеет значение COMPLETED.

Operation Data Present - присутствуют данные операции

Это логическое поле указывает, имеются дополнительные данные для Operation Data.

Requested Operation Data - данные запрошенной операции

Это поле содержит данные, переданные агенту для завершения желаемой операции. Например, если операцией является добавление маршрута, Operation Data будет включать префикс маршрута, размер префикса и сведения о next-hop для вставки, а также конкретную таблицу маршрутизации, в которую помещается маршрут. При наличии Operation Data поле Operation Data Present **должно** иметь значение TRUE. Некоторые операции могут не предоставлять данных. В таких случаях поле Operation Data Present **должно** иметь значение FALSE, а это поле **должно** быть пустым. Поле может не соответствовать данным, использованным для операции, фактически применённой к агенту.

При аутентификации клиента агентом в Requested Operation Data **должен** указываться приоритет клиента. **Могут** записываться другие атрибуты, использованные для аутентификации, такие как свидетельства.

Applied Operation Data - данные примененной операции

Это поле содержит данные, которые были фактически применены как часть Applied Operation. Если агент не может выполнить Requested Operation с Requested Operation Data, это поле может отличаться от Requested Operation Data. Поле остаётся пустым, если не задано Requested Operation Data. Поле может не записываться, если Request State отличается от COMPLETED.

Transaction ID - идентификатор транзакции

Идентификатор транзакции указывает, что эта конкретная операция является частью длительной транзакции I2RS, состоящей из множества связанных операций I2RS. Используя это значение можно связать вместе журнальные записи, поскольку они относятся к одной общей операции I2RS. Это поле не обязательно и может не записываться, если событие не является частью длительной транзакции.

Result Code - код результата

Это поле содержит результат операции после Request State со значением COMPLETED. Для операций RIB это **должен** быть код возврата, указанный в разделе 4 [RIBINFO]. Операция может не завершиться с кодом результата, если возникнет тайм-аут. Если при операции возник отказ, **должна** записываться попытка операции с соответствующим кодом результата.

Timeout Occurred - возник тайм-аут

Это логическое поле указывает, был ли тайм-аут при выполнении операции. При значении этого поля true в Ending Timestamp **должно** указываться время, когда агент зафиксировал тайм-аут. Это поле может не записываться, если Request State отличается от COMPLETED.

Ending Timestamp - временная метка завершения

Время, когда операция I2RS вышла из указанного состояния Request State в агенте I2RS. Если запись журнала охватывает всю продолжительность запроса, это будет время достижения запросом завершающей точки в агенте. Поле **должно** присутствовать во всех записях, которые задают завершение смены состояния, а также в записях, которые указывают всю продолжительность запроса. Время указывается полной меткой в формате [RFC3339], включая дату и часовой пояс (смещение от UTC. Описание подходящего формата приведено выше (Starting Timestamp).

End Of Message - конец сообщения

Каждой записи журнала следует включать подходящий индикатор конца сообщения (End Of Message или EOM). Подробности приведены в параграфе 5.3. Маркер конца сообщения.

5.3. Маркер конца сообщения

Из-за изменчивости полей журнала I2RS разработчики **должны** использовать подходящий для формата идентификатор конца сообщения (End Of Message или EOM), указывающий завершение отдельной записи. Независимо от формата, журнал I2RS **должен** обеспечивать чёткий способ отделения конца одной записи от начала другой. Например, в журнале с линейным форматом (как в syslog) маркером EOM может служить перевод строки. В журнале с форматом XML схема будет предусматривать теги элементов, указывающих начало и конец записи. В журнале JSON разделение записей обеспечивает синтаксис (вероятно с помощью разделённых запятыми элементов массива).

6. Примеры

В этом разделе приведён образец полей с возможными значениями.

```
Event ID: 1
Starting Timestamp: 2013-09-03T12:00:01.21+00:00
Request State: COMPLETED
Client ID: 5CEF1870-0326-11E2-A21F-0800200C9A66
Client Priority: 100
Secondary ID: com.example.RoutingApp
Client Address: 2001:db8:c0c0::2
Requested Operation: ROUTE_ADD
Applied Operation: ROUTE_ADD
Operation Data Present: TRUE
Requested Operation Data: PREFIX 2001:db8:feed:: PREFIX-LEN 64
NEXT-HOP 2001:db8:cafe::1
Applied Operation Data: PREFIX 2001:db8:feed:: PREFIX-LEN 64
NEXT-HOP 2001:db8:cafe::1
Transaction ID: 2763461
Result Code: SUCCESS(0)
Timeout Occurred: FALSE
Ending Timestamp: 2013-09-03T12:00:01.23+00:00
```

7. Эксплуатационные рекомендации

Конкретные процедуры, связанные с временным хранилищем журнала, заменой и поиском файлов, доступом к журналам трассировки I2RS выходят за рамки этого документа. Организации, ведущие журналы трассировки I2RS, отвечают за организацию надлежащих рабочих процедур, соответствующих конкретным требованиям и операционной среде. В этом разделе приведены лишь базовые фундаментальные рекомендации, независимые от реализации.

7.1. Создание журнала отслеживания

Агент I2RS взаимодействует с функциями маршрутизации и сигнализации элемента маршрутизации. Поскольку агент I2RS отвечает за фактическое внесение изменений в маршруты на связанном с ним сетевом устройстве, он создаёт и поддерживает журнал операций, который можно извлечь для устранения неполадок, связанных с влиянием I2RS на сеть. Изменения в локальной конфигурации элементов сети выходят за рамки протокола I2RS вытесняют состояние I2RS и будут регистрироваться лишь при уведомлении агента I2RS элементом сети.

7.2. Временное хранилище для журнала

Сведения трассировки могут временно храниться в буфере оперативной памяти или в локальном файле у агента. Следует учитывать число операций I2RS, ожидаемых на данном агенте для определения подходящего носителя данных и обеспечения максимальной эффективности журнала при минимальном влиянии на производительность и работоспособность агента. Запросы клиентов могут не всегда обрабатываться синхронно или в ограниченном интервале времени. Поэтому для гарантии попадания полей журнала, таких как Operation и Result Code в одну запись может потребоваться буферизация журнальных записей, которая может привести к дополнительной нагрузке на ресурсы агента и элементы сети.

В параграфе 7.3 обсуждается ротация журнала трассировки для сохранения истории операций без исчерпания ресурсов агента или сетевого устройства. Поэтому вполне разумно использовать буфер в памяти для недавних операций, а также применять архивирование и ротацию прошлых операций в локальных файлах.

В задаче этого документа не входит указание деталей реализации (размера, пропускной способности, защиты данных и т. п.) физического хранилища журнальных файлов I2RS. В части сохранения данных следует учитывать продолжительность хранения записей трассировки I2RS, если эти данные содержат атрибуты, относящиеся к безопасности или приватности. Чем дольше хранятся такие данные, тем серьезней будет влияние возможной утечки. Законодательство может устанавливать свои требования к минимальному и/или максимальному сроку хранения некоторых видов данных.

7.3. Ротация файлов журнала

Для предотвращения исчерпания ресурсов агента I2RS или связанного с ним сетевого устройства агентам I2RS **рекомендуется** реализовать ротацию журналов. Детали этого выходят за рамки документа и остаются за реализацией. Однако следует поддерживать ротацию файлов по времени или размеру текущего журнала. Если поддерживается кольцевая ротация (rollover), рекомендуется сохранять несколько архивных файлов для достижения максимальных преимуществ при устранении неполадок и учёте.

7.4. Поиск журналов

Разработчики могут предоставлять свои фирменные (proprietary) интерфейсы и разрабатывать собственные инструменты для поиска и отображения журналов трассировки I2RS. Это может включать просмотр журналов I2RS на консоли через командный интерфейс (command-line interface или CLI). Однако основная цель определения этой информационной модели заключается в создании независимого от производителей согласованного интерфейса для сбора данных трассировки I2RS. Извлечение данных также должно быть независимым от производителя.

Несмотря на то, что экспорт журнала трассировки I2RS может быть бесценным диагностическим инструментом для автономного (off-box) анализа, **недопустимо** его влияние на возможности клиента обрабатывать новые входящие операции.

В трёх следующих параграфах рассмотрены возможные способы доступа к журналам трассировки. Поддержка подписки и публикации I2RS (pub/sub) для доступа к журналам обязательна для реализации.

7.4.1. Поиск через Syslog

Протокол syslog [RFC5424] является стандартным способом передачи уведомлений о событиях от хоста к сборщику. Однако этот протокол не задаёт стандартного формата для хранения сообщений, поэтому разработчикам трассировки I2RS приходится создавать свои форматы. Поэтому, несмотря на соответствие данных в сообщении syslog этой информационной модели и возможности их представления человеку, они могут быть малоприспособлены для машинного анализа. Syslog **можно** применять как средство извлечения и распространения содержимого журналов трассировки I2RS.

Если syslog применяется для извлечения журналов трассировки, следует использовать имеющуюся инфраструктуру ведения журналов и возможности syslog [RFC5424] без необходимости определять и расширять имеющиеся форматы. Поля, описанные в параграфе 5.2, **следует** моделировать и кодировать как структурированные элементы данных (Structured Data Element или SD-ELEMENT) в соответствии с параграфом 6.3.1 в [RFC5424].

7.4.2. Извлечение через сбор информации I2RS

В параграфе 7.7 описания архитектуры I2RS [RFC7921] задан механизм для сбора сведений, включающий получение «моментальных снимков» (snapshot) большого объёма данных от элементов сети. Цель I2RS заключается в обеспечении доступности таких данных независимо от разработчика. Поэтому журналы трассировки I2RS **следует** делать доступными для механизма сбора сведений I2RS в форме моментальных снимков или потока подписки.

7.4.3. Извлечение через подписку и публикацию I2RS

В параграфе 7.6 спецификации архитектуры I2RS [RFC7921] описаны механизмы уведомлений для потока изменений, происходящих на уровне I2RS. Требования к системе подписки и публикации I2RS заданы в [RFC7923]. Агенты I2RS должны поддерживать публикацию сведений из журнала трассировки I2RS в канале, описанном в [RFC7923]. Подписчики будут получать прямую трансляцию взаимодействий I2RS в формате журнала трассировки и смогут гибко выбирать свои действия по сообщениям из журналов. Например, подписчики могут записывать сообщения в хранилище данных, агрегировать и обобщать взаимодействия от одного клиента и т. д. Спектр возможных действий почти безграничен, а детали их выполнения выходят за рамки этого документа.

8. Вопросы безопасности

Журнал трассировки I2RS, как и другие журнальные файлы, раскрывает состояние создавшего его объекта, а также идентификационные сведения и детали взаимодействий в содержащей объект системе. Описанная в этом документе информационная модель сама по себе не создаёт проблем безопасности, но может задавать набор атрибутов, включаемых в журнал I2RS. Эти атрибуты могут содержать деликатные сведения и поэтому должны соответствовать правилам безопасности, приватности и разрешений организации, использующей файлы журналов I2RS.

В задачи этого документа не входит указание мер защиты хранимых журнальных файлов, но предполагаются адекватные меры предосторожности и проверенные методы защиты, такие как шифрование дисков, подобающее ограничение доступа к файлам и каталогам, физическая защита объектов с журналами, взаимная аутентификация, транспортное шифрование, защита конфиденциальности и целостности при передаче файлов журнала. Кроме того, представляющиеся деликатными сведения в журнальном файле **следует** должным образом обезличивать или «затемнять» (obfuscate) для обеспечения приватности.

9. Литература

9.1. Нормативные документы

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <<http://www.rfc-editor.org/info/rfc3339>>.
- [RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, DOI 10.17487/RFC5424, March 2009, <<http://www.rfc-editor.org/info/rfc5424>>.
- [RFC7921] Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", RFC 7921, DOI 10.17487/RFC7921, June 2016, <<http://www.rfc-editor.org/info/rfc7921>>.
- [RFC7923] Voit, E., Clemm, A., and A. Gonzalez Prieto, "Requirements for Subscription to YANG Datastores", RFC 7923, DOI 10.17487/RFC7923, June 2016.

9.2. Дополнительная литература

- [RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <<http://www.rfc-editor.org/info/rfc6536>>.
- [RFC7920] Atlas, A., Ed., Nadeau, T., Ed., and D. Ward, "Problem Statement for the Interface to the Routing System", [RFC 7920](#), DOI 10.17487/RFC7920, June 2016, <<http://www.rfc-editor.org/info/rfc7920>>.
- [RIBINFO] Bahadur, N., Ed., Kini, S., Ed., and J. Medved, "Routing Information Base Info Model", Work in Progress¹, draft-ietf-i2rs-rib-info-model-08, October 2015.

¹Опубликовано в [RFC 8430](#). Прим. перев.

Благодарности

Авторы благодарны Alia Atlas за исходные отклики и общую поддержку работы. Спасибо Alvaro Retana, Russ White, Matt Birkner, Jeff Haas, Joel Halpern, Dean Bogdanovich, Ignas Bagdonas, Nobo Akiya, Kwang-koog Lee, Sue Hares, Mach Chen, Alex Clemm, Stephen Farrell, Benoit Claise, Les Ginsberg, Suresh Krishnan, Elwyn Davies за их рецензии, текст для документа и предложенные улучшения.

Адреса авторов

Joe Clarke

Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
United States
Phone: +1-919-392-2867
Email: jclarke@cisco.com

Gonzalo Salgueiro

Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
United States
Email: gsalguei@cisco.com

Carlos Pignataro

Cisco Systems, Inc.
7200-11 Kit Creek Road
Research Triangle Park, NC 27709
United States
Email: cpignata@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru