Internet Engineering Task Force (IETF) R. Arends
Request for Comments: 9567 M. Larson
Category: Standards Track ICANN
ISSN: 2070-1721 April 2024

DNS Error Reporting

Отчёты об ошибках DNS

Аннотация

Отчёты об ошибках DNS - это облегченный механизм информирования, предоставляющий администратору полномочного сервера сведений о записях ресурсов DNS, которые не удалось распознать или подтвердить (проверить). Владелец домена или поддерживающая DNS организация могут использовать такие отчёты для улучшения поддержки доменов. Отчёты основаны на расширенных ошибках DNS, описанных в RFC 8914.

Когда доменное имя не удаётся распознать или проверить из-за неверной конфигурации или атаки, оператор полномочного сервера может не знать об этом. Для смягчения проблемы отсутствия обратной связи этот документ предлагает метод, позволяющий проверяющему распознавателю автоматически сообщать об ошибке агенту мониторинга, указанному полномочным сервером. Ошибка кодируется в QNAME, таким образом сама отправка запроса является отчётом об ошибке.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9567.

Оглавление

1. Введение....1
2. Уровни требований....2
3. Терминология....2
4. Обзор....2
4.1. Пример....2
5. Спецификация опции EDNS0....2
6. Спецификация отчётов об ошибках DNS....3
6.1. Спецификация отвечающего распознавателя....3
6.1.1. Создание запроса отчёта....3
6.2. Спецификация полномочного сервера....3
6.3. Спецификация агента мониторинга....3
7. Взаимодействие с IANA....3
8. Вопросы эксплуатации....4
8.1. Выбор домена агента....4
8.2. Управление оптимизацией кэширования....4
9. Вопросы безопасности....4
10. Литература....5
10.1. Нормативные документы....5
10.2. Дополнительная литература....5
Благодарности....5
Адреса авторов....5

1. Введение

При обслуживании полномочным сервером устаревшей зоны с подписью DNSSEC криптографические подписи для наборов записей о ресурсах (resource record set или RRset) могут теряться и проверяющий распознаватель не сможет подтвердить эти записи. Аналогичная ситуация возникает и при несоответствии записей подписавшего делегирование (Delegation Signer или DS) в родительской зоне ключу подписи в дочерней зоне.

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

Эти два случая отказов могут в течение некоторого времени оставаться незаметными для оператора зоны.

В настоящее время нет прямых взаимоотношений между операторами проверяющих распознавателей и полномочных серверов. Отказы часто воспринимаются конечными пользователями по косвенным признакам и сведения об этом передаются (не всегда) по электронной почте или через социальные сети. Невозможно автоматически оповещать об отказах при проверке записей. Сведения об ошибках и предупреждениях могут скрываться в журнальных файлах распознавателей или не фиксироваться совсем.

В этом документе описан метод, который проверяющие распознаватели могут применять для автоматического информирования об ошибках при проверке DNSSEC. Это позволяет полномочному серверу указать агент мониторинга, которому проверяющие распознаватели могут сообщать о проблемах (если они настроены на это). Забота об информировании при отказах ложится на проверяющие распознаватели. Важно, чтобы издержки, связанные с информированием об отказах, были невелики и не оказывали существенного влияния на основные функции. Для этого с целью отправки отчётов об ошибках используется непосредственно DNS.

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), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Терминология

В документе применяется терминология DNS из BCP 219 [RFC9499], а также определён ряд терминов.

Reporting resolver - информирующий распознаватель
: Проверяющий распознаватель, поддерживающий отчёты об ошибках DNS.

Report query - запрос отчета
: Запрос DNS, применяемый для отчёта об ошибке. Этот запрос относится к типу записей о ресурсах DNS TXT. Содержимое отчёта кодируется в QNAME запроса DNS к агенту мониторинга.

Monitoring agent - агент мониторинга
: Полномочный сервер, получающий запросы отчётов и отвечающий на них. Агент указывается доменным именем (домен агента).

Agent domain - домен агента
: Доменное имя, возвращаемое в опции EDNS0 Report-Channel и указывающее, куда распознаватели DNS могут направлять отчёты об ошибках.

4. Обзор

Полномочный сервер указывает поддержку отчётов об ошибках DNS включением в отклик опции EDNS0 Report-Channel с OPTION-CODE=18 и домена агента. Агент указывается полным доменным именем без сжатия в формате передачи DNS. Полномочному серверу **недопустимо** включать эту опцию в отклик, если имя домена агента пусто или указано null-меткой (указывает корень DNS). Полномочный сервер включает опцию EDNS0 Report-Channel без её запроса, т. е. независимо от наличия этой опции в запросе.

Если полномочный сервер указал поддержку отчётов об ошибках DNS и имеется проблема, о которой можно сообщить с помощью расширенных ошибок DNS, сообщающий распознаватель кодирует отчёт об ошибке в QNAME запроса отчёта. Отвечающий распознаватель создаёт QNAME путём конкатенации метки _er, QTYPE, QNAME, вызвавшего отказ, расширенного кода ошибки DNS (в соответствии с [RFC8914]), ещё одной метки _er и домена агента. Пример представлен в параграфе 4.1, а спецификация - в параграфе 6.1.1. Отметим, что обычный код RCODE не включается, поскольку он не относится к расширенным кодам ошибок DNS. Полученный в результате запрос передаётся отвечающим распознавателем как стандартный запрос DNS для записи TXT.

Запрос отчёта в конечном счёте поступает к агенту мониторинга, возвращающему отклик, который может кэшироваться отвечающим распознавателем. Это кэширование очень важно, поскольку оно снижает число запросов отчётов, передаваемых отвечающим распознавателем для одной и той же проблемы (т. е. при кэшировании отправляется лишь 1 запрос в интервале TTL). Число запросов отчётов об ошибках может быть снижено путём оптимизаций, подобных описанным в [RFC8020] и [RFC8198].

В этом документе не даётся рекомендаций по содержимому RDATA в записях TXT.

4.1. Пример

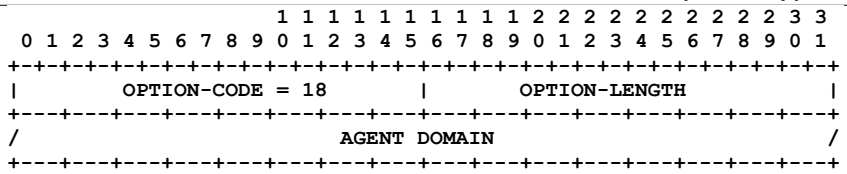
Отвечающий распознаватель передаёт для имени broken.test. запрос тип A. Домен test. размещён на нескольких полномочных серверах, один из которых обслуживает устаревшую версию зоны (test.). На этом сервере задан домен агента a01.agent-domain.example. При получении этим сервером запроса для broken.test. он будет передавать отклик с опцией EDNS0 Report-Channel и доменным именем a01.agent- domain.example.

Отвечающий распознаватель не сможет проверить broken.test. RRset для типа A (тип 1 для RR), поскольку запись RRSIG является просроченной. Распознаватель создаёт QNAME _er.1.broken.test.7._er.a01.agent-domain.example. и распознает это имя. QNAME указывает расширенную ошибку DNS 7, возникшую при попытке подтвердить broken.test. для типа A (тип 1 для RR).

При получении этого запроса агентом мониторинга (оператор полномочного сервера для a01.agent-domain.example.) агент может определить, что зона test. содержит просроченную подпись (расширенная ошибка DNS 7) для типа A применительно к имени broken.test.. Агент мониторинга может связаться с операторами test. для исправления ошибки.

5. Спецификация опции EDNS0

Метод использует опцию EDNS0 [RFC6891] для указания домена агента в откликах DNS, как показано на рисунке.



OPTION-CODE

2-октетный код EDNS0, используемый в опции EDNS0 для индикации поддержки отчётов об ошибках. Этот код опции EDNS0 называется Report-Channel.

OPTION-LENGTH

2-октетное значение размера поля AGENT DOMAIN в октетах.

AGENT DOMAIN

Полное доменное имя [RFC9499] в формате передачи DNS без сжатия.

6. Спецификация отчётов об ошибках DNS

Ошибки, о которых может сообщать отвечающий распознаватель, указаны в [RFC8914]. Отметим, что распознаватель может поддерживать не все указанные там ошибки и этот документ не указывает, что считается ошибкой.

Класс DNS не указывается в отчётах об ошибках.

6.1. Спецификация отвечающего распознавателя

Следует соблюдать осторожность, если требуется дополнительное распознавание DNS для распознавания QNAME с отчётом об ошибке. Такое распознавание может само по себе вызывать создание ещё одного отчёта об ошибке. Для предотвращения каскада ошибок **должно** устанавливаться ограничение максимального расхода или глубины.

В запросы **недопустимо** включать опцию EDNS0 Report-Channel.

Отвечающему распознавателю **недопустимо** использовать отчёт об ошибках DNS, если полномочный сервер вернул пустое поле AGENT DOMAIN в опции EDNS0 Report-Channel.

Чтобы агент мониторинга имел большую уверенность в достоверности отчёта, отвечающему распознавателю **следует** передавать отчёты об ошибках по протоколу TCP [RFC7766] или иному протоколу с явным соединением, а также **следует** использовать DNS Cookie [RFC7873]. Это затруднит подмену адреса источника.

Отвечающий распознаватель **должен** проверять полученные от агента мониторинга отклики. Для откликов на запросы отчётов об ошибках не предусмотрено специальной обработки. Обоснование этого приведено в разделе 9.

6.1.1. Создание запроса отчёта

QNAME для запроса отчёта создаётся путём конкатенации указанных ниже элементов.

- Метка, содержащая строку _er.
- QTYPE из запроса, вызвавшего расширенную ошибку DNS, в виде десятичного значения в одной метке DNS. При наличии в запросе дополнительных QTYPE, как описано в [MULTI-QTYPES], они представляются уникальными упорядоченными десятичными значениями через дефис (-). Например при наличии в запросе QTYPE A и AAAA они представляются как метка 1-28.
- Список непустых меток, представляющих имя запроса, вызвавшего отчёт об ошибке DNS.
- Расширенный код ошибки DNS, представленный десятичным значением в одной метке DNS.
- Метка, содержащая строку _er.
- Домен агента, полученный в опции EDNS0 Report-Channel от полномочного сервера.

Передача запроса отчёта с QNAME размером более 255 октетов **недопустима**.

Метки _er позволяют агенту мониторинга отличать домен агента и имя в вызвавшем ошибку запросе. Если домен агента указан пустым именем или null-меткой (несмотря на запрет этого данной спецификацией), запрос отчёта будет иметь _er в качестве домена верхнего уровня, а не домен верхнего уровня из вызвавшего ошибку запроса. Назначение первой метки _er состоит в индикации получения полного запроса отчёта (а не сокращённого путём минимизации).

6.2. Спецификация полномочного сервера

Полномочному серверу **недопустимо** включать в отклик более одной опции EDNS0 Report-Channel. Полномочный сервер включает в отклики опцию EDNS0 Report-Channel без запроса. Наличие EDNS0 Report-Channel в запросах не требуется.

6.3. Спецификация агента мониторинга

Полномочному серверу для домена агента **рекомендуется** возвращать позитивный отклик (без NODATA и NXDOMAIN) с записью TXT.

Агенту мониторинга **следует** отвечать на запросы без DNS Cookie, полученные по протоколу UDP, откликом с битом отсечки (TC), чтобы предложить распознавателю передать запрос по протоколу TCP.

7. Взаимодействие с IANA

Агентство IANA выделило указанный в таблице 1 код в реестре DNS EDNS0 Option Codes (OPT).

Таблица 1.

Значение	***Имя***	***Статус***	***Документ***
18	Report-Channel	Standard	RFC 9567

Агентство IANA выделило указанный в таблице 2 код в реестре Underscored and Globally Scoped DNS Node Names.

Таблица 2.

Тип RR	***Имя узла***	***Документ***
TXT	_er	RFC 9567

8. Вопросы эксплуатации

8.1. Выбор домена агента

Имя домена агента рекомендуется делать достаточно коротким, чтобы в запрос отчёта можно было включить более длинное значение QNAME. В качестве домена агента **недопустимо** указывать поддомен домена, для которого передаются отчёты. Например, если полномочный сервер обслуживает домен foo.example, **недопустимо** использовать домен агента с суффиксом foo.example.

8.2. Управление оптимизацией кэширования

Отвечающий распознаватель может оптимизировать кэширование для предотвращения передачи множества отчётов об ошибке одному и тому же агенту мониторинга.

Если агент мониторинга возвращает NXDOMAIN (ошибка имени), в соответствии с [RFC8020] любое имя в этом домене или его иерархии считается недоступным и негативное кэширование будет предотвращать последующие запросы для всего, что находится в этом домене или его иерархии, на время, определяемое TTL негативного отклика [RFC2308]. Поскольку агент мониторинга может не знать содержимого всех зон, для которых он служит агентом, ему **недопустимо** передавать NXDOMAIN для отслеживаемых доменов, поскольку это может препятствовать последующим запросам. Одним из методов предотвращения NXDOMAIN является использование шаблонного имени домена [RFC4592] в зоне для домена агента.

При подписанном домене агента распознаватель может использовать интенсивное негативное кэширование (см. [RFC8198]). Эта оптимизация использует записи NSEC и NSEC3 (без opt-out) и позволяет распознавателю синтезировать шаблонные имена. В таких случаях распознаватель не передаёт последующих запросов, поскольку может синтезировать отклик из кэшированных сведений.

Решением является отказ от DNSSEC для домена агента. Подписание домена агента создаёт дополнительную нагрузку на отвечающий распознаватель, поскольку тому приходится проверять отклик, который на деле не приносит пользы распознавателю, кроме снижения числа запросов на отчеты.

9. Вопросы безопасности

При использовании отчётов об ошибках DNS агент мониторинга может узнать об ошибках в настройке конфигурации отвечающего распознавателя, таких как устаревшие привязки доверия DNSSEC.

Отчёты об ошибках DNS **следует** выполнять с использованием минимизации имён в запросах DNS [RFC9156] для повышения уровня приватности.

Отчёты DNS выполняются без какой-либо проверки подлинности между отвечающим распознавателем и полномочным сервером домена агента.

Распознавателям **следует** передавать отчёты об ошибках по протоколу TCP [RFC7766] или использовать DNS Cookie [RFC7873]. Это осложнит подмену адреса отправителя. Агенту мониторинга **следует** отвечать на полученные по протоколу UDP запросы без DNS Cookie откликом с установленным битом отсечки (TC), чтобы предложить распознавателю передавать запросы по протоколу TCP.

Общеизвестные адреса отвечающих распознавателей могут обеспечить более высокий уровень доверия к отчётам об ошибках, а также позволить автоматизированную обработку отчётов.

Агентам мониторинга, получающим отчёты об ошибках по протоколу UDP, следует учитывать, что адрес отправителя и сам отчёт могут быть поддельными.

Описанный в документе метод вызывает дополнительны запросы отвечающих распознавателей к полномочным серверам для распознавания запросов отчёта. Этим методом можно злоупотреблять, намеренно создавая зоны с нарушениями и доменами агентов, делегированными жертвам. Это особенно эффективно, когда запросы DNS, вызывающие ошибку, передаются через открытые распознаватели или сильно распределенные системы мониторинга, выполняющие распределенные по всему миру запросы.

Злоумышленник может организовать лавинную отправку отчётов об ошибках для маскирования атаки.

Хотя этот документ не задаёт содержимого RDATA в записях TXT, при записи содержимого RDATA в системный журнал агент мониторинга **должен** предполагать возможную вредоносность этого содержимого и принимать соответствующие меры для предотвращения использования такого содержимого. Одним из решений является запись в журнал в шестнадцатеричном формате, что позволяет предотвратить возможность исполнения кода, представленного строками, как в уязвимости, описанной в [CVE-2021-44228].

Необходимость обязательной проверки DNSSEC для откликов от агента отчётов (даже если домен предлагается оставлять неподписанным) обусловлена снижением риска атак на понижение, организованных злоумышленниками. При таких атаках легитимно подписанный домен жертвы злоумышленники могут обманным путём выдавать за домен агента. Если проверяющий распознаватель считает его неподписанным, он раскрывается для атак с отравлением кэша. Принудительная проверка DNSSEC позволяет заранее устранить эту уязвимость.

10. Литература

10.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Дополнительная литература

[CVE-2021-44228] CVE, "CVE-2021-44228", 26 November 2021, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>.

[MULTI-QTYPES] Bellis, R., "DNS Multiple QTYPEs", Work in Progress, Internet-Draft, draft-ietf-dnssd-multi-qtypes-00, 4 December 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-multi-qtypes-00>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <https://www.rfc-editor.org/info/rfc2308>.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, DOI 10.17487/RFC4592, July 2006, <https://www.rfc-editor.org/info/rfc4592>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP — Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873>.

[RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", RFC 8020, DOI 10.17487/RFC8020, November 2016, <https://www.rfc-editor.org/info/rfc8020>.

[RFC8198] Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198, July 2017, <https://www.rfc-editor.org/info/rfc8198>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/info/rfc9156>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

Благодарности

Этот документ основан на идее Roy Arends и David Conrad. Авторы благодарны Peter van Dijk, Stephane Bortzmeyer, Shane Kerr, Vladimir Cunat, Paul Hoffman, Philip Homburg, Mark Andrews, Libor Peltan, Matthijs Mekking, Willem Toorop, Tom Carpay, Dick Franks, Ben Schwartz, Yaron Sheffer, Viktor Dukhovni, Wes Hardaker, James Gannon, Tim Wicinski, Warren Kumari, Gorry Fairhurst, Benno Overeinder, Paul Wouters, Petr Spacek за их вклад в работу.

Адреса авторов

Roy Arends
ICANN
Email: roy.arends@icann.org

Matt Larson
ICANN
Email: matt.larson@icann.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru