Internet Engineering Task Force (IETF)
Request for Comments: 9606
Category: Standards Track
ISSN: 2070-1721

T. Reddy.K
Nokia
M. Boucadair
Orange

June 2024

DNS Resolver Information

Сведения о распознавателе DNS

Аннотация

Этот документ задаёт для распознавателей DNS метод публикации сведений о себе. Клиенты DNS могут использовать эти сведения для определения возможностей распознавателя DNS. Способ использования сведений клиентами DNS выходит за рамки этого документа.

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/rfc9606.

Оглавление

1. Введение

Исторически сложилось так, что клиенты DNS взаимодействуют с распознавателями без необходимости знать что-либо о поддерживаемых теми функциях. Однако все больше рекурсивных распознавателей поддерживает разные функции, что может влиять на предоставляемые ими услуги DNS (сохранение приватности, фильтрация, прозрачность поведения и т. п.). Клиенты DNS могут находить и аутентифицировать распознаватели DNS с поддержкой шифрования в своей локальной сети, используя, например, протоколы обнаружения назначенных сетью распознавателей (Discovery of Network-designated Resolvers или DNR) [RFC9463] и обнаружения назначенных распознавателей (Discovery of Designated Resolvers или DDR) [RFC9462]. Однако эти клиенты DNS не могут получить от найденных рекурсивных распознавателей сведений об их возможностях для процесса выбора распознавателя. Вместо того, чтобы приспосабливаться к распознавателям, клиентам DNS нужны более надёжные механизмы определения функций, настроенных на этих распознавателях.

Данный документ задаёт механизм, позволяющий передавать клиентам DNS сведения о распознавателях DNS в процессе выбора распознавателя. Например, процедура выбора распознавателя может использовать извлечённые сведения о распознавателях для установки более высокого приоритета сохраняющим приватность распознавателям по отношению к не поддерживающим минимизацию QNAME [RFC9156].Другим примером является выбор клиентом DNS

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

распознавателя на основе возможностей фильтрации. Например, клиент DNS может выбрать распознаватель, фильтрующий домены на основе правил безопасности с блокировкой расширенных ошибок (Blocked (15) Extended DNS Error или EDE) [RFC8914]. Как вариант, клиент может использовать правило отказа от выбора распознавателей, подменяющих отклики с использованием Forged Answer (4) EDE. Однако определение процедур и правил выбора выходит за рамки документа. Если явно не указано иное, этот документ не влияет на операции распознавателя после выбора распознавателя клиентом DNS.

Документ определяет новый тип записи о ресурсах (resource record или RR), позволяющий клиентам DNS подавать запросы к рекурсивным распознавателям. Исходные сведения, которые может захотеть предоставлять распознаватель, указаны в разделе 5. Эта информация включает свойства, влияющие на политику приватности и прозрачности распознавателя. В будущем могут регистрироваться и другие сведения, как указано в параграфе 8.2. Сведения о распознавателях не предназначены для конечного пользователя.

2. Термины

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.

В документе применяются термины, определённые в [RFC9499], а также приведённые ниже термины.

Encrypted DNS - DNS с шифрованием
: Схема DNS где обмен сообщениями DNS выполняется по шифрованному каналу между клиентом и сервером DNS (например, DNS over HTTPS (DoH) [RFC8484], DNS over TLS (DoT) [RFC7858], DNS over QUIC (DoQ) [RFC9250]).

Encrypted DNS resolver - распознаватель DNS с шифрованием
: Распознаватель DNS, поддерживающий схему DNS с шифрованием.

Reputation - репутация
: Оценка, получаемая идентифицируемым участником в сообществе или Internet в целом, как указано в разделе 1 [RFC7070].

3. Извлечение сведений о распознавателе

Клиент DNS, желающий получить сведения о распознавателе, может использовать RR типа RESINFO, определённого в этом документе. Содержимое RDATA в отклике на запрос RESINFO RR QTYPE описано в разделе 5. Если распознаватель понимает RESINFO RR, в RRset **должна** включаться единственная запись. Клиенты DNS **должны** игнорировать недействительные записи. RESINFO - это свойство распознавателя, а не субъект рекурсивного распознавания.

Клиент DNS может извлекать сведения о распознавателе и помощью RESINFO RR и QNAME доменного имени, применяемого для аутентификации распознавателя DNS и названного Authentication Domain Name (ADN) в DNR [RFC9463].

Если применяется специальное имя resolver.arpa, определённое в [RFC9462], для обнаружения распознавателей DNS с шифрованием, клиент может получить сведения о распознавателе с помощью RESINFO RR и QNAME resolver.arpa. В этом случае клиенту придётся сталкиваться с риском отсутствия поддержки распознавателем типа RESINFO. Распознаватель может передать запрос выше (upstream) и тогда клиент может получить положительный отклик RESINFO от любого легитимного распознавателя DNS или от злоумышленника.

Клиент DNS **должен** сбрасывать (0) в запросе бит желательности рекурсии (Recursion Desired или RD). Клиент DNS **должен** отбрасывать отклик, если в нем сброшен (0) флаг AA, что указывает отсутствие у распознавателя DNS полномочий для данного отклика.

Если группа распознавателей имеет общий домен ADN и/или anycast-адрес, этим распознавателям **следует** раскрывать согласованные сведения RESINFO.

4. Формат сведений о распознавателе

Записи сведений о распознавателе имеют такой же формат, как DNS TXT. Правила для записей TXT заданы в базовой спецификации DNS (параграф 3.3.14 в [RFC1035]) и более подробно описаны в спецификации обнаружения служб на основе DNS (DNS-based Service Discovery или DNS-SD) (параграф 6.1 в [RFC6763]). Рекомендации по ограничению размера записей TXT рассмотрены в параграфе 6.1 [RFC6763].

Подобно DNS-SD, тип RESINFO RR использует пары ключ-значение для передачи сведений о распознавателе. Каждая пара кодируется с использованием правил, заданных в параграфе 6.3 [RFC6763]. Использование стандартизованного синтаксиса для типа RESINFO RR упрощает определение новых ключей. Если клиент DNS встречает в RESINFO RR неизвестный ключ, он **должен** игнорировать его. Для ключей RESINFO **должны** применяться правила параграфа 6.4 [RFC6763].

Ключи сведений о распознавателе **должны** быть определены в реестре IANA (параграф 8.2) или начинаться с префикса temp-, обозначающего локальное использование.

5. Ключи и значения сведений о распознавателе

Ниже приведены определения ключей сведений о распознавателе.

qnamemin
: Наличие этого ключа указывает поддержку распознавателем DNS минимизации QNAME [RFC9156] для повышения уровня приватности DNS. Отметим, что в соответствии с правилами параграфа 6.4 в [RFC6763] отсутствие символа = делает ключ логическим атрибутом, не имеющим значения.
: Наличие ключа указывает, что распознаватель DNS настроен на минимизацию влияющих на приватность данных, передаваемых полномочному серверу имён.
: Этот атрибут является необязательным.

exterr

Если распознаватель DNS поддерживает опцию EDE, определённую в [RFC8914], для возврата дополнительных сведений о причинах ошибок DNS, значение этого ключа содержит коды EDE, которые может возвращать этот распознаватель DNS. Это может быть один или несколько кодов EDE. Диапазоны значений **должны** указываться через дефис (-), набор несмежных значений **должен** указываться через запятые.

Возвращаемые коды EDE (например, Blocked (15), Censored (16), Filtered (17)) показывают, настроен ли распознаватель DNS на раскрытие причин, по которым запрос был отфильтрован/заблокирован при возникновении соответствующего события. Если возможности распознавателя обновляются для включения новых похожих кодов, он может прервать сессию TLS, предлагая клиенту организовать новое соединение TLS и снова извлечь сведения о распознавателе. Это позволяет клиенту иметь актуальные сведения о возможностях распознавателя. При получении клиентом для запроса DNS кода EDE, не указанного в exterr, клиент может снова запросить распознаватель о его возможностях в части возврата новых кодов ошибок. Если несоответствие сохраняется, клиент может счесть сведения о распознавателе недостоверными и отбросить их.

Этот атрибут является необязательным.

infourl

Ссылка URL, указывающая базовые неструктурированные сведения о распознавателе (например, поддерживаемые DoH API, возможные коды статуса HTTP, возвращаемые сервером DoH, способы оповещения о проблемах) для поиска неполадок. Сервер, раскрывающий такие сведения, называется сервером сведений о распознавателе (resolver information server). Такой сервер **должен** поддерживать для сведений о распознавателе только тип содержимого text/html. Клиент DNS **должен** отвергать, как недействительные, URL с отличной от https схемой. Недействительные URL **должны** игнорироваться. Полученные по URL сведение **должны** рассматриваться лишь как диагностическая информация для персонала IT. Они не предназначены для конечных пользователей, поскольку могут вводить их в заблуждение.

Этот ключ может применяться персоналом IT для получения иных полезных сведений о распознавателе, а также для процедур информирования о проблемах (например, некорректная фильтрация).

Этот атрибут является необязательным.

Новые ключи могут создаваться по процедуре, указанной в параграфе 8.2.

6. Пример

На рисунке 1 представлен пример записи со сведениями о распознавателе.

```
resolver.example.net. 7200 IN RESINFO qnamemin exterr=15-17
                              infourl=https://resolver.example.com/guide
```

Рисунок 1. Пример записи сведений о распознавателе.

Как отмечено в разделе 3, клиент DNS, обнаруживший ADN resolver.example.net своего распознавателя с использованием DNR, будет передавать запрос RESINFO RR QTYPE для ADN и узнает, что:

- распознаватель поддерживает минимизацию QNAME;
- распознаватель может возвращать коды Blocked (15), Censored (16), Filtered (17);
- дополнительную информацию можно получить по ссылке https://resolver.example.com/guide.

7. Вопросы безопасности

Клиенты DNS, взаимодействующие с обнаруженными распознавателями DNS, **должны** использовать одну из указанных мер предотвращения атак с поддельными откликами DNS.

1. Организация аутентифицированного защищённого соединения с распознавателем DNS.
2. Реализация локальной проверки DNSSEC (раздел 10 в [RFC9499]) для контроля подлинности сведений о распознавателе.

Важно отметить, что для запросов resolver.arpa подходит лишь первый вариант.

Распознаватель с шифрованием может возвращать в RESINFO некорректные сведений. Если клиент не может проверить полученные от распознавателя атрибуты, которые будут служить для выбора распознавателя или отображаться конечному пользователю, клиенту следует обрабатывать такие атрибуты лишь при наличии у распознавателя с шифрованием достаточной в соответствии с локальной политикой репутации (например, настройки пользователя или администратора, встроенный список проверенных распознавателей). Такой подход ограничивает возможности злонамеренных распознавателей в части нанесения вреда ложными заявлениями.

8. Взаимодействие с IANA

8.1. Тип RESINFO RR

Агентство IANA обновило реестр Resource Record (RR) TYPEs в рамках группы реестров Domain Name System (DNS) Parameters [RRTYPE], как показано ниже.

```
Type:  RESINFO
Value:  261
Meaning:  Resolver Information as Key/Value Pairs
Reference:  RFC 9606
```

8.2. Регистрация ключей DNS Resolver Information

Агентство IANA создало новый реестр DNS Resolver Information Keys в рамках группы реестров Domain Name System (DNS) Parameters [IANA-DNS]. Этот реестр содержит определения ключей, которые могут применяться для предоставления сведений о распознавателях. Ключи добавляются в реестр по процедуре Specification Required (параграф 4.6 в [RFC8126]). Назначенным экспертам следует тщательно рассматривать влияние на безопасность в результате добавления ключа в этот реестр. Дополнительные подробности приведены в параграфе 8.3. Структура реестра приведена ниже.

Name

Имя ключа, которое должно соответствовать определению из раздела 4. В реестр IANA недопустимо включать имена с префиксом temp-, поскольку такие имена могут свободно применяться в любой реализации.

Description

Описание зарегистрированного ключа.

Reference

Указание документа со спецификацией зарегистрированного элемента.

Исходное содержимое реестра представлено в таблице 1.

Таблица 1. Исходное содержимое реестра DNS Resolver Information Keys.

Имя	***Описание***	***Документ***
qnamemin	Наличие этого ключа указывает поддержку минимизации QNAME.	RFC 9606
exterr	Список поддерживаемых кодов расширенных ошибок DNS. Это должны быть десятичные значения INFO-CODE из реестра Extended DNS Error Codes <https://www.iana.org/assignments/dns-parameters/>.	RFC 9606
infourl	Ссылка URL на неструктурированные сведения о распознавателе, используемые для устранения неполадок.	RFC 9606

8.3. Рекомендации для назначенных экспертов

Предполагается назначать несколько экспертов для рассмотрения запросов на включение в реестр.

Критерии, которым следует руководствоваться назначенным экспертам, включают проверку дублирования имеющихся записей, чёткость описания и соответствие целям данного реестра.

Запросы на регистрацию рассматриваются в течение двухнедельного срока по результатам рассмотрения одним или несколькими назначенными экспертами. В течение этого срока назначенные эксперты одобряют или отклоняют запрос и передают своё решение в IANA. При отказе следует включать объяснение причин и, при необходимости, рекомендации по внесению изменений для последующего одобрения запроса.

9. Литература

9.1. Нормативные документы

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[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>.

[RFC9462] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", RFC 9462, DOI 10.17487/RFC9462, November 2023, <https://www.rfc-editor.org/info/rfc9462>.

[RFC9463] Boucadair, M., Ed., Reddy.K, T., Ed., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", RFC 9463, DOI 10.17487/RFC9463, November 2023, <https://www.rfc-editor.org/info/rfc9463>.

9.2. Дополнительная литература

[IANA-DNS] IANA, "Domain Name System (DNS) Parameters", <https://www.iana.org/assignments/dns-parameters/>.

[RESINFO] Sood, P. and P. Hoffman, "DNS Resolver Information Self-publication", Work in Progress, Internet-Draft, draft-pp-add-resinfo-02, 27 June 2020, <https://datatracker.ietf.org/doc/html/draft-pp-add-resinfo-02>.

[RFC7070] Borenstein, N. and M. Kucherawy, "An Architecture for Reputation Reporting", RFC 7070, DOI 10.17487/RFC7070, November 2013, <https://www.rfc-editor.org/info/rfc7070>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[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>.

[RRTYPE] IANA, "Resource Record (RR) TYPEs", <https://www.iana.org/assignments/dns-parameters/>.

Благодарности

В этой спецификации используется документ [RESINFO].

Спасибо Tommy Jensen, Vittorio Bertola, Vinny Parla, Chris Box, Ben Schwartz, Tony Finch, Daniel Kahn Gillmor, Eric Rescorla, Shashank Jain, Florian Obser, Richard Baldry, Martin Thomson за обсуждения и комментарии.

Спасибо Mark Andrews, Joe Abley, Paul Wouters, Tim Wicinski за обсуждение правил форматирования RR.

Отдельная благодарность Tommy Jensen за тщательную вдумчивую рецензию Shepherd.

Спасибо Johan Stenstam и Jim Reid за рецензию dns-dir, Ray Bellis за рецензию выделения RRTYPE, Arnt Gulbrandsen за рецензию ART и Mallory Knodel за рецензию gen-art.

Спасибо Éric Vyncke за рецензию AD.

Спасибо Gunter Van de Velde, Erik Kline, Paul Wouters, Orie Steele, Warren Kumari, Roman Danyliw, Murray Kucherawy за рецензию IESG.

Адреса авторов

Tirumaleswar Reddy.K
Nokia
India
Email: kondtir@gmail.com

Mohamed Boucadair
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru