21 октября 2013 года

Часто задаваемые вопросы о Централизованной службе файлов корневой зоны

На конференции ICANN-47 в Дурбане персонал провел презентацию Централизованной службы файлов корневой зоны (известной тогда как CZDAP), которая является предлагаемым ICANN решением для увеличения объемов предоставления данных зоны в условиях, когда в интернете появляются сотни новых gTLD. В ходе этого заседания нам задали немало вопросов, на которые мы не имели возможности ответить из-за ограничений во времени. Ниже вы найдете ответы на эти и различные другие вопросы, связанные с CZDS. С дополнительными вопросами и ответами можно ознакомиться на справочных страницах: https://czds.icann.org/en/help

Конечный пользователь

Вопрос: Сможет ли пользователь изменить IP-адрес, который он использует для доступа?

Ответ: Да, вы можете указать один или более IP-адресов, с которых собираетесь связываться с серверами SFTP, в разделе «Профиль пользователя».

Вопрос: Если конечному пользователю предоставляется доступ к большому количеству TLD — например, 1400 — должен ли он загружать каждый файл данных отдельно?

Ответ: Нет, мы создали интерфейс программирования приложений CZDS (CZDS API) , систему с использованием токенов, которая позволяет осуществлять загрузку массивов учетных данных SFTP. Токен позволяет автоматизировать доступ, давая

возможность пользователям получать новые данные зоны без выполнения входа в систему вручную. В случаях, когда обнаруживается факт неправомерного использования, аннулирование срока действия токена (администратором CZDS или самими пользователями оператора регистратуры) приведет к тому, что любой скрипт уже не сможет выполнить дальнейшие загрузки, пока в него не будет введен новый, действующий токен пользователя.

Инструменты для загрузки массивов учетных данных SFTP уже созданы. Всю информацию об этих инструментах можно найти в хранилище ПО с открытым кодом по адресу:

https://github.com/fourkitchens/CZDS-tools

Вопрос: Возможно, было бы полезно иметь страницу загрузки, на которой были бы указаны все файлы, к которым я имею доступ, чтобы не открывать каждую страницу отдельно. Должна быть одна страница со списком всех TLD, которые мне доступны, и с ней должны быть связаны какие-то метаданные. Например, дата ее последнего обновления регистратурой и другая информация, которая предоставляется на FTP. Должна быть учетная запись FTP, где бы я мог все это посмотреть.

Ответ: В настоящее время такая функция отсутствует.

Вопрос: Существует ли возможность посмотреть какие-то архивные данные, например, за последнюю неделю или за последние четыре недели?

Ответ: Система такую функцию не предлагает.

Вопрос: Существует ли возможность оспорить отказ регистратуры?

Ответ: Соглашение об администрировании домена верхнего уровня требует, чтобы регистратура gTLD предоставляла данные зоны потребителю данных бесплатно. Если конечный пользователь считает, что регистратура несправедливо отказывает ему в доступе, или не получает ответа от регистратуры, то он может подать жалобу в отдел соблюдения договорных обязательств ICANN, который свяжется с регистратурой и изучит этот вопрос.

Операторы регистратур

Вопрос: Когда регистратуры новых gTLD должны будут начать предоставлять свои данные зоны? При подписании контракта, при техническом делегировании, или же этот вопрос еще не решен?

Ответ: Регистратуры новых gTLD должны начинать предоставлять свои данные зоны при делегировании.

Вопрос: Каким образом регистратуры размещают свои данные зоны в системе CZDS? Путем загрузки по FTP или в виде передачи зоны?

Ответ: Существуют две возможности: оператор регистратуры может контролировать свои данные, просто одобряя доступ и предоставляя пользователям (через CZDS) учетные данные для доступа к своему SFTP серверу, или же может разрешить ICANN периодически осуществлять передачу зоны (полную передачу зоны DNS — AXFR) и конфигурировать данные от своего имени, после чего пользователи смогут загружать эти данные непосредственно через систему CZDS.

Вопрос: Если оператор регистратуры выбирает вариант с предоставлением доступа к зоне через собственные системы, а не методом прямой загрузки через систему Централизованной службы файлов корневой зоны, то как будет происходить этот процесс?

Ответ: Оператор регистратуры должен выбрать в качестве метода загрузки «учетные данные SFTP». Когда конечный пользователь обратится с запросом, оператор регистратуры одобрит этот запрос и предоставит конечному пользователю имя сервера SFTP и учетные данные для входа. Конечный пользователь может затем получить данные на указанном хосте, введя имя пользователя и пароль, предоставленные ему в CZDS.

Перед тем как сохранить учетные данные, веб-сайт CZDS зашифрует их с помощью открытого ключа каждого пользователя в отдельности.

Вопрос: Каким образом оператору регистратуры следует предоставлять свой файл зоны в CZDS? Нужно ли отсылать файлы через API в несжатом виде?

Ответ: Оператор регистратуры должен предоставить свой ключ транзакционной подписи (ключ TSIG) и адрес сервера администратору CZDS и/или разрешить передачу файлов (AXFR) с IP-адресов из списка, указанного ICANN. ICANN выполнит передачу и предоставит данные в указанном формате для прямой загрузки конечным пользователем через CZDS.

Вопрос: Должны ли регистратуры новых gTLD предоставлять системе данные зоны?

Ответ: Да. Регистратура новых gTLD должна (согласно разделу 2 Спецификации 4 Соглашения об администрировании домена общего пользования верхнего уровня) предоставлять данные зоны тем конечным пользователям, которые их запросят. Кроме того, регистратуры новых gTLD должны использовать CZDS. Они могут сделать это, или разрешив ICANN выполнять передачу данных зоны, или предоставив имя своего SFTP-сервера с учетными данными, и тогда конечный пользователь сможет получать эти данные, не входя в систему.

Вопрос: Когда я стану регистратурой, то смогу ли одобрять все запросы автоматически?

Ответ: Вы можете одобрить сразу все запросы, выбрав «Все запросы» и нажав «Одобрить», но на данный момент отсутствует возможность «предварительно одобрить» все запросы по умолчанию. ICANN изучит возможность введения такой функции автоматического одобрения в одной из будущих версий.

Вопрос: Как оператор регистратуры узнает о поступлении запроса, который он должен одобрить или отклонить?

Ответ: Оператор регистратуры имеет возможность отключать или включать функцию уведомления по электронной почте. Таким образом, он может получать уведомление каждый раз, когда поступает новый запрос, однако, если количество запросов начнет достигать больших объемов, эту функцию можно будет отключить. В последнем случае оператору регистратуры придется периодически входить в систему и проверять наличие новых запросов.

Вопрос: Если оператор регистратуры обязан предоставить файл зоны перед подписанием Соглашения об администрировании домена верхнего уровня, то не лучше ли было бы использовать функцию «Одобрить» по умолчанию?

Ответ: На самом деле новый оператор регистратуры обязан предоставлять свои данные зоны *после* подписания Соглашения об администрировании домена верхнего уровня, при делегировании, а не *перед* подписанием Соглашения об администрировании домена верхнего уровня. Функция автоматического предварительного одобрения в настоящее время отсутствует.

Вопрос: Я не хочу каждый день регистрироваться в системе и одобрять запросы. Было бы хорошо просто все одобрять предварительно или автоматически.

Ответ: Операторы регистратур не обязаны каждый день регистрироваться в системе и одобрять запросы, однако они отвечают за проверку запросов конечных пользователей. Правило 24 часов означает, что операторы регистратур должны загружать свои данные зоны в систему каждые 24 часа – и этот процесс может быть автоматизирован.

Вопрос: Есть ли какие-либо примерные нормативы того, насколько быстро регистратуры должны отвечать на запросы? И собирается ли отдел соблюдения договорных обязательств ICANN это контролировать?

Ответ: Конкретные временные рамки выполнения запросов не установлены, однако предполагается, что регистратуры отреагируют на них в разумные сроки. Отдел соблюдения договорных обязательств ICANN будет следить за выполнением требования о предоставлении доступа к данным зоны.

Вопрос: Должен ли оператор регистратуры одобрять каждый запрос на получение данных зоны? Например, может ли .veryprivate, который на самом деле не согласен с концепцией предоставления таких данных по умолчанию, отклонять каждый запрос?

Ответ: Базовое Соглашение об администрировании домена общего пользования верхнего уровня требует от регистратур предоставления доступа к их файлам зоны. Существуют определенные условия, при которых они могут отклонять запросы. Условия, при которых оператор регистратуры может отклонить запрос на доступ к файлам зоны, см. в конкретном Соглашении об администрировании домена верхнего уровня.

Вопрос: Если конечный пользователь сделал несколько запросов на получение данных, и оператор регистратуры рассмотрел и одобрил по крайней мере один из таких запросов, то сможет ли в таком случае оператор регистратуры одобрять все другие запросы от этого пользователя пакетом?

Ответ: Оператор регистратуры обязан одобрять запрос, полученный от пользователей в отношении каждого TLD, отдельно. Каждое одобрение действует не менее 90 дней или дольше, если регистратура примет такое решение.

Вопрос: Существует ли какое-то наказание за *не*предоставление разрешения на доступ к данным зоны?

Ответ: Данную информацию см. в вашем Соглашении об администрировании домена верхнего уровня.

Вопрос: Если оператор регистратуры управляет несколькими TLD, то сколько учетных записей с отдельными комплектами учетных данных для входа потребуется для обработки запросов на доступ к данным зоны для всех его TLD?

Ответ: Учетная запись в CZDS должна представлять только одного пользователя, пока не будет указана другая политика. Одна отдельная учетная запись может управлять большим количеством TLD. CZDS имеет функцию, которая позволяет наделять пользователей и суперменеджеров оператора регистратуры правом заключать договор об условиях обслуживания от имени всех TLD, связанных с соответствующей регистратурой. Конкретные подробности, связанные с каждым «суперменеджером», зависят от деловых решений каждой регистратуры. Например, оператор регистратуры может поручить одному или нескольким пользователям оператора регистратуры управление доступом к данным зоны целого ряда TLD, находящихся в его ведении, в зависимости от их количества.

Вопрос: Можно ли использовать более одного контактного лица оператора регистратуры?

Ответ: Да, функция суперменеджера позволяет оператору регистратуры назначать/добавлять других пользователей оператора регистратуры, которые будут управлять их TLD. Суперменеджер должен подтвердить, что назначенные им операторы регистратуры наделены полномочиями заключать договор об условиях обслуживания от имени данной регистратуры.

Вопрос: Сможет ли один оператор регистратуры, представляющий портфель регистратур, войти в систему и просмотреть все, что там есть, за один раз, или же придется входить неоднократно?

Ответ: Как только устанавливается, что индивидуальный пользователь оператора регистратуры связан с регистратурой, он сможет просмотреть все запросы в отношении любого TLD, которым он управляет, с помощью одного входа в систему.

Вопрос: Если я назначу кого-то суперменеджером, каким образом я смогу проверить, что он сделал? Например, у меня есть 5 регистратур: я войду в систему и назначу своего администратора для выполнения этой роли для всех 5 регистратур, а он нажмет «одобрить все», а потом уволится из компании? Что тогда?

Ответ: Если назначенный пользователь оператора регистратуры уволится из компании, то суперменеджер может понизить его статус до конечного пользователя, лишив его статуса пользователя оператора регистратуры. Такое лицо уже не сможет одобрять запросы, но все, что оно одобрило ранее, будет действительно до тех пор, пока не истечет срок действия договора об условиях обслуживания. Если вы не хотите одобрять все запросы, то можете объявить недействительными один, несколько или все запросы, и тогда конечным пользователям придется входить в систему и повторно запрашивать доступ.

Вопрос: Планируется ли использование «песочницы» — как в SFTP-версии, так и в HTTP-версии?

Ответ: Использование «песочницы» не планируется. Регистратуры могут совместно с администратором CZDS наладить правильную работу в системе и протестировать передачу своего файла зоны. ICANN поможет убедиться, что все работает надлежащим образом, перед тем как оператор регистратуры начнет одобрять запросы конечных пользователей.

Вопрос: Станет ли договор об условиях обслуживания заменой договору о доступе к файлу корневой зоны?

Ответ: Да. По сути, текст договора об условиях обслуживания был взят непосредственно из действующих договоров о корневой зоне.

Вопрос: Должны ли мы как регистратуры создать свой собственный договор об условиях обслуживания, и, если да, то должны ли мы создать различные версии для каждого из наших TLD?

Ответ: В разделе 2.1.1 Спецификации 4 нового Соглашения об администрировании домена общего пользования верхнего уровня указано, что договор о доступе к файлу корневой зоны «будет стандартизироваться, упрощаться и администрироваться поставщиком услуг централизованного доступа к файлам корневой зоны».

Вопрос: Если регистратура обнаружит факт неправомерного использования со стороны пользователя, как нужно уведомлять об этом ICANN?

Ответ: Оператор регистратуры может отменить право на доступ для пользователя за нарушение соглашения о доступе между пользователем и оператором регистратуры. Любые вопросы или сообщения, касающиеся системы CZDS, следует направлять по адресу CZDS@icann.org.

Вопрос: Как CZDS использует шифрование с открытым ключом? Как работает первоначально загружаемый ключ? Данные представлены в формате ASCII и могут быть прочитаны — для чего расшифровывать эти данные? Почему бы не использовать, например, HTTPS?

Ответ: HTTPS защищает конфиденциальность информации, в данном случае, учетные данные доступа к серверам файлов корневой зоны на маршруте от сервера к клиенту, то есть между двумя сторонами. В то же время CZDS подразумевает наличие трех сторон: оператора регистратуры, пользователя файла зоны и оператора CZDS, который выступает в качестве посредника. При использовании HTTPS защищалась бы только информация, передаваемая от одной стороны другой, но не вся коммуникационная цепь, соединяющая две стороны через посредника. Используя шифрование с открытым ключом, мы можем обеспечить конфиденциальность передачи данных от оператора регистратуры пользователю файла корневой зоны. Оператор CZDS (посредник) не будет иметь доступа к учетным данным.

Веб-сайт CZDS генерирует пару 2048-битных ключей RSA (не PGP). На веб-сервере CZDS генерируются как открытый, так и закрытый ключи. Закрытый ключ направляется по сети через HTTPS, чтобы пользователь мог его загрузить, после чего этот ключ уничтожается и никогда не записывается на диск, в сеансе браузера или с помощью любого другого механизма хранения данных. Открытый ключ хранится вместе с другими данными профиля пользователя на веб-сайте CZDS. Эта пара ключей (закрытый ключ, который хранится у каждого пользователя, а также открытый ключ, который хранится в CZDS) необходима для расшифровки учетных данных SFTP. HTTPS не используется, чтобы защитить учетные данные от раскрытия третьей стороной.

CZDS генерирует пару ключей с закрытым и открытым ключами. «Открытый» ключ остается на сервере (так же, как на сервере остается открытый ключ SSH), и хотя мы не намерены делать этот ключ достоянием общественности, если бы он каким-то образом оказался известен посторонним, это событие с точки зрения безопасности относилось бы лишь к разряду некритических. Таким образом, мы действительно храним его в базе данных. Что касается «закрытого ключа», то после создания пары ключей он отправляется пользователю в ходе однократной операции (он передается вместе с веб-страницей, содержащей указания по загрузке ключа). Пользователь должен загрузить себе этот ключ и обеспечить его безопасность. Мы настоятельно рекомендуем пользователям следить за безопасностью ключа при просмотре страницы, содержащей этот ключ.

Если пользователь уйдет со страницы, содержащей закрытый ключ, предварительно его не загрузив, он тем самым потеряет возможность расшифровать учетные данные, и ему придется сгенерировать новую пару с закрытым и открытым ключами, что легко сделать в интерфейсе CZDS. В тех случаях, когда пользователь пытается сгенерировать новый ключ, а открытый ключ уже хранится в его учетной записи, интерфейс, перед тем как перезаписать существующий открытый ключ пользователя, выдает предупреждение (чтобы пользователь случайно не заменил действующий ключ).

Для расшифровки пользователь вводит свой «закрытый ключ» на веб-страницу, содержащую зашифрованные учетные данные, которые затем расшифровываются с помощью JavaScript, языка программирования клиентских приложений, используемого во всех веб-браузерах. В ходе этой операции закрытый ключ НЕ отправляется на сервер. Расшифровка происходит на компьютере каждого пользователя.

Существует ОТДЕЛЬНЫЙ токен (для доступа через API), который «совершенно не связан» с ключами шифрования/расшифровки. API-токен позволяет пользователю загружать массивы учетных данных SFTP и не принимает никакого участия в процессе расшифровки. API-токен является дополнительной функцией CZDS, и некоторые пользователи, возможно, даже не будут его создавать.

Вопрос: Если закрытый ключ RSA используется для расшифровки учетных данных SFTP, а API-ключ обеспечивает массовый доступ к этим учетным данным SFTP, то обходит ли система API RSA-шифрование учетных данных? Или их (учетные данные) нужно расшифровывать вне полосы?

Нет, API не обходит шифрование. Ни один из компонентов системы не может обойти расшифровку, потому что учетные данные никогда не хранятся в виде обычного текста, а закрытый ключ, который необходим для расшифровки, никогда не хранится на сервере.

Прочее

Вопрос: Если договор об условиях обслуживания изменится, то какой механизм будет использоваться для уведомления конечного пользователя? Будут ли какие-то последствия для конечного пользователя, если он не подтвердит изменения в условиях? Например, ему откажут в предоставлении данных?

Ответ: Каждый раз, когда договор об условиях обслуживания изменяется или обновляется, оператор регистратуры может принять решение об отмене доступа для всех своих текущих пользователей: в этом случае им придется войти в систему и повторно запросить доступ к файлу корневой зоны на новых условиях. Если этого не произойдет, то на конечного пользователя будут по-прежнему распространяться обязанности, прописанные в договоре об условиях обслуживания, с которыми он согласился в случае с каждым TLD в отдельности. Важно отметить, что отмена доступа в рамках системы CZDS не означает автоматической отмены доступа для конечного пользователя, который осуществляет доступ к данным зоны по SFTP. Вне рамок системы CZDS оператор регистратуры сам изменяет для пользователей учетные данные, которые были отменены или срок действия которых истек.

Вопрос: Какие элементы данных предоставляются в CZDS?

Ответ: Файлы зоны TLD содержат список доменных имен, которые зарегистрированы и активны в данной регистратуре. В файле зоны также содержатся записи DNS, которые регистратуры используют в зависимости от предлагаемых ими услуг регистратуры. Формат файла зоны описан в RFC 1035 и последующих RFC. Требуемый формат файлов корневой зоны, распространяемый CZDS, на самом деле является компонентом этих RFC; он был описан консультативной группой по вопросам доступа к файлу корневой зоны в ее Предложении по стратегии, в разделе 5.1.7 на странице 9 и включен в Спецификацию 4 Соглашения об администрировании домена верхнего уровня.

Вопрос: По каким IP-адресам осуществляется доступ? Вы получаете их через систему DNS? Как это отображается, как вы это делаете и каким путем это происходит?

Ответ: IP-адрес конечного пользователя предоставляется самим пользователем при создании профиля пользователя и передается оператору регистратуры.

Вопрос: Если пользователь загружает данные для регистратуры, то получает ли регистратура историю людей, которые их использовали?

Ответ: У оператора регистратуры есть история запросов каждого пользователя, но не история загрузок пользователя. Теоретически в системе CZDS возможно регистрировать прямые загрузки, но в настоящее время такая функция в системе отсутствует.

Вопрос: Одобрение дается на запрос на загрузку или на доступ к TLD?

Ответ: На TLD. Доступ для получения данных зоны TLD предоставляется один раз и на все время действия договора об условиях обслуживания — не менее чем на 90 дней или на срок, устанавливаемый по усмотрению регистратуры. После окончания срока действия договора об условиях обслуживания пользователь должен снова запросить доступ.

Вопрос: Нам нужны эксперты в предметной области для полной автоматизации, чтобы система заработала в полную силу. А как насчет игр — насколько часто можно загружать файлы зоны? Было бы хорошо получать доступ нажатием одной кнопки.

Ответ: В договоре об условиях обслуживания существует требование, согласно которому ограничивается количество обращений конечного пользователя к файлам зоны: он может сделать это один раз в течение суток. Файлы загружаются в систему один раз в сутки, поэтому, если бы конечный пользователь загружал их на свой компьютер чаще, чем раз в сутки, то никакой новой информации он бы не получил. Кроме того, пользователю не разрешается осуществлять прямую загрузку в CZDS чаще трех раз для каждого TLD в течение суток. Если он попытается это сделать, то получит сообщение об ошибке.