БИБЛИОТЕКА РАЗРАБОТЧИКА

Е. Ю. Хрусталева

ОБЛАЧНЫЕ ТЕХНОЛОГИИ «1С:ПРЕДПРИЯТИЯ»



1С ПАБЛИШИНГ

Хрусталева Е.Ю.

Облачные технологии "1С:Предприятия"

Электронная книга в формате pdf; ISBN 978-5-9677-2610-1.

Электронный аналог издания "Облачные технологии "1С:Предприятия 8"" (ISBN 978-5-9677-2608-8, М.: ООО "1С-Паблишинг", 2016; артикул печатной книги по прайс-листу фирмы "1С": 4601546128010; по вопросам приобретения печатных изданий издательства "1С-Паблишинг" обращайтесь к партнеру "1С", обслуживающему вашу организацию, или к другим партнерам фирмы "1С").

Книга адресована разработчикам прикладных решений, которые хотят познакомиться с технологиями, обеспечивающими работу системы «1С:Предприятие 8» через Интернет. Кроме этого в книге рассматривается новая технология, 1cFresh, которая позволяет организовать работу с прикладными решениями «1С:Предприятия 8» в модели сервиса. На нескольких примерах показываются разные варианты использования сервиса: для внутренних целей холдинга или для использования опубликованных приложений внешними клиентами.
Основная цель книги – познакомить с новыми облачными технологиями системы «1С:Предприятие 8». Поэтому в ней нет подробных инструкций, выполняя которые, читатель может достигнуть описанного результата. Однако она содержит замечания и советы по установке и настройке сервиса, а также по адаптации типовых или собственных прикладных решений к работе в модели сервиса. В сочетании с документацией эти советы помогут читателям выполнить примеры, описываемые в книге.
Книга выпущена под редакцией Максима Радченко.

Оглавление

Глава 1. Облачные технологии «1С:Предприятия» 5
Подключение к информационной базе по протоколу HTTP 6
Механизм разделения данных 8
OpenID-аутентификация 12
Общая информация 12
Настройка OpenID-аутентификации 14
Защищенное соединение, сертификаты безопасности 15
Глава 2. Технология 1cFresh 17
Варианты использования сервиса 1cFresh 18
Компоненты сервиса 21
Особенности использования облачных технологий в сервисе 23
Multitenancy 23
Разделение данных 24
OpenID-аутентификация пользователей 25
Защищенные соединения, сертификаты безопасности 25
Возможности сервиса 1cFresh 26
Возможности для поставщика 26
Возможности для пользователя 27
Преимущества применения технологии 1cFresh 28
Преимущества для поставщика 28
Преимущества для пользователя 28
Механизмы сервиса 29

Глава 3. Установка и настройка сервиса 1cFresh 41
Пример развертывания сервиса 1cFresh 41
Особенности развертывания сервиса 1cFresh 43
Перенос файлов на сервер для настройки 1cFresh 43
Установка и настройка СУБД PostgreSQL 44
Включение и настройка IIS 46
Публикация приложений на веб-сервере 48
Регистрация информационных баз в менеджере сервиса 50
Ссылки для скачивания утилит для установки сертификатов и WinSW 50
Особенности запуска и написания команд в командной оболочке Windows PowerShell 51
Установка и запуск NGINX 51
Установка сертификата безопасности 53
Использование приложений с общим внешним адресом 53
Настройка Apache Tomcat 54
Установка сайта 55
Настройка форума 57
Создание нового пользователя сервера 57
Общие рекомендации при проверке работы шлюза, сайта, форума 58
Глава 4. Примеры использования сервиса 1cFresh 59
Общий подход к разработке конфигураций для работы в сервисе 59
Пример 1. Доработка типовой конфигурации для работы в сервисе 60
Работа в веб-клиенте 61
Длительная операция, работающая на сервере 64
Регламентное задание 71
Поставляемые данные 78
Пример 2. Доработка нетиповой конфигурации для работы в сервисе 92
Внедрение БСП и БТС 93
Доработка командного ролевого интерфейса, начальной страницы и основного раздела 179
Проверка внедрения БСП и БТС 185
Проверка функционирования конфигурации в локальном режиме 193
Размещение конфигурации и создание приложений в сервисе 201
Проверка функционирования приложения в сервисе 202
Пример 3. Приложение сервиса в качестве бэк-энда мобильных приложений 214
Заключение 217

Глава 1. Облачные технологии «1С:Предприятия»

Развитие и повсеместное применение Интернета в современном мире, а также совершенствование техники и оборудования привели к широкому распространению облачных технологий при использовании программного обеспечения. Применение этих технологий позволяет постоянно «держать руку на пульсе своего бизнеса» и работать on-line с данными своей организации из любого места земного шара, где есть Интернет.

Кроме того, пользователям, работающим в облачной модели, не нужно заботиться об администрировании своих приложений, резервном копировании, своевременном обновлении. Достаточно просто включить компьютер, и пользоваться приложениями, как пользуются электричеством, вставляя вилку в розетку.

Такие возможности работы обеспечиваются целым набором технологий, которые реализованы в платформе «1С:Предприятие 8». Все эти технологии можно объединить одним словом «облачные». Термин «облако» используется здесь как метафора. Она основана на том, что Интернет изображается на компьютерных диаграммах в виде облака, за которым от клиента скрывается сложная инфраструктура со всеми техническими деталями. Рассмотрим более подробно эти технологии.

Подключение к информационной базе по протоколу HTTP

В платформе «1С:Предприятие» реализованы клиентские приложения: тонкий клиент и веб-клиент, с помощью которых пользователи могут удаленно работать с прикладными решениями через Интернет.

Тонкий клиент – это «облегченный» вариант клиентского приложения «1С:Предприятия», который работает только в режиме 1С:Предприятие и не поддерживает режим разработки в конфигураторе. За счет своей легкости он может работать через Интернет, но требует предварительной установки небольшого по объему дистрибутива системы на компьютер пользователя.

Веб-клиент – это клиентское приложение «1С:Предприятия», работающее в среде интернет-браузера, в том числе и на мобильных устройствах, и не требующее предварительной установки системы на компьютер пользователя. Но веб-клиент не поддерживает некоторые возможности платформы, в отличие от тонкого клиента.

Прикладные решения не требуют какой-либо доработки для того, чтобы работать с ними через Интернет. И тонкий, и веб-клиент самостоятельно обеспечивают функционирование интерфейса «1С:Предприятия» на компьютере пользователя.

Они подключаются к специальным образом настроенному веб-серверу, который осуществляет их взаимодействие с кластером серверов «1С:Предприятия» (рис. 1.1).

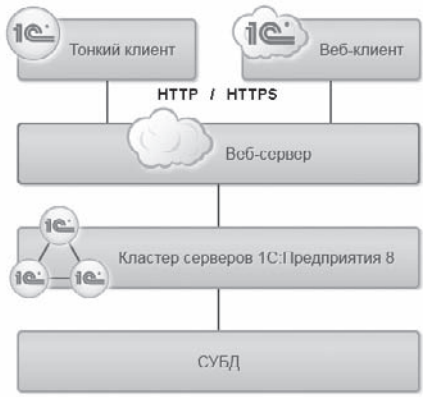


Рисунок 1.1. Подключение через Интернет в клиент-серверном варианте работы

Подключение клиентских приложений может выполняться как по протоколу HTTP (протокол прикладного уровня передачи данных), так и по протоколу HTTPS, поддерживающему шифрование передаваемых данных.

Для подключения к информационной базе по протоколу HTTP необходимо сначала в конфигураторе выполнить публикацию информационной базы на веб-сервере с помощью диалога публикации по команде Администрирование – Публикация на веб-сервере.

Для запуска веб-клиента необходимо использовать адрес, который формируется по следующим правилам: <Имя хоста веб-сервера>/<Имя виртуального каталога>. Например, если имя виртуального каталога, в котором опубликован веб-клиент, – Taxi, то для запуска веб-клиента в интернет-браузере или в «Проводнике» следует набрать следующий URL (для получения доступа с локальной машины): http://localhost/Taxi.

В результате прямо в браузере будет запущено «1С:Предприятие» в режиме веб-клиента (рис. 1.2).

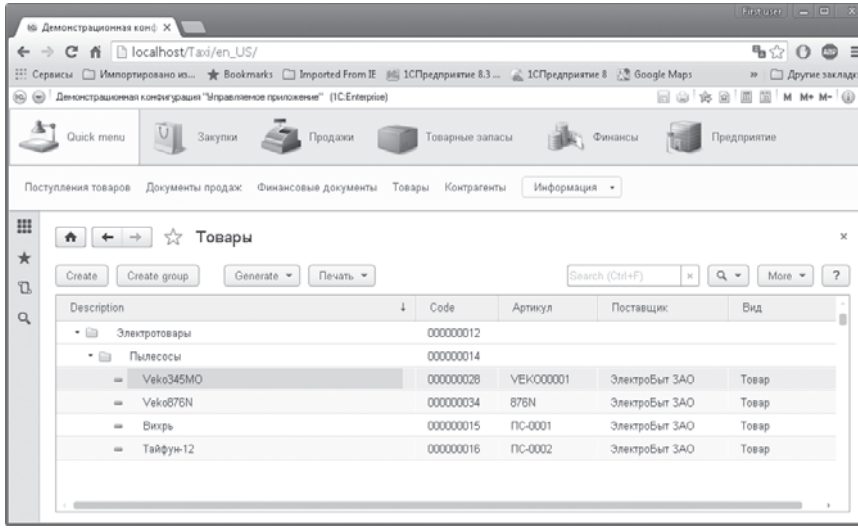


Рисунок 1.2. «1С:Предприятие», запущенное в режиме веб-клиента

Чтобы подключиться к информационной базе, опубликованной на веб-сервере, с помощью тонкого клиента, нужно в диалоге создания или редактирования информационной базы, в стартовом окне «1С:Предприятия», выбрать вид расположения информационной базы На веб-сервере. И затем

в строке адреса информационной базы указать http://localhost/Taxi, то есть такой же адрес, что и при подключении с помощью веб-клиента.

Веб-клиент, в отличие от толстого и тонкого клиентов, исполняется не в среде операционной системы компьютера, а в среде интернет-браузера (Microsoft Edge, Windows Internet Explorer, Mozilla Firefox, Google Chrome или Safari). Поэтому любому пользователю достаточно всего лишь запустить свой браузер, ввести адрес веб-сервера, на котором опубликована информационная база, и веб-клиент начнет свою работу.

Для работы веб-клиента важно, чтобы браузер имел некоторые настройки, поэтому при первом запуске веб-клиента выполняются некоторые автоматические проверки, и, если браузер не настроен нужным образом, выводится инструкция по настройке или даже диалог настройки браузера (для Mozilla Firefox).

В целом работа с «1С:Предприятием» в режиме веб-клиента аналогична работе в режиме тонкого клиента, но имеет некоторые особенности и ограничения при работе с табличными документами, графическими схемами, диаграммами, географическими схемами и т. п. Все эти особенности подробно описаны в документации.

Особо следует отметить ряд ограничений, которые накладывает веб-клиент на работу с файловой системой. Политика безопасности веб-браузеров такова, что приложения, работающие в их среде, не имеют прямого доступа к файловой системе компьютера. Поэтому все операции с файловой системой (получение файла с сервера, передача файла на сервер, удаление файла и т. п.) требуют явного подтверждения пользователя и выполняются строго интерактивно.

Для обеспечения полнофункциональной работы с файловой системой в браузерах нужно установить расширение для работы с файлами. Расширения для работы веб-клиента с файлами, криптографией можно установить в самом приложении, запущенном в режиме веб-клиента, если установка этих расширений предусмотрена в прикладном решении.

Механизм разделения данных

Одним из важнейших механизмов облачных технологий является механизм разделения данных.

Механизм разделения данных позволяет хранить данные нескольких независимых организаций в одной информационной базе. В режиме разделения данных все эти организации используют один и тот же экземпляр прикладного решения (одну и ту же информационную базу) для работы со своими данными.

То есть в обычном режиме (без использования разделения данных) каждая организация запускает свой отдельный экземпляр программы и видит в ней только свои данные, потому что других данных изначально там нет. А в режиме разделения данных все организации запускают один и тот же экземпляр программы, но видят в ней только свои данные. При этом у них создается ощущение, что с программой работают только они, потому что они видят только ту часть данных, которая относится к их области.

Для этого используются *общие реквизиты* конфигурации, которые позволяют автоматически добавлять многим объектам конфигурации одинаковый реквизит с одним и тем же именем и одинаковым типом.

Если у общего реквизита свойство Разделение данных установлено в значение Разделять, то он становится *разделителем*, то есть позволяет идентифицировать независимые области данных, создаваемые внутри информационной базы.

Например, в конфигурации существует общий реквизит Организация. Это значит, что у каждого справочника, документа или другого объекта конфигурации также будет существовать реквизит Организация.

В случае если общий реквизит Организация является разделителем данных, то в информационной базе будет создано несколько независимых областей данных, в каждой из которых будут храниться данные только для одной конкретной организации (рис. 1.3).

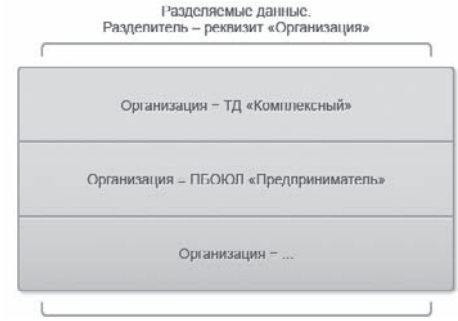


Рисунок 1.3. Деление информационной базы на независимые области

Таким образом, заходя в программу, пользователь получает доступ не ко всей информации, которая есть в информационной базе, а только к данным «своей» области, в данном случае к документам, справочникам и др. своей организации (рис. 1.4).



Рисунок 1.4. Доступ пользователей к независимым областям

Возможен и другой вариант использования механизма разделения данных, когда в информационной базе существует несколько независимых областей данных и наряду с этим существуют данные, которые доступны всем пользователям программы. Например, они содержат справочник банков, который одинаков для всех организаций (рис. 1.5).

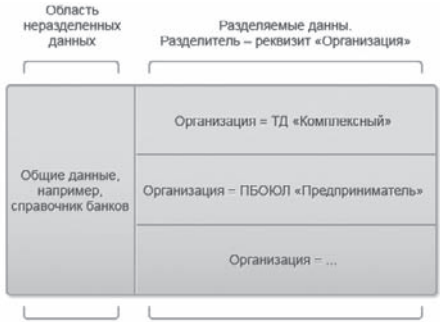


Рисунок 1.5. Общие и независимые области данных

В этом случае пользователь имеет доступ к «своей» области данных и к области неразделенных данных, которая является общей для всех пользователей (рис. 1.6).

На уровне платформы, если разделитель используется, то в текущем сеансе видны только те записи, в которых значение разделителя совпадает с текущим значением параметра сеанса, на который ссылается разделитель. Это достигается за счет того, что платформа добавляет отбор во все запросы к базе данных на чтение, обновление, удаление по текущим значениям используемых разделителей. При добавлении и записи данных тех объектов конфигурации, которые входят в состав разделителя, также устанавливаются текущие значения этого разделителя.

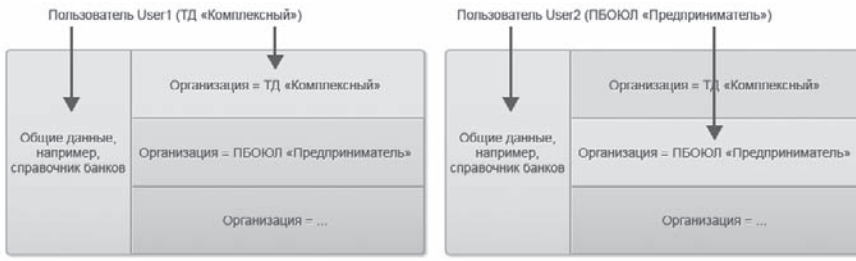


Рисунок 1.6. Доступ пользователей к общим и независимым областям данных

Механизм разделения данных имеет следующие особенности:

- Может использоваться не один, а несколько разделителей.
- Могут применяться разные режимы использования разделяемых данных: *независимо/независимо и совместно*. При независимом разделении данных разделенные данные из одной области данных недоступны для другой области данных. Этот режим может использоваться в тех случаях, когда прикладное решение в своей работе использует только данные одной области данных. При независимом и совместном разделении данных из неразделенного сеанса доступны все данные, разделенные независимо и совместно. Такой режим может использоваться в большинстве случаев, когда прикладное решение работает только с данными одной области данных (например, при вводе документов), а в некоторых режимах могут использоваться данные нескольких или всех областей (например, для получения консолидированной отчетности).
- Может применяться так называемое *условное разделение*, когда прикладное решение предполагается использовать как в разделенном, так и в неразделенном вариантах. Например, прикладное решение может использоваться для автономной работы – в этом случае разделители не используются, но в самом решении они предусмотрены, а может использоваться для работы некоторого количества абонентов, никак не связанных друг с другом.
- Может использоваться *разделение пользователей*, при котором определяется, какая часть списка пользователей будет доступна, в зависимости от того, используется данный разделитель или нет. Разделение пользователей используется при программном доступе к списку пользователей, а также в конфигураторе при редактировании списка пользователей.

- Может использоваться *разделение аутентификации*, при котором возможно создание одноименных пользователей для разных областей данных. Например, можно создать несколько пользователей Администратор, которые будут различаться только значениями разделителей.

Публикацию базы на веб-сервере (файл default.vrd) можно настроить так, что значение разделителя можно будет указывать прямо в строке подключения, например http://localhost/Taxi/1. Здесь 1 – это значение разделителя.

OpenID-аутентификация

Общая информация

Еще одним важным и полезным механизмом облачных технологий является OpenID-аутентификация.

OpenID-аутентификация – это один из видов аутентификации (проверки подлинности), поддерживаемых механизмом аутентификации «1С:Предприятия».

В этом случае аутентификацию пользователя выполняет не конкретная информационная база, к которой пытается подключиться пользователь, а внешний *OpenID-провайдер*. Это информационная база «1С:Предприятия», специальным образом опубликованная на веб-сервере, которая выполняет процедуру аутентификации пользователей и хранит список пользователей для проверки.

В качестве OpenID-идентификатора используются имена пользователей информационной базы, которая обращается к OpenID-провайдеру. Имя пользователя должно совпадать с именем пользователя информационной базы OpenID-провайдера.

Если используется аутентификация «1С:Предприятия», то каждый раз при подключении к информационной базе пользователь должен вводить логин и пароль.

Если же используется OpenID-аутентификация, то, однажды выполнив процедуру аутентификации при подключении к одной из баз, во все остальные базы пользователь будет заходить без запроса логина и пароля. OpenID-провайдер будет автоматически аутентифицировать пользователя на основе имеющейся у него информации.

Последовательность действий, выполняемых при подключении пользователя, представлена на следующей схеме (рис. 1.7).

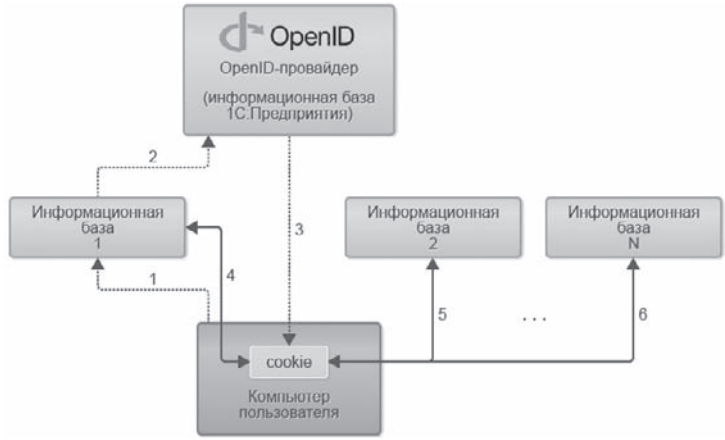


Рисунок 1.7. OpenID-аутентификация

На схеме цифрами показана последовательность действий при подключении пользователя с помощью OpenID-аутентификации:

- 1 – клиентское приложение обращается к информационной базе 1.
- 2 – информационная база 1 обращается к OpenID-провайдеру, с тем чтобы он аутентифицировал пользователя.
- 3 – OpenID-провайдер выполняет процедуру аутентификации: пользователь вводит логин и пароль; в случае успешной аутентификации на компьютере пользователя в cookie сохраняется признак того, что провайдер аутентифицировал пользователя.
- 4 – используя признак аутентификации, сохраненный в cookie, пользователь подключается к информационной базе 1 и начинает работу.
- 5, 6 – при обращении к другой информационной базе пользователю не нужно снова вводить логин и пароль; на основании признака аутентификации, сохраненного ранее в cookie, OpenID-провайдер выполняет аутентификацию незаметно для пользователя.

Тем самым повышается комфортность и скорость работы пользователей с прикладными решениями «1С:Предприятия».

OpenID-аутентификация работает только в тех случаях, когда доступ к информационной базе осуществляется по протоколу http и https. Это означает, что использовать OpenID-аутентификацию могут только веб-клиент и тонкий клиент, подключенный к информационной базе через веб-сервер. Взаимодействие с OpenID-провайдером осуществляется только по HTTPS-соединению.

Настройка OpenID-аутентификации

Для того чтобы система выполняла аутентификацию с помощью протокола OpenID, необходимо, чтобы у пользователя в информационной базе, которая использует OpenID-аутентификацию, был установлен флажок Аутентификация OpenID и соответствующим образом была настроена публикация данной информационной базы на веб-сервере (файл default.vrd).

В файле публикации информационной базы default.vrd, в описании элемента <openid>, можно указать адрес информационной базы, которая используется в качестве OpenID-провайдера для публикуемой информационной базы, или же указать, что сама эта база является OpenID-провайдером для других информационных баз.

В первом случае файл публикации default.vrd должен содержать, например, следующий фрагмент (листинг 1.1).

Листинг 1.1. Указание адреса базы, являющейся OpenID-провайдером

```
<openid>
        <rely url="https://myserver.org/users-ib/e1cib/oid2op"/>
</openid>
```

Атрибут <url> элемента <rely> содержит адрес информационной базы, которая является OpenID-провайдером для опубликованной информационной базы.

Можно вручную отредактировать файл публикации, а можно внести указанные изменения через диалог публикации на веб-сервере, включив там флажок Использовать OpenID-аутентификацию и указав Адрес OpenID-провайдера.

Во втором случае файл публикации default.vrd должен содержать, например, следующий фрагмент (листинг 1.2).

Листинг 1.2. Эта база сама является OpenID-провайдером

```
<openid>
        <provider/>
</openid>
```

Элемент <provider> указывает, что опубликованная таким образом информационная база выступает в роли OpenID-провайдера.

При этом можно задать время жизни признака аутентифицированности. Это позволяет заново запрашивать аутентификацию в тех случаях, когда подключение к информационным базам происходит с большими промежутками времени.

За это отвечает подчиненный элемент <lifetime>, в котором задается время действия признака аутентифицированности. Если этот элемент не указан, то значением по умолчанию является 86 400 секунд (24 часа).

Можно внести указанные изменения как вручную, так и через диалог публикации на веб-сервере, включив там флажок Использовать в качестве OpenID-провайдера (Время жизни аутентификации).

Защищенное соединение, сертификаты безопасности

Подключение клиентских приложений к информационным базам может выполняться как по протоколу HTTP, так и по протоколу HTTPS, поддерживающему шифрование передаваемых данных.

HTTPS (Hypertext Transfer Protocol Secure) – расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL, тем самым обеспечивается защита этих данных.

Для того чтобы использовать HTTPS-соединение, нужно получить цифровой сертификат для доменного имени из доверенных центров сертификации. Можно использовать также «самоподписанный» сертификат, сгенерированный и подписанный самим владельцем доменного имени. Но в этом случае все пользователи этого доменного имени должны будут настроить используемые ими веб-браузеры, чтобы они доверяли этому сертификату.