

# 1 Установка сервера УРМ

## 1.1 Технические требования

Сервер УРМ рекомендуется устанавливать на отдельном компьютере. Для работы Сервера УРМ необходима следующая конфигурация аппаратных средств:

- 1-4 CPU x 2-4 Core 2-3GHz
- RAM 2-12Gb
- HDD 120Gb
- Lan 1Gbps
- USB, UPS
- ОС: Windows Server 2012, Windows Server 2008, Windows Server 2003 R2
- Internet explorer 7.0 и выше.

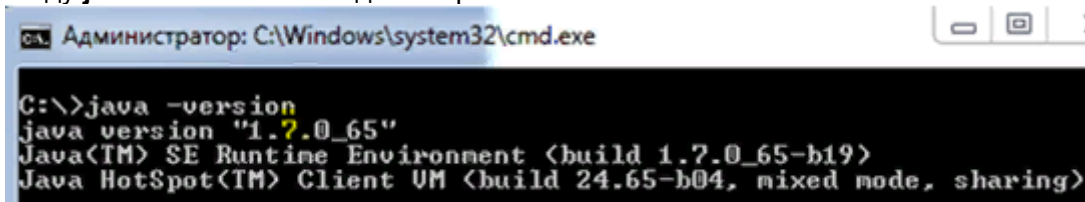
## 1.2 Нагрузочная способность сервера обмена данными

Рекомендуется планировать нагрузку на один сервер из расчета не более 120-400 удаленных клиентов. При необходимости работы более 400 клиентов рекомендуется использовать дополнительные сервера УРМ. В случае повышенной нагрузки количество серверов УРМ, необходимых для комфортной работы, может оказаться больше.

## 1.3 Подготовка к установке сервера УРМ

Установка и настройка сервера УРМ осуществляется под пользователем ОС с правами администратора.

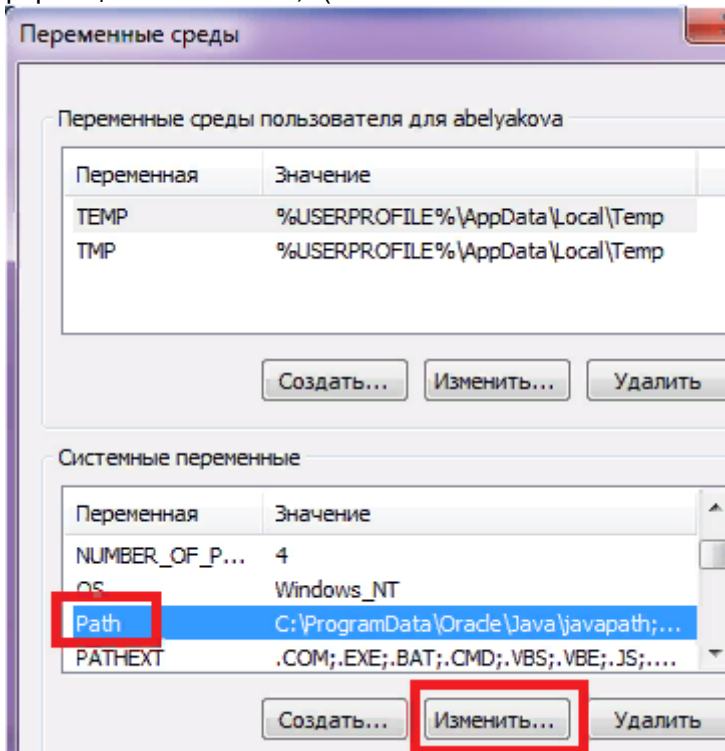
1) Для работы сервера УРМ необходимо установить Java-машину 7 версии, 32-х разрядную (вне зависимости от разрядности ОС). Дистрибутив Java-машины можно скачать с сайта <http://www.oracle.com>. Проверить версию Java, установленную на машине, можно набрав команду `java -version` командной строке.



```
Администратор: C:\Windows\system32\cmd.exe
C:\>java -version
java version "1.7.0_65"
Java(TM) SE Runtime Environment (build 1.7.0_65-b19)
Java HotSpot(TM) Client VM (build 24.65-b04, mixed mode, sharing)
```

После установки Java-машины проверьте, что путь до папки *Bin* каталога установки Java прописан в системной переменной *Path* (Свойства системы - Дополнительно - Переменные среды). Если этого не произошло автоматически, необходимо добавить этот путь вручную, отделив от имеющейся

информации символом ";" ("точка с запятой" - без кавычек).



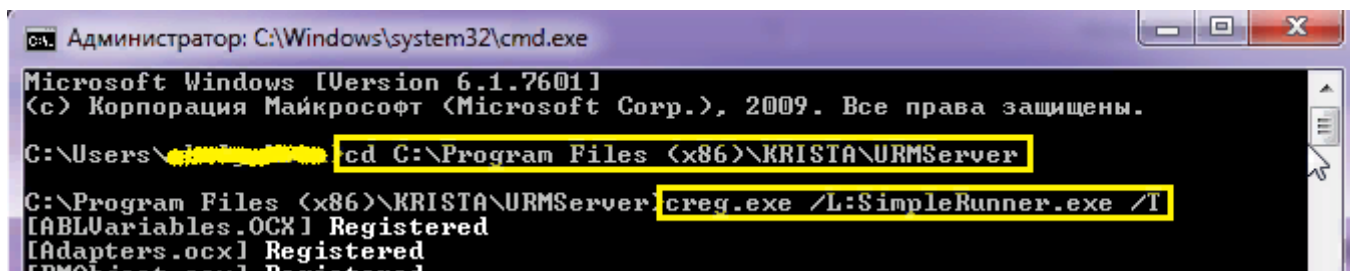
2) Если на компьютере ранее был установлен сервер UPM, необходимо его деинсталлировать.

3) Установить на машине СУБД (*FireBird* или *Oracle*), версия которой должна совпадать с версией СУБД на сервере базы данных АС «Бюджет».

## 1.4 Установка сервера UPM и создание файлов манифестов

Установка сервера UPM осуществляется путем запуска инсталляционной программы *UrmServer\_SETUP.exe*. По-умолчанию программа будет установлена в каталог *C:\Program Files\KRISTA\URMServer*. В процессе установки будут зарегистрированы модули сервера. При необходимости, регистрацию можно повторить, запустив утилиту *creg.exe* из папки *URMServer*. Если на машине с Севером UPM есть необходимость запускать АС UPM либо АС Бюджет, то для разграничения модулей используемых сервером и клиентом необходимо сгенерировать манифесты для файлов *SimpleRunner.exe* и *AdminUtil.exe*. Для создания манифестов надо выполнить команды:

```
creg.exe /L:SimpleRunner.exe /T
creg.exe /L:AdminUtil.exe /T
```



В результате выполнения команд в каталоге *URMServer* будут созданы файлы *SimpleRunner.exe.manifest* и *AdminUtil.exe.manifest*.

## 2 Настройка сервера обмена данными

### 2.1 Настройка конфигурации сервера UPM с помощью утилиты QConfig.exe

Запустите утилиту конфигурирования *QSConfig.exe*.

Укажите *Максимальное количество одновременных подключений* (рекомендуемое 15-20).

*Уровень детализации логов* оставить нормальным. Менять этот параметр следует только по рекомендации разработчиков.

Определите, как будет установлен сервер - службой или приложением - поставьте либо снимите галочку *Установить как сервис с автозагрузкой*.

Если сервер установлен приложением, запуск и остановка происходят путем запуска или выгрузки утилиты *QSAgent.exe*.

Если сервер установлен службой, то запуск службы **QueryServerJ** происходит автоматически, при включении компьютера. Службу можно принудительно останавливать или запускать через «Панель управления» компьютера или через меню утилиты *QSAgent.exe*, что предпочтительнее.

## 2.2 Настройка конфигурации сервера УРМ с помощью утилиты настроек администратора AdminUtil

### 1) Настройка полей секции **Автообновление**

- Требуемая версия УРМ – установить текущий номер версии клиентской части АС «УРМ».
- Каталог с обновлениями – задать путь к папке, в которую будут выкладываться файлы автообновлений.
- Запись версии клиента – при установленном флаге при каждом соединении клиента с сервером в базе АС Бюджет в списке удаленных клиентов будет сохраняться текущая версия удаленного клиента. Просмотреть версию можно в интерфейсе *Права удаленных клиентов*, поле "Версия клиента".
- Наличие обновления для предварительной заочки – данная опция включает функцию предварительной заочки автообновлений, которая используется при необходимости заочать на клиента большие по объему централизованные обновления АС «УРМ» при наличии линий со слабыми техническими характеристиками. Параметры устанавливаются следующим образом:
- Требуемый процент предварительной заочки - 0
- Ежедневный прирост процента предварительной заочки – указывается процент от общего объема обновления, который должен быть закачан на клиента УРМ за один день.
- Быстрое скачивание обновления – параметр используется для хранения обновления в оперативной памяти для уменьшения числа операций чтения с жесткого диска машины с сервером обмена данными.

**2)** В секции **Настройка соединения** можно указать Допустимое отклонение времени клиента от времени на сервере (в минутах). При установленном значении, если при отправке документов будет установлено, что время на сервере УРМ отличается от времени на клиентской машине более чем на указанное значение, то отправка документов будет заблокирована. Если параметр не задан или равен нулю, то проверка не производится

**3)** В секции **Подключение к базе Бюджета** в форме *"Редактирование списка доступных баз"* (открывается по кнопке с тремя точками) необходимо задать список баз данных АС «Бюджет», к которым смогут подключаться пользователи АС «УРМ»:

- "Идентификатор" – целочисленное значение, стандартно - это финансовый год.

Для основной базы АС Бюджет и для криптографической базы (если в работе применяется электронная подпись) необходимо сделать аналогичные настройки:

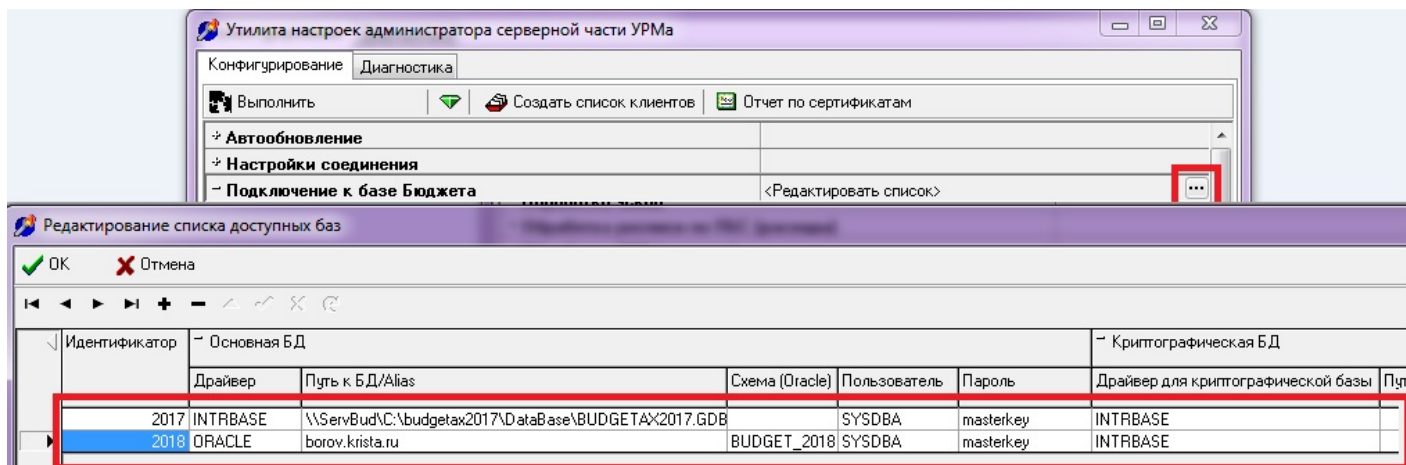
- выбрать "Драйвер" (СУБД, под которой работает база):

Для баз, работающих под управлением *FireBird*, указывается драйвер Interbase и путь к базе, в формате: <СерверБД>:<Физический путь к базе на сервере>.

Для баз, работающих под управлением *Oracle*, указывается драйвер Oracle, в поле "Alias" – имя сервера базы данных, в поле "Схема" – название схемы.

- заполнить поля "Пользователь" и "Пароль" - по-умолчанию пользователь SYSDBA,

пароль masterkey.



- **Отладочный режим** - при установленном значении в логи сервера будет выводиться более детальная информация о подключении к базе АС «Бюджет». Данную опцию необходимо использовать в случае проблем при подключении, по согласованию с отделом сопровождения.
- **Проверять пароль пользователя по базе Бюджета** – при установленном флаге пароль клиента АС «УРМ» будет проверяться сначала по базе пользователей сервера УРМ, а затем по базе АС «Бюджет». Если флаг не установлен, то проверка производится только по базе пользователей сервера УРМ.

4) Далее идут секции (**Обработка платежных поручений, Обработка чеков, Обработка росписи по ПБС (расходы)** и т.д.), в которых можно указать требуемые настройки для обработки поступающих в финансовый орган электронных документов, отдельно для каждого интерфейса. Рассмотрим возможные настройки на примере секции **Обработка платежных поручений**:

- **Отладочная информация** – опция включается только по рекомендации технической поддержки. В логи будет выводиться более подробная информация об обработке документа, необходимая разработчикам для устранения возникающих проблем.
- В следующих полях (**Вид учета старый** (код бух операции), **Тип документа плательщика** (Документы), **Тип документа получателя**, **Вид операции** (код операции) и т.д.) указывается значение соответствующего классификатора, которое будет автоматически присвоено электронному документу при его отсылке из АС «УРМ» в АС «Бюджет». Значение в *AdminUtil* вводится в ручную и должно обязательно присутствовать в соответствующем справочнике АС «Бюджет». Если в автоматическом заполнении параметра нет необходимости, поле должно остаться пустым, в этом случае документ придет в АС «Бюджет» с тем значением, которое было выбрано в АС «УРМ».

Аналогичные настройки можно выполнить для других интерфейсов.

#### 5) Секция Настройки синхронизации

- При установленной опции **Отладочная информация сервер УРМ** будет выводиться в журнал событий более подробную информацию в процессе проведения синхронизации, размер логов будет значительно увеличен. Опция устанавливается только по рекомендации сотрудников сопровождения.
- При установленном параметре **Запись даты последней синхронизации** происходит фиксация даты и времени последней синхронизации клиента УРМ. Данную информацию можно увидеть в АС «Бюджет» интерфейсе **Права удаленных клиентов**, индивидуально для каждого удаленного клиента.
- Секция **Синхронизация реестра** используется только разработчиками.

6) Параметры секции **Криптография** заполняются при использовании средств криптографической защиты информации, передаваемой между клиентом и сервером УРМ.

При использовании **электронной подписи** необходимо, чтобы **Сервер УРМ** был запущен как **приложение**. На машине с **Сервером УРМ** должны быть установлены **корневой сертификат** и **список отзыва** удостоверяющего центра.

- **Криптопровайдеры** - определяет используемую систему криптографии
- **Предупреждение о завершении срока действия сертификата** – установка параметра включает механизм предупреждения клиентов УРМ об окончании срока действия их сертификатов. Если до

истечения срока действия одного из сертификатов, используемых удаленным клиентом для наложения электронной подписи на документы, осталось меньше указанного в данной константе числа дней, то при входе в АС «UPM» пользователю будет выводиться соответствующее сообщение. Нулевое значение константы отключает проверку и предупреждение.

- Правила проверки OID Определяет правила проверки OID (Объектный идентификатор области использования ключа). Список OID задается в фигурных скобках, через запятую (OID в списке указываются в одинарных кавычках, через запятую). Каждый список может содержать несколько требующихся OID и несколько, которых не должно быть (знак ~ перед OID указывает на то, что данного OID не должно быть в списке OID в сертификате). Списку можно задать имя (английские буквы, цифры, первый символ – буква).

Пример:

Правила проверки OID	PBS{~"1.2.3.4.5.6.7";'2.3.4.5.6.7.8'};GRBS{'1.1.4.5.6.7.8'}
----------------------	---

В следующих параметрах необходимо выполнить настройку параметров проверки *сроков действия списков отзыва* удостоверяющего центра:

- Режим проверки действия CRL – параметр может принимать следующие значения:
  - Использовать срок годности текущего CRL - срок действия CRL, выданный удостоверяющим центром
  - Задать время действия вручную - задается срок действия текущего CRL, ко времени его издания (начала срока действия) добавляется "время действия CRL" и сравнивается с текущей датой, т.е. CRL будет считаться действительным в течении "время действия CRL" начиная от момента издания CRL. После истечения заданного времени CRL будет просрочен.
  - Использовать срок годности текущего CRL, и заданный срок действия - режим предназначен для использования в экстренном режиме, когда нужно продлить срок действия текущего CRL. Т.е. если CRL будет просрочен, а заданное время еще не истекло, то CRL будет действовать до окончания заданного времени.
- Время действия CRL (в часах). Указывается время действия CRL в часах (целое, положительное число).
- При отсутствии актуального CRL – параметр может принимать следующие значения:
  - Генерировать ошибку - проверяет CRL выданный удостоверяющим центром
  - Запросить разрешение на продолжение работы у пользователя - проверяет список отзыва выданный удостоверяющим центром. Если список отзыва просрочен, то будет выходить предупреждение и диалог о действиях пользователя.
  - Игнорировать, и продолжить работу (ОПАСНЫЙ РЕЖИМ!) - не проверяется CRL
  - Игнорировать, и продолжить работу, вывесив оповещение - проверяет CRL выданный удостоверяющим центром. Если список отзыва просрочен, то будет выходить предупреждение.

Настройки в следующих секциях осуществляются при использовании средств соответствующей криптозащиты.

#### • Шифрование

- Криптопровайдер определяет используемую систему криптографии.
- Имя ключевого контейнера указывается имя ключевого контейнера, содержащего закрытый ключ сервера UPM, который используется для шифрования данных при обмене между клиентом и сервером.

#### • Сервер штампов времени

*Штамп времени* – это механизм, который используется для подтверждения времени подписания. Основой механизма штампов времени является сервер штампов времени или TSA (Time Stamp Authority). Это отдельная структура, которая занимается выдачей штампов и подтверждает их наличие и целостность в случае юридических разбирательств.

- Сервер штампов времени (URL) - указывается URL страницы, с которой ассоциирован сервер штампов времени. Например: <http://ca.krista.ru/tsp/tsp.srf> (тестовый сервер). Если данное поле не заполнено, то штампы времени считаются отключенными.

- Порт сервера штампов времени - обычно остается 80, если TSA не выдало другого порта.

- Прокси-сервер - эта настройка используется только в том случае, если доступ к серверу штампов времени происходит с использованием прокси-сервера, отвечающего за доступ в Интернет. Порт прокси-сервера, Имя пользователя и Пароль - задаются значения для доступа в глобальную сеть.

- Политика - в этой строке должен указываться OID политики безопасности. Предоставляется TSA. Например: 1.2.643.3.41.1.1.5 (тестовая политика для ca.krista.ru/tsp/tsp.srf).

- Алгоритм хэширования - выпадающий список, с алгоритмами хэширования, установленными на машине. Выбираем «ГОСТ Р 34.10-94».

- Алгоритмы подписи сервера штампов времени – список со множественным выбором – в нем

следует отметить алгоритм, который указывается в корневом сертификате сервера TSA (обычно, это «ГОСТ Р 34.10-2001»).

- **Сервер OCSP.** Протокол получения статуса сертификата в реальном времени (проверка списка отзыва).
  - Сервер OCSP. URL-адрес сервера OCSP (без <http://>). Предоставляется владельцем используемого OCSP.
  - Порт сервера OCSP. Порт, через который идет подключение к серверу OCSP (по умолчанию 80, не менять).
  - Прокси-сервер. Используется, если доступ к серверу OCSP происходит с использованием прокси-сервера, отвечающего за доступ в интернет.
  - Алгоритм хэширования. На данный момент ГОСТ 34.11 – 94.
  - Сертификат сервера OCSP. Серийный номер сертификата, которым сервер OCSP подписывает ответы. Прописывается без пробелов. Предоставляется владельцем используемого OCSP.
  - Использовать OCSP при подписании. Определяет необходимость проверки сертификата с помощью OCSP перед наложением подписи.

**7)** В секции **Проверка дат блокирования** можно настроить проверку того, что «Дата принятия» отсылаемого с *клиента УРМ* документа не попадает в закрытый период:

- Делать проверку даты блокирования включает проверку для документов, не относящихся к казначейству - роспись, бюджетные обязательства и т.д.
- Делать проверку даты блокирования казначейства включает проверку для казначейских документов – п/п, чеков и т.д.

Закрытые периоды определяются в зависимости от настроек *АС Бюджет*:

- либо по значению константы «*Константы системы*» - «*Дата последнего редактирования (последняя дата, закрытая для редактирования)*»,
- либо с использованием данных интерфейса *Открытие операционного дня*

**8)** В секции **Настройка сервера ПД** необходимо задать настройки сервера проверки достоверности:

- Сервер ПД - имя машины, на которой запущен сервер проверки достоверности
- Порт сервера ПД - порт, через который идет подключение к серверу проверки достоверности (по умолчанию 8000)

**9)** На закладке «**Диагностика**» по кнопке «*Выполнить*» необходимо проверить *возможность подключения* к указанным *базам данных* и *серверу проверки достоверности*. На экран будет выведен результат подключения:

- Ко всем базам (*АС «Бюджет»* и криптографическим). При наличии каких-либо проблем с подключением, будут выданы соответствующие сообщения.
- К серверу ПД. При корректной настройке сервера ПД должно быть выдано сообщение: «*Подключение к серверу ПД успешно*». На экран будет выведено разрешенное к использованию количество копий УРМ. При наличии каких-либо проблем с подключением, будут выданы соответствующие сообщения.

**10)** На закладке «**Конфигурирование**» нажатием на кнопку «*Создать список клиентов*» необходимо создать список пользователей, который будет использоваться *сервером УРМ* для проверки авторизации клиентов при подключении. Формируется список на основании данных интерфейса «*Права удаленных клиентов*» *РМ «Администрирование УРМ» АС «Бюджет»*.

После выбора базы, произойдет подключение к выбранной базе *АС «Бюджет»* и в окне будет отображен список зарегистрированных в ней удаленных клиентов.

Для создания/обновления списка необходимо нажать кнопку «*Добавить*» и ввести логин и пароль администратора (по умолчанию ADMIN/ADMIN).

Параметр Способ формирования имени пользователя влияет на то, в каком виде будет отображаться имя пользователя в логах, формируемых при работе сервера.

Параметр Принципы добавления имеет значение, когда пользователи подключаются для синхронизации к базам *АС Бюджет* разных лет, в которых список пользователей УРМ может отличаться:

- при выборе значения «Удалять из базы QueryServer отсутствующие в этой базе Бюджета» база пользователей будет заменена на пустую, список пользователей будет заново сгенерирован по выбранной базе *АС «Бюджет»*.

- при выборе значения «Не удалять отсутствующие, добавить новых и обновить существующих» в существующей базе пользователей *Сервера УРМ* будет обновлена информация об наименовании и пароле имеющихся пользователей на основании выбранной базы *АС «Бюджет»*; пользователи УРМ, отсутствующие в базе пользователей *Сервера УРМ*, будут добавлены из базы *АС «Бюджет»*.

**12)** По кнопке «Отчет по сертификатам» утилита *AdminUtil* позволяет сформировать отчет по используемым в системе *сертификатам клиентов УРМ*, установленных на машине с *сервером УРМ*. Такой отчет требуется администраторам финансового органа для того, чтобы своевременно принимать меры по выдаче новых ключей взамен просроченных.

При нажатии на кнопку выводится диалог выбора базы данных АС «Бюджет», после чего на основании этой базы формируется отчет, который содержит следующую информацию:

- Код удаленного клиента;
- Организация - наименование организации удаленного клиента;
- Количество дней, за которое клиент будет предупрежден об истечении срока действия сертификата – данный параметр задается в АС «Бюджет» в «Правах удаленных клиентов».
- Данные сертификата: дата выдачи, дата окончания действия, серийный номер; владелец сертификат, Регион.
- Информация о возможной ошибке, возникшей при формировании отчета (сертификат не установлен, возникло исключение и т.д.).

Кнопка «Сохранить в Excel» позволяет экспортировать сформированный отчет в формат *MS Excel*.

Информация о владельцах сертификатах, их сроках действия будет выведена в отчет только если личные сертификаты клиентов установлены или импортированы на машину с *сервером УРМ*.

Для работы *сервера УРМ* личные сертификаты клиентов устанавливать на *Сервер УРМ* не требуется, но если есть необходимость формирования отчета по сертификатам, то личные сертификаты нужно установить.

## 3 Запуск Сервера УРМ

Если *сервер УРМ* установлен приложением, то для запуска сервера надо загрузить утилиту *QSAgent.exe*.

Если *сервер УРМ* установлен службой, то запуск службы, которая называется **QueryServerJ** происходит автоматически, при включении компьютера. Утилиту *QSAgent.exe* в этом случае надо запускаться вручную или добавить в «Автозагрузку».

## 4 Администрирование Сервера УРМ

### 4.1 Меню управления сервером

По щелчку правой кнопки мыши по значку *QSAgent.exe* в панели задач Windows (systray) доступны следующие пункты контекстного меню.

- **Подключения** - выводит на экран *web-интерфейс* мониторинга **QueryServer** (по умолчанию имя пользователя и пароль совпадают: *HTTPUSER* (большими буквами)) со списком текущих подключений пользователей (удаленных клиентов) к *серверу*, а также общую статистическую информацию. В таблице подключений пользователей для каждого подключения есть элемент управления («X»), позволяющий принудительно разорвать соответствующее подключение.
- **Объекты сервера** – выводит на экран браузер со служебной информацией о внутренних, системных параметрах *сервера*.
- **Лог сервера** – выводит на экран браузер, где открыта страница с логами сервера. На экран выводятся последние события, системного протокола работы сервера, их количество задается в настройках. Протоколы предметных обработчиков на данную страницу не попадают.
- **Приоритетный доступ** – настройка списка пользователей с приоритетным доступом. Приоритетный доступ предназначен для того, чтобы обеспечить одному или нескольким пользователям гарантированную возможность подключения к серверу на определенный промежуток времени. Необходимость в этой функции может возникнуть в случае, когда удаленному клиенту требуется произвести срочные операции (отправить документы) при высокой общей загруженности сервера. Такой приоритетный доступ в каждый момент времени может быть предоставлен только небольшому количеству клиентов, во избежание перегрузки сервера. Приоритетный доступ является временным. Он назначается на определенный промежуток времени и автоматически отключается по истечении заданного интервала времени. Сохранение данных о приоритетном доступе при выгрузке сервера не происходит; после выгрузки сервера и повторной загрузки список пользователей с приоритетным доступом будет пуст.

Для предоставления удаленному клиенту приоритетного доступа следует указать код клиента и длительность действия приоритета в минутах.

- **Пользователи** – редактирование базы пользователей Сервера. В окне «Пользователи» отображается список пользователей с параметрами их доступа. Панель инструментов содержит следующие кнопки:
  - **Загрузить** – загрузить список удаленных клиентов с диска, из конфигурационных файлов QueryServer. Любые изменения, сделанные в окне до этого, будут потеряны;
  - **Сохранить** – сохранение сделанных изменений на диск, в конфигурационные файлы Сервера. Изменения немедленно учитываются в запущенном Сервере (перезагрузка не требуется);
  - **Удалить** – удаление выбранного в таблице пользователя;
  - **Создать** – добавление пользователя;
  - **Свойства** – редактирование параметров выбранного в таблице пользователя.**Внимание!** Сделанные в данном окне вступают в силу сразу после сохранения списка пользователей по кнопке "Сохранить".
- **Веб-пользователи** – редактирование списка пользователей, имеющих право на подключение к *web-интерфейсу* мониторинга **QueryServer**. Для ограничения доступа пользователей локальной сети к *web-интерфейсу* мониторинга работы сервера UPM предусмотрен запрос имени пользователя и пароля при подключении. Уровень защиты не является достаточным для того, чтобы противостоять атакам из *Internet*, поэтому для обеспечения безопасности сервера он должен быть закрыт для доступа из *Internet* по портам, указанным для *web-интерфейса*. По умолчанию (если список пользователей не указан) на сервере зарегистрирован единственный пользователь, который имеет совпадающие *имя пользователя* и *пароль*: HTTPUSER (регистр имеет значение). Для настройки списка пользователей, имеющих доступ к *web-интерфейсу*, следует использовать форму настройки, вызываемую из контекстного меню **Веб-пользователи**. В открывшемся списке следует ввести одну или несколько строк с именем пользователя и паролем. **Внимание!** В именах пользователей и паролях следует использовать только латинские буквы. Имена и пароли чувствительны к регистру.
- **Настройки** – редактирование настроек сервера. Изменения настроек записываются в конфигурационные ini-файлы, которые хранятся в каталоге установки сервера и вступают в силу только после перезагрузки сервера.
- **Управление** – оперативное редактирование настройки сервера. Может понадобиться для экспериментального определения максимального количества одновременных подключений к серверу, то есть допустимой нагрузки на него. Сделанные здесь изменения вступают в силу немедленно после их сохранения (в отличие от изменений, которые делаются по пункту меню **Настройки** - они вступают в силу только после перезагрузки сервера).
- **Шифрование** – настройка шифрования трафика. **Внимание!** Настройки вступают в силу сразу после сохранения (по кнопке "Сохранить").
- **Блокировка** – выводит на экран форму для блокирования приема новых подключений и выгрузки сервера.
- **Выход** – выгрузка утилиты QSAgent. В случае, если сервер установлен приложением, выгрузка сервера производится одновременно с выгрузкой агента. **Внимание!** Выгрузка сервера сопряжена с выполнением некоторых системных операций и может занять некоторое время (до нескольких минут).

## 4.2 Настройка параметров сервера

Настройка параметров сервера производится через **форму настроек**, вызываемую при выборе пункта **Настройки** контекстного меню. Изменения настроек записываются в конфигурационные файлы **QueryServer** и вступают в силу только после перезагрузки сервера.

**Форма настроек** содержит несколько вкладок.

- Закладка **Параметры запуска** содержащих следующие параметры:
  - **Каталог установки программы** – каталог, из которого запускается сервер;
  - **Каталог временных файлов** – каталог, в котором сервер будет хранить свои временные файлы. По умолчанию это подкаталог «IPC» каталога установки сервера. Значения в этих полях можно поменять, после того, как будет снята галка «По умолчанию».
  - **Каталог хранения обновлений** – показывает где сервер будет искать обновления для клиентов (параметр доступен только для чтения, настраивается через *AdminUtil.exe*).
  - **Режим запуска сервера** - определяет способ запуска сервера – приложением или службой.



- Закладка **Сеть** – основные *параметры сетевого взаимодействия*:
  - Адреса – IP-адреса, на которых *сервер* должен принимать входящие подключения. Заполнение параметра может потребоваться, если машина с *сервером* имеет несколько сетевых интерфейсов, и принимать подключения необходимо только с некоторых из них. По умолчанию параметр можно оставить пустым; в этом случае *сервер* будет принимать подключения на все доступные сетевые интерфейсы.
  - Порт – порт протокола TCP/IP, на котором *сервер* принимает подключения клиентов (по умолчанию 5000). Изменение параметра крайне не рекомендуется, поскольку требует синхронного изменения настройки *клиентов* и решения сопутствующих проблем
  - Максимальное количество подключений – ограничение на максимальное количество одновременно обрабатываемых *сервером* подключений
  - Макс. время обработки запроса, мин. – максимальное время, в течение которого предметный обработчик имеет право обрабатывать запрос от *удаленного клиента*. В случае, когда данное время превышено, *сервер* считает, что в обработчике произошел сбой, и принудительно выгружает процесс с одновременным разрывом соединения
  - Макс. длительность сессии, мин. – максимально время работы сессии одного *клиента*. По истечению заданного времени сессия закрывается. Значение 0 – ограничение не применяется
  - Макс. объем данных, Мб – максимальный объем данных, который может пересылаться по сети в рамках одной сессии. При превышении указанного объема данных сессия закрывается, соединение разрывается. Значение 0 – ограничение не применяется.
- Закладка **Обработчики** – параметры, определяющие *время жизни процессов-обработчиков*:
  - Максимальное количество сессий – количество подключений *удаленных клиентов*, после обработки которых происходит перезагрузка процесса
  - Максимальное количество пакетов – количество обработанных запросов (пакетов), после которого происходит перезагрузка процесса
  - Максимальное время работы, мин. – общее время работы процесса, по истечении которого происходит перезагрузка процесса
  - Время жизни свободного обработчика, мин. – время простоя (работы процесса в режиме ожидания, без обработки пакетов от *клиентов*), после которого процесс считается «лишним» и выгружается для экономии ресурсов *сервера*.
- На закладке **Журналирование** – устанавливаются параметры, определяющие ведение *логов внутренних событий сервера*.
  - Режим журналирования – предоставляет возможность выбора одного из трех вариантов:
    - \*Нормальный – в логах отражаются основные события процесса работы сервера. Этот режим рекомендован как основной для работы сервера в процессе опытно-промышленной эксплуатации.
    - \*Диагностика – уровень логов достаточный для выявления фатальных проблем в работе сервера
    - \*Отладка – в лог собираются все сообщения, в том числе предназначенные для отладки приложения в процессе разработки.
  - Создавать дампы всех пакетов и Удалять временные файлы после завершения - используются только в процессе отладки работы сервера и должны меняться только по рекомендации разработчиков. Их применение может привести к очень быстрому исчерпанию свободного места на диске.
- На закладке **Веб-сервер** – делаются настройки для функционирования *web-интерфейса мониторинга активности сервера*:
  - Адрес внутреннего HTTP – список IP-адресов, на которых должен слушать web-сервер. Параметр можно оставить пустым (по умолчанию); при этом сервер будет слушать на всех доступных сетевых интерфейсах;
  - Порт внутреннего HTTP – порт, на котором будет принимать подключения web-сервер;
  - Максимальное количество подключений к серверу. – определяет сколько пользователей смогут одновременно подключиться к *web-интерфейсу*
  - Количество записей в веб-логе – количество событий, которое будет отображаться в *web-интерфейсе сервера* на вкладке *Лог сервера* (старые события не отображаются)
  - Количество веб-логов сессий – количество сессий, для которых будут отображаться логи в *web-интерфейсе сервера* на вкладке *Логи сессий*
  - Количество записей веб-лога сессий – количество событий, которое будет отображаться в *web-интерфейсе сервера* для каждой сессии, на вкладке *Логи сессий*.

### 4.3 Доступ к Web- интерфейсу для мониторинга работы сервера

*WEB-интерфейс* имеет несколько вкладок. Некоторые из них (*Подключения, Объекты сервера, Лог*) открываются напрямую при выборе соответствующего пункта из контекстного меню *QSAgent*, переход к другим возможен только через браузер.

На машине с сервером УРМ *web-интерфейс* можно вызвать из контекстного пункта меню агента - Подключения. Для доступа с другой машины необходимо в браузере набрать [http:// <имя машины с сервером УРМ>:8001](http://<имя машины с сервером УРМ>:8001)

Если в локальной сети настроены брандмауэры, необходимо открыть для доступа порт 8001. Для ограничения доступа пользователей к управлению сервером браузер при подключении запрашивает имя пользователя и пароль. По умолчанию имя пользователя и пароль совпадают: *HTTPUSER*(большими буквами).

## 5 Дополнительные утилиты сервера обмена данными

### 5.1 Монитор отладочных сообщений EventMonitor.exe

*EventMonitor.exe* – утилита для просмотра *журналов работы сервера УРМ*. Журналы ведутся постоянно и сохраняются в лог-файлы в папке *LOGS* каталога установки сервера обмена данными. За каждый день в указанном каталоге создается папка с названием, соответствующем дате создания в формате <год>.

<месяц>.<день> (например, 2018.01.21). Чтобы посмотреть логи, необходимо открыть все файлы за нужный день. Панель управления утилиты содержит следующие функции:

Показать панель фильтрации (Ctrl+G), – показать/скрыть панель параметров фильтрации;

Показать «подвал» (Ctrl+M), – показать/скрыть панель текста сообщения;

Фильтрация (Ctrl+F), – установить/снять фильтрацию;

Открыть файл лога (Ctrl+O), – открыть файлы;

Сохранить лог в файле (Ctrl+S), – сохранить логи;

Очистить лог – очистить рабочую область;

Обновить (F5), – перечитать логи.

Если установить *фильтр «Сообщение»* – содержит *«Подстрока»* – **соединен**, то можно увидеть записи, соответствующие началу соединения и закрытию соединений.

Если установить *фильтр «Сообщение»* – содержит *«Подстрока»* – **синхрониз**, то можно увидеть записи, соответствующие запросам на синхронизацию: (номер удаленного клиента, время запроса, по периоду синхронизации определить – полная или простая).

Если установить *фильтр «Сообщение»* – содержит *«Подстрока»* – **ошибка на**, то можно увидеть записи, соответствующие ошибкам при синхронизации, в том числе текст ошибки (при условии, что клиент отправил сообщение об ошибке на сервер). Чтобы увидеть записи, соответствующие ошибкам вообще, то можно установить *фильтр «Сообщение»* – содержит *«Подстрока»* – **ошибк**.