

**«Интеграционная платформа для организации продаж
железнодорожных билетов и сопутствующих услуг со
встроенным биллингом»**

Инструкция по установке

Оглавление

1 Первичные действия	3
1.1 Специалисты, необходимые для обеспечения работы системы.....	3
2 Действия системного администратора при установке и наладке системы	4
2.1 Требования к рабочему месту системного администратора.....	4
2.2 Параметры программного обеспечения, необходимые для работы с АИС	4
2.3 Общий вид системы.....	5
2.4 Развертывание приложения B2B.....	6
2.4.1 Требования и подготовка системы.....	6
2.4.2 Установка IIS	6
2.4.3 Развертывание приложения	9
2.5 Настройка Redis	14
2.6 Настройка Nginx.....	14
2.6.1 Общее описание	15
2.6.2 Конфигурация сервиса	15
3 Обновление 1С	18
3.1 Обновление 1С: Восстановление работоспособности интеграционного модуля.....	18
3.2 Пошаговая инструкция настройки web-сервисов для 1Сv8.3 и IIS 8.5	20
4 Эксплуатация, техническое обслуживание, ремонт и хранение компонентов системы	30
5 Действия при возникновении ошибок и неполадок	31

Перечень сокращений

Термин	Определение
АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
АИС	Автоматизированная информационная система
База данных (БД)	Совокупность данных, организованных в соответствии с концептуальной схемой, описывающей характеристики этих данных и связи между соответствующими им объектами, поддерживающая одну или несколько предметных областей
Доступ к информации (Доступ)	Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации
Пользователь	Лицо, сотрудник Заказчика или организаций-агентов, участвующее в функционировании Системы или использующее результаты ее функционирования
ПО	Программное обеспечение
ПК	Персональный компьютер
Система	Интеграционная платформа для организации продаж ЖД билетов и сопутствующих услуг организациями агентами со встроенным биллингом и порталом самообслуживания сотрудников организаций агентов
Nginx	Веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах (тестировалась сборка и работа на FreeBSD, OpenBSD, Linux, Solaris, Mac OS X, AIX и HP-UX). Начиная с версии 0.7.52 появилась экспериментальная бинарная сборка под Microsoft Windows
Redis	(англ. remote dictionary server) – сетевое журналируемое хранилище данных типа «ключ – значение» с открытым исходным кодом. Нереляционная высокопроизводительная СУБД
Zabbix	Свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования

1 Первичные действия

1.1 Специалисты, необходимые для обеспечения работы системы

Минимальное количество специалистов, необходимое для обеспечения работы системы.

Для работы системы минимально необходимы:

- 1 системный администратор;
- 1 администратор баз данных.

Системный администратор и администратор баз данных должны обладать высоким уровнем квалификации в следующих областях:

- администрирование технических средств (серверы, рабочие станции);
- администрирование программного обеспечения операционных систем и систем управления базами данных;
- разработка, управление и реализация эффективной политики информационной безопасности;
- модернизация программных и технических средств.

2 Действия системного администратора при установке и наладке системы

2.1 Требования к рабочему месту системного администратора

Рабочее место системного администратора:

- стандартный офисный персональный компьютер, оснащённый браузером, Интернетом и снабженный источниками бесперебойного питания 220 вольт;
- операционная система не ниже Windows 7/8/10, Linux с ядром 2.6/3.x;
- наличие непрерывного подключения каждого из пользовательских ПК к АСУ посредством сети TCP/IP, не хуже 256 кбит/с и задержкой (ping) не более 50 мсек.

2.2 Параметры программного обеспечения, необходимые для работы с АИС

Доступ пользователя к Системе осуществляется в режиме тонкого клиента, функционирующего в различных операционных средах – Microsoft Windows, Unix (Linux), Mac OS.

Доступ к Системе возможен с любого терминального устройства (терминала) в режиме реального времени.

Для работы с Системой необходимо:

- терминальное устройство (компьютер, смартфон, планшет и т.п.);
- доступ к сети Интернет;
- браузер с поддержкой HTML 4.0, CSS Level 2, JavaScript 1.1. и выше, режима асинхронного взаимодействия JavaScript/XML (XMLHttpRequest и т.п.). Пользовательские интерфейсы Системы совместимы с браузерами: Microsoft Internet Explorer версии 8.0 или выше, Mozilla FireFox версии 6.0 или выше, Google Chrome версии 10.0 или выше;
- сертификат безопасности (при наличии). Необходимость установки, установка и выдача сертификата безопасности определяется и производится системным администратором.

Примечание:

В настоящий момент используется корневой SSL сертификат, подтверждающий валидность доменного имени, по которому доступно приложение для пользователя из сети Интернет.

Данный сертификат публичен, и его может кто угодно посмотреть/установить к себе. На самом деле браузер сам так и делает при первом обращении на partner.fps.ru.

Доступ к приложению выдаётся по логину и паролю с использованием двойной (двухфакторной) аутентификации пользователя. Администратор должен выдать логин и пароль, и доверенным способом сообщить его клиенту (в разрезе B2B).

Доступ пользователей к функциональным сервисам осуществляется по технологии «тонкого клиента» на базе web-обозревателя (браузера) посредством АРМ (автоматизированных рабочих мест). Тип используемого АРМ и состав функций, доступных пользователю, определяется в зависимости от его роли. При этом роль определяется правами пользователей на доступ к сервисам, функциям и данным, а АРМ – способ представления информации и размещения управляющих элементов, оптимизированные для соответствующей категории пользователей.

2.3 Общий вид системы

Общий вид системы представлен ниже (Рисунок 1).

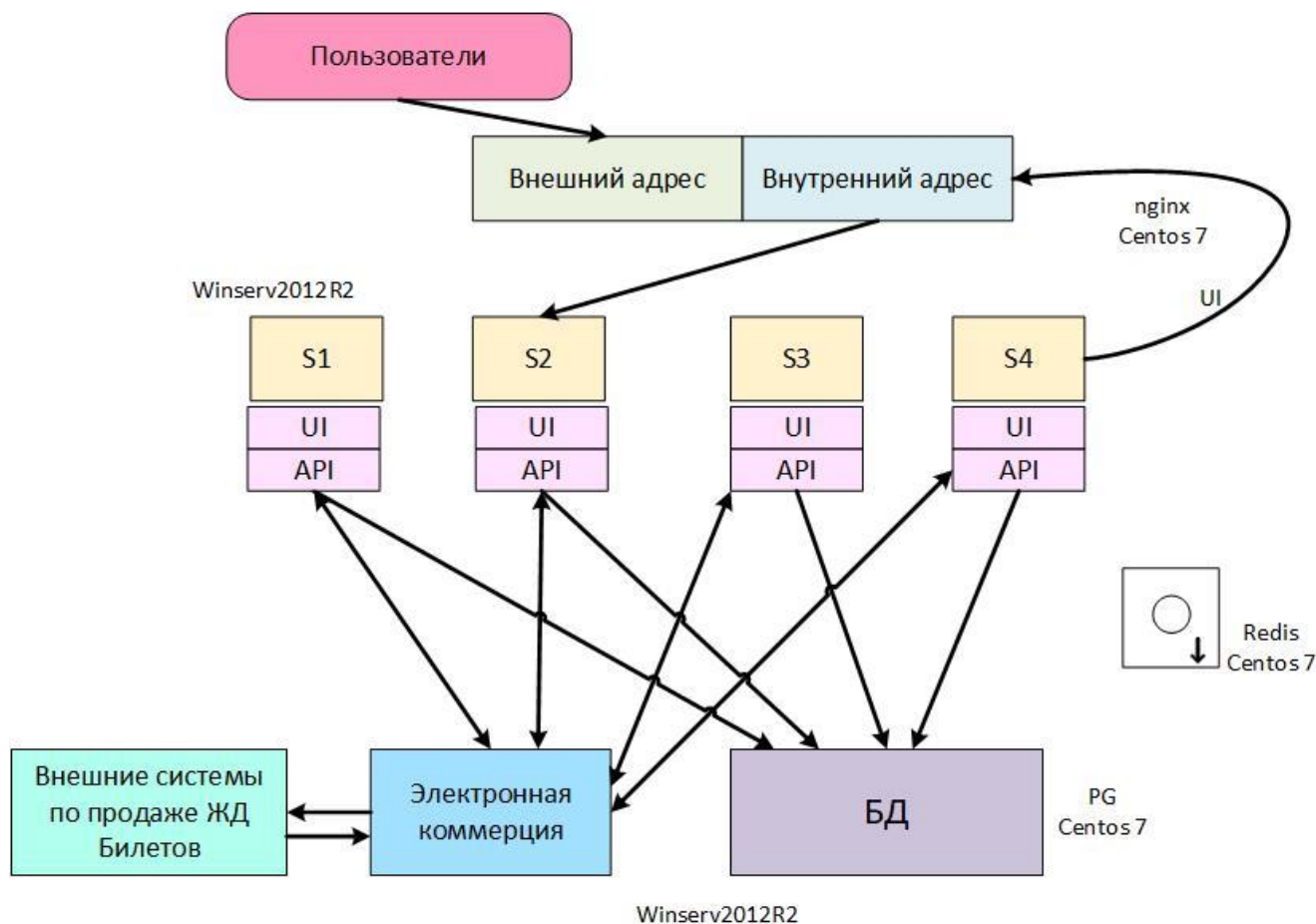


Рисунок 1 – Общий вид системы

S1, S2, S3, S4 – это сервера.

БД – база данных;

API – программный интерфейс приложения;

UI – интерфейс пользователя

2.4 Развертывание приложения B2B

Системный администратор получает доступ к системе, после заключения договора между Заказчиком и Исполнителем. Все подробные детали необходимо смотреть в соответствующем договоре.

2.4.1 Требования и подготовка системы

1. Windows 2012 R2;
2. Должны стоять все актуальные обновления;
3. Обязательно должно стоять обновление (KB3102467)

Microsoft .NET Framework 4.6.1 в Windows Server 2012 R2 для 64-разрядных систем;

4. Для тестовой среды, на сервере БД в конце файла postgresql.conf нужно добавлять строчку `custom_settings.working_mode = 'test'`.

2.4.2 Установка IIS

1. Запустить мастер добавления ролей, выделяем Веб-сервер (IIS).

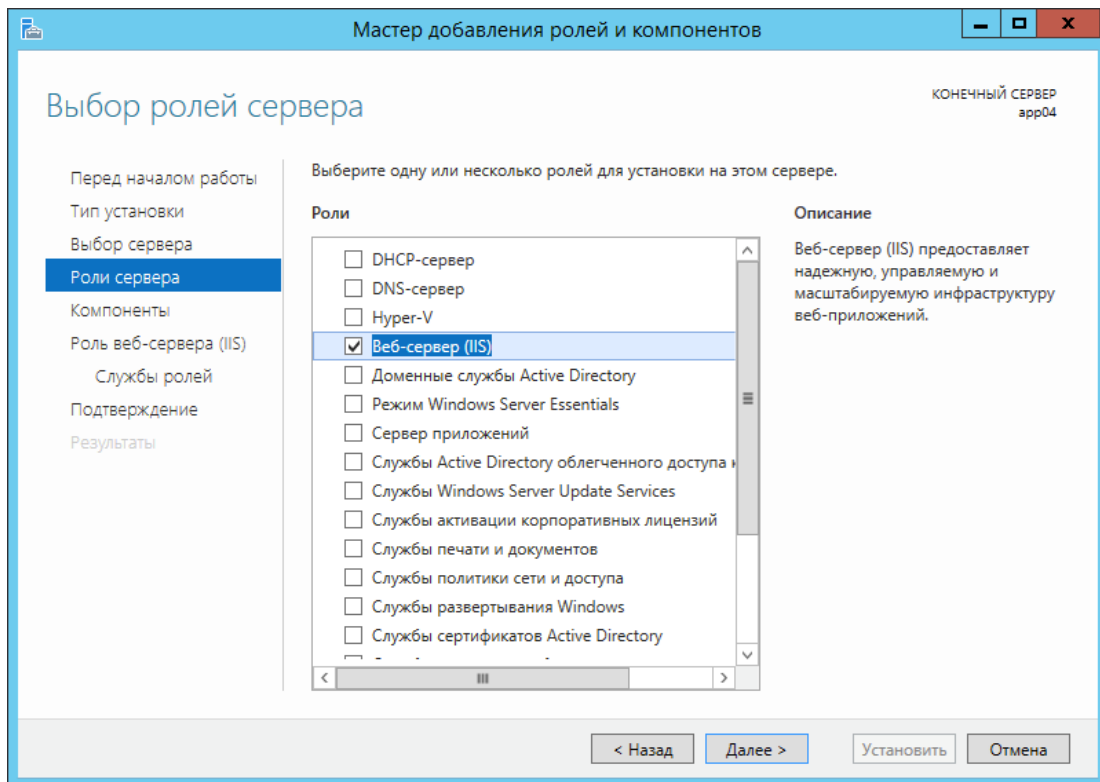


Рисунок 2 – Добавление ролей и компонентов

2. Нажать далее.

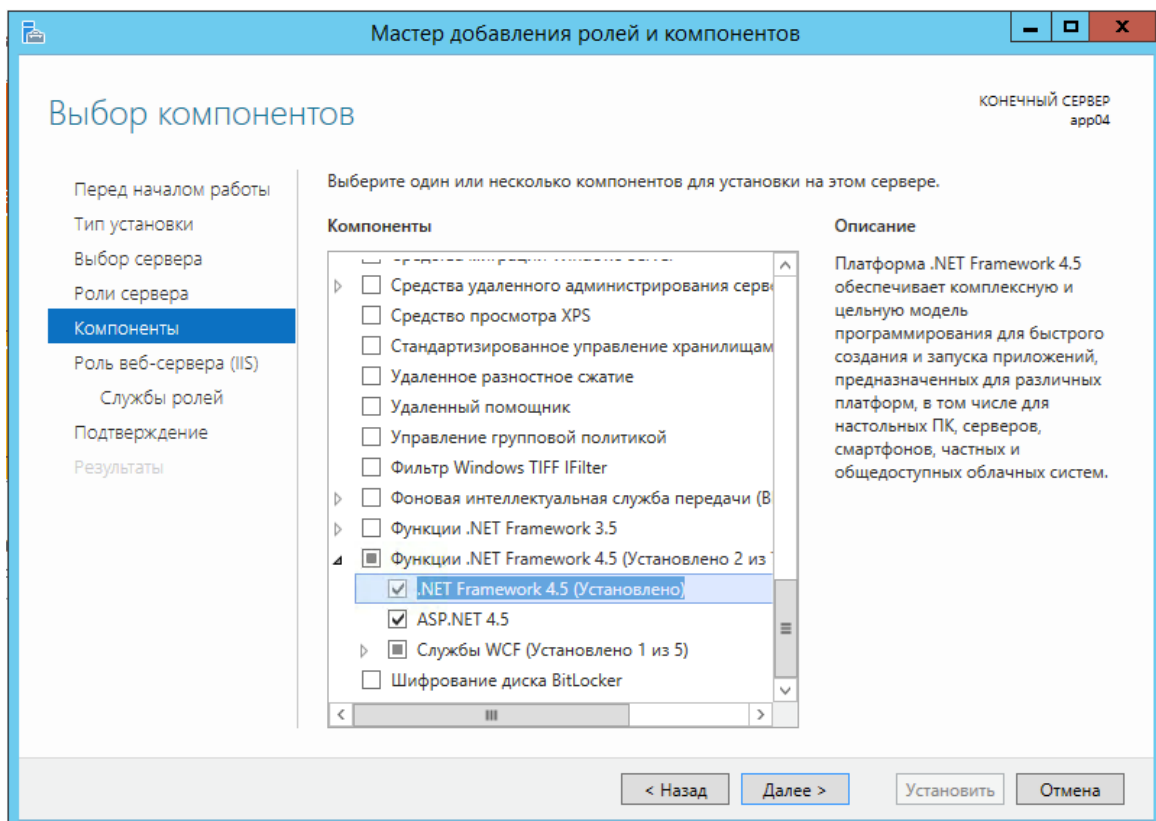


Рисунок 3 – Нажать далее

3. На экране компонентов выделить .NET 4.5.

4. Нажать далее.
5. Далее установить компоненты IIS как показано на скриншотах.

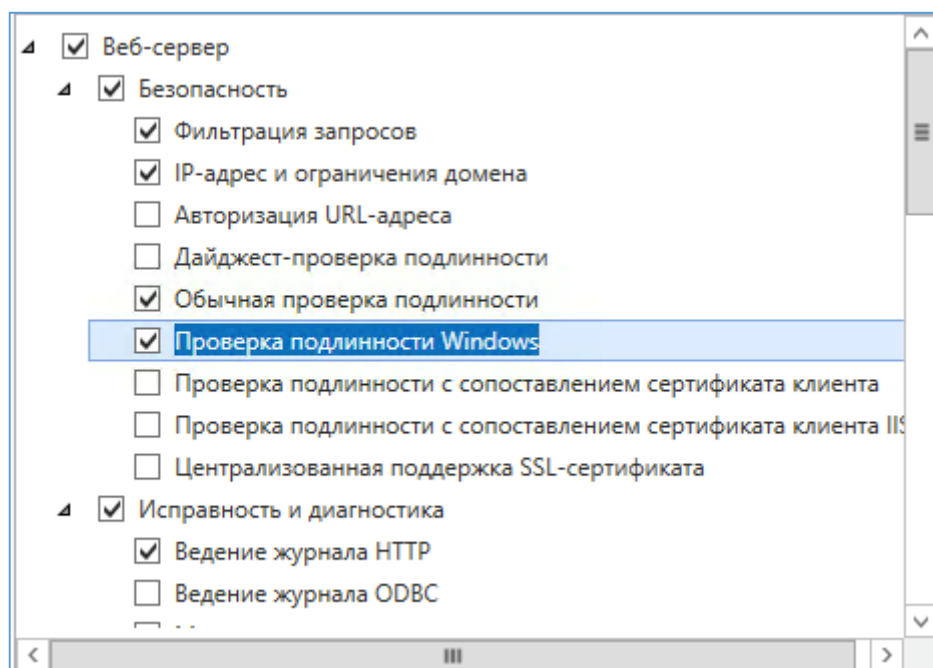


Рисунок 4 – Установка компонентов часть 1

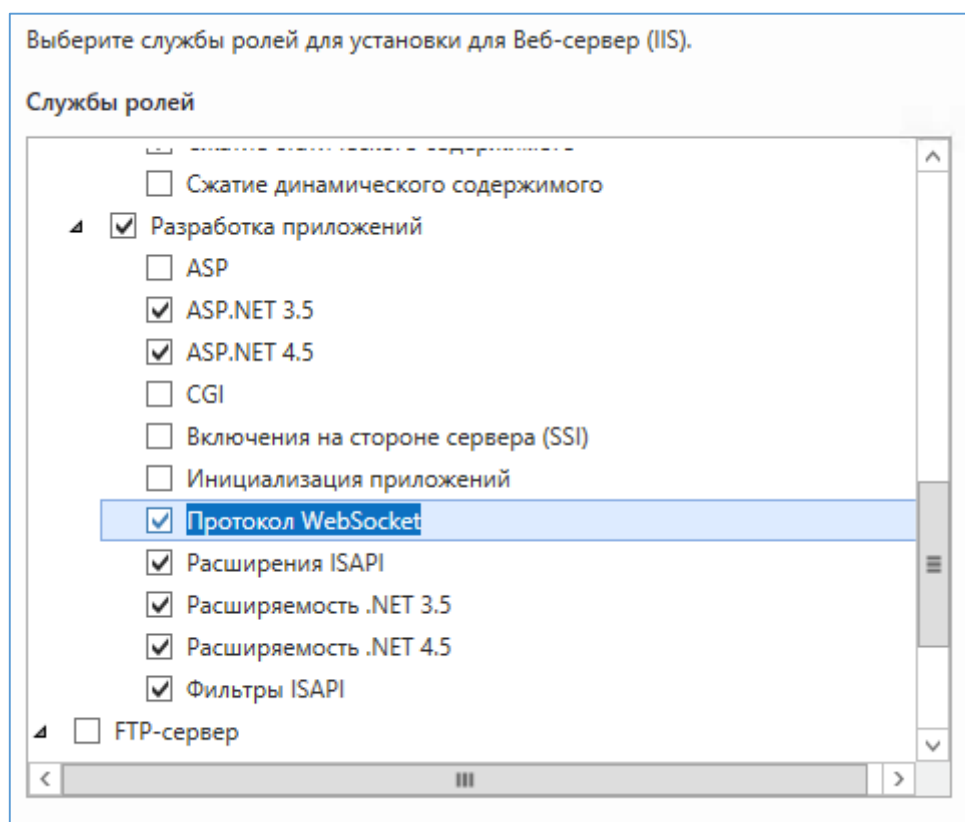


Рисунок 5 – Установка компонентов часть 2

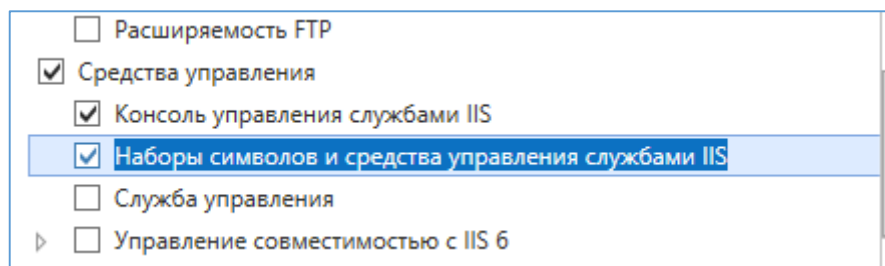


Рисунок 6 – Установка компонентов часть 3

2.4.3 Развертывание приложения

1. Проверить права на папки.

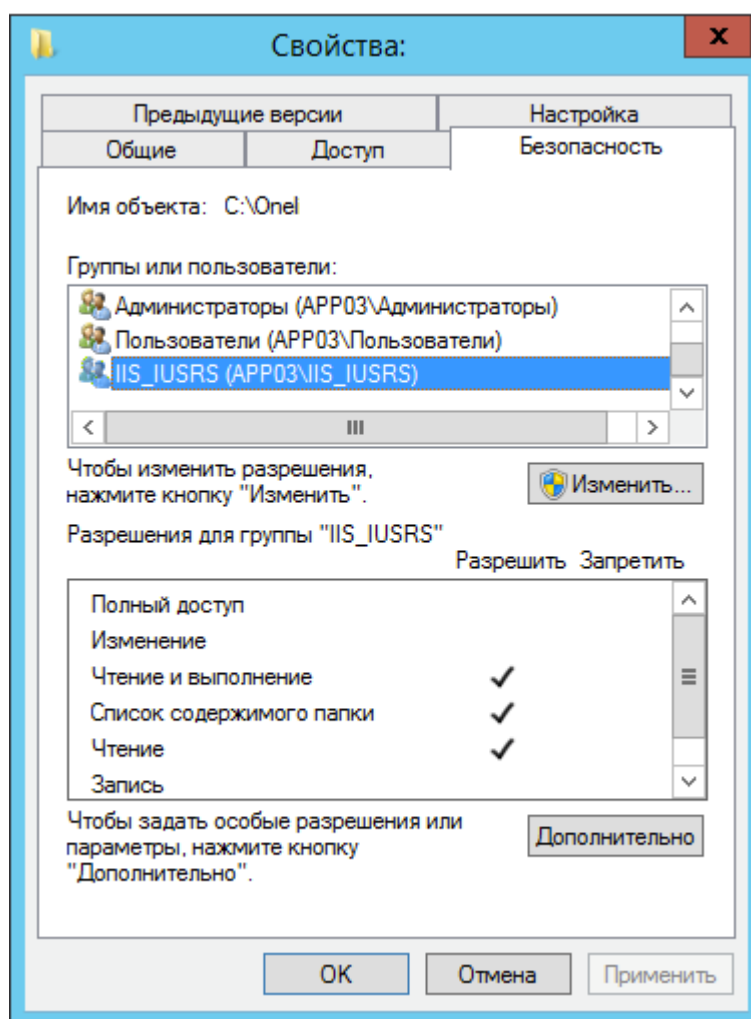


Рисунок 7 – Свойства папки 1

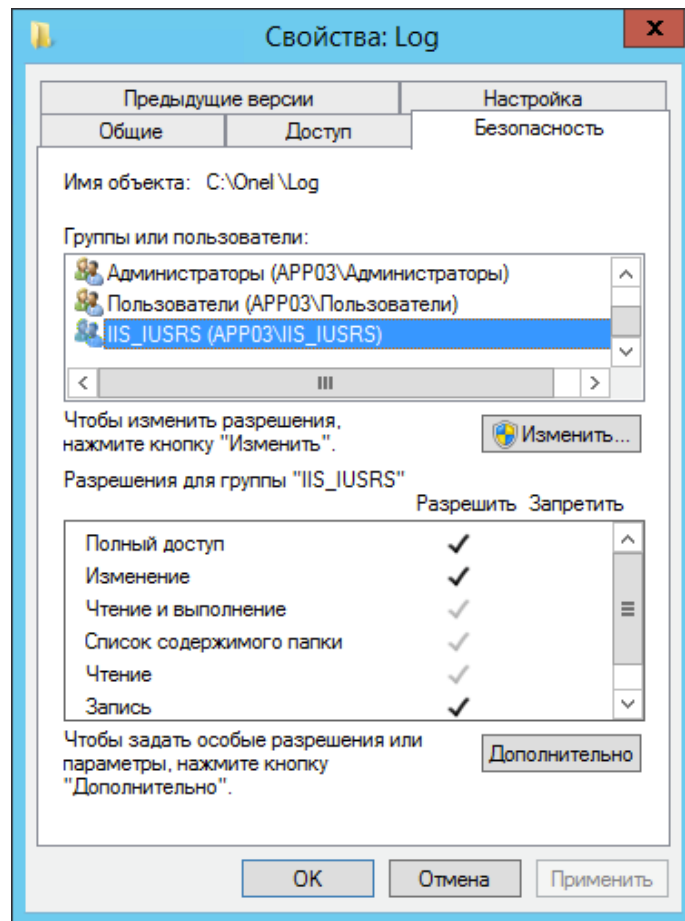


Рисунок 8 – Свойства папки 2

2. Открыть оснастку «Диспетчер служб IIS»;
3. Добавить сайт;

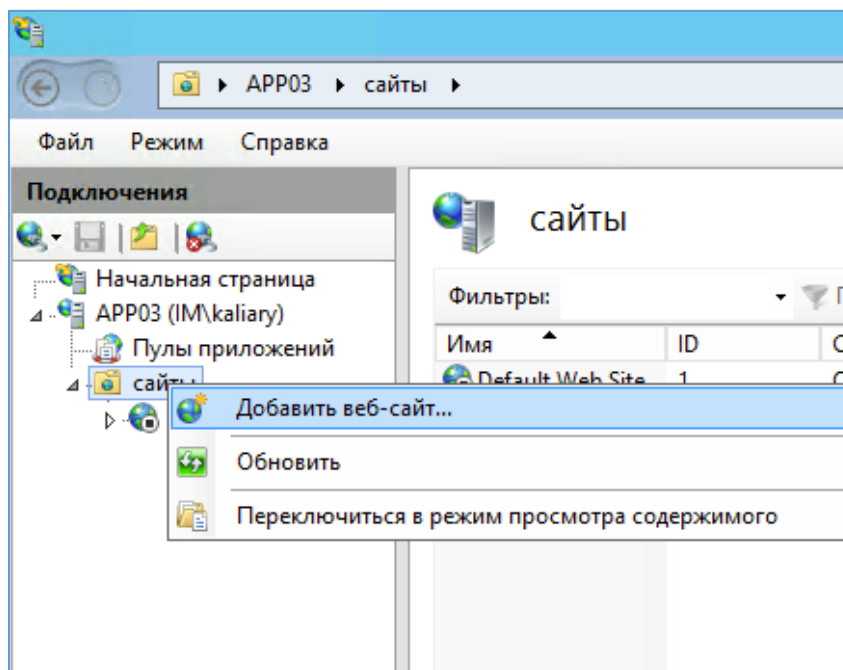


Рисунок 9 – Добавление сайта

4. Заполнить поля.

Имя сайта: Ui

Физический путь: C:\Onel\Production\UiRoot

Привязка: тип http, IP-адрес указываем фактический на сетевом адаптере, порт [PORT],

Имя узла: partner.fpc.ru im.local

Добавить веб-сайт

Имя сайта: Ui

Пул приложений: Ui

Выбрать...

Каталог содержимого

Физический путь: C:\Onelia\Production\UiRoot

Проверка подлинности

Подкл. как... Тест настроек...

Привязка

Тип: http

IP-адрес:

Порт:

Имя узла: partner.fpc.ru

Пример: www.contoso.com или marketing.contoso.com

☒ Запустить веб-сайт сейчас

OK Отмена

Рисунок 10 – Заполнение полей

5. Далее нужно добавить в сайт приложения.

Приложения два:

- B2B;
- Backoffice.

Добавление приложения

Название сайта: Ui
Путь: /

Псевдоним: B2b
Пул приложений: Ui
Выбрать...

Пример: продажи

Физический путь: C:\Onel\Production\B2b ...

Проверка подлинности
Подкл. как... Тест настроек...

☐ Включить предварительную загрузку

OK Отмена

Рисунок 11 – Добавление в сайт приложения B2B

Добавление приложения

Название сайта: Ui
Путь: /

Псевдоним: Backoffice
Пул приложений: Ui
Выбрать...

Пример: продажи

Физический путь: C:\Onel\Production\Backoffice ...

Проверка подлинности
Подкл. как... Тест настроек...

☐ Включить предварительную загрузку

OK Отмена

Рисунок 12 – Добавление в сайт приложения Backoffice

6. Добавляем второй сайт Api.
7. Заполнить поля.

Имя сайта: Арі

Физический путь: C:\Onel\Production\Арі

Привязка: тип http, IP-адрес указываем фактический на сетевухе, порт [PORT];

Имя узла: api.partner.fpc.ru api.im.local

Добавить веб-сайт

Имя сайта: Арі

Пул приложений: Арі

Выбрать...

Каталог содержимого

Физический путь: C:\Onel\Production\Арі

Проверка подлинности

Подкл. как... Тест настроек...

Привязка

Тип: http

IP-адрес:

Порт:

Имя узла: api.partner.fpc.ru

Пример: www.contoso.com или marketing.contoso.com

☒ Запустить веб-сайт сейчас

OK Отмена

Рисунок 13 – Добавление второго сайта Арі

8. Далее нужно добавить в сайт одно приложение.

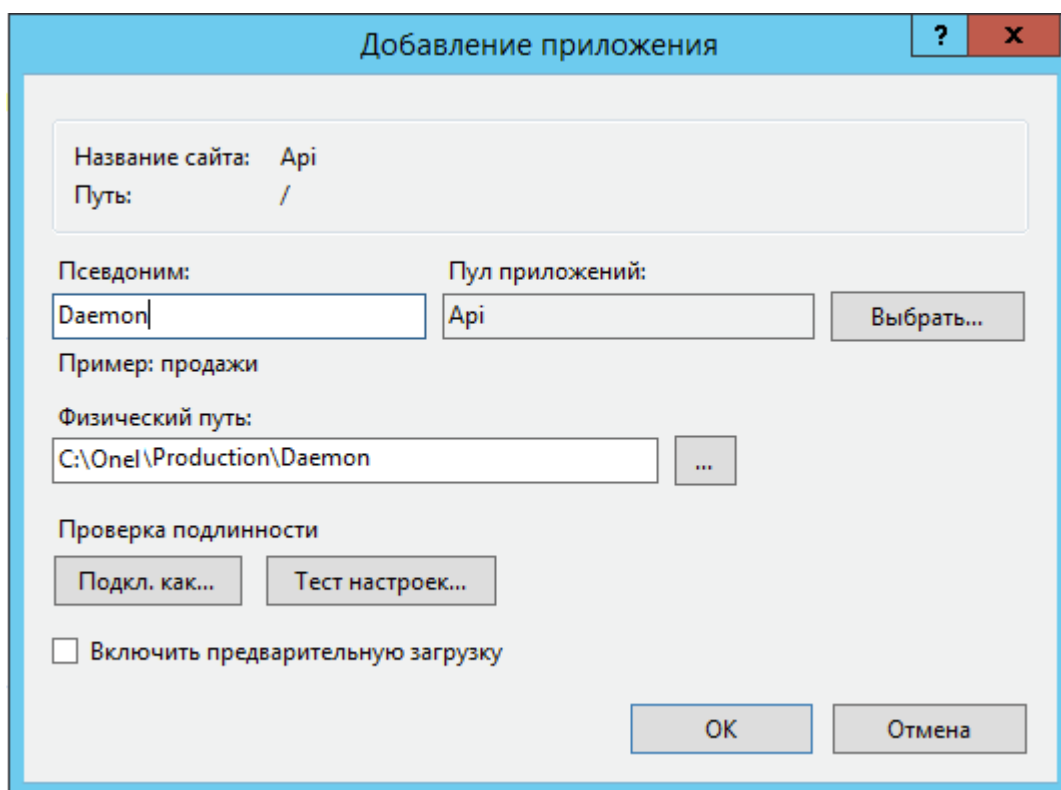


Рисунок 14 – Добавление приложения

2.5 Настройка Redis

Redis – сетевое журналируемое хранилище данных типа «ключ – значение» с открытым исходным кодом. Нереляционная высокопроизводительная СУБД.

Конфигурация сервиса: /etc/redis.conf

Лог сервиса: /var/log/redis/

Настройки ОС, выполненные для корректной работы сервиса:

/etc/sysctl.d/redis.conf:

net.core.somaxconn = 1024 - настройка максимального количества прослушиваемых портов;

vm.overcommit_memory = 1 - правило работы overcommit.

/etc/sysconfig/grub - отключение transparent hugepages (THP) (transparent_hugepage=never).

Сервис добавлен в автозапуск.

2.6 Настройка Nginx

Nginx – веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах (тестировалась сборка и работа на FreeBSD, OpenBSD, Linux, Solaris, Mac OS X, AIX и HP-UX). Начиная с версии 0.7.52 появилась экспериментальная бинарная сборка под Microsoft Windows.

2.6.1 Общее описание

Сервер nginx предназначен для проксирования запросов к сайту partner.fpc.ru на 2 сервера приложений (бэкенды), при этом запросы балансируются на бэкенды по принципу Round-Robin.

Также сервер обслуживает сайт im.local, для которого не применяется балансировка нагрузки.

2.6.2 Конфигурация сервиса

Конфигурация сервиса представлена далее:

```
upstream backend {
```

```
server IP_APPSERVER : [PORT];
```

```
server IP_APPSERVER : [PORT]; }
```

 - параметры балансировки: запросы будут распределяться по указанным серверам по принципу Round-Robin.

Выход из строя сервера определяется по невозможности установить с ним TCP-соединение, критерий выхода из строя - "хотя бы один запрос", после этого сервер на 10 секунд помечается как сбойный и запросы на него не отправляются.

```
server {
```

```
listen [PORT];
```

```
server_name partner.fpc.ru api.partner.fpc.ru;
```

```
return 301 https://$host$request_uri;
```

```
}
```

 - описание сайта: в случае, если клиент обращается по указанным доменным именам на 80 порт, то в ответ получает 301 код с редиректом на HTTPS.

```
server {
```

```
listen 443 ssl;
```

```
server_name partner.fpc.ru api. partner.fpc.ru im.local api. im.local IP_APPSERVER;
```

```
ssl_certificate /etc/nginx/ssl/ partner.fpc_ru_2017_10_14.crt;
```

```
ssl_certificate_key /etc/nginx/ssl/ partner.fpc.key;
```

 - описание сайта с указанием сертификатов, которые будем использовать.

```
ssl_ciphers "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-DSS-AES256-GCM-SHA384:DHE-DSS-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-DSS-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-
```

AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES128-SHA256:DHE-DSS-AES128-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:DHE-DSS-SEED-SHA:DHE-DSS-CAMELLIA128-SHA:EDH-DSS-DES-CBC3-SHA:EC DH-RSA-AES128-GCM-SHA256:EC DH-ECDSA-AES128-GCM-SHA256:EC DH-RSA-AES128-SHA256:EC DH-ECDSA-AES128-SHA256:EC DH-RSA-AES128-SHA:EC DH-ECDSA-AES128-SHA:EC DH-RSA-DES-CBC3-SHA:EC DH-ECDSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:SEED-SHA:CAMELLIA128-SHA:DES-CBC3-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-DES-CBC3-SHA:KRB5-IDEA-CBC-MD5:KRB5-DES-CBC3-MD5:EC DH-ECDSA-RC4-SHA:EC DH-RSA-RC4-SHA:EC DH-ECDSA-RC4-SHA:PSK-RC4-SHA:KRB5-RC4-SHA:KRB5-RC4-MD5"; - Список шифров, считающихся безопасными на 10.2016 (нужно периодически проверять).

`ssl_prefer_server_ciphers on;` - принудительное использование клиентами только тех шифров, которые описаны выше.

`ssl_protocols TLSv1.1 TLSv1.2;` - список используемых протоколов, считающихся безопасными на 10.2016 (нужно периодически проверять).

Эти настройки могут вызвать проблемы (невозможность соединения) на стороне клиентов в тех случаях, если у них будет стоять старый браузер, не поддерживающий указанные протоколы и шифры.

```
location / {
    proxy_read_timeout 1200;
    proxy_connect_timeout 1200;
    proxy_pass http://backend;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr; - проброс заголовков на бэкенд
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for; - проброс заголовков на
бэкенд
    proxy_set_header X-HTTPS yes; - проброс заголовков на бэкенд
```

```
access_log /var/log/nginx/upstream-access-onelya.log upstreamlog;  
}
```

```
error_page 404 /404.html;  
location = /40x.html {  
}
```

```
error_page 500 502 503 504 /50x.html;  
location = /50x.html {  
}  
}
```

Для сайта `im.local` настройки аналогичны, за исключением SSL (потому что там его нет).

3 Обновление 1С

3.1 Обновление 1С: Восстановление работоспособности интеграционного модуля

Восстановление работоспособности интеграционного модуля (1С --> В2В). Для обновления 1С необходимо совершить следующие действия:

1. После обновления конфигурации 1С, необходимо вручную изменить исполняемый файл обработчика внешних запросов (Рисунок 15).

Настройки IIS → Сайты (innovationmobility) → Сопоставления обработчиков → 1С Web-service Extension (изменить значение в графе «Исполняемый файл»:

C:\Program Files (x86)\1cv8\НОМЕР АКТУАЛЬНОЙ КОНФИГУРАЦИИ\bin\wsisapi.dll

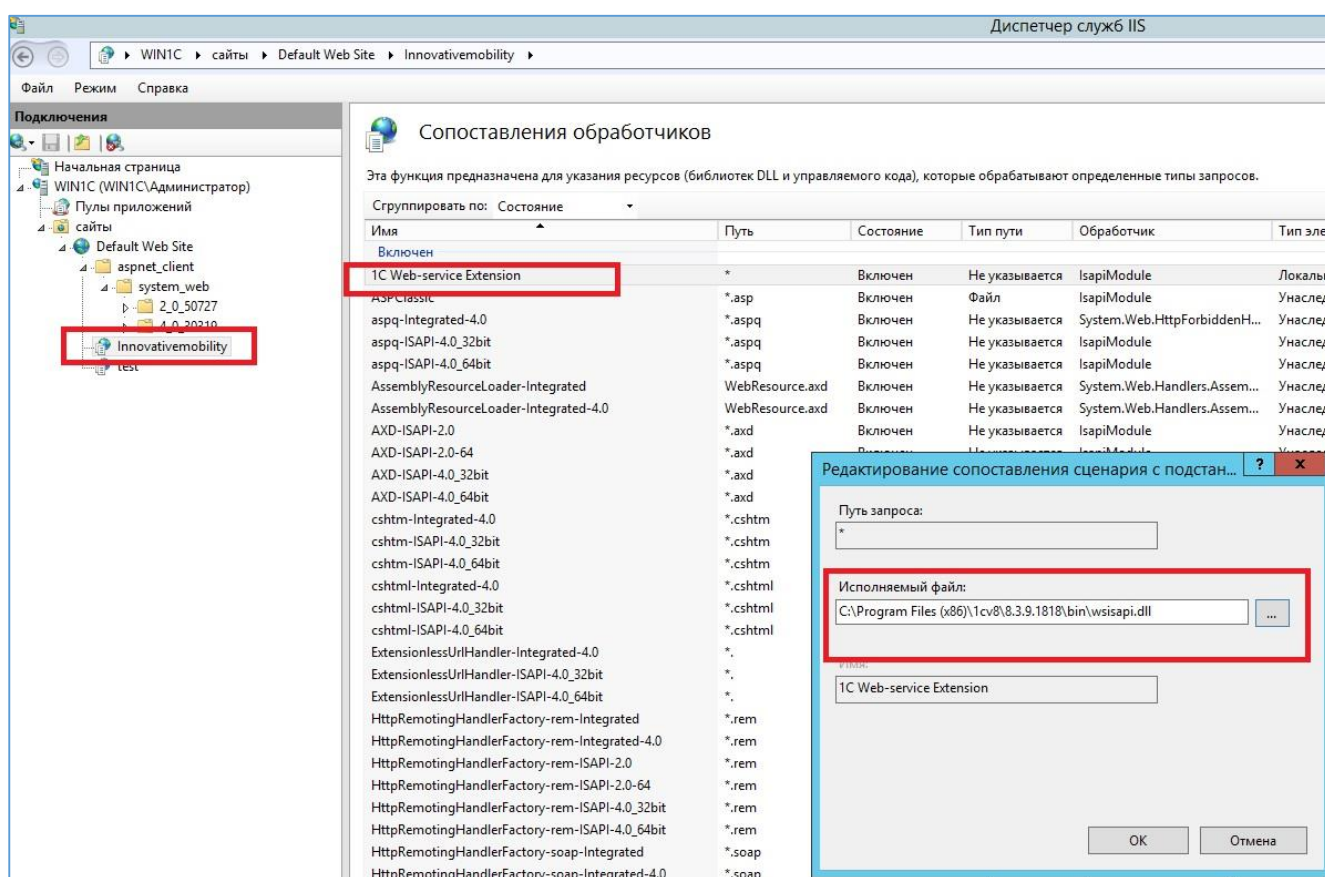


Рисунок 15 – Интеграционный модуль

При эксплуатации могут быть выявлены периодические подвисания служб IIS на сервере 1С. Восстановление работоспособности, после таких подвисаний, происходит путём перезапуска служб IIS.

Проверка корректности запуска служб:

1. Войти, используя свои идентификационные данные – логин и пароль (залогиниться), в базу через браузер.

2. Проверить статусы пулов приложений (Рисунок 16).

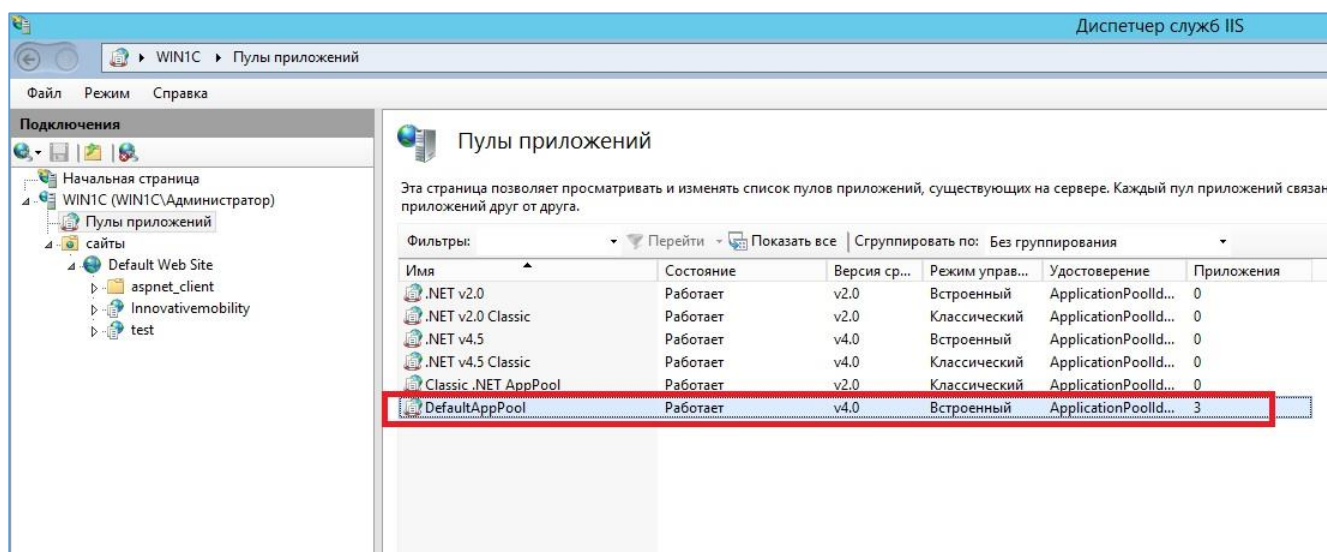


Рисунок 16 – Пулы приложений

При возникновении необходимости запретить пользователю import_user заходить в базу 1С (Рисунок 17) следует действовать в соответствии с рекомендациями, казанными далее.

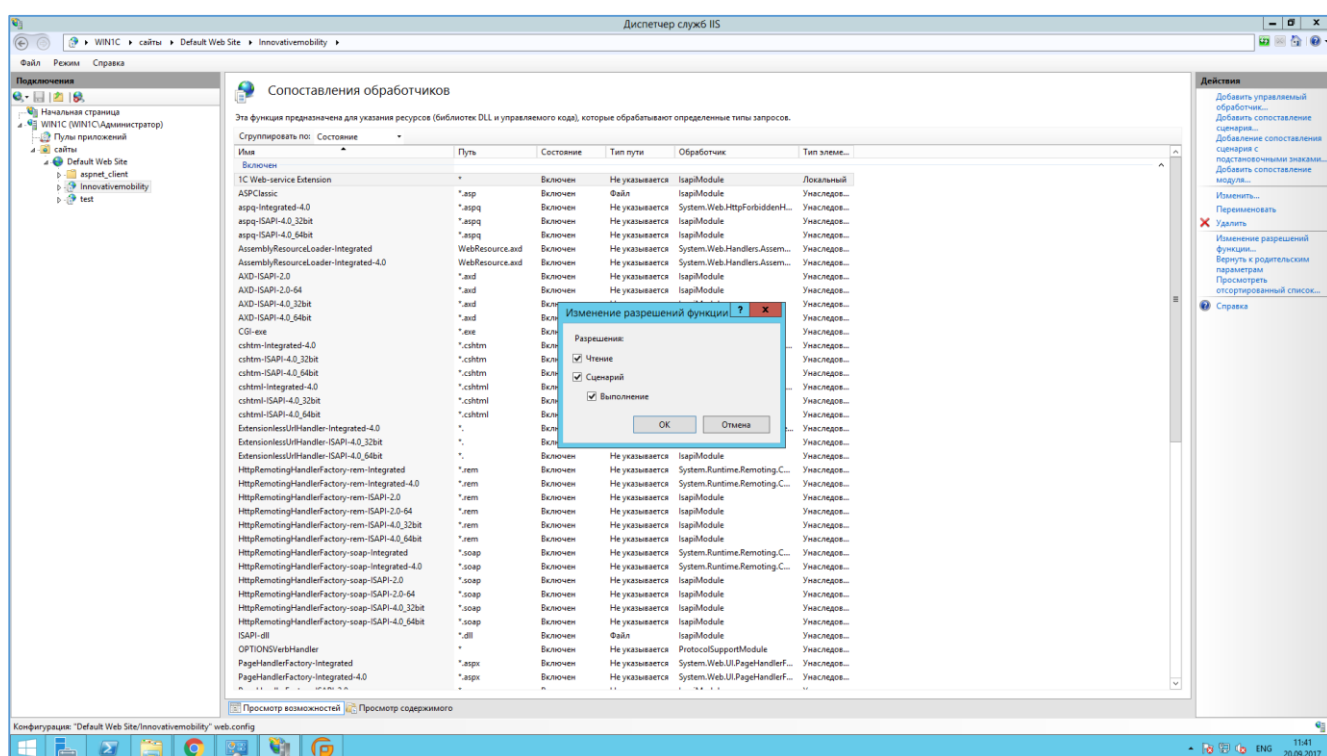


Рисунок 17 – Запрет на вход пользователя import_user в базу 1С

Для того чтобы запретить пользователю import_user заходить в базу 1С необходимо:

1. Зайти на Сервер 1С.
2. Выбрать диспетчер IIS.

3. Затем выбрать InnovativeMobility.
4. После выбрать «Сопоставления обработчиков».
5. Далее, найти в списке «1С Web-service Extension».
6. Выбрать изменение разрешений функции.
7. Снять все галочки.
8. После вышеописанных манипуляций можно проводить обновления конфигураций и платформ 1С, предварительно сняв бэкапы баз.

При выявлении случаев, когда конфигурация основной базы не обновляется, то, скорее всего, это связано с наличием доработок в базе.

Решение: дождаться выхода очередного релиза конфигурации, после чего обновляться.

3.2 Пошаговая инструкция настройки web-сервисов для 1Сv8.3 и IIS 8.5

Далее представлена пошаговая инструкция настройки web-сервисов для 1Сv8.3 и IIS 8.5, Windows Server 2012 R2 Standard, 1С:Предприятие 8.3 (8.3.4.465).

1. Установка IIS выполняется стандартными средствами. Набор достаточных компонент приведен на скриншоте (Рисунок 18).

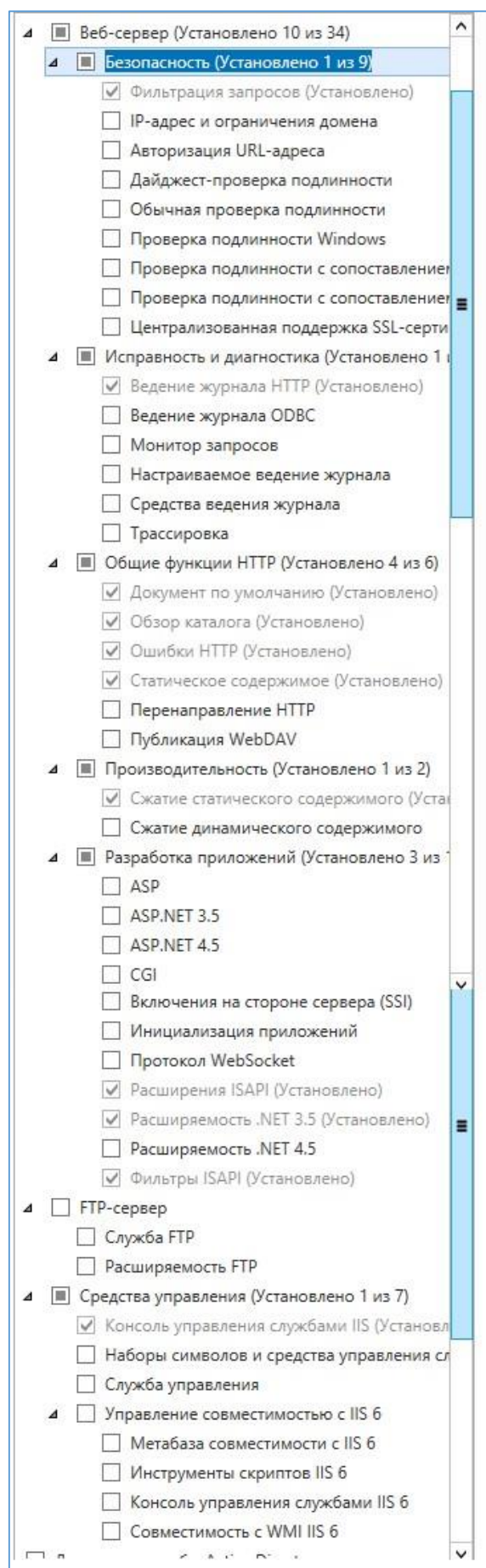


Рисунок 18 – Набор компонент

2. Создать папку на web-сервере. В примере папка называется «1С».

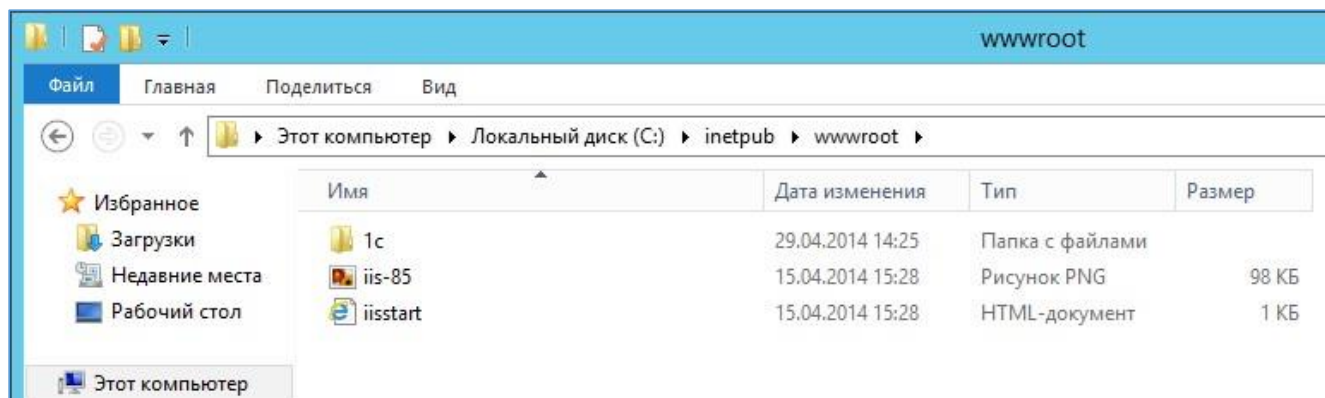


Рисунок 19 – Создание папки на web-сервере

3. Опубликовать сервис из 1С.

Администрирование -> 1С -> Конфигуратор -> Администрирование -> Публикация на web-сервере.

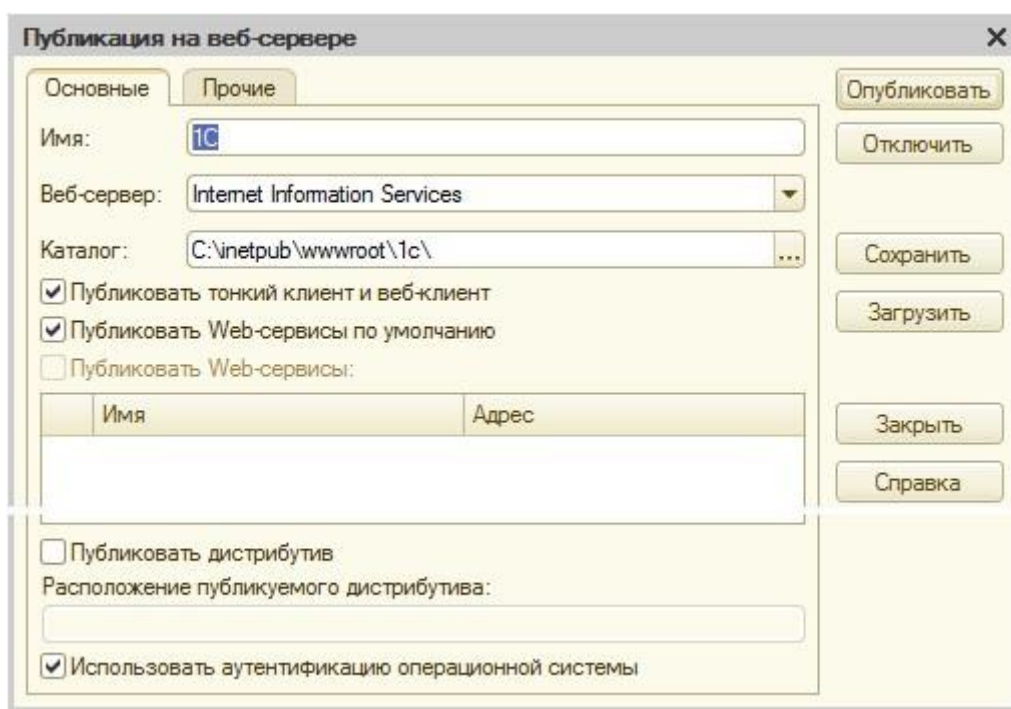


Рисунок 20 – Публикация на web-сервере

Содержимое (Рисунок 21).

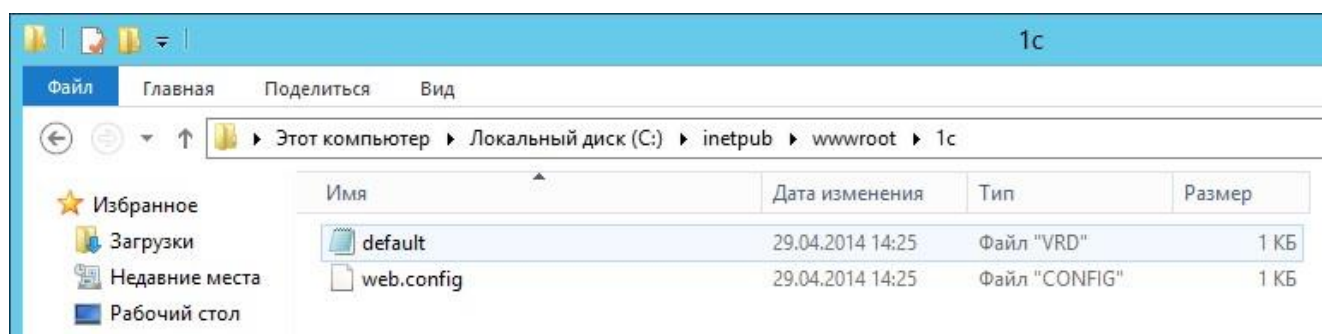


Рисунок 21 – Содержимое

4. Задать права для обработчика web-сервисов 1С (Рисунок 22).

Права на запуск (Выполнение) модулей добавляются для группы IIS_IUSRS на папку C:\Program Files (x86)\1cv8\8.3.4.465\bin.

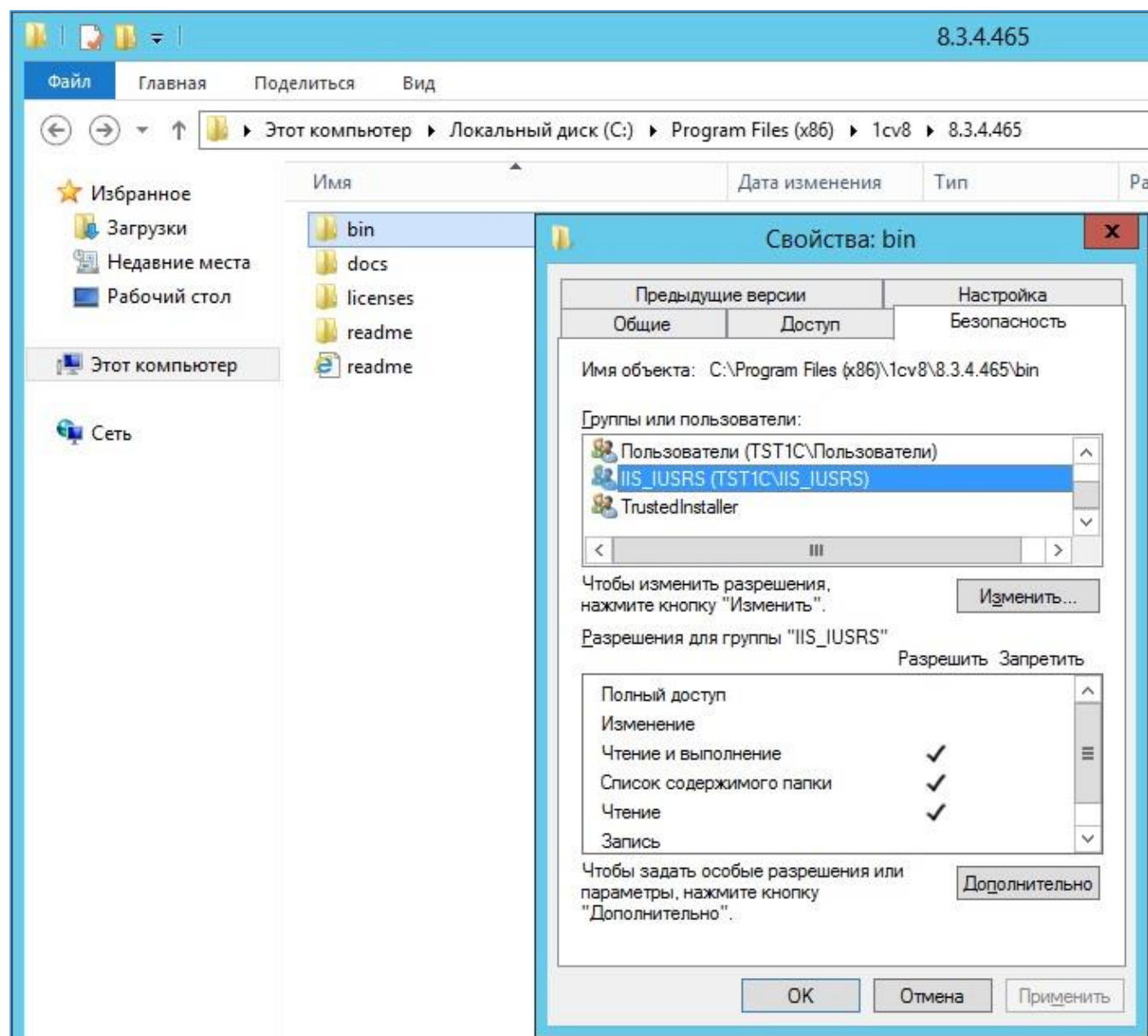


Рисунок 22 – Задание прав для обработчика

5. Если база файловая, то нужно добавить права на изменение (Изменение) на папку и подпапки базы для той же группы.

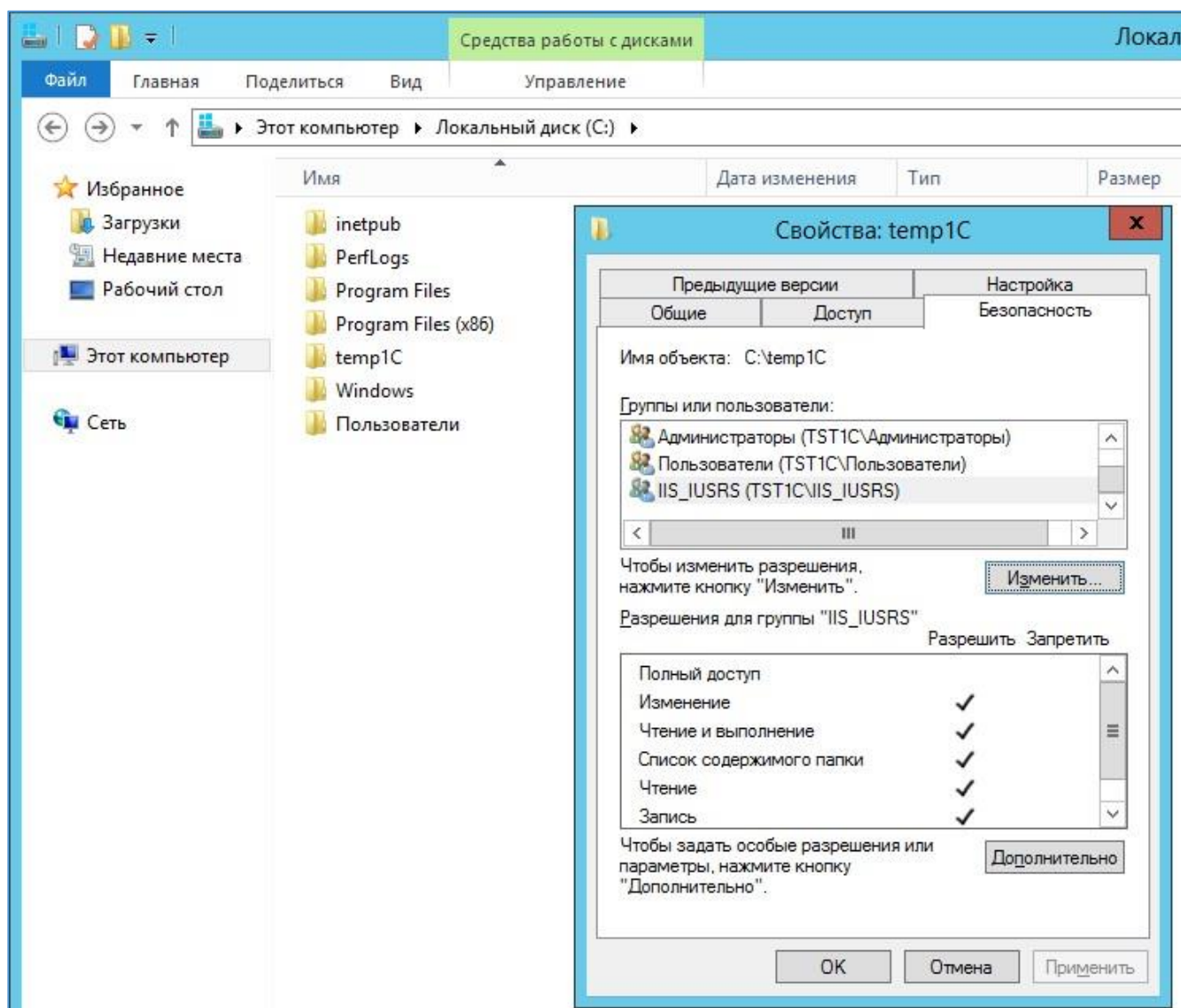


Рисунок 23 – Права на изменение

6. Зайти в консоль IIS.
7. Нажать правой кнопкой мыши на строку с созданной ранее папкой (Рисунок 24).

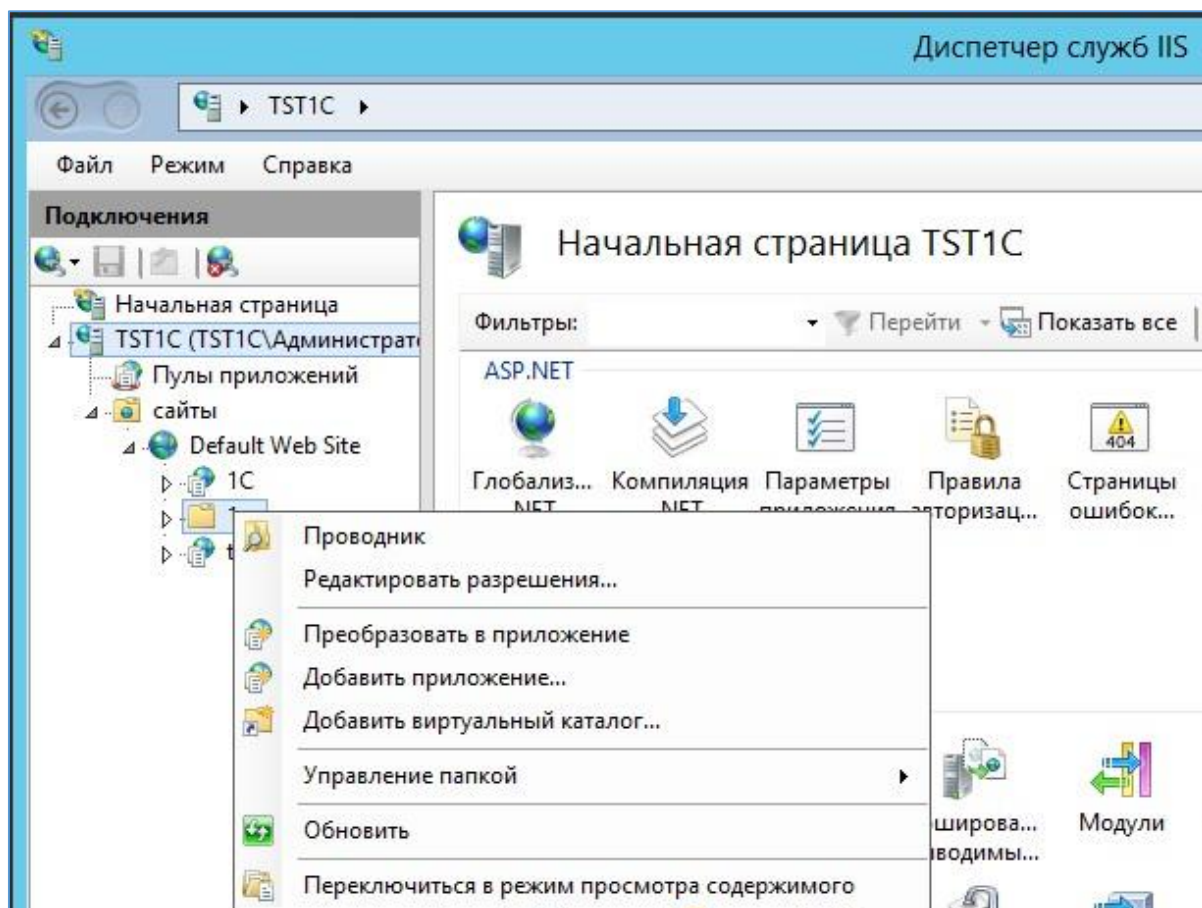


Рисунок 24 – Выбор ранее созданной папки

8. Преобразовывать её в приложение.

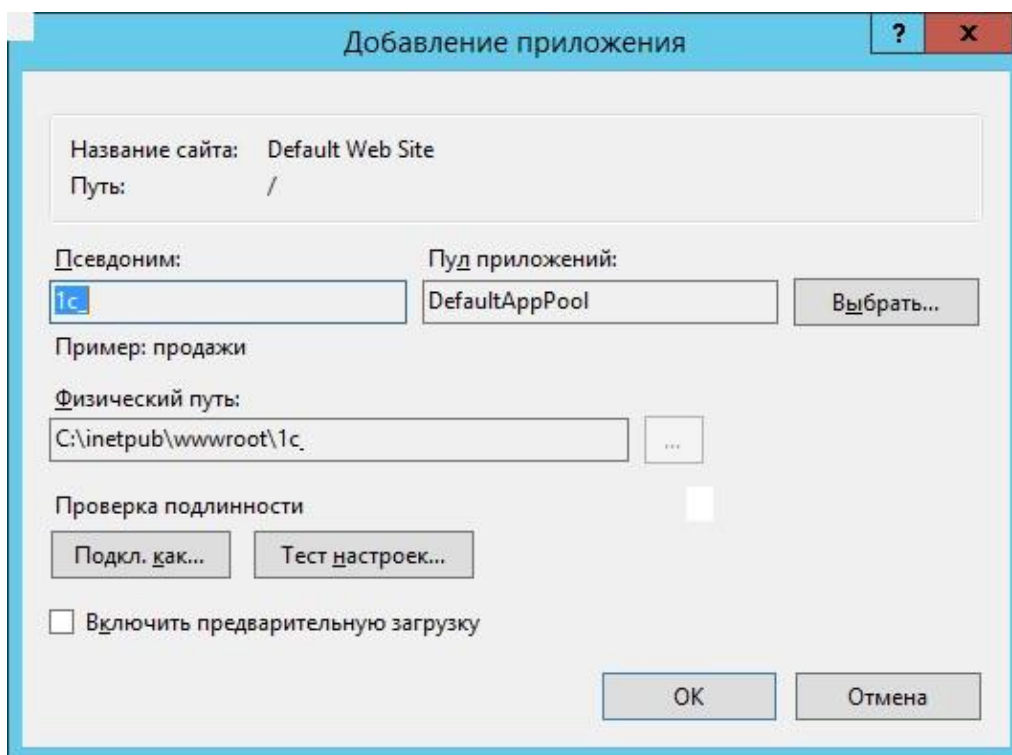


Рисунок 25 – Преобразование папки в приложение

9. Добавить MIME типы 1C.

Делать это можно для сервера или для сайта, или для папки. Наследование присутствует.

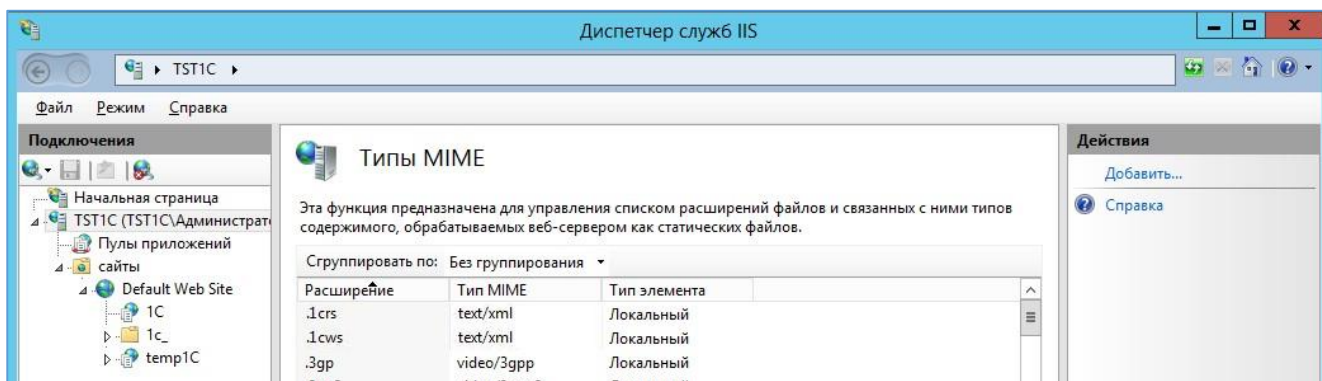


Рисунок 26 – Добавление MIME

10. Добавить настройки для обработки файлов 1C.

На вкладке «Сопоставление обработчиков» добавляем скрипты (не скрипты со звездочкой) для каждого расширения - "*.1cws" и "*.1crs".

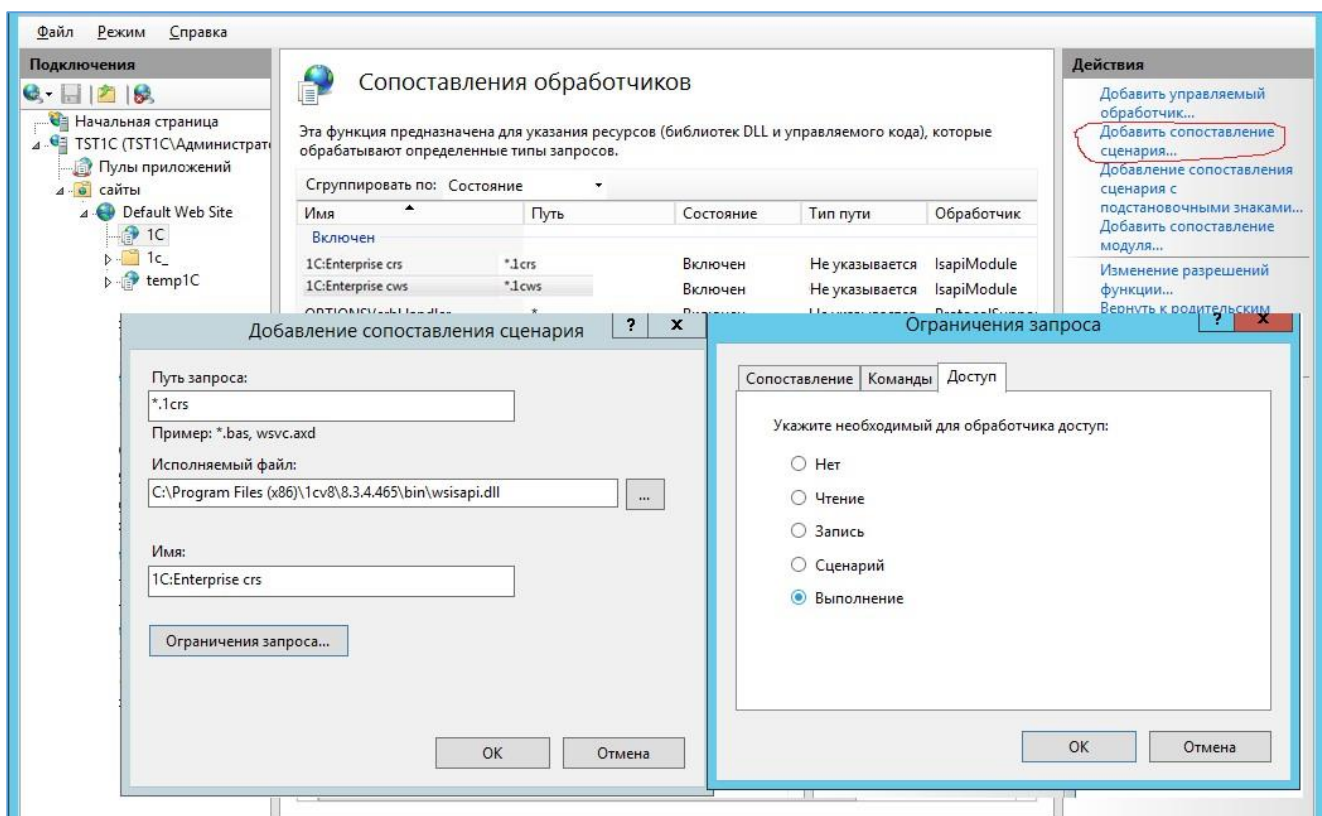


Рисунок 27 – Добавление настроек для обработки файлов 1C

Имена могут быть любые.

Главное – для каждого расширения отдельное правило!

Ограничения запроса -> Доступ -> Сценарий или Выполнение.

11. Для обработчиков нужно задать дополнительные параметры (Edit Feature Permission).

12. Установить флаги запуска скриптов и приложений.

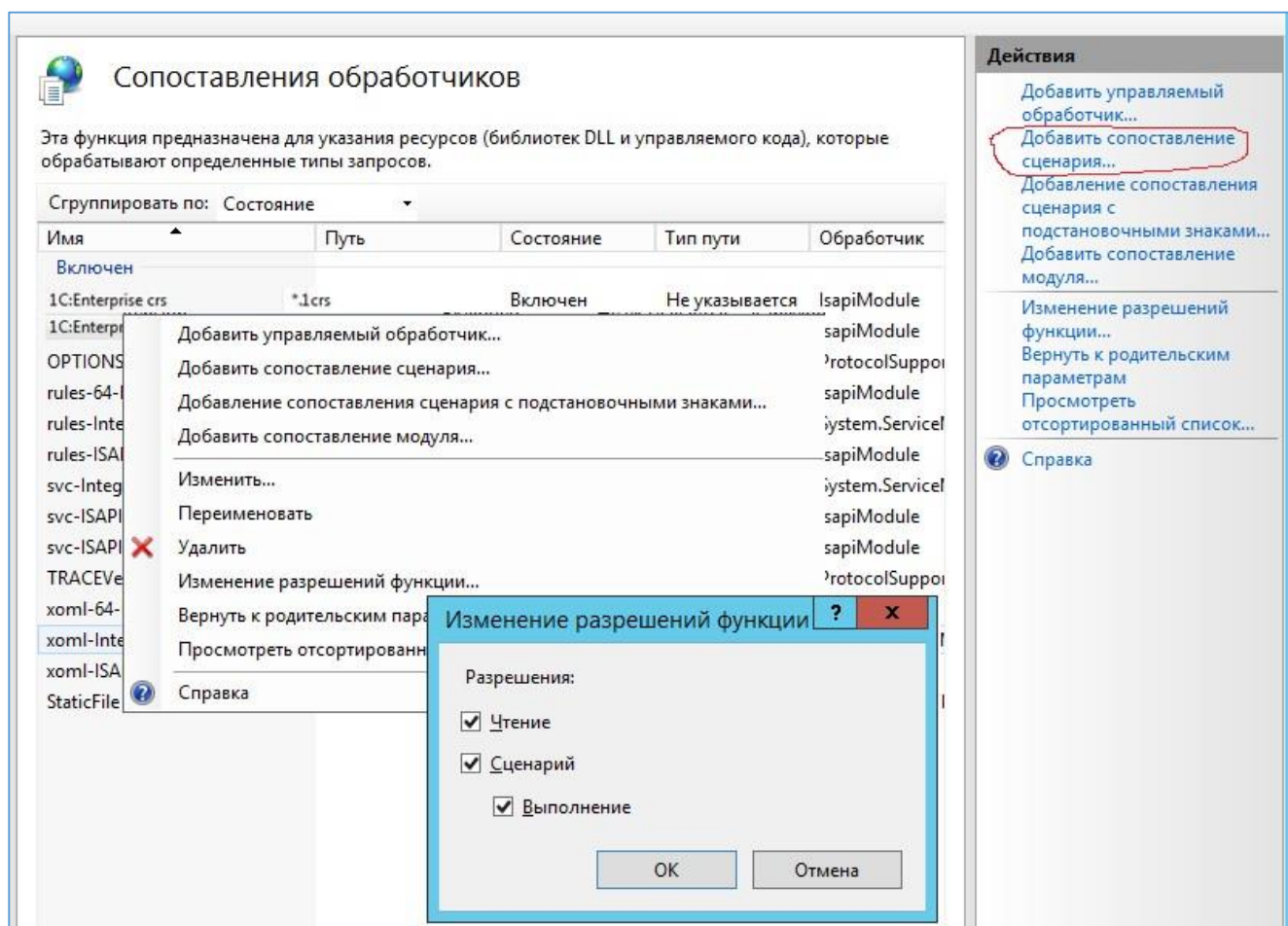


Рисунок 28 – Установить флаги скриптов и приложений

13. Можно проверить наличие обработчика web-сервисов 1C на вкладке ISAPI and CGI Restrictions для сервера.

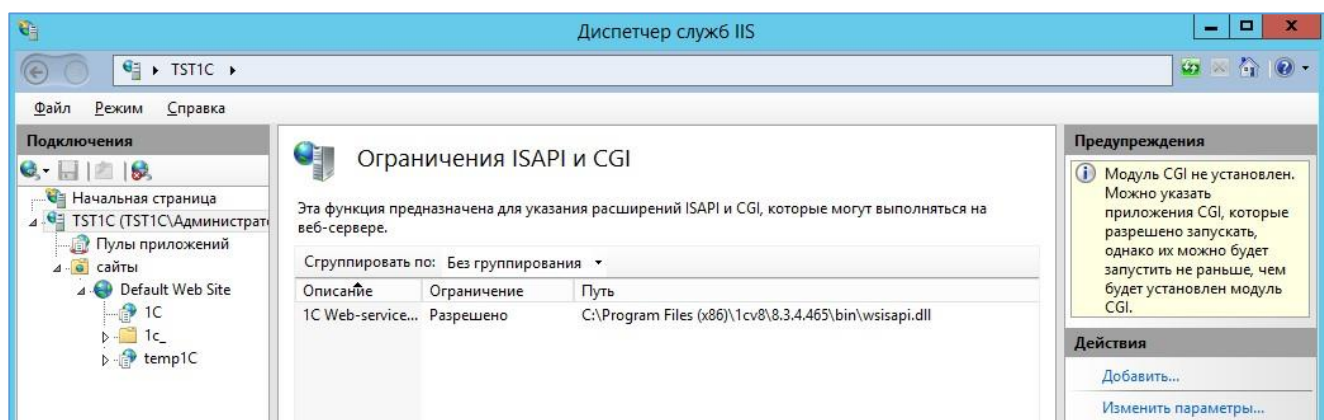


Рисунок 29 – Проверка наличия обработчика

Так как установка идёт в 64 разрядном окружении, то для обработчика нужно включить следующий режим:

Пулы приложений -> DefaultAppPool -> Дополнительные параметры -> Разрешены 32-разрядные приложения -> True.

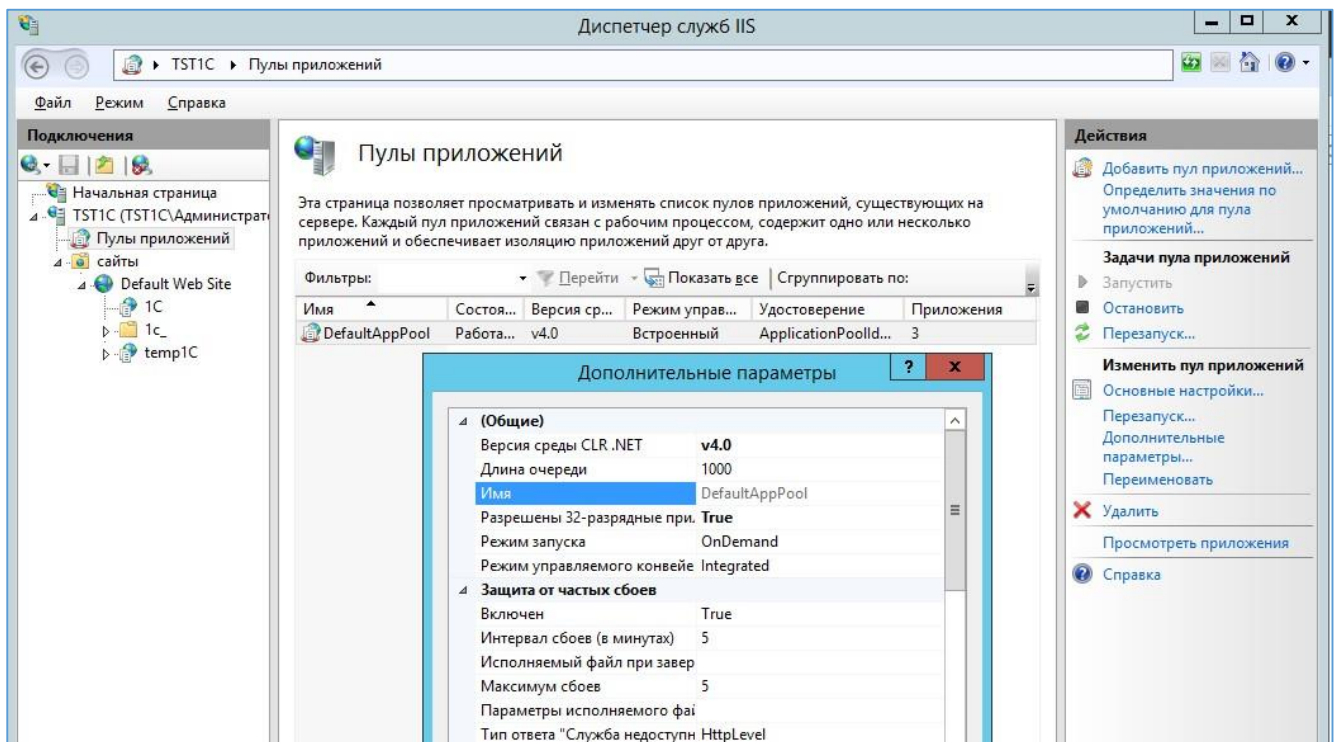


Рисунок 30 – Изменение режима для обработчика

14. Затем обратиться по адресу <http://localhost/1C/>.

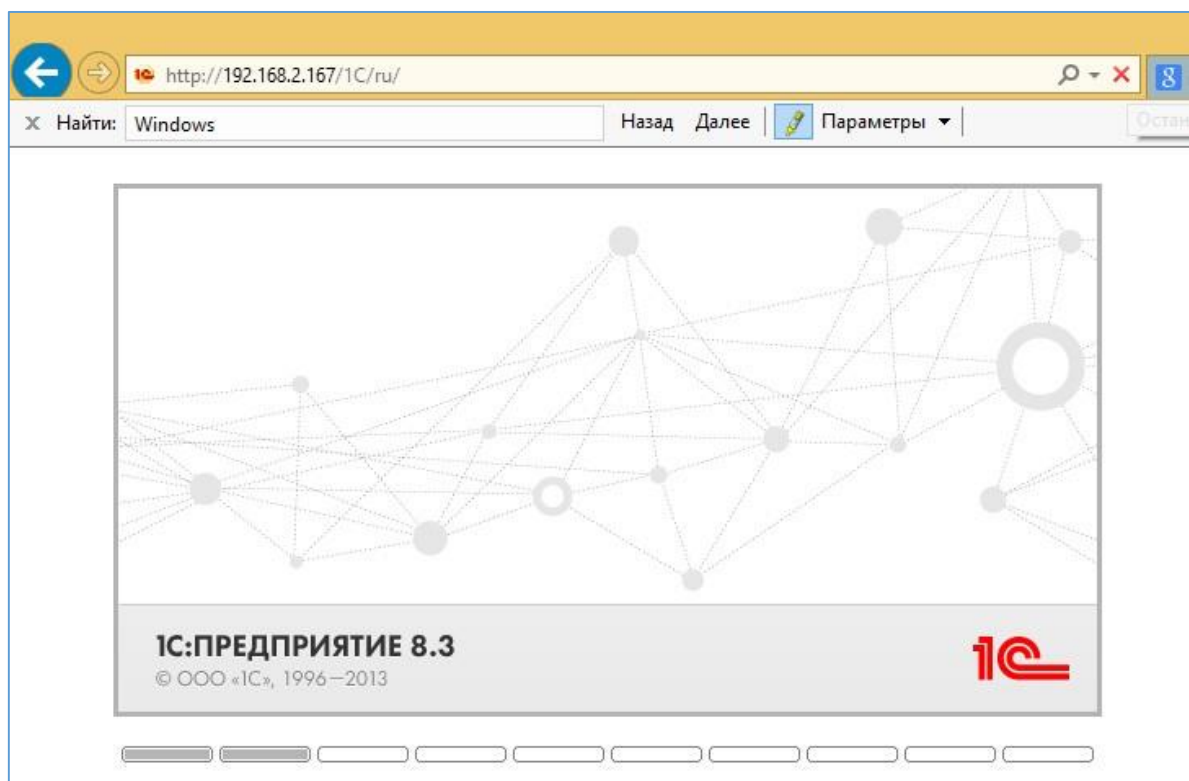


Рисунок 31 – Обращение по адресу

В случае анонимной аутентификации на IIS и доступе к базе следует:

15. Настроить доступ с использованием автоматически создаваемого пользователя IUSR.

16. Важно проверить, что Анонимная проверка подлинности включена как в корне сервера, ТАК И НА САЙТЕ. (Иначе не будет работать работает!)

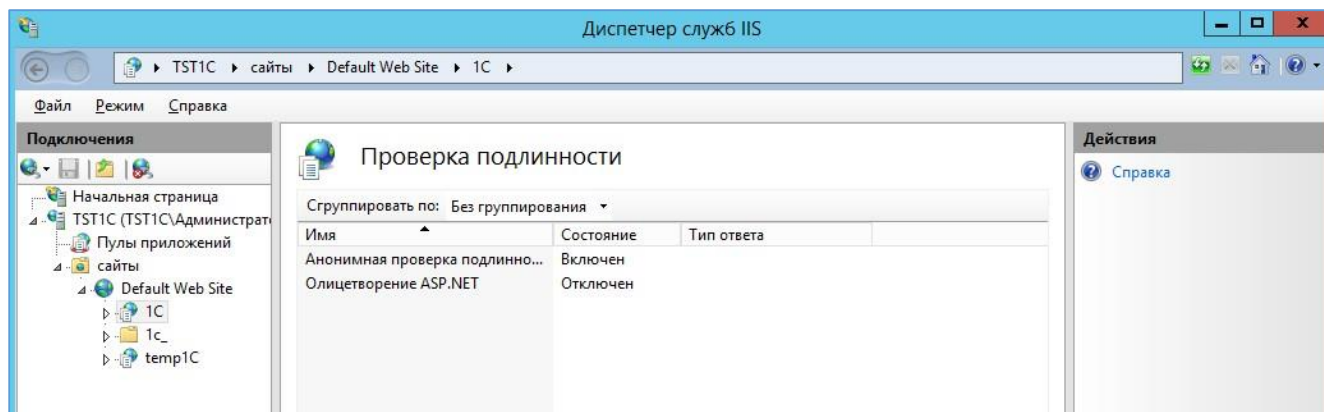


Рисунок 32 – Настройка доступа при аномальной аутентификации

4 Эксплуатация, техническое обслуживание, ремонт и хранение компонентов системы

Специального регламентного обслуживания Системы не требует.

Контроль над используемым дисковым пространством БД осуществляется штатными средствами администрирования Linux, таким как logrotate.

Logrotate - приложение, разработанное для облегчения управления лог-файлами. ... Утилита позволяет в автоматическом режиме архивировать, удалять, очищать и отправлять на e-mail лог-файлы. Этот процесс обычно называется ротацией лог файлов. Logrotate может быть настроен на ежедневную, еженедельную или ежемесячную ротацию.

Контроль над приложением осуществляется штатными средствами администрирования Windows.

Контроль за изменением БД осуществляет администратор базы данных с помощью системы мониторинга Zabbix, используя следующие плагины:

- pgbadger (позволяет осуществлять аналитику по БД);
- mamonsu (позволяет осуществлять мониторинг БД);
- rowa (позволяет собирать статистику и строить по ней аналитику).

Zabbix – свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

5 Действия при возникновении ошибок и неполадок

В случае возникновения любой критической ошибки, при использовании системы, требуется:

- ввести систему в аварийный режим;
- связаться с разработчиком.

Критической ошибкой в Системе является любая невозможность использования основного функционала.