**8. ПЕРЕДАЧА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛОВ HTTP И FTP**

Веб-сервер представляет собой некоторую программу (службу), принимающую HTTP-запросы от клиентов, обычно от веб-браузеров, обрабатывающую данные запросы и выдающую им ответ, как правило, вместе с HTLM-страницей (сайтом), изображением, файлом, медиа-потоком или другими данными.

Если управление сетью осуществляется на основе Windows Server, то логично будет использовать веб-сервер IIS. Это весьма популярная платформа, которая позволяет работать как с большинством популярных CMS, так и имеет широкий спектр систем, предназначенных для работы именно на Windows и IIS.

Несомненным достоинством IIS является его тесная интеграция с другими технологиями и средствами разработки Microsoft. В частности веб-решения для IIS могут использовать богатые возможности .NET и легко взаимодействовать с настольными приложениями на этой платформе. К тому же для IIS имеется богатый выбор готовых CMS.

Однако далее в рамках курса «Компьютерные сети» мы прежде всего будет уделять внимание не созданию «мощных» и удобных веб-ресурсов, а базовым элементам, а именно настройке и работе по HTTP и FTP протоколам, которые в полной мере поддерживаются IIS-сервером.

**8.1. Установка IIS-сервера**

По своей сути установка IIS идентична установки DHCP или DNS серверов, т.е. ее удобно выполнять, используя мастер настройки сервера, а именно через добавление ролей (рис. 8.1). Необходимо отметить, что если стоит задача сразу установить HTTP и FTP составляющие IIS-сервера, то после выбора роли *Web Server (IIS)* необходимо выбрать *Add Features (Добавить компоненты)* и в появившемся окне галочками отметить, что необходимо инсталлировать (например, *FTP Server* и *Management Tools*) (рис. 8.2).

Далее необходимо будет отвечать утвердительно на всех последующих диалоговых окнах, т.е. выбирая *Next (Далее)*. После завершения установки в консоли *Server Manager* отдельно появится сервер *IIS* (рис. 8.3).

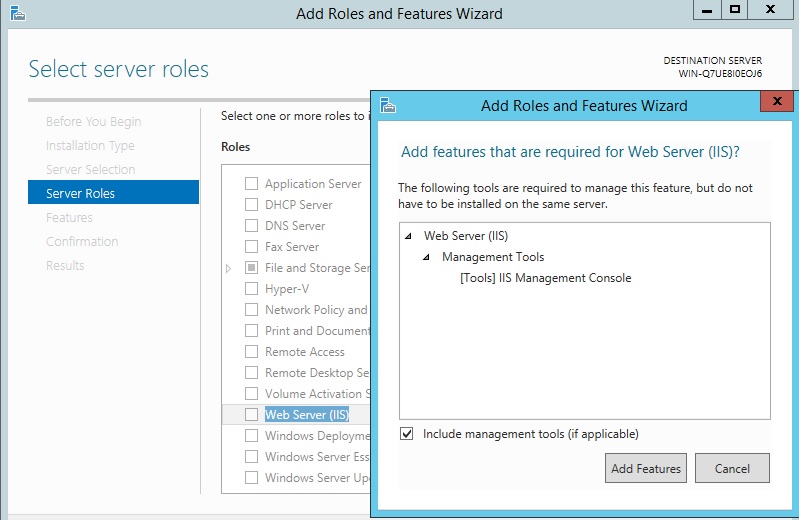


Рис. 8.1. Выбор устанавливаемой роли *Web Server (IIS)*

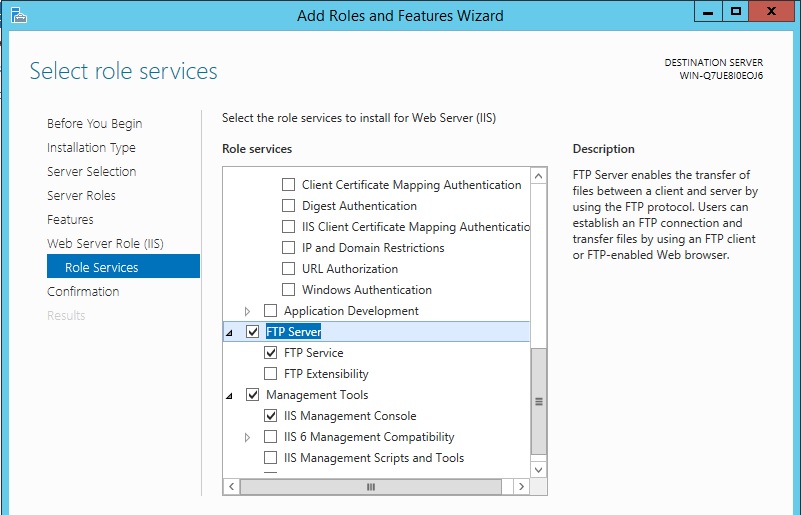


Рис. 8.2. Выбор компонент при установке роли *Web Server (IIS)*

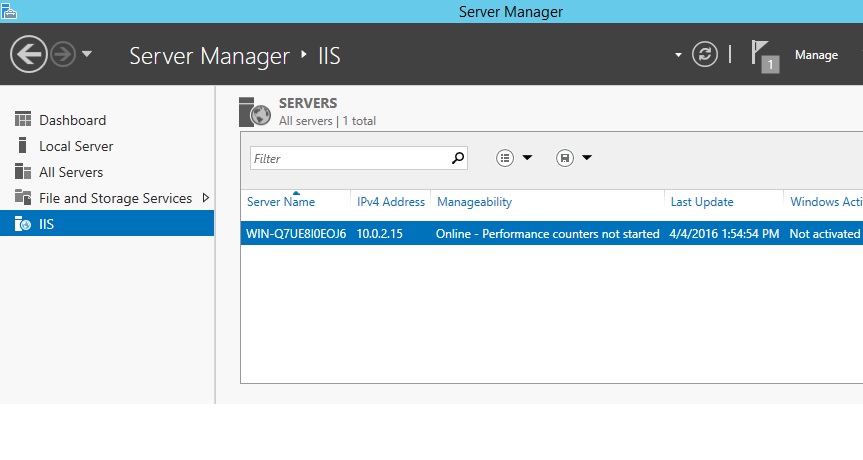
**

Рис. 8.3. Консоль *Server manager* c установленным *IIS*

Далее можно переходить к настройке HTTP или FTP составляющих сервера.

**8.2. Настройка и передача данных по протоколу HTTP. Web-узлы и виртуальные каталоги**

***8.2.1. Настройка web-узлов***

Для настройки HTTP или FTP составляющих сервера необходимо выбрать через контекстное меню *Internet Information Services (IIS) Manager*, или перейдя в него через *Server Manager / Tools / Internet Information Services (IIS) Manager* (рис. 8.4).

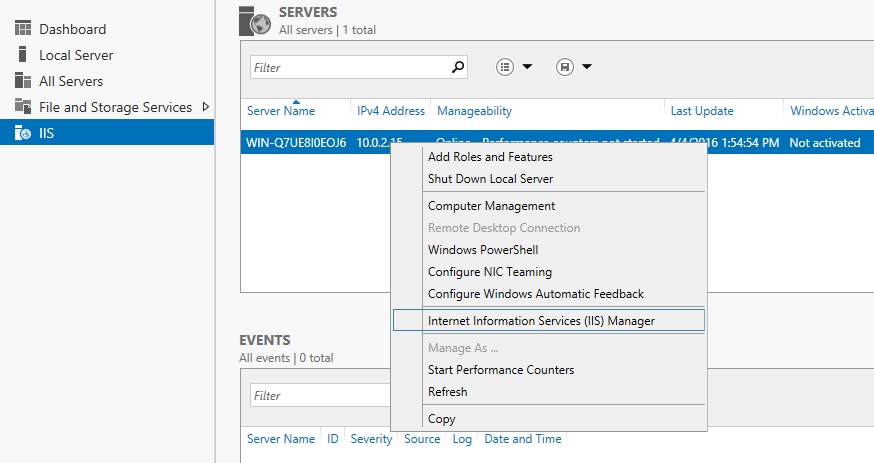


Рис. 8.4. Переход в консоль управления IIS-сервера

(*Internet Information Services (IIS) Manager*)

В первоначальном виде консоль управления IIS-сервера выглядит, как показано на рис. 8.5.

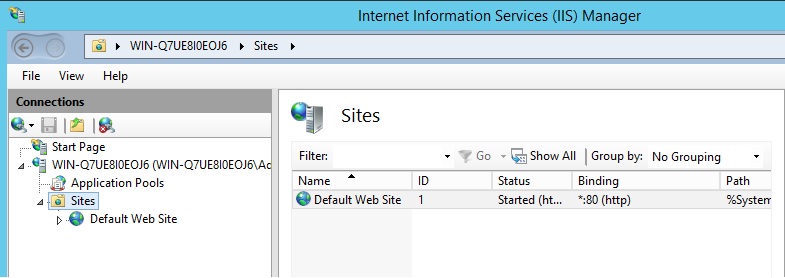


Рис. 8.5. Первоначальный вид консоли управления IIS-сервера

(*Internet Information Services (IIS) Manager*)

Прежде чем далее приступать к настрой web и ftp узлов, рекомендуется создать некоторое количество альтернативных IP-адресов, которые логически связаны с основным IP-адресов (в примере он равен 192.168.1.100/24). В качестве дополнительных (альтернативных) адресов в дальнейших примерах будут использоваться 192.168.1.120/24, 192.168.1.121/24, 192.168.1.122/24, 192.168.1.123/24 и 192.168.1.124/24 (рис. 8.6). Именно они будут присваиваться отдельным web и ftp узлам.

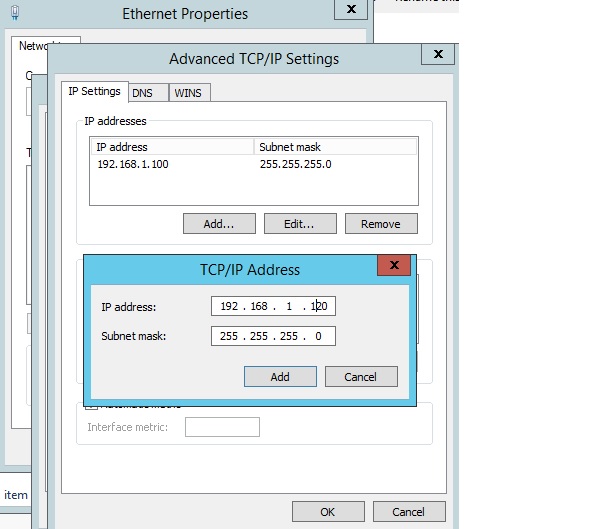


Рис. 8.6. Ввод дополнительных IP-адресов

Теперь можно непосредственно приступать к настройке, например web-узла. На каком-либо диске, например *С*, создадим папку *iis\_http*, которая будет являться домашним каталогом для создаваемого web-узла *my\_site* (рис. 8.7) и разместим там файл с именем index.html (фактически это web-страница, которая будет отображаться в браузере при обращении пользователя к web-узлу).

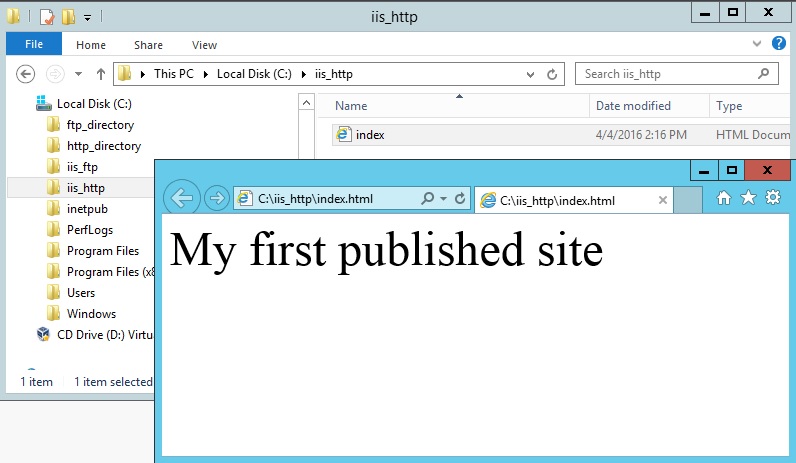


Рис. 8.7. Домашний каталог для web-узла

Далее перейдем непосредственно к созданию и настройке web-узла. Для этого в консоли управления сервером *IIS* вызываем контекстное меню для *Sites* и выбираем *Add Website… (Добавить Web-сайт…)*, как паказано на рисунке 8.8.

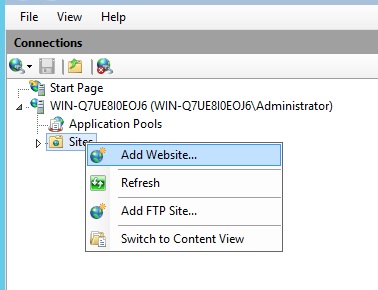


Рис. 8.8. Старт процедуры добавления нового web-узла

Далее в появившемся окне необходимо задать имя web-узла, а также физический путь к его домашней директории (каталогу) (рис. 8.9). Также необходимо выбрать IP-адрес web-узла (один из созданных дополнительных IP-адресов) (рис. 8.10).

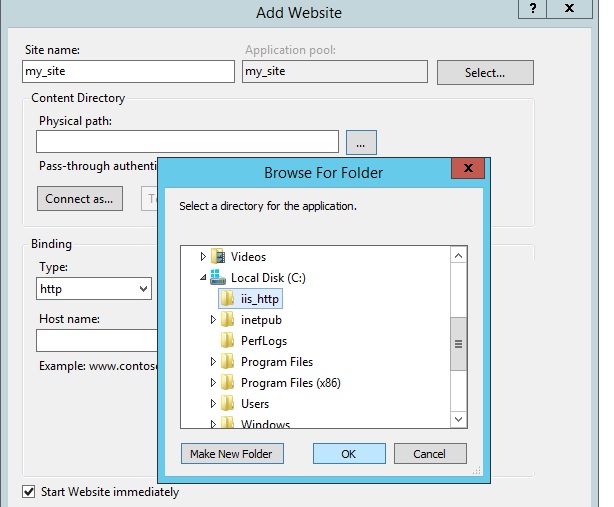


Рис. 8.9. Выбор имени web-узла и домашнего каталога

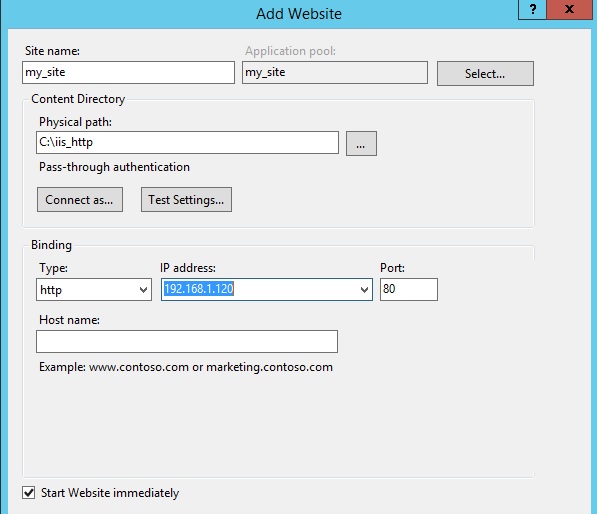


Рис. 8.10. Выбор IP-адреса web-узла

Далее необходимо будет отвечать утвердительно на всех последующих диалоговых окнах, т.е. выбирая *Next (Далее)*. После завершения установки в консоли *IIS* в категории сайтов появится созданный web-узел с именем *my\_site* (рис. 8.11). Проверить работу web-узла можно, написав в строке браузера соответствующий IP-адрес (рис. 8.12) (можно также добавить соответствующую запись в DNS-сервер, чтобы вызывать сайт по символьному имени).

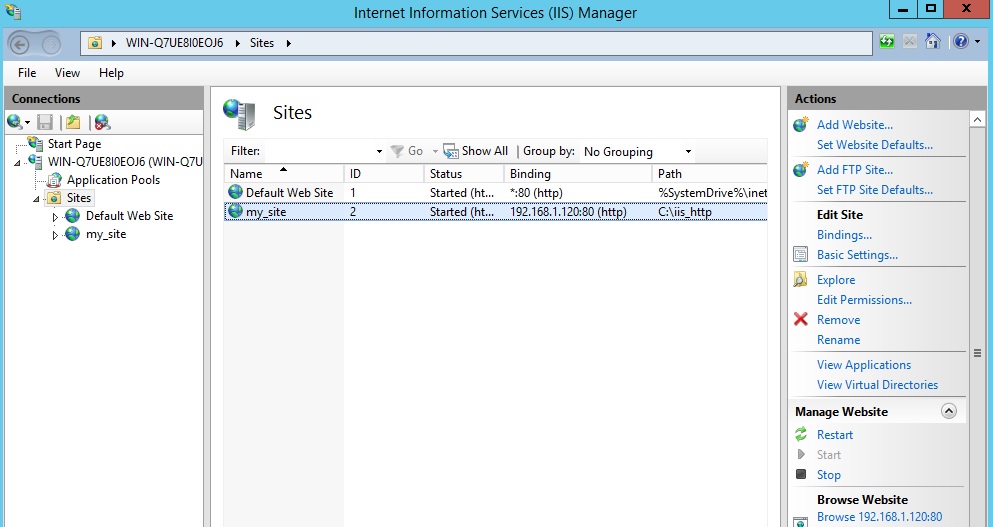


Рис. 8.11. Консоль *IIS*-сервера с созданным web-узлом *my\_site*

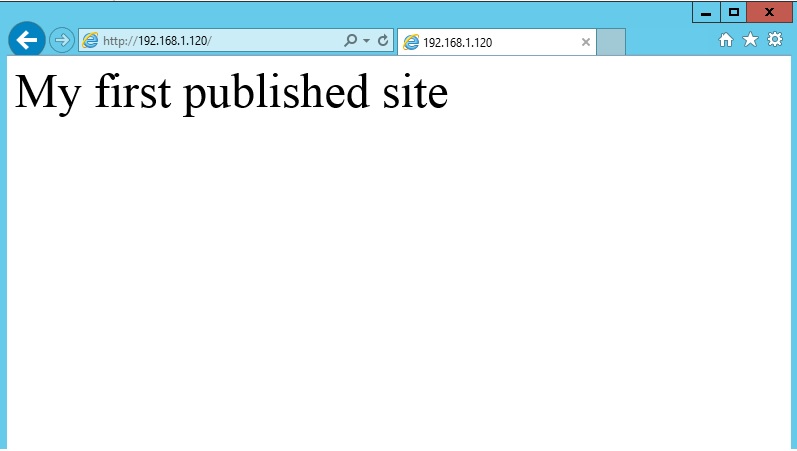


Рис. 8.12. Просмотр сайта с помощью браузера

***8.2.2. Настройка виртуальных каталогов***

Виртуальный каталог — это понятное имя или псевдоним либо для физического каталога на жестком диске сервера, расположенного вне области основного каталога, либо для основного каталога на другом компьютере. Поскольку псевдоним обычно бывает короче, чем запись пути к физическому каталогу, он более удобен для ввода пользователем. Кроме того, использование псевдонимов повышает безопасность, так как не дает пользователям сведений о физическом местоположении файлов на сервере и тем самым исключает возможность изменения этих файлов пользователями. Псевдонимы упрощают также перемещение каталогов на узле. Вместо того чтобы изменять URL-адрес для каталога, достаточно изменить сопоставление псевдонима и физического адреса каталога.

Если на веб-узле имеются файлы, размещенные вне основного каталога или на других компьютерах, то для добавления этих файлов на веб-узел следует создать виртуальный каталог. Данный метод можно применять также, например, для опубликования данных из каких-либо каталогов, размещенных вне основного каталога.

Виртуальные каталоги для web-узла бывают двух типов: локальные и сетевые. *Локальный виртуальный каталог* физически расположен на той же виртуальной машине (операционной системе), что непосредственно web-сервер, обеспечивающий работу web-узла. *Сетевой виртуальный каталог* физически расположен на любом сетевом компьютере, но не на компьютере с web-сервером. При этом правила доступа к каталогам обоих типов для пользователей одинаковы – в строке браузера необходимо ввести [*http://адрес*](http://адрес) *web-узла/имя виртуального* каталога.

Для создания виртуального каталога необходимо перейти в консоль управления IIS-сервером (*Internet Information Services (IIS) Manager*) и в контекстном меня для web-узла выбрать *View Virtual Directories (Посмотреть виртуальные каталоги)* (рис. 8.13), тем самым мы перейдем в окно с имеющимися виртуальными каталогами для выбранного web-узла (в примере на рис. 8.14 виртуальные каталоги пока не создавались). Далее также через контекстное меню, вызываемое нажатием правой кнопки мыши, выбираем команду Add Virtual Directory (Добавить виртуальный каталог) (рис. 8.15), чтобы запустить мастер создания и настройки виртуальных каталогов, который представлен на рис. 8.16. В процессе создания (рис. 8.15) необходимо ввести имя каталога, под которым его будет видеть пользователь (имя виртуального каталога может не совпадать с физическим именем каталога), а также путь к нему. Для виртуального локального каталога вводится локальный путь, например, *С:\http\_virtual\local* (показано на рис. 8.16), а в случае настройки сетевого виртуального каталога – сетевой путь [*\\имя*](file:///\\имя) *компьютера\имя сетевой папки*, например [*\\192.168.1.200\net*](file:///\\192.168.1.200\net), где 192.168.1.200 – IP-адрес компьютера, где физически расположен каталог, net – сетевое имя открытой для доступа по сети папки на компьютере с IP-адресом компьютера 192.168.1.200. Соответственно для данной папки должен предварительно открыт доступ по сети с установкой соответствующих прав для выбранного пользователя. В процессе настройки виртуального каталога необходимо будет ввести имя данного пользователя и его пароль (возможно потребуется создание пользователя с совпадающим именем и паролем на компьютере с web-сервером, т.к. клиент, обращаясь к виртуальному каталогу, будет в него заходить фактически с правами данного пользователя).

Проверка работы виртуального каталога осуществляется, как показано на рис. 8.17 (виртуальный каталог с именем *local\_directory* ассоциирован с web-узлом с адресом 192.168.1.120).

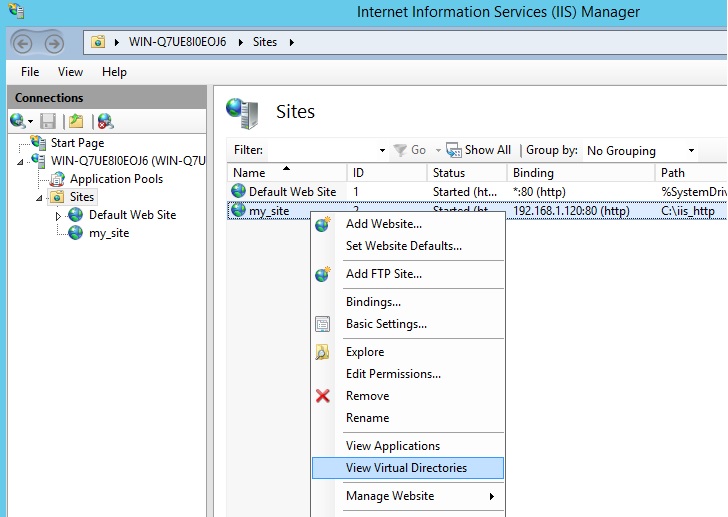


Рис. 8.13. Переход в окно с виртуальными каталогами web-узла

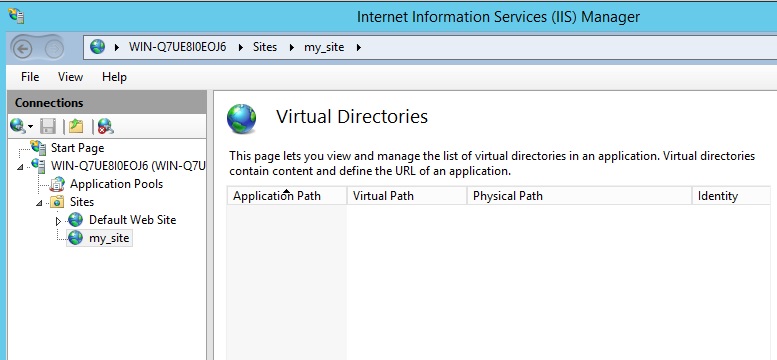


Рис. 8.14. Окно с виртуальными каталогами web-узла

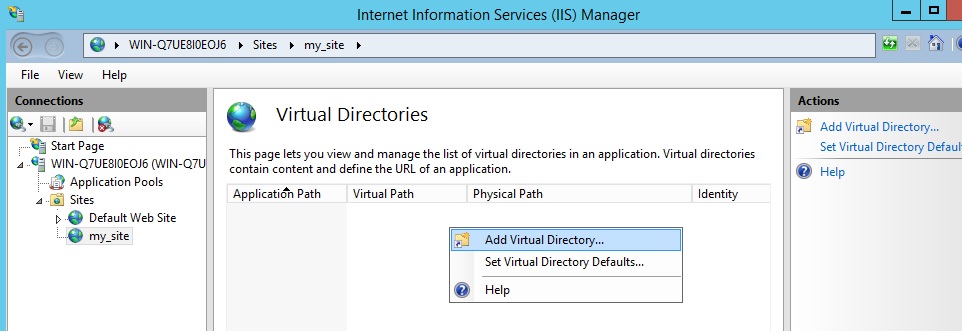


Рис. 8.15. Запуск мастера для создания виртуального каталога web-узла

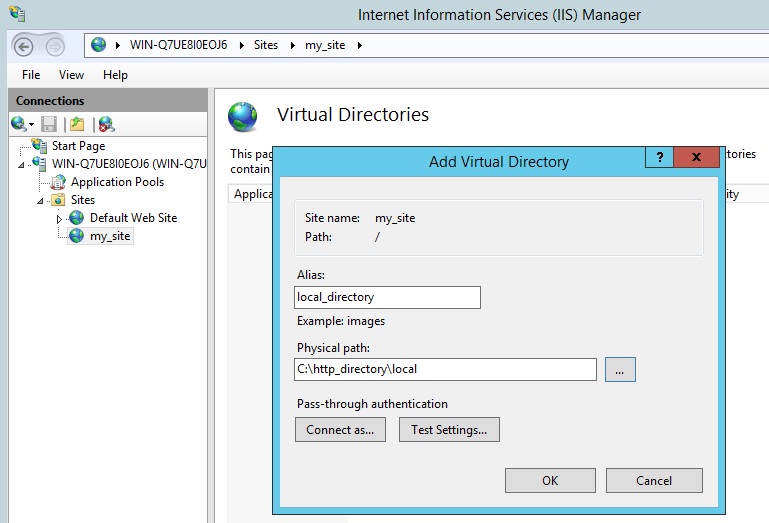


Рис. 8.16. Процесс создания виртуального каталога web-узла

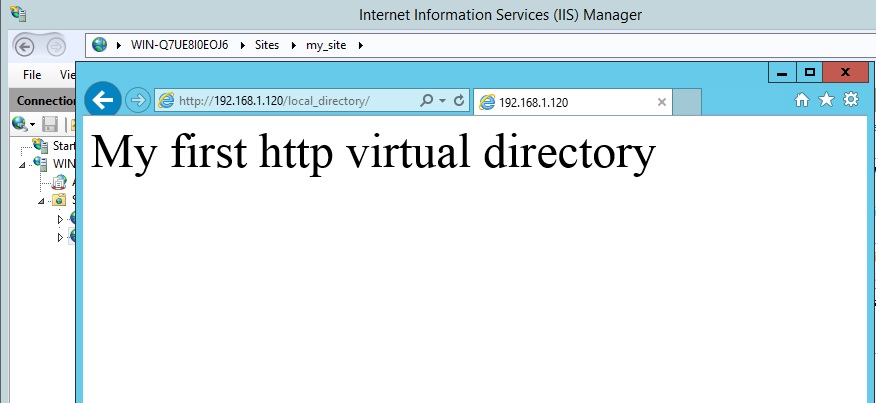


Рис. 8.17. Проверка работы виртуального каталога web-узла

***8.2.3. Лабораторная работа №15***

**Цель:** Изучение методов настройки IIS-сервера для передачи данных по протоколу http.

**Задание:** Лабораторная работа заключается в настройке следующих элементов.

1. Web-узла с анонимным доступом, тем самым должен быть опубликован web-сайт, разработанный студентом.
2. Виртуального локального каталога для созданного web-узла с анонимным доступом).
3. Виртуального сетевого каталога для созданного web-узла с анонимным доступом).

Доступ к web-ресурсам (сайт, каталоги) необходимо демонстрировать с помощью браузера любого компьютера в сети (например, второй виртуальной машины).

**8.3. Настройка и передача данных по протоколу FTP**

Если протокол http прежде всего используется для доступа к web-ресурсам в виде отдельных web-страниц, то FTP предназначен для организации хранения и передачи различных типов файлов (графических, тестовых, мультимедийных и т.д.). На базе данного протокола как правило организуются файловые хранилища.

Web-сервер IIS позволяет организовывать и настраивать FTP-узлы трех типов:

* с гостевым (анонимным) доступом;
* с авторизированным доступом;
* с изоляцией пользователей.

Далее рассмотрим процесс создания и использования каждого типа узла отдельно.

Отметим, что служба FTP, как часть веб сервера IIS, уже была установлено совместно с HTTP составляющей, как показано в подразделе 8.2.

***8.3.1. Создание FTP-узла с гостевым (анонимным) и авторизированным доступом***

Для запуска мастера настройки ftp необходимо в консоли управления сервером IIS вызвать контекстное меню (для веб-сервера IIS) и выполнить команду Add FTP Site… (Добавить FTP-сайт), как показано на рис. 8.18.

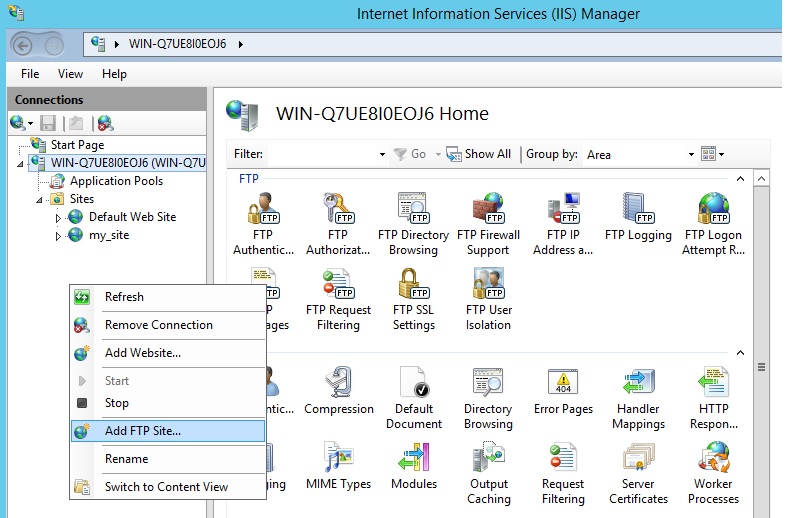


Рис. 8.18. Вызов мастера настройки службы FTP

Далее необходимо по аналогии с настройкой web-узла заполнить с ходе диалога с «мастером» заполнить соответствующие поля: выбрать имя ftp-узла и путь к его домашней директории (рис. 8.19 и 8.20); выбрать IP-адрес узла из доступных в выпадающем списке и способ шифрования передаваемых данных (на рис. 8.21 выбран вариант без SSL); способ аутентификации пользователя (рис. 8.22 – выбран вариант анонимной аутентификации, т.е. гостевой доступ). При необходимости можно также определить вариант доступа (полный, чтение) к ftp-узлу. Отметим, что такая настройка будет достаточно «грубой», поэтому целесообразно ее выполнять через управление доступом к домашней директории ftp-узла в файловой системе NTFS (как было показано в разделе 2.4).

После того, как все будет настроено, ftp-узел появится в консоли управления IIS-сервера, как показано на рис. 8.23. Подключиться же к ресурсам данного ftp-узла можно через браузер, введя в адресной строке соответствующий IP-адрес (рис. 8.24 и 8.25).

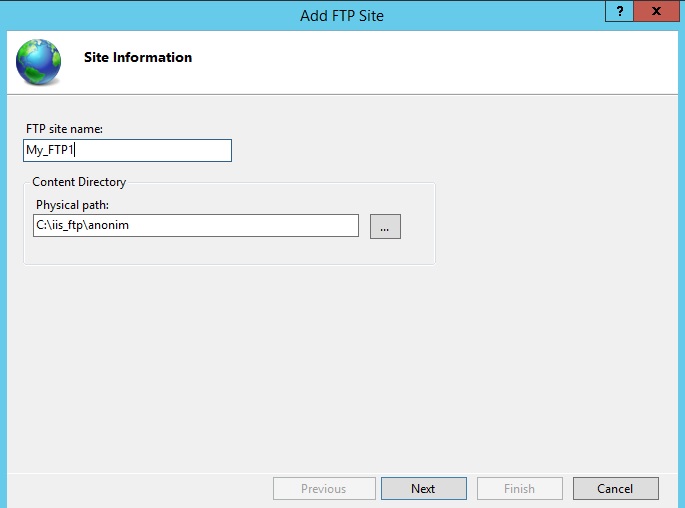


Рис. 8.19. Диалог для ввода имени и домашней директории ftp-узла

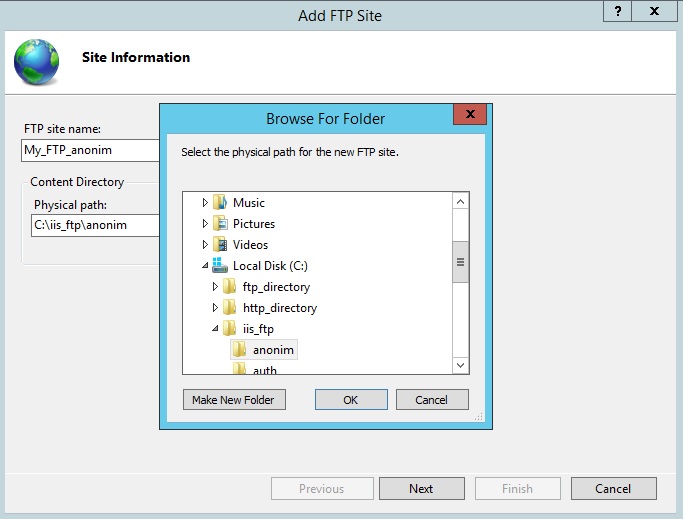


Рис. 8.20. Диалог для пути к домашней директории ftp-узла

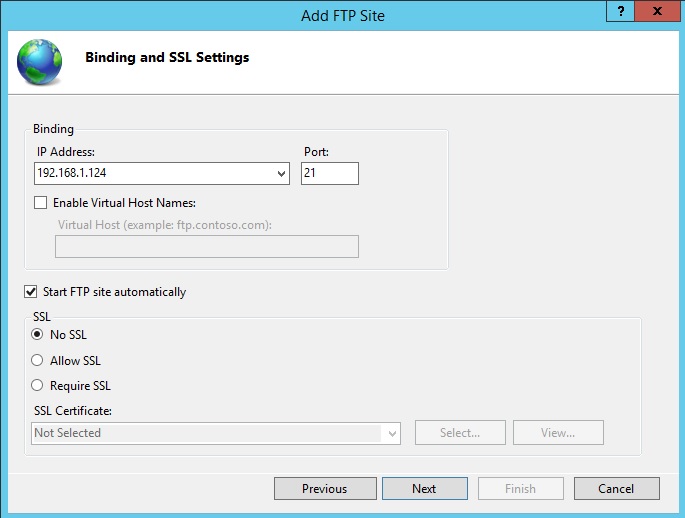


Рис. 8.21. Выбор IP-адреса ftp-узла

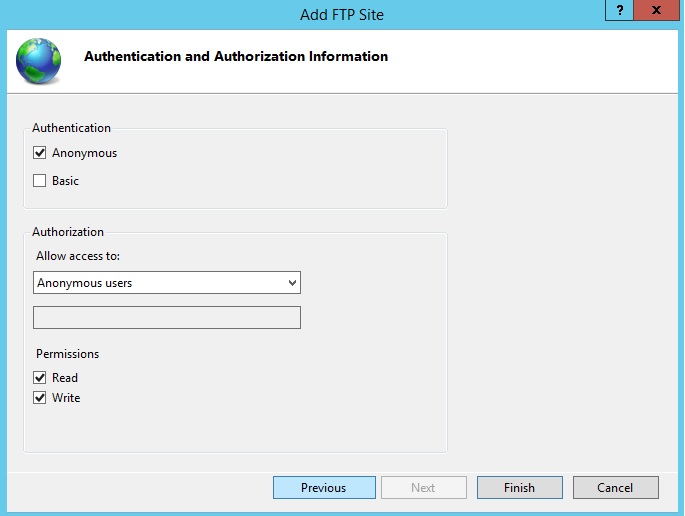


Рис. 8.22. Выбор способа аутентификации при подключении к ftp-узлу

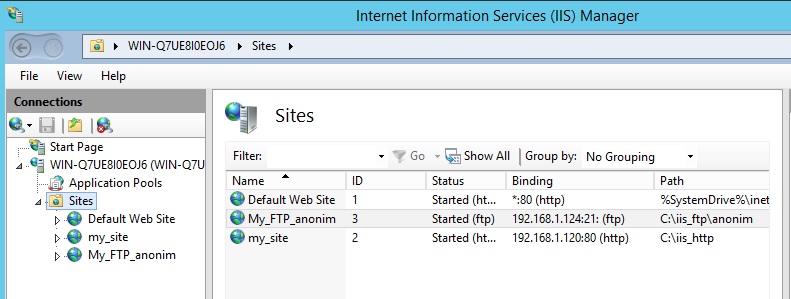


Рис. 8.23. Общий вид консоли управления IIS-сервером с настроенным ftp-узлом

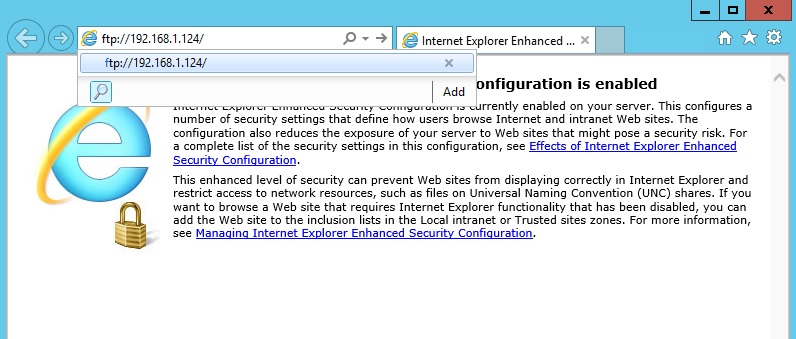


Рис. 8.24. Подключение к ftp-узлу через браузер

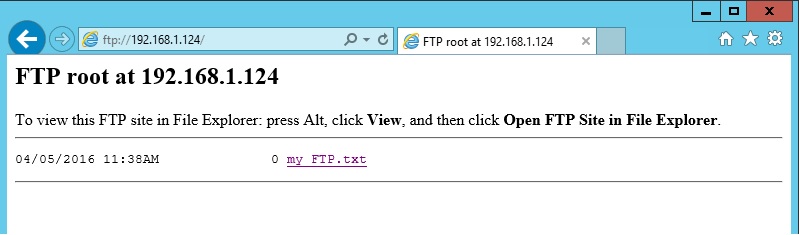


Рис. 8.25. Просмотр содержимого ftp-узла

Отметим, что именно «тонкая» настройка доступа к домашней директории может позволить создавать ftp-узлы с «интересным» функционалом, например «черный ящик». Подключения к такому ресурсу осуществляется под гостевой учетной записью (без запроса логина и пароля) таким образом, чтобы пользователь мог записывать файлы, но не видел содержимого «черного ящика». Т.е. для гостевой учетной записи IIS сервера должна применять настройка показанная на рис 8.26. При этом целесообразно оставить доступ к домашней директории только гостевой учетной записи IIS сервера и группе администраторов (рис. 8.27). Поэтому если осуществить подключение под логином пользователя, имеющего административные права (принадлежит группе *Администраторы*), то ему будет доступна вся информация, хранящаяся на данном ftp-узле, а также любые операции с ней (запись, удаление, изменение, просмотр и т.д.)

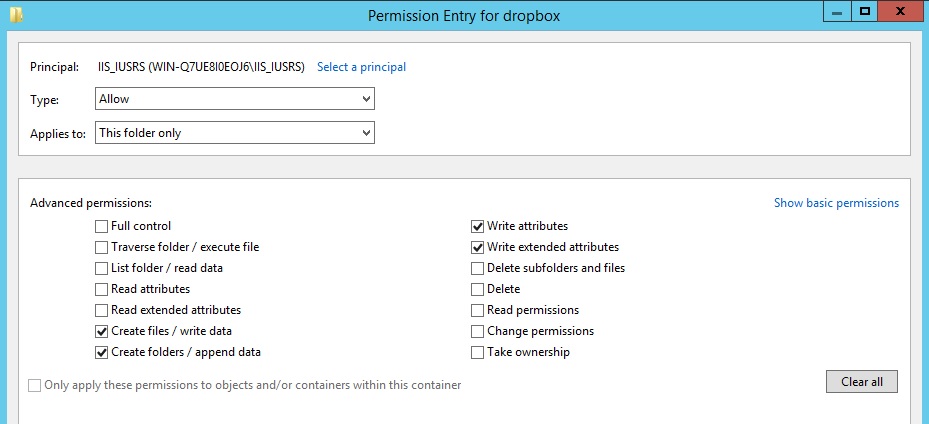


Рис. 8.26. Настройка доступа к домашней директории для ftp-узла типа «черный ящик» для гостевой учетной записи IIS-сервера

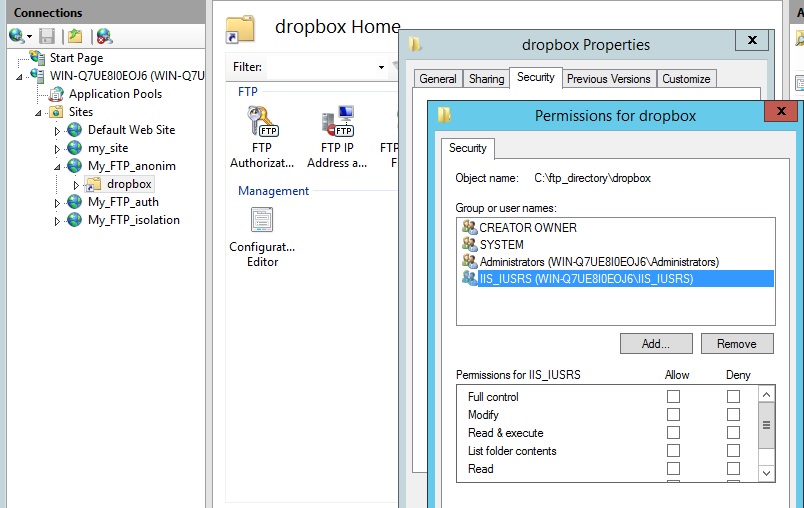


Рис. 8.27. «Тонкая» настройка доступа к домашней директории для ftp-узла типа «черный ящик»

Процесс создания ftp-узла с авторизированным доступом осуществляется аналогичным образом с той лишь разницей, что необходимо выбрать тип авторизации basic и указать пользователей, которым будет разрешен доступ (рис. 8.28). Данные пользователи должны быть предварительно созданы, как показано на рис. 8.29– 8.31, а также выполнена «тонкая» настройка доступа данным пользователям к домашнему каталогу через файловую систему NTFS. При доступе к ftp-узлу с авторизацией (например, через браузер) обязательно будет осуществлен запрос на ввод логина и пароля.

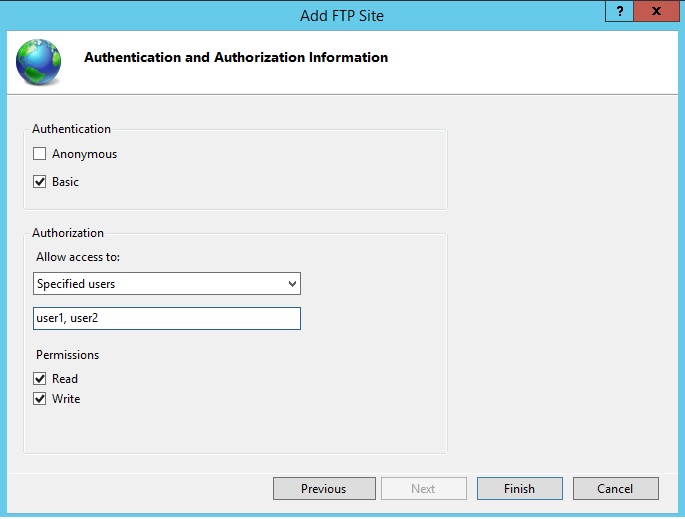


Рис. 8.26. Выбор способа аутентификации при подключении к ftp-узлу для пользователей user1 и user2

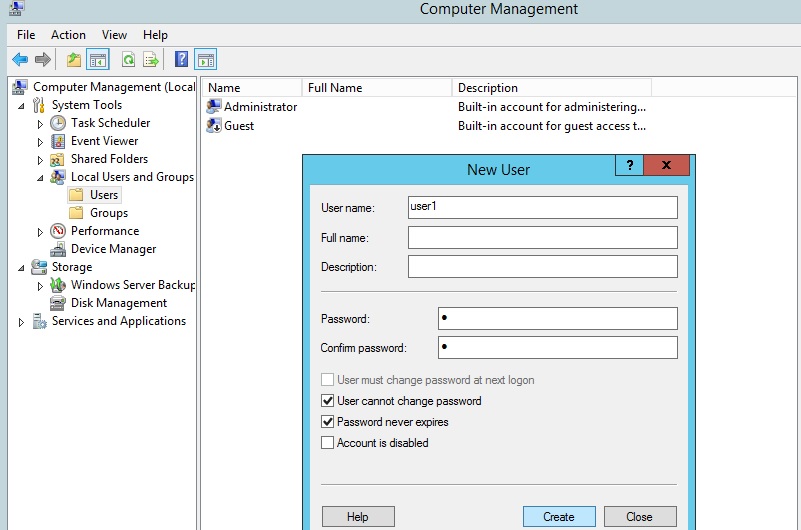


Рис. 8.27. Создание пользователя user1

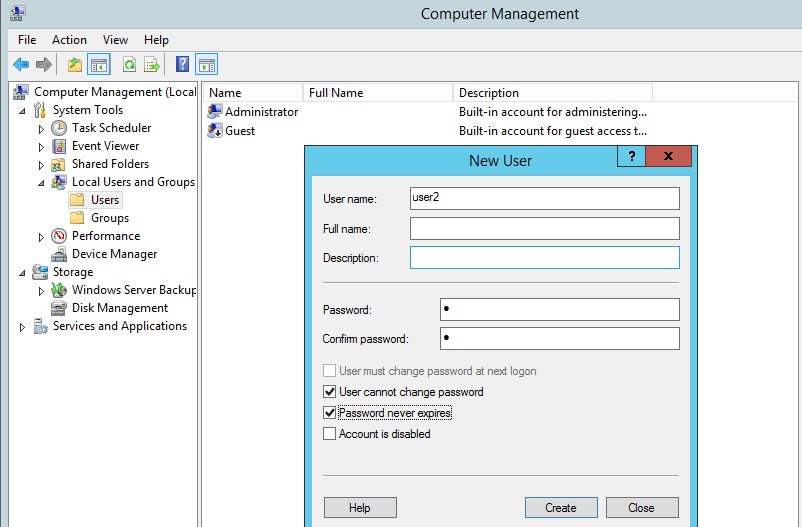


Рис. 8.28. Создание пользователя user2

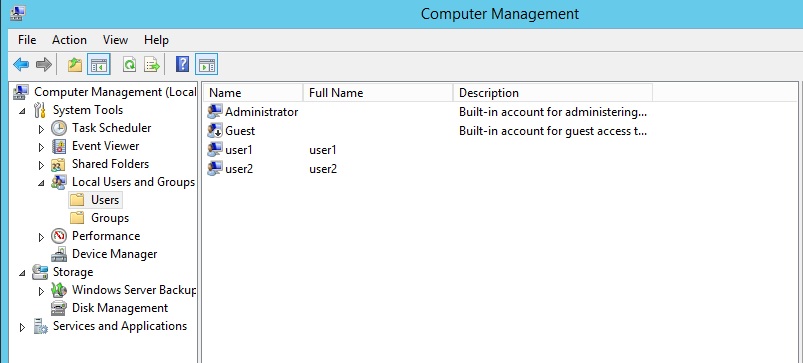


Рис. 8.29. Окно управления компьютером с созданными

пользователями user1 и user2

***8.3.2. Создание FTP-узла с изоляцией пользователей***

Создание ftp-узла с изоляцией предполагает первоначально создание ftp-узла с авторизацией (как описано выше) с дальнейшей ее настройкой. Вызывается окно настройки (рис. 8.30) можно, предварительно выбрав ftp-узел в левой части окна с консолью управления IIS сервером и далее в правой ее части щелкнув по иконке *Ftp User Isolation* (рис. 8.31). Отметим, что для такого типа узла необходимо создать структуру каталогов в домашней директории ftp-узла (в примере на рис 8.32 это *isolation*), как показано на рис. 8.32 (имена папок в папке *localuser* должны точно совпадать с именами пользователей).

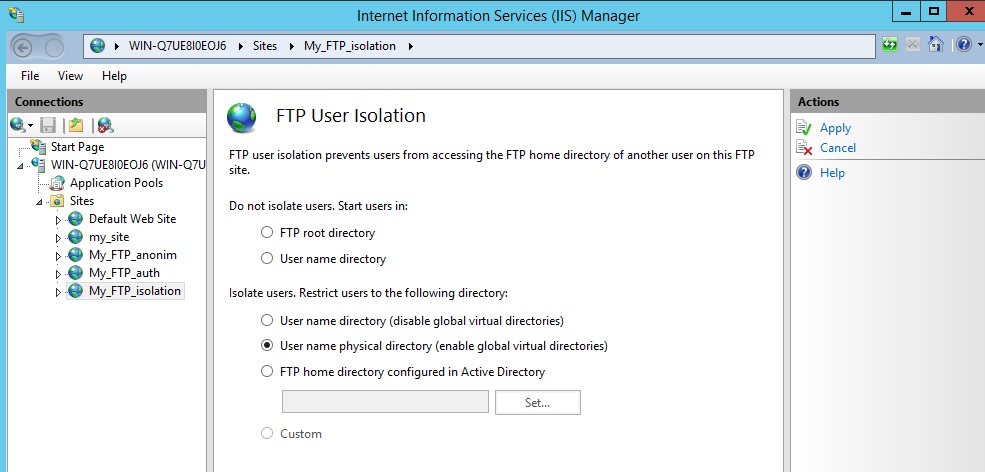


Рис. 8.30. Настройка ftp-узла с изоляцией пользователей

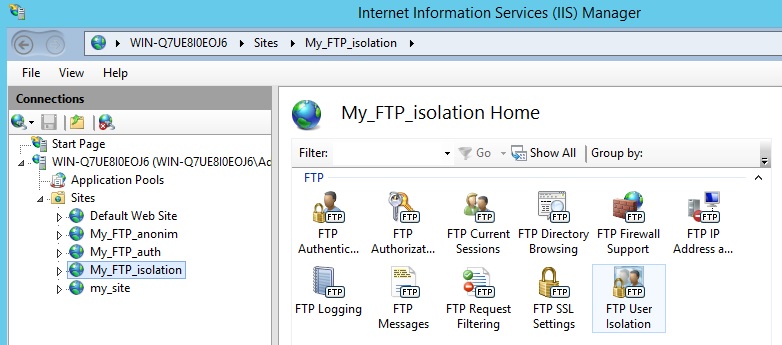


Рис. 8.31. Запуск мастера настройки ftp-узла с изоляцией пользователей

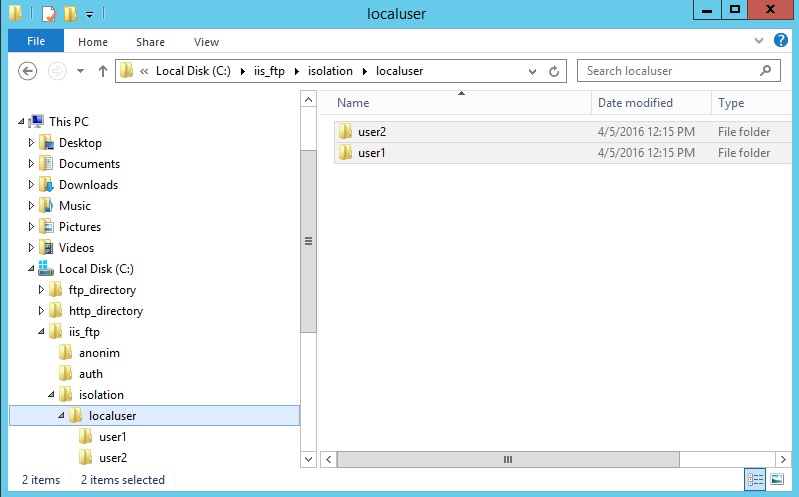


Рис. 8.32. Структура папок для ftp-узла с изоляцией

(для двух пользователей user1 и user2)

***8.3.3. Лабораторная работа № 16 и 17***

**Цель:** Изучение методов настройки IIS-сервера для передачи данных по протоколу ftp.

**Задание:** Лабораторная работа заключается в настройке следующих элементов.

1. Ftp-узел с гостевым (анонимным) доступом с возможностью записи информации, но запретом на удаление.
2. Ftp-узел с авторизированным доступом для двух пользователей: первый пользователь получает полный доступ, а второй – только чтение.
3. Ftp-узел с изоляцией пользователей. Все пользователи получают полный доступ, но только к своей папке (папке с именем пользователя).
4. Ftp-узел, работающий по принципу «черного ящика». Подключения к данному ресурсу осуществляется под гостевой учетной записью (без запроса логина и пароля) таким образом, чтобы пользователь мог записывать файлы, но не видел содержимого «черного ящика». Если осуществить подключение под логином пользователя, имеющего административные права (полный доступ), то ему будет доступна вся информация, хранящаяся на данном ftp-узле, а также любые операции с ней (запись, удаление, изменение, просмотр и т.д.)

Доступ к ftp-ресурсам необходимо демонстрировать с помощью браузера (либо другого ftp-клиента, например total commander) любого компьютера в сети (например, второй виртуальной машины).