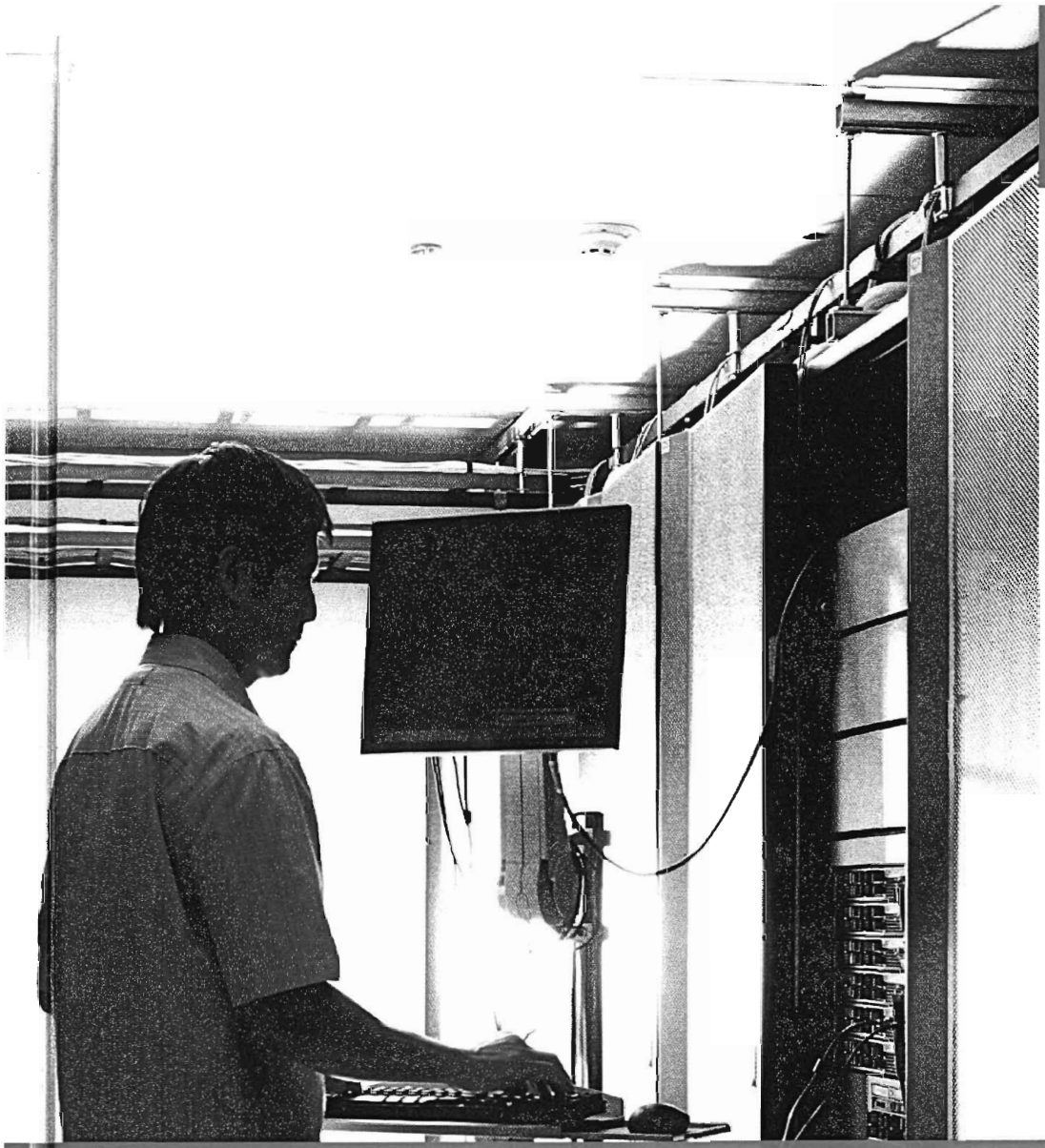


Том 2

Основные темы тома

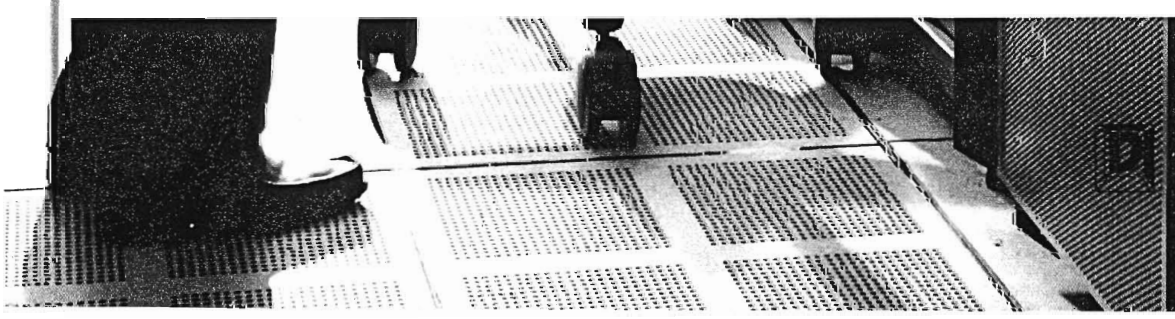
- дистанционное управление серверами
- подключение клиентов Windows и Mac
- планирование, установка, конфигурирование и запуск служб IIS
- организация виртуальных частных сетей
- создание сред Active Directory с несколькими доменами
- внедрение виртуализации с помощью Hyper-V
- работа со службами удаленного рабочего стола
- мониторинг, резервное копирование и обслуживание Windows Server 2012 R2 и Active Directory

Windows Server 2012 R2

Полное руководство

ДИСТАНЦИОННОЕ АДМИНИСТРИРОВАНИЕ, УСТАНОВКА СРЕДЫ С НЕСКОЛЬКИМИ ДОМЕНАМИ, ВИРТУАЛИЗАЦИЯ, МОНИТОРИНГ И ОБСЛУЖИВАНИЕ СЕРВЕРА

МАРК МИНАСИ, КЕВИН ГРИН, КРИСТИАН БУС, РОБЕРТ БАТЛЕР, ДЖОН МАК-КЕЙБ, РОБЕРТ ПАНЕК, МАЙКЛ РАЙС, СТЕФАН РОТ



SYBEX
A Wiley Brand

Mastering Windows Server® 2012 R2

Mark Minasi
Kevin Greene
Christian Booth
Robert Butler
John McCabe
Robert Panek
Michael Rice
Stefan Roth

SYBEX®
A Wiley Brand

Windows Server 2012 R2 Полное руководство

ТОМ 2

ДИСТАНЦИОННОЕ АДМИНИСТРИРОВАНИЕ, УСТАНОВКА СРЕДЫ С НЕСКОЛЬКИМИ ДОМЕНАМИ, ВИРТУАЛИЗАЦИЯ, МОНИТОРИНГ И ОБСЛУЖИВАНИЕ СЕРВЕРА

Марк Минаси
Кевин Грин
Кристиан Бус
Роберт Батлер
Джон Мак-Кейб
Роберт Панек
Майкл Райс
Стефан Рот

ДИАЛЕКТИКА

Москва • Санкт-Петербург • Киев
2015

ББК 32.973.26-018.2.75
М61
УДК 681.3.07

Компьютерное издательство "Диалектика"
Зав. редакцией *С.Н. Тригуб*
Перевод с английского *О.Л. Пелявского*
Под редакцией *Ю.Н. Артеменко*

По общим вопросам обращайтесь в издательство "Диалектика" по адресу:
info@dialektika.com, http://www.dialektika.com

Минаси, Марк, **Грин**, Кевин, **Бус**, Кристиан, **Батлер**, Роберт, и др.

М61 Windows Server 2012 R2. Полное руководство. Том 2: дистанционное администрирование, установка среды с несколькими доменами, виртуализация, мониторинг и обслуживание сервера. : Пер. с англ. — М. : ООО "И.Д. Вильямс", 2015. — 864 с. : ил. — Парал. тит. англ.

ISBN 978-5-8459-1936-6 (рус., том 2)
ISBN 978-5-8459-1934-2 (рус., многотом.)

ББК 32.973.26-018.2.75

Научно-популярное издание

Марк Минаси, Кевин Грин, Кристиан Бус, Роберт Батлер, и др.

Windows Server 2012 R2. Полное руководство.
Том 2: дистанционное администрирование,
установка среды с несколькими доменами,
виртуализация, мониторинг и обслуживание сервера

Верстка *Т.Н. Артеменко*
Художественный редактор *В.Г. Павлютин*

Подписано в печать 05.05.2014. Формат 70×100/16.
Гарнитура Times.
Усл. печ. л. 69,66. Уч.-изд. л. 59,5.
Тираж 500 экз. Заказ № 2446.

Отпечатано способом ролевой струйной печати
в АО «Первая Образцовая типография»
Филиал «Чеховский Печатный Двор»
142300, Московская область, г. Чехов, ул. Полиграфистов, д.1

ООО "И. Д. Вильямс"
127055, г. Москва, ул. Лесная, д. 43, стр. 1

ISBN 978-5-8459-1936-6 (рус., том 2)
ISBN 978-5-8459-1934-2 (рус., многотом.)
ISBN 978-1-1182-8942-6 (англ.)

Оглавление

Содержание

Глава 17

Дистанционное администрирование сервера

Повседневное администрирование любого сервера редко выполняется непосредственно возле сервера. Напротив, администраторы, как правило, подключаются к серверам дистанционно.

Серверы тихо шумят в прохладном (подчас очень холодном) серверном помещении, которое весьма надежно защищено в физическом смысле. Администраторы зачастую пребывают в комфортабельном офисе, работая с какой-либо операционной системой для настольных компьютеров, например, Windows 7 или Windows 8. Когда необходимо администрирование, они подключаются к серверам дистанционно.

С учетом этого обстоятельства вам нужно знать, как конфигурировать серверы для дистанционного администрирования и как подключаться к серверам со своего рабочего стола. В противном случае вам придется проводить бо́льшую часть своего времени в серверном помещении (а там даже в середине лета придется работать в теплой одежде).

В этой главе вы изучите следующие темы:

- конфигурирование серверов Windows Server 2012 R2 для дистанционного администрирования;
- дистанционное подключение к серверам Windows Server 2012 R2 с помощью подключения к удаленному рабочему столу;
- дистанционное подключение к серверам Windows Server 2012 R2 с помощью файла протокола удаленного рабочего стола;
- конфигурирование сервера для получения дистанционной помощи;
- установка инструментов дистанционного администрирования сервера.

Удаленный рабочий стол для администрирования

Удаленный рабочий стол для администрирования (Remote Desktop for Administration) представляет собой стандартную реализацию службы удаленных рабочих столов (Remote Desktop Services — RDS) на сервере Windows Server 2012 R2. В этом режиме с сервером могут одновременно работать не более двух администраторов, выполняющих удаленное администрирование.

Сервер можно также сконфигурировать как хост-сервер сеансов удаленных рабочих столов (Remote Desktop Session Host server), чтобы на нем могли выполняться рабочие столы или приложения рабочих столов для удаленных пользователей. Однако конфигурирование сервера в качестве хост-сервера сеансов удаленных рабочих столов требует дополнительных лицензий и сервера лицензирования. При использовании сервера в режиме удаленного рабочего стола для администрирования никакого дополнительного лицензирования не требуется.

Новое название терминальных служб

Если вам приходилось работать с предыдущими версиями Windows, то вы наверняка знакомы с некоторыми возможностями RDS — но под другим названием. В прошлых версиях служба удаленного рабочего стола была известна как терминальные службы (Terminal Services). В Windows Server 2008 R2 она была переименована в RDS.

Удаленный рабочий стол для администрирования позволяет вам подключаться к серверу и выполнять дистанционно практически любые действия, которые пришлось бы выполнять, если бы вы находились непосредственно у сервера. В режиме дистанционного подключения к серверу вы можете пользоваться меню Start (Пуск), запускать на выполнение нужные инструменты, устанавливать приложения, проводить обновления и делать многие другие действия. Двумя основными инструментами, которые вы будете применять при выполнении дистанционного администрирования, являются подключение к удаленному рабочему столу (Remote Desktop Connection — RDC) и удаленный рабочий стол (Remote Desktop).

Самое существенное ограничение, с которым вам придется столкнуться, связано с необходимостью перезагрузки или перезапуска удаленной системы. Несмотря на то что дистанционная перезагрузка системы, в принципе, возможна, ее выполнение влечет за собой отключение вас от сервера. Если что-либо мешает перезагрузке системы, то вы не сможете узнать, в чем именно заключается проблема, и не сумеете решить ее.

Конфигурирование сервера для удаленного рабочего стола

Активизировать удаленный рабочий стол на сервере можно несколькими способами. Вы можете перейти на страницу расширенных свойств сервера, воспользовавшись одним из перечисленных ниже методов.

- Щелкните на ссылке рядом с обозначением Remote Desktop (Удаленный рабочий стол) в окне свойств локального сервера внутри диспетчера серверов, которое появляется при первой загрузке системы.

- Нажмите клавишу <Windows> на клавиатуре, щелкните правой кнопкой мыши на значке Computer (Компьютер) и выберите пункт Properties (Свойства) в динамическом меню, которое появляется внизу (рис. 17.1). Щелкните на Remote Settings (Удаленные параметры), чтобы получить доступ к вкладке Remote (Удаленные) диалогового окна System Properties (Свойства системы).

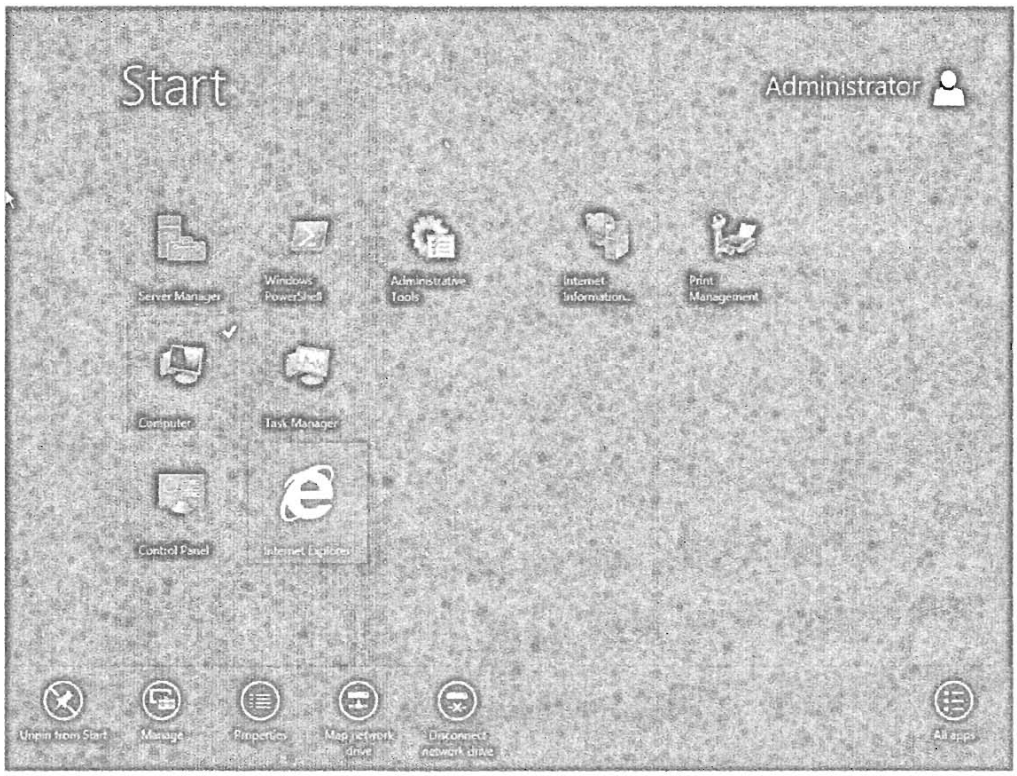


Рис. 17.1. Открытие диалогового окна System Properties

На рис. 17.2 показаны варианты конфигурации, которые предлагает вкладка Remote.

Рис. 17.2. Конфигурирование удаленного рабочего стола на вкладке Remote диалогового окна System Properties

Нетрудно заметить, что Windows Server 2012 R2 предоставляет в ваше распоряжение три варианта конфигурирования сервера для дистанционного администрирования.

- **Don't Allow Remote Connections to This Computer** (Не разрешать удаленное подключение к этому компьютеру). Удаленный рабочий стол заблокирован.
- **Allow Remote Connections to This Computer** (Разрешить удаленное подключение к этому компьютеру). Этот вариант разрешает удаленные подключения от клиентов.
- **Allow Connections Only from Computers Running Remote Desktop with Network Level Authentication (Recommended)** (Разрешить подключения только от компьютеров с удаленными рабочими столами с аутентификацией сетевого уровня (рекомендуется)). Этот вариант поддерживает подключения от клиентов, использующих протокол RDC 6.0 или более новые версии. RDC 6.0 и более новые версии имеются в Windows Vista и Windows 7. Протокол RDC 6.1 может быть установлен в системах Windows XP с пакетом обновлений, по меньшей мере, SP2.

Когда вы активизируете подключение к удаленному рабочему столу, в брандмауэре на локальной системе автоматически создается исключение. Нет необходимости добавлять на этот локальный брандмауэр другие исключения. Однако если вы подключаетесь через сетевой брандмауэр, то понадобится открыть порт 3389, чтобы сделать возможным удаленное подключение. Если же открыть порт 3389 на сетевом брандмауэре в вашей сети не представляется возможным, можете создать сервер шлюза удаленного рабочего стола (Remote Desktop Gateway), как будет описано далее в этой главе.

Аутентификация сетевого уровня (Network Level Authentication — NLA) — это средство обеспечения безопасности, предусмотренное в Remote Desktop Services, когда выбирается более защищенная конфигурация. NLA обеспечивает дополнительную безопасность за счет выполнения аутентификации пользователя до осуществления удаленного подключения. Если NLA не применяется, сервер может оказаться беззащитным перед атакой типа "отказ в обслуживании".

Аутентификация NLA должна использоваться каждый раз, когда есть такая возможность. Ниже перечислены требования к поддержке NLA.

- На клиентском компьютере должен использоваться, по меньшей мере, протокол версии RDC 6.0. Поддержка RDC 6.0 автоматически обеспечивается в клиентах Windows Vista.
- Клиентский компьютер должен поддерживать протокол CredSSP (Credential Security Support Provider — поставщик поддержки учетных данных безопасности).
- Сервер должен работать под управлением Windows Server 2008 R2 или Windows Server 2012 R2.

RDC 6.1 для Windows XP

Первоначальная версия RDC, которая применялась в Windows XP, не поддерживает NLA. Однако впоследствии в Microsoft разработали RDC 6.1 для клиентов, функционирующих под управлением Windows XP с пакетом обновлений SP2 или SP3; RDC 6.1 обеспечивает поддержку многих возможностей, реализованных в подключениях Windows Server 2012 R2.

Версия RDC 6.1 доступна для бесплатной загрузки и снабжена подробной документацией в форме статьи KB 952155 (`http://support.microsoft.com/kb/952155/`). RDC 6.0 поддерживается в Windows XP SP3.

Кроме того, протокол CredSSP можно активизировать путем модификации реестра в Windows XP, как описано в статье KB 951608 (`http://support.microsoft.com/kb/951608/`).

Использование подключения к удаленному рабочему столу

Для подключения к удаленному серверу используется RDC (Remote Desktop Connection — подключение к удаленному рабочему столу). Версией, которая лучше всего работает с Windows Server 2012 R2, является RDC 6.0 (или более поздняя). Предшествующие версии не поддерживают все имеющиеся возможности, такие как NLA.

RDC можно запустить в Windows Vista, Windows 7 и Windows Server 2008 R2, выбрав пункт меню Start⇨All Programs⇨Accessories⇨Remote Desktop Connection (Пуск⇨Все программы⇨Стандартные⇨Подключение к удаленному рабочему столу). После того как RDC будет запущено на выполнение, можно щелкнуть на кнопке Options (Опции), чтобы увидеть все доступные возможности (рис. 17.3).

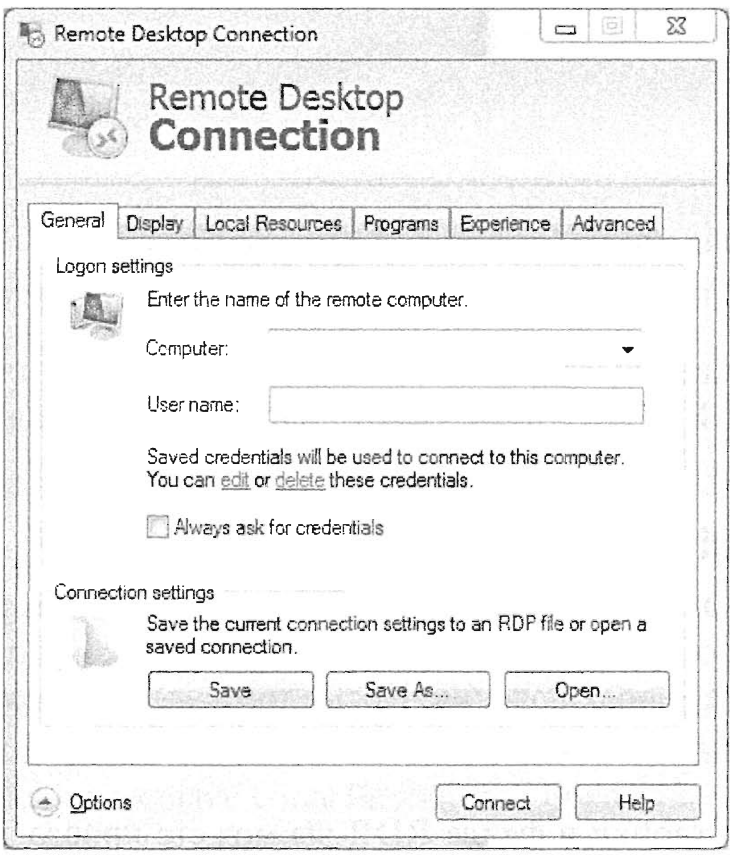


Рис. 17.3. Подключение к удаленному рабочему столу с развернутыми опциями

Получить доступ к RDC в среде Windows 8 и Windows Server 2012 R2 можно несколько по-другому.

1. Нажмите клавишу <Windows>, чтобы перейти на экран пуска в стиле Metro.
2. В нижнем правом углу экрана находится значок свертывания. Когда вы установите над этим значком курсор мыши, на экране появится боковая врезка. В поле поиска этой боковой врезки наберите слово `remote`.
3. Когда вы начнете набирать в поле поиска слово `remote`, вы увидите, как слева на экране появится значок Remote Desktop Connection (рис. 17.4).

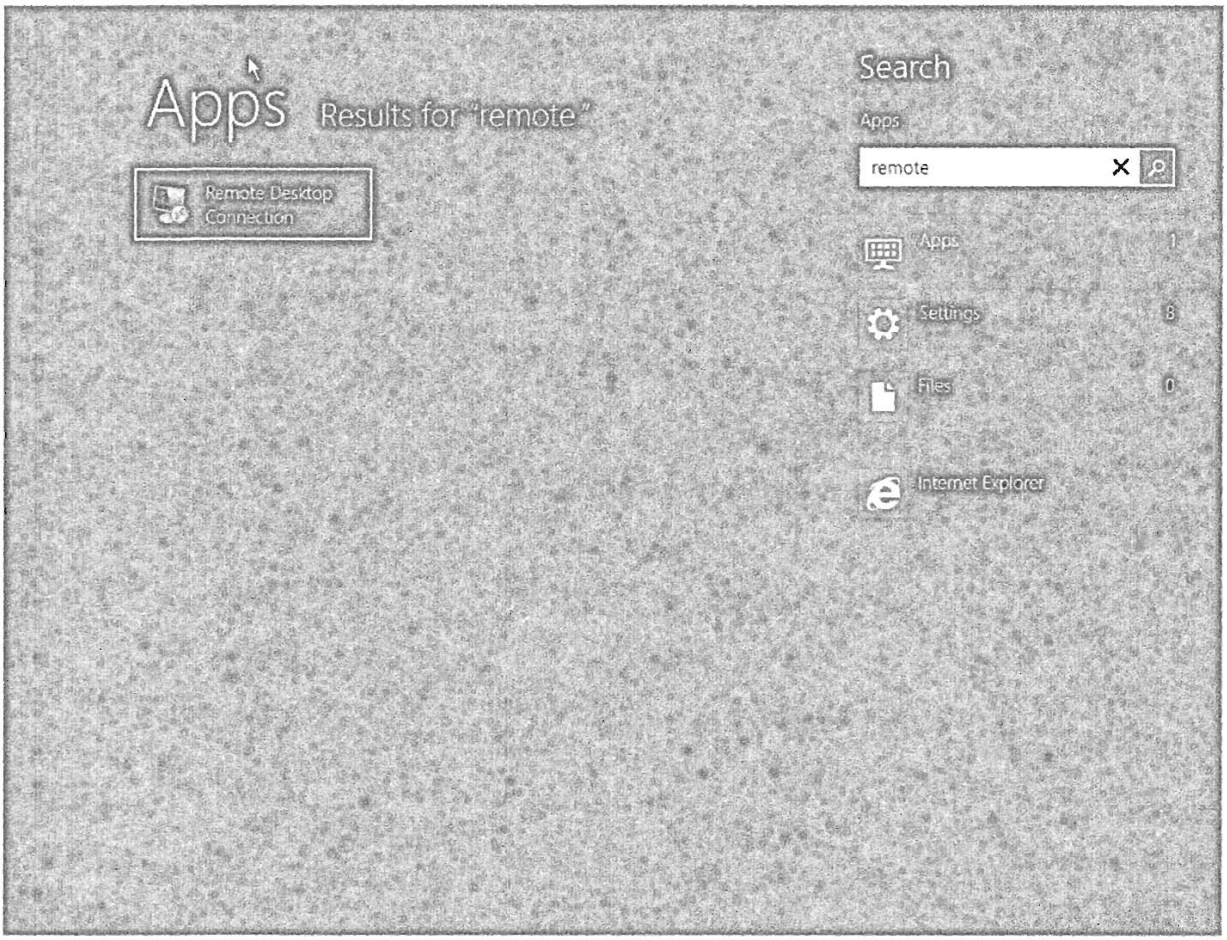


Рис. 17.4. Получение доступа к RDC в среде Windows Server 2012 R2

Окно RDC включает шесть вкладок, с помощью которых можно применять разные возможности RDC, которые более подробно обсуждаются в последующих разделах.

Вкладка General окна RDC

Вкладка General (Общие) используется для идентификации удаленного компьютера, к которому вы хотите подключиться, и учетной записи пользователя, которую вы будете применять для подключения. Кроме того, здесь вы можете сохранить свои настройки в файле RDP (Remote Desktop Protocol — протокол удаленного рабочего стола).

Сохранив свои настройки в файле RDP, вы можете просто дважды щелкнуть на имени этого файла, чтобы инициировать сеанс. Выполните описанную ниже последовательность действий, чтобы сохранить и использовать свой файл RDP.

Удаленные сеансы возможны на локальных компьютерах

Если у вас есть только один компьютер, вы по-прежнему можете применять приведенные ниже шаги. Вы можете инициировать удаленный сеанс компьютера, войдя в систему локально. Для удаленного сеанса вы должны использовать другую учетную запись с административными разрешениями. Хотя от этого нет особой пользы в плане повседневной работы, это все же позволяет увидеть соответствующий процесс в тестовой системе.

1. Запустите приложение Remote Desktop Connection.
2. Щелкните на кнопке Options (Опции), чтобы развернуть опции.
3. Введите имя удаленного компьютера в текстовом поле Computer (Компьютер).
4. Введите имя пользователя, который располагает разрешением на использование RDC на удаленном компьютере.

   Если вы хотите, чтобы это имя пользователя было сохранено, отметьте флажок Allow me to save credentials (Разрешить мне сохранять учетные данные). Впоследствии вам будет предложено указать пароль.
5. Щелкните на кнопке Save As (Сохранить как) и перейдите на соответствующий рабочий стол. Переименуйте файл в `RDC.rdp` и щелкните на кнопке Save (Сохранить).
6. Закройте приложение Remote Desktop Connection.
7. Перейдите на рабочий стол своего компьютера и дважды щелкните на имени файла `RDC.rdp`, чтобы запустить его на выполнение.
8. Ознакомьтесь с предупреждениями в открывшемся диалоговом окне (рис. 17.5).

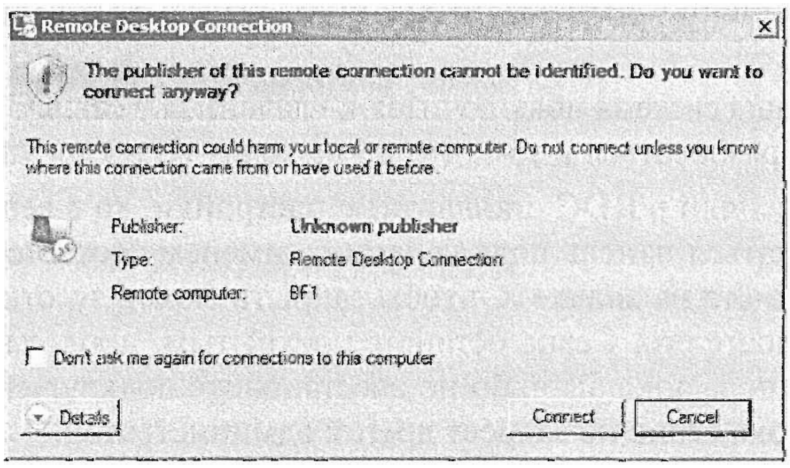


Рис. 17.5. Предупреждение о неизвестном издателе

9. Щелкните на кнопке Details (Подробности) в диалоговом окне.

   Это диалоговое окно позволяет использовать определенные локальные ресурсы, которые вы можете задействовать в своем удаленном сеансе. Когда открывается инструмент Remote Desktop Connection, вы можете также изменять параметры локальных ресурсов на вкладке Local Resources (Локальные ресурсы).
10. После того как вы создали файл RDP, вы можете положиться на него и не обращать внимания на предупреждения. Щелкните на кнопке Connect (Подключиться).

Откроется диалоговое окно, позволяющее ввести пароль для своей учетной записи или воспользоваться какой-то другой учетной записью.

11. Введите пароль для учетной записи с административными привилегиями и щелкните на кнопке OK.

    Спустя мгновение на экране появится еще одно предупреждение, подобное показанному на рис. 17.6.

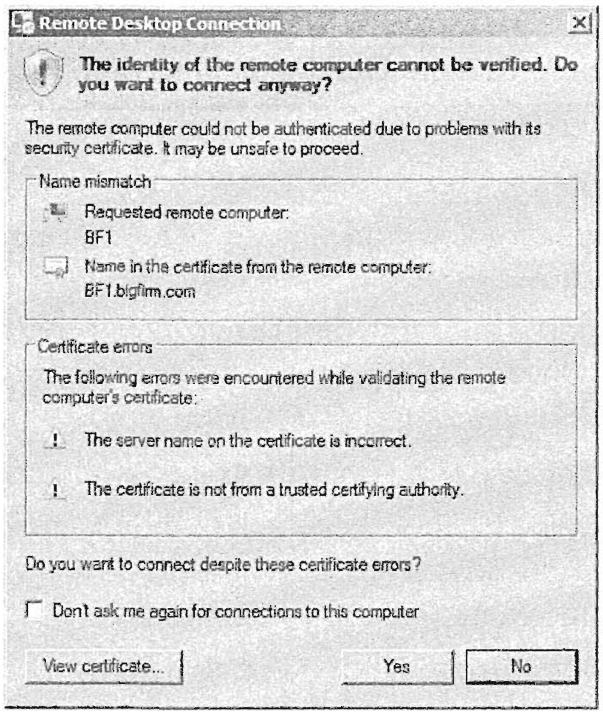


Рис. 17.6. Предупреждение о неизвестном центре сертификации

12. Щелкните на кнопке Yes (Да), чтобы подключиться, невзирая на предупреждение.

    После этого ваша система подключится к удаленному сеансу. Отведите какое-то время, чтобы разобраться в том, что происходит во время удаленного сеанса.

    Если вы применяли в RDC стандартные настройки, то в верхней части экрана будет отображаться панель подключения с именем соответствующего сервера. Если вы щелкнете на значке X, чтобы закрыть экран, то отключитесь от сеанса, но не закроете его. Сеанс останется открытым, продолжая потреблять ресурсы, до тех пор, пока вы либо не восстановите подключение или завершите сеанс, либо пока сеанс не закроет другой администратор.

13. Щелкните на кнопке Start (Пуск) и выберите Log Off (Завершить сеанс), чтобы закрыть подключение и завершить сеанс.

Предупреждения о неизвестном издателе

В случае использования файла RDP без подписи вы увидите два предупреждения, которые указывают на то, что издатель удаленного соединения не может быть идентифицирован, и запрашивают, хотите ли вы подключиться в любом случае. Первое предупреждение отображается в верхней части диалогового окна, показанного на рис. 17.5, а второе предупреждение можно видеть в окне на рис. 17.6.

В целях безопасности файлы RDP могут быть подписаны с помощью сертификатов. Подписанный файл RDP содержит внутри себя подпись, которая указывает удостоверение клиента центра сертификации (Certification Authority — CA), проверившего его идентичность. Если вы доверяете центру сертификации, то вы доверяете и этому файлу RDP. При распространении файлов RDP по множеству клиентов такая дополнительная функция безопасности может оказаться весьма ценной.

Тем не менее, файлы RDP не обязаны быть подписанными. Поскольку именно вы создаете этот файл RDP, можете просто игнорировать упомянутые предупреждения.

Файл RDP ассоциируется с приложением Remote Desktop Connection, поэтому двойной щелчок на нем приводит к запуску RDC. Однако файл RDP является просто текстовым файлом. Если вы хотите взглянуть на его содержимое, можете запустить Notepad (Блокнот), открыть этот файл и посмотреть, что в нем находится.

Вкладка Display окна RDC

Вкладка Display (Экран) позволяет сконфигурировать дисплей для удаленного рабочего стола. Здесь можно настроить размер этого рабочего стола и его цвета. Вкладка Display показана на рис. 17.7.

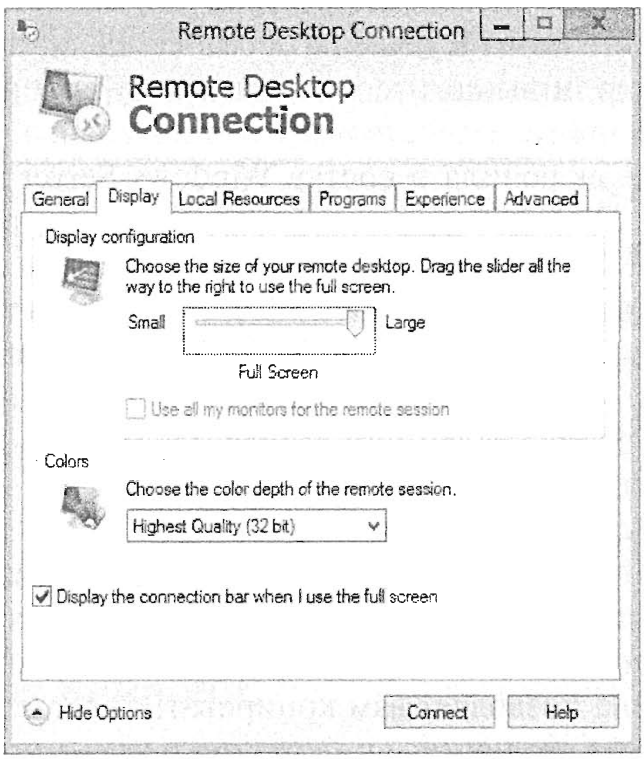


Рис. 17.7. Вкладка Display приложения Remote Desktop Connection

Если перетащить ползунок до упора вправо, то удаленный рабочий стол будет отображаться в полноэкранном режиме. По умолчанию при отображении в полноэкранном режиме панель подключения будет отображаться в верхней части экрана.

В панели подключения указывается имя удаленного сервера, что может оказаться полезным, если у вас одновременно выполняется несколько экземпляров RDC. Если, например, вы занимаетесь устранением проблемы и подключены дистанционно к трем разным серверам с помощью трех разных экземпляров RDC, то можете буквально с одного взгляда на панель подключения, расположенную в верхней части окна, выяснить, с каким именно сервером вы работаете в данный момент.

Повышение производительности при использовании WAN-соединения

Если вы обращаетесь к удаленному серверу посредством медленного WAN-соединения, у вас есть возможность увеличить производительность за счет использования меньшего экрана или сокращения количества отображаемых цветов. Это не является проблемой в сети с быстродействующими соединениями с максимум двумя удаленными сеансами, но в случае медленного соединения приходится экономить буквально на каждой мелочи.

Когда вы подключены дистанционно к серверу посредством RDC в полноэкранном режиме, эта панель подключения является единственным зримым свидетельством этого. Все остальное выглядит так, словно вы сидите непосредственно у сервера.

Слева от панели подключения расположен значок с изображением канцелярской кнопки. По умолчанию он отмечен, что обеспечивает закрепление панели подключения к верхней части экрана. Вы можете снять с него отметку, чтобы панель подключения автоматически скрывалась и не отображалась на экране.

Вкладка Local Resources окна RDC

Вкладка Local Resources (Локальные ресурсы) позволяет определить, какие ресурсы могут быть задействованы в удаленном сеансе. Если, например, к вашей системе подключен принтер, и вы хотите распечатать журнал регистрации событий с удаленного сервера, то можете задействовать этот локальный принтер.

Компания Microsoft включила в состав Windows Server 2008 инструмент Easy Print (Простая печать). Этот инструмент облегчает перенаправление принтера при использовании службы удаленного рабочего стола (RDS) и гарантирует установку клиентских принтеров в удаленных сеансах. Чтобы выполнять распечатку из сеанса RDS, вам не придется устанавливать драйверы печати на сервере.

Щелкнув на кнопке More (Дополнительно), вы можете активизировать дополнительные ресурсы во время удаленного сеанса. На рис. 17.8 представлена вкладка Local Resources и дополнительные ресурсы, которые могут быть задействованы после щелчка на кнопке More.

Основной причиной, по которой вы будете обращаться к этой вкладке, является необходимость подключения или отключения локальных устройств и ресурсов. Локальные принтеры и локальный буфер обмена активизируются по умолчанию. Локальный буфер обмена позволяет вам копировать текст из своей системы (такой как сценарий) и вставлять его внутрь приложения в удаленном сеансе.

Локальные диски по умолчанию не активизируются, но если вы хотите скопировать данные с какого-то локального диска в удаленную систему, ничто не мешает вам отметить соответствующий флажок. Однако это представляет угрозу для безопасности системы. Если либо удаленная система, либо ваша локальная система заражена вирусом или содержит иное вредоносное ПО, то подключение дисков обеспечивает доступ к ним со стороны этого вредоносного ПО и делает их уязвимыми в смысле заражения.

Вы можете также сконфигурировать параметры аудиосистемы и клавиатуры.

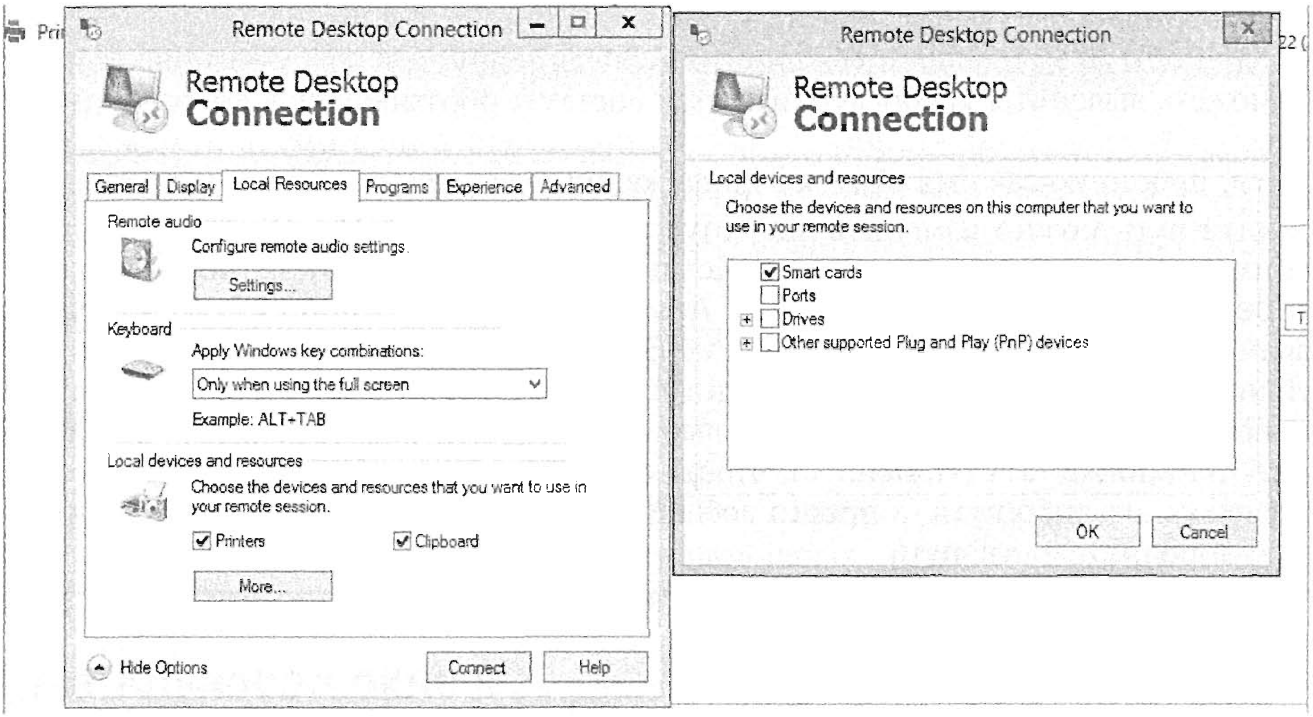


Рис. 17.8. Вкладка Local Resources приложения Remote Desktop Connection с дополнительными опциями

К числу настроек аудиосистемы относятся следующие:

- Play on this computer (Воспроизвести на этом компьютере) (ваш локальный компьютер)
- Do not play (Не воспроизводить)
- Play on remote computer (Воспроизвести на удаленном компьютере)

Если же вы предпочитаете пользоваться клавиатурными сокращениями, то может возникнуть потребность изменить настройки клавиатуры. Для этого доступны следующие варианты:

- On this computer (На этом компьютере)
- On the remote computer (На удаленном компьютере)
- Only when using the full screen (Только при использовании полноэкранного режима)

Вкладка Programs окна RDC

Вкладка Programs (Программы) позволяет идентифицировать программу, которая запустится на выполнение, когда будет установлено удаленное соединение. Например, вы можете всегда запускать на выполнение диспетчер серверов (Server Manager), когда стартуете определенный сервер и хотите, чтобы эта программа запускалась на выполнение автоматически. Вкладка Programs показана на рис. 17.9. В текстовое поле вводится `ServerManager.msc`, что приведет к запуску диспетчера серверов при установлении соединения.

Поскольку путь к диспетчеру серверов уже известен системе как `%systemroot%\System32`, указывать его не придется. Тем не менее, если вы хотите запустить другую программу или сценарий из неизвестного системе пути, то этот путь должен быть указан полностью.

Системная переменная Path

Вы можете выяснить, какой путь известен системе, обратившись к командной строке, введя `Path` и нажав <Enter>. К любому приложению по этому пути можно обратиться, просто указав имя нужного приложения.

Данный путь можно изменить, щелкнув на кнопке Start (Пуск), щелкнув правой кнопкой мыши на значке Computer (Компьютер), выбрав в контекстном меню пункт Properties (Свойства), а затем пункт Advanced system settings (Дополнительные параметры системы). В диалоговом окне System Properties (Свойства системы) перейдите на вкладку Advanced (Дополнительно) и щелкните на кнопке Environment Variables (Переменные среды). Затем выберите системную переменную `Path` и щелкните на кнопке Edit (Изменить), чтобы изменить эту переменную. Вы не должны удалять какие-либо пути, а просто добавить необходимые, введя точку с запятой и затем дополнительные пути.

Вкладка Experience окна RDC

С помощью вкладки Experience (Внешний вид) можно добавлять или удалять функциональные средства RDC. Доступны разные средства, такие как фоновый рисунок рабочего стола, визуальные эффекты при отображении меню и окон, а также стили оформления, которые позволят достичь большей выразительности при отображении удаленного подключения.

На рис. 17.10 представлена вкладка Experience, на которой скорость соединения установлена как LAN (10 Mbps or higher) (Локальная сеть (10 Мбит/с и выше)). Эти возможности требуют увеличения полосы пропускания, поэтому стандартные функциональные средства выбраны на основе скорости соединения, заданной на этой странице.

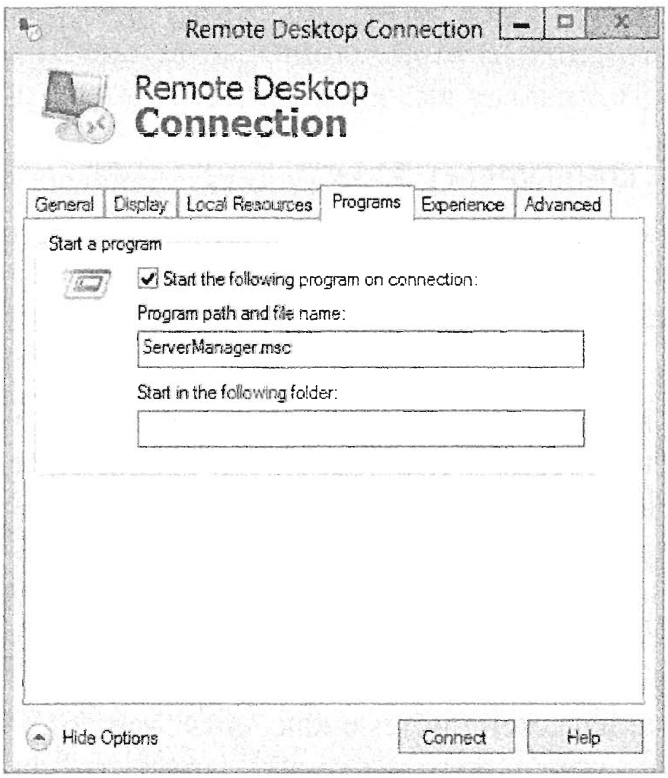


Рис. 17.9. Вкладка Programs приложения Remote Desktop Connection

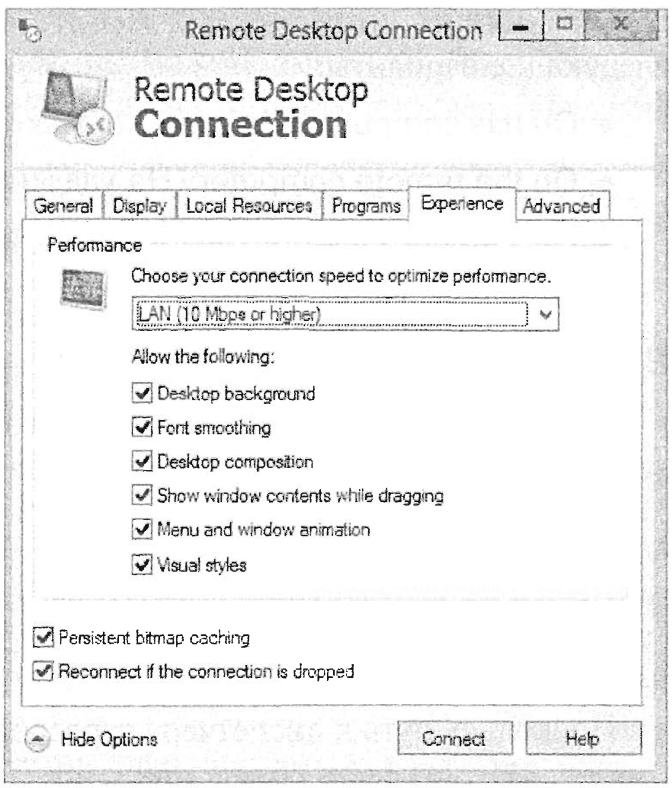


Рис. 17.10. Вкладка Experience приложения Remote Desktop Connection

Если вы подключены к локальной сети, то располагаете быстродействующим соединением, поэтому вам доступны все функциональные средства RDC. Если вы наблюдаете снижение производительности, то некоторые средства RDC можно отключить. Кроме того, если вы подключаетесь с помощью модема по каналу связи 56 Кбит/с, то можете выбрать вариант Modem (56 Kbps) (Модем (56 Кбит/с)); при этом по умолчанию будет активизировано только кеширование постоянных растровых изображений.

Вариант скорости автоматически не определяется. Когда она выбрана, выбираются стандартные функциональные средства, но ничего не мешает вам добавлять или удалять эти средства, отмечая или снимая отметку с соответствующих флажков.

Эта вкладка также включает флажок Reconnect if the connection is dropped (Восстановить подключение при разрыве). Данная настройка может оказаться полезной при использовании ненадежных каналов связи. Если сетевое соединение прервано, RDC автоматически попытается восстановить его.

Вкладка Advanced окна RDC

Вкладка Advanced (Дополнительно) состоит из двух разделов: Server Authentication (Аутентификация сервера) и Connect from anywhere (Подключиться из любого места).

Аутентификация сервера является новым средством обеспечения безопасности, которое можно применять при подключении к Windows Server 2008 или более поздним версиям серверной ОС. Это средство проверяет, действительно ли вы подключаетесь к тому компьютеру, к которому собирались подключиться, и помогает предотвратить непреднамеренное разглашение конфиденциальной информации.

Аутентификация сервера предоставляет в ваше распоряжение три варианта действий.

- **Connect and Don't Warn Me (Подключаться без предупреждения).** Вы можете использовать этот вариант, если всегда подключаетесь к более ранним, чем Windows Server 2008, версиям сервера, которые не поддерживают аутентификацию сервера. Поскольку такие серверы не поддерживают аутентификацию сервера, они всегда будут выдавать предупреждения.
- **Warn Me (Предупреждать).** Этот вариант предусмотрен по умолчанию. Он применяется в смешанной среде серверов Windows Server и Windows Server 2003 (или предшествующих версий).
- **Do Not Connect (Не соединять).** Если ваша среда состоит исключительно из серверов Windows Server 2008 или последующих версий, этот вариант гарантирует, что соединения не будут создаваться, если соответствующий сервер не может пройти аутентификацию.

На рис. 17.11 показана вкладка Advanced приложения Remote Desktop Connection с раскрытыми настройками шлюза удаленного рабочего стола (Remote Desktop Gateway — RD Gateway).

Если вы подключаетесь к удаленному серверу через сервер RD Gateway, то именно на этой вкладке вы можете конфигурировать настройки соединения. Шлюз удаленного рабочего стола более подробно рассматривается далее в этой главе.

Важно понимать, что имя сервера, которое вы вводите здесь, является именем сервера шлюза.

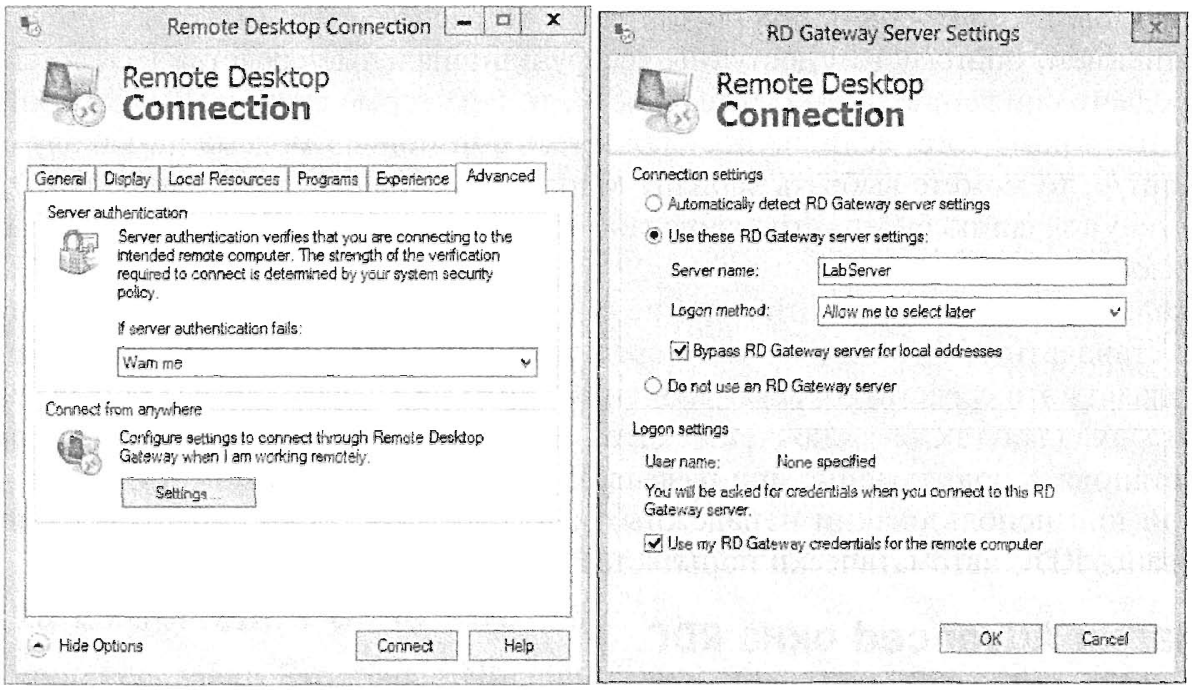


Рис. 17.11. Вкладка Advanced приложения Remote Desktop Connection и настройки шлюза удаленного рабочего стола

Сначала средство RDC подключится к этому серверу RDC, а затем к удаленному серверу, указанному на вкладке General.

Вам понадобится аутентифицировать как сервер RD Gateway, так и удаленный компьютер. Если вы применяете одни и те же учетные данные для них обоих, то флажок Use my RD Gateway credentials for the remote computer (Использовать мои учетные данные шлюза удаленного рабочего стола для удаленного компьютера) можно оставить отмеченным. Если этот флажок отмечен, вводить свои учетные данные вам придется только один раз. Если же снять отметку с этого флажка, вы должны будете вводить свои учетные данные два раза, причем учетные данные могут быть разными для этих двух серверов.

Хотя знание того, какую пользу может принести каждая из вкладок Remote Desktop Connection, отнюдь не повредит, вам понадобится изучить и ряд других деталей. Например, RDC можно запускать из командной строки, а при использовании любой команды в таком режиме доступны удобные переключатели, которые следует освоить. Кроме того, вы можете управлять несколькими ограничениями, касающимися удаленных соединений.

MSTSC

Запустить Remote Desktop Connection можно через строку Run (Выполнить) или в командной строке с помощью команды `mstsc.exe`. Имя `mstsc` является производным от Microsoft Terminal Services Connection (Подключение к терминальным службам Microsoft). Несмотря на то что терминальные службы (Terminal Services) в свое время были переименованы в службу удаленных рабочих столов (Remote Desktop Services), название команды `mstsc` осталось прежним.

Доступ к справочному экрану для `mstsc` можно получить, введя в командной строке **`mstsc /?`**.

В приведенном ниже перечне демонстрируются некоторые типичные применения команды `mstsc`.

- **Стандартное применение.** Используйте следующую команду для запуска Remote Desktop Connection (RDC):

  ```
  mstsc
  ```

- **Идентификация сервера.** Подключайтесь к серверу по имени `Srv1` с помощью переключателя `/v`:

  ```
  mstsc /v:Srv1
  ```

- **Использование файла RDP.** Запускайте RDC с применением файла RDP, находящегося по пути `c:\data\srv1.rdp`, следующим образом:

  ```
  mstsc c:\data\Srv1.rdp
  ```

- **Подключение в полноэкранном режиме.** Используйте для запуска RDC в полноэкранном режиме переключатель `/f`:

  ```
  mstsc /f
  ```

- **Использование нескольких мониторов.** Если вы хотите, чтобы приложение RDC охватывало несколько мониторов, задействованных в локальной системе, применяйте переключатель `/span`. Это заставит удаленную систему использовать такую же ширину и высоту вашего локального рабочего стола:

  ```
  mstsc /span
  ```

- **Подключение для административных целей.** Переключатель `/admin` используется для подключения к серверу Windows Server 2012 R2 в административных целях. Это имеет смысл, только если на данном сервере установлена служба удаленных рабочих столов. Другими словами, когда данный сервер применяется только для режима Remote Desktop for Administration (Удаленный рабочий стол для администрирования), все соединения предназначены для администрирования и этот переключатель не нужен. Однако если сервер сконфигурирован как хост-сервер сеансов удаленных рабочих столов, то вы можете использовать этот переключатель для подключения к одному из двух сеансов администратора.

Переключатель `/admin` можно также применять для запуска RDC в режиме унаследованной консоли при подключении к серверам Windows Server 2003. Серверы Windows Server 2003 поддерживают сеанс консоли, который в Windows Server 2012 R2 не поддерживается. Переключатель `/admin` обеспечивает подключение к сеансу консоли в Windows Server 2003.

Ограничения подключений

Лишь два подключения разрешены к серверу, когда он используется для обычных административных задач. Другими словами, только два администратора могут одновременно войти на один и тот же сервер.

Если же сервер применяется в качестве хоста для рабочих столов или приложений конечных пользователей, то количество подключений не ограничено. Служба Remote Desktop Services требует лицензий для подключения, если она используется в режиме хост-сервера сеансов удаленных рабочих столов. Тем не менее, для двух подключений администраторов лицензии не требуются.

Эти два подключения охватывают либо удаленные сеансы, либо сеанс за компьютером. Прежние операционные системы разрешали подключаться к двум удаленным сеансам и сеансу за компьютером. Сеанс за компьютером было принято называть *консольным сеансом*; при этом даже была возможность подключиться к этому консольному сеансу дистанционно, однако консольный сеанс больше не доступен.

На рис. 17.12 показано, что произойдет, если третий пользователь попытается подключиться в ситуации, когда уже инициированы два сеанса.

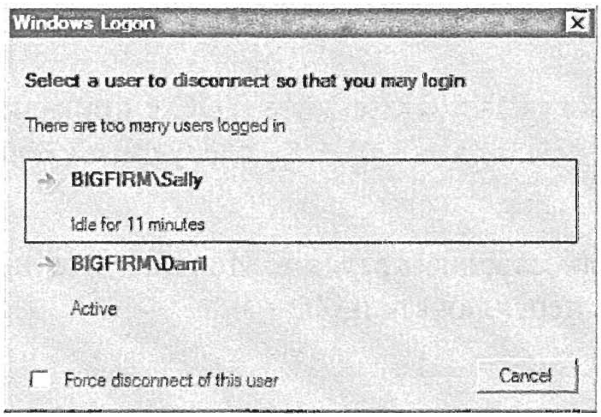


Рис. 17.12. Блокирование третьего удаленного сеанса

Здесь пользователь по имени `Darril` физически находится непосредственно у сервера, и он вошел в систему. Пользователь по имени `Sally` подключен посредством удаленного сеанса. Пользователь по имени `Joe` пытается войти в систему, но поскольку его сеанс стал бы уже третьим, этот сеанс блокируется. Обратите внимание, что в этом диалоговом окне также указано состояние сеансов. Сеанс может пребывать либо в активном состоянии, либо в состоянии бездействия. На этом рисунке сеанс пользователя `Sally` в течение 11 минут находится в состоянии бездействия, тогда как сеанс пользователя `Darril` пребывает в активном состоянии.

Если пользователь `Joe` отметит флажок Force disconnect of this user (Принудительное отключение этого пользователя) и выберет одного из пользователей, то этот пользователь будет немедленно отключен с выдачей ему сообщения следующего содержания.

> *Ваш сеанс удаленного рабочего стола завершен. Какой-то другой пользователь подключился к удаленному компьютеру, в результате чего ваше соединение было разорвано. Попробуйте подключиться еще раз или обратитесь к своему сетевому администратору либо группе технической поддержки.*

Если пользователь `Joe` не отметит этот флажок, а взамен выберет одного из пользователей, чтобы прервать его сеанс, то этот пользователь получит уведомление. На рис. 17.13 показано, что увидит на экране `Darril` во время своего сеанса, когда `Joe` попытается прервать его сеанс, не отметив при этом флажок Force disconnect of this user. Если `Darril` работает за компьютером, он сможет увидеть эту попытку подключения и щелкнуть на кнопке Cancel (Отмена), чтобы блокировать ее. В противном случае запрос через 30 секунд автоматически прервет сеанс пользователя `Darril` и разрешит запуск сеанса для пользователя `Joe`.

Если сеанс пользователя `Darril` находился в активном состоянии и `Darril` щелкнул на кнопке Cancel, то `Joe` получит уведомление, указывающее на то, что пользователь, работающий в системе, запретил запрос прерывания сеанса.

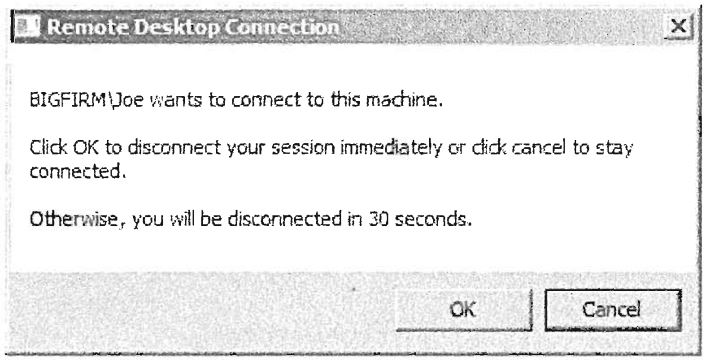


Рис. 17.13. Запрос прерывания сеанса

Активные подключения для неактивных сеансов

Этот метод закрытия неактивного сеанса администратора может служить реальным решением распространенной проблемы. Нам приходилось работать в нескольких крупных средах, в которых администраторы подключались к серверу дистанционно, но вместо того чтобы завершать сеанс, они просто прерывали соединение путем закрытия приложения RDC.

Когда подобное происходит, на сервере остается открытым неактивный сеанс. Если на этом сервере было достигнуто максимально допустимое количество сеансов, другим администраторам не удастся открыть удаленный сеанс. Такие неактивные сеансы могут оставаться открытыми до истечения тайм-аута (если соответствующий тайм-аут был задан при конфигурировании), до возвращения пользователя в систему и надлежащего закрытия им своего сеанса или до закрытия соответствующего сеанса в диспетчере службы удаленного рабочего стола.

Благодаря возможностям, доступным теперь в RDC, вы можете без труда выяснить, кто подключен к системе, просмотреть состояние сеансов (активное или бездействующее) и даже прервать отдельный сеанс.

Установка службы удаленных рабочих столов со службой хоста сеансов

Для освоения нескольких последующих разделов этой главы вам понадобится установить на сервере роль Remote Desktop Services.

Чтобы установить эту роль, выполните описанные ниже действия.

1. На вкладке Dashboard (Управляющая панель) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты).
2. Щелкните на кнопке Next (Далее), чтобы пропустить экран Before you begin (Прежде чем начать).
3. На следующем экране (рис. 17.14) выберите переключатель Role-based or feature-based installation (Установка на основе ролей или на основе компонентов).
4. Выберите сервер, на котором будет установлена роль Remote Desktop Services.

   Как видно на рис. 17.15, в нашем распоряжении имеется только один сервер. Выберите его и щелкните на кнопке Next.
5. Отметьте флажок для роли Remote Desktop Services, как показано на рис. 17.16, и щелкните на кнопке Next.

6. Поскольку вас не интересуют компоненты, представленные на экране Select features (Выбор компонентов), который приведен на рис. 17.17, просто щелкните на кнопке Next, чтобы продолжить.

   На рис. 17.18 показан результирующий экран, на котором объясняется, какую роль вы собираетесь установить. Это выглядит очевидным излишеством: если вы до сих пор не знаете, какую роль вы устанавливаете, то о чем вообще может идти речь!

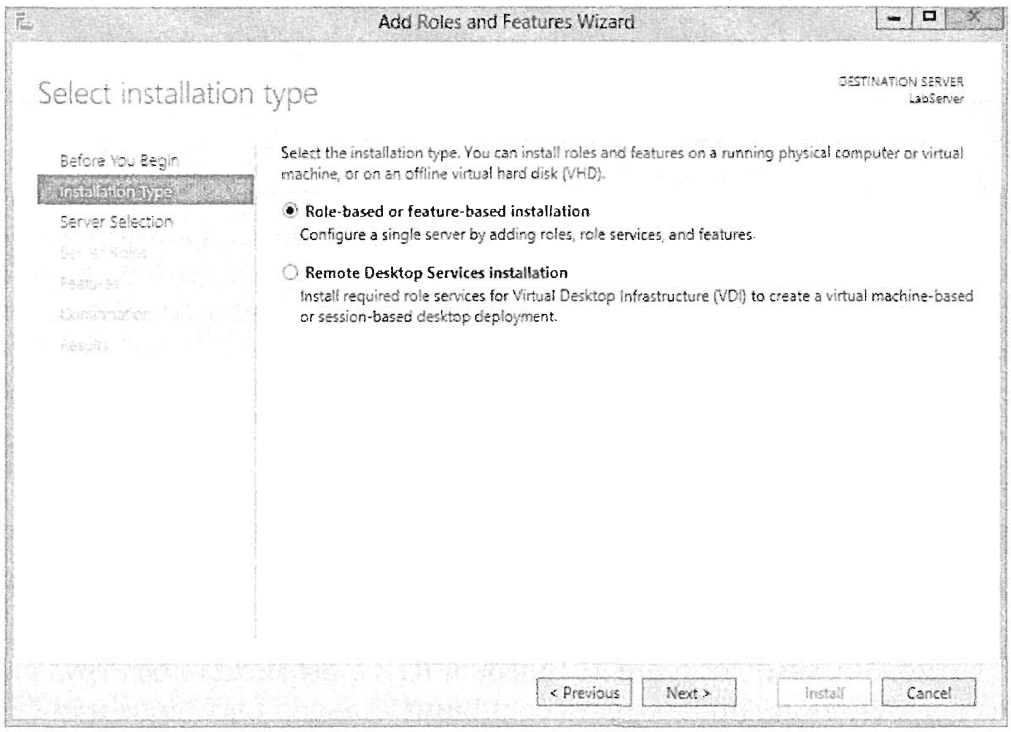


Рис. 17.14. Выбор типа установки роли

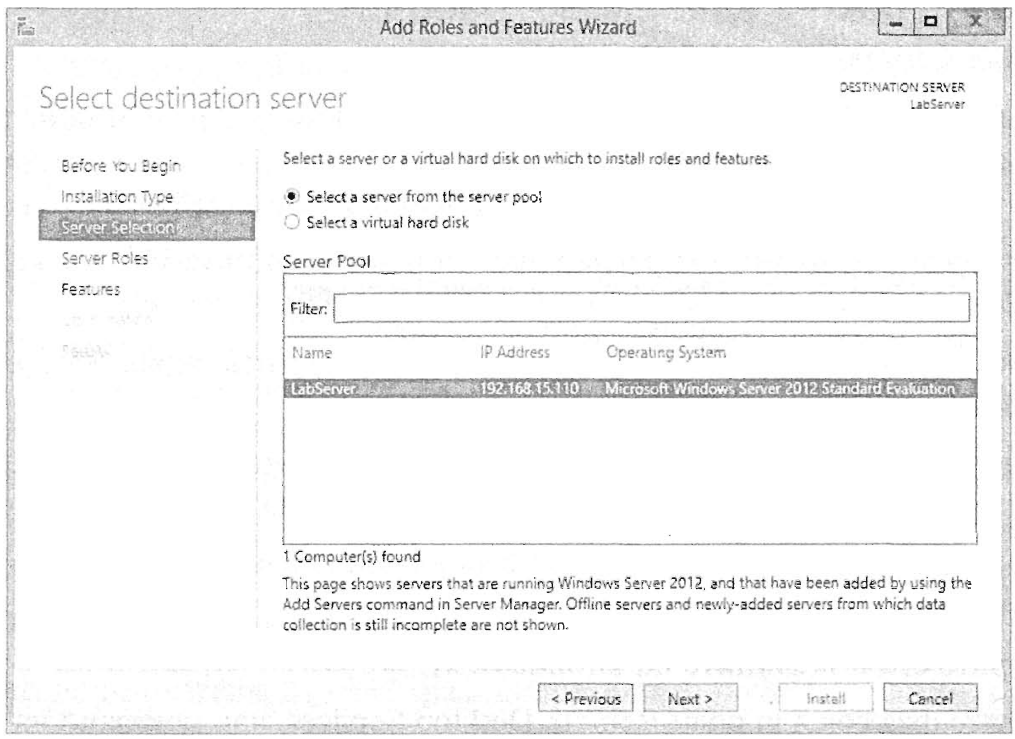


Рис. 17.15. Выберите сервер, на котором будет устанавливаться роль RDS

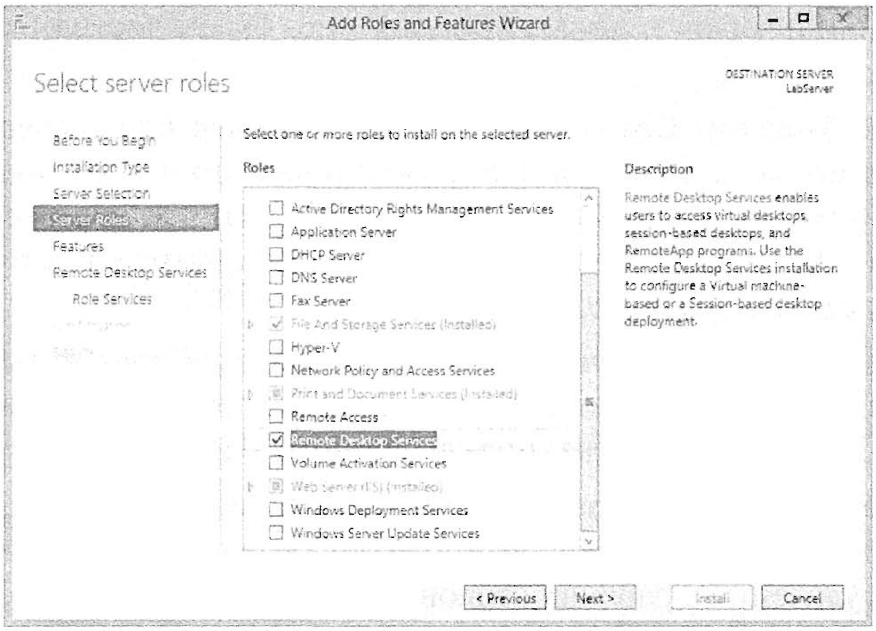


Рис. 17.16. Выбор роли Remote Desktop Services

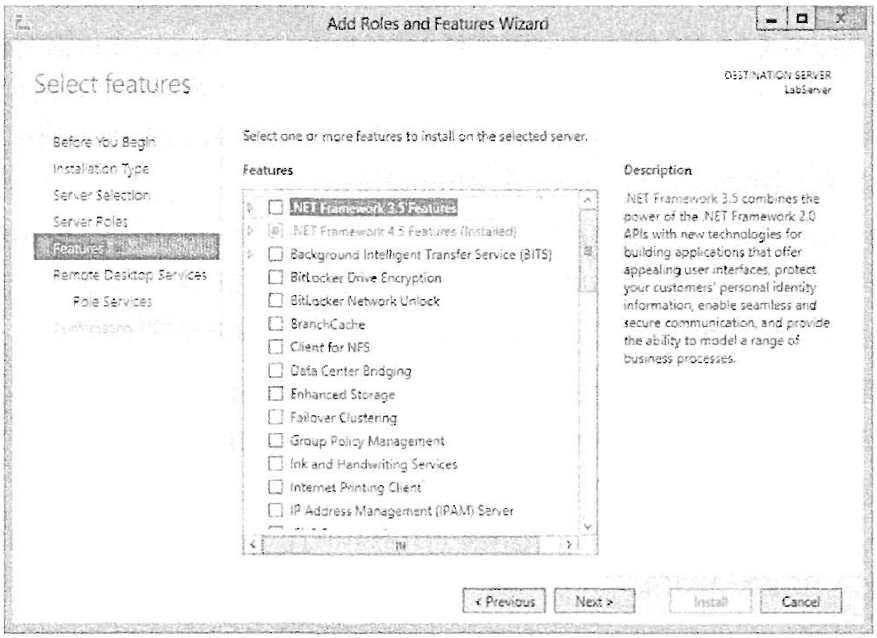


Рис. 17.17. Экран выбора компонентов

Рис. 17.18. Итоговый экран для выбранной роли

7. На следующем экране, показанном на рис. 17.19, доступны перечисленные ниже службы роли.
   - **Remote Desktop Connection Broker (Брокер подключений к удаленным рабочим столам).** Позволяет пользователям повторно подключаться к их существующим виртуальным рабочим столам и рабочим столам на основе сеансов. Он также позволяет балансировать нагрузку в пуле виртуальных рабочих столов внутри совокупности.
   - **Remote Desktop Gateway (Шлюз удаленного рабочего стола).** Позволяет авторизованным пользователям подключаться к внутренней корпоративной сети из любого устройства, подключенного к Интернету.
   - **Remote Desktop Licensing (Лицензирование удаленного рабочего стола).** Управляет лицензиями, которые требуются для подключения к хост-серверу сеансов удаленных рабочих столов.
   - **Remote Desktop Session Host (Хост сеансов удаленных рабочих столов).** Позволяет серверу стать хостом для рабочих столов, основанных на сеансах.
   - **Remote Desktop Virtualization Host (Хост виртуализации удаленного рабочего стола).** Интегрируется с Hyper-V, чтобы развернуть пулы или персональные совокупности виртуальных рабочих столов внутри организации за счет применения Remote Desktop Connection.
   - **Remote Desktop Web Access (Доступ к удаленным рабочим столам посредством веб).** Разрешает пользователям подключаться через веб-браузер.

   Выберите службу Remote Desktop Session Host.

   После выбора этой службы может появиться всплывающее окно с запросом на установку дополнительных компонентов, поддерживающих выбранный вариант.
8. Щелкните на кнопке Add Features (Добавить компоненты), чтобы установить компоненты поддержки.

   На рис. 17.20 показан экран Network Policy and Access Services (Службы сетевой политики и доступа), информирующий о том, что на следующем экране также понадобится установить эту службу роли.
9. На рис. 17.21 видно, что по умолчанию флажок для службы Network Policy Server (Сервер сетевой политики) выбран автоматически. Для продолжения щелкните на кнопке Next.

   Итак, мы почти у цели. На рис. 17.22 вы видите экран подтверждения для устанавливаемой роли.
10. Отметьте флажок Restart the destination server automatically if required (Перезапустить целевой сервер автоматически, если требуется), чтобы перезапустить сервер после установки.
11. Щелкните на кнопке Install (Установить), чтобы начать установку роли Remote Desktop Services и всех ее компонентов поддержки.

    На рис. 17.23 можно видеть ход процесса установки.
12. После перезагрузки сервера войдите в систему и обратите внимание на появление в меню диспетчера серверов пункта Remote Desktop Services.

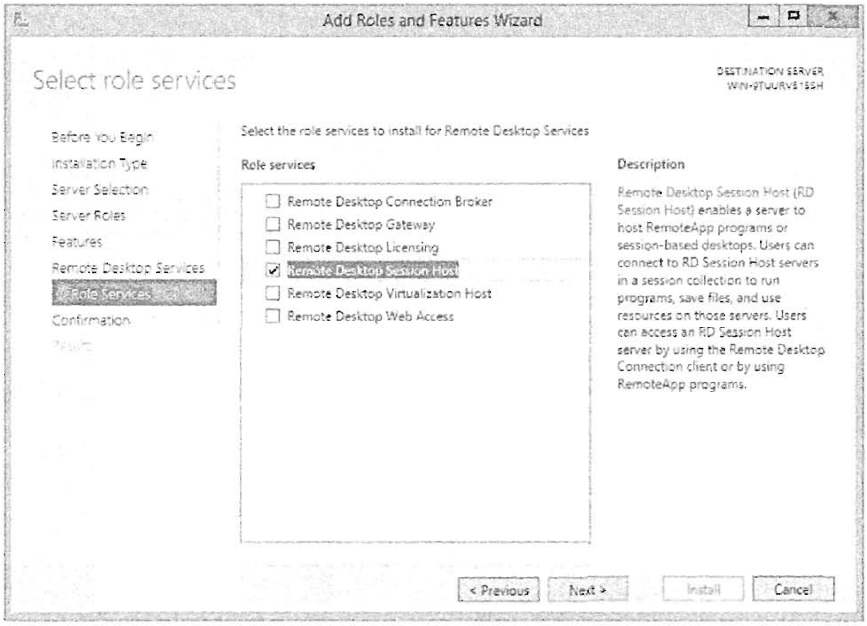


Рис. 17.19. Выбор служб роли

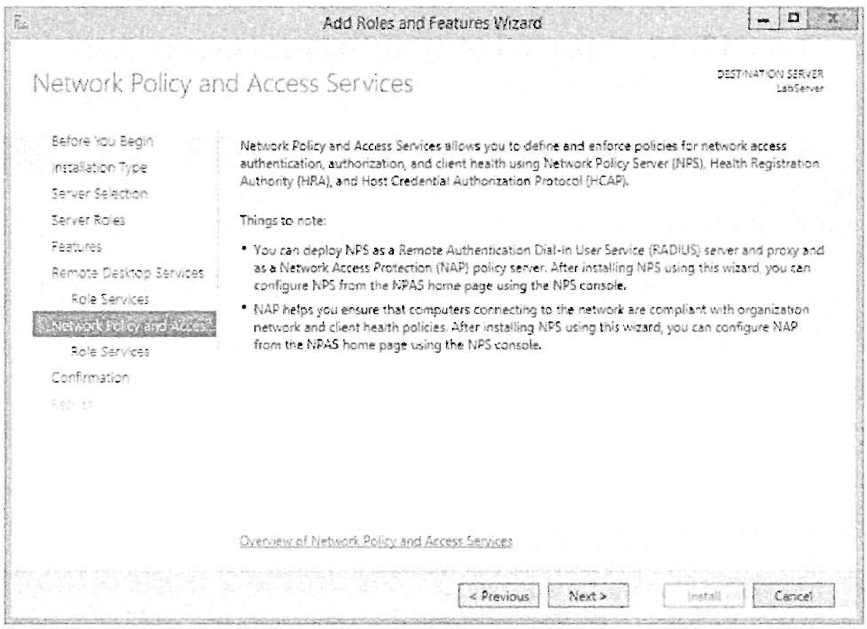


Рис. 17.20. Уведомление о предстоящей установке Network Policy and Access Services

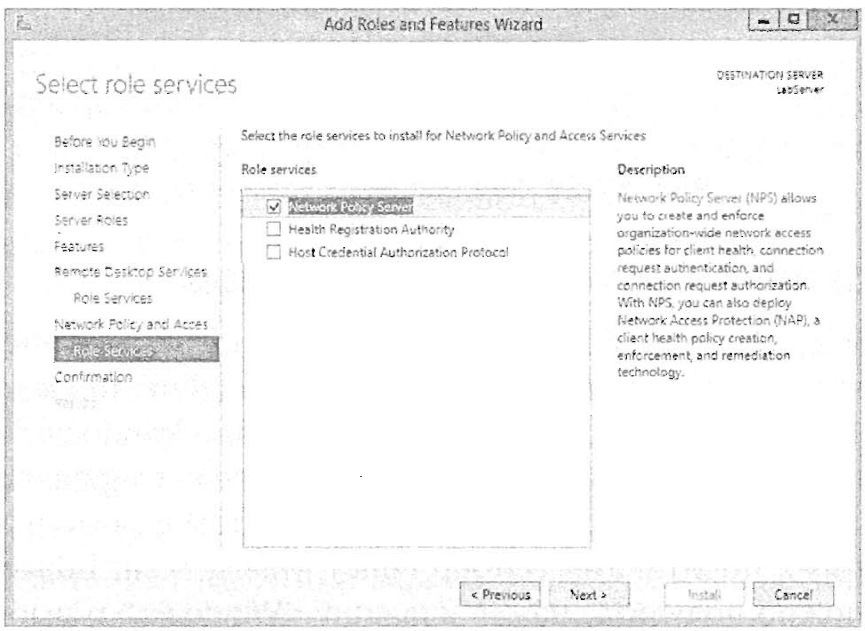


Рис. 17.21. Выбор службы Network Policy Server

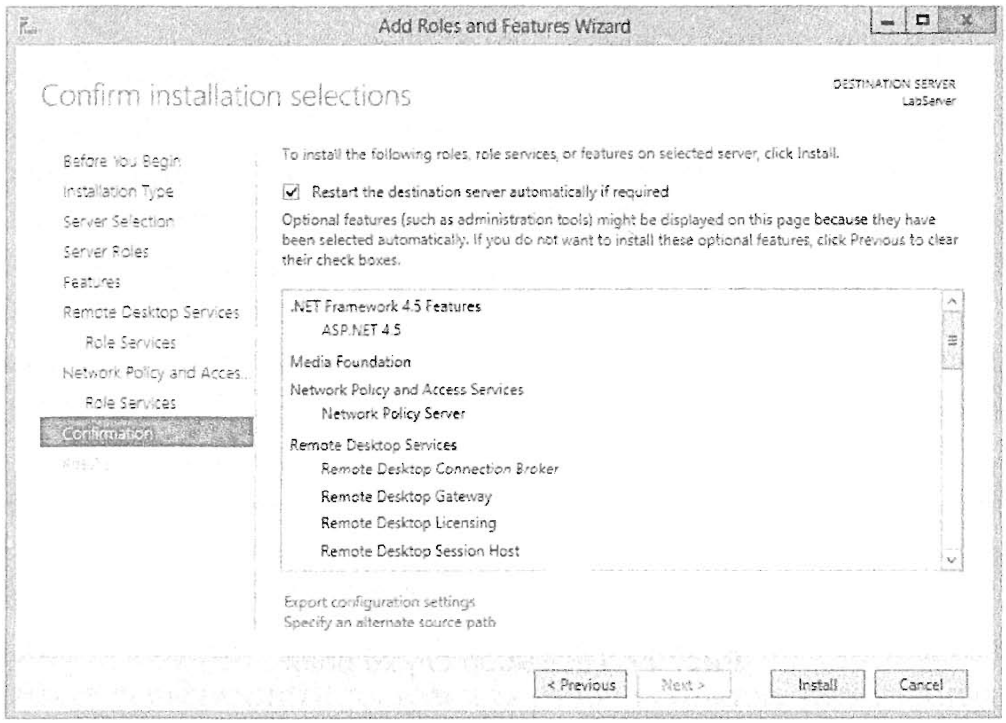


Рис. 17.22. Экран подтверждения установки роли

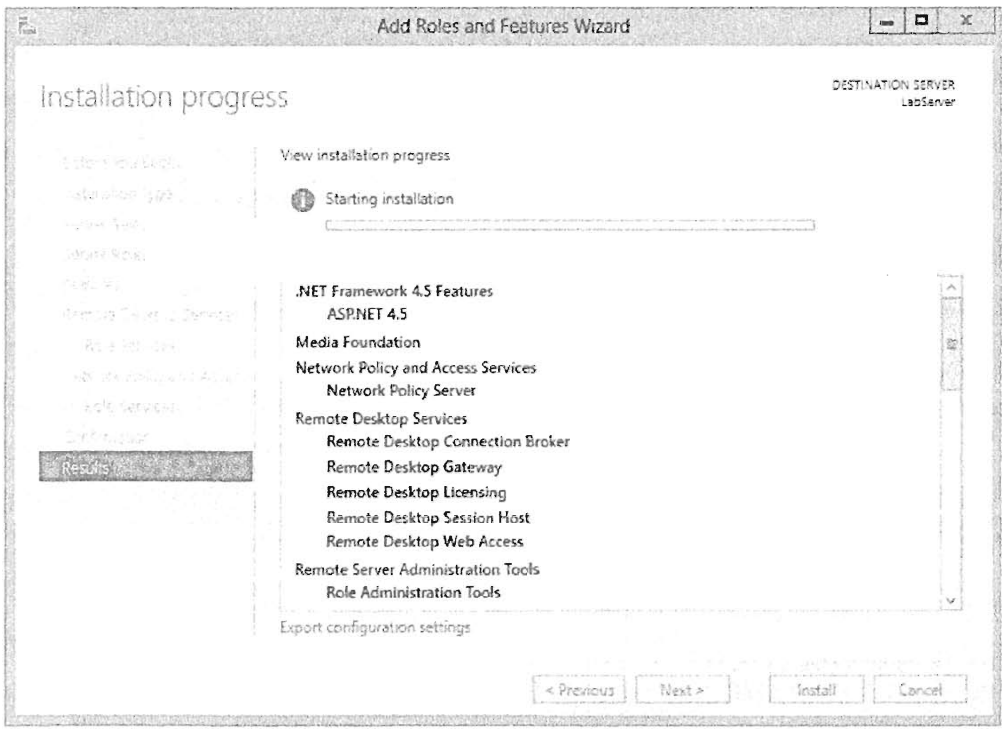


Рис. 17.23. Ход процесса установки

Конфигурирование свойств хоста сеансов

В версии Windows Server 2012 R2 больше нельзя использовать инструмент конфигурирования хоста сеансов удаленных рабочих столов (Remote Desktop Session Host Configuration Tool), который вы, возможно, применяли в Windows Server 2008 R2.

Свойства сеанса для удаленных сеансов можно конфигурировать в хосте сеансов удаленных рабочих столов (Remote Desktop Session Host) с помощью редактора управления групповыми политиками (Group Policy Management Editor). Доступ к этому инструменту можно получить, нажав клавишу <Windows> и выбрав пункт Group Policy Management (Управление групповой политикой).

Главной конфигурацией, которую вы будете здесь задействовать при использовании Remote Desktop Services, является Remote Desktop Session Host. На рис. 17.24 представлены свойства, доступные для Remote Desktop Session Host.

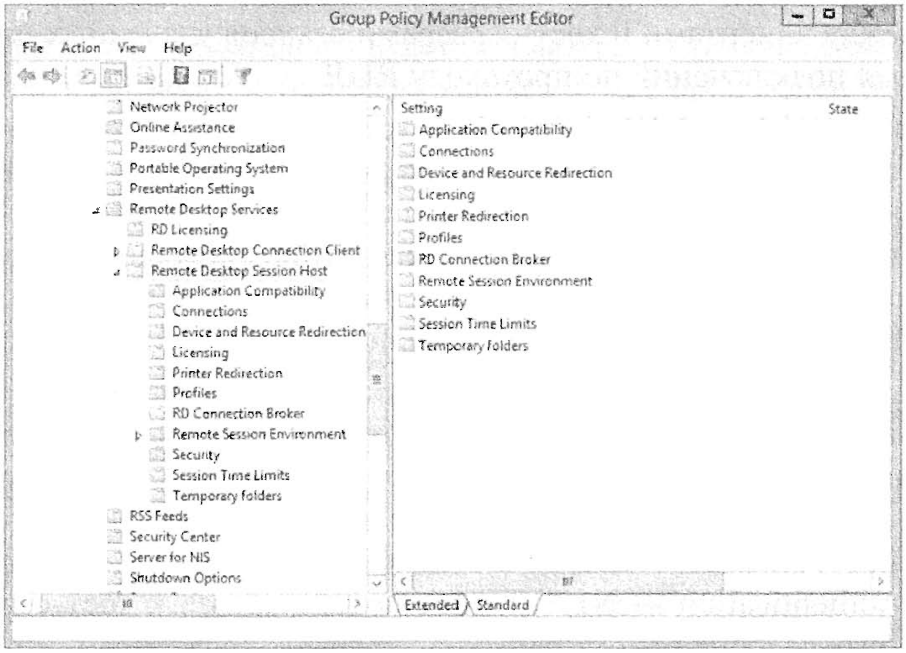


Рис. 17.24. Использование редактора управления групповыми политиками для конфигурирования хоста сеансов удаленных рабочих столов

Поскольку для Remote Desktop Session Host предусмотрено довольно много свойств, мы рассмотрим лишь пару важных из них, о которых вы обязательно должны знать.

Security (Безопасность). Поскольку пользователи обращаются к серверу дистанционно, свойства безопасности должны быть заботой администратора. Ниже перечислены свойства безопасности, которые можно устанавливать.

- **Server Authentication Certificate Template (Шаблон сертификата аутентификации сервера).** Эта настройка политики позволяет указывать имя шаблона сертификата, который определяет, какой сертификат выбирается автоматически для аутентификации хост-сервера сеансов удаленных рабочих столов.
- **Set Client Connection Encryption Level (Установить уровень шифрования подключений клиентов).** Эта настройка политики указывает, нужно ли требовать использования определенного уровня шифрования, чтобы обеспечить безопасные коммуникации между клиентскими компьютерами и хост-серверами сеансов удаленных рабочих столов во время соединений по протоколу удаленного рабочего стола.
- **Always Prompt for Password upon Connection (Всегда запрашивать пароль при подключении).** Эту настройку можно применять для обеспечения запросов на ввод пароля у пользователей, входящих в Remote Desktop Services, даже если они уже предоставили свои пароли клиенту Remote Desktop Connection.
- **Require Secure RPC Communications (Требовать безопасных коммуникаций RPC).** Эту настройку политики можно использовать для повышения безопасности коммуникаций RPC с клиентами, разрешив только аутентифицированные и зашифрованные запросы.

- **Require Use of Specific Security Layer for Remote (RDP) Communications (Требовать использования определенного уровня безопасности для удаленных подключений (RDP)).** Эта настройка политики указывает, требовать ли применения определенного уровня безопасности, чтобы защитить коммуникации между клиентами и хост-серверами сеансов удаленных рабочих столов во время подключений по протоколу RDP.
- **Do Not Allow Local Administrators to Customize Permissions (Не позволять локальным администраторам настраивать разрешения).** Эту настройку политики можно использовать, чтобы не дать возможность администраторам вносить изменения в пользовательские группы, которым разрешено дистанционно подключаться к хост-серверу сеансов удаленных рабочих столов. По умолчанию администраторам позволено вносить такие изменения.
- **Require User Authentication for Remote Connections by Using Network Level Authentication (Требовать аутентификации пользователей для удаленных подключений путем использования аутентификации на сетевом уровне).** Если вы задействуете эту настройку политики, то лишь клиентские компьютеры, которые поддерживают аутентификацию на сетевом уровне (Network Level Authentication — NLA), могут подключаться к хост-серверу сеансов удаленных рабочих столов.

Session Time Limits (Лимиты продолжительности сеанса). Другими свойствами, которые вам, вероятно, придется изменять, являются лимиты продолжительности сеанса. Ниже перечислены свойства, касающиеся лимитов продолжительности сеанса, с краткими описаниями каждого из этих свойств.

- **Set Time Limit for Disconnected Sessions (Установить лимит времени для отключенных сеансов).** Эту настройку политики можно применять для указания максимальной продолжительности времени, в течение которого отключенный сеанс будет оставаться активным на сервере. По умолчанию служба RDS разрешает пользователям отключаться от сеанса Remote Desktop Services, не выходя и не завершая сеанс.
- **Set Time Limit for Active but Idle Remote Desktop Services Sessions (Установить лимит времени для активных, но бездействующих сеансов службы удаленного рабочего стола).** Если вы задействуете эту настройку политики, то должны выбрать желаемый лимит времени в списке лимитов для бездействующего сеанса. По истечении заданного вами времени служба удаленного рабочего стола автоматически отключит активные, но бездействующие сеансы. Пользователь получает соответствующее предупреждение за две минуты до прерывания сеанса, что позволяет пользователю нажать какую-то клавишу или переместить указатель мыши, чтобы сеанс остался активным.
- **Set Time Limit for Active Remote Desktop Services Sessions (Установить лимит времени для активных сеансов службы удаленного рабочего стола).** Эта настройка политики позволяет указать максимальную продолжительность времени, в течение которого сеанс Remote Desktop Services может быть активным, прежде чем он будет автоматически отключен.
- **End Session When Time Limits Are Reached (Завершать сеанс, когда будут достигнуты лимиты времени).** Эта настройка политики указывает, завершать

ли сеанс Remote Desktop Services, который исчерпал установленный для него лимит времени, вместо того чтобы отключать его.

- **Set Time Limit for Logoff of RemoteApp Sessions (Установить лимит времени для выхода сеансов RemoteApp).** Эта настройка политики позволяет указать, насколько долго будет оставаться в отключенном состоянии сеанс RemoteApp пользователя, прежде чем будет произведен его выход из хост-сервера сеансов удаленных рабочих столов.

  По умолчанию, если пользователь закрывает программу RemoteApp, соответствующий сеанс отключается от хост-сервера сеансов удаленных рабочих столов.

Несмотря на то что Remote Desktop Connection — исключительно ценный инструмент, с помощью которого можно дистанционно администрировать серверы внутри управляемой локальной сети, подчас он может не отвечать вашим потребностям. Например, вам может понадобиться дистанционно подключаться к серверу через Интернет, но администраторы брандмауэра просто откажутся открыть соответствующие порты. В подобных случаях Remote Desktop Gateway может оказаться именно тем инструментом, без которого не обойтись.

Remote Desktop Gateway

Шлюз Remote Desktop Gateway используется для разрешения подключений к внутренней сети через Интернет. Когда шлюз RD Gateway задействован, пользователи могут подключаться к ресурсам внутренней сети из любого устройства, имеющего доступ в Интернет. RD Gateway действует одинаково и когда он применяется, чтобы предоставить возможность администратору получить доступ к внутреннему ресурсу, и когда он используется, чтобы предоставить возможность обычному пользователю получить доступ к хост-серверу сеансов, о чем подробно рассказывается в главе 29.

Для установления безопасного, шифрованного подключения между удаленными пользователями и внутренним ресурсом, RD Gateway применяет протокол RDP поверх HTTPS.

На рис. 17.25 показано, как можно было бы сконфигурировать RD Gateway. Сервер Windows Server 2012 R2 по имени `BF4` помещен в демилитаризованную зону (DMZ) и на нем установлена служба роли Remote Desktop Gateway. Клиент может подключаться к `BF4` через Интернет с помощью RDP поверх HTTPS.

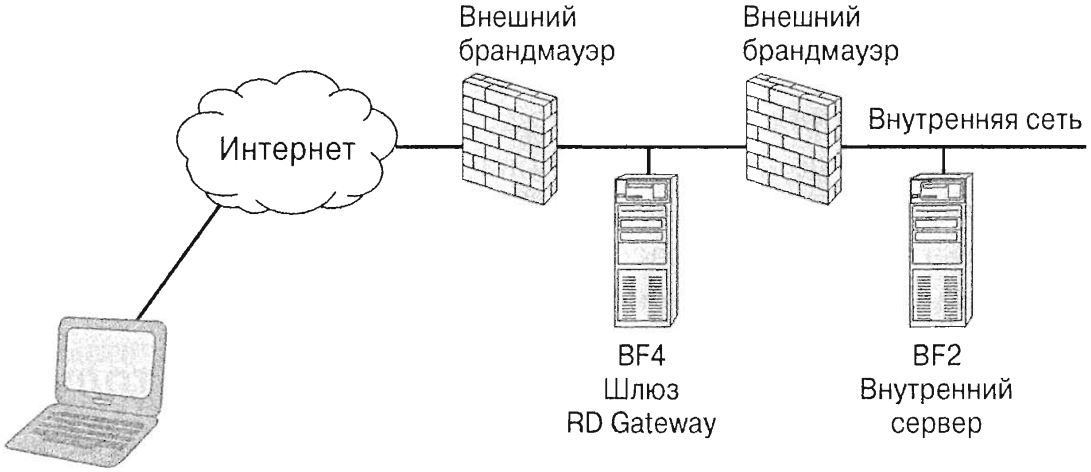


Рис. 17.25. RD Gateway обеспечивает доступ к внутреннему серверу

Для шифрования сеанса в HTTPS используется протокол защищенных сокетов (Secure Sockets Layer — SSL) и порт 443. Чтобы поддерживать трафик HTTPS, внешний брандмауэр должен открыть порт 443.

Сервер BF4 будет аутентифицировать клиента, а также играть роль шлюза к внутренним ресурсам. Шлюз RD Gateway можно сконфигурировать с политикой авторизации ресурсов с целью ограничения доступа одним сервером (например, BF2 на рисунке) или любыми ресурсами в сети.

Политики авторизации подключения к удаленному рабочему столу (Remote Desktop Connection Authorization Policies — RD CAP) применяются для ограничения круга лиц, имеющих право подключаться к серверу RD Gateway. Политики авторизации ресурсов удаленного рабочего стола (Remote Desktop Resource Authorization Policies — RD RAP) используются для ограничения круга серверов, к которым возможен доступ пользователя после его подключения.

Шлюз TS Gateway переименован в RD Gateway

Шлюз RD Gateway когда-то назывался шлюзом терминальных служб (Terminal Services Gateway — TS Gateway). Переименование Terminal Services в Remote Desktop Services повлияло на другие названия, в числе которых и RD Gateway.

В предшествующих версиях Windows было возможно дистанционно администрировать серверы из Интернета. Однако для этого нужно было открыть порт 3389 на брандмауэре (или уговорить сделать это администратора брандмауэра). Но каждый дополнительный открытый порт на брандмауэре увеличивает степень уязвимости, требуя выполнения дополнительных действий.

С точки зрения безопасности гораздо легче просто оставить этот порт закрытым. Хотя дистанционное администрирование через порт 3389 было удобным средством, часто оно блокировалась на сетевом брандмауэре с целью снижения связанных с этим рисков в плане безопасности.

Поскольку в RD Gateway применяется протокол RDP поверх HTTPS через порт 443, внешнему брандмауэру требуется лишь открытый порт 443. Порт 443 обычно открыт для обеспечения прохождения другого трафика HTTPS. Если порт 443 открыт для другого трафика HTTPS, то нет необходимости открывать дополнительные порты, чтобы пользоваться RDP поверх HTTPS.

Например, если бы компания применяла в качестве хоста веб-сервер, использующий HTTP и HTTPS, то порты 80 и 443 были бы открыты для поддержки этого веб-сервера. В таком случае можно было бы реализовать RD Gateway на каком-то сервере в DMZ без внесения изменений в настройки брандмауэра.

Даже если порт 443 еще не открыт, безопасность HTTPS хорошо понятна большинству администраторов. Администратору легче взвесить риски HTTPS и принять решение открыть этот порт, чем рассматривать возможность открытия порта 3389 для трафика дистанционного администрирования.

Клиент подключения к удаленному рабочему столу

В RD Gateway поддерживаются подключения из Remote Desktop Connection 6.0 и более поздних версий. Однако чтобы поддерживать все средства, доступные в RD

Gateway в версии Windows Server 2012 R2, рекомендуется применять Remote Desktop Protocol 8.0. Это предусмотрено в клиенте RDC, поставляемом вместе с Windows 8 и Windows Server 2012. Клиент RDP 8.0 также используется как дополнительный компонент для Windows 7 SP1 и Windows Server 2008 R2 SP1 (`http://support.microsoft.com/kb/2592687`).

Хотя перечисленные возможности наиболее эффективны, когда для управления рабочими столами и удаленными приложениями применяется Remote Desktop Services, администраторы также могут счесть их полезными. Ниже перечислены дополнительные возможности, которыми могут воспользоваться администраторы.

- **RemoteFX.** Технология RemoteFX расширяет визуальный пользовательский интерфейс. Появился ряд новых усовершенствований, касающихся RemoteFX:
  - поддержка WAN;
  - Network Auto Detect (автоматическое обнаружение сетей);
  - Adaptive Graphics (адаптивная графика);
  - Media Streaming (создание потоков медиа-данных);
  - перенаправление USB для виртуальных рабочих столов vGPU, не связанных с RemoteFX.
- **Поддержка вложенных сеансов**. Теперь есть возможность запускать сеанс удаленного рабочего стола изнутри другого сеанса удаленного рабочего стола.
- **Счетчики производительности для мониторинга квалификации пользователя.** Счетчики производительности позволяют администраторам контролировать и устранять проблемы, вызванные практическими действиями пользователя.

Службы и компоненты, требуемые RD Gateway

Шлюз RD Gateway требует наличия перечисленных ниже дополнительных служб ролей и компонентов на сервере Windows Server 2012 R2, где RD Gateway размещен (ранее в этом разделе речь шла о его установке).

- Роль Web Server (IIS):
  - Компонент Management Tools (Инструменты управления) для управления IIS
  - Служба Web Server (Веб-сервер) для поддержки веб-сайтов HTML и ASP.NET
- Роль Network Policy and Access Services (Службы сетевой политики и доступа): служба Network Policy Server (Сервер сетевой политики)
- Компонент RPC over HTTP Proxy (Прокси RPC поверх HTTP)
- Компонент Remote Server Administration Tools (Инструменты дистанционного администрирования сервера)

Когда вы добавляете роль RD Gateway, мастер установки напоминает о необходимости автоматически установить все требуемые роли, службы и компоненты. Вам не нужно устанавливать их по отдельности. Однако если они уже установлены, то мастер установки распознает, что они активны.

Политики, требуемые RD Gateway

Прежде чем пользователи смогут подключаться посредством RD Gateway, у вас должно быть развернуто, по меньшей мере, две политики.

- **RD Connection Authorization Policy (RD CAP) (Политика авторизации подключения к удаленному рабочему столу).** Политика RD CAP определяет пользователей, которые могут подключаться к серверу RD Gateway. Например, вы можете предоставить право подключаться каждому члену группы `Administrators` сервера RD Gateway или создать для этой цели глобальную группу доступа (например, `G RD Gateway Users`). Затем в эту новую глобальную группу можно поместить всех пользователей, которым необходимо предоставить доступ к подключению.
- **RD Resource Allocation Policy (RD RAP) (Политика выделения ресурсов удаленного рабочего стола).** Политика RD RAP определяет ресурсы, к которым могут иметь доступ пользователи после их подключения. Например, вы можете создать эту политику таким образом, чтобы администраторы могли дистанционно администрировать определенный сервер. Конкретный сервер указывается в RD RAP. Администраторы могли бы подключаться к этому серверу (но ни к какому другому серверу) посредством сервера RD Gateway.

  Можно также сконфигурировать RD RAP так, чтобы пользователи получили возможность подключаться к любому компьютеру в сети без каких-либо ограничений.

Активизация Remote Desktop Gateway

Выполните описанную ниже шаги, чтобы активизировать службу роли Remote Desktop Gateway на сервере Windows Server 2012 R2. Эти шаги также приведут к добавлению требуемых ролей, служб и компонентов, равно как RD CAP и RD RAP.

1. Запустите диспетчер серверов из панели задач.
2. Щелкните на ссылке Add Roles and Features (Добавить роли и компоненты).
3. Ознакомьтесь с информацией на экране Before you begin (Прежде чем начать) и щелкните на кнопке Next (Далее).
4. Выберите переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) и щелкните на кнопке Next.
5. Выберите сервер, на который будет выполняться установка, и щелкните на кнопке Next.
6. Раскройте роль Remote Desktop Services на экране Select Server Roles (Выбор серверных ролей) и отметьте флажок Remote Desktop Gateway (Шлюз удаленного рабочего стола). Щелкните на кнопке Next.
7. Вы получите уведомление о том, что может понадобиться установка дополнительных компонентов. Щелкните на кнопке Add Features (Добавить компоненты).
8. Когда всплывающее окно закроется, щелкните на кнопке Next.
9. На экране компонентов щелкните на кнопке Next.

10. Ознакомьтесь с информацией на экране Network Policy and Access Services (Службы сетевой политики и доступа) и щелкните на кнопке Next.
11. Служба роли Network Policy (Сетевая политика) должна быть отмечена; щелкните на кнопке Next.
12. Просмотрите экран Confirmation (Подтверждение), отметьте флажок для перезапуска сервера в случае необходимости и щелкните на кнопке Install (Установить).

Через несколько минут и перезагрузки на сервере появится установленная служба роли Remote Desktop Gateway. Для доступа к ней можно нажать клавишу <Windows>. Вы увидите новую кнопку в стиле Metro под названием Remote Desktop Gateway, как показано на рис. 17.26.

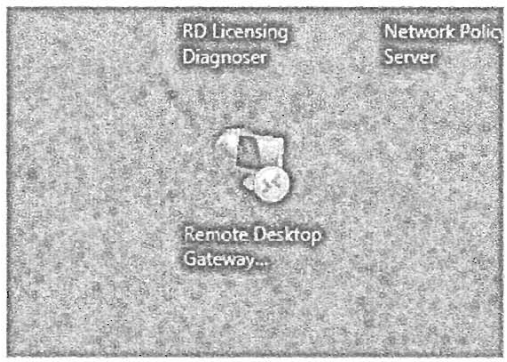


Рис. 17.26. Кнопка Remote Desktop Gateway

Открыв диспетчер шлюза удаленного рабочего стола (RD Gateway Manager), вы увидите, что он очень похож на инструмент Group Policy Management (Управление групповой политикой). С помощью этого инструмента можно управлять всеми аспектами RD Gateway.

В левой панели окна вы увидите имя своего сервера с двумя расположенными ниже папками: Policies (Политики) и Monitoring (Мониторинг). Если вы щелкнете на имени сервера, то увидите информацию о текущем подключении и требуемые дополнительные конфигурации (рис. 17.27).

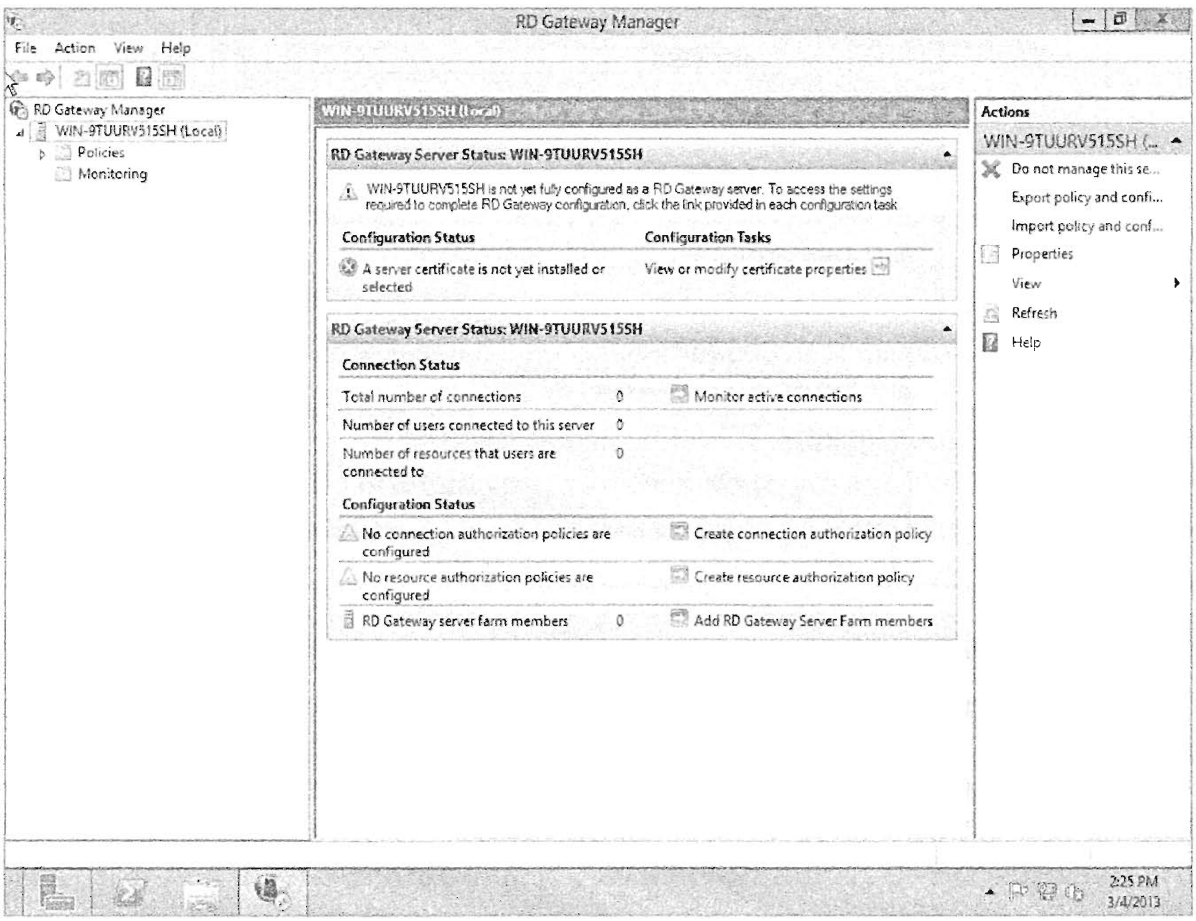


Рис. 17.27. Информация о подключении шлюза

Как видно на рис. 17.27, нам остается еще сконфигурировать сертификат для шлюза.

1. Щелкните на ссылке View or modify certificate properties (Просмотреть или модифицировать свойства сертификата).

   Отобразится экран Choose a Server Authentication Certificate for SSL Encryption (Выбор сертификата аутентификации сервера для шифрования SSL). Вы можете установить существующий сертификат, создать самозаверяющий сертификат либо импортировать сертификат.

   Сертификат можно приобрести у внешнего CA или получить его от внутреннего CA.

2. В данном случае выберите вариант Create a self-signed certificate for SSL encryption (Создать самозаверяющий сертификат для шифрования SSL). Щелкните на кнопке Create and Import Certificate (Создать и импортировать сертификат).

3. На рис. 17.28 вы видите, что мы можем создать самозаверяющий сертификат с установками по умолчанию. Щелкните на кнопке OK.

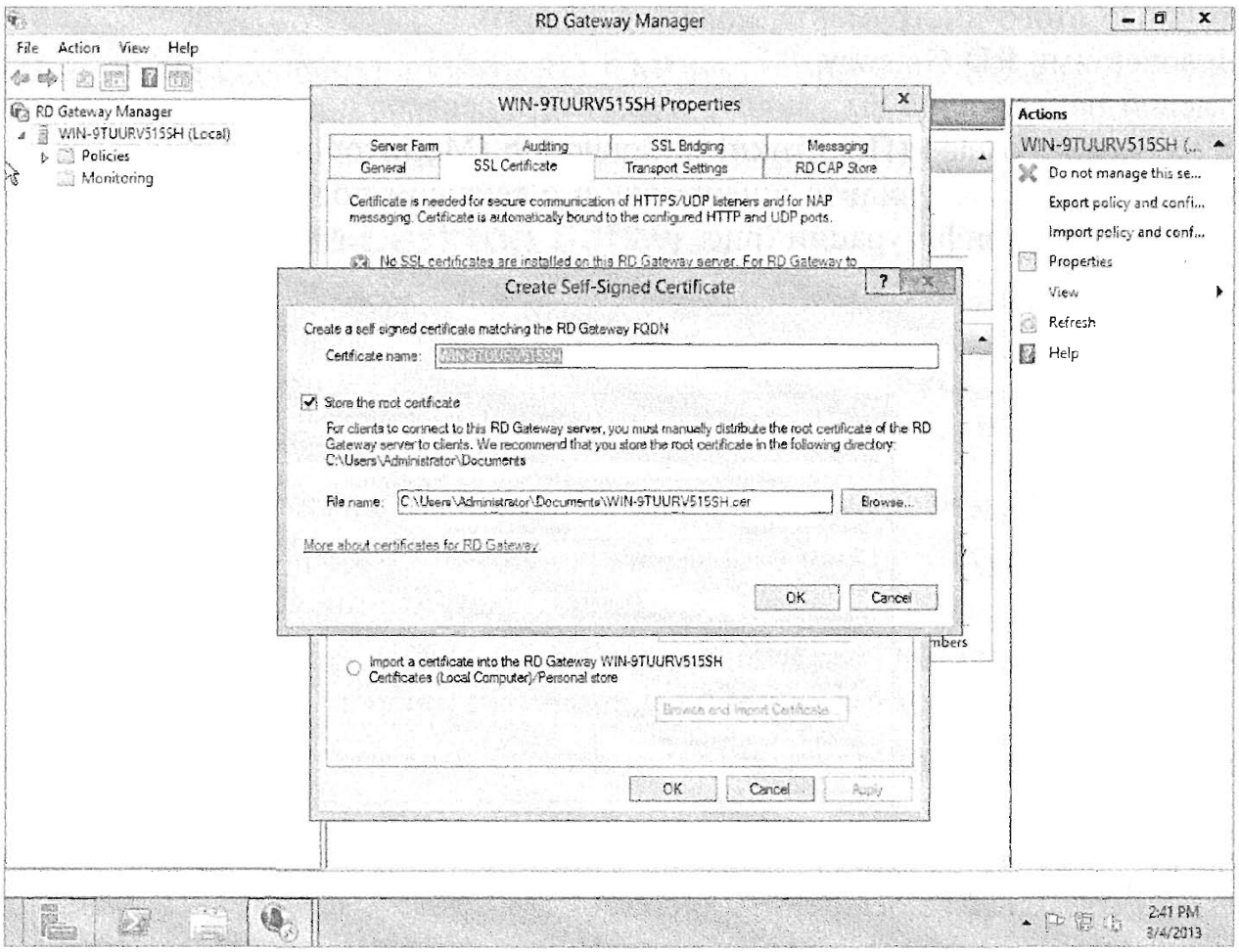


Рис. 17.28. Создание самозаверяющего сертификата

На рис. 17.29 видно, что сертификат был успешно установлен.

Как показано на рис. 17.30, нам еще предстоит исследовать несколько конфигураций. Одна из них касается политики авторизации подключения к удаленному рабочему столу (RD CAP), а другая — политики авторизации ресурсов удаленного рабочего стола (RD RAP).

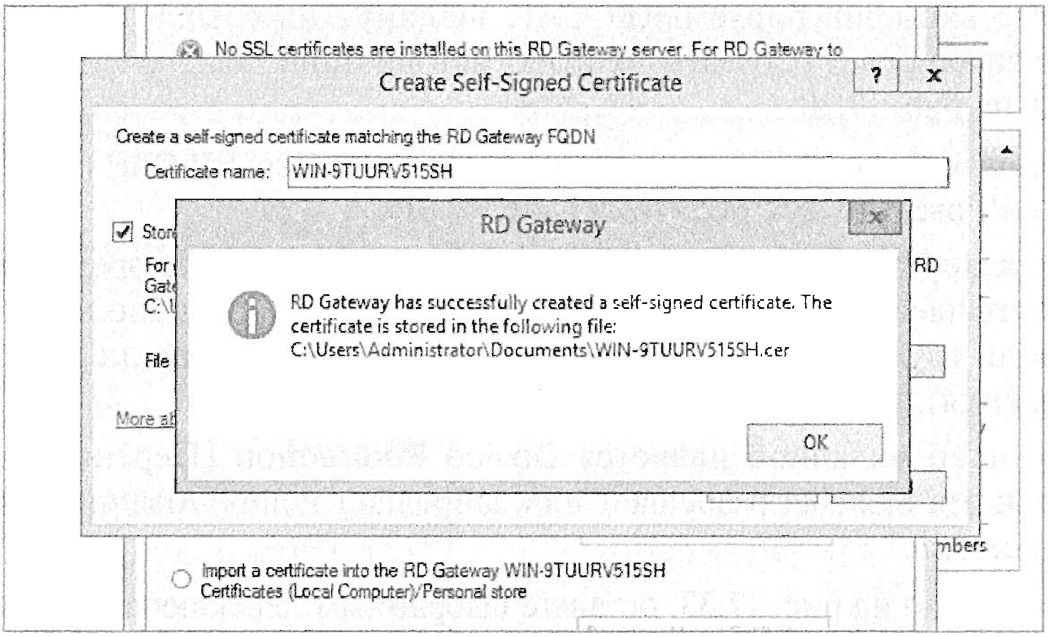


Рис. 17.29. Сертификат, установленный надлежащим образом

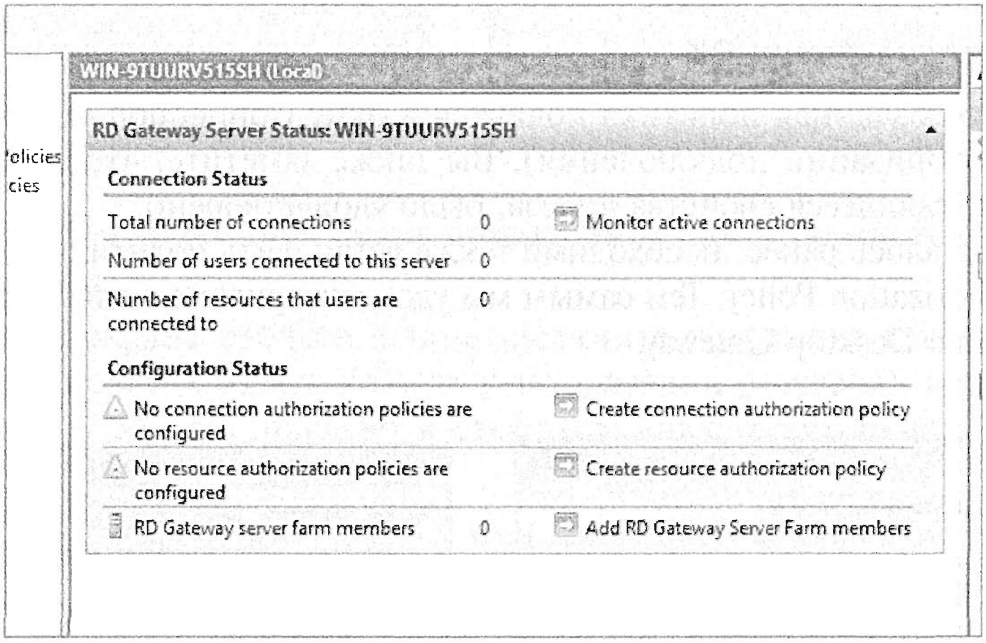


Рис. 17.30. Требования, которые необходимо удовлетворить для завершения конфигурирования шлюза

Те из вас, кто знаком с Windows Server 2008 R2, наверняка заметили, что все они, начиная с сертификата, конфигурируются в ходе установки роли Remote Desktop Services. В Windows Server 2012 R2 они конфигурируются в диспетчере шлюза (Gateway Manager).

Получение сертификата от CA

Самозаверяющие сертификаты удобны при тестировании, но их не рекомендуется использовать в производственной среде. Вместо этого вы должны получить сертификат в центре сертификации (CA). Поскольку сертификат, применяемый RD Gateway для администрирования, будет использоваться только администраторами, вы можете создать этот сертификат с помощью внутреннего CA, а не приобретать его у стороннего CA.

1. Давайте сконфигурируем RD CAP, щелкнув на ссылке Create connection authorization policy (Создать политику авторизации подключения), которая показана на рис. 17.30.
2. На вкладке General (Общие) диалогового окна New RD CAP (Новая политика RD CAP) введите имя политики (рис. 17.31).

   На вкладке Requirements (Требования) можно добавить разрешения для групп и указать членство для клиентских компьютеров. Как видно на рис. 17.32, мы добавили группу `Remote Management Users` (Пользователи дистанционного управления).

   Следующей вкладкой является Device Redirection (Перенаправление устройств); эта вкладка разрешает или запрещает использование этих устройств в ходе сеанса.
3. Как показано на рис. 17.33, оставьте выбранным переключатель, как предлагается по умолчанию, чтобы разрешить применение всех клиентских устройств.
4. Последней является вкладка Timeouts (Тайм-ауты). Установите желаемым образом тайм-ауты для своего сеанса (рис. 17.34).
5. Щелкните на кнопке OK.

Только что созданная политика появится в окне Connection Authorization Policy (Политика авторизации подключения). Вы также заметите, что соответствующее требование, касающееся свойства шлюза, было удовлетворено.

Как упоминалось ранее, необходимо также установить политику Remote Desktop Resource Authorization Policy. Тем самым мы удовлетворим последнее требование настройки Remote Desktop Gateway.

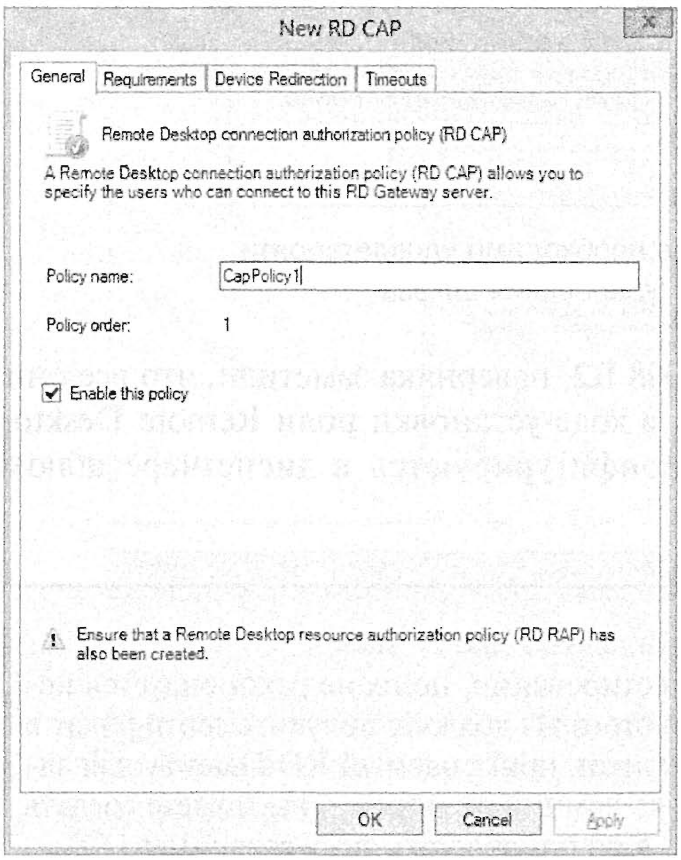


Рис. 17.31. Ввод имени политики

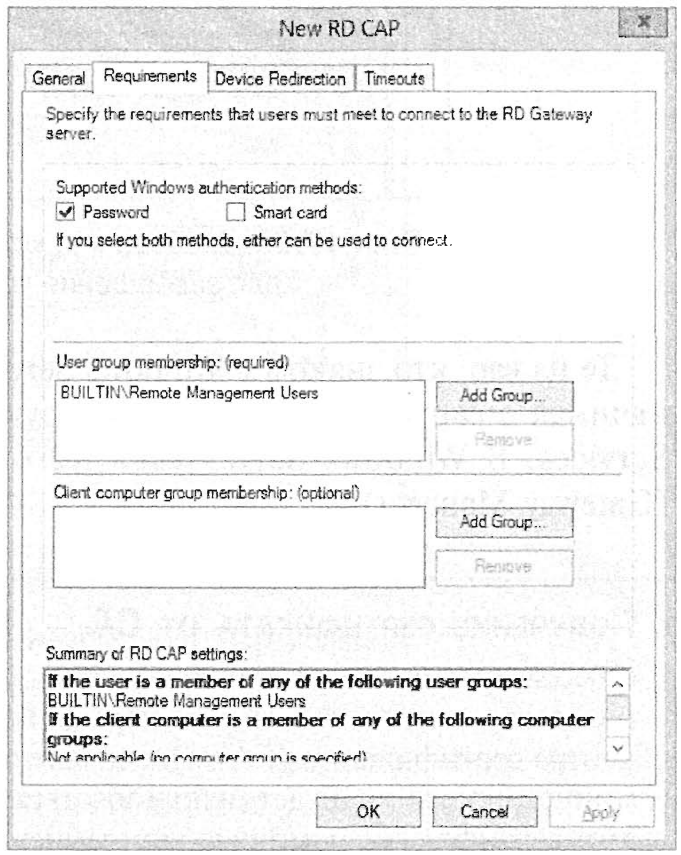


Рис. 17.32. Вкладка Requirements

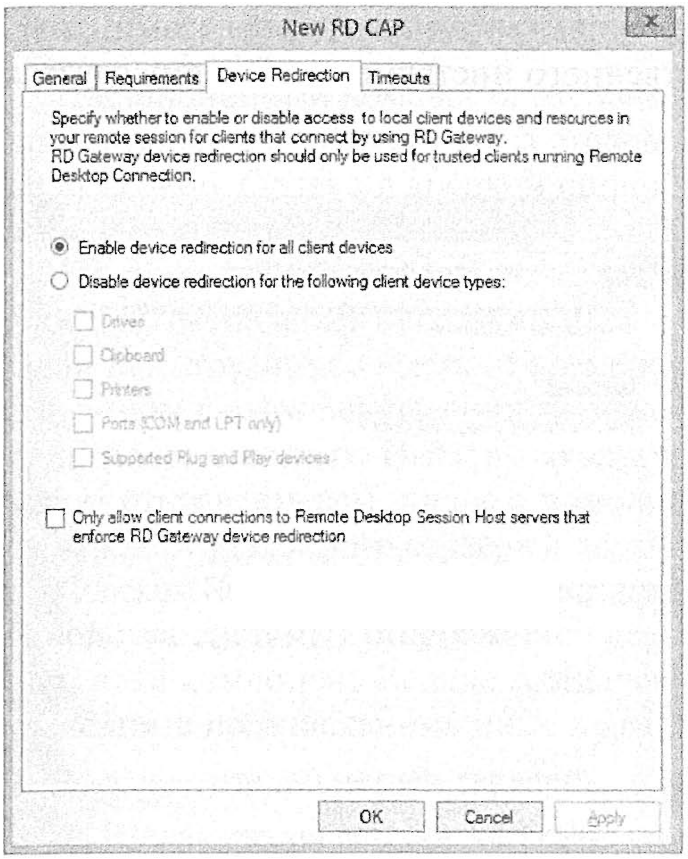


Рис. 17.33. Вкладка Device Redirection

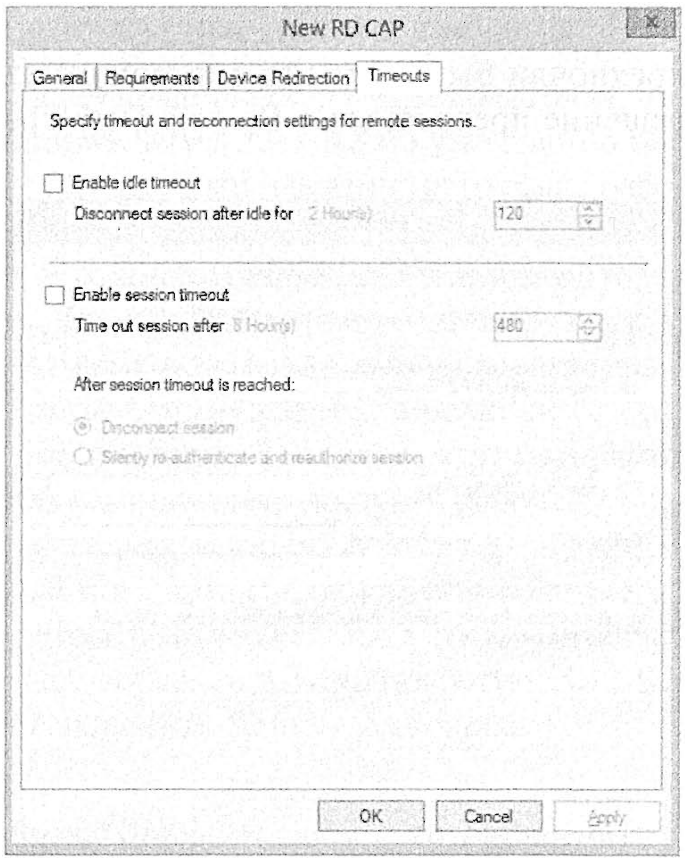


Рис. 17.34. Вкладка Timeouts

Процедура конфигурирования очень похожа на ту, которую мы только что выполнили для RD CAP.

1. На итоговом экране свойств шлюза щелкните на ссылке Create Resource Authorization Policy (Создать политику авторизации ресурсов), которая показана на рис. 17.30. Это приведет к открытию диалогового окна New RD RAP (Новая политика RD RAP).
2. На вкладке General (Общие) введите имя политики и ее описание (рис. 17.35).
3. Вкладка User Groups (Пользовательские группы) предназначена для добавления группового разрешения для этой политики. Как показано на рис. 17.36, добавьте группу `Remote Management Users` (Пользователи дистанционного управления).
4. На вкладке Network Resource (Сетевой ресурс) добавьте группы сетевых ресурсов.
5. Выберите переключатель Allow users to connect to any network resource (Разрешить пользователям подключаться к любому сетевому ресурсу), как показано на рис. 17.37.
6. Последняя вкладка, Allowed Ports (Разрешенные порты), предназначена для выбора разрешенных портов; выберите переключатель, разрешающий только порт 3389 (рис. 17.38).

Поздравляем! Ваш шлюз сконфигурирован и готов к обработке подключений.

Remote Desktop Connection и Remote Gateway — ценные инструменты, применяемые для дистанционного администрирования серверов. Тем не менее, каждый из них будет запускаться в виде одиночных экземпляров.

Но бывают ситуации, когда приходится управлять многими серверами, и вы предпочли бы делать это с помощью единственного инструмента. В таких случаях решение предоставляет Remote Desktops.

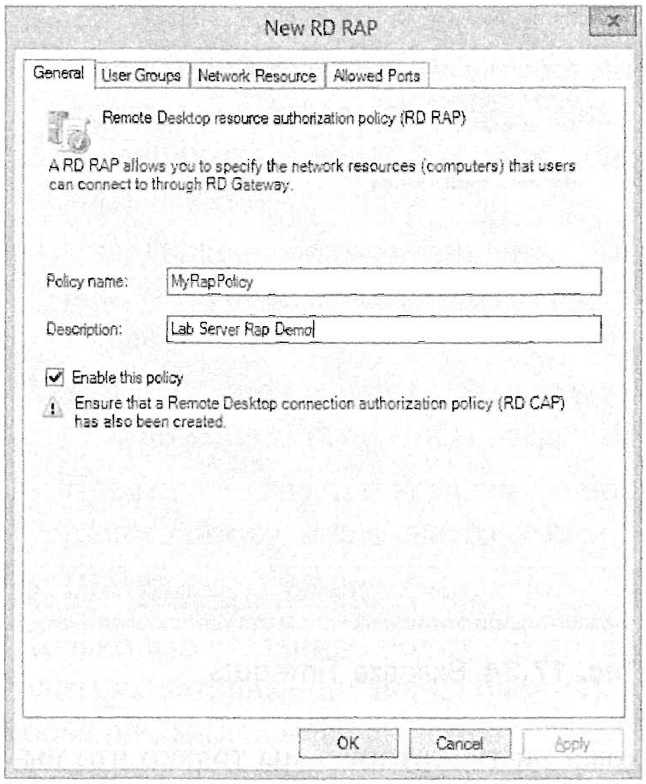


Рис. 17.35. Ввод имения и описания политики

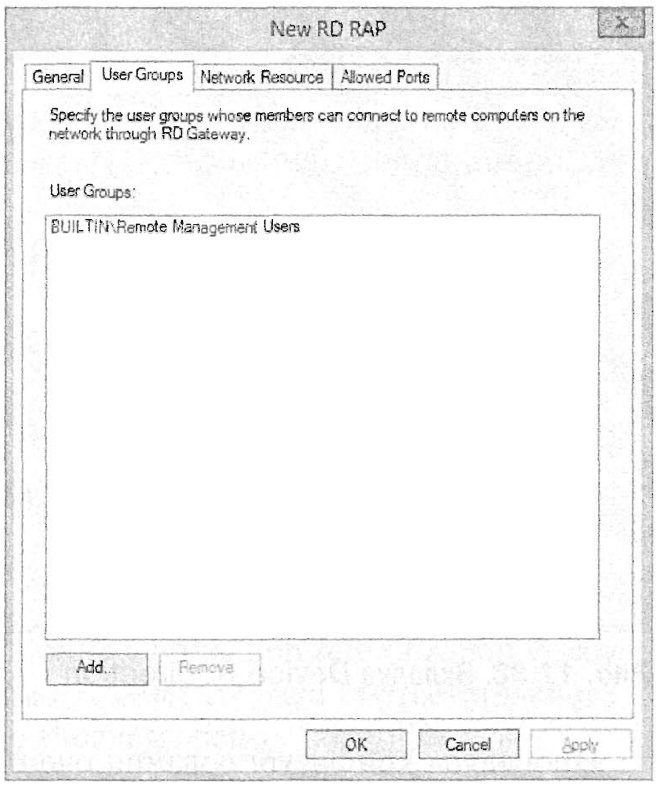


Рис. 17.36. Добавление группы на вкладке User Groups

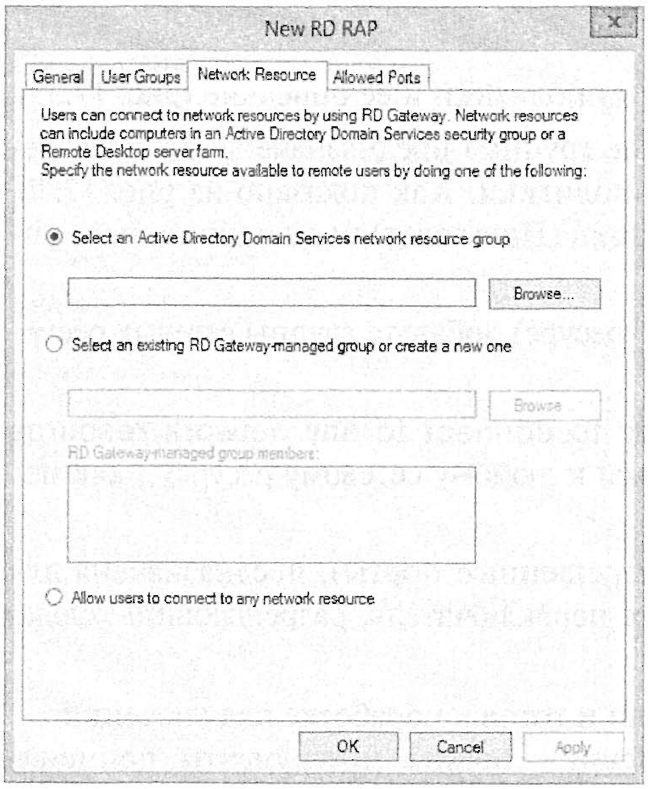


Рис. 17.37. Вкладка Network Resource

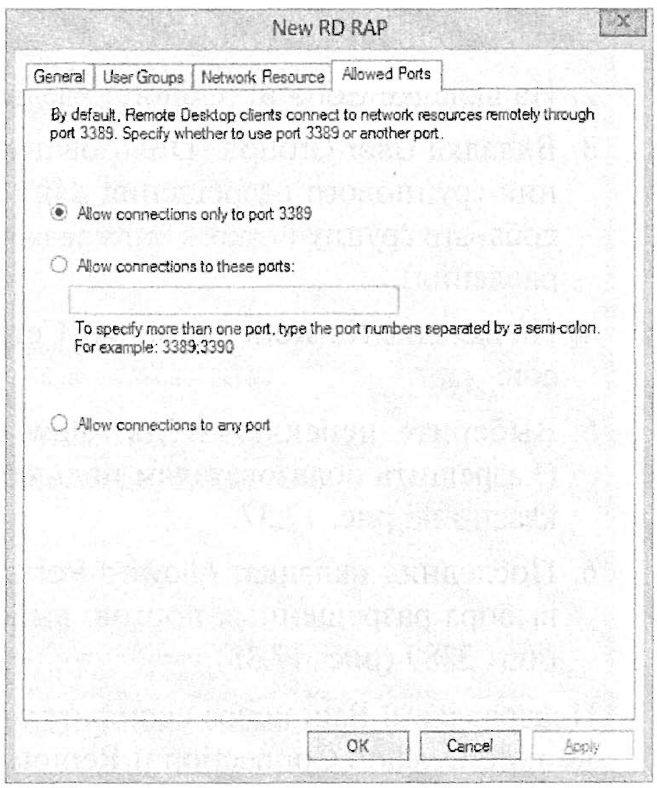


Рис. 17.38. Вкладка Allowed Ports

Конфигурирование сервера для дистанционной помощи

Дистанционный помощник (Remote Assistance) является основным средством, используемым в системах рабочих столов. В Windows Server 2012 R2 по умолчанию оно не включено. Однако в крупной организации с младшими администраторами, работающими в удаленных местах, это средство может оказаться чрезвычайно удобным.

Представьте, например, что вы работаете в головном офисе компании, которая вдобавок располагает периферийным офисом, где находятся только 20 сотрудников. Один из сотрудников время от времени выполняет рутинные задачи на сервере, размещенном в этом периферийном офисе, но иногда он нуждается в помощи со стороны более опытных. Имея включенное средство Remote Assistance, этот сотрудник может отправлять вам запрос о помощи. Затем вы получаете доступ к рабочему столу нужного удаленного сервера и демонстрируете, как выполнить задачу.

Флажок Remote Assistance (Дистанционный помощник) в окне System Properties (Свойства системы) отображается серым цветом и не может быть отмечен до тех пор, пока компонент Remote Assistance не будет добавлен в Windows Server 2012 R2. Выполните перечисленные ниже шаги, чтобы включить Remote Assistance.

1. Запустите диспетчер серверов.
2. Щелкните на ссылке Add roles and features (Добавить роли и компоненты).
3. Принимайте все стандартные настройки и щелкайте на кнопке Next (Далее), пока не доберетесь до экрана Select features (Выбор компонентов).
4. Отметьте флажок Remote Assistance (Дистанционный помощник) и щелкните на кнопке Next.
5. На экране Confirmation (Подтверждение) щелкните на кнопке Install (Установить).
6. Когда мастер установки завершит работу, щелкните на кнопке Close (Закрыть).

После добавления компонента Remote Assistance на соответствующем сервере должен быть включен дистанционный помощник. Проверить это можно, выполнив следующие действия.

1. Нажмите клавишу <Windows>, щелкните правой кнопкой мыши на значке Computer (Компьютер) и выберите в контекстном меню пункт Properties (Свойства).
2. Щелкните на кнопке Remote Settings (Удаленные параметры).
3. Проверьте, отмечен ли флажок Allow Remote Assistance connections to this computer (Разрешить подключения к этому компьютеру для получения дистанционной помощи).
4. Щелкните на кнопке Advanced (Дополнительно). Проверьте, отмечен ли флажок Allow this computer to be controlled remotely (Разрешить дистанционное управление этим компьютером).

   Стандартный срок действия приглашений составляет шесть часов, но его можно изменить. По истечении этого лимита времени данное приглашение больше нельзя будет применять для подключения.

Теперь этот сервер сконфигурирован на использование дистанционной помощи. Чтобы инициировать сеанс Remote Assistance, пользователь должен отправить запрос дистанционной помощи.

Отправка запроса дистанционной помощи

Пользователь, которому необходима помощь, должен выполнить описанные ниже шаги, чтобы создать запрос дистанционной помощи и начать процесс.

1. Щелкните на кнопке Start (Пуск), введите в поле Run (Выполнить) команду `msra` и нажмите клавишу <Enter>. Откроется диалоговое окно Windows Remote Assistance (Дистанционная помощь Windows).
2. Щелкните на ссылке Invite someone you trust to help you (Пригласить того, кому вы доверяете, для оказания помощи).
3. Щелкните на ссылке Save this invitation as a file (Сохранить приглашение в файле).
4. Перейдите в подходящее место на своем жестком диске. Файл приглашения по умолчанию называется `Invitation.msrcIncident`, но при желании имя можно изменить. Щелкните на кнопке Save (Сохранить).
5. Автоматически создается пароль, который не может быть изменен. Этот пароль понадобится сообщить тому, кто будет оказывать помощь.
6. Отправьте приглашение тому, кто окажет помощь, в почтовом вложении или поместите приглашение в общую папку, доступную этому человеку.

Затем пользователь, нуждающийся в помощи, должен ожидать ответа от того, кто окажет помощь.

Выдача ответа на запрос дистанционной помощи

Человек, оказывающий помощь, может выполнить следующие действия совместно с пользователем, запросившим помощь, чтобы начать сеанс Remote Assistance.

1. Дважды щелкните на приглашении, которое получено от лица, запросившего помощь.

   Это приглашение могло быть получено по электронной почте или размещено в общей папке. Открытие приглашения может занять некоторое время.

2. Введите пароль в диалоговом окне Windows Remote Assistance (Дистанционная помощь Windows) и щелкните на кнопке OK.

   Если вы ввели неправильный пароль, то немедленно получите соответствующее уведомление.

   На экране пользователя, запросившего помощь, появится диалоговое окно с вопросом, желает ли он разрешить подключение.

3. Пользователь должен щелкнуть на кнопке Yes (Да).

   Начиная с этого момента, вы будете видеть все, что находится на рабочем столе пользователя, но у вас не будет возможности взаимодействовать с этим рабочим столом.

4. Щелкните на кнопке Request Control (Запросить управление) в верхней части окна Windows Remote Assistance.

   На экране пользователя, запросившего помощь, появится диалоговое окно с вопросом, желает ли он совместно управлять рабочим столом с лицом, предлагающим помощь.

5. Пользователь должен щелкнуть на кнопке Yes.

   Обратите внимание, что пользователь имеет полный контроль и может отклонить запрос. Однако поскольку именно он запросил помощь и сообщил пароль, предполагается, что он должен щелкнуть на кнопке Yes.

Тот, кто согласился оказать помощь, теперь может управлять мышью на удаленном компьютере. На рис. 17.39 показано диалоговое окно Windows Remote Assistance, которое видит тот, кому оказывают помощь.

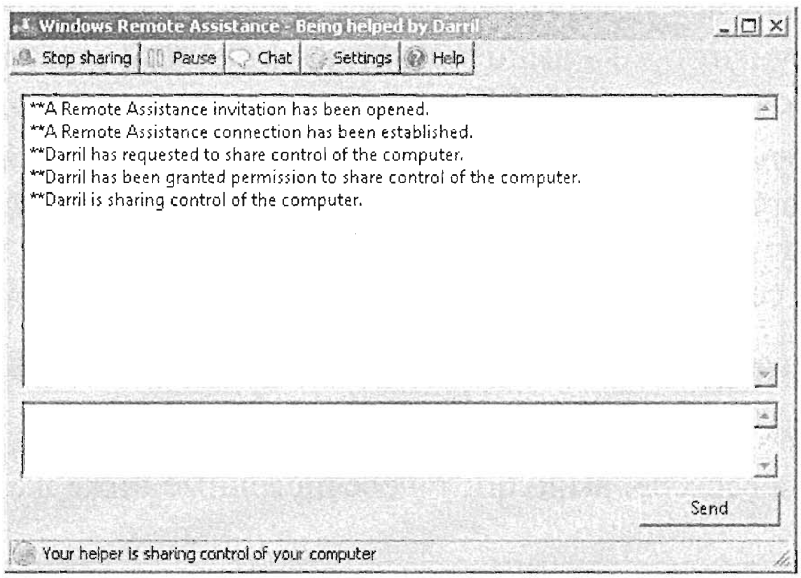


Рис. 17.39. Сеанс Remote Assistance на удаленном компьютере

Далее лицо, оказывающее помощь, может управлять мышью и клавиатурой удаленного компьютера, чтобы продемонстрировать решение любых задач. В этом заключается суть совместного управления удаленным компьютером. Другими словами, рабочим столом может управлять и тот, кто запросил помощь, и тот, кто ее оказывает.

Неплохо, если лицо, запросившее помощь, и лицо, оказывающее помощь, в ходе этого процесса могут общаться по телефону, но это не является обязательным требованием. Диалоговые окна Windows Remote Assistance включают средство Chat (Диалог), которое позволяет каждому из пользователей вводить с клавиатуры вопросы и комментарии.

Лицо, оказывающее помощь, может продемонстрировать выполнение той или иной задачи, а потом просто ввести текст "А теперь попробуйте сделать то же самое" и наблюдать за всем, что происходит на экране удаленного рабочего стола. Лицо, оказывающее помощь, может прекратить пользоваться мышью, а лицо, запросившее помощь, может попытаться воспроизвести на своем компьютере ранее продемонстрированные действия. Кроме того, лицо, запросившее помощь, может в любой момент прекратить сеанс, щелкнув на кнопке Stop Sharing (Остановить совместное использование) или Pause (Приостановить).

Служба дистанционного управления Windows

Служба дистанционного управления Windows (Windows Remote Management Service — WinRM) позволяет выдавать любую команду командной строки с одного компьютера на удаленный компьютер.

Например, вы можете работать на компьютере под управлением Windows 7 или Windows 8, но хотите запросить какую-то информацию из удаленного сервера. Если этот сервер был сконфигурирован с WinRM, то вы можете запустить команду `WinRS` из настольной системы и получить результаты так, как если бы вы работали непосредственно за этим компьютером или были подключены к нему с помощью RDC.

Одно из преимуществ такого подхода заключается в том, что вам не приходится занимать один из двух удаленных сеансов для сервера или даже запускать RDC. Вы просто вводите команду в окне командной строки.

Ниже описаны две команды, используемые Windows Remote Management Service.

- **`WinRM`**. Инструмент `WinRM` выполняется на удаленном сервере и позволяет этому серверу прослушивать WinRS-запросы и отвечать на них.
- **`WinRS`**. Инструмент `WinRS` запускается из командной строки на рабочем столе или другом сервере, к которому у администратора есть доступ. Этот инструмент позволяет администратору выполнять любые команды командной строки на удаленном сервере.

Включение WinRM

В Windows Server 2012 R2 служба WinRM по умолчанию не включена. Чтобы включить WinRM на сервере, выполните перечисленные ниже шаги.

RD Gateway включает WinRM

По умолчанию служба WinRM не включена, поэтому удаленный доступ с целью управления не разрешен. Однако если вы выполнили описанную ранее последовательность действий для включения RD Gateway, то увидите, что на том же сервере активизирована также и служба WinRM. Средство RD Gateway использует службу Windows Remote Management и включает ее при установке службы роли RD Gateway. Если вы начнете выполнять приведенные далее шаги, то будете проинформированы о том, что служба WinRM уже сконфигурирована.

---

1. Выберите Power Shell и введите **`cmd`** в командной строке.
2. Наберите следующую команду и нажмите <Enter>:

   ```
   WinRM qc
   ```

   У вас будет запрошено разрешение на внесение следующих изменений в систему.

   - Создание прослушивателя WinRM на `HTTP://*`, чтобы получить доступ к запросам WS-Man к любому IP-адресу на этой машине.
   - Создание исключения брандмауэра для WinRM.
   - Конфигурирование политики `LocalAccountTokenFilterPolicy` для выдачи административных прав дистанционно локальным пользователям.
3. Наберите **`Y`** и нажмите <Enter>, чтобы разрешить внесение этих изменений.

   Вы увидите сообщение о состоянии, указывающее на то, что изменения были внесены.

4. Введите **WinRM /?**, чтобы просмотреть справочные сведения, доступные для инструмента командной строки Windows Remote Management.

   WinRM включает обширный набор команд, а справочный файл поможет в случае необходимости получить дополнительную информацию.

5. Введите следующую команду для перечисления свойств WinRM:

   ```
   WinRM enumerate WinRM/config/listener
   ```

   Обратите внимание на наличие пробела между WinRM и enumerate и еще одного пробела между enumerate и WinRM; других пробелов в команде нет.

   Эта команда предоставит некоторые детали относительно того, как сконфигурирована данная служба, и вы сможете также удостовериться в том, что она включена для прослушивания транспорта HTTP, используя все доступные IP-адреса в системе. Команду можно также ввести, указав только первую букву слова *enumerate* (e):

   ```
   WinRM e WinRM /config/listener
   ```

   Формат вывода можно изменять, модифицируя переключатель -format. По умолчанию вывод представлен в текстовом формате, но допускается выводить также простой XML (-format:#XML) или форматированный XML (-format:#pretty).

6. Попробуйте выполнить следующие команды:

   ```
   WinRM e WinRM /config/listener -format:#text
   WinRM e WinRM /config/listener -format:#xml
   WinRM e WinRM /config/listener -format:#pretty
   ```

Хотя с помощью WinRM на сервере можно делать гораздо больше того, о чем речь шла выше, основное назначение этого инструмента для удаленного администратора связано с включением прослушивателя с помощью команды quickconfig. Сделав это, вы, скорее всего, переключите внимание на клиента, где будет происходить фактическое администрирование.

Использование WinRS

Оболочка удаленных команд Windows (Windows Remote Shell — WinRS) используется для выполнения команд на удаленном сервере, который сконфигурирован с WinRM. Например, WinRS можно было бы применять из системы Windows 7 или Windows 8 для выполнения команд на удаленном сервере.

Команды WinRS главным образом имеют следующий формат:

```
WinRS -r:имя_сервера команда
```

Переключатель -r используется для идентификации имени удаленного сервера. Несмотря на наличие дополнительных переключателей, -r применяется чаще других.

Выдача команд WMIC с помощью WinRS

Командой WinRS может быть любая команда, которую вы выдаете из командной строки. Например, вы можете использовать инструмент WMIC (Windows Management Instrumentation Command-line — командная строка инструментария управления Windows) для документирования служб, функционирующих на компьютерах.

Прежде чем применять WinRS, вы можете воспользоваться этой командой, чтобы посмотреть, как WMIC можно применять для документирования информации о службах, выполняющихся в любой системе. Откройте окно командной строки и введите следующую команду:

```
Wmic /output:services.htm /node:localhost service list brief /format:htable
```

Команда создает файл в формате HTML по имени `services.htm`. Вы можете просмотреть его, введя **`services.htm`** в командной строке, что приведет к запуску браузера Internet Explorer, который отобразит соответствующий документ. В этом документе будут перечислены все службы в данной системе, а также их режим запуска, состояние и другие сведения.

Воспользуйтесь той же командой, чтобы документировать службы удаленного компьютера, который был сконфигурирован с WinRS. Замените `Srv2012` именем сервера, который вы сконфигурировали с WinRS, и измените имя HTML-файла:

```
WinRS -r:Srv2012 Wmic /output:Srv2012services.htm
  /node:Srv2012 service list brief /format:htable
```

Чтобы просмотреть содержимое этого файла, введите его имя в командной строке — `Srv2012services.htm` в данном примере.

Если вас интересует более подробная информация о службах, измените `list brief` на **`list full`**. Этот простой инструмент позволяет легко получить важную документацию по многим серверам, которую можно просто распечатать или сохранить.

Выдача команд PowerShell с помощью WinRS

Несмотря на все богатство возможностей WMIC, это не единственная команда, которой вы можете воспользоваться. Любую команду, которую можно ввести на сервере, допускается вводить дистанционно с помощью WinRS. Это относится и к командам PowerShell. По приведенной ниже ссылке доступен список командлетов PowerShell:

```
http://msdn.microsoft.com/en-us/library/windows/desktop/ee309371(v=vs.85).aspx
```

Команды PowerShell соответствуют формату "глагол-существительное". Глагол указывает действие, а существительное идентифицирует объект, в отношении которого действие будет выполнено.

Самым популярным глаголом является `get`, и если вы введете **`get-`** в командной строке PowerShell, то можете пройтись с помощью <Tab> по всем существительным, ассоциированным с глаголом `get`.

К числу остальных глаголов относятся `set`, `copy`, `move` и многие другие. Вы можете проделывать то же самое действие с любым из этих глаголов: ввести интересующий глагол с дефисом (-) и пройтись с помощью <Tab> по всем возможным существительным, связанным с этим глаголом. Полный список глаголов можно найти на следующей странице MSDN:

```
http://msdn.microsoft.com/en-us/library/ms714428(VS.85).aspx
```

Например, чтобы выяснить состояние служб в системе, введите следующую команду PowerShell в окне командной строки PowerShell:

```
Get-Service
```

Вам даже не понадобится вводить название команды полностью. Достаточно просто ввести `Get-S` и нажать <Tab>.

Эта команда выведет список всех служб в системе с указанием состояния (функционирует или остановлена), имени и отображаемого имени. Используя такой подход в сочетании с WinRS, можно запустить ту же команду дистанционно:

```
WinRS -r:SRV2012 PowerShell Get-Service
```

Если вы хотите перенаправить результаты в файл, добавьте символ перенаправления (>), как показано ниже:

```
WinRS -r:SRV2012 PowerShell Get-Service > services.txt
```

Вывод сохранится в файле по имени `services.txt`. Затем этот файл можно открыть из командной строки с помощью Notepad:

```
Notepad services.txt
```

Инструменты дистанционного администрирования серверов

Инструменты дистанционного администрирования серверов (Remote Server Administration Tools — RSAT) — это то, что вам нужно для управления ролями и компонентами на сервере Windows Server 2012 R2 из настольной операционной системы.

Несмотря на то что Remote Desktop Connection и Remote Desktops позволяют подключаться к рабочему столу сервера, иногда бывает нужно просто выполнить одиночную задачу вроде переустановки пароля для учетной записи пользователя или проверки корректности конфигурации DNS.

В состав RSAT входят такие инструменты, как ADUC (Active Directory Users and Computers — Пользователи и компьютеры Active Directory) и консоль DNS. После установки RSAT на рабочем столе можно запустить ADUC для манипулирования учетными записями пользователей или открыть консоль DNS, чтобы проверить правильность конфигурации DNS.

Для запуска установленных инструментов пользователям по-прежнему требуются подходящие разрешения. Например, младший администратор, который устанавливает эти инструменты на своей настольной системе, не будет добавлен в группу `Enterprise Admins` (Администраторы предприятия) и не сможет выполнять все, что ему вздумается, в лесе.

Инструменты, доступные в RSAT, могут применяться для управления ролями и компонентами Windows Server 2012 R2.

Вопросы совместимости RSAT

Инструменты RSAT не совместимы с пакетом инструментов администрирования (Administration Tools Pack), используемым для дистанционного администрирования серверов Windows Server 2000 и Windows Server 2003. Если эти инструменты установлены в системе, вы должны удалить их, прежде чем приступать к установке RSAT.

Кроме того, RSAT не позволит дистанционно управлять сервером с ролью Streaming Media Services (Службы потокового медиа). Для роли Streaming Media Services предусмотрены отдельные инструменты дистанционного администриро-

вания серверов, которые можно загрузить и установить для управления сервером Windows Server 2012 R2, размещающем роль Streaming Media Services.

За более подробными сведениями о проблемах с сервером роли Streaming Media Services можно обратиться к статье по адресу `http://support.microsoft.com/kb/934518`. Информация об инструментах RSAT находится ближе к концу этой статьи.

Инструменты RSAT

После установки RSAT в настольной системе вы получите доступ к полному комплекту инструментов, который можно обнаружить на сервере Windows Server 2012 R2 со всеми установленными ролями и компонентами. При условии, что на удаленном сервере установлена требуемая роль или компонент, для его администрирования можно применять инструмент RSAT клиентской стороны.

Другими словами, если на сервере функционирует роль DHCP, то для ее дистанционного администрирования можно использовать консоль DHCP. Однако если этот сервер не является сервером DHCP, то с помощью консоли DHCP, установленной RSAT, сделать его сервером DHCP не получится.

В приведенном ниже списке перечислены некоторые часто применяемые инструменты, доступные в RSAT. Список не является исчерпывающим, а представляет собой лишь подборку распространенных инструментов. Полный перечень инструментов можно найти в статье по адресу `http://support.microsoft.com/kb/941317`.

- **Active Directory Domain Services Tools (Инструменты служб доменов Active Directory).** Инструменты AD DS включают Active Directory Users and Computers (Пользователи и компьютеры Active Directory), Active Directory Domains and Trusts (Домены и доверительные отношения Active Directory), Active Directory Sites and Services (Сайты и службы Active Directory), а также другие оснастки и инструменты командной строки для дистанционного управления службами доменов Active Directory.
- **Active Directory Certificate Services Tools (Инструменты для служб сертификатов Active Directory).** К числу этих инструментов относятся инструменты Active Directory Certification Authority (Центр сертификации Active Directory), используемые для центров сертификации предприятий, и инструменты для автономных центров сертификации.
- **Dynamic Host Configuration Protocol Server Tools (Инструменты для сервера протокола динамической конфигурации хостов).** В их состав входит оснастка DHCP.
- **Domain Name System Server Tools (Инструменты для сервера системы доменных имен).** Инструменты DNS включают оснастку DNS Manager и инструмент командной строки `Dnscmd.exe`.
- **File Services Tools (Инструменты для файловых служб).** К числу этих инструментов относятся оснастка Share and Storage Management (Управление общим доступом и хранением), инструменты для распределенной файловой системы (Distributed File System) и инструменты для диспетчера ресурсов файлового сервера (File Server Resource Manager).

- **Network Policy and Access Services Tools (Инструменты для служб сетевой политики и доступа).** Для службы сетевой политики и доступа предусмотрена оснастка Routing and Remote Access (Маршрутизация и удаленный доступ).
- **Remote Desktop Services Tools (Инструменты для служб удаленных рабочих столов).** В их состав входят оснастки Remote Desktops и Remote Desktop Services Manager.
- **BitLocker Drive Encryption Tools (Инструменты для шифрования дисков BitLocker).** В состав включен сценарий `Manage-bde.wsf` для BitLocker Drive Encryption.
- **Failover Clustering Tools (Инструменты для кластеризации с обходом отказа).** Эти инструменты включают оснастку Failover Cluster Manager и инструмент командной строки `Cluster.exe`.
- **Group Policy Management Tools (Инструменты для управления групповой политикой).** В их состав входят Group Policy Management Console (Консоль управления групповой политикой), Group Policy Management Editor (Редактор управления групповыми политиками) и Group Policy Starter GPO Editor (Редактор стартовых объектов GPO групповой политики).
- **Network Load Balancing Tools (Инструменты для балансировки сетевой нагрузки).** В их состав включены утилита Network Load Balancing Manager (Диспетчер балансировки сетевой нагрузки), а также инструменты командной строки `Nlb.exe` и `Wlbs.exe`.
- **SMTP Server Tools (Инструменты для сервера SMTP).** Доступна оснастка SMTP.
- **Storage Manager for SANs Tools (Инструменты для диспетчера хранилищ для сетей SAN).** В их состав входят оснастка Storage Manager for SANs (Диспетчер хранилищ для сетей SAN) и инструмент командной строки `ProvisionStorage.exe`.
- **Windows System Resource Manager Tools (Инструменты для диспетчера системных ресурсов Windows).** В их состав включена оснастка Windows System Resource Manager (Диспетчер системных ресурсов Windows) и инструмент командной строки `Wsrmc.exe`.

Установка RSAT

Инструменты RSAT доступны для бесплатной загрузки на сайте Microsoft. Чтобы загрузить RSAT, перейдите на сайт загрузок Microsoft по адресу `www.Microsoft.com/downloads` и наберите **RSAT**.

32- и 64-разрядная версии RSAT

В вашем распоряжении имеется как 32-, так и 64-разрядная версии RSAT. Они должны соответствовать платформе, на которой планируется установка RSAT. Другими словами, если настольный компьютер функционирует под управлением 32-разрядной ОС Windows 8, то для дистанционного управления 64-разрядным сервером Windows Server 2012 R2 понадобится 32-разрядная версия RSAT.

После загрузки RSAT выполните перечисленные ниже действия, чтобы установить и включить RSAT.

1. В проводнике Windows перейдите в папку, в которой был сохранен загруженный файл.
2. Дважды щелкните на установочном пакете и предоставьте возможность мастеру завершить установку.
3. Когда установка завершится, щелкните на кнопке Close (Закрыть).

   Обычно можно рассчитывать, что установка завершится к этому моменту, но для включения RSAT в своей системе понадобится выполнить дополнительные шаги.
4. Выберите пункт меню Start⇨Control Panel (Пуск⇨Панель управления), чтобы открыть панель управления.
5. Щелкните на значке Programs (Программы), а затем на ссылке Turn Windows Features on or off (Включение или отключение компонентов Windows). Если отобразится предупреждение от системы управления учетными записями пользователей (User Account Control), щелкните на кнопке Continue (Продолжить).
6. Отметьте флажок Remote Server Administration Tools (Инструменты дистанционного администрирования сервера). Диалоговое окно будет выглядеть подобно показанному на рис. 17.40.

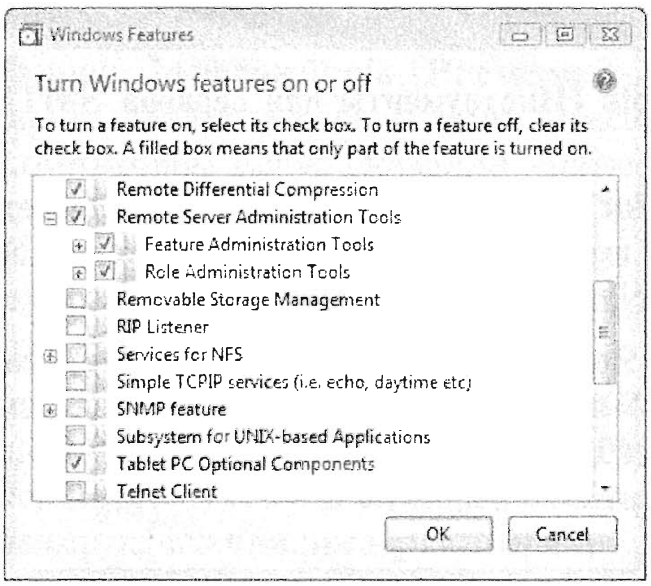


Рис. 17.40. Добавление компонента Remote Server Administration Tools

   При желании можете выбрать отдельные необходимые вам инструменты администрирования или же просто добавить их все, отметив флажок Remote Server Administration Tools.
7. Щелкните на кнопке OK. Соответствующие инструменты будут сконфигурированы для работы в вашей системе.

Если папка Administrative Tools (Административные инструменты) отсутствует в меню Start (Пуск), добавьте ее с помощью описанных ниже шагов.

1. Щелкните правой кнопкой мыши на кнопке Start (Пуск) и выберите в контекстном меню пункт Properties (Свойства).

2. Перейдите на вкладку Start Menu (Меню "Пуск") и щелкните на кнопке Customize (Настроить).
3. Найдите раздел System administrative tools (Администрирование). Выберите вариант Display on the All Programs menu and the Start menu (Отображать в меню "Все программы" и "Пуск").
4. Два раза щелкните на кнопке OK.

После того как инструменты RSAT установлены в системе, вы можете пользоваться ими точно таким же способом, как делали бы это на сервере.

Удаленный рабочий стол и PowerShell

Прежде чем завершить эту главу, давайте обсудим способы применения PowerShell для удаленного подключения к другому сеансу PowerShell. Если вы не планируете использовать PowerShell для дистанционного администрирования своего сервера, то можете пропустить этот раздел. Если же вы собираетесь применять PowerShell, то вам предстоит выяснить, как удаленно подключаться с помощью командлетов PowerShell.

Когда вы отправляете командлеты серверу, вам нужно предоставлять имя пользователя и пароль точно так же, как в пользовательском интерфейсе удаленного рабочего стола. Если необходимо ввести несколько команд, то придется вводить имя пользователя и пароль для каждой команды. Чтобы упростить себе задачу, присвойте имя пользователя и пароль переменной сеанса, которая будет хранить ваши учетные данные.

После ввода приведенной ниже команды появится всплывающее окно регистрации, в котором вы должны ввести свои учетные данные (рис. 17.41):

```
$cr = Get-Credential -Credential jpwebconsulting\administrator
```

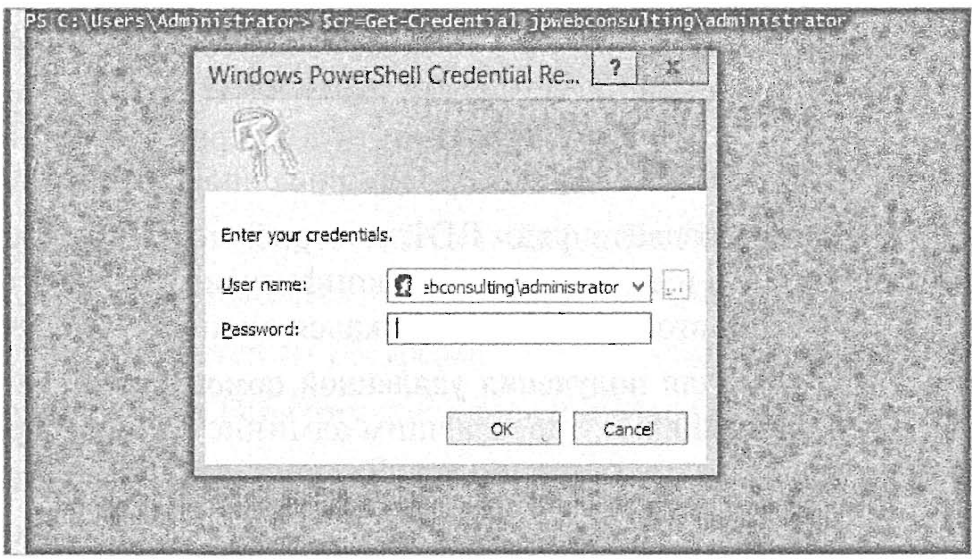


Рис. 17.41. Всплывающее окно для ввода учетных данных

Теперь вся ваша регистрационная информация хранится в переменной `$cr`. В следующем командлете будет показано, как этим воспользоваться. Следующим командлетом будет подключение к удаленной системе. Теперь вы можете видеть эту переменную в действии:

```
Enter-PSSession -ComputerName TestServer-1 -Credential $cr
```

Теперь вы дистанционно подключены к серверу посредством PowerShell. Должна появиться представленная ниже командная строка, которая переключена на сервер `TestServer-1`. Далее можно администрировать сервер так, словно вы сидите непосредственно перед ним. Готовы биться об заклад, что все это казалось вам гораздо более сложным!

```
[TestServer-1]: PS C:\Users\Administrator\Documents>
```

Резюме

Сконфигурируйте серверы Windows Server 2012 R2 для дистанционного администрирования. Прежде чем администраторы смогут подключаться дистанционно, серверы должны быть сконфигурированы таким образом, чтобы обеспечить возможность дистанционного администрирования.

> *Контрольный вопрос.* Сконфигурируйте сервер так, чтобы могли дистанционно подключаться клиенты, у которых выполняется RDC версии 6.0 или выше.

Дистанционно подключайтесь к серверам Windows Server 2012 R2 с помощью Remote Desktop Connection. Вы можете дистанционно подключаться к серверам для выполнения практически любой административной работы. Серверы зачастую находятся в надежно защищенном серверном помещении, которое охлаждается для обеспечения бесперебойной работы электронного оборудования. Таким помещением может быть специальная комната; это помещение может находиться в другом здании или даже в отдаленном географическом пункте. Однако в любом случае серверы можно дистанционно администрировать с помощью либо RDC, либо Remote Desktops.

> *Контрольный вопрос.* Подключитесь к какому-то серверу с помощью RDC. Позаботьтесь о том, чтобы при подключении к удаленному серверу обеспечивался доступ к вашим локальным дискам.

Дистанционно подключайтесь к серверам Windows Server 2012 R2 с помощью файла Remote Desktop Protocol. Если вы регулярно подключаетесь к удаленному серверу с помощью RDC, то можете сконфигурировать файл RDP, который можно заранее настроить с учетом потребностей в отношении этого сервера. В файле RDP будут храниться все настройки, которые вы сконфигурировали для этого подключения.

> *Контрольный вопрос.* Создайте файл RDP, который можно применять для подключения к серверу по имени `Server1`. Сконфигурируйте этот файл так, чтобы при подключении автоматически запускался диспетчер серверов.

Сконфигурируйте сервер для получения удаленной помощи. Если в состав вашей среды входят удаленные площадки, где младшим администраторам время от времени требуется помощь, вы можете использовать Remote Assistance для получения доступа к их сеансу и демонстрации соответствующих процедур.

> *Контрольный вопрос.* Сконфигурируйте сервер для Remote Assistance.

Установите инструменты дистанционного администрирования сервера. Инструменты Remote Server Administration Tools (RSAT) включают оснастки и инструменты командной строки, применяемые для управления серверами Windows Server 2003, Windows Server 2008 и Windows Server 2012 из настольных компьютеров, которые функционируют под управлением Windows Vista, Windows 7 или Windows 8.

> *Контрольный вопрос.* Получите и установите RSAT в системе Windows Vista, Windows 7 или Windows 8.

Глава 18

Подключение клиентов Windows и Mac

Итак, вы собрали сервер, создали пользователей и открыли совместный доступ к сетевым ресурсам. Теперь вам необходимо сконфигурировать свои клиентские системы так, чтобы они могли подключаться к сети и использовать эти ресурсы. В настоящей главе мы покажем, как создавать разные клиентские системы с сетевыми компонентами, каким образом входить в сеть, как находить и подключаться к общим ресурсам, каким образом управлять паролями и как находить и подключиться к Active Directory, если эта служба развернута.

Мы также раскроем способы подключения клиентов Mac к сети Windows Server 2012 и объясним, как получить доступ к разнообразным возможностям, таким как общие файловые ресурсы и принтеры из компьютера Mac.

В этой главе вы изучите следующие темы:

- проверка правильности конфигурирования сети;
- подключение клиентского компьютера к домену;
- изменение пользовательских паролей;
- подключение к сетевым ресурсам;
- подготовка Active Directory для клиентов Mac OS X;
- подключение компьютера Mac к домену;
- подключение к общим файловым ресурсам и принтерам;
- использование Remote Desktop из клиента Mac.

Что нужно знать, прежде чем приступить к работе

Перед тем, как подключать рабочие станции к домену, вы должны знать несколько аспектов о клиентских компьютерах и сетевой среде. Если вы не знакомы с се-

тями Microsoft, то прежде чем пытаться конфигурировать клиентов, имеет смысл ознакомиться с материалом ряда других глав.

- В главе 2 раскрыты основы сетевого программного обеспечения и безопасности.
- Главы 4 и 20 посвящены протоколу TCP/IP и инфраструктуре. Практически все сети Microsoft используют TCP/IP.
- В главе 8 показано, как создавать учетные записи пользователей и компьютеров.
- В главе 29 рассматриваются вопросы подключения клиентов к ресурсам домена с применением Remote Desktop.

Если вы уже прочитали эти главы или в целом знакомы с перечисленными выше концепциями, тогда продолжайте изучение дополнительной информации о способах подключения клиентов к сети и необходимых видах учетных записей.

При изложении материала этой главы мы будем подключаться к одному и тому же серверу, в одном и том же домене и с участием одной и той же учетной записи пользователя.

- Именем пользователя является `kevinb` (когда действует как обычный пользователь) или `bigadmin` (когда действует как администратор домена);
- Имя домена выглядит как `bigfirm.com`.
- В сети имеется контроллер домена Windows Server 2012 под названием `bf1.bigfirm.com`.
- В сети присутствует несколько клиентских машин, представляющих клиентские операционные системы, с которыми мы будем иметь дело в этой главе. Вот их имена:
  - `WIN8CLIENT`
  - `WIN7CLIENT`

Требования к программному обеспечению клиентской стороны

В прошлом для каждого клиента вам приходилось конфигурировать три базовых программных компонента: *драйвер* для сетевой интерфейсной платы (network interface card — NIC), *сетевой протокол* и *сетевой клиент*. Хорошие новости заключаются в том, что в наши дни все, что вам требуется, уже встроено в систему, кроме тех редких случаев, когда может понадобиться установить драйвер NIC.

Чтобы у вас сложилось четкое понимание лежащей в основе технологии, которая приводит все это в действие, мы еще раз рассмотрим эти три базовых программных компонента.

Драйвер NIC позволяет операционной системе (ОС) взаимодействовать с NIC. Перед загрузкой любого сетевого протокола или клиентского программного обеспечения ОС должна распознать сетевую плату и загрузить соответствующий драйвер. В результате появления усовершенствованной технологии Universal Plug and Play (UPnP) и встроенных библиотек драйверов большинство клиентских систем, обсуждаемых в этой главе, могут автоматически обнаруживать NIC и загружать драйвер, включенный в комплект ОС. Если же требуемый драйвер не входит в состав ОС или вашей клиентской системе не удается обнаружить сетевую плату, вы должны

использовать драйвер и инструкции по установке для ОС, которые предоставлены изготовителем NIC.

Сетевой протокол, встроенный в ОС, позволяет узлам одной и той же сети взаимодействовать друг с другом. Чтобы такое взаимодействие было возможным, все узлы должны применять те же самые протоколы. В наши дни TCP/IP является фактическим стандартом для сетей Microsoft. Поскольку в большинстве сетей используется IPv4, в настоящей главе мы также будем применять эту версию. В современных сетях хорошее понимание IPv6 становится гораздо более актуальным, поэтому мы настоятельно рекомендуем основательно изучить данную тему.

Windows RT

Помимо сетевых компонентов и протоколов в целом, IT-профессионал должен также понимать, каким образом подключать другие версии Windows, подобные Windows RT, и как функционируют подключения в Windows RT. Эти устройства разработаны как предварительно сконфигурированные версии ОС Windows, и любые добавления производятся через магазин Microsoft Store.

Windows RT представляет собой систему, основанную на ARM. Она была разработана специально для планшетных устройств, которые должны быть легкими и компактными, а срок службы их аккумуляторных батарей должен быть как можно более долгим. (Дополнительные сведения об ARM доступны по адресу `http://tinyurl.com/c18WinRTARM`.)

Поскольку устройства Windows RT имеют ОС, которая не может быть изменена, производственные среды не в состоянии настраивать образы Windows на таких устройствах и, как следствие, они не могут подсоединиться к домену Windows. Некоторые варианты подключения Windows RT мы обсудим в ходе этой главы. Следующая ссылка позволяет получить дополнительную информацию о Windows RT: `http://windows.microsoft.com/en-US/windows/rt-welcome`.

Поддержка IPv6 в Windows Server 2012

В Windows Server 2012 и Windows 8 протокол IPv6 установлен и включен по умолчанию. Более подробную информацию по этому протоколу и его конфигурированию для вашей среды можно найти в главе 4.

Клиенты в примерах, приведенных в настоящей главе, получат уникальный IP-адрес и другую необходимую информацию для конфигурации протокола от сервера DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации хостов) в соответствующей сети. Большинство серверов в производственной среде будут иметь статические IP-адреса. Однако рабочие станции чаще всего получают IP-адреса, выделяемые динамически. Сервер DHCP не только назначает IP-адреса клиентским рабочим станциям, но может также предоставлять все остальные значения, требуемые в конкретной среде TCP/IP (включая маску подсети, используемые DNS-серверы, стандартный шлюз для маршрутизации и суффикс домена для применения к подключению). Сервер DHCP также отслеживает назначения IP-адресов и динамически обновляет клиентов, когда вы хотите внести какие-то изменения в конфигурацию IP-адресов. (Будут возникать ситуации, когда предпоч-

тительно не использовать сервер DHCP для назначения клиенту адресной информации. В этой главе мы также рассмотрим, как устанавливать такую информацию вручную в каждой клиентской ОС.)

Клиент сети обнаруживает сетевые ресурсы и подключается к ним. Для любого заданного варианта ПО монтирования файлов и общего доступа к принтерам, которое функционирует на сервере, существует дополнение в виде клиентского подключения.

Доменные учетные записи и локальные учетные записи

Ключевыми аспектами к использованию клиентской рабочей станции и получению доступа к сетевым ресурсам являются два вида учетных записей: доменные учетные записи и локальные учетные записи. Вообще говоря, доменные учетные записи применяются для аутентификации доступа к общим ресурсам домена, а локальные учетные записи — для аутентификации доступа с целью использования или управления локальным компьютером.

Домен — это логическая группировка компьютеров, пользовательских учетных записей и связанных сетевых ресурсов, которые все имеют общую базу данных безопасности под названием Active Directory. Домены обеспечивают централизованную систему безопасности наряду с функцией группирования ресурсов для рабочих групп. Доменные учетные записи разрешают людям применять единое имя для входа в любую рабочую станцию и получения доступа к ресурсам на любом сервере, который принадлежит домену (при условии, что пользователь имеет разрешение на доступ к этим ресурсам). К доменам могут присоединяться все операционные системы Microsoft кроме Windows RT (`http://windows.microsoft.com/en-US/windows/rt-welcome`). Пользовательская учетная запись, которая не является членом данного домена или членом доверяемого домена, не может иметь доступ к сетевым ресурсам, защищенным системой безопасности домена. За дополнительной информацией о доменах обращайтесь в главу 7.

Рабочая группа — это логическая группировка компьютеров, не имеющая централизованной базы данных безопасности, но организованная под единым именем. Несмотря на то что современные операционные системы могут присоединяться к рабочим группам, это не характерно для производственных сред; даже в небольших офисах в целях безопасности строятся домены. Управлять доступом к ресурсам рабочих групп гораздо труднее, к тому же они лишены функции обнаружения, которую предоставляет Active Directory.

Доступ к рабочей группе — это метод, с помощью которого устройства Windows RT обращаются друг к другу или пересылают информацию в сеть. Поскольку устройства Windows RT не могут присоединяться к домену Active Directory, они остаются в рабочей группе, что предусмотрено по умолчанию.

Хотя членство в домене является ключом для доступа к централизованным ресурсам, у локальных учетных записей есть и свои цели: они нужны для локального управления рабочей станцией. Все текущие операционные системы Microsoft поддерживают локальные базы данных безопасности. Изменения конфигурации, которые вам предстоит выполнить, требуют наличия административных привилегий, поэтому для внесения таких изменений вы должны войти в систему от имени локальной учетной записи `Administrator` (или какой-то учетной записи из локальной группы `Administrators`).

Выдача пользователям прав для администрирования клиентского компьютера

В прошлом администраторы, как правило, добавляли пользовательскую учетную запись `Domain User` (Пользователь домена) в локальную группу `Administrators` на клиентском компьютере, чтобы у этого пользователя была возможность выполнять определенные задачи с повышенными разрешениями.

В наши дни рекомендуется избегать предоставления пользователям административного доступа подобным способом. Вместо этого вы можете воспользоваться новыми более совершенными опциями безопасности и делегирования (например, Dynamic Access Control (Динамическое управление доступом)) в Windows Server 2012 R2, чтобы обеспечить пользователям необходимый уровень контроля. Лучше всего, если вы попытаетесь следовать подходу наименьшего уровня привилегий как противоположности предоставления пользователям доступа ко всем ресурсам.

Проверка правильности конфигурации сети

Первым шагом в присоединении к домену является подключение к сети этого домена, чтобы клиентский компьютер мог взаимодействовать с контроллером домена. Шаги по подключению к сети являются по существу одинаковыми для всех клиентских операционных систем, обсуждаемых в этой главе.

1. Установите на клиентском компьютере работоспособную сетевую интерфейсную плату и драйвер для нее.
2. Сконфигурируйте NIC с настройками, подходящими для взаимодействия с сетью.

В ходе рассмотрения этих шагов мы будем отмечать любые отличия в пользовательском интерфейсе (а также и другие) между клиентскими операционными системами, но сейчас давайте обеспечим готовность для присоединения к домену. Войдите в систему с применением локальной учетной записи `Administrator`. Прежде чем предпринимать попытку присоединения к домену, неплохо убедиться в том, что NIC и связанный драйвер были установлены корректно, и для таких проверок понадобятся административные права.

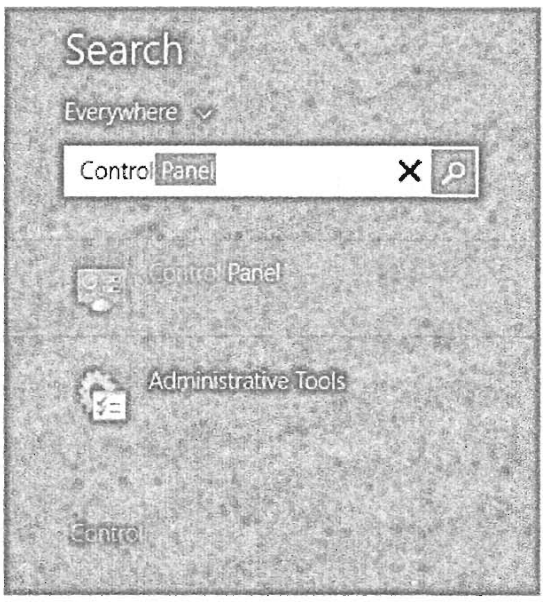


Рис. 18.1. Использование экрана Start операционной системы Windows 8 для получения доступа к панели управления

Устройства, обнаруженные на вашем компьютере, отображаются в диспетчере устройств (Device Manager). Чтобы попасть в него, откройте сначала панель управления и затем диспетчер устройств (можете открыть меню Start (Пуск), начать набор на клавиатуре **`Control Panel`**, как показано на рис. 18.1, после чего выбрать значок Control Panel (Панель управления), в итоге открыв панель управления). Откроется консоль Computer Management (Управление компьютером). В левой части окна будет отображаться список всех устройств; раскройте папку Network Adapters (Сетевые адаптеры), в которой должна находиться ваша NIC.

При наличии проблем с NIC (например, связанных с драйвером), вы обязательно узнаете об этом по отсутствию сетевого адаптера в списке или по его "нерабочему" состоянию (устройство находится в списке, но помечено восклицательным знаком желтого цвета). Сетевая интерфейсная плата может также быть нерабочей и располагаться в папке Other Devices (Другие устройства). Решить проблемы с оборудованием помогут документация от изготовителя NIC и справочная система ОС.

Проверка правильности настроек подключения по локальной сети

Если во время установки вы принимаете типовые настройки сети, то программа установки установит и создаст программное представление NIC, которое называется *подключением по локальной сети*. Кроме того, будут установлены следующие компоненты подключения по локальной сети.

- **TCP/IP.** Позволяет компьютеру взаимодействовать с другими узлами и устройствами в сети.
- **Client for Microsoft Networks (Клиент для сетей Microsoft).** Позволяет компьютеру получать доступ к ресурсам в сети Microsoft.
- **QoS Packet Scheduler (Планировщик пакетов QoS).** Планировщик пакетов QoS (Quality of Service — качество обслуживания) предоставляет службы управления сетевым трафиком и назначением приоритетов для данных, передаваемых на и из локального устройства.

По умолчанию подключение по локальной сети будет сконфигурировано на получение перечисленных ниже конфигурационных настроек от сервера DHCP.

- **IP Address Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)).** Адрес компьютера по отношению к сети, к которой он присоединяется. Каждый узел этой сети должен иметь уникальный IP-адрес.
- **IP Address Version 6 (TCP/IPv6) (Протокол Интернета версии 6 (TCP/IPv6)).** Это самая последняя версия протокола Интернета (Internet Protocol), которая постепенно внедряется крупными организациями, и многие продукты и компоненты Microsoft Server требуют его для поддержки своей функциональности. Одним из таких продуктов является Microsoft UAG (Microsoft Unified Access Gateway — шлюз унифицированного доступа Microsoft). Наличие включенного протокола IPv6 для DHCP не приводит к возникновению каких-либо проблем с конфигурацией, поэтому по умолчанию он включен. Типичный адрес IPv6 выглядит как 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- **Subnet Mask (Маска подсети).** Число, которое логически сегментирует крупную сеть на отдельные подсети (взаимодействие между этими подсетями должно проходить через маршрутизатор).
- **Default Gateway (Основной шлюз).** IP-адрес маршрутизатора, который будет маршрутизировать коммуникации между узлами, находящимися в разных подсетях или в других сетях.
- **Domain Name System Server (Сервер службы доменных имен).** IP-адрес DNS-сервера в данной сети.

- **DNS Suffix (Optional) (Суффикс DNS) (необязательно).** Доменное имя Active Directory, к которому присоединен или присоединится компьютер (в этой главе им является `bigfirm.com`).

Самый быстрый способ узнать, получила ли ваша NIC надлежащие настройки автоматически, предусматривает открытие окна командной строки и ввод следующей команды:

```
ipconfig /all
```

Вы должны получить результаты, подобные показанным на рис. 18.2.

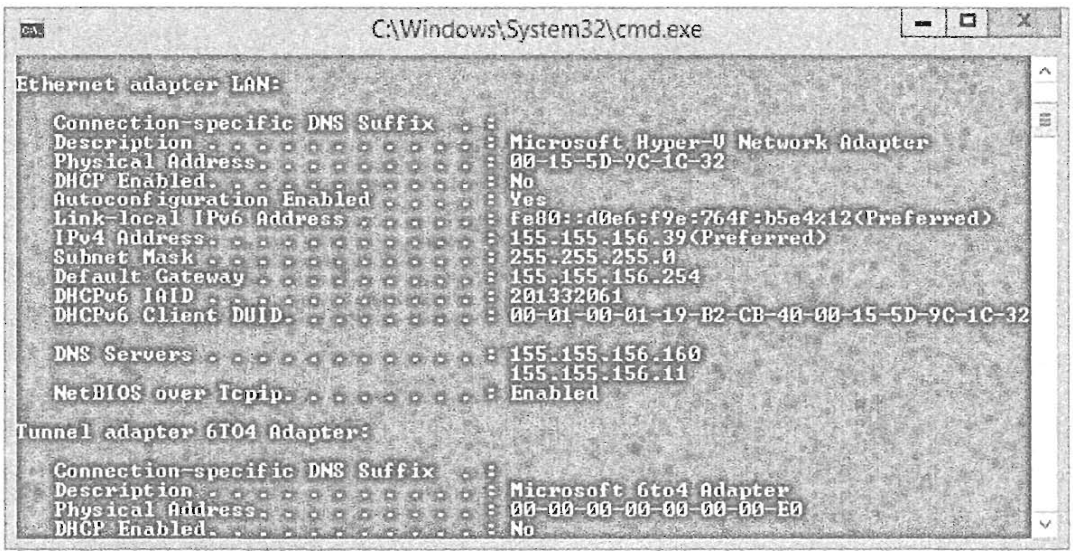


Рис. 18.2. Результаты выполнения команды `ipconfig`

Строки в результатах запуска `ipconfig`, которые позволяют понять, правильно ли сконфигурирована NIC, находятся в разделе `Ethernet Adapter LAN` (Ethernet adapter Подключение по локальной сети).

- **`DHCP Enabled` (DHCP включен).** Если этот параметр установлен в `Yes` (Да), то NIC настроена на получение информации об IP-адресе от сервера DHCP. Если же он установлен в `No` (Нет), то вам понадобится вручную сконфигурировать IP-адрес для этого подключения по локальной сети.
- **`Autoconfiguration Enabled` (Автонастройка включена).** Этот параметр присутствует и установлен в `Yes` (Да), только если NIC настроена на автоматическое получение IP-адресов от сервера DHCP.
- **`IPv4 Address` (IPv4-адрес).** Это уникальный IP-адрес, назначенный подключению по локальной сети.
- **`Subnet Mask` (Маска подсети).** Это подсеть, к которой принадлежит данный узел.
- **`Default Gateway` (Основной шлюз).** Это маршрутизатор, который будет маршрутизировать трафик между назначенной подсетью и другими подсетями и сетями.
- **`DNS Servers` (DNS-серверы).** DNS-серверы преобразуют IP-адреса в имена компьютеров. Вы должны располагать назначенным DNS-сервером, иначе вы не сможете присоединиться к домену. В большинстве случаев адрес DNS-сервера предоставляется сервером DHCP.

Если результаты выполнения `ipconfig` оказались пустыми, это может говорить об отсутствии сервера DHCP для выделения IP-адресов; в этом случае вам придется сконфигурировать параметры подключения по локальной сети вручную. Чтобы сделать это, откройте окно свойств подключения по локальной сети, ассоциированного с NIC, и введите нужную информацию вручную. Пока мы будем предполагать, что результаты выполнения `ipconfig` показали наличие у NIC требуемой информации об адресах.

Проверка возможности подключения к сети с помощью команды `ping`

Чтобы иметь абсолютную уверенность в том, что сетевая карта и TCP/IP функционируют надлежащим образом, а информация об IP-адресах, назначенная NIC, является корректной, откройте окно командной строки и воспользуйтесь командой `ping` для тестирования базовой возможности подключения к сети.

Если вы ранее не имели дело с командой `ping`, то по адресу `http://tinyurl.com/c18PingCommand` доступно описание самой команды и всех ее переключателей.

Ниже приведены типичные команды `ping`, которые можно применять для проверки возможности подключения к сети.

- **`ping 127.0.0.1`** Выполняет пингование вашего компьютера (этот адрес всегда указывает на узел, из которого производится пингование, и называется *адресом обратной связи*).
- **`ping localhost -4`** Выполняет пингование вашего компьютера. Сообщает, способно ли подключение по локальной сети отправлять и принимать информацию. Для получения результатов в формате IPv4 используйте опцию `-4`.
- **`ping x.x.x.x`** Выполняет пингование другого узла (замените `x.x.x.x` нужным IP-адресом).
- **`ping ИМЯ_DNS.ДОМЕН.СУФФИКС`** Выполняет пингование узла с применением его полного доменного имени (имени, хранящегося в DNS, которое отображается на IP-адрес). Примером может служить `ping bf1.bigfirm.com`.

Проверка и установка информации подключения по локальной сети с помощью графического пользовательского интерфейса

Знание того, как найти свойства клиентского подключения по локальной сети, важно по следующим причинам.

- Можно проверить корректность конфигурации подключения по локальной сети с применением графического пользовательского интерфейса.
- Можно установить информацию подключения по локальной сети вручную, если отсутствует сервер DHCP, который бы обеспечил автоматическое получение необходимых параметров.

Подключения по локальной сети в Windows 8

Чтобы найти подключения по локальной сети в клиенте Windows 8, выберите меню Start (Пуск), наберите `Control Panel`, щелкните на значке Control Panel (Панель управления) и затем щелкните на Network and Sharing Center (Центр управления сетями и общим доступом); откроется окно Network and Sharing Center, представленное на рис. 18.3.

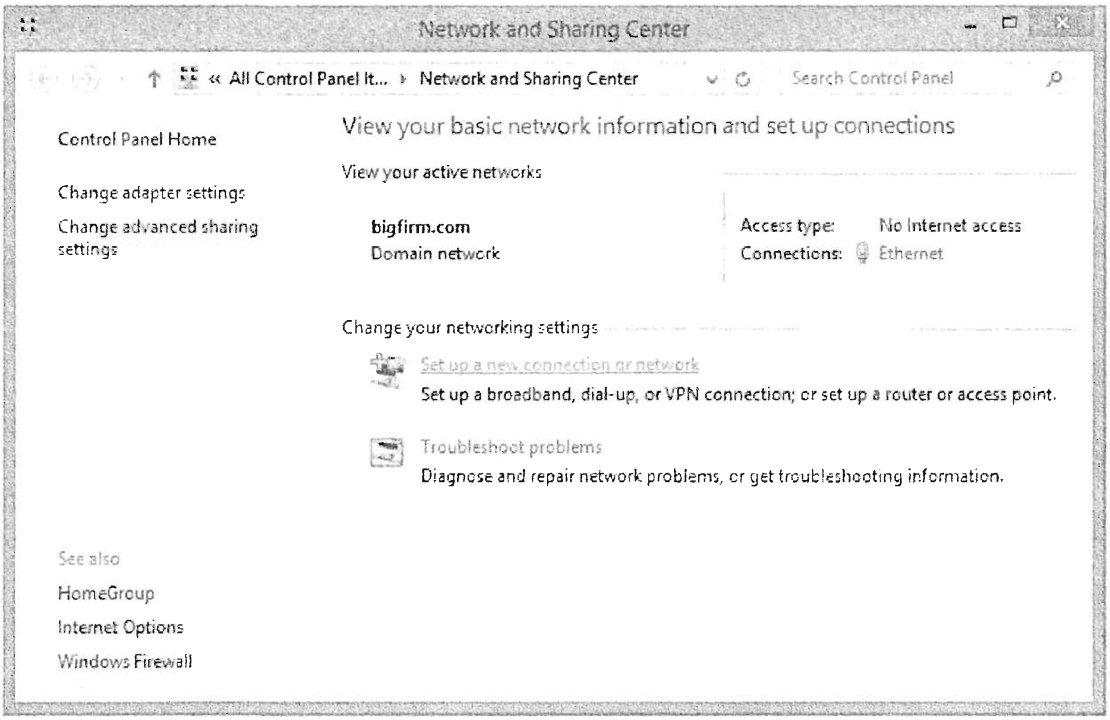


Рис. 18.3. Просмотр подключения по локальной сети в окне Network and Sharing Center (Windows 8)

Точно такая же информация о подключении по локальной сети будет на устройствах Windows RT. Сетевые интерфейсы Windows являются общими для операционных систем Windows 8, RT и Windows Server 2012.

Если вы не видите подключение по локальной сети в разделе View your active networks (Просмотр активных сетей), это может означать, что NIC не была обнаружена должным образом. Воспользуйтесь диспетчером устройств для изоляции проблемы или попробуйте добавить сетевой адаптер вручную посредством мастера добавления оборудования из панели управления.

1. Щелкните на ссылке Local Area Connection (Подключение по локальной сети), чтобы открыть окно Local Area Connection Status (Состояние — Подключение по локальной сети), показанное на рис. 18.4.

   Здесь вы можете видеть, что указанное соединение активизировано (в Media State (Состояние среды) указано Enabled (Подключено)).

2. Щелкните на кнопке Details (Сведения), чтобы открыть окно Network Connection Details (Сведения о сетевом подключении), которое приведено на рис. 18.5.

   Отображаемые здесь данные являются подмножеством данных, которые можно получить с помощью команды `ipconfig`.

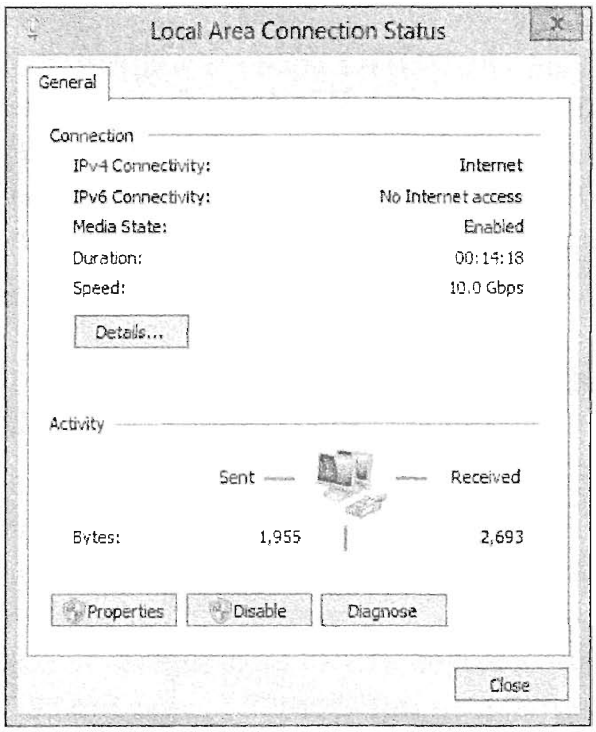


Рис. 18.4. Окно Local Area Connection Status (Windows 8)

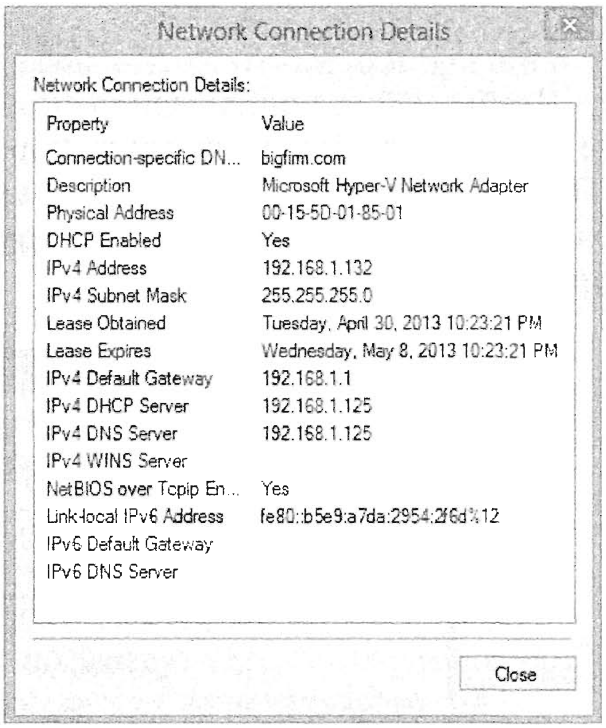


Рис. 18.5. Окно Network Connection Details (Windows 8)

Сведения о сетевом подключении показывают, что для подключения по локальной сети включен DHCP, т.е. оно получает свою конфигурацию от сервера DHCP. Подключение сконфигурировано с DNS-суффиксом `bigfirm.com`, IP-адресом 192.168.1.132, маской подсети 255.255.255.0, адресом основного шлюза 192.168.1.1 и адресом DNS-сервера 192.168.1.125. Здесь также видно, когда была выдана информация DHCP (дата в Lease Obtained (Аренда получена)), и когда она утратит свою силу (дата в Lease Expires (Аренда истекает)).

Ручное конфигурирование параметров подключения по локальной сети в Windows 8

Закройте окно Network Connection Details и щелкните на кнопке Properties (Свойства) в окне Local Area Connection Status, чтобы открыть диалоговое окно Ethernet Properties (Подключение по локальной сети — свойства), которое приведено на рис. 18.6.

Это диалоговое окно показывает, с какой сетевой интерфейсной платой ассоциировано подключение по локальной сети, и отображает используемые ею компоненты. Именно здесь вы должны вручную назначать подключению статический IP-адрес, если это действительно необходимо. Выполните следующие шаги.

1. Выберите элемент Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)) и щелкните на кнопке Properties (Свойства).

   Откроется диалоговое окно Internet Protocol Version 4 (TCP/IPv4) Properties (Свойства: Протокол Интернета версии 4 (TCP/IPv4)), показанное на рис. 18.7.

2. Выберите переключатель Use the following IP address (Использовать следующий IP-адрес).

3. Введите IP-адрес, маску подсети и адрес основного шлюза.

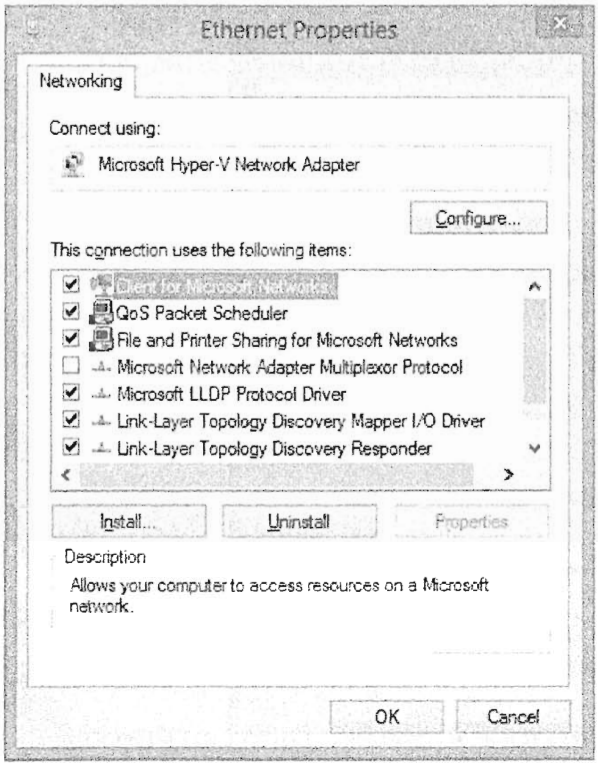


Рис. 18.6. Окно Ethernet Properties (Windows 8)

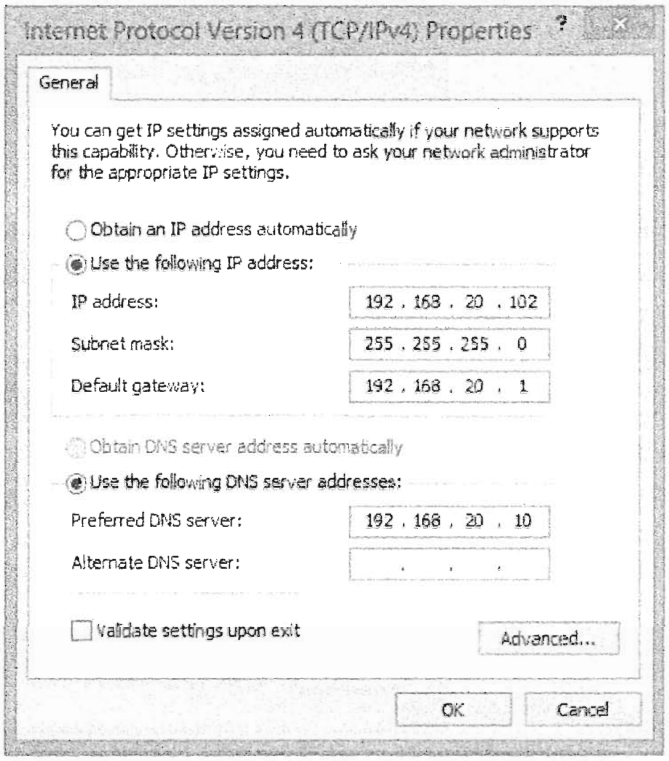


Рис. 18.7. Окно Internet Protocol Version 4 (TCP/IPv4) Properties (Windows 8)

4. Выберите переключатель Use the following DNS server addresses (Использовать следующие адреса DNS-серверов) и введите предпочитаемый и альтернативный адреса DNS-серверов.
5. Щелкните на кнопке Advanced (Дополнительно), в открывшемся диалоговом окне перейдите на вкладку DNS и введите суффикс DNS, который вы хотите присоединить к имени этого компьютера (чтобы создать полное доменное имя (FQDN)). Щелкните на кнопке OK.
6. Отметьте флажок Validate settings upon exit (Подтвердить параметры при выходе), чтобы запустить на выполнение аплет Network Diagnostics (Диагностика сети).

   Этот аплет запустится, когда вы покинете окно Local Area Connection Properties, и проверит правильность параметров, связанных с IP-адресами. При наличии проблемы вы получите уведомление, а также информацию, которая поможет решить эту проблему.
7. Два раза щелкните на кнопке OK и закройте остальные окна.

Подключения по локальной сети в Windows 7

Чтобы найти подключения по локальной сети в клиенте Windows 7, выберите пункт меню Start⇨Control Panel⇨Network and Sharing Center (Пуск⇨Панель управления⇨Центр управления сетями и общим доступом). Окно Network and Sharing Center (Центр управления сетями и общим доступом) показано на рис. 18.8. Чтобы попасть в него быстрее, наберите в поле поиска (в нижней части меню Start) слово `Network` и затем щелкните на пункте Network and Sharing Center в верхней части меню Programs (Программы).

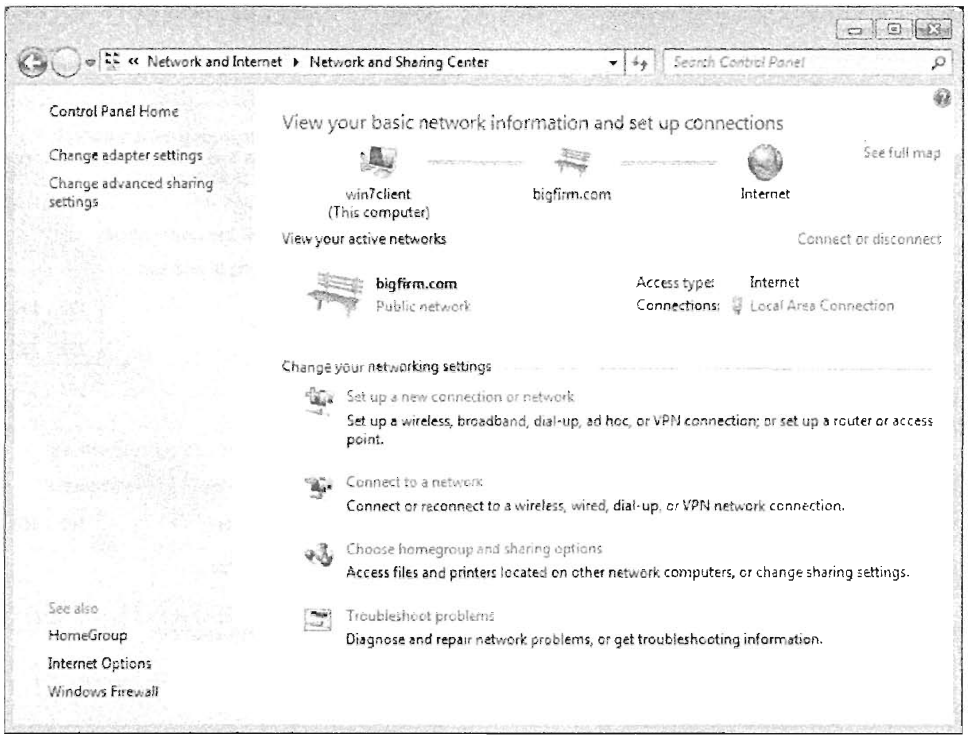


Рис. 18.8. Просмотр подключения по локальной сети в окне Network and Sharing Center (Windows 7)

Если вы не видите подключение по локальной сети в разделе View your active networks (Просмотр активных сетей), это может означать, что NIC не была обнаружена должным образом. Воспользуйтесь диспетчером устройств для изоляции проблемы или попробуйте добавить сетевой адаптер вручную посредством мастера добавления оборудования, доступного в панели управления.

1. Щелкните на ссылке Local Area Connection (Подключение по локальной сети), чтобы открыть окно Local Area Connection Status (Состояние — Подключение по локальной сети), как показано на рис. 18.9.

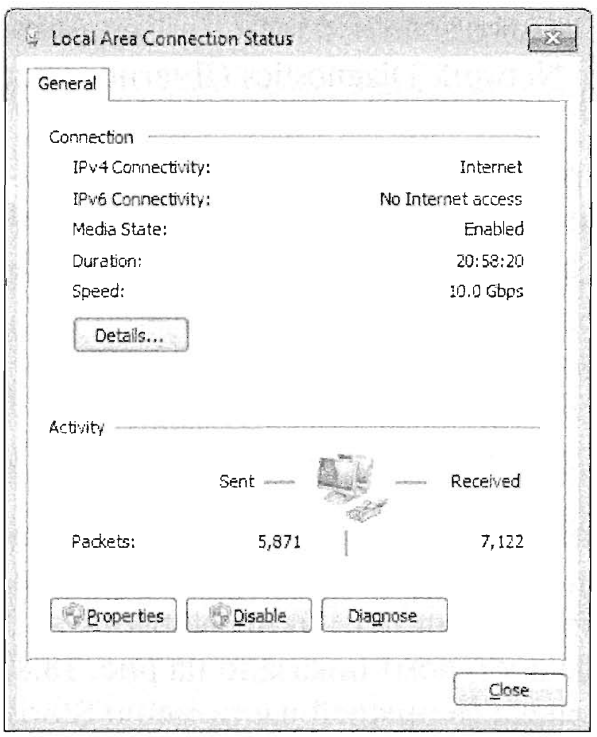


Рис. 18.9. Окно Local Area Connection Status (Windows 7)

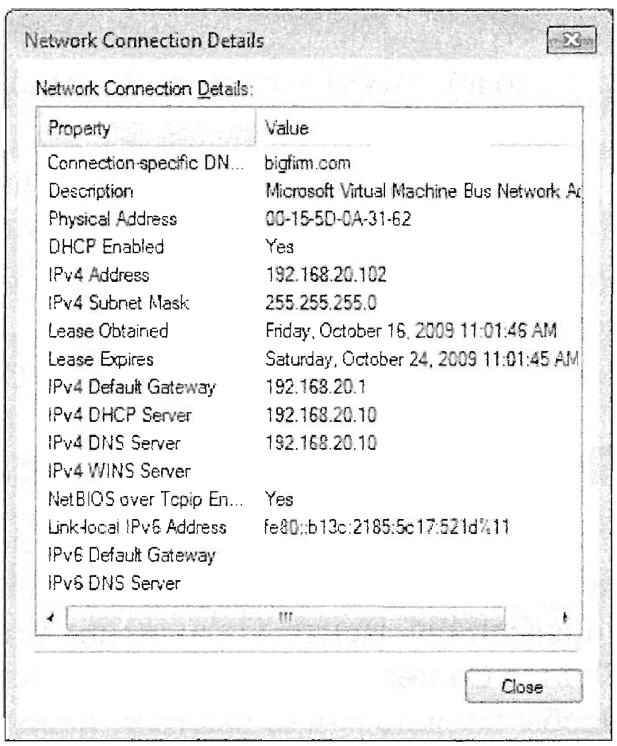


Рис. 18.10. Окно Network Connection Details (Windows 7)

Здесь видно, что соединение подключено (в Media State (Состояние среды) указано Enabled (Подключено)).

2. Щелкните на кнопке Details (Сведения), чтобы открыть окно Network Connection Details (Сведения о сетевом подключении), представленное на рис. 18.10.

Отображаемые здесь данные являются подмножеством данных, которые можно получить с помощью команды `ipconfig`. Сведения о сетевом подключении показывают, что для подключения по локальной сети включен DHCP, т.е. оно получает свою конфигурацию из сервера DHCP. Подключение сконфигурировано с DNS-суффиксом `bigfirm.com`, IP-адресом 192.168.20.102, маской подсети 255.255.255.0, адресом основного шлюза 192.168.20.1 и адресом DNS-сервера 192.168.20.10. Здесь также видно, когда была выдана информация DHCP (дата в Lease Obtained (Аренда получена)), и когда истечет ее срок (дата в Lease Expires (Аренда истекает)).

Ручное конфигурирование параметров подключения по локальной сети в Windows 7

Закройте окно Network Connection Details и щелкните на кнопке Properties (Свойства) в окне Local Area Connection Status, чтобы открыть диалоговое окно Local Area Connection Properties (Свойства подключения по локальной сети), которое показано на рис. 18.11. В этом диалоговом окне можно видеть, с какой сетевой интерфейсной платой ассоциировано подключение по локальной сети, а также используемые ею компоненты. Именно здесь вы должны вручную назначать подключению статический IP-адрес, если это действительно необходимо. Выполните следующие действия.

1. Выберите элемент Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)) и щелкните на кнопке Properties (Свойства). Откроется диалоговое окно Internet Protocol Version 4 (TCP/IPv4) Properties (Свойства: Протокол Интернета версии 4 (TCP/IPv4)), показанное на рис. 18.12.

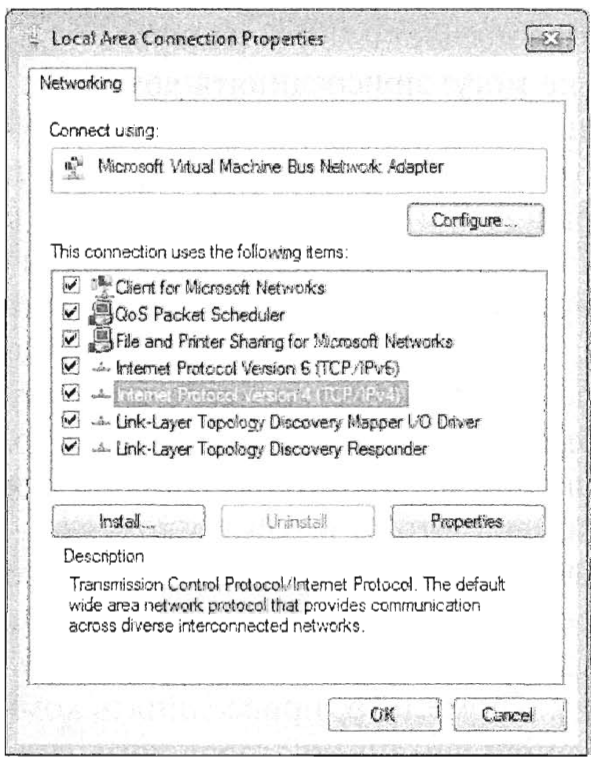


Рис. 18.11. Окно Local Area Connection Properties (Windows 7)

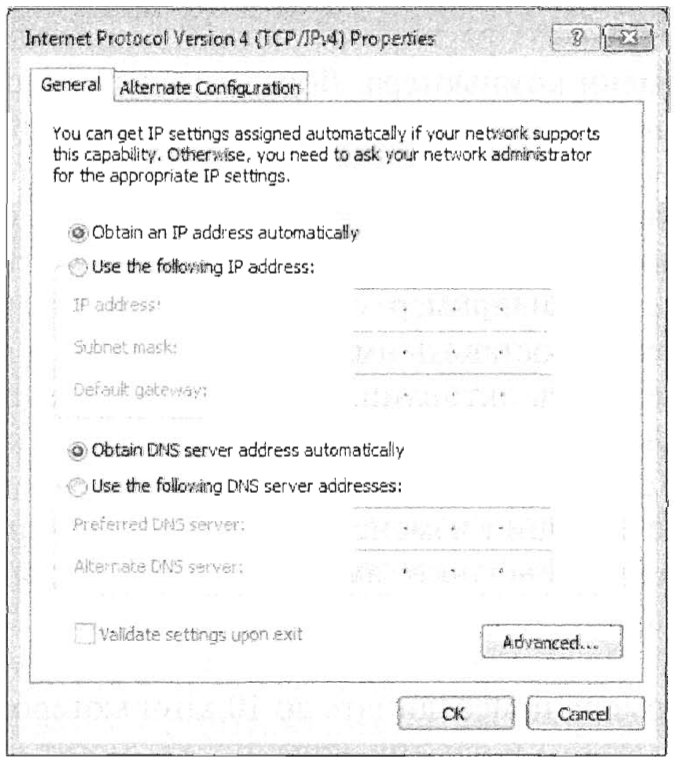


Рис. 18.12. Окно Internet Protocol Version 4 (TCP/IPv4) Properties (Windows 7)

2. Выберите переключатель Use the following IP address (Использовать следующий IP-адрес).
3. Введите IP-адрес, маску подсети и адрес основного шлюза.
4. Выберите переключатель Use the following DNS server addresses (Использовать следующие адреса DNS-серверов) и введите предпочитаемый и альтернативный адреса DNS-серверов.
5. Щелкните на кнопке Advanced (Дополнительно), в открывшемся диалоговом окне перейдите на вкладку DNS и введите суффикс DNS, который вы хотите присоединить к имени этого компьютера (чтобы создать полное доменное имя (FQDN)). Щелкните на кнопке OK.
6. Отметьте флажок Validate settings upon exit (Подтвердить параметры при выходе), чтобы запустить на выполнение аплет Network Diagnostics (Диагностика сети).

   Этот аплет запустится, когда вы покинете окно Local Area Connection Properties, и проверит правильность параметров, связанных с IP-адресами. При наличии проблемы вы получите уведомление, а также информацию, которая поможет решить эту проблему.
7. Два раза щелкните на кнопке OK и закройте остальные окна.

Присоединение к домену

Чтобы присоединиться к домену из клиента с любой ОС Windows, вам понадобится следующая информация:

- полное доменное имя или NetBIOS-имя домена;
- имя и пароль учетной записи с разрешением на присоединение к домену.

Присоединиться к домену легко. Основные проблемы могут возникать в случае незнания правильных учетных данных для домена и предоставление некорректного имени компьютера. Локальные администраторы не могут присоединять компьютеры к домену, и вы не должны присоединять компьютер к домену с использованием такого же имени, как у другого компьютера, который был присоединен ранее и располагает объектом учетной записи компьютера в Active Directory. В сценариях с заменой применение той же самой учетной записи компьютера может быть приемлемым; например, если у ноутбука был заменен жесткий диск, то вы вполне можете решить оставить имя этого компьютера прежним, т.к. имена компьютеров являются ценными активами. Для этого рекомендуется с помощью оснастки Active Directory Users and Computers аккуратно удалить старый объект, представляющий компьютер. Вдобавок удостоверьтесь в том, что предоставили системе достаточно времени для репликации изменения на другие контроллеры домена, чтобы избежать возникновения конфликта имен. Убедитесь, что имя компьютера является уникальным, и что вы имеете правильные учетные данные для присоединения к домену.

По умолчанию домены Windows Server 2012 позволяют обычным пользователям домена присоединять до 10 компьютеров к домену. Кроме того, присоединять компьютеры к домену, конечно же, могут учетные записи администраторов домена, и вы также можете делегировать это право другим пользователям через групповую по-

литику (Group Policy). Сведения о том, как делегировать это право, можно найти по адресу http://technet.microsoft.com/library/dd392267(WS.10).aspx.

Клиентские компьютеры всегда начинают как члены рабочей группы под названием WORKGROUP. Это является начальной настройкой для всех клиентских операционных систем, обсуждаемых в настоящей главе.

Добавление доменных учетных записей в локальные группы компьютера

Чтобы войти и пользоваться компьютером с применением доменной учетной записи, доменная учетная запись пользователя должна быть добавлена в локальную группу на этом компьютере. Подобное справедливо для всех клиентских ОС Windows 8, Windows 7 и более старых версий Windows вплоть до Windows 2000/XP, которые присоединяются к домену.

Когда компьютер присоединяется к домену, группа Domain Admins добавляется к локальной группе Administrators на этом компьютере. Затем администраторы домена становятся администраторами локального компьютера и могут полностью управлять машиной (добавлять или удалять оборудование, устанавливать ПО и т.д.). Аналогично, группа Domain Users добавляется к локальной группе Users компьютера. После этого пользователи домена получают обычные права локальных пользователей на компьютере (задачи неуправленческого характера, такие как использование ПО, доступ к сетевым ресурсам и т.п.).

Присоединение к домену из Windows 8

Обычно вы будете присоединяться к домену из компьютера, подключенного к нему, но операционные системы Windows 7 и Windows 8 поддерживают как сетевые, так и автономные присоединения.

Сетевое присоединение к домену

Чтобы присоединиться к домену из Windows 8, когда компьютер подключен к сети, выполните следующие шаги.

1. Откройте аплет System (Система): чтобы обратиться к нему, щелкните на кнопке Start (Пуск) и начните набирать на клавиатуре Control Panel. Оказавшись в панели управления, щелкните на значке System.

   Вы должны увидеть диалоговое окно, подобное показанному на рис. 18.13.

   В этом примере компьютер еще не присоединен к домену, поэтому он находится в стандартной рабочей группе (по имени WORKGROUP), с которой начинают функционировать все компьютеры Windows.

2. Щелкните на ссылке Change settings (Изменить параметры), чтобы открыть диалоговое окно System Properties (Свойства системы), которое показано на рис. 18.14.

3. Простейший способ присоединиться к домену предусматривает щелчок на кнопке Change (Изменить). Это приводит к открытию диалогового окна, представленного на рис. 18.15.

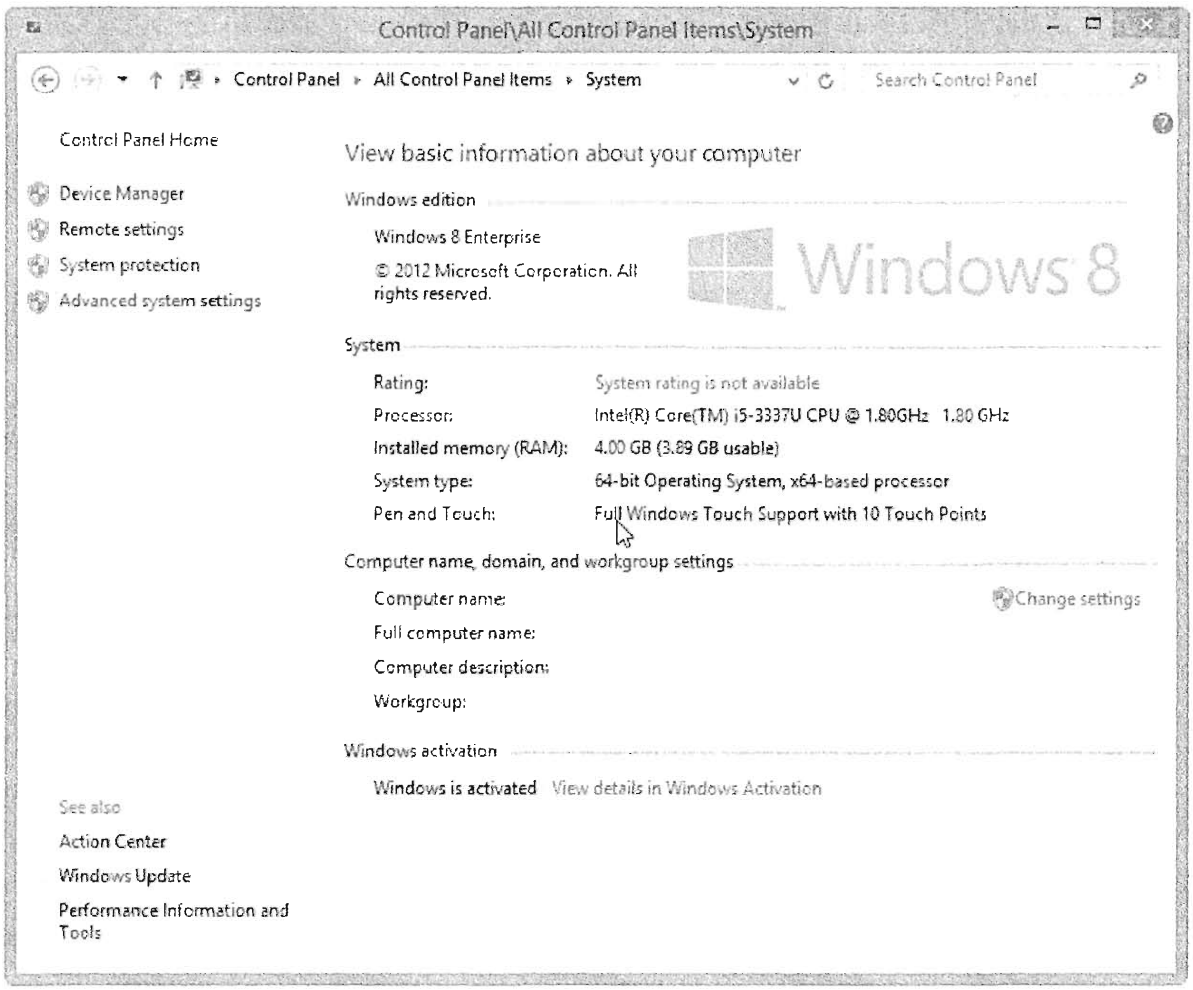


Рис. 18.13. Информация о системе для клиента Windows 8

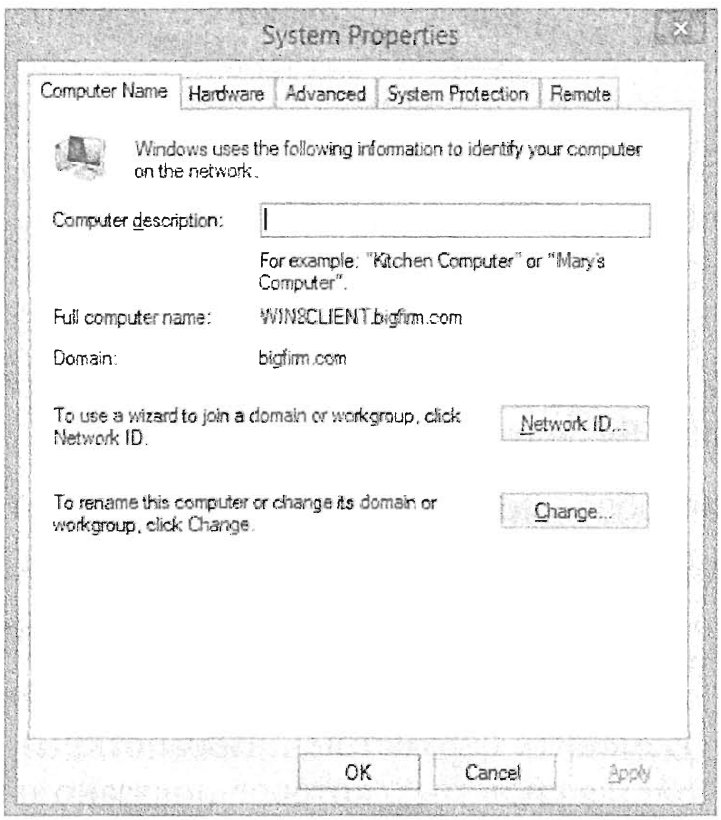


Рис. 18.14. Диалоговое окно System Properties

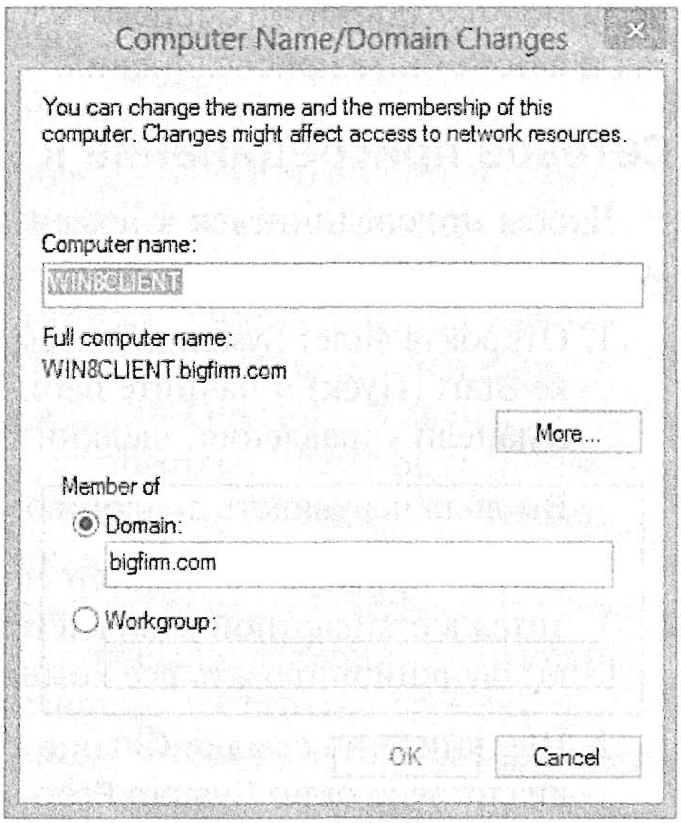


Рис. 18.15. Введите имя домена, чтобы присоединиться к нему

4. Введите имя домена (либо имя NetBIOS, либо имя FQDN) и щелкните на кнопке OK.

   После щелчка на кнопке OK будет предложено ввести имя пользователя и пароль учетной записи, имеющей разрешение на присоединение к домену (рис. 18.16).

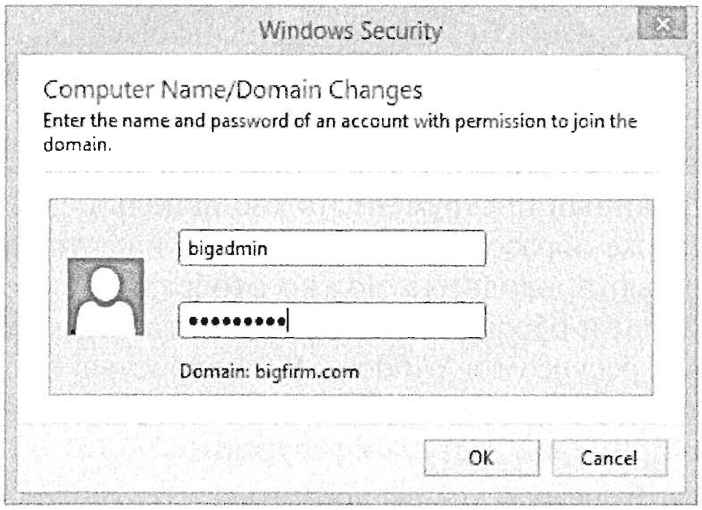


Рис. 18.16. Предоставьте учетные данные для присоединения к домену

5. Введите учетные данные. Не забывайте, что локальные администраторы не могут присоединять компьютеры к домену. Вы должны предоставить данные доменной учетной записи и щелкнуть на кнопке OK.

   Вы должны увидеть диалоговое окно, приглашающее в домен `bigfirm.com`.

6. Щелкните на кнопке OK; выдается предупреждение о том, что понадобится перезагрузка.
7. Щелкните на кнопке OK еще раз. После этого вам будет предложено перезагрузить компьютер.
8. Перезагрузите компьютер, чтобы завершить процедуру присоединения к домену.

Если вам не удалось присоединиться к домену, проверьте правильность указываемых учетных данных.

Автономное присоединение к домену с помощью `djoin.exe`

С присоединением к домену связана одна проблема: как быть, если вы не можете попасть на контроллер домена, чтобы создать учетную запись компьютера, или не можете выполнять запись на нем? Возможность связи с контроллером домена также иногда отсутствует, если вы организуете группу клиентских компьютеров перед их развертыванием или установкой клиентской ОС, когда они находятся в автономном режиме.

Появившаяся в Windows 7 и по-прежнему доступная в Windows 8 и Windows Server 2012 утилита `djoin.exe` позволяет присоединить компьютер к домену, даже если этот клиентский компьютер не может взаимодействовать с контроллером домена.

Windows RT и доступ к ресурсам

Операционная система Windows RT относится к другому типу, отличающемуся от Windows 8, но многие наборы средств и возможности доступа у них совпадают. Хотя, как утверждалось ранее, присоединиться к домену Active Directory не удастся, все же можно получать доступ к ресурсам в сети.

Диспетчер конфигурации системного центра Microsoft (Microsoft System Center Configuration Manager) версии 2012 SP1 поддерживает управление и конфигурирование устройств Windows RT посредством усовершенствованных служб управления мобильными устройствами (mobile device management — MDM).

Более распространенный способ доступа к ресурсам предусматривает применение проводника Windows; данный инструмент можно использовать для управления файлами и папками таким же образом, как это делается в настольных ОС, отличных от Windows RT. С помощью проводника можно отображать сетевые диски, получать доступ к общим ресурсам и обращаться к производственным устройствам хранения. Для доступа к сетевым ресурсам в Windows RT полностью поддерживаются многие типы соединений в точности, как это имеет место в устройствах Windows 8. Ниже приведено несколько примеров доступа к ресурсам.

- **Беспроводные сети.** В таких сетях вы должны устанавливать соединение и конфигурации вручную, поэтому наличие надлежащих SSID, учетных записей соединений и деталей, касающихся безопасности для соединений, является обязательным. В зависимости от методов обеспечения безопасности, принятых в организации, возможно, будет предоставлен только ограниченный доступ к ресурсам в среде.
- **Проводные сети.** Многие изготовители устройств предоставляют адаптер порта Ethernet. В большинстве организаций применяется DHCP, поэтому вам не потребуется конфигурировать свою сеть. Если необходимо настроить IP-адрес и подсеть, то это можно делать с помощью тех же самых шагов, что и в Windows 8 посредством панели управления.
- **Прокси-серверы.** Поскольку из-за отсутствия присоединения к домену групповые политики неприменимы, вам придется вручную сконфигурировать настройки прокси-сервера. Если вам нужно обнаруживать присутствие внутреннего прокси-сервера, то вы должны активизировать в корпоративной сети протокол автообнаружения веб-прокси (Web Proxy Autodiscovery Protocol). Это предусматривает конфигурирование специфичных параметров DHCP, а также веб-сервера, но с ростом числа компаний, внедряющих сценарии BYOD (bring-your-own-device — принеси свое собственное устройство), имеет смысл обдумать и такой вариант.
- **Возможность использования VPN-соединений.** Устройства Windows RT могут использовать VPN-подключения для создания в сети организации более четкого ощущения о наличии присоединения к домену. Многие IT-специалисты предпочитают применять этот вариант, потому что он помогает управлять безопасностью и доступом. Поскольку для Windows RT доступны многие опции VPN, вы должны ознакомиться с обзором VPN Windows RT, предоставленным Microsoft по адресу `https://technet.microsoft.com/ru-ru/library/jj900206.aspx`.

В настоящем разделе будет показано, как использовать утилиту `djoin.exe` для присоединения нового клиентского компьютера Windows 8 (`WIN8CLIENT`) к домену `bigfirm.com`, когда этот клиент функционирует в автономном режиме.

По существу утилита `djoin.exe` подготавливает для компьютера учетную запись в AD и затем экспортирует данные (называемые *большим двоичным объектом* (blob),

который необходим компьютеру с заданным именем для присоединения к домену) в текстовый файл. После этого автономный компьютер импортирует большой двоичный объект и присоединяется к домену. Такой большой двоичный объект может быть также добавлен в файл ответов для автономной установки, чтобы присоединить компьютер к домену (автономно) как часть процесса установки ОС.

По поводу большого двоичного объекта есть одно замечание: если вы создадите учетную запись компьютера в AD с помощью `djoin.exe` и затем откроете результирующий текстовый файл в надежде прочитать его, то вас ожидает разочарование, поскольку такой файл непригоден для восприятия человеком. Однако он содержит чувствительные данные наподобие пароля учетной записи машины и другую важную информацию, связанную с доменом. Ниже приведены шаги, позволяющие присоединить автономный компьютер к домену.

1. Запустите `djoin` на машине Windows 8 или Windows Server 2012, которая *может* взаимодействовать с контроллером домена.

   В результате будет создана учетная запись компьютера в AD для указанного имени компьютера и текстовый файл, используемый на шаге 3.

2. Переместите этот файл на автономный клиентский компьютер (безопасным образом).

3. Запустите `djoin` на автономной машине и импортируйте упомянутый текстовый файл.

Требования утилиты `djoin.exe`

Утилиту `djoin` можно запускать только на компьютерах с Windows 7 и выше, а также с Windows Server 2012. Допускается применение `djoin` для присоединения компьютера Windows 8 или Windows Server 2012 к контроллеру домена более низкого уровня (с указанием параметра `/downlevel`), но в рассматриваемом здесь примере клиентский компьютер Windows 8 будет присоединяться к домену Windows Server 2012.

Существует еще несколько общих требований. Пользователь, который запускает `djoin` на машине, предоставляющей учетную запись в AD, должен иметь право на добавления компьютеров в домен. Пользователи домена имеют такое разрешение, хотя по умолчанию они могут добавлять к домену только до 10 компьютеров.

Вы также должны быть знакомы с параметрами `djoin`, чтобы понимать команды, выдаваемые в приведенном ниже примере. Эти параметры описаны в табл. 18.1.

Таблица 18.1. Параметры `djoin`

Параметр	Описание
`/provision`	Создает учетную запись компьютера в Active Directory
`/domain`	Указывает домен, к которому будет присоединен компьютер
`/machine`	Указывает имя компьютера, который будет добавлен к AD DS, и который вы хотите присоединить к домену
`/savefile <путь_к_файлу>`	Указывает местоположение и файл для сохранения подготовленных метаданных
`/dcname` (необязательный)	Указывает имя конкретного контроллера домена, который вы хотите применять для создания учетной записи компьютера

Окончание табл. 18.1

Параметр	Описание
`/reuse` (необязательный)	Повторно использует существующую учетную запись машины (пароль этой учетной записи будет сброшен)
`/downlevel` (необязательный)	Предоставляет поддержку для применения контроллера домена, который функционирует под управлением Windows Server 2008 или более старой версии
`/printblob` (необязательный)	Создает большой двоичный объект, корректно закодированный для использования в файле ответов, который применяется при автономной установке
`/defpwd` (необязательный)	Использует стандартный пароль учетной записи машины (не рекомендуется)
`/requestodj`	При перезагрузке запрашивает автономное присоединение к домену (offline domain join — ODJ)
`/loadfile <путь_к_файлу>`	Указывает файл (созданный с помощью параметра `/savefile`), предназначенный для импортирования на автономный компьютер
`/windowspath`	Указывает путь к каталогу Windows в автономном образе; обычно `%systemroot%` или `%windir%`
`/localos`	Указывает локальную ОС как противоположность автономному образу (требует перезагрузки)

Добавление компьютера к домену в автономном режиме

Чтобы использовать `djoin` для присоединения компьютера к домену, команды `djoin` понадобится выполнять на двух разных машинах. В этом примере участвуют две машины.

- **`win8client.bigfirm.com`.** Эта машина уже присоединена к домену и может взаимодействовать с контроллером домена. Она будет применяться для подготовки новой учетной записи компьютера в AD (мы ссылаемся на нее как на *машину подготовки*).
- **`win8client2`.** Это вновь созданный клиент Windows 8, который находится в рабочей группе и не может взаимодействовать с контроллером домена.

Запуск `djoin.exe` с применением учетной записи обычного пользователя

Во избежание путаницы для запуска `djoin.exe` лучше всего использовать учетную запись, которая является членом группы `Domain Admins`, либо учетную запись, которой было делегировано право добавления компьютеров в домен. Обычные пользователи могут запускать `djoin.exe` и создавать учетные записи компьютеров, но не более 10 раз (потому что по умолчанию обычные пользователи ограничены присоединением к домену максимум 10 компьютеров). После этого такой пользователь получит отказ, как показано ниже:

```
Djoin djoin /provision /domain bigfirm.com /machine win7client11
/savefile c:\join.txt

Provisioning the computer account...

Failed to provision [win8client11] in the domain [bigfirm.com]: 0x216d.

Computer account provisioning failed: 0x216d.
Your computer could not be joined to the domain. You have exceeded the
maximum number of computer accounts you are allowed to create in this domain.
Contact your system administrator to have this limit reset or increased.
```

```
Подготовка учетной записи компьютера...

Не удалось подготовить [win8client11] в домене [bigfirm.com]: 0x216d.

Отказ при подготовке учетной записи компьютера: 0x216d.
Ваш компьютер не может быть присоединен к домену. Вы превысили
максимальное количество учетных записей компьютера, которые разрешено
создать в этом домене. Чтобы сбросить либо увеличить этот лимит,
обратитесь к своему системному администратору.
```

Начиная с этого момента, вам придется применять учетную запись администратора домена или делегировать это право другим (через групповую политику).

Для начала войдите в систему на клиентском компьютере `win8client.bigfirm.com` под учетной записью администратора домена и откройте окно командной строки с повышенными разрешениями. Затем запустите следующую команду, чтобы создать учетную запись компьютера в Active Directory и также создать текстовый файл для подготовки:

```
C:\Users\bigadmin>djoin /provision
  /domain bigfirm.com/machine win7client2 /savefile c:\join.txt
```

Вот результаты выполнения этой команды:

```
Provisioning the computer account...

Successfully provisioned [win8client2] in the domain [bigfirm.com].
Provisioning data was saved successfully to [c:\join.txt].

Computer account provisioning completed successfully.
The operation completed successfully.

Подготовка учетной записи компьютера...

Успешно подготовлена [win8client2] в домене [bigfirm.com].
Данные подготовки были успешно сохранены в [c:\join.txt]

Подготовка учетной записи компьютера успешно завершена.
Операция успешно завершена.
```

Оснастка Active Directory Users and Computers на контроллере домена (`bf1`) теперь будет содержать учетную запись компьютера `win8client2`, сохраненную в стандартной папке Computers (Компьютеры), как можно видеть на рис. 18.17.

Переместите результирующий текстовый файл `join.txt` из компьютера подготовки (`win8client`) на компьютер, который вы хотите присоединить (`win8client2`). В этом примере данный файл помещается в корневой каталог диска C. Затем откройте на клиентском компьютере (`win8client2`) окно командной строки с повышенными разрешениями и введите следующую команду:

```
Djoin /requestODJ /loadfile c:\join.txt /windowspath %systemroot% /localos
```

После перезагрузки компьютер присоединится к домену.

За дополнительными сведениями по поводу использования `djoin` с автоматическими установками и делегированию права на присоединение компьютеров к домену обращайтесь по адресу `http://technet.microsoft.com/en-us/library/ff793312.aspx`.

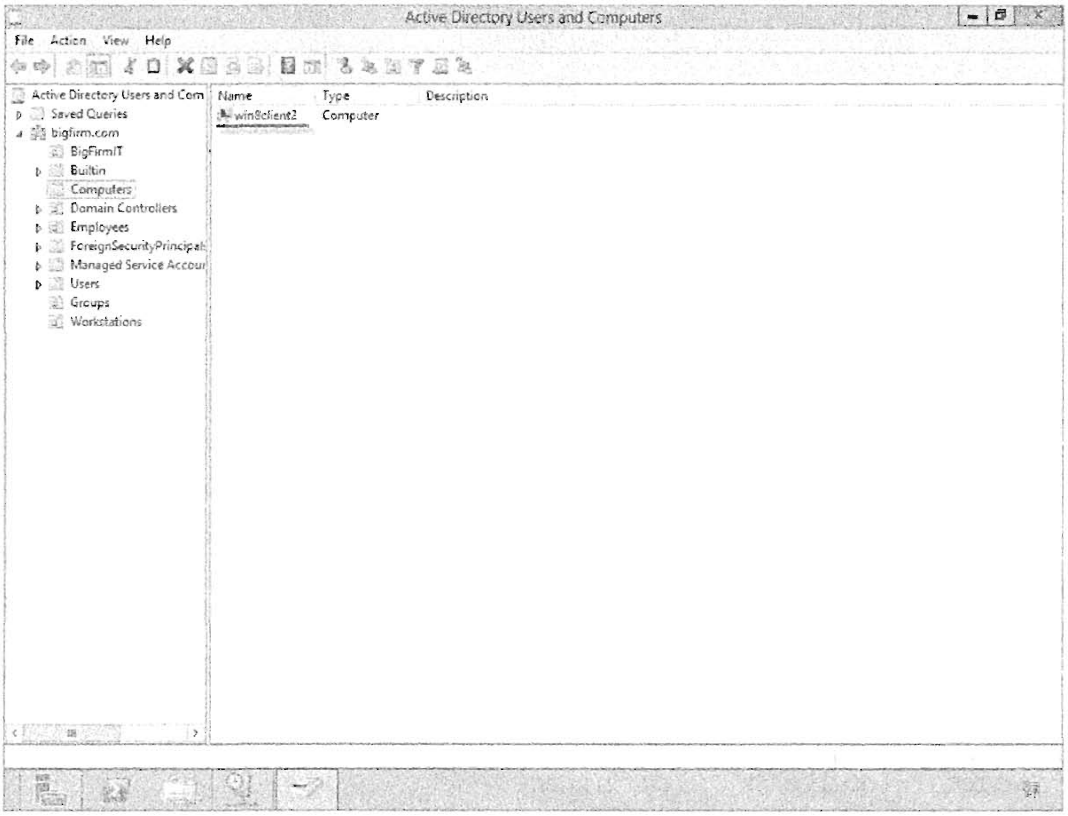


Рис. 18.17. Выполнение `djoin` привело к добавлению учетной записи компьютера в AD DS

Присоединение к домену с помощью PowerShell

Дополнения к PowerShell, появившиеся в Windows Server 2012, а также тот факт, что в Windows 8 есть прочный фундамент везде, где применяется PowerShell, очень полезны для IT-профессионала. Маловероятно, что вы будете сидеть непосредственно за клиентским компьютером и присоединять его к домену через PowerShell, но поскольку вы можете запустить эту команду дистанционно или, возможно, сделать ее частью сценария, мы рассмотрим процесс подобного рода.

Чтобы присоединить компьютер к домену из PowerShell, вы будете использовать командлет `Add-Computer`.

1. Откройте консоль PowerShell от имени администратора.
2. Введите **`Add-Computer -DomainName Bigfirm.com`**
3. Предоставьте учетные данные с правами на присоединение машины к домену (на рис. 18.18 приведен пример).

Более подробную информацию о командлете `Add-Computer` можно найти по адресу `http://tinyurl.com/c18PSAdd`.

Изменение паролей пользователей домена

Надежный подход к обеспечению безопасности требует регулярного изменения паролей, которые должны быть известны только пользователям. Операционная система, применяемая пользователями для присоединения к домену Windows Server 2012, предполагает вмешательство пользователей в процесс изменения паролей.

Несмотря на то что бо́льшая часть этой книги адресована администраторам, данный раздел содержит информацию, которую администратор должен будет донести до рядовых пользователей, чтобы они сами могли менять свои пароли.

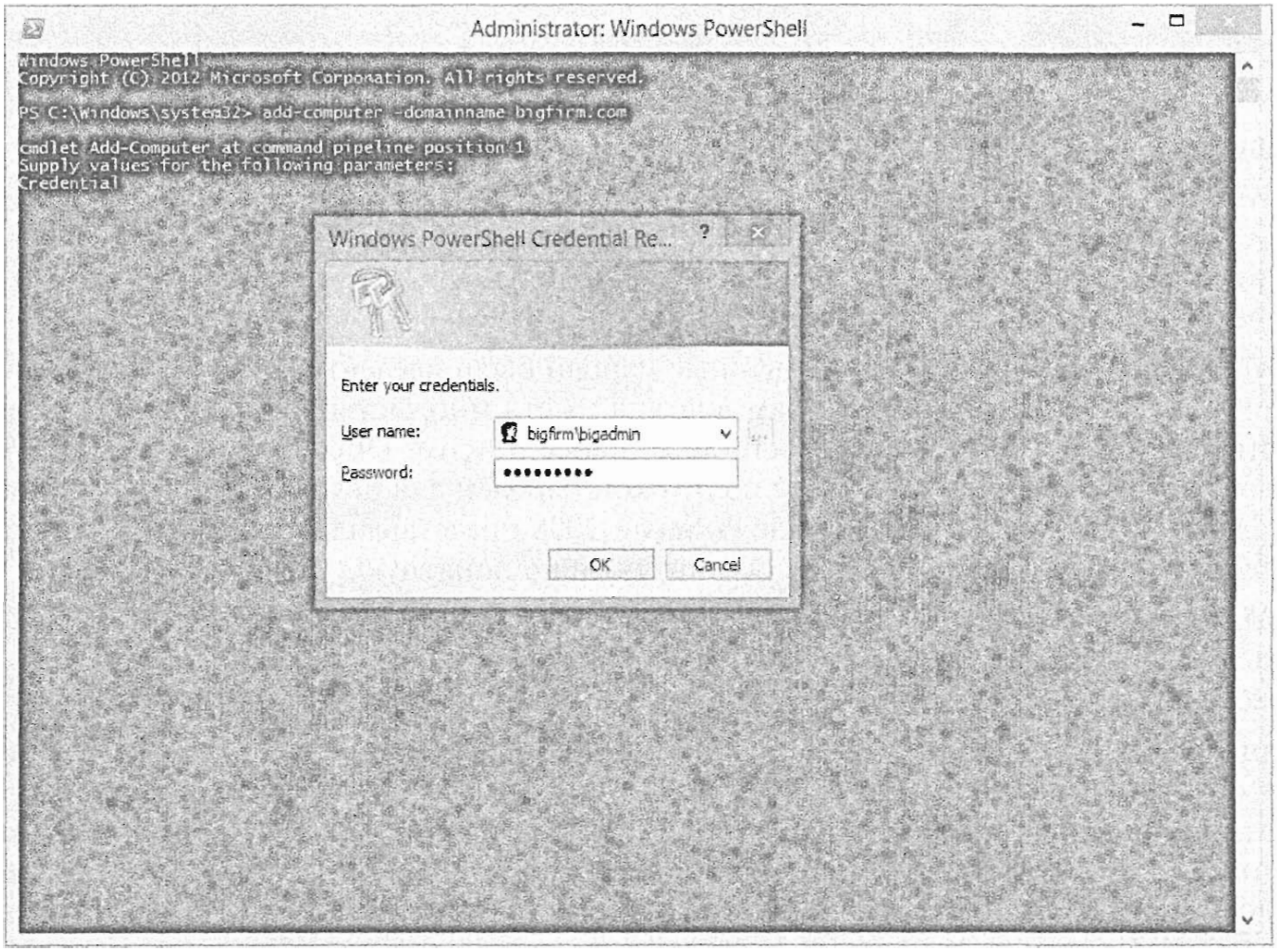


Рис. 18.18. Командлет PowerShell по имени `Add-Computer` и окно аутентификации

Хорошая новость заключается в том, что изменить пароль чрезвычайно просто: вся информация, необходимая для успешного выполнения этого процесса, предоставляется пользовательским интерфейсом.

- Если политика требует, чтобы пользователь изменял свой пароль при первом использовании учетной записи, ему будет предложено сделать это.
- Если политика требует, чтобы пользователь изменял свой пароль из-за того, что срок его действия вскоре истекает, ему будет предложено изменить пароль, объяснено, каким образом это делается, и указано, сколько времени остается до истечения срока действия пароля.
- Если пароль, введенный пользователем, не отвечает стандартам безопасности, определенным групповой политикой, пользователь получит напоминание о том, каковы эти стандарты, чтобы он мог привести пароль в соответствие с ними.

Если пользователь *забыл* свой старый пароль, то он не сможет изменить его самостоятельно, а если администратор следует рекомендуемым приемам обеспечения безопасности, то и ему этот пароль не известен. Администратору понадобится обновить пароль для учетной записи пользователя домена, а затем указать, что пароль должен был изменен при первом входе пользователя в систему.

Пример из практики

Политики паролей и расширенные возможности

В Windows Server 2012 предоставляются те же самые политики пользовательских паролей, которые существовали со времен Windows Server 2008 и Windows Server 2008 R2. В Windows Server 2012 были расширены уже доступные возможности, такие как детализированные пароли.

В Windows Server 2008 детализированные пароли были введены для того, чтобы позволить IT-специалистам и группам доступа иметь множество участников безопасности в одном и том же домене или лесе. Ранее в Active Directory можно было управлять только одной стандартной политикой паролей для целого домена. Установка детализированных паролей в Windows Server 2008 представляла собой довольно утомительную задачу, к тому же не особо интуитивно понятную.

В Windows Server 2012 это средство стало намного более ясным и позволяло проводить конфигурирование в диспетчере серверов или задействовать полный набор своих возможностей из PowerShell 3.0.

Стандартная политика домена (Default Domain Policy) в Windows Server 2012 обеспечивает принудительные регулярные изменения пароля и соблюдение правил, регламентирующих сложность паролей. Настройка групповой политики находится в узле Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Account Policies \ Password Policy (Конфигурация компьютера \ Политики \ Настройки Windows \ Настройки безопасности \ Настройки учетных записей \ Политика паролей).

Настройки стандартной политики паролей перечислены ниже.

- Enforce Password History (Принудительно применять хронологию паролей). Это требует от пользователей применять определенное количество уникальных паролей, прежде чем можно будет повторно использовать какой-то старый пароль. Стандартное количество составляет 24 пароля.
- Maximum Password Age (Максимальный возраст пароля). Это количество дней, в течение которых пароль можно применять, прежде чем пользователь будет обязан его изменить. По умолчанию равно 42 дня.
- Minimum Password Age (Минимальный возраст пароля). Это минимальное количество дней, в течение которых пароль должен использоваться, прежде чем пользователь сможет его изменить. По умолчанию составляет 1 день.
- Minimum Password Length (Минимальная длина пароля). Это минимальное количество символов, которые должен содержать пароль. По умолчанию равно 7.
- Passwords Must Meet Complexity Requirements (Пароли должны удовлетворять требованиям к сложности). Этот параметр, включаемый по умолчанию, вводит в действие несколько правил, касающихся создания пароля. Например, пароль не должен содержать больше двух следующих друг за другом символов, которые являются частью полного имени пользователя.

Еще более удачная идея состоит в том, чтобы рекомендовать пользователям применять кодовые фразы вместо простых паролей. *Кодовая фраза* — это комбинация слов, которые в правильно указанном порядке формируют пароль. Кодовая фраза как единое целое по-прежнему должна удовлетворять требованиям к сложности, устанавливаемым политикой паролей, но в общем случае она длиннее и может содержать пробелы, поэтому угадать кодовую фразу злоумышленникам гораздо труднее, чем обычный пароль.

В сочетании с подстановкой гласных (с заменой некоторых букв, скажем, гласных, цифрами) пользователи могут создавать очень сложные кодовые фразы. Например, хорошим кодовой фразой может быть My g00d d0g c4tch3s fr1sb33s! Ее довольно легко запомнить, вместе с тем она длинная (29 символов), сложная (из-за наличия нескольких слов, пробелов и подстановки гласных) и трудная для взлома.

В главе 9 приведен пример создания объекта GPO для сложных паролей.

Соображения безопасности требуют, чтобы вы ни в коем случае не разрешали двум пользователям применять одну и ту же учетную запись. Даже если они никогда не используют такую учетную запись одновременно (такое дублирование учетной записи создаст массу проблем вплоть до потери изменений профиля), все равно это неудачная идея. Если учетную запись применяют сразу несколько человек, то вы никогда не узнаете, кто какими ресурсами пользуется в сети — или пытается использовать ресурсы, для которых отсутствует авторизация. Аудит безопасности требует, чтобы у каждого пользователя была одна учетная запись и один пароль.

Кстати, этот совет относительно уникальных паролей для каждого пользователя применим не только к обычным пользователям. Чтобы сделать возможным аудит безопасности, все администраторы Windows Server должны иметь собственные базовые учетные записи пользователей (вместо использования всеми ими учетной записи `Administrator`). Рекомендуемый подход предусматривает наличие отдельной учетной записи пользователя-администратора. Ниже приведен пример.

Учетная запись обычного пользователя: `KevinB`. Кевин мог бы применять эту учетную запись для обращения ко всем своим базовым производственным ресурсам, электронной почте и личным файлам.

Учетная запись пользователя-администратора: `A-KevinB`. Кевин мог бы использовать эту учетную запись для входа на серверы, для внесения изменений в домен или для выполнения любых задач, требующих повышенных разрешений.

Вы также должны с помощью групповой политики требовать регулярных изменений паролей. Хотя такая модель требует большего объема работы по управлению учетными записями, она позволяет отслеживать действия каждого администратора сервера и легко отключать административный доступ, когда кто-то увольняется из компании, без необходимости в изменении административных паролей для всех. Политики паролей распространяются на целый домен, поэтому имеет смысл следовать рекомендуемым подходам в отношении всех пользователей в домене.

Изменение доменных паролей из Windows 8 и Windows 7

Чаще всего пользователь будет изменять пароли при двух обстоятельствах:

- когда администратор только что сбросил пароль его доменной учетной записи и потребовал изменить его;
- когда групповая политика обусловила истечение срока действия пароля.

В Windows 7 и Windows Vista применяется тот же самый процесс и предусмотрен одинаковый графический пользовательский интерфейс, поэтому в последующих разделах мы объединяем информацию об изменении доменных паролей в этих двух операционных системах.

Изменение паролей при первом входе в систему

Когда администратор инициирует сброс пароля (по причинам, связанным с безопасностью, или для новой учетной записи), пользователю будет предложено ввести новый пароль, когда он попытается в первый раз войти в систему (рис. 18.19). Стандартный пароль, применяемый администратором, предназначен просто для защиты учетной записи до тех пор, пока она не начнет использоваться.

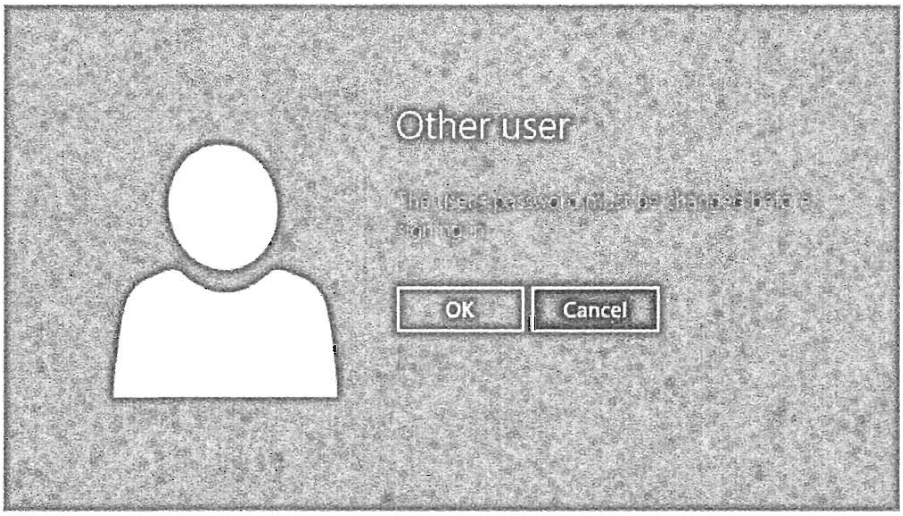


Рис. 18.19. Изменение пароля перед входом в первый раз

Когда пользователь щелкает на кнопке OK, ему сообщается о необходимости ввода нового пароля (рис. 18.20).

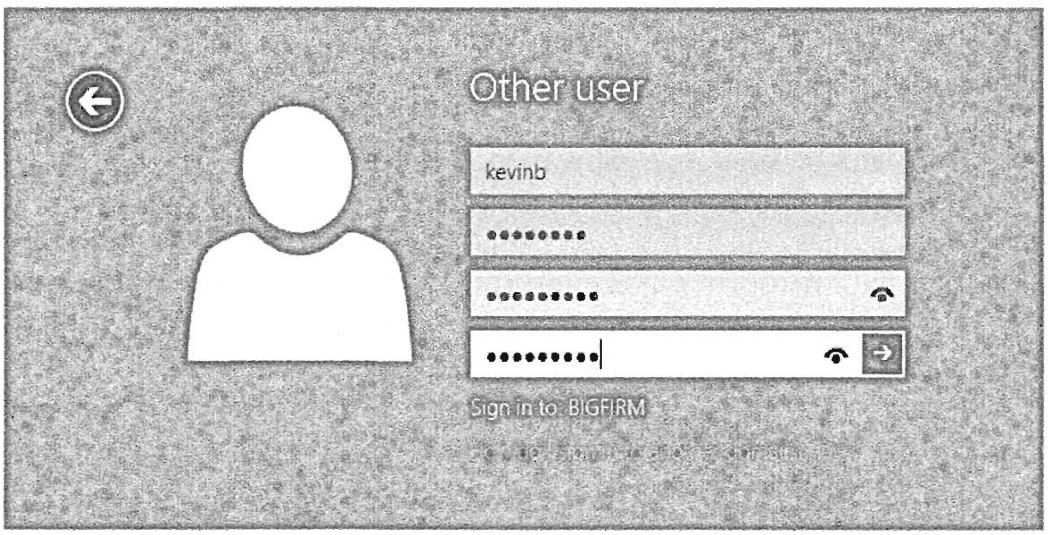


Рис. 18.20. Ввод нового пароля

Пользователь указывает старый пароль и вводит новый пароль. Согласно стандартной политике домена, новый пароль не может совпадать со старым и должен удовлетворять требованиям к длине и сложности, иначе пользователю будет предложено ввести пароль, который соответствует руководящим принципам безопасности, и указано, каким образом удовлетворить их требования. После того, как пользователь успешно изменит пароль, на экране появится сообщение о том, что пароль был изменен. Щелкнув на кнопке OK, пользователь сможет войти в систему с новым паролем. Вот и все действия. После смены пароля пользователь может входить в систему как обычно.

Изменение паролей по требованию

Когда срок действия пароля приближается к своему истечению, за несколько дней до этого момента пользователь начинает получать сообщения, которые уведомляют о скором окончании срока действия пароля и объясняют, что конкретно необходимо предпринять для изменения пароля. Иногда потребность изменить пароль может возникнуть у самого пользователя. Простейший способ изменения пароля предусматривает нажатие комбинации клавиш <Ctrl+Alt+Del> для открытия графического пользовательского интерфейса безопасности Windows и выбор пункта Change a password (Изменить пароль), как показано на рис. 18.21. Чтобы попасть на этот экран, можно также щелкнуть на кнопке Windows Security (Безопасность Windows), расположенной в меню Start (Пуск).

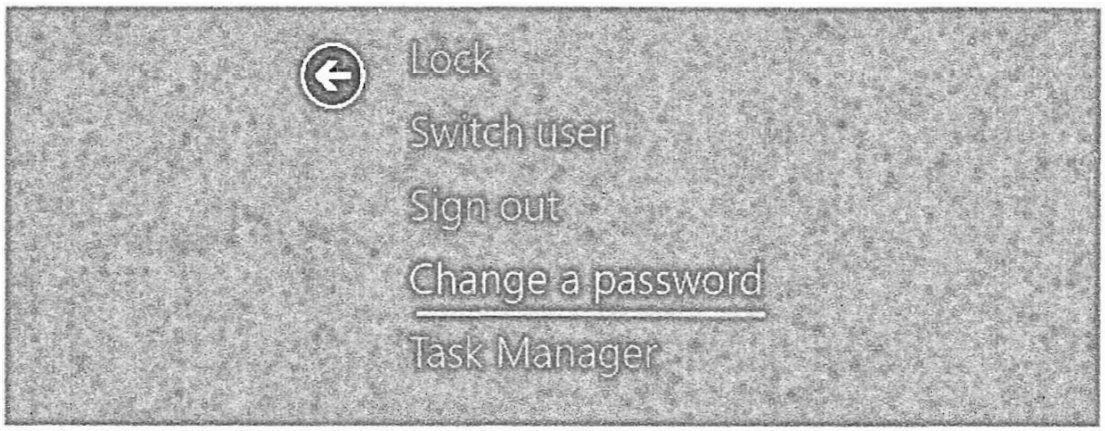


Рис. 18.21. Изменение пароля из графического пользовательского интерфейса безопасности Windows

Когда пользователь выбрал вариант Change a password, он увидит экран Change a Password (Изменение пароля), представленный на рис. 18.22. Здесь пользователю предлагается ввести старый и новый пароли. Опять-таки, если новый пароль не отвечает требованиям безопасности, пользователь увидит сообщение об ошибке, уведомляющее о действующих политиках паролей. После ввода старого и нового паролей (два раза) и щелчка на значке со стрелкой влево пароль изменится.

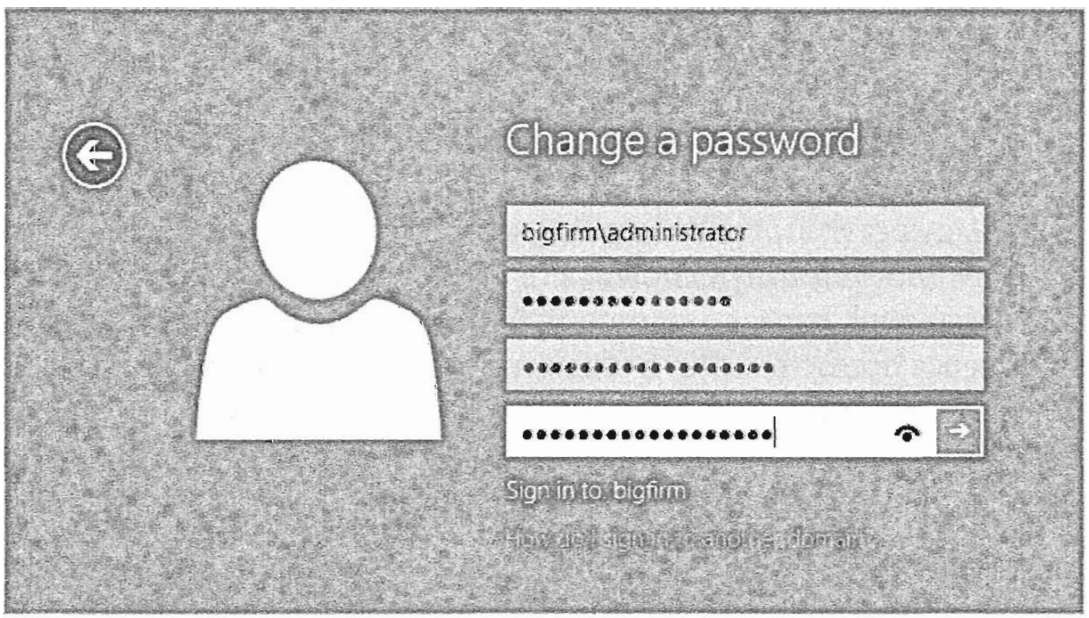


Рис. 18.22. Форма изменения пароля

Избегайте повторных запросов пароля после его изменения

Если у пользователя есть более одного компьютера (например, ноутбука и настольной машины), и он вошел в системы обоих компьютеров, то после изменения пароля пользователь должен выйти из систем на одной и на другой машине, после чего снова войти. Сеансы по-прежнему будут работать, но поскольку доменный пароль изменился, могут выдаваться повторные запросы на его ввод при обращении к сетевым ресурсам, таким как серверы Exchange, сайты SharePoint и другие приложения, требующие аутентификации. Конечно, можно продолжать вводить пароль при каждом запросе, но проще войти в систему с новым паролем и тем самым избежать появления таких запросов.

Подключение к сетевым ресурсам

Одной из главных причин присоединения к домену является доступ к ресурсам этого домена, таким как принтер, расположенный в другом крыле офисного здания, или файлы документов, с которыми вам необходимо работать. Вы могли бы получать доступ к фотоматериалам компании, слайд-шоу и другим носителям, нужным для проведения маркетинговой кампании. В чем бы ни состояла конкретная потребность, суть заключается в том, что вовсе необязательно, чтобы все необходимые устройства и информационные ресурсы были подключены непосредственно к вашему клиентскому компьютеру или хранились в нем. Более того, хранение их в сети является идеальным вариантом, поскольку в этом случае они более защищены (доступ к ним контролируется централизованно и в идеальном случае файлы подвергаются регулярному резервному копированию). Ниже приведены примеры сетевых ресурсов:

- принтеры;
- общие папки и файлы;
- беспроводные устройства (вроде беспроводных принтеров);
- службы (такие как веб-службы);
- приложения компании.

Благодаря множеству изменений в Active Directory и Group Policy, подключение к общим ресурсам для пользователей выглядит довольно просто. Вы по-прежнему можете пользоваться средствами наподобие Network Discovery (Сетевое обнаружение) в качестве простого способа поиска компьютером интересующих ресурсов в сети, хотя в большинстве производственных сред так поступать не рекомендуется. С появлением предпочтений групповой политики (Group Policy preferences — GPP) IT-специалистам теперь гораздо проще публиковать ресурсы для сотрудников или подразделений через объекты GPO и членство в группах домена. Пользователи могут продолжать выполнять поиск нужных опубликованных ресурсов в Active Directory. Это означает, что пользователю нет необходимости знать, где именно устройство установлено или находится. Пользователь даже может не знать точного имени общей папки или принтера либо сервера, на котором это хранится. Если ресурс опубликован в Active Directory, то пользователь, выполнив несложный поиск, почти наверняка найдет этот ресурс и сможет воспользоваться им.

Существует несколько способов доступа к общим ресурсам. В настоящем разделе мы рассмотрим эти более распространенные приемы для каждой клиентской ОС из числа обсуждаемых в главе.

- Ресурсы публикуются посредством объектов GPO.
- Вы можете искать и получать доступ к ресурсам, которые опубликованы в Active Directory.
- Вы можете подключаться к общим сетевым ресурсам (например, общим папкам и принтерам) из командной строки.
- Вы можете создавать сетевой диск для общих сетевых папок.
- Вы можете использовать проводник Windows для подключения к путям UNC (Uniform Naming Convention — универсальное соглашение по именованию), которые описывают путь к месту в сети в форме `\\имя_компьютера\имя_общего_ресурса`.

В последующих примерах будет производиться доступ к ресурсам, находящимся в домене `bigfirm.com`. Эти ресурсы и их сетевые размещения указаны в табл. 18.1.

Таблица 18.1. Сетевые ресурсы, используемые в примерах этого раздела

Тип сетевого ресурса	Путь к сетевому ресурсу	Адрес машины с сетевым ресурсом
Файловый общий ресурс отдела маркетинга	`\\bf1\\BF_Marketing`	`bf1.bigfirm.com`
Черно-белый принтер	`\\bf1\BF_Main_Printer`	`bf1.bigfirm.com`

Публикация ресурсов посредством объектов групповой политики

Начиная с версии Active Directory в Windows Server 2008, вы можете публиковать все наиболее распространенные ресурсы для клиентских (и серверных) устройств в централизованном порядке. Новым средством, которое обсуждалось в главе 9, являются предпочтения групповой политики (GPP). Они позволяют выполнять такие операции, как создание отображений дисков, создание ярлыков и конфигурирование настроек среды (рис. 18.23). Это можно делать как для пользователей, так и для компьютеров, находящихся в определенных организационных единицах (organizational unit — OU) или группах домена.

Управление конфигурацией ресурсов в любой организации должно проводиться централизованно и контролироваться членством в группах Active Directory. После установки этих групп вы можете управлять доступом к общим файлам, принтерам и приложениям с помощью политик. Подходы из прошлого, предусматривающие разрешение использования Network Discovery и открытие совместного доступа к ресурсам на локальных компьютерах, больше неактуальны, т.к. в организациях производится аудит безопасности и соответствия. В следующем разделе мы пройдемся по созданию и публикации ряда ресурсов на рабочих станциях. В рассмотренных далее примерах мы сосредоточим внимание на отделе маркетинга `bigfirm.com` и опубликуем требуемые ресурсы на устройстве `WIN8CLIENT`, которое применяется сотрудниками этого отдела.

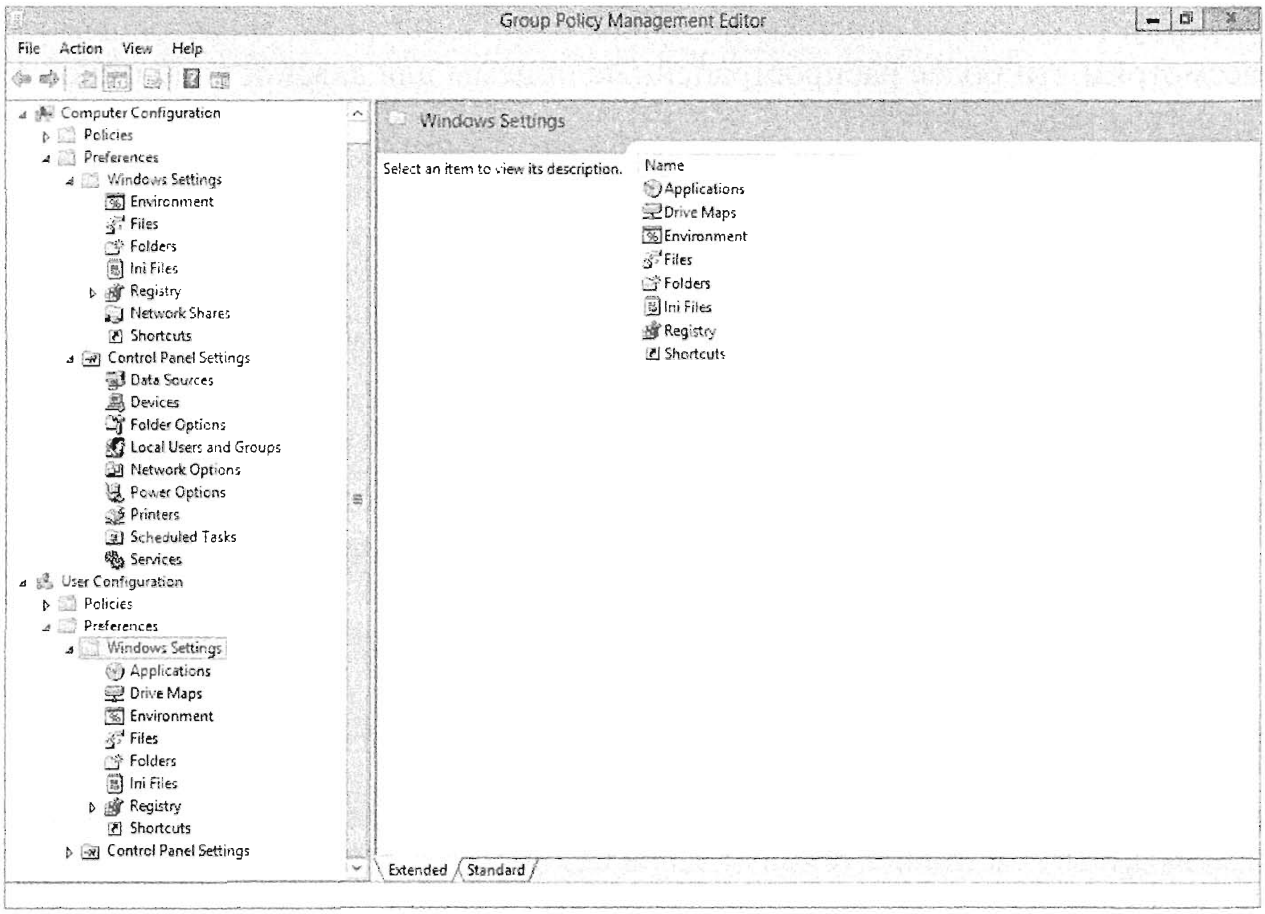


Рис. 18.23. Предпочтения групповой политики в редакторе управления групповыми политиками

Обычно администраторы домена хранят файлы компании в централизованных, безопасных и надежных местах, для которых легко создавать резервные копии (т.е. такие файлы не хранятся на индивидуальных компьютерах). Чтобы получить доступ к этим ресурсам, вы должны позаботиться о применении к общим файлам подходящих групп Active Directory (AD) и приступить к конфигурированию объектов GPO для их опубликования.

Публикация сетевого общего файлового ресурса

В следующем примере вы ознакомитесь с процедурой предоставления опубликованных ресурсов конечному пользователю. Вы начнете процесс с создания организационной единицы `Groups` и группы `Marketing` в Active Directory. Здесь предполагается, что вы понимаете, как создавать организационные единицы и глобальные группы домена. Если вы этого не знаете, обратитесь в главу 7.

1. Откройте оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory) и создайте организационную единицу по имени `Groups`.
2. Выберите организационную единицу `Groups` и создайте новую глобальную группу под названием `Marketing`. Пример того, как это может выглядеть, представлен на рис. 18.24.
3. Откройте группу `Marketing` и добавьте в нее сотрудника по имени `KevinB`.
4. Щелкните на кнопке Apply (Применить) и пользователь будет добавлен в группу `Marketing`, после чего можно приступать к конфигурированию объекта GPO.

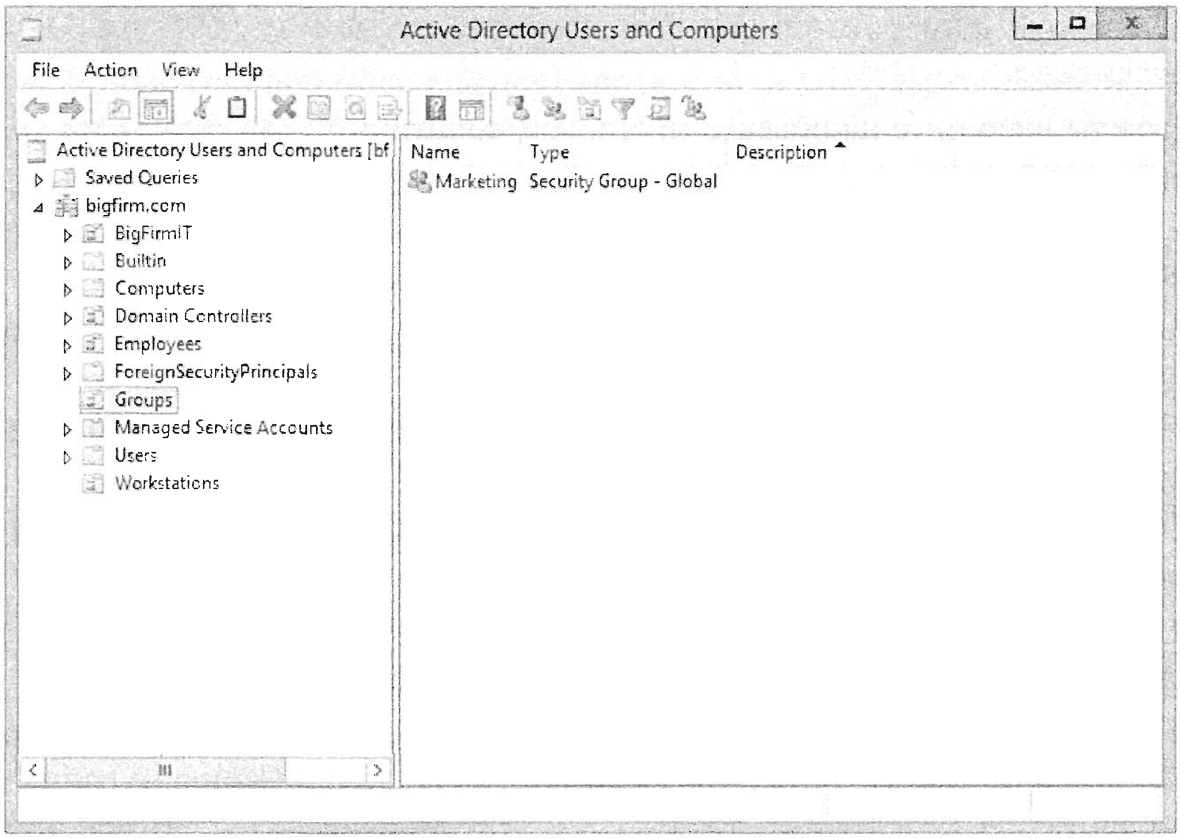


Рис. 18.24. Настройка организационной единицы и группы в Active Directory

5. Чтобы создать GPO, сначала откройте инструмент Administrative Tools⇨Group Policy Management (Администрирование⇨Управление групповой политикой).
6. Щелкните правой кнопкой мыши на папке Group Policy Objects (Объекты групповой политики) и выберите в контекстном меню пункт New (Создать), как показано на рис. 18.25.

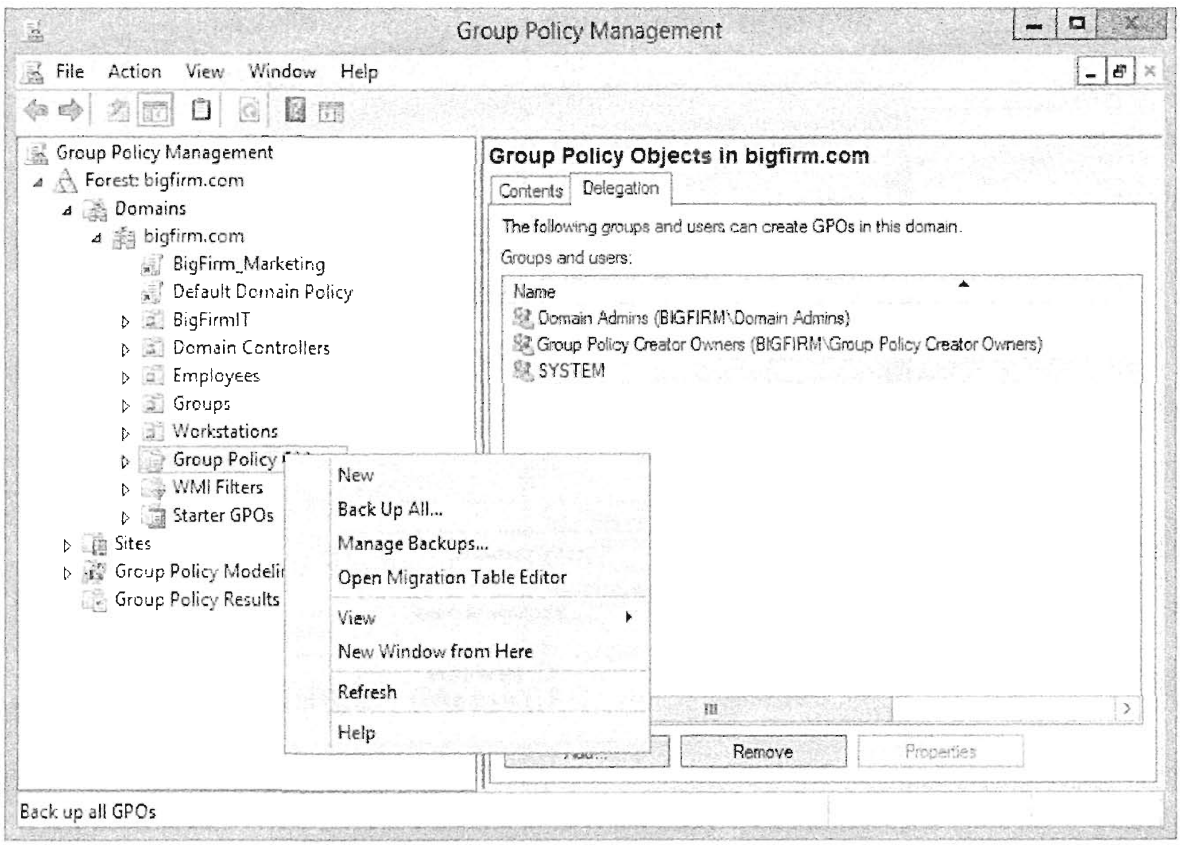


Рис. 18.25. Создание нового объекта GPO

7. Для целей данного примера назначьте этому объекту GPO имя `BigFirm_Marketing`.
8. Дважды щелкните на объекте групповой политики `BigFirm_Marketing`.

   Вы увидите первую вкладку диалогового окна Group Policy под названием Scope (Область действия). В разделе Scope понадобится указать, что этот объект GPO должен применяться к группе `Marketing`.
9. Щелкните на кнопке Add (Добавить) в разделе Security Filtering (Фильтрация безопасности), введите `Marketing` и щелкните на кнопке OK.
10. Теперь выберите все остальные группы и щелкните на кнопке Remove (Удалить).

    Единственной группой, к которой должен применяться этот объект GPO, является `Marketing`.
11. Щелкните правой кнопкой мыши на политике `BigFirm_Marketing` в левой панели и выберите в контекстном меню пункт Edit (Правка).
12. Откроется редактор управления групповыми политиками (Group Policy Management Editor). Выберите узел User Configuration (Конфигурация пользователя).
13. Раскройте узел User Configuration\Preferences\Windows Settings (Конфигурация пользователя \ Предпочтения \ Настройки Windows). Вы увидите все базовые предпочтения, которые можно модифицировать для пользователя.
14. Щелкните правой кнопкой мыши на Drive Maps (Отображения устройств) и выберите в контекстном меню пункт New⇨Mapped Drive (Создать⇨Отображенное устройство).

    Откроется диалоговое окно New Drive Properties (Свойства нового устройства). На рис. 18.26 показана основная конфигурация.

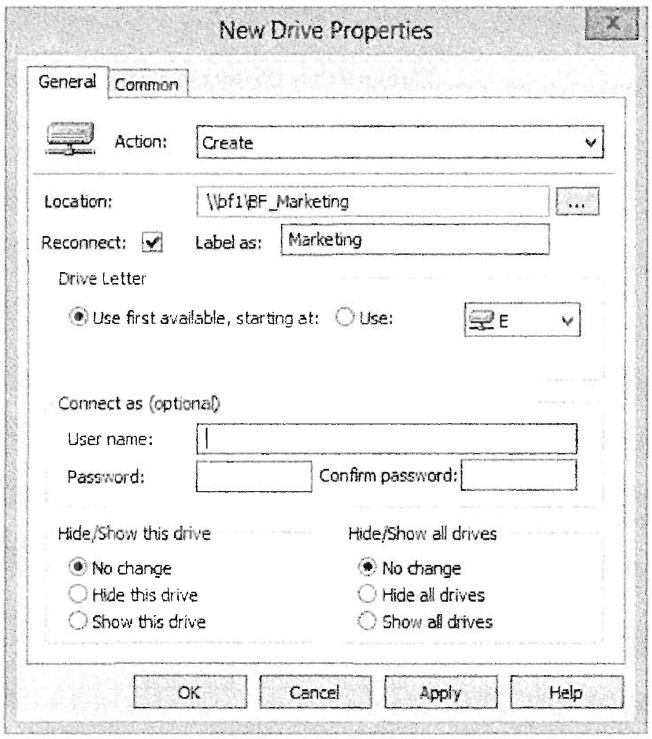


Рис. 18.26. Создание нового предпочтения политики по отображению устройств

- В поле Action (Действие) выберите Create (Создать).
- В поле Location (Размещение) введите путь UNC к отображенному устройству: **\\bf1\BF_Marketing**.
- Отметьте флажок Reconnect (Подключать повторно).
- В поле Label as (Пометить как) укажите, как этот диск должен выглядеть для конечных пользователей. В нашем примере используется `Marketing`.
- В разделе Drive Letter (Буква устройства) выберите переключатель Use first available, starting at: (Использовать первую доступную, начиная с:). Можно также выбрать переключатель Use: (Использовать:) и выбрать одну из букв в раскрывающемся списке.
- Для всех остальных параметров оставлен выбор по умолчанию, но вы можете модифицировать их, приведя в соответствие с имеющейся средой.

15. Щелкните на кнопке Apply и на кнопке OK, чтобы возвратиться в раздел Drive Maps.

    Вы должны увидеть, что в правой панели появилось отображенное устройство E.

Теперь, когда вы располагаете созданным объектом GPO и определенной политикой для отображения устройств, вам нужно связать их с `bigfirm.com`, чтобы можно было начать пользоваться этой политикой (рис. 18.27). После связывания данного объекта GPO с `bigfirm.com` эта политика будет применена к пользователям отдела `Marketing`, независимо от того, в какой дочерней организационной единице они находятся.

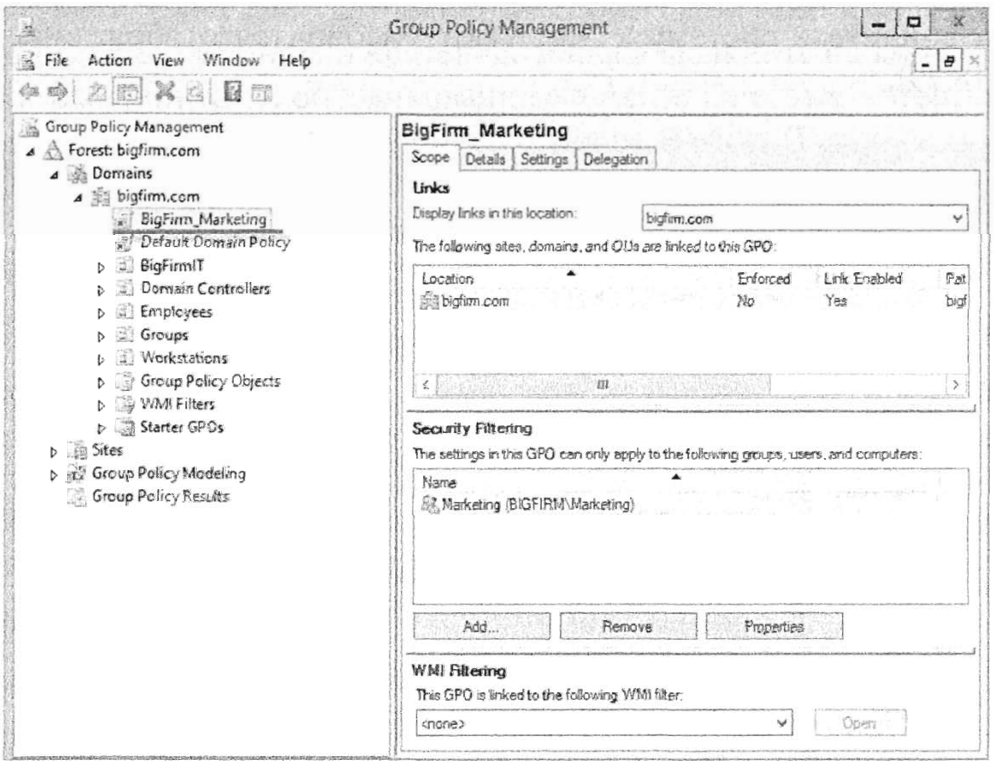


Рис. 18.27. Объект GPO, примененный к `bigfirm.com`

Все последующие действия выполняются на стороне клиента. Вам нужно удостовериться в том, что объекты GPO применяются к пользователю. После входа в систему `WIN8CLIENT` вы можете принудительно обновить групповую политику в

окне командной строки. Чтобы обновить политику на рабочей станции, выполните следующие шаги.

1. Откройте окно командной строки с повышенными разрешениями.
2. Введите команду `GPUPDATE.EXE /FORCE`.

   Вам будет предложено выйти из системы `WIN8CLIENT`, т.к. созданные вами настройки являются специфичными для пользователя (рис. 18.28).

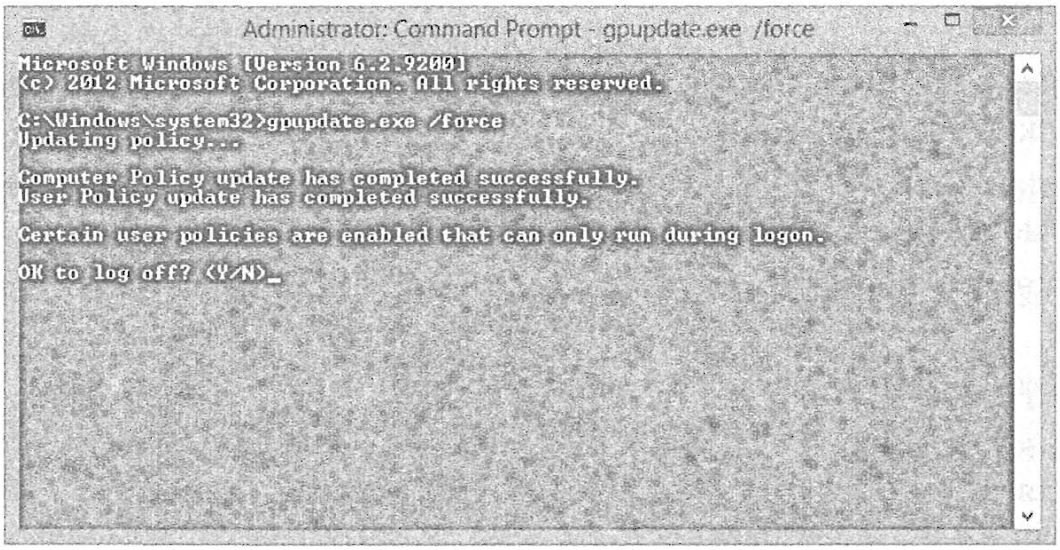


Рис. 18.28. Обновление групповой политики с помощью настроек для пользователя

3. Введите `Y`, чтобы ответить утвердительно, в результате чего вы выйдете из системы.
4. Снова войдите в систему `WIN8CLIENT`. Появится отображение устройства (рис. 18.29).

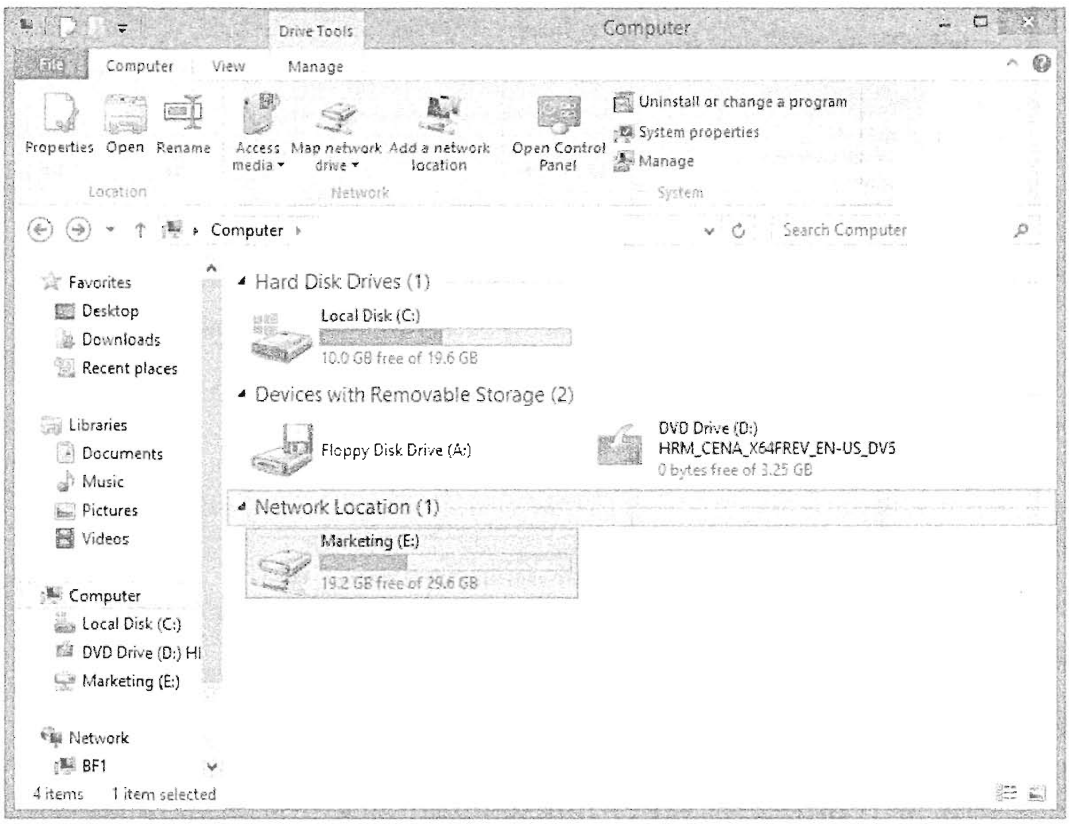


Рис. 18.29. Диск `Marketing`, отображенный на папку `Computer`

Добавление сетевого принтера

Сетевой принтер можно добавить путем нахождения устройства в графическом пользовательском интерфейсе, посредством инструментов командной строки или с помощью аплета Network (Сеть).

Обнаружение принтера с помощью поиска устройства

В Windows 8 поиск устройств и носителей был существенно упрощен за счет добавления в проводник файлов значка Access media (Доступ к носителям). Как показано на рис. 18.30, вы можете выбрать значок Access media для проведения поиска в сети любого общего или опубликованного устройства, будь оно принтером или общим носителем.

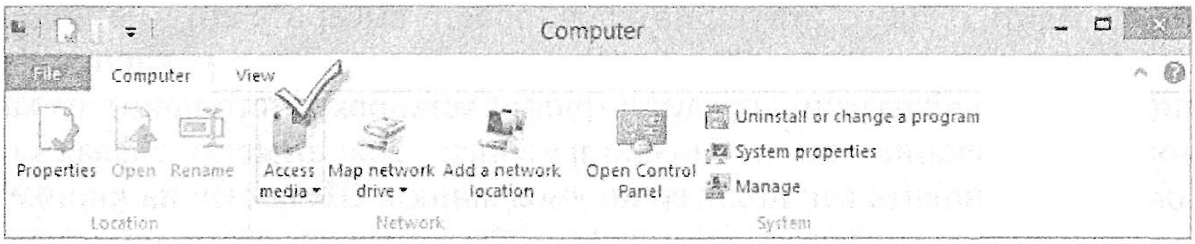


Рис. 18.30. Значок Access media в проводнике файлов

В раскрывающемся списке Find (Искать) выберите вариант Printers (Принтеры). При наличии в сети множества доменов поиск можно конкретизировать, выбрав нужное имя домена в раскрывающемся списке, который находится справа от списка Find. Если список принтеров оказывается довольно длинным, можете искать по имени или ключевому слову либо воспользоваться вкладкой Advanced для поиска по другим свойствам. После установки критериев поиска щелкните на кнопке Find Now (Начать поиск). Все принтеры, опубликованные в Active Directory, которые удовлетворяют заданным критериям поиска, появятся в окне Results (Результаты).

Чтобы добавить найденный принтер в свой компьютер, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Connect (Подключиться). Принтер будет установлен, и вы увидите его в своей папке Printers (Принтеры).

Добавление сетевого принтера из командной строки

Зная имя необходимого принтера и имя сервера печати, к которому он присоединен, принтер можно добавить из командной строки с помощью команды `start`. Например, чтобы добавить принтер `bf_main_printer`, находящийся на сервере `bf1`, к клиенту Windows 8 или Windows 7, откройте окно командной строки и введите следующую команду:

```
start \\bf1\bf_main_printer
```

Когда принтер устанавливается, откроется очередь печати для этого принтера и он будет перечислен в аплете Devices and Printers (Устройства и принтеры).

Добавление сетевого принтера с помощью аплета Network

Чтобы добавить сетевой принтер к клиенту Windows 8 или Windows 7, откройте аплет Network и щелкните на ссылке Add a Printer (Добавить принтер) в панели инструментов диалогового окна Network Folder (Сеть). Откроется окно мастера добавления принтера (Add Printer Wizard). Это тот же самый мастер, которым вы

пользуетесь при добавлении принтера после выбора пункта Devices and Printers (Устройства и принтеры), находящегося в меню Start (Пуск) в Windows 7, и аплета Printers (Принтеры), доступного в панели управления в среде Windows Vista. Не забывайте, что средства операционной системы достижимы разными способами.

Подобно всем предшествующим версиям мастера добавления принтера, данная версия позволяет добавлять локальные принтеры, Bluetooth-принтеры и принтеры, размещенные в сети. Этот раздел посвящен сетевым ресурсам, к числу которых относятся подключенные с помощью кабеля или беспроводные сетевые принтеры. Чтобы добавить сетевой принтер, выберите переключатель Add a network, wireless or Bluetooth printer (Добавить сетевой, беспроводный или Bluetooth-принтер) и щелкните на кнопке Next (Далее). Мастер выполнит поиск принтеров в сети и возвратит все, что удалось найти.

Чтобы добавить один из этих принтеров, просто выберите его имя и щелкните на кнопке Next; затем на экране Results (Результаты) щелкните на кнопке Next еще раз. Стандартная конфигурация предусматривает установку этого принтера как применяемого по умолчанию, но это можно изменить, сняв отметку с флажка Set as default printer (Установить как принтер по умолчанию). Щелкните на кнопке Print a test page (Распечатать тестовую страницу), чтобы отправить этому принтеру тестовую страницу, и щелкните на кнопке Finish (Готово).

Доступны следующие варианты:

- поиск в Active Directory опубликованных сетевых принтеров;
- ввод размещения и имени принтера (в форме `\\имя_сервера\имя_принтера`);
- указание принтера с использованием его имени хоста или адреса TCP/IP (такой принтер часто называют *TCP/IP-принтером*).

Выбор переключателя Find a printer in the directory, based on location and feature (Найти принтер в каталоге на основе размещения и возможностей) приводит к открытию диалогового окна Find Printers (Найти принтеры). Поиск принтеров в Active Directory осуществляется путем указания определенных критериев (таких как имя или модель принтера) либо функциональной характеристики принтера (вроде возможности двусторонней печати). Щелкните на кнопке Find Now (Начать поиск), и мастер возвратит принтеры, которые соответствуют заданным критериям поиска (рис. 18.31). Если не указывать критерии поиска, то будут возвращены все принтеры, найденные в Active Directory.

В нашем примере мастер возвратил один результат. Найдя интересующий принтер, выберите его, щелкните на кнопке OK, и мастер добавит этот принтер. На открывшемся после этого экране Results (Результаты) щелкните на кнопке Next (Далее). Щелкните на кнопке Print a test page (Распечатать тестовую страницу), чтобы отправить на этот принтер тестовую страницу, и затем щелкните на кнопке Finish (Готово).

Вместо поиска принтера в Active Directory общий принтер можно также добавить по имени. Выберите переключатель Select a shared printer by name (Выбрать общий принтер по имени) и затем либо введите сетевой путь и имя принтера в форме `\\имя_сервера\имя_принтера`, либо щелкните на кнопке Browse (Обзор), чтобы перейти к принтеру на конкретном компьютере в сети. После добавления имени принтера щелкните на кнопке Next, затем еще раз на кнопке Next (на отобразившемся экране с информацией) и, наконец, на кнопке Finish.

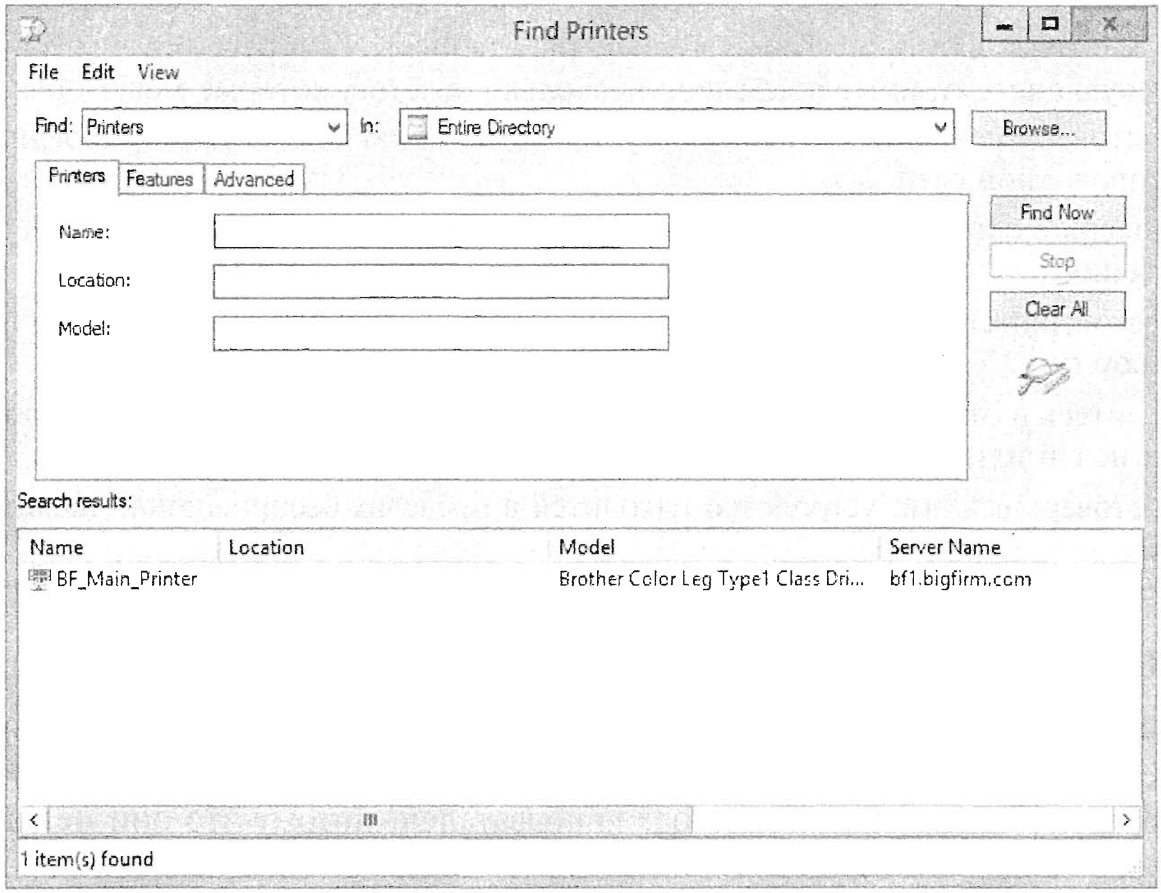


Рис. 18.31. С помощью диалогового окна Find Printers производится поиск в Active Directory принтеров, отвечающих заданным критериям поиска

Для добавления TCP/IP-принтера выберите переключатель Add a printer using a TCP/IP address or hostname (Добавить принтер по его TCP/IP-адресу или имени хоста). В поле Hostname or IP address (Имя или IP-адрес) введите IP-адрес принтера. Имя порта автоматически повторяет вводимый IP-адрес (можете изменить это имя, если нужно что-то более описательное). По умолчанию в списке Device type (Тип устройства) выбран вариант AutoDetect (Автовыбор). Вы должны оставить этот выбор, если только не знаете точный тип устройства. Щелкните на кнопке Next, и мастер попытается обнаружить принтер и установить его.

Добавление беспроводных устройств к клиентскому компьютеру Windows

Операционные системы Windows 7 и Windows 8 поддерживают возможность добавления беспроводных устройств, таких как Bluetooth-клавиатуры и Bluetooth-мыши, беспроводные телефоны, Bluetooth-модемы или Bluetooth-принтеры. Они не являются сетевыми ресурсами в точном смысле этого понятия (в идеальном случае пользователь не должен совместно применять мышь с кем-либо еще), но ради полноты мы кратко обсудим и такой вариант.

Чтобы добавить беспроводное устройство к клиентскому компьютеру Windows 7 или Windows 8, откройте аплет Network и щелкните на ссылке Add a wireless device (Добавить беспроводное устройство) в панели инструментов. Откроется окно мастера добавления беспроводного устройства в сеть (Add a Wireless Device to the Network Wizard); в Windows 7 этот мастер можно также инициировать из аплета Devices and Printers (Устройства и принтеры). Данный мастер выполнит автоматический поиск беспроводных устройств.

Если у вас возникли проблемы с добавлением сетевого беспроводного устройства в клиентскую систему, ниже приведено несколько советов, которые могут помочь.

- Удостоверьтесь, что добавляемое устройство включено и уже присоединено к беспроводной сети.
- Проверьте сетевой брандмауэр, убедившись, что он не блокирует процесс обнаружения.
- Удостоверьтесь, что на клиентском компьютере активизировано средство Network Discovery.
- Убедитесь в отсутствии помех со стороны бытовых приборов вроде микроволновых печей или беспроводных телефонов.
- Удостоверьтесь, что устройство находится в пределах беспроводной досягаемости компьютера (примерно 1,8 м для Bluetooth-устройств и 30,5 м для устройств Wi-Fi).

Отображение диска на общую папку

Временами для подключения к общему сетевому ресурсу проще применять букву диска, чем путь UNC, особенно если просмотр производится из командной строки. В некоторых приложениях такой подход обязателен, потому что они не сохраняют данные или не запускаются из путей UNC. По этой причине вы можете назначать общим сетевым ресурсам буквы дисков — во всяком случае, до тех пор, пока эти буквы не исчерпаются. В Windows 7 и Windows 8 это можно делать с помощью графического пользовательского интерфейса, в командной строке или за счет создания ярлыков для сетевого размещения.

Чтобы отобразить диск на общий сетевой ресурс, выполните перечисленные ниже шаги.

1. Откройте аплет Network (Сеть) и щелкните на ссылке Search Active Directory (Искать в Active Directory).
2. В открывшемся окне выберите из раскрывающегося списка Find (Искать) пункт Shared Folders (Общие папки).
3. Щелкните на кнопке Find Now (Начать поиск), и в окне Search results (Результаты поиска) появятся общие папки, которые опубликованы в Active Directory.
4. Чтобы подключиться к общей папке, щелкните на ней правой кнопкой мыши и выберите в контекстном меню пункт Map Network Drive (Отобразить сетевой диск), как показано на рис. 18.32.

   Каждый отображенный диск должен иметь уникальную букву диска. В результирующем диалоговом окне Map Network Drive (Отображение сетевого диска), приведенном на рис. 18.33, автоматически установлена неиспользуемая буква диска и заполнено местоположение папки. Если оставить флажок Reconnect at logon (Восстанавливать при входе в систему) отмеченным, то отображенные диски станут постоянными. По умолчанию будут использоваться текущие имя пользователя и пароль.
5. Чтобы указать другую учетную запись, применяемую для этого подключения, отметьте флажок Connect using different credentials (Использовать другие учетные данные).

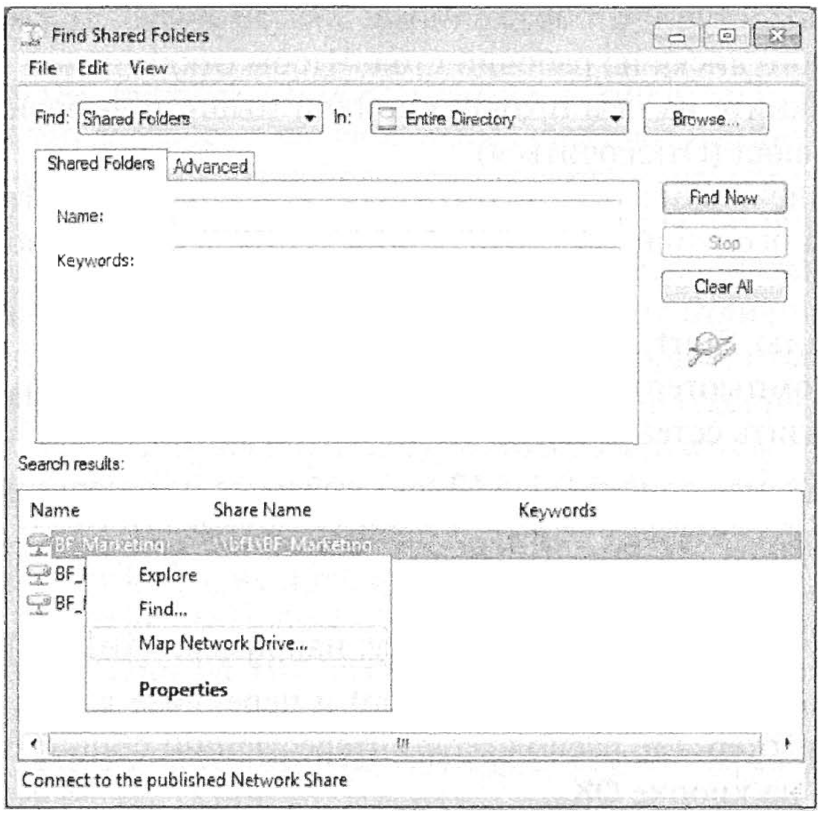


Рис. 18.32. Отображение диска на общую папку, найденную в Active Directory

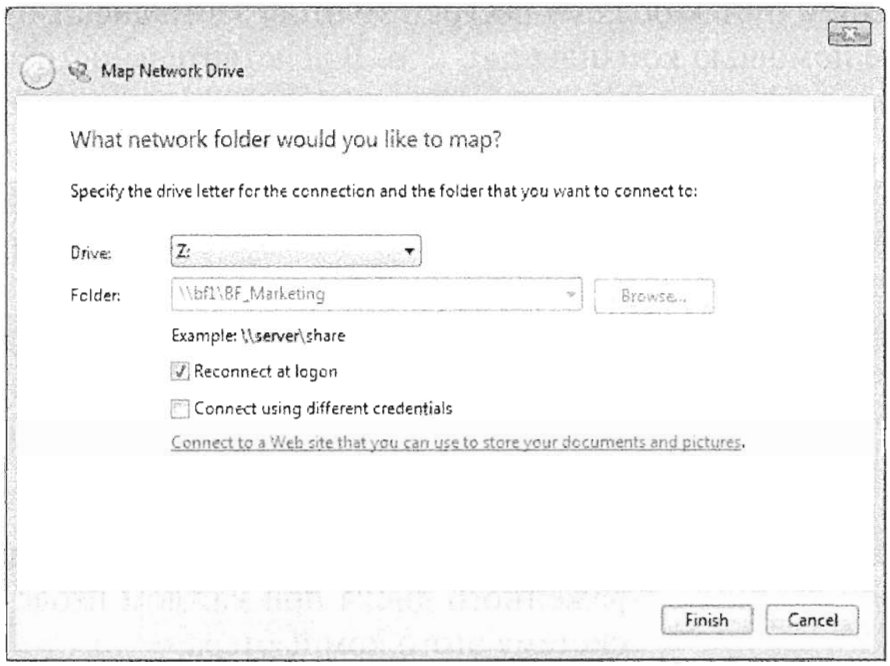


Рис. 18.33. Диалоговое окно Map Network Drive

Щелчок на ссылке Connect to a Web site that you can use to store your documents and pictures (Подключение к сайту, на котором можно хранить документы и изображения) приводит к открытию мастера добавления сетевого размещения (Add Network Location Wizard).

6. Щелкните на кнопке Finish (Готово).

Для доступа к отображенному диску выберите пункт меню Start⇨Computer (Пуск⇨Компьютер) и дважды щелкните на отображенном диске, находящемся в разделе Network Location (Сетевое размещение) окна Computer (Компьютер).

Чтобы ускорить доступ к отображенному диску в будущем, можете перетащить ярлык отображенного диска на рабочий стол. Чтобы отключиться от отображенного диска, просто щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Disconnect (Отключиться).

Некоторые общие папки могут не быть перечисленными в Active Directory. Чтобы отобразить диск на неопубликованный общий ресурс в сети, выполните следующие действия.

1. Откройте меню Start (Пуск), щелкните правой кнопкой мыши на пункте Computer (Компьютер) и выберите в контекстном меню пункт Map Network Drive (Отобразить сетевой диск).
2. В раскрывающемся списке Drive (Диск) выберите неиспользуемую букву диска.
3. Теперь вы должны указать расположение этой папки с применением одного из перечисленных ниже методов.
   - Введите путь UNC к общему ресурсу; например, `\\BF1\BF_Marketing`.
   - Щелкните на кнопке Browse (Обзор) и перейдите к общим папками, раскрыв компьютер, где расположен интересующий общий ресурс, выбрав его и щелкнув на кнопке OK.
4. Щелкните на кнопке Finish (Готово), и отображенный диск появится в разделе Network Location (Сетевое размещение) окна Computer (Компьютер).

Если вам известен путь к общему ресурсу, то отобразить диск можно также в командной строке с помощью команды `net use`. В действительности администраторы часто создают для пользователей сценарии входа, которые автоматически отображают диски, когда пользователи входят в системы своих компьютеров. Например, чтобы отобразить диск на общий ресурс `bf_marketing` сервера `bf1`, понадобится выдать следующую команду:

```
net use M: \\bf1\bf_marketing /PERSISTENT:YES
```

Ниже приведено объяснение параметров этой команды.

M:	Представляет букву диска.
\\bf1\bf_marketing	Путь UNC к общему ресурсу.
/PERSISTENT:YES	Обеспечивает автоматическое восстановление отображенного диска при каждом входе пользователя в систему этого компьютера.

Чтобы получить полный список параметров для команды `net use`, откройте окно командной строки и введите **net use /?**.

Но что, если вы не знаете, к чему можно подключиться посредством интерфейса командной строки? Ничего страшного. Вы можете воспользоваться командой `net use`, чтобы получить перечень общих ресурсов в сети. Однократный запуск этой команды позволяет вывести список компьютеров, видимых в сети. Продолжив погружаться глубже, можно выдать команду `net use` для определенного компьютера в сети и получить список его общих ресурсов. Чтобы удалить отображенный диск в командной строке, введите команду **net use X: /delete**, где **X** — буква отображенного диска, подлежащего удалению.

Создание сетевой папки

Вы уже знаете, каким образом отображать диск в Windows 8 способами, очень похожими на то, как это делалось в операционных системах ранних версий. Но есть еще один метод доступа к общим папкам (и другим сетевым размещениям): создание *сетевой папки* (по существу ярлыка) для общего размещения внутри окна Computer. Зачем это делать, вместо того чтобы просто отобразить диск? Между отображенными дисками и ярлыками сетевых размещений существуют отличия как в положительном, так и в отрицательном отношении. С одной стороны, отображенный диск действует подобно локальному диску на компьютере. Приложения, которым необходимо обращаться к элементам на дисках, будут трактовать сетевое размещение как локальный диск. Тем не менее, вы не можете отобразить букву диска на другие виды размещений, такие как FTP-сайты и общие веб-ресурсы. Таким образом, существуют причины для применения обоих приемов доступа.

Сетевое размещение включает общие папки, общие веб-ресурсы, FTP-сайты и UNC-пути. Добавлять ссылки на эти сетевые размещения можно в окне Computer с использованием мастера добавления сетевого размещения (Add Network Location Wizard). Мастер добавления сетевого размещения доступен через один из пунктов меню окна My Network Places (Мои сетевые размещения) в Windows XP. В Windows 7 и Windows 8 окно My Network Places трансформировалось в Network and Sharing Center (Центр управления сетями и общим доступом).

Чтобы открыть мастер добавления сетевого размещения в Windows 7 или Windows 8, выполните следующие шаги.

1. Выберите пункт меню Start⇨Computer (Пуск⇨Компьютер).
2. В открывшемся окне щелкните правой кнопкой мыши и выберите в контекстном меню пункт Add a network location (Добавить сетевое размещение), как показано на рис. 18.34.

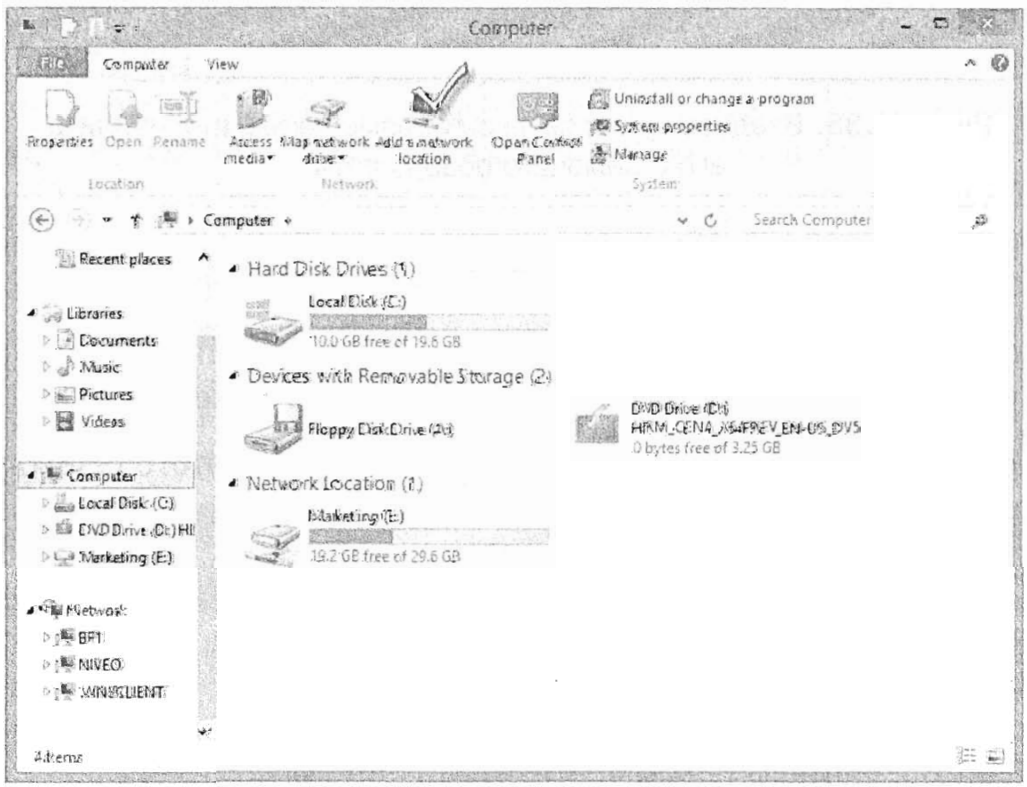


Рис. 18.34. Запуск мастера добавления сетевого размещения из окна Computer

3. Появится экран Welcome (Добро пожаловать) мастера. Щелкните на кнопке Next (Далее), выберите вариант Choose a custom network location (Выберите другое сетевое размещение) и щелкните на кнопке Next.

4. Теперь вы можете либо ввести сетевой адрес, если он вам известен (UNC-путь к общему сетевому ресурсу, адрес FTP-сайта, URL общего веб-ресурса), либо щелкнуть на кнопке Browse (Обзор), чтобы перейти к интересующей общей папке. (Кнопка Browse позволяет искать в сети только общие папки, но не другие виды сетевых размещений.)

5. Щелкните на кнопке Next. На рис. 18.35 демонстрируется ввод URL для FTP-сайта компании `bigfirm.com`: **`ftp://ftp.bigfirm.com`**.

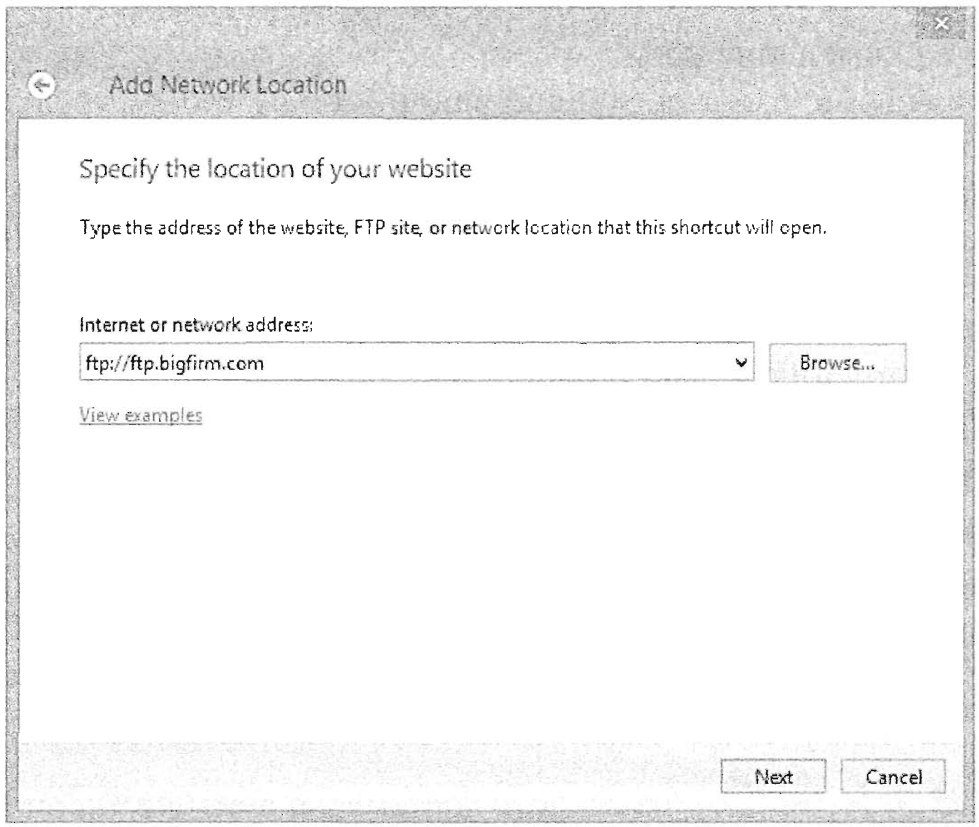


Рис. 18.35. Введите путь к сетевому размещению или найдите его с помощью обзора сети

По умолчанию мастер разрешает анонимный доступ к FTP-сайту. Если вы хотите изменить это, выполните описанные ниже действия.

1. Снимите отметку с флажка Log on anonymously (Анонимный вход) и введите имя пользователя, которое должно применяться для входа.

2. Щелкните на кнопке Next (Далее) и введите имя для этого сетевого размещения (например, **`ftp.bigfirm.com`**).

3. Щелкните на кнопке Next и затем на кнопке Finish (Готово).

Сетевое размещение откроется и будет перечислено в разделе Network Location (Сетевое размещение) окна Computer (рис. 18.36).

Чтобы отключить сетевое размещение, просто щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Delete (Удалить).

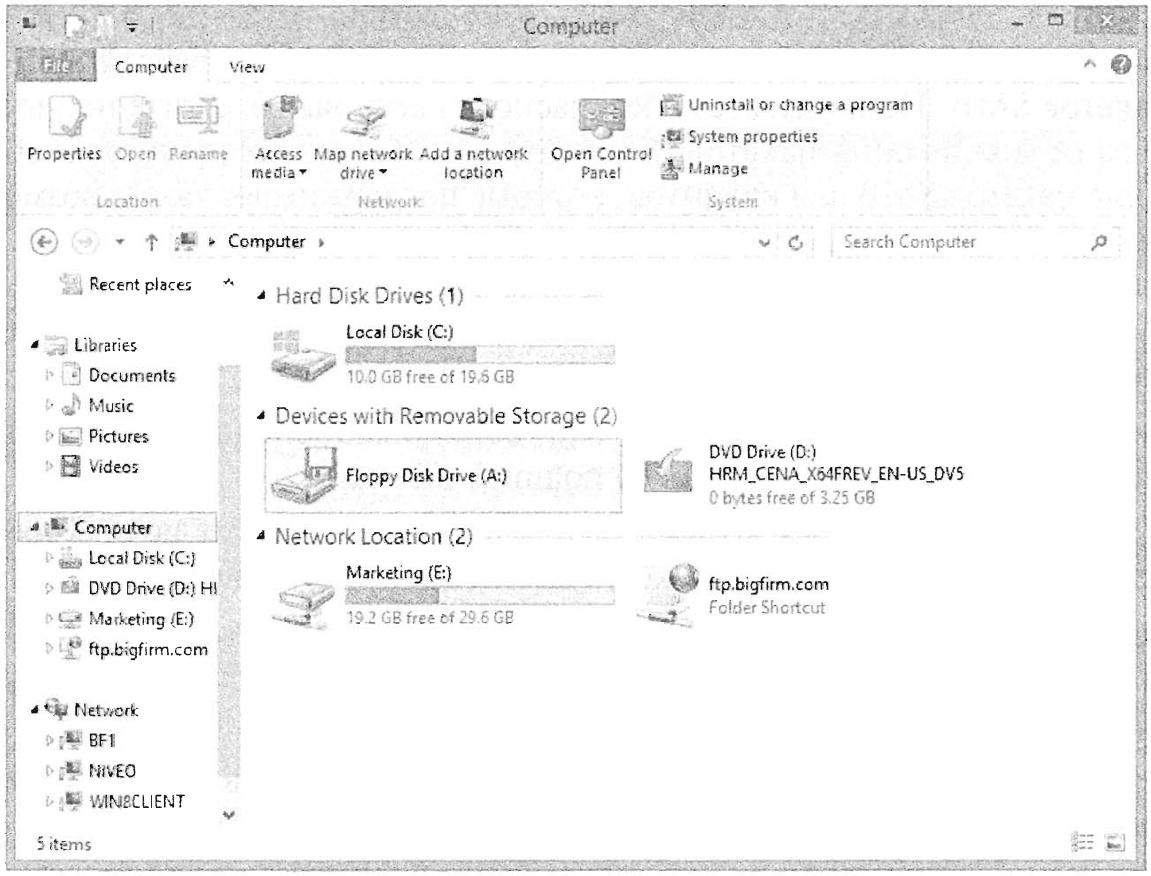


Рис. 18.36. Сетевое размещение добавлено в окно Computer

Подключение клиентов Mac OS X

Каждый год все большее число организаций интегрируют в свои сети Active Directory компьютеры Apple Macintosh. Этому процессу способствует не только компания Apple, которая наращивает сетевые возможности своих компьютеров, но и компания Microsoft, добавившая службы федерации, которые облегчают разнообразным сетевым клиентам получать преимущества от использования Active Directory.

В прошлом процесс подключения клиента Mac к машине Windows Server требовал дополнительного ПО, которое позволяло компьютеру Mac понимать файловые протоколы SMB (Server Message Block — блок сообщений сервера), применяемые Windows. В Mac OS X все необходимые компоненты входят в состав ОС. Это объясняется тем, что компания Apple включила в OS X одну из версий Samba, которая дает возможность UNIX-подобным операционным системам, таким как Linux и OS X, взаимодействовать на собственных диалектах SMB, используемых операционными системами Windows. Таким образом, проблема с подключением клиентов Mac в большей степени связана с аутентификацией, чем с возможностью соединения как таковой.

Несмотря на то что компьютеры Mac могут взаимодействовать на языке SMB, ОС Windows Server 2012 ожидает определенного стандартного уровня безопасности для коммуникаций SMB, который OS X не способна обеспечить самостоятельно, а именно — подписание пакетов SMB. Подписание пакетов помогает серверу Windows и клиенту обеспечить более защищенные коммуникации за счет применения цифровой подписи в каждом пакете, отправляемом посредством SMB. Этот метод может способствовать снижению риска перехвата пакетов и манипулирования ими в случае атаки типа “человек посередине”.

Чтобы позволить клиентам Mac эффективно взаимодействовать со средами Windows Server 2012 Active Directory, вам придется отключить требование о подписании пакетов SMB. Но в интересах безопасности сети вы не хотите полностью отказываться от подписания пакетов. К счастью, необходимая настройка обеспечит подписание пакетов SMB для клиентов, которые поддерживают такую возможность, но не требует подписания от клиентов (вроде Mac), ее не поддерживающих.

Для предоставления клиентам Mac, функционирующим под управлением OS X, возможности подключения к домену Active Directory, вы должны использовать перечисленные ниже настройки групповой политики.

- Microsoft network server: Digitally sign communications (always) (Сервер сети Microsoft: использовать цифровую подпись (всегда)).

  Установите эту политику в Disabled (Отключена), чтобы отключить требование подписания пакетов SMB при коммуникациях между клиентом и сервером.

- Microsoft network server: Digitally sign communications (if client agrees) (Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)).

  Установите эту политику в Enabled (Включена), чтобы позволить клиентам Windows по-прежнему использовать подписание пакетов SMB при коммуникациях с серверами Windows.

- Network security: LAN Manager authentication level (Сетевая безопасность: уровень аутентификации LAN Manager).

  Установите эту политику в Send LM & NTLM; use NTLMv2 session security if negotiated (Отправлять LM и NTLM; использовать сеансовую безопасность NTLMv2 при согласовании). Эта политика будет предоставлять доступ клиентам Mac, по-прежнему разрешая клиентам Windows согласовывать более высокий уровень безопасности.

Вы можете настраивать эти политики в локальных политиках для контроллеров домена, что обеспечит доступ для клиентов Mac по сети. Чтобы установить эти политики, выполните следующие шаги.

1. Откройте инструмент Group Policy Management (Управление групповой политикой). Это можно сделать двумя способами.
   - Выберите пункт меню Start⇨Administrative Tools⇨Group Policy Management (Пуск⇨Администрирование⇨Управление групповой политикой).
   - В диспетчере серверов раскройте узел Features (Компоненты) и щелкните на элементе Group Policy Management (Управление групповой политикой).
2. Раскройте узел Default Domain Policy (Стандартная политика домена).
3. В диспетчере серверов последовательно раскройте узел Group Policy Management, узел леса, узел Domains (Домены) и свой домен.
4. Щелкните правой кнопкой мыши на элементе Default Domain Policy и выберите в контекстном меню пункт Edit (Правка).
5. Если в этот момент вы получите приглашение, щелкните на кнопке OK.
6. В окне редактора управления групповыми политиками (Group Policy Management Editor) перейдите к папке Computer Configuration\Policies\Windows Settings\Local Policies\Security Options (Конфигурация компьютера \ Политики \

Настройки Windows \ Локальные политики \ Параметры безопасности), как показано на рис. 18.37.

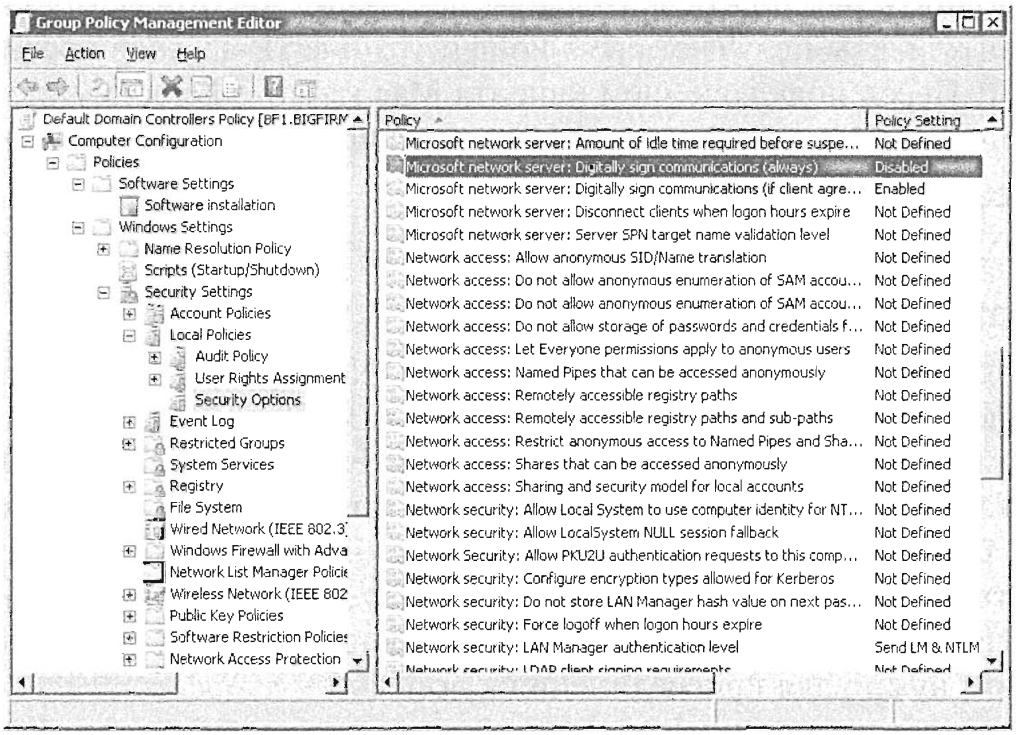


Рис. 18.37. Использование редактора управления групповыми политиками

7. Выполните прокрутку до политик, начинающихся с Microsoft network server (Сервер сети Microsoft).
8. Дважды щелкните на политике Microsoft network server: Digitally sign communications (always) (Сервер сети Microsoft: использовать цифровую подпись (всегда)).
9. Выберите переключатель Define the policy setting (Определить эту настройку политики) и укажите Disabled (Отключена).
10. Щелкните на кнопке OK.
11. Дважды щелкните на политике Microsoft network server: Digitally sign communications (if client agrees) (Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)).
12. Выберите переключатель Define the policy setting и укажите Enabled (Включена).
13. Щелкните на кнопке OK.
14. Выполните прокрутку политик, начинающихся с Network security (Сетевая безопасность).
15. Дважды щелкните на политике Network security: LAN Manager authentication level (Сетевая безопасность: уровень аутентификации LAN Manager).
16. Выберите переключатель Define the policy setting.
17. В раскрывающемся списке выберите вариант Send LM & NTLM; use NTLMv2 session security if negotiated (Отправлять LM и NTLM; использовать сеансовую безопасность NTLMv2 при согласовании).
18. Щелкните на кнопке OK.

Подключение клиента Mac к домену

Прежде чем можно будет подключить клиент Mac OS X к Active Directory, вы должны выполнить ряд подготовительных действий. Некоторые из них уже быть сделаны, если клиенты получают свою конфигурацию IP-адресов посредством протокола DHCP. Перед подключением клиента Mac к Active Directory удостоверьтесь, что на компьютере Mac сконфигурированы перечисленные ниже элементы:

- IP-адрес;
- адрес DNS-сервера;
- стандартный шлюз.

Критически важной частью является адрес DNS-сервера. В большинстве организаций, использующих Active Directory, серверы DNS чаще всего будут контроллерами домена или, по крайней мере, они будут интегрированы с Active Directory. Это важно, т.к. клиент Mac будет отправлять DNS-запрос, чтобы найти сервер LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам), ответственный за это доменное имя. Сервер DNS, интегрированный с Active Directory, ответит IP-адресом контроллера домена, который представляет собой именно то, что нужно для присоединения к домену.

В ходе процесса присоединения понадобится предоставить перечисленные ниже дополнительные элементы информации:

- учетные данные пользователя с разрешением на добавление компьютера к домену;
- имя компьютера Mac в том виде, в каком оно появляется в Active Directory;
- полное доменное имя (такое как `bigfirm.com`);
- точный путь к организационной единице, где должна быть создана учетная запись компьютера;
- учетные данные администратора для компьютера Mac.

Имея под рукой всю эту информацию, вы готовы к присоединению клиента Mac к домену Active Directory. Войдите в систему OS X на компьютере Mac и выполните следующие шаги.

1. Откройте окно System Preferences (Системные предпочтения).
2. В разделе System (Система) выберите Users & Groups (Пользователи и группы).
3. Выберите Login Options (Параметры входа в систему); если эта настройка неактивна, понадобится щелкнуть на значке с изображением замка в нижней части экрана, чтобы разрешить внесение изменений в систему.
4. Щелкните на кнопке Network Account Server: Join (Сервер учетных записей сети: присоединиться).
5. Щелкните на Open Directory Utility (Открыть утилиту Directory).

   Для внесения изменений может потребоваться щелкнуть на значке с изображением замка еще раз.
6. Откроется утилита Directory. Введите необходимую информацию в перечисленных ниже полях:

- Active Directory Forest (Лес Active Directory)
- Active Directory Domain (Домен Active Directory)
- Computer ID (Идентификатор компьютера)

7. В поле Active Directory Domain укажите полное доменное имя, такое как **bigfirm.com**.
8. В поле Computer ID введите имя клиентского компьютера Mac; имя не должно содержать дефисы.
9. Щелкните на кнопке Bind (Связать). По запросу предоставьте имя администратора Mac и пароль, чтобы разрешить внесение изменений. Щелкните на кнопке OK.
10. Укажите отличительное имя для учетной записи, имеющей разрешение добавлять учетную запись клиента Mac в Active Directory, например,

```
administrator@bigfirm.com
```

11. Введите пароль для этой учетной записи.
12. Укажите полный путь к организационной единице, где будет создана учетная запись для этого компьютера (рис. 18.38).

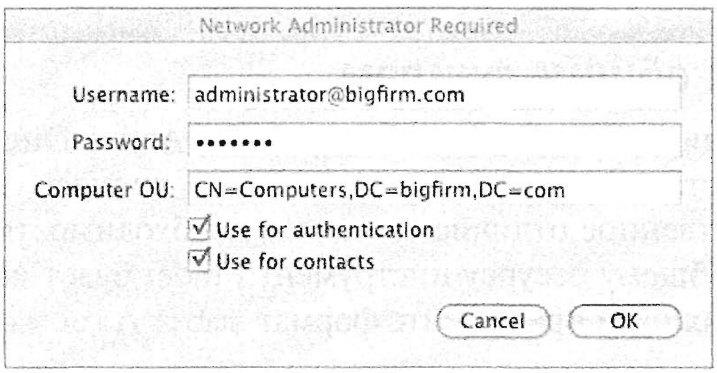


Рис. 18.38. Указание полного пути к организационной единице

13. Щелкните на кнопке OK, чтобы сохранить настройки Active Directory.
14. По запросу введите учетные данные администратора Mac и щелкните на кнопке OK.

Утилита Directory также позволяет конфигурировать и присоединяться к домену или лесу Active Directory из командной строки. Для конфигурирования клиента Mac из командной строки в следующем примере применяется утилита `dsconfigad`.

1. Откройте утилиту Terminal.
2. Выберите контроллер домена и введите такую команду:

```
dsconfigad -preferred bf1.bigfirm.com -a "ИМЯ_КОМПЬЮТЕРА"
           -domain bigfirm.com -u administrator -p "пароль"
```

3. Выберите Login Options (Параметры входа в систему); если эта настройка неактивна, понадобится щелкнуть на значке с изображением замка в нижней части экрана, чтобы разрешить внесение изменений в систему.

   Связав клиент Mac с доменом, вы можете использовать дополнительные команды для получения более подробной информации. Следующий шаг заклю-

чается в применении утилиты `dsconfigad` для установки административных параметров, которые доступны через Active Directory.

4. Оставаясь в сеансе Terminal, введите следующую команду:

```
Dsconfigad -alldomains enable -groups domain BigAdmin@Bigfrim.com,
Enterprise BigAdmins@bigfirm.com
```

Данные команды требуют использования паролей в виде простого текста, поэтому если домен Active Directory не разрешает такое, то вам придется настроить включение этого для ведения журнала утилиты Directory. Еще одним часто применяемым инструментом является `odutil`. Эта команда анализирует внутреннее состояние служб и записей каталога, позволяя включать ведение журнала и вносить изменения в статистические данные.

5. Введите следующую команду:

```
odutil set log debug
```

Эта команда установит ведение журнала на устройстве в режим Debug (Отладка); так что если у вас возникли какие-то проблемы с подключением к домену Active Directory, вы можете просмотреть в журналах события отладки, чтобы получить более подробную информацию. Журналы для `odutil` хранятся в `/var/log/opendirectoryd.log`.

Подключение к общим файлам

После того как клиент Mac стал частью домена Active Directory, подключение к общим папкам представляет собой почти такой же процесс, как и подключение к серверу OS X. Единственное отличие связано с необходимостью указания того, что для подключения к общему ресурсу инструмент Finder будет использовать протокол SMB. Для определения пути применяйте формат `smb://имя_сервера/имя_общего_ресурса` (рис. 18.39).

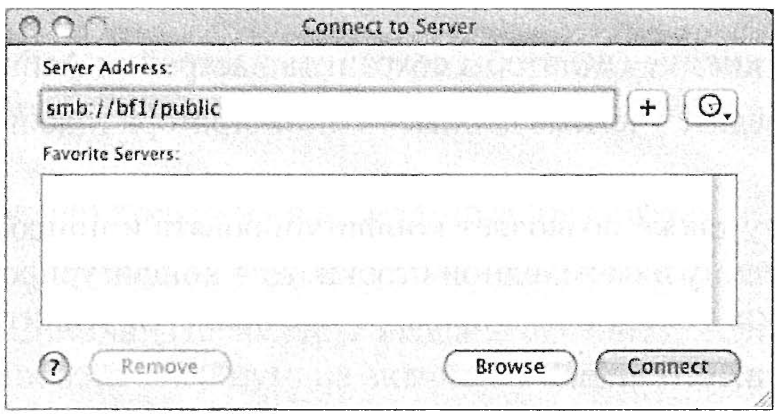


Рис. 18.39. Определение пути к серверу Windows

Чтобы подключить клиент Mac к общей папке Windows Server 2012, выполните описанные ниже действия.

1. В окне Finder щелкните на меню Go (Перейти) и затем на кнопке Connect to Server (Подключиться к серверу).
2. Введите путь к нужной общей папке в формате `smb://имя_сервера/имя_общего_ресурса`.

3. Дополнительно щелкните на значке "плюс" (+), чтобы добавить этот сервер в список избранных серверов. Если вы сделаете это, то сможете щелкать на имени сервера в списке, после чего на кнопке Connect (Подключиться).
4. Щелкните на кнопке Connect.
5. Предоставьте свои учетные данные пользователя Active Directory и щелкните на кнопке OK.

Подключение к принтерам

Подобно подключению к общим папкам, подключение к сетевым принтерам, которые опубликованы в Active Directory, является относительно прямолинейной задачей. После присоединения клиента Mac к домену Active Directory опубликованные принтеры будут отображаться на вкладке Default (Стандартные) при добавлении принтера на странице Print & Fax (Печать и факс) в окне System Preferences (Системные предпочтения) примерно так, как показано на рис. 18.40.

Рис. 18.40. Добавление принтера из Active Directory

Чтобы добавить принтер, опубликованный в Active Directory, выполните следующие шаги.

1. Откройте окно System Preferences (Системные предпочтения).
2. Щелкните на Print & Fax (Печать и факс).
3. Щелкните на значке "плюс" (+), чтобы добавить новый принтер.
4. На вкладке Default (Стандартные) щелкните на имени принтера, который вы хотите добавить.
5. Щелкните на кнопке Add (Добавить).

Добавление принтеров из среды рабочей группы Windows производится аналогично. Для добавления нового принтера вы по-прежнему будете применять страницу Print & Fax в System Preferences, но вместо выбора принтеров из Active Directory,

перечисленных на вкладке Default, вам придется использовать вкладку Windows и искать их вручную. Посредством раздела Print & Fax в System Preferences можно также добавлять принтеры, имеющие IP-адреса, а также любые аппараты факсимильной связи, которые могут оказаться доступными.

Использование удаленного рабочего стола из клиента Mac

Теперь, когда клиент OS X добавлен к домену Active Directory и можно получать доступ к общим файлам и принтерам, возникает вопрос: как администрировать сеть? К счастью, в Microsoft создали клиент Remote Desktop для OS X, который позволяет обращаться к компьютерам Windows Server 2012 из Mac. Вы можете бесплатно загрузить Remote Desktop Connection for Mac (RDC) для OS X из разделов загрузки либо сайта Microsoft (`www.microsoft.com/downloads`), либо сайта Apple (`www.apple.com/downloads`). Поищите на этих сайтах "Remote Desktop Connection".

Чтобы установить клиент Remote Desktop Connection, выполните перечисленные ниже действия.

1. Загрузите последнюю версию Remote Desktop Connection. Пакет с образом диска будет автоматически смонтирован и запустится процесс установки. Щелкните на кнопке Continue (Продолжить).
2. Ознакомьтесь с информацией в файле Read Me и затем щелкните на кнопке Continue.
3. Просмотрите лицензионное соглашение и щелкните на кнопке Continue. Щелкните на кнопке Agree (Согласен), чтобы принять условия лицензии.
4. Щелкните на кнопке Install (Установить), чтобы выполнить стандартную установки, и значок Remote Desktop Connection for Mac 2 будет помещен в папку `Applications` (Приложения) на первичном жестком диске.

   Щелкнув на кнопке Change Install Location (Изменить место установки), можно изменить место, куда будет произведена установка.
5. Появится страница Installation Type (Тип установки), показанная на рис. 18.41.

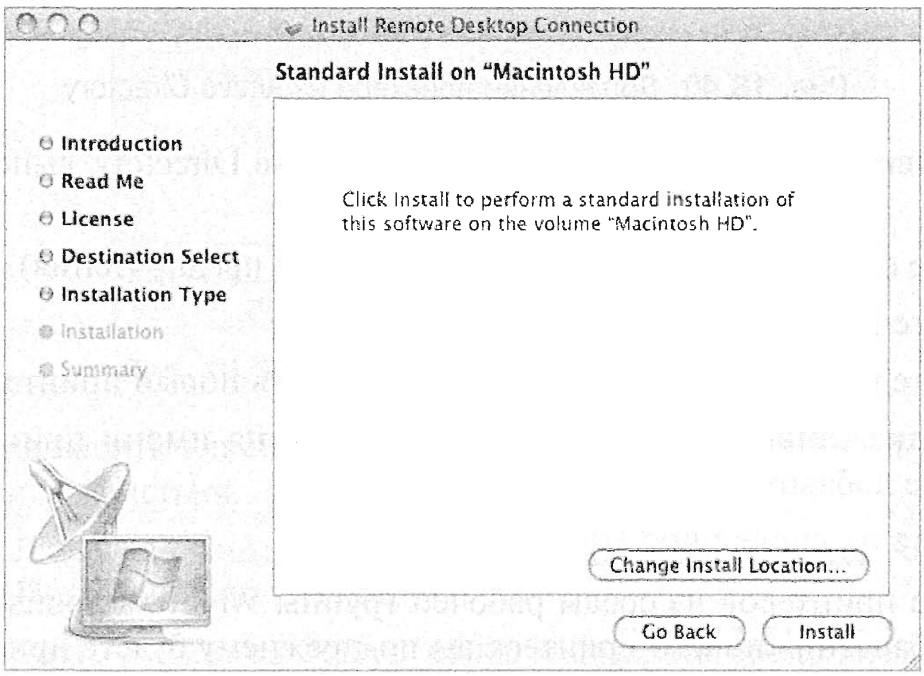


Рис. 18.41. Выбор местоположения для установки RDC

6. Введите свой пароль администратора Mac, чтобы подтвердить установку, и щелкните на кнопке OK.

7. Когда процесс установки завершится, щелкните на кнопке Close (Закрыть), чтобы выйти из программы установки.

Применение RDC подобно использованию Remote Desktop в Windows за исключением некоторых изменений интерфейса, призванных привести его в соответствие со стилем OS X. Начальное окно содержит только поле для ввода имени компьютера, к которому вы хотите подключиться. Для указания учетных данных, необходимых для входа в систему, и корректировки предпочтений применяйте систему меню RDC в верхней части экрана. Подобно Windows-версии Remote Desktop, когда вы впервые подключаетесь к удаленному компьютеру, вам будет предложено указать свое имя пользователя, пароль и имя домена. Средство RDC позволяет сэкономить некоторое время, предоставляя возможность сохранить свои учетные данные для Windows на экране Preferences (Предпочтения) и затем сохранить их в вашей связке ключей (Keychain). Присоединение компьютера Mac к домену Active Directory не является требованием для использования клиента Remote Desktop. Если компьютер Mac получает информацию DHCP и DNS из сети, то у вас будет возможность получать доступ к серверам и рабочим станциям Windows, как если бы вы имели дело с любым стандартным рабочим столом Windows.

Устранение проблем

В этом разделе мы предложим набор советов по устранению проблем, которые могут пригодиться, если вы столкнетесь с такими проблемами при попытке связывания клиента Mac с Active Directory.

- **Возникла проблема с доменами Active Directory, заканчивающимися на `.local`.** Многие пользователи сообщают о проблемах при подключении к домену Active Directory, который заканчивается на `.local` (такому, который часто используется с сетями Windows Small Business Server). Реализация Multicast DNS от Apple, называемая Bonjour, не воспринимает `.local` как допустимый домен верхнего уровня и предполагает, что он должен быть распознан посредством Bonjour. Из-за этого клиент Mac не запрашивает у DNS-сервера IP-адрес любого хоста в домене `.local`. Вы можете разрешить клиенту Mac просматривать адреса домена `.local`, добавив `local` в список доменов для поиска (рис. 18.42).

- **Active Directory не реагирует при связывании.** Если вы получили сообщение об ошибке, уведомляющее о том, что домен Active Directory не смог ответить, когда вы попытались связать компьютер Mac с этим доменом, проверьте несколько моментов.

  - Убедитесь в том, что в настройках сети указан допустимый DNS-сервер в домене.

  - Убедитесь в том, что в Active Directory корректно установлено подписание пакетов SMB.

- **Домен Active Directory перестал отвечать.** В различных версиях OS X возникали проблемы с подключением к Active Directory. Удостоверьтесь в том, что вы располагаете самыми последними обновлениями для операционной системы. Если клиент Mac теряет связь с Active Directory, попробуйте отсоединиться от домена и затем присоединиться заново.

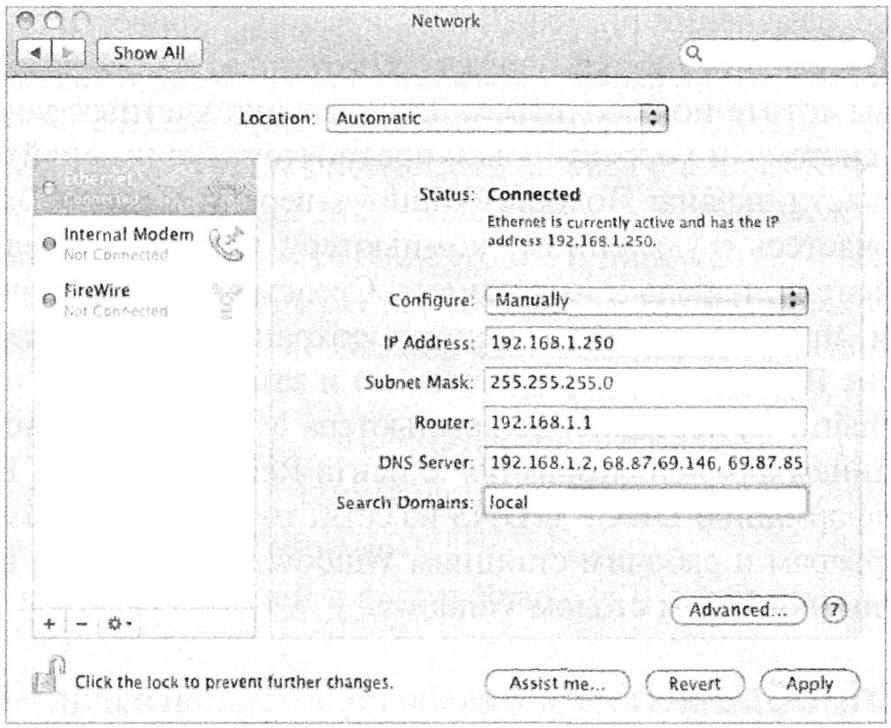


Рис. 18.42. Добавление `local` в список доменов для поиска

Резюме

Проверьте конфигурацию своей сети. Протокол DHCP предоставляет централизованные конфигурации IP-адресов, и все клиенты Windows понимают DHCP, не требуя установки дополнительных компонентов.

Контрольный вопрос. Вам нужно проверить, что клиентская машина получила правильную конфигурацию IP-адресов через DHCP для сети, в которой вы работаете. Какая из перечисленных ниже команд возвратит нужные результаты?

- `ipconfig /all`
- `ipconfig /refresh`
- `msconfig /show`
- `msconfig`

Присоедините клиентский компьютер к домену. Присоединение к домену Active Directory является одной из важнейших задач для рабочих станций, поскольку это обеспечивает централизованное управление из группы `Domain Admins` внутри домена. Групповая политика является централизованной, можно обеспечить защиту, и даже программным обеспечением можно управлять централизованным образом.

Контрольный вопрос. Является ли следующее утверждение правильным? Присоединить компьютер к домену Active Directory можно лишь в случае, если выполняющий это действие пользователь является администратором данного домена.

Измените пароли пользователей. По умолчанию Windows Active Directory обеспечивает 42-дневный максимальный возраст пароля. За 14 дней до истечения этого срока начинают ежедневно поступать напоминания о необходимости изменения пароля. Этот 42-дневный максимум предусмотрен с целью обеспечения определенного уровня безопасности для производственной среды, не позволяющий паролям устаревать.

Контрольный вопрос. Кого-то из пользователей одолела паранойя, поэтому он желает изменить пароль своей учетной записи прямо сейчас. Он не знает, как это сделать, и обращается в службу технической поддержки. Компьютер пользователя функционирует под управлением Windows 7. Что вы посоветуете данному пользователю?

Подключитесь к сетевым ресурсам. Вот типичный сценарий: пользователь желает подключиться к такому принтеру в домене, который выполняет двустороннюю печать, а также сшивает документы. Но пользователю не известно, где в компании установлены такие принтеры. Пользователь обращается в службу технической поддержки.

Контрольный вопрос. Какой из перечисленных ниже способов является наиболее эффективным для пользователя, желающего отыскать принтеры, которые соответствуют этому описанию?

- Предложите пользователю пройтись по офисному зданию и проверить каждый принтер, чтобы выяснить, обладает ли он нужными характеристиками.
- Предложите пользователю воспользоваться командой `net view`, чтобы проверить общие принтеры, подключенные к каждому компьютеру.
- Предложите пользователю запустить мастер добавления принтера (Add Printer Wizard) и выбрать в нем опцию Search Active Directory (Искать в Active Directory).

Подготовьте Active Directory для клиентов Mac OS X. Несмотря на то что операционная система Mac OS X позволяет присоединяться к доменам Active Directory, вы должны предпринять ряд подготовительных действий, чтобы обеспечить возможность коммуникации клиентов Mac OS X с Windows Server 2012.

Контрольный вопрос. Вы хотите, чтобы ваши пользователи Active Directory, имеющие дело с клиентами Mac, могли подключаться к серверам Windows Server 2008 R2 с помощью единственного входа в Active Directory. Какой компонент сетевой безопасности Windows необходимо изменить, чтобы разрешить клиентам Mac взаимодействовать с доменом Windows Server 2012?

Подключите компьютер Mac к домену. Mac OS X может подключаться к Active Directory и присоединяться к доменам. Поддержка протокола SMB обеспечивается встроенной версией Samba, что позволяет подключать OS X к Windows для получения доступа к общим файловым ресурсам и общим принтерам.

Контрольный вопрос. Вы хотите добавить клиент Mac OS X к домену Active Directory. Какую утилиту OS X вы должны применять?

Подключите компьютер Mac к общим файловым ресурсам и общим принтерам. OS X подключается к общим файлам и принтерам Windows с использованием поддержки SMB, предоставляемой Samba. Поскольку поддержка является интегрированной, для прямого подключения к Windows-ресурсам можно применять инструмент Finder, не устанавливая дополнительное программное обеспечение.

> *Контрольный вопрос.* Вы пытаетесь получить доступ к сетевой папке, которая является общей на компьютере Windows Server 2012, из клиента Mac, присоединенного к домену. Как использовать Finder для такого подключения?

Используйте Remote Desktop из клиента Mac. В Microsoft разработали Remote Desktop Connection для Mac, чтобы обеспечить клиентам Mac возможность подключения к Remote Desktop. Применяя RDC, можно получать доступ к функциональности компьютера Windows непосредственно из клиентов Mac.

> *Контрольный вопрос.* Вы используете RDC для подключения к серверу Windows Server 2012 и хотите сохранить свои учетные данные для доступа в сеть, чтобы не приходилось вводить их при каждом подключении. Что вы можете предпринять?

Глава 19

Управление веб-сервером с помощью IIS

Реализация инициативы Microsoft Cloud OS (Облачная операционная система Microsoft) идет полным ходом, при этом информационным службам Интернета (Internet Information Services — IIS) отведено особое место. Используете вы System Center 2012 R2 для управления своей инфраструктурой, Windows Server Update Services для поддержки обновлений и исправлений программного обеспечения или расширяете инфраструктуру на облако с помощью Windows Azure Pack, ключевым компонентом во всех случаях является IIS. Учитывая настолько важную роль этой службы, в Microsoft внесли ряд важных усовершенствований в IIS, получив самую быстродействующую и безопасную версию IIS из всех существующих, с которой по-прежнему легко работать.

В этой главе вы изучите следующие темы:

- планирование и установка службы IIS 8.5;
- управление стандартными глобальными параметрами IIS 8;
- создание и защита веб-сайтов в IIS 8;
- управление IIS 8 с помощью расширенных приемов администрирования.

Что нового в версиях IIS 8.0 и IIS 8.5

В версии IIS 8.0 и IIS 8.5 было внесено несколько захватывающих усовершенствований, которые связаны с виртуализацией, безопасностью, масштабируемостью, администрированием и производительностью. Ниже приведены краткие описания новых возможностей.

- **Динамические ограничения IP-адресов.** В IIS 8 ограничения IP-адресов переведены на новый качественный уровень: теперь администраторы имеют возможность конфигурировать серверы так, чтобы они заносили в "черный список" IP-адреса, с которых превышено указанное число одновременных запросов или количество запросов за определенный промежуток времени.

В фильтрацию IP-адресов добавлен новый прокси-режим, который позволит блокировать IP-адрес не только по клиентскому IP-адресу, видимому IIS, но также по значениям, полученным в HTTP-заголовке `x-forwarded-for`. Администраторы также имеют возможность указывать, что должен делать сервер IIS, когда IP-адрес заблокирован — скажем, отправлять сообщения о неавторизованном доступе, запрете доступа или отсутствии запрошенного ресурса либо даже разрывать подключение.

- **Ограничения попыток входа на FTP-сайт.** Это средство помогает предотвратить получение доступа к FTP-сайту неавторизованными пользователями. Оно позволяет администраторам конфигурировать FTP-серверы так, чтобы блокировать доступ пользователям, которые превысили заданное количество запросов на вход за определенный промежуток времени. Это отличается от динамических ограничений IP-адресов в том, что блокируется только учетная запись нарушителя, а не инициирующий запросы IP-адрес.
- **Плавная регулировка центрального процессора для пулов приложений.** Теперь администраторы могут управлять нагрузкой центрального процессора для каждого пула приложений, предотвращая полное занятие сервера одним сайтом и ухудшение производительности всех остальных сайтов на данном хосте. В предыдущих версиях IIS регулировка центрального процессора отключала бы сайт по достижении сконфигурированного порога, но это привело бы к невозможности доступа к нему со стороны пользователей. В IIS 8 сайт не будет отключен, но продолжит обслуживать запросы с пониженной скоростью. Администраторы IIS могут также сконфигурировать регулировку центрального процессора так, чтобы она была активной постоянно или вступала в действие, только когда в системе хоста возникает повышенная нагрузка.
- **Инициализация приложений.** Эта возможность позволяет инициализировать веб-приложения заранее, чтобы они были готовы при первом обращении к ним пользователем. Это помогает избежать ситуации, когда конечному пользователю приходится ожидать запуска веб-приложения, но в случае, когда именно пользователь является инициатором запуска веб-приложения, IIS 8 можно настроить на возвращение статического содержимого, пока не будут завершены необходимые задачи инициализации. Этот вариант можно применять в сочетании с правилами переписывания URL-адресов для создания более сложного статического содержимого, пока приложение инициализируется.
- **Централизованное хранилище сертификатов.** Управление сертификатами SSL внутри веб-ферм может оказаться затратным по времени и утомительным, начиная с импортирования сертификатов в каждый сервер и заканчивая ручной проверкой, находятся ли сертификаты в состоянии синхронизации. В IIS 8 положение дел изменилось за счет появления централизованного хранилища сертификатов, которое позволяет хранить все веб-сертификаты в сетевом файловом общем ресурсе.
- **Индикация имени сервера.** Предыдущие версии IIS позволяли задействовать заголовки `Host`, так что администраторы могли назначать одному IP-адресу несколько веб-сайтов. В IIS 8.0 такая возможность предоставляется сайтам, защищенным посредством протокола SSL (Secure Sockets Layer — уровень

защищенных сокетов). Эта возможность требует, чтобы клиентские браузеры поддерживали средство индикации имени сервера (Server Name Indication — SNI). В большинстве современных браузеров SNI поддерживается, но это не относится к версиям Internet Explorer из Windows XP.

- **Масштабируемость SSL.** В IIS 8 были внесены значительные усовершенствования в способ обработки сертификатов. В предыдущих версиях IIS каждый сертификат SSL должен был загружаться в память, когда клиент впервые обращался к сайту, и оставаться в памяти неопределенно долго. В IIS 8 в память загружается только сертификат, который необходим в текущий момент, и по истечении конфигурируемого промежутка времени сертификат из памяти выгружается. Вдобавок было радикально уменьшено время перечисления и загрузки сертификатов SSL, что сделало возможным существование тысяч сайтов SSL на одном хосте.
- **Динамическая активация сайтов.** В предшествующих версиях IIS при размещении большого количества веб-сайтов, скорее всего, вы сталкивались с ситуацией, когда загрузка файла конфигурации IIS требовала много времени. Причина была в том, что после запуска служба активации процессов Windows (Windows Process Activation Service — WAS) загружала полную конфигурацию для всех веб-сайтов, размещенных на сервере. В версии Windows Server 2012 R2 и IIS 8.5 этот процесс был оптимизирован, приводя к резкому увеличению производительности. Для этого средства не предусмотрен специальный пользовательский интерфейс, но его можно настраивать через редактор конфигурации (Configuration Editor).
- **Откачка неактивного рабочего процесса.** В IIS 8.5 оптимизирован подход к неактивному рабочему процессу. В предыдущих версиях IIS, если вследствие бездействия возникал тайм-аут рабочего процесса, служба IIS завершала данный процесс, освобождая связанные с ним ресурсы. У этого подхода были свои достоинства и недостатки, поскольку ресурсы становились доступными для использования в каком-то другом месте, но когда рабочий процесс запрашивался снова, приходилось ожидать завершения процедуры его начального запуска. В IIS 8.5 рабочий процесс можно приостанавливать. Это приводит к выгрузке процесса на диск, освобождая в итоге память, а когда процесс запрашивается вновь, он загружается с диска без необходимости в ожидании завершения процедуры его начального запуска. Применяя сочетание неактивного рабочего процесса и средства инициализации приложений, вы можете, в сущности, вообще не допускать такого явления, как время запуска для любого веб-приложения.
- **Усовершенствования регистрации в журналах.** В IIS 8.5 предусмотрено больше вариантов регистрации в журналах. Теперь имеется возможность выполнения регистрации полей внутри заголовка запроса (Request Header), заголовка ответа (Response Header) и/или серверных переменных (Server Variable). На выбор доступно большое количество полей или же можно создать специальное поле.
- **События ETW.** В IIS 8.5 теперь имеется встроенное отслеживание событий. Вы можете по-прежнему пользоваться стандартными журналами, применять средство трассировки событий для Windows (Event Tracing for Windows — ETW) либо то и другое.

Установка IIS 8

После краткого обзора новых возможностей IIS мы подробно рассмотрим процесс установки. Операционная система Windows Server 2012 поставляется в виде нескольких редакций и располагает новыми методами использования разных ролей для сервера. В данной главе мы не будем вдаваться в детальный анализ этих редакций, памятуя о том, что служба IIS 8.0 доступна во всех полных редакциях Windows Server 2012, а также в Windows 8.

Хотя одни серверы IIS 8.x могут быть внутренне реализованы как серверы корпоративной сети или ориентированы на поддержку сетевого приложения на основе веб, другие будут относиться к внешнему адресному пространству сети TCP/IP, иногда называемому *демилитаризованной зоной* (demilitarized zone — DMZ), будучи интерфейсными веб-серверами. Независимо от предполагаемого назначения сервера IIS 8, процесс установки будет тем же самым.

Добавление роли Web Server посредством диспетчера серверов

В Windows Server 2012 продолжается следование концепции добавления функциональности в операционную систему за счет применения определенных ролей на сервере. Назначение роли не только устанавливает соответствующие службы, но также регламентирует зависимые службы и подразумевает меры по дальнейшему развитию. Чтобы установить IIS 8, понадобится развернуть на сервере роль Web Server (Веб-сервер).

Как и предшествующие версии, IIS 8 состоит из многочисленных модулей. Следует особо подчеркнуть, что вы должны добавлять лишь модули, необходимые для поддержки запланированного веб-содержимого. В табл. 19.1 перечислены роли и компоненты, доступные при использовании роли Web Server в ОС, наряду с названиями соответствующих им средств в PowerShell. Устанавливая абсолютный минимум необходимых модулей, вы можете построить экономный веб-сервер с небольшим набором ресурсов и сокращенной поверхностью атаки. Следование такой стратегии даст вам более защищенный и высокопроизводительный веб-сервер.

Таблица 19.1. Службы ролей ОС для IIS 8 (в том же порядке, в каком они следуют в мастере добавления ролей и компонентов)

Имя службы (в графическом пользовательском интерфейсе)	Имя средства PowerShell	Описание	Включена по умолчанию
Web Server (Веб-сервер)	`Web-WebServer`	Публикует веб-сайты, веб-службы и веб-приложения	Да
Default Document (Стандартный документ)	`Web-Default-Doc`	Конфигурирует для веб-сайтов стандартный файл, который должен доставляться в случае, если вызов страницы в URL не указан	Да
Directory Browsing (Просмотр каталогов)	`Web-Dir-Browsing`	Автоматически генерирует для веб-сайтов список всех каталогов/файлов, который должен доставляться в случае, если вызов страницы в URL не указан, а стандартный документ отключен или не сконфигурирован	Да

Продолжение табл. 19.1

Имя службы (в графическом пользовательском интерфейсе)	Имя средства PowerShell	Описание	Включена по умолчанию
HTTP Errors (Ошибки HTTP)	`Web-Http-Errors`	Настраивает сообщения об ошибках	Да
Static Content (Статическое содержимое)	`Web-Static-Content`	Публикует форматы статических веб-файлов	Да
HTTP Redirection (Перенаправление HTTP)	`Web-Http-Redirect`	Перенаправляет один URL на другой URL	Нет
WebDAV Publishing (Публикация WebDAV)	`Web-DAV-Publishing`	Публикует файлы на веб-сервере или с веб-сервера через HTTP	Нет
HTTP Logging (Ведение журналов HTTP)	`Web-Http-Logging`	Обеспечивает регистрацию действий веб-сайта в журнале	Да
Custom Logging (Специальное ведение журналов)	`Web-Custom-Logging`	Создает специальные модули ведения журнала	Нет
Logging Tools (Инструменты ведения журналов)	`Web-Log-Libraries`	Предоставляет инфраструктуру управления и автоматизации ведения журналов веб-сервера	Нет
ODBC Logging (Ведение журналов ODBC)	`Web-ODBC-Logging`	Предоставляет инфраструктуру для регистрации действий веб-сервера в ODBC-совместимой базе данных и их извлечения для веб-отображения	Нет
Request Monitor (Монитор запросов)	`Web-Request-Monitor`	Предоставляет инфраструктуру для захвата информации о рабочем процессе IIS, включая детали HTTP-запроса	Нет
Tracing (Трассировка)	`Web-Http-Tracing`	Предоставляет инфраструктуру для захвата определенных событий	Нет
Static Content Compression (Сжатие статического содержимого)	`Web-Stat-Compression`	Предоставляет инфраструктуру для сжатия статического содержимого с целью кеширования	Да
Dynamic Content Compression (Сжатие динамического содержимого)	`Web-Dyn-Compression`	Предоставляет инфраструктуру для сжатия динамического содержимого	Нет
Request Filtering (Фильтрация запросов)	`Web-Filtering`	Фильтрует входящие запросы на основе правил, определенных администратором	Да
Basic Authentication (Базовая аутентификация)	`Web-Basic-Auth`	Поддерживает базовую аутентификацию	Нет
Centralize SSL Certificate Support (Поддержка централизованных сертификатов SSL)	`Web-CertProvider`	Поддерживает централизованные сертификаты SSL	Нет

Продолжение табл. 19.1

Имя службы (в графическом пользовательском интерфейсе)	Имя средства PowerShell	Описание	Включена по умолчанию
Client Certificate Mapping Authentication (Аутентификация с помощью сопоставления с клиентским сертификатом)	`Web-Client-Auth`	Поддерживает аутентификацию с помощью клиентских сертификатов, используя Active Directory (сопоставление "один к одному" среди множества веб-серверов)	Нет
Digest Authentication (Аутентификация с помощью дайджеста)	`Web-Digest-Auth`	Поддерживает аутентификацию с помощью хеширования паролей	Нет
IIS Client Certificate Mapping Authentication (Аутентификация с помощью сопоставления с клиентским сертификатом IIS)	`Web-Cert-Auth`	Поддерживает аутентификацию с помощью клиентских сертификатов, используя IIS (сопоставления "один к одному" или "многие к одному")	Нет
IP and Domain Restrictions (Ограничения IP-адресов и доменов)	`Web-IP-Security`	Доставляет содержимое по IP-адресу или доменному имени инициатора запроса	Нет
URL Authorization (Авторизация URL)	`Web-Url-Auth`	Поддерживает основанные на правилах ограничения содержимого, связанные с пользователями, группами или глаголами HTTP-заголовка	Нет
Windows Authentication (Аутентификация Windows)	`Web-Windows-Auth`	Поддерживает аутентификацию с применением учетных записей Windows	Нет
.NET Extensibility 3.5	`Web-Net-Ext`	Расширяет функциональность веб-сервера в запросе, конфигурации или пользовательском интерфейсе	Нет
.NET Extensibility 4.5	`Web-Net-Ext45`	Расширяет функциональность веб-сервера в запросе, конфигурации или пользовательском интерфейсе	Нет
Application Initialization (Инициализация приложений)	`Web-AppInit`	Выполняет затратные задачи инициализации веб-приложений перед обслуживанием веб-страниц	Нет
ASP	`Web-ASP`	Предоставляет возможность написания серверных сценариев Active Server Page (на VBScript и JScript)	Нет
ASP.NET 3.5	`Web-Asp-Net`	Предоставляет объектную модель серверной стороны для управляемых приложений, основанных на .NET Framework 3.5	Нет
ASP.NET 4.5	`Web-Asp-Net45`	Предоставляет объектную модель серверной стороны для управляемых приложений, основанных на .NET Framework 4.5	Нет
CGI	`Web-CGI`	Предоставляет поддержку для написания сценариев CGI для внешних программ	Нет

Продолжение табл. 19.1

Имя службы (в графическом пользовательском интерфейсе)	Имя средства PowerShell	Описание	Включена по умолчанию
ISAPI Extensions (Расширения ISAPI)	`Web-ISAPI-Ext`	Поддерживает динамическое веб-содержимое посредством ISAPI-расширений, подключаемых по запросу	Нет
ISAPI Filters (Фильтры ISAPI)	`Web-ISAPI-Filter`	Поддерживает файлы, которые фильтруют запросы к веб-серверу для расширения либо изменения определенной функциональности	Нет
Server-Side Includes (SSI) (Включения серверной стороны)	`Web-Includes`	Обеспечивает генерацию с помощью сценариев динамических HTML-страниц	Нет
WebSocket Protocol (Протокол WebSocket)	`Web-WebSockets`	Поддерживает приложения, которые взаимодействуют по протоколу WebSocket	Нет
FTP Server (FTP-сервер)	`Web-Ftp-Server`	Предоставляет инфраструктуру для построения FTP-сайтов, которые используют протокол FTP для выгрузки и загрузки файлов	Нет
FTP Service (Служба FTP)	`Web-Ftp-Service`	Разрешает публикацию FTP	Нет
FTP Extensibility (Расширяемость FTP)	`Web-Ftp-Ext`	Поддерживает средства расширяемости FTP, такие как специальные поставщики, пользователи ASP.NET или пользователи диспетчера IIS	Нет
IIS Hostable Web Core (Размещаемое веб-ядро IIS)	`Web-WHC`	Разрешает обслуживание HTTP-запросов приложениями, находящимися за пределами IIS, с использованием собственных файлов `.config`	Нет
IIS Management Console (Консоль управления IIS)	`Web-Mgmt-Console`	Обеспечивает графический пользовательский интерфейс для управления веб-службами IIS 7.5 (не FTP или SMTP)	Да
IIS 6 Management Compatibility (Совместимость с управлением IIS 6)	`Web-Mgmt-Compat`	Обеспечивает поддержку ABO и ADSI для существующих сценариев управления IIS 6.0	Нет
IIS 6 Metabase Compatibility (Совместимость с метабазой IIS 6)	`Web-Metabase`	Обеспечивает поддержку запросов и конфигурирования метабазы IIS 6.0 для приложений ABO и ADSI	Нет
IIS 6 Management Console (Консоль управления IIS 6)	`Web-Lgcy-Mgmt-Console`	Предоставляет инфраструктуру для администрирования удаленных веб-серверов IIS 6 и для администрирования FTP и SMTP	Нет
IIS 6 Scripting Tools (Инструменты написания сценариев IIS 6)	`Web-Lgcy-Scripting`	Предоставляет инфраструктуру для запуска сценариев IIS 6 в среде IIS 7.5, включая ABO и ADSI (требует WAS)	Нет

Окончание табл. 19.1

Имя службы (в графическом пользовательском интерфейсе)	Имя средства PowerShell	Описание	Включена по умолчанию
IIS 6 WMI Compatibility (Совместимость с IIS 6 WMI)	`Web-WMI`	Предоставляет интерфейс написания сценариев WMI для управления и автоматизации задач с использованием средств WMI CIM Studio, WMI Event Registration, WMI Event Viewer и WMI Object Browser	Нет
IIS Management Scripts and Tools (Сценарии и инструменты управления IIS)	`Web-Scripting-Tools`	Предоставляет средства командной строки и сценариев для управления IIS, полезные при автоматизации администрирования	Нет
Management Service (Служба управления)	`Web-Mgmt-Service`	Предоставляет инфраструктуру для дистанционного управления IIS с помощью графического пользовательского интерфейса	Нет

Веб-сервер для Bigfirm

Мы будем применять графический пользовательский интерфейс диспетчера серверов, чтобы создать два веб-сайта на хосте Windows Server 2012 R2 с функционирующей службой Microsoft IIS 8.5. Веб-сайт 1 (Apples) будет посвящен яблокам, а веб-сайт 2 (Oranges) сосредоточится на апельсинах.

Первым делом запустите диспетчер серверов и выберите в меню Manage (Управление) пункт Add Roles and Features (Добавить роли и компоненты), чтобы добавить к серверу роль Web Server (Веб-сервер), как показано на рис. 19.1.

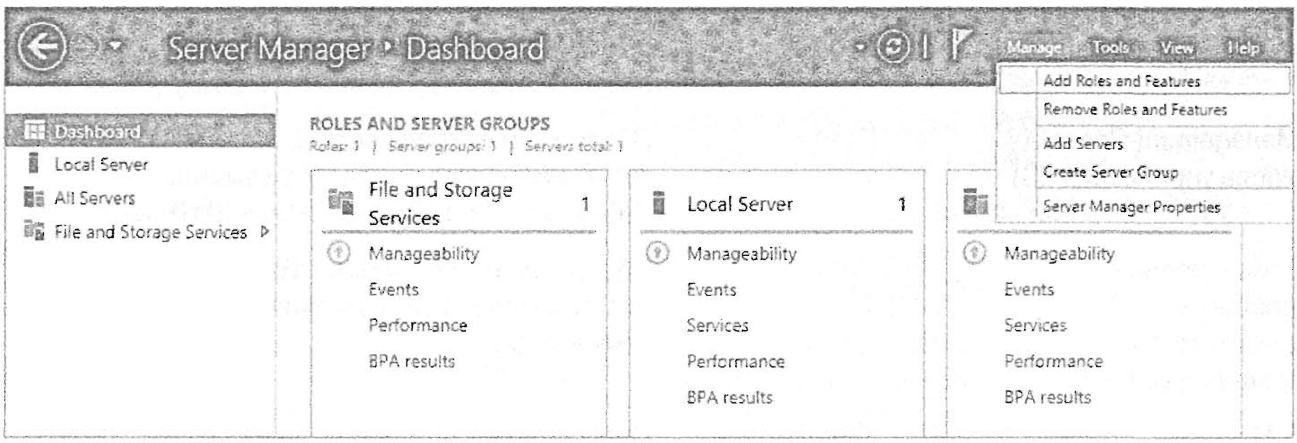


Рис. 19.1. Управление списком задач в диспетчере серверов

В качестве альтернативы для установки IIS можно использовать PowerShell и даже написать сценарии для автоматической или дистанционной установки (дополнительные сведения об этом приводятся далее в главе).

1. На экране Before You Begin (Прежде чем начать) щелкните на кнопке Next (Далее).
2. На экране Select Installation Type (Выбор типа установки) щелкните на кнопке Next.

3. На экране Select Destination Server (Выбор сервера назначения) щелкните на кнопке Next, чтобы принять в качестве целевого локальный сервер.
4. На экране Select Server Roles (Выбор серверных ролей) отметьте флажок возле роли Web Server (IIS) (Веб-сервер (IIS)) и щелкните на кнопке Next.
5. В открывшемся всплывающем окне щелкните на кнопке Add Features (Добавить компоненты), чтобы установить также инструменты IIS Management на сервер IIS, и щелкните на кнопке Next.
6. На экране Web Server (IIS) (Веб-сервер (IIS)) щелкните на кнопке Next, чтобы продолжить.
7. На экране Role Services (Службы роли) отметьте флажки возле всех служб роли и для продолжения щелкните на кнопке Next (краткие описания этих служб приведены в табл. 19.1).
8. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) посмотрите выбранные варианты и щелкните на кнопке Install (Установить).
9. На экране Installation Progress (Ход установки) удостоверьтесь, что установка завершилась успешно, и щелкните на кнопке Close (Закрыть).

Установка IIS 8 посредством PowerShell

Как и все другие компоненты Windows Server 2012, веб-сервер IIS 8 можно устанавливать, конфигурировать и удалять с применением PowerShell. Чтобы установить IIS из PowerShell, просто выполните следующую команду:

```
Install-WindowsFeature -Name Web-Server -IncludeManagemntTools
```

Это приведет к установке роли Web Server со всеми стандартными параметрами, в точности, как при установке роли Web Server в графическом пользовательском интерфейсе. Для добавления дополнительных компонентов к функционирующему серверу IIS запустите командлет `Install-WindowsFeature` еще раз с именем компонента, который вы хотите установить. В табл. 19.1 содержится список всех названий компонентов веб-сервера. Получить этот список можно также с помощью следующей команды PowerShell:

```
Get-WindowsFeature -name web*
```

Изменение структуры IIS

Изменить структуру IIS столь же легко, как вытащить из розетки вилку блока питания ноутбука, чтобы взамен вставить вилку зарядного устройства мобильного телефона. Вы вольны добавлять или удалять модули для ознакомления, тестирования или действительного применения в производственной среде. Добавление компонента к IIS не является решением, которое не допускает изменения. В будущем вы всегда можете удалить этот компонент, просто сняв отметку с соответствующего ему флажка.

Если вы не выполняли *полную* установку всех служб роли Web Server в данной среде, когда первоначальную устанавливали IIS, тогда вам придется добавить соответствующую службу роли, прежде чем связанные с ней собственные модули будут доступны для добавления к какому-то веб-сайту IIS. В следующем разделе показано, как зарегистрировать собственный модуль с помощью ОС, позволив Windows Server 2012

доверять его коду и предоставлять ему неограниченный доступ ко всем ресурсам. Как и в случае с любым кодом с повышенными разрешениями, регистрировать следует только собственные модули IIS, поступившие из заслуживающих доверия источников, поскольку эти модули будут иметь привилегированный доступ к системе.

Добавление служб роли к роли Web Server для Bigfirm

Для конфигурирования веб-сайтов в нашем примере вам потребуется поддержка ASP-страниц на веб-сайте Oranges, если только вы не перепишете определенное содержимое и затем с помощью HTTP Redirection направите посетителей на готовое новое содержимое. Добавлять службы роли к уже примененной серверной роли можно с использованием диспетчера серверов, утилиты `AppCmd.exe` или PowerShell. Например, чтобы добавить службу роли ASP к существующей серверной роли на сервере `BF1` компании `Bigfirm` посредством диспетчера серверов, выполните следующие шаги.

1. Запустите диспетчер серверов.
2. В древовидном представлении слева выберите роль IIS.
3. Выполните прокрутку вниз в правой панели деталей, чтобы добраться до раздела Roles and Features (Роли и компоненты), где приведена сводка по установленным ролям веб-сервера (рис. 19.2).

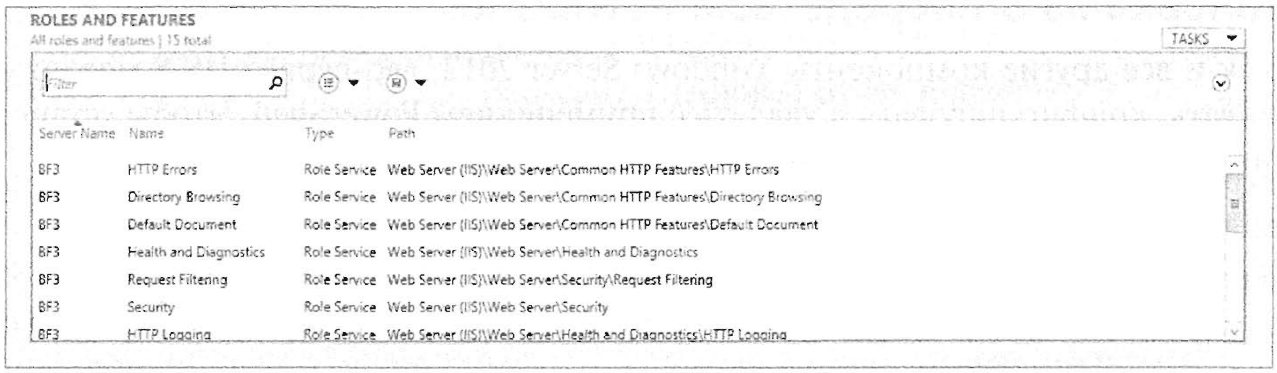


Рис. 19.2. Установленные роли и компоненты

4. Щелкните на раскрывающемся меню Tasks (Задачи) справа и выберите пункт Add Roles and Features (Добавить роли и компоненты).
5. В открывшемся мастере добавления ролей и компонентов доберитесь до экрана Select Server Roles (Выбор серверных ролей) и отметьте флажок возле службы роли ASP, расположенной в разделе Web Server (IIS)\Web Server\Application Development (Веб-сервер (IIS) \ Веб-сервер \ Разработка приложений).

   Обратите внимание, что службы роли, которые уже установлены, отображаются серым цветом и не могут быть удалены с помощью этого мастера. Если вы хотите удалить какую-то службу роли, выполните такие действия.
6. Отмените работу мастера (подтвердив отмену).
7. Выберите в раскрывающемся меню Tasks пункт Remove Roles and Features (Удалить роли и компоненты).

   Поскольку только что добавленная служба роли ASP требует зависимой службы роли под названием ISAPI Extensions, которая еще не установлена, отображается диалоговое окно, информирующее об этом и предоставляющее возможность также установить эту зависимую службу роли (рис. 19.3).

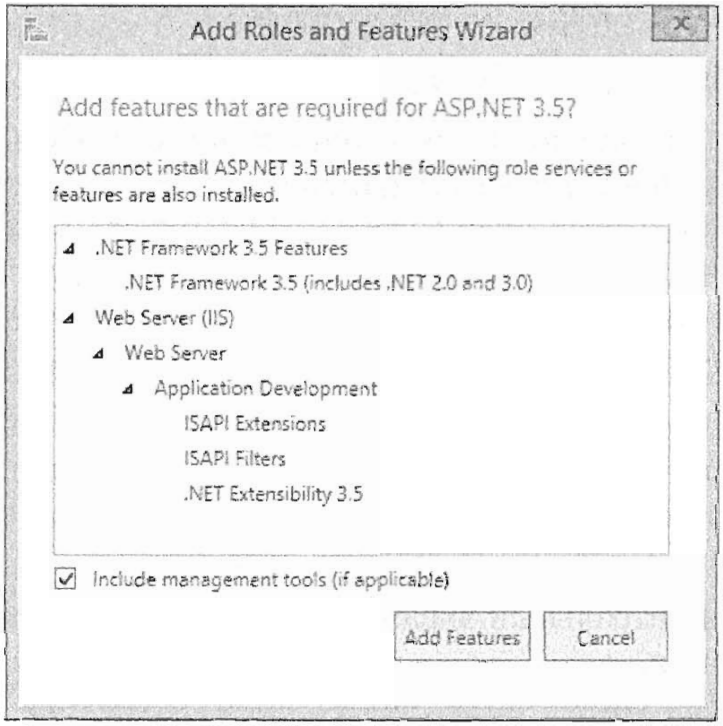


Рис. 19.3. Мастер добавления ролей и компонентов

8. Щелкните на кнопке Add Features (Добавить компоненты), чтобы разрешить установку зависимостей.
9. Щелкните на кнопке Next (Далее) и переместитесь до экрана Features (Компоненты).

   На экране Confirmation (Подтверждение) отображаются итоги произведенного выбора.
10. Щелкните на кнопке Install (Установить), чтобы завершить установку и возвратиться в окно диспетчера серверов.

    Обратите внимание, что носитель с установкой Windows Server 2012 не запрашивается. Вам больше не придется лихорадочно рыться по коробкам с дисками до того, как приступить к администрированию своего IIS-сервера.

Если для добавления служб роли к роли Web Server вы предпочитаете применять PowerShell, то эту работу сделает командлет `Install-WindowsFeature`. Вот синтаксис для добавления службы роли HTTP Redirection:

```
Install-WindowsFeature Web-Http-Redirect
```

Во время выполнения этой команды на экране отображается индикатор хода работ (от 0% до 100%), после чего окно PowerShell должно содержать строки, показанные на рис. 19.4.

Рис. 19.4. Завершение установки службы роли в PowerShell

Регистрация собственных модулей с использованием диспетчера IIS

Собственный модуль можно зарегистрировать с помощью графического пользовательского интерфейса IIS Manager (Диспетчер IIS). Диспетчер IIS не настолько интуитивно понятен, как диспетчер серверов. Однако если вы относитесь к той категории администраторов, которые предпочитают проводить весь свой рабочий день, пользуясь одной утилитой, а диспетчер IIS является для вас предпочитаемым инструментом, то с его помощью можно решить и эту очень важную задачу. Чтобы зарегистрировать собственный модуль "на лету", выполните перечисленные ниже действия.

1. Запустите диспетчер IIS и подключитесь или выделите интересующий сервер IIS с использованием расположенной слева панели Connections (Подключения).

   По умолчанию центральный экран диспетчера IIS отражает категории инструментов управления.

2. Внутри категории IIS щелкните на значке Modules (Модули), чтобы отобразить список модулей, установленных на уровне сервера.

3. Щелкните на гиперссылке Configure Native Modules (Конфигурировать собственные модули) из расположенной справа панели Actions (Действия), специфичной для модулей.

   Откроется диалоговое окно Configure Native Modules (Конфигурирование собственных модулей), перечисляющее собственные модули, которые установлены в настоящий момент (рис. 19.5).

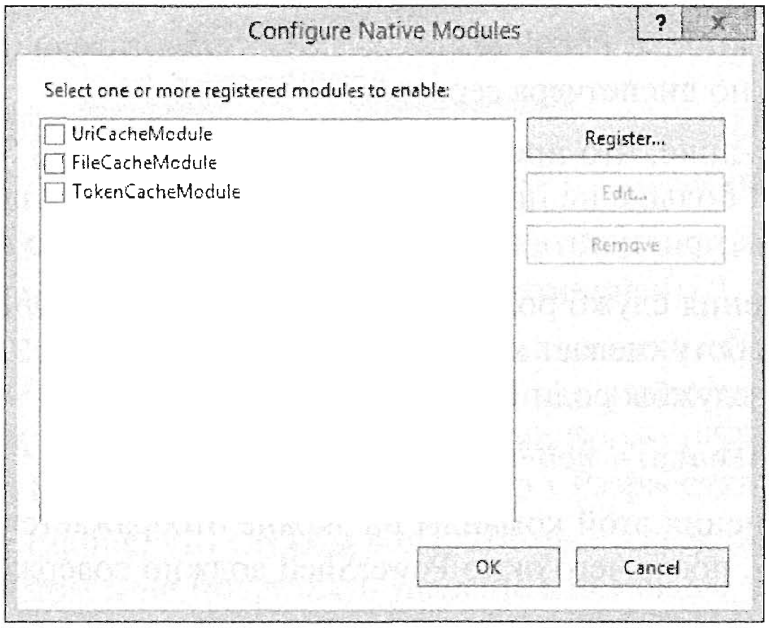


Рис. 19.5. Диалоговое окно Configure Native Modules

4. Щелкните в этом диалоговом окне на кнопке Register (Зарегистрировать), чтобы вручную зарегистрировать собственный модуль "на лету". Разумеется, это требует знания фактического имени файла собственного модуля.

5. После добавления собственного модуля в список выберите его, чтобы включить на уровне сервера.

Управление модулями с помощью PowerShell

Хотя по-прежнему допускается редактировать файл `applicationhost.config`, как это делалось в предшествующих версиях IIS, вы можете счесть более удобным решать задачи управления модулями, доступными на уровне сервера или сайта, с помощью PowerShell. Использование PowerShell для установки собственных модулей на уровне сервера позволит им быть автоматически установленными на каждом сайте, и это докажут приведенные ниже команды.

- Чтобы установить модуль, используйте команду:

```
New-WebGlobalModule -Name {имя_модуля} -Image {путь_к_модулю}
```

- Чтобы удалить модуль, применяйте команду:

```
Remove-WebGlobalModule -Name {имя_модуля}
```

- Чтобы включить модуль, используйте команду:

```
Enable-WebGlobalModule -Name {имя_модуля}
```

- Чтобы включить модуль для определенного сайта, применяйте команду:

```
Enable-WebGlobalModule -Name {имя_модуля} -PSPath "IIS:\sites\{имя_сайта}"
```

- Чтобы отключить модуль, используйте команду:

```
Disable-WebGlobalModule -Name {имя_модуля}
```

- Чтобы отключить модуль для определенного сайта, применяйте команду:

```
Disable-WebGlobalModule -Name {имя_модуля} -PSPath "IIS:\sites\{имя_сайта}"
```

Конфигурирование модулей на уровне сайта

После установки необходимых служб роли в IIS станут доступными связанные с ними модули, которые позволят надлежащим образом обрабатывать клиентские запросы. На самом деле собственные модули автоматически включаются на всех веб-сайтах, которые наследуют свою конфигурацию от родительского файла `applicationhost.config`. Модули IIS можно конфигурировать или отключать на уровне сайта путем непосредственного изменения файла `web.config` в текстовом редакторе, с использованием утилиты `AppCmd.exe`, с применением PowerShell или посредством пользовательского интерфейса диспетчера IIS. Давайте начнем с интуитивно понятного пользовательского интерфейса. Выполните следующие шаги.

1. Запустите диспетчер IIS и подключитесь или выделите интересующий сервер IIS с использованием расположенной слева панели Connections (Подключения).

   По умолчанию центральный экран диспетчера IIS отражает категории инструментов управления.

2. Внутри категории IIS щелкните на значке Modules (Модули), чтобы отобразить список модулей, установленных на уровне сервера; этими модулями можно управлять на уровне сайта.

   Обратите внимание, что любой веб-сайт, настроенный на наследование структуры его возможностей от своего родителя, будет наследовать эти модули из уровня сервера.

3. Перейдите к элементу Default Web Site (Веб-сайт по умолчанию) в узле Sites (Сайты) внутри панели Connections слева и выделите его.

   Обратите внимание на наличие значков Home (Домой) и в особенности значков ASP и HTTP Redirect (Перенаправление HTTP), которые сейчас доступны только потому, что вы установили необходимые службы роли на уровне сервера (ранее они отсутствовали).

4. Дважды щелкните на значке Modules и внимательно ознакомьтесь с перечнем установленных модулей, как собственных, так и управляемых, которыми можно пользоваться в Default Web Site.

   Следует отметить, что модуль ASP не появляется отдельно в списке, а скрывается внутри IsapiModule.

5. Чтобы отключить здесь один из унаследованных собственных модулей на уровне сайта в Default Web Site, такой как IsapiModule, просто выделите его и щелкните на ссылке Remove (Удалить) в панели Actions (Действия) справа.

   Конечно, операционная система запросит подтверждение удаления, поэтому вы должны быть уверены в своем решении. После удаления модуль исчезает из списка.

   Включение установленного собственного модуля (того, который зарегистрирован в файле `applicationhost.config`) на уровне сайта не настолько очевидно.

6. Если вы хотите снова включить IsapiModule в Default Web Site, щелкните на гиперссылке Configure Native Modules (Конфигурировать собственные модули) в расположенной справа панели Actions, специфичной для модуля.

   Откроется диалоговое окно Configure Native Modules (Конфигурирование собственных модулей), подобное показанному на рис. 19.6, которое позволяет включить IsapiModule, просто отметив предусмотренный для него флажок.

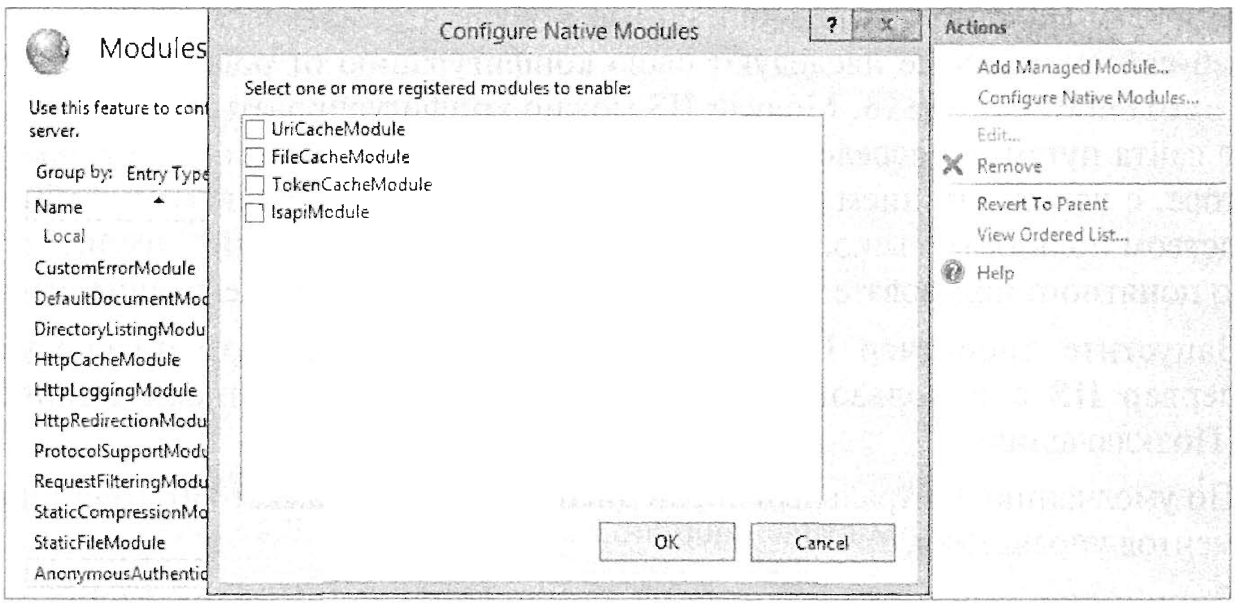


Рис. 19.6. Диалоговое окно Configure Native Modules

Вспомните, что модули, зарегистрированные на уровне сервера в конфигурационном файле `applicationhost.config`, автоматически включены на всех сайтах, которые наследуют свою структуру модулей от сервера. Эти модули не имеет смысла

включать на каждом сайте в экземпляре IIS. Несмотря на наличие многих сложностей, связанных с новыми специфичными для сайтов файлами `web.config`, реальность такова, что сайт даже не получает созданный для него файл `web.config` до тех пор, пока вы не внесете в конфигурацию для сайта изменение, которое запрещает наследование из родительского уровня. После этого изменения в специфичный для сайта файл `web.config` записывается только новая уникальная настройка конфигурации, и запись происходит немедленно. Таким образом, применение собственных модулей за счет их регистрации на уровне сервера еще не приводит к генерации файла `web.config`, специфичного для сайта. В следующем разделе мы взглянем на настройку веб-сайтов.

Подготовка веб-сайта

Подготовка веб-сайта — это искусство выделения ресурсов и создания структуры для нового веб-сайта. В наши дни поддерживается несколько протоколов доступа клиентов (HTTP, FTP, SOAP и т.п.), поэтому всестороннее обсуждение темы создания веб-сайта должно прояснить, какой тип трафика планируется поддерживать на создаваемом веб-сайте. Используемая терминология может снова породить некоторые проблемы при поиске лучшего метода создания сайтов.

Вспомните, что *сайт* в IIS — это логический объект, который просто определяет поведение, связанное с обработкой протокола и прослушиванием конечной точки, с целью приема клиентских запросов и реагирования на них. Любой клиентский запрос, содержащий IP-адрес назначения, порт назначения или заголовок запрашиваемого хоста в URL, который соответствует конфигурации нового сайта, будет немедленно направлен на этот новый сайт, а не на какой-то другой сайт, существующий на том же самом сервере IIS. Такой IP-адрес, порт и заголовок в контексте IIS называются *привязками*.

Поскольку значения привязок каждого HTTP-сайта должны быть уникальными для корректного направления обработки, сервер IIS выдаст сообщение об ошибке, если вы попытаетесь создать идентичные привязки протокола на более чем одном сайте. Однако имеются многие возможные комбинации IP-адреса, порта и заголовка хоста, которые позволят строить множество сайтов на одном и том же экземпляре IIS безо всяких конфликтов. Вскоре мы обсудим хостинг нескольких сайтов более подробно.

Внутри одного сайта наименьшая логическая единица, которая представляет часть или всю функциональность сайта, называется *приложением*. В рамках одного сайта может существовать множество приложений, которые допускается конфигурировать отдельно, исходя из соображений производительности и безопасности. Пространство имен URL каждого приложения отображается на физический диск посредством параметра конфигурации *виртуального каталога*. Сайт должен содержать минимум одно приложение, называемое *корневым приложением*. Это корневое приложение должно быть сконфигурировано с не менее чем одним виртуальным каталогом.

Прежде чем переходить к созданию сайта, важно осмыслить архитектуру в IIS. Сервер IIS основан на системе распределенной конфигурации в файлах XML. Настройки серверного уровня хранятся в файле `applicationhost.config`, и каждый сайт может иметь собственный файл `web.config`, в котором определены

настройки конфигурации сайта и ASP.NET. С учетом такой архитектуры, а также требований к уникальности привязок, можно перечислить некоторые из доводов в пользу создания новых сайтов:

- поддержка разных доменных имен;
- поддержка разных протоколов аутентификации;
- хостинг нескольких сайтов в единственном экземпляре IIS;
- хостинг отдельных приложений ASP.NET в единственном экземпляре IIS;
- максимизация производительности путем изоляции приложений в отдельные пулы приложений;
- максимизация утилизации дискового пространства с отдельными виртуальными каталогами;
- делегирование задач администрирования сайтов.

Понятие глобальных параметров

Прежде чем создавать новый веб-сайт, вы должны знать, что глобальные параметры определяются на уровне сервера в трех файлах конфигурации сервера.

- **`Machine.config`**. Находится в каталоге `%windir%\Microsoft.Net\Framework\версия_инфраструктуры\CONFIG`. Этот файл содержит стандартные глобальные параметры для ASP.NET.
- **`RootWeb.config`**. Находится в каталоге `%windir%\Microsoft.NET\Framework\версия_инфраструктуры\CONFIG`. Этот файл содержит остальные параметры для ASP.NET.
- **`applicationhost.config`**. Находится в каталоге `%windir%\system32\inetsrv\config`, который по умолчанию представляет собой папку с жестко ограниченным доступом посредством ACL (access control list — список управления доступом) файловой системы NTFS (табл. 19.2).

Корневым файлом конфигурации является `applicationhost.config`. В дополнение к стандартным глобальным параметрам он включает определение всех сайтов, приложений, виртуальных каталогов и пулов приложений.

Таблица 19.2. Разрешения NTFS для файла `applicationhost.config`

Запись управления доступом	Разрешение
`Administrators`	Full Control (Полный доступ)
`SYSTEM`	Full Control (Полный доступ)
`TrustedInstaller`	Full Control (Полный доступ)

Планирование веб-сайтов Apples и Oranges в Bigfirm

Одним из самых популярных протоколов для доставки статического содержимого по-прежнему является HTTP, поэтому давайте сосредоточим внимание на создании простых статических веб-сайтов HTTP.

Сначала вы создадите на сайте Default Web Site виртуальный каталог `apples`, а затем отдельный веб-сайт Oranges, воспользовавшись другими привязками протокола. Поскольку сайту Oranges нужно будет поддерживать страницы ASP, вы должны запускать его в отдельном пуле приложений. С учетом того, оба сайта должны иметь разные привязки и URL, вам придется создавать страницы Oranges как новый отдельный веб-сайт. Однако страницы Apples будут использовать те же параметры и пул приложений, что и Default Web Site, поэтому вы можете просто добавить содержимое сайта Apples в Default Web Site в виде нового виртуального каталога.

При выборе между добавлением `apples` как виртуального каталога к существующему корневому приложению Default Web Site и созданием второго приложения в Default Web Site для поддержки содержимого сайта Apples решающим фактором является поддержка кода. Вспомните, что приложения предназначены для предоставления и содержимого, и кода, следовательно, они дают возможность назначить им уникальный пул приложений. Поскольку страницы сайта Apples доставляют только статическое содержимое `.htm`, создание полностью нового приложения для этих страниц было бы явным излишеством для такой иллюстрации. Тем не менее, когда вы планируете собственную реализацию IIS, то должны ориентироваться на рост, масштаб и развитие. Если вы полагаете, что какой-то набор страниц со временем будет включать код, постройте для них приложение с самого начала и предоставьте ему возможность расти в будущем.

В версии IIS 8 по-прежнему предлагается сайт Default Web Site, который прослушивает на TCP-порте 80 все сетевые интерфейсы и не сконфигурирован для какого-то определенного заголовка хоста. Если эти характеристики приемлемы для нового веб-сайта, можете нацелить Default Web Site на свои каталоги содержимого, не создавая дополнительный сайт. Такой подход хорошо подойдет для сайта Apples.

Чтобы внести изменения в конфигурацию на уровне сервера, вы можете либо редактировать непосредственно файл `applicationhost.config`, либо воспользоваться диспетчером IIS, утилитой `AppCmd.exe` или PowerShell. Если вы решили редактировать файл `applicationhost.config`, обратите особое внимание на файл `%windir%\system32\inetsrv\config\schema\IIS_schema.xml`, где задается допустимая структура, которую можно записывать в `applicationhost.config`. На всякий случай можно создать резервную копию файла `applicationhost.config`, прежде чем вносить в него какие-то изменения. Если вы собираетесь часто редактировать файл `applicationhost.config` напрямую, благоразумно применять настоящее приложение для редактирования XML, такое как XML Notepad от Microsoft, доступное для бесплатной загрузки по адресу `http://tinyurl.com/MS2012XMLNotepad`.

Существует множество параметров, которыми вам, возможно, хотелось бы управлять на уровне сервера. Первым делом на ум приходят регистрация и безопасность модулей. Многими параметрами легче управлять в графическом пользовательском интерфейсе диспетчера IIS, с помощью утилиты `AppCmd.exe` или посредством PowerShell. Позже мы рассмотрим дополнительные темы, связанные с администрированием, а пока достаточно сказать, что имеет смысл идентифицировать параметры уровня сервера, которые будут настраиваться на новом сайте, и запланировать запрет наследования после создания нового сайта.

Важные разделы файла applicationhost.config

XML-файл applicationhost.config содержит настолько много элементов, что на первый взгляд довольно нелегко определить, какой тип конфигурационных настроек содержится в том или ином разделе этого файла. Чтобы помочь вам правильно ориентироваться в этом важном файле конфигурации на уровне сервера, ниже приведены описания основных разделов. Отступы отражают иерархию разделов в XML-схеме applicationhost.config.

<configuration>: корневой элемент.

<configSections>: регистрации невложенных разделов, организованных в виде групп.

<Section>: строительные блоки разворачиваемых, блокируемых, отыскиваемых параметров.

<configProtectedData>: регистрации поставщиков криптографии (алгоритмов).

<system.applicationHost>: конфигурации сайта, веб-приложения, виртуального каталога и пула приложений.

<applicationPools>: регистрации пулов приложений для изолированного выполнения.

<customMetadata>: данные совместимости с ABO (*не вносите изменения в этот раздел*).

<listenerAdapters>: привязки WAS (Windows Process Activation Service — служба активации процессов Windows).

<log>: определения двоичного журнала и журнала W3C.

<sites>: определения сайтов.

<system.webServer>: стандартные глобальные веб-параметры, отсутствующие в system.applicationHost.

<globalModules>: регистрации собственных модулей.

<http...>: сжатие HTTP, специальные ошибки, специальные заголовки, перенаправление, трассировка, фильтры ISAPI и ведение журналов ODBC.

<security>: параметры безопасности на уровне сервера.

<modules>: состояние блокировки модулей для распределенного управления.

Создание простого веб-сайта

Для создания новых веб-сайтов в IIS 8 можно применять инструменты администрирования с графическим пользовательским интерфейсом, утилиту AppCmd.exe или PowerShell в зависимости от уровня комфорта и от потребности в написании сценариев. Позже мы подробно рассмотрим PowerShell, а сейчас сосредоточим внимание на графическом пользовательском интерфейсе. Прежде чем вы приступите к действительному созданию сайта, потребуется провести планирование, чтобы определить подходящие параметры для своего нового сайта.

- Какой IP-адрес должен быть ассоциирован с этим сайтом?
- Какой номер порта TCP/IP должен быть связан с этим сайтом?
- Будет ли сайт использовать в URL специальный заголовок хоста?
- Какие пулы приложений будут применять приложения этого сайта?
- Куда будет указывать виртуальный каталог для нахождения содержимого для сайта?

Для начала вы должны ознакомиться с новым интерфейсом диспетчера IIS.

Создание сайта с помощью диспетчера IIS

После запуска нового диспетчера IIS вы, несомненно, обнаружите, что эта оснастка претерпела радикальные преобразования. Тем не менее, она по-прежнему является заранее сконфигурированным файлом консоли, и ее можно встраивать в любую специальную консоль управления. Начальная страница (рис. 19.7) по большей части предоставляет ссылки на новости и ресурсы, хотя панели Recent connections (Последние подключения) и Connection tasks (Задачи подключения) могут оказаться полезными при поиске и устранении проблем с несколькими серверами IIS из одной консоли управления.

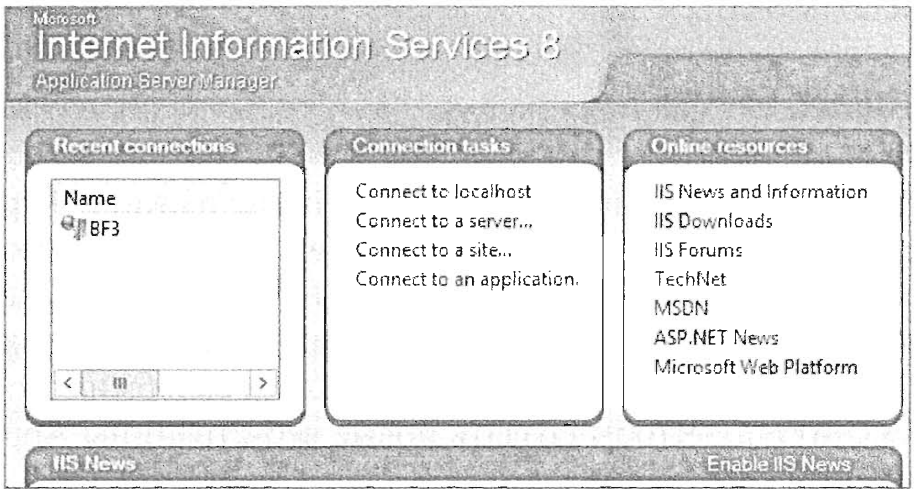


Рис. 19.7. Диспетчер IIS

После подключения к веб-серверу вы заметите, что в плане навигации со времен IIS 7 изменилось не особо много. В находящейся слева панели Connections (Подключения) по-прежнему легко перемещаться по вертикали, отображая пулы приложений и сайты разных серверов IIS, к которым в данный момент подключена консоль управления. Эта панель остается видимой на протяжении использования консоли. Поле в верхней части консоли, содержащее путь, располагает знакомыми кнопками Forward (Вперед), Back (Назад), Refresh (Обновить) и Help (Справка).

После выбора в панели Connections подключенного сервера вместо начальной страницы отобразится домашняя (Home) страница сервера с представлением Features (Компоненты) с группированием по областям, принятым по умолчанию. Справа появится также панель Actions (Действия), причем задачи в этой панели, доступные посредством гиперссылок, будут изменяться в соответствии с выделенным узлом внутри панели Connections (пример внешнего вида панели консоли показан на рис. 19.8).

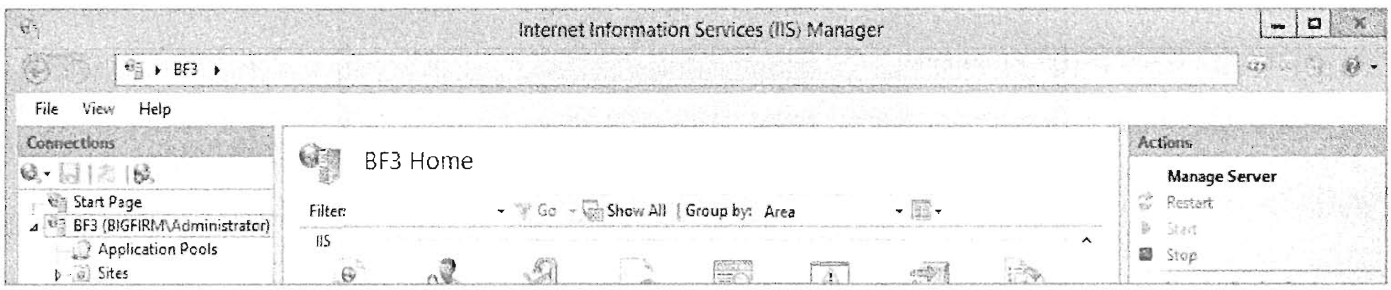


Рис. 19.8. Окно диспетчера IIS с выделенным сервером

Выполнение задач администрирования в диспетчере IIS будет подробно раскрыто на протяжении этой главы. Пока мы сосредоточимся на создании нового веб-сайта. Запомните компоненты, доступные на уровне сервера, потому что на новом сайте вы будете ограничены только этой функциональностью. Если новый сайт должен выполнять какую-то задачу, которая отсутствует в перечне компонентов данного сервера, лучше добавить необходимый компонент на сервер до создания нового сайта. Кроме того, вы заметите, что панель Actions предлагает многие средства конфигурирования, которые доступны в контекстном меню, открывающемся по щелчку правой кнопкой мыши на узле в панели Connections. Только представьте себе — более одного способа решения той же самой задачи в продукте Microsoft! Как бы то ни было, можете воспользоваться этой возможностью и ознакомиться с применением панели Actions вместо контекстных меню.

Конструирование веб-сайтов Bigfirm

В целях демонстрации предположим, что новые страницы Apples Rule!! будут частью домена `bigfirm.com` и обслуживать статическое содержимое `.htm` по всем сетевым интерфейсам сервера через TCP-порт 80. Кроме того, предположим, что текстовое содержимое и изображения для этих новых страниц уже хранятся в каталоге `apples`, созданном внутри стандартного каталога содержимого IIS 8 по имени `%systemdrive%\inetpub`. Чтобы создать новые веб-страницы Apples Rule!! в диспетчере IIS, выполните следующие шаги.

1. Раскройте узел сервера и узел Sites (Сайты) в панели Connections (Подключения).
2. Щелкните на элементе Default Web Site, затем щелкните на ссылке View Virtual Directories (Показать виртуальные каталоги) в панели Actions (Действия) и далее на ссылке Add Virtual Directory (Добавить виртуальный каталог) в панели Actions. Откроется диалоговое окно Add Virtual Directory (Добавление виртуального каталога), показанное на рис. 19.9.
3. В поле Alias (Псевдоним) введите дружественное к URL имя, которое является описательным, но кратким. В этом случае новым именем будет **`apples`**.

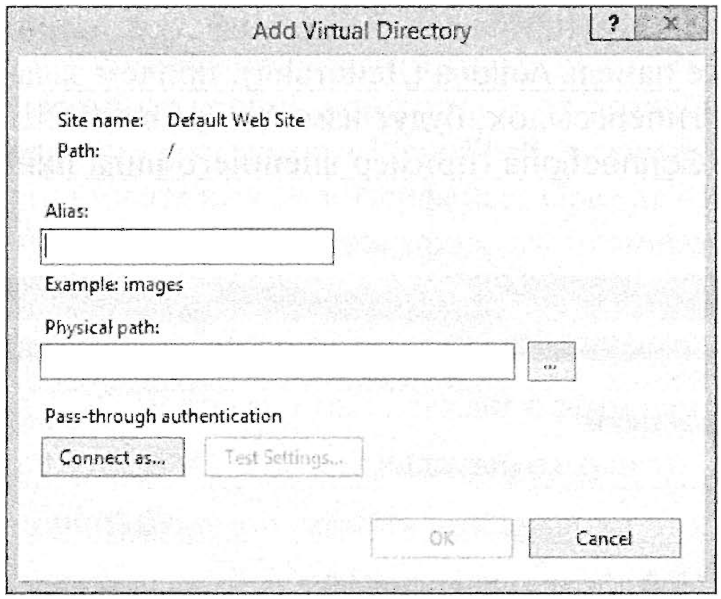


Рис. 19.9. Диалоговое окно Add Virtual Directory

4. В поле Physical path (Физический путь) введите `C:\inetpub\apples`.

   Если содержимое хранится в локальной папке на сервере IIS, который по стечению обстоятельств также совместно используется, для обеспечения максимальной производительности применяйте локальный путь вместо пути UNC. Как это всегда справедливо в случае использования путей UNC к удаленным папкам, по причинам, связанным с производительностью или конфиденциальностью, вы можете заменить имя хоста в пути IP-адресом.

5. Щелкните на кнопке OK в диалоговом окне Add Virtual Directory.

   Новый виртуальный каталог должен появиться в списке Virtual Directories (Виртуальные каталоги) внутри панели подробностей диспетчера IIS. Отсюда вы можете управлять свойствами и разрешениями нового виртуального каталога.

Теперь, когда виртуальный каталог создан и нацелен на содержимое Apples Rule!!, вы должны протестировать новую среду, перейдя на страницу Apples Rule!!. Не покидая окно диспетчера IIS, выполните одно из описанных ниже действий.

1. Щелкните правой кнопкой мыши на новом виртуальном каталоге в панели Connections (Подключения), выберите в контекстном меню пункт Manage Virtual Directory (Управлять виртуальным каталогом) и затем пункт Browse (Обзор).
2. Щелкните на новом виртуальном каталоге в списке Virtual Directories (Виртуальные каталоги).
3. Щелкните на ссылке Browse *.80 (HTTP) (Просмотреть *.80 (HTTP)) в панели Actions (Действия).

Каким бы из перечисленных методов вы ни воспользовались, запустится новый экземпляр Internet Explorer и перейдет прямо на новую страницу Apples Rule!! (рис. 19.10).

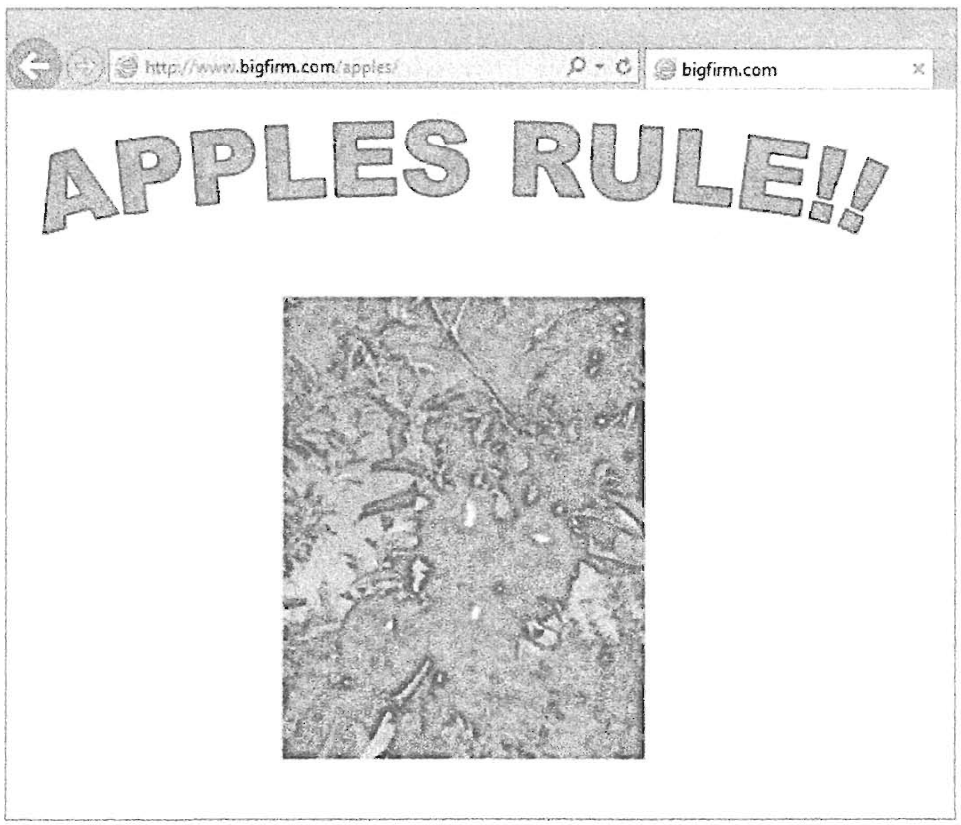


Рис. 19.10. Домашняя страница сайта Apples

В качестве стороннего замечания: в состав Windows Server 2012 входит Internet Explorer 8 с расширенной безопасностью, которая задействована по умолчанию. Если ваша страница не отображается, попробуйте либо добавить URL в список доверенных сайтов (Trusted Sites), либо отключите параметр IE Enhanced Security Configuration (Конфигурация с расширенной безопасностью IE).

Теперь, когда содержимое Apples Rule!! готово, наступило время построить сайт Oranges. Вспомните, что на этом сайте вы планируете применять дополнительные модули и код, поэтому он должен быть совершенно отдельным от Default Web Site и запускаться в отдельном пуле приложений. Чтобы создать новый веб-сайт Oranges в диспетчере IIS, выполните следующие шаги.

1. Раскройте узел сервера в панели Connections (Подключения), щелкните на узле Sites (Сайты) и щелкните на ссылке Add Website (Добавить веб-сайт) в панели Actions (Действия).

   Откроется диалоговое окно Add Website (Добавление веб-сайта), представленное на рис. 19.11.

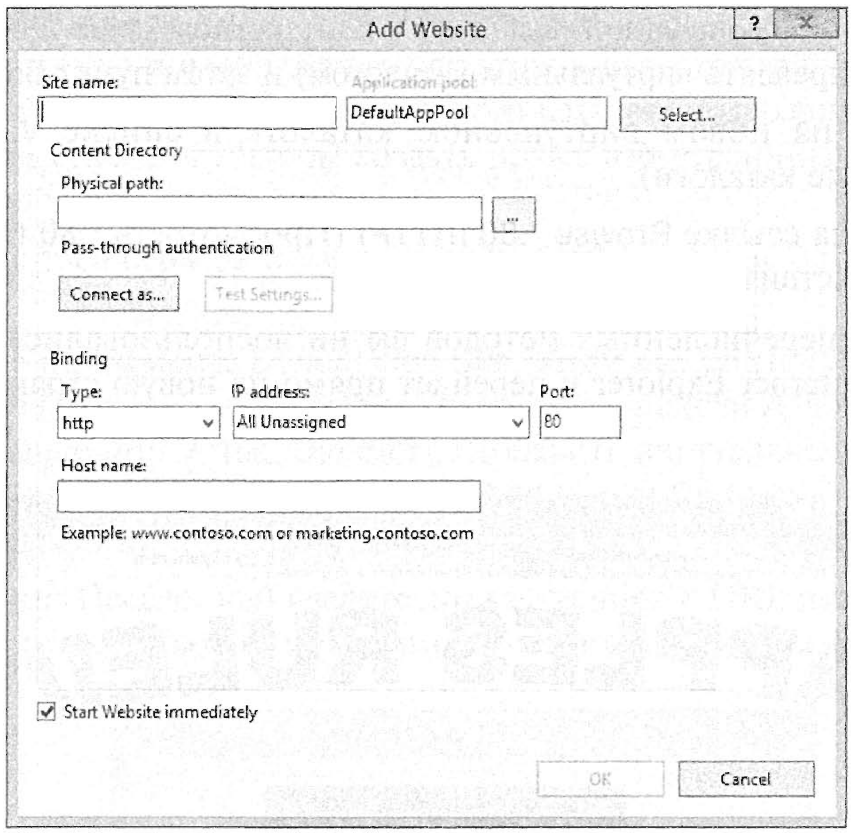


Рис. 19.11. Диалоговое окно Add Website

2. В поле Site name (Имя сайта) введите описательное и вместе с тем краткое имя сайта; в данном случае введите `Oranges`.

   Значение, введенное в этом поле, по умолчанию автоматически сгенерирует новый пул приложений в режиме, интегрированном с .NET, и назначит его новому сайту, если только вы не укажете какой-то существующий пул приложений, щелкнув на кнопке Select (Выбрать). Новый пул приложений будет создан с настройками параметров, которые определяются с помощью ссылки Set Application Pool Defaults (Установить стандартные параметры пула приложений), доступной в панели Actions, когда внутри панели Connections выбран узел Application Pools (Пулы приложений). Кроме того, по умолчанию для

целей безопасности будет создана генерируемая системой учетная запись удостоверения с тем же именем, что и пула.

3. В поле Physical path (Физический путь) введите физический путь к папке веб-сайта: `C:\inetpub\Oranges`.
4. По умолчанию используются учетные данные сквозной аутентификации; если вам понадобится заменить их определенной учетной записью, щелкните на кнопке Connect as (Подключаться как).
5. В раскрывающемся списке Type (Тип) внутри области Binding (Привязка) выберите `http`.
6. В раскрывающемся списке IP address (IP-адрес) внутри области Binding выберите вариант All Unassigned (Все неназначенные), чтобы привязать новый сайт Oranges к любым IP-адресам, которые сконфигурированы на всех сетевых интерфейсах сервера, но еще не назначены другим веб-сайтам в IIS.
7. В поле Port (Порт) оставьте значение `80`.

   Обратите внимание, что изменение этого значения потребует от клиентов предоставления в каждом запросе выбранного специального номера порта.
8. В поле Host name (Имя хоста) введите `oranges`, чтобы отличать его от страниц сайта Apples в Default Web Site.

Чтобы все создаваемые в дальнейшем сайты получали специальные параметры, можете изменить параметры в диалоговых окнах Application Pool Defaults (Стандартные параметры пула приложений) и Website Defaults (Стандартные параметры веб-сайта) и тем самым повлиять на создание сайтов в будущем. Ссылки на эти диалоговые окна, показанные на рис. 19.12, 19.13 и 19.14, появляются в панели Actions диспетчера IIS при выделении узлов Application Pools и Sites в панели Connections.

Имея созданный сайт Oranges, вы можете воспользоваться одним из двух описанных ранее методов навигации в диспетчере IIS, чтобы протестировать новый сайт, перейдя на него (рис. 19.15). Не забудьте при необходимости отключить параметр IE Enhanced Security Configuration или добавить URL-адрес `http://oranges` в список доверенных сайтов.

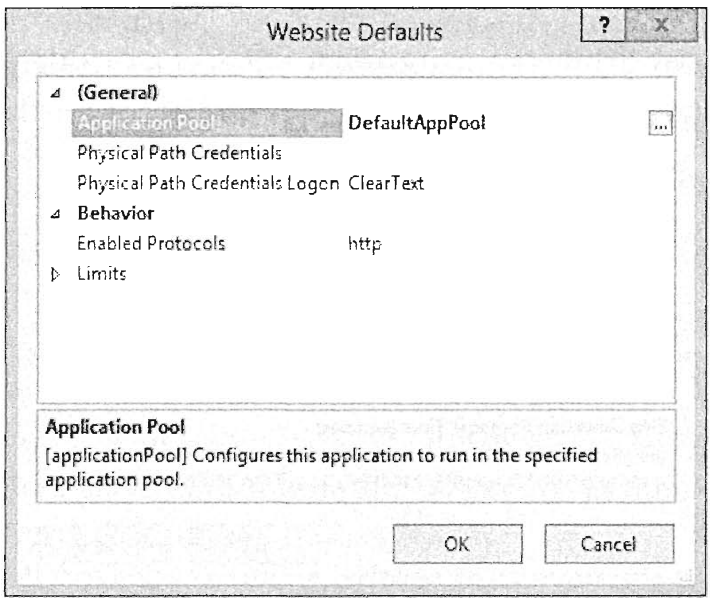


Рис. 19.12. Диалоговое окно Website Defaults

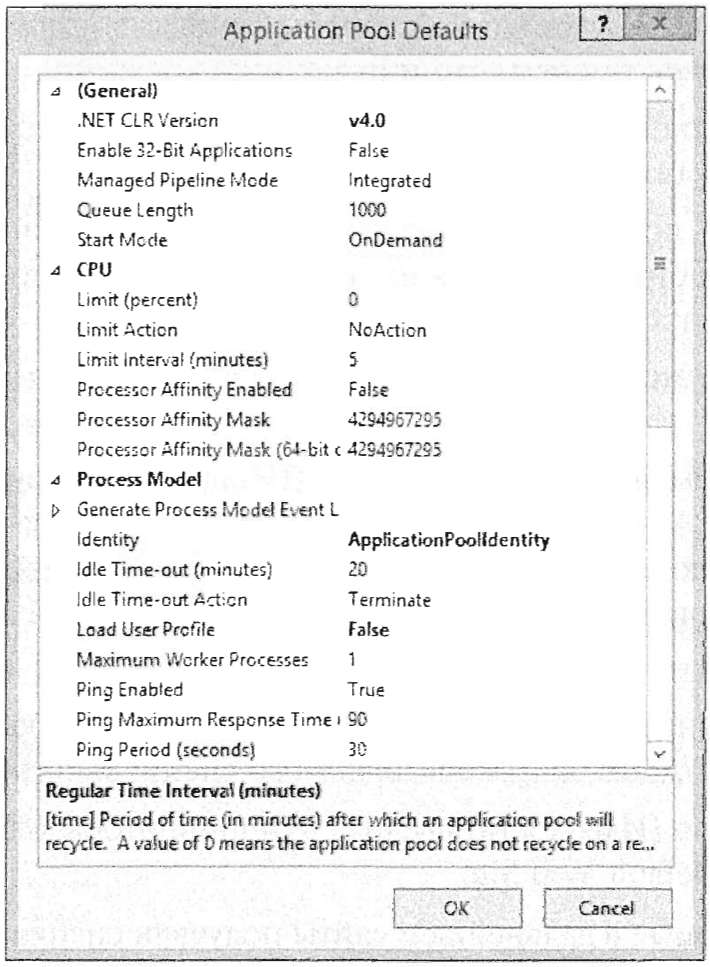


Рис. 19.13. Диалоговое окно Application Pool Defaults (первая часть)

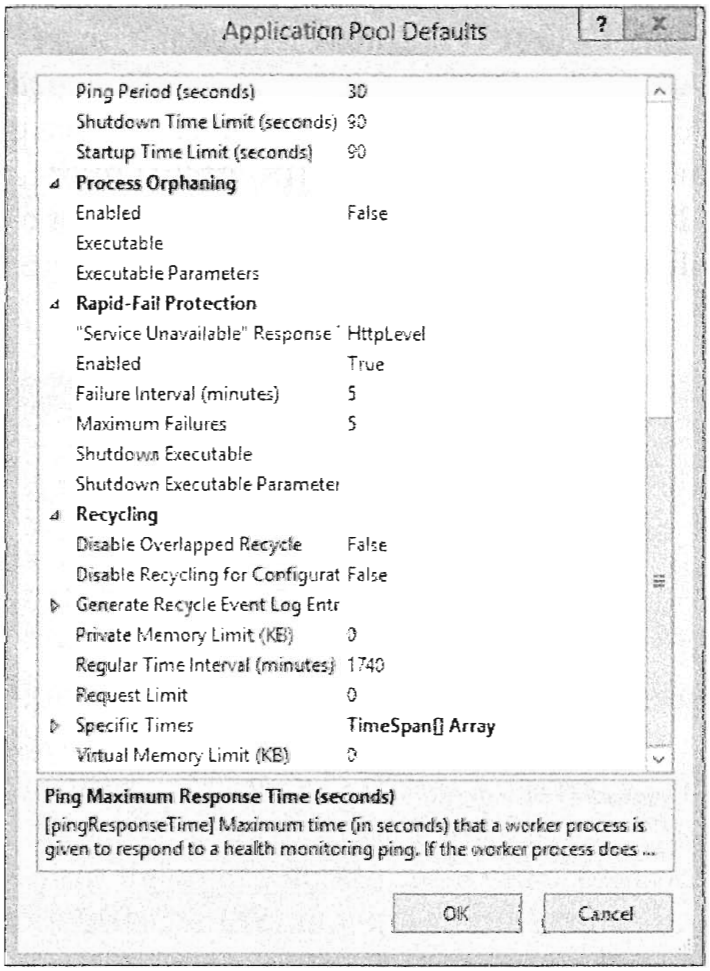


Рис. 19.14. Диалоговое окно Application Pool Defaults (вторая часть)

Рис. 19.15. Веб-сайт Oranges

Создание сайта с помощью PowerShell

В качестве альтернативы создать веб-сайт на своем веб-сервере можно с применением PowerShell. Преимущество инструмента PowerShell связано с тем, что он позволяет разрабатывать сценарии для создания сайтов и использовать их впоследствии. В действительности такие сценарии можно даже параметризировать, что дает возможность вставлять имя сайта и другие значения при запуске сценариев. Создание сайтов с помощью сценариев помогает развертывать сайты с похожей структурой и содержимым в рамках фермы веб-серверов с балансировкой сетевой нагрузки, а также проводить восстановление в случае аварии и документировать для контроля изменений.

Инструментом для создания сайтов в PowerShell является командлет `New-WebSite`. Ниже приведен синтаксис PowerShell, который позволит создать сайт по имени Oranges на TCP-порте 80, который нацелен на предполагаемый путь к каталогу, заканчивающийся на `\inetpub\oranges`, и применяет специальный заголовок хоста `oranges`:

```
New-Website -Name Oranges -Port 80 -HostHeader Oranges
  -PhysicalPath "$env:systemdrive\inetpub\oranges"
```

Если при создании нового сайта с помощью PowerShell не указать параметр `-Id` (как в этом примере), то IIS просто назначит новому сайту следующий доступный идентификатор. Кроме того, если не указать параметр `-PhysicalPath`, то для нового сайта не будут созданы приложения или виртуальный каталог, и после создания сайта вам придется добавить эти параметры вручную.

Инструмент PowerShell позволяет также отображать существующие сайты для целей инвентаризации или устранения проблем.

Для этого предусмотрена следующая команда:

```
Get-Website
```

В результате выполнения этой команды экран PowerShell должен содержать строки, показанные на рис. 19.16.

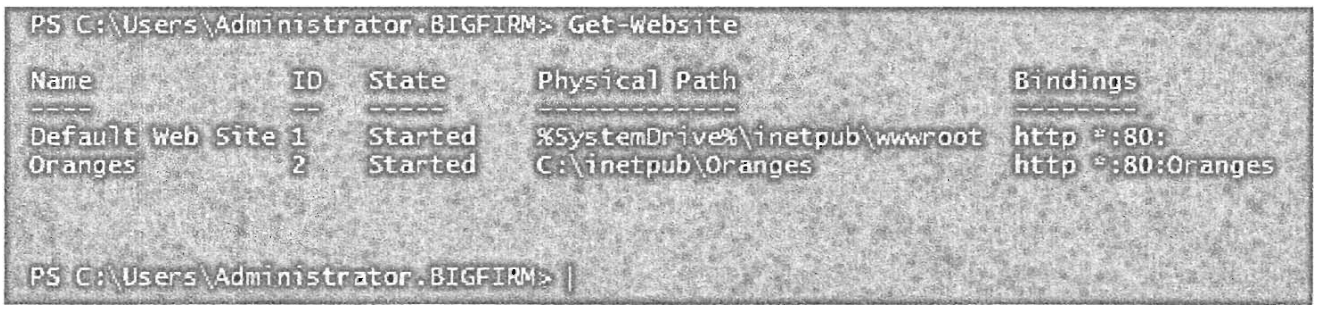


Рис. 19.16. Выполнение командлета PowerShell по имени `Get-WebSite`

Конфигурирование параметров сайта

После того как сайт будет создан, может понадобиться усовершенствовать его конфигурацию, прежде чем пригласить на него первых посетителей. Например, сайт Oranges нуждается в поддержке ASP и перенаправления HTTP, тогда как страницам Apples это не требуется. По умолчанию новый сайт немедленно начнет наследование параметров конфигурации из файла `applicationhost.config`. Прямо сейчас страницы Apples и Oranges включают все параметры из файла уровня сервера, атрибут `enabled` которых установлен в `true`. Вдобавок все модули, перечисленные в разделе `<globalModules>` файла `applicationhost.config`, также активизированы на Default Web Site, который управляет страницами Apples, равно как и на сайте Oranges.

Перед тем, как вносить любые изменения в стандартную сборку нового сайта, вы должны учитывать, что он не располагает файлом `web.config`. Однако если бы вы изменили сайт, то в его корневом виртуальном каталоге появился бы новый файл `web.config`, содержащий только измененный параметр, а все остальные параметры продолжали бы наследоваться из файла `applicationhost.config`. Тем не менее, то, появится ли запись в файле `web.config`, зависит от природы настройки. Например, отключение собственных модулей не приводит к генерации записи в `web.config`. Чтобы отключить HTTP Redirection и ASP (модуль ISAPI) на Default Web Site, выполните перечисленные ниже действия.

1. Запустите диспетчер IIS и раскройте узел сервера IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите элемент Default Web Site.

   По умолчанию центральная панель становится домашней страницей сайта, отображающей представление Features (Компоненты).
3. Дважды щелкните на значке Modules (Модули), чтобы увидеть список задействованных собственных модулей.

   Обратите внимание, что в списке присутствуют и `HttpRedirectionModule`, и `IsapiModule`.
4. Выделите модули `HttpRedirectionModule` и `IsapiModule` и щелкните на гиперссылке Remove (Удалить) в панели Actions (Действия).

5. Подтвердите удаление, щелкнув на кнопке Yes (Да) в открывшемся диалоговом окне.

Но что если настройка не касалась использования модулей, а сводилась просто к изменению параметра сайта? Например, как быть, если на какой-то странице, поддерживаемой в настоящий момент сайтом Default Web Site, вы решили задействовать просмотр каталогов? Это изменение приведет к созданию нового файла `web.config` в подпапке `\inetpub\wwwroot`, которая содержит новую функциональность просмотра каталогов. Чтобы включить просмотр каталогов на Default Web Site, выполните следующие шаги.

1. Запустите диспетчер IIS и раскройте узел сервера IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите Default Web Site.

   По умолчанию центральная панель становится домашней страницей сайта, отображающей представление Features (Компоненты).
3. Дважды щелкните на значке Directory Browsing (Просмотр каталогов).
4. Щелкните на гиперссылке Enable (Включить) в панели Actions (Действия).

Включением параметра просмотра каталогов вы инициировали добавление новой записи в файл `web.config` для Default Web Site:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <directoryBrowse enabled="true" />
   </system.webServer>
</configuration>
```

Достоинство файла `web.config` заключается в том, что теперь независимо от того, какое решение относительно просмотра каталогов примет администратор уровня сервера, страницы Default Web Site обеспечат возможность просмотра благодаря специальному файлу `web.config`. Это возможно лишь потому, что файл `applicationhost.config` любезно "разрешает" режим переопределения (`overrideMode`) для конфигурации `directoryBrowse`. Если бы администратор уровня сервера действительно хотел контролировать поведение вашего сайта, он мог бы модифицировать файл `applicationhost.config` так, чтобы администратор уровня сайта не имел возможности изменять параметр `directoryBrowse` (установив `overrideMode="Deny"`). Позже мы обсудим администрирование более подробно.

Хостинг нескольких веб-сайтов

Существует много причин для хостинга нескольких веб-сайтов на одном сервере IIS. Иногда это просто попытка извлечь максимум возможного из потенциала оборудования. Другая стратегия может предусматривать хостинг одного и того же сайта на множестве серверов с целью создания фермы веб-серверов с балансировкой рабочей нагрузки. Затем то же самое делается для второго сайта, третьего сайта и т.д. Когда речь идет о хостинге нескольких веб-сайтов, вам придется принять ряд решений, чтобы обеспечить бесперебойное администрирование и доставку содержимого.

- Во-первых, решите, сколько сайтов будет размещаться на данном веб-сервере.

  Динамическая активизация сайтов (Dynamic Site Activation) по умолчанию вступает в действие только при наличии более 99 сайтов. Поэтому, если вы имеете дело с меньшим количеством сайтов, но хотите воспользоваться средствами ускорения, вам придется скорректировать соответствующие параметры.

- Во-вторых, вы должны принять во внимание изоляцию веб-сайтов.

  Отделите друг от друга пулы приложений и сконфигурируйте регулировку центрального процессора, чтобы ни один из сайтов не мог неумышленно повлиять на другой сайт, потребляя слишком много ресурсов.

- В-третьих, делегирование задач администрирования делает возможным такое распределение работ, при котором у администраторов не возникают ситуации чрезмерной загруженности обязанностями, связанными с обслуживанием многих сайтов.

  Распределенное управление может быть даже *требованием* политики, принятой в среде.

- В-четвертых, если какой-то сайт должен быть развернут на нескольких серверах (как в решении с фермой веб-серверов), то применение предпочтительного метода развертывания может упростить данный процесс и обеспечить его согласованность.

  Уникальность привязок сайтов, назначение учетных записей пулов приложений и процессы аутентификации образуют набор других проблем, которые необходимо решить, прежде чем приступать к хостингу нескольких веб-сайтов.

Развертывание сайтов

Одна из положительных сторон модели конфигурирования, используемой в IIS, заключается в том, что конфигурация и содержимое сайта могут находиться в том же самом каталоге. Файл `web.config`, специфичный для сайта, теперь содержит как конфигурацию веб-сайта, так и конфигурацию ASP.NET, поэтому все необходимые параметры сайта сосредоточены в одном месте. Преимущество такого подхода связано с тем, что теперь можно переносить целиком веб-сайты и их конфигурацию с одного сервера на другой легко и эффективно.

Встроенная группа `IIS_IUSRS` в IIS 8 получает в качестве члена каждый процесс в ходе работы, и посредством такого членства принимаемый процесс получает доступ к конфигурационным файлам и содержимому данного веб-сайта. Поскольку встроенная группа `IIS_IUSRS` применяет один и тот же идентификатор SID во всех операционных системах Windows Server 2012, развертывание сайтов на новых серверах больше не требует обширного переопределения разрешений каталогов.

Чтобы отключить автоматическую вставку удостоверений процесса во встроенную группу `IIS_IUSRS` в ходе работы, включите `manualGroupMembership` следующим образом:

```
<applicationPools>
  <add name="DefaultAppPool">
      <processModel manualGroupMembership="true" />
  </add>
</applicationPools>
```

Это одна из стандартных установок, которые необходимо редактировать непосредственно в файле `applicationhost.config`, т.к. в графическом пользовательском интерфейсе диспетчера IIS она не нашла своего отражения.

Если вы являетесь большим поклонником низкоуровневого копирования файлов, то для переноса веб-сайтов IIS с одного сервера на другой можете пользоваться утилитой командной строки `xcopy.exe`. Но существует более удобный способ. Инструмент Microsoft Web Deploy 3.0 (`msdeploy.exe`) доступен в 32-разрядной и 64-разрядной версиях и полностью поддерживает IIS 7 и IIS 8 для модернизации, синхронизации или перемещения целых веб-сайтов. На самом деле инструмент Web Deploy можно сконфигурировать также и для миграции поддерживающей структуры IIS, такой как ключи реестра и списки ACL. Описание инструмента Web Deploy выходит за рамки данной книги, но дополнительные сведения о нем можно получить на следующих сайтах в Интернете:

- полное описание инструмента Microsoft Web Deploy — `http://tinyurl.com/MS2012WDTInfo`
- место для загрузки Microsoft Web Deploy — `http://tinyurl.com/MS2012WDTInstaller`

В дополнение к миграции или переносу веб-сайтов новый инструмент Microsoft Web Deploy также обладает возможностью создания *снимка*, или архива, веб-сайта. Хотя такой снимок не является заменой надежной стратегии резервного копирования, он может предоставлять быструю копию веб-сайта для поиска и устранения проблем, для восстановления или для развертывания на другой машине. Инструмент Microsoft Web Deploy можно установить в режиме удаленного обслуживания или в автономном режиме. Автономный режим — это всего лишь применение `msdeploy.exe` для создания снимка веб-сайта и ручное копирование этого снимка на другой сервер. Режим удаленного обслуживания позволяет выполнять `msdeploy.exe` из целевого сервера и запрашивать данные из исходного сервера, на котором функционирует зависимая *служба агента веб-развертывания* (Web Deployment Agent Service), по умолчанию прослушивающая `http://+:80/MSDEPLOYAgentService/`; однако во время установки может быть указан специальный URL-адрес в командной строке.

Прежде чем использовать `msdeploy.exe` для переноса веб-сайта, может потребоваться идентификация списка зависимых компонентов, которые должны находиться на целевом сервере, чтобы сайт мог нормально функционировать в своем новом месте обитания. Ниже показан синтаксис командной строки для просмотра списка зависимых компонентов:

```
Msdeploy -verb:getDependencies -source:apphostconfig="{имя_сайта}"
```

Удостоверившись в том, что все зависимые объекты успешно установлены на целевом сервере, можете применить `msdeploy.exe` для переноса своего веб-сайта из экземпляра IIS 7.5 в новый экземпляр IIS 8.5.

1. Возьмите архив существующего сайта на целевом сервере (*если* в прошлом выполнялось его копирование):

```
Msdeploy -verb:sync -source:apphostconfig="{имя_сайта}" -dest:archivedir={путь}
```

2. Запустите имитированную синхронизацию, чтобы проверить действие перед фактическим копированием данных:

```
Msdeploy -verb:sync -source:archivedire={путь}
  -dest:apphostconfig="имя_сайта" -whatif > {filename}.log
```

3. После того как файл журнала будет утвержден, синхронизируйте исходный сайт с целевым:

```
Msdeploy -verb:sync -source:archivedire={путь} -dest:apphostconfig="имя_сайта"
```

Вышеупомянутый метод синхронизирует снимок или архив, сгенерированный `msdeploy.exe`, с вашим экземпляром IIS 8.5.

Динамическая активизация сайтов

Ранее мы уже рассказывали о том, что динамическая активизация сайтов (Dynamic Site Activation) увеличивает скорость начального запуска сервера IIS. При наличии большого количества сайтов служба Windows Process Activation Service (WAS) будет загружать каждый сконфигурированный сайт на сервер. Динамическая активизация сайтов будет пропускать активизацию любых сайтов, когда служба WAS запущена, выполняя ее только в случае получения запроса. Это приводит к увеличению времени начальной загрузки в первом запросе, но в дальнейшем сайт должен реагировать нормально. Стандартное количество сконфигурированных сайтов, позволяющее применять Dynamic Site Activation, составляет 100, но его можно уменьшить или увеличить, как описано ниже.

1. В консоли диспетчера IIS выберите сервер в панели Connections (Подключения) и дважды щелкните на элементе Configuration Editor (Редактор конфигурации).
2. Выберите раздел `system.applicationHost/weblimits`.
3. Измените значение `dynamicRegistrationThreshold` желаемым образом.

Уникальность сайтов

Ранее в этой главе мы обсуждали определение нескольких сайтов внутри одного экземпляра IIS за счет использования уникальных привязок сайтов, а именно — выбора определенного IP-адреса, сконфигурированного на один или более интерфейсов NIC, указания специального номера TCP-порта (отличного от 80) или добавления к новому сайту специального заголовка хоста. Несмотря на содействие в корректной маршрутизации запросов, привязки TCP/IP не являются единственным способом, с помощью которого сайт можно различать от других сайтов на том же самом сервере.

Вспомните, что по умолчанию создание нового веб-сайта приводит к автоматическому созданию для него нового пула приложений, имя которого совпадает с именем этого сайта. Памятуя о том, что новые пулы приложений создаются в соответствии со стандартными параметрами пула приложений, которые упоминались ранее в главе, можно оказывать воздействие на удостоверение всех новых пулов приложений, редактируя свойство Identity (Удостоверение) в диалоговом окне Application Pool Defaults (Стандартные параметры пула приложений), как показано на рис. 19.17.

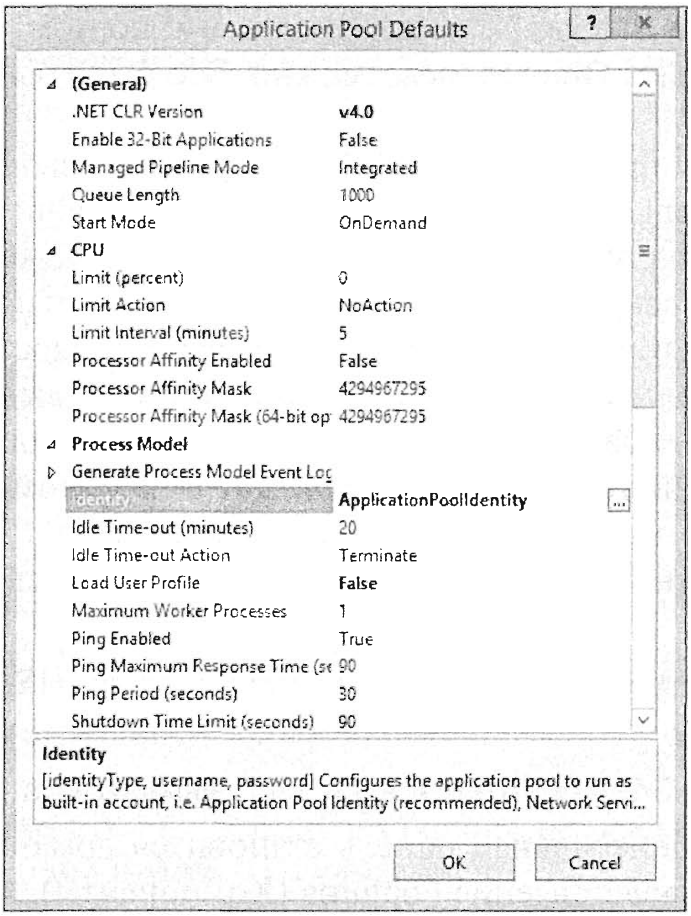


Рис. 19.17. Свойство Identity в диалоговом окне Application Pool Defaults

Стандартным значением Identity в IIS 8 является новая учетная запись удостоверения пула приложений (Application Pool Identity Account), которая автоматически генерируется во время создания пула. Однако это значение можно изменить на `LocalService`, `LocalSystem`, `NetworkService` либо именованную учетную запись по вашему выбору.

Настройка анонимной учетной записи

Теперь, когда вы знаете, как применять учетную запись конкретного пользователя к пулу приложений либо в процессе создания (уникально), либо через стандартные параметры пула приложений, разве не было бы удобно задействовать ту же самую учетную запись пользователя для чего-то большего, чем просто удостоверения пула приложений? Обычно вы ожидаете видеть в среде Windows учетную запись `IUSR_`*имямашины*, которая автоматически назначается всем анонимным действиям. Однако `IUSR_`*имямашины* была заменена учетной записью `IUSR`, чтобы избежать проблем с развертыванием на ферме с множеством веб-серверов. Если требуется обеспечить обратную совместимость, вы по-прежнему можете создавать учетную запись `IUSR_`*имямашины*, но учтите, что в недоверяемых доменах вы будете ограничены возможностями этой учетной записи.

Управление несколькими сайтами для Bigfirm

Вспомните, что сайту Oranges требуется модуль HTTP Redirection, т.к. вы планируете построить новый сайт и со временем перейти на него.

Создать новый сайт Oranges с тем же IP-адресом, портом TCP и заголовком хоста, что и у текущего сайта Oranges, невозможно. Это было бы недопустимо на очень многих уровнях.

Представьте, что вы проводите на сайте Oranges аудит ввода-вывода и инициализации процесса. Поскольку сайт Oranges может быть сконфигурирован на использование уникального пула приложений, а каждый пул приложений можно настроить на самостоятельную идентификацию посредством уникальной учетной записи, вы можете упростить задачу аудита, ограничив посредством удостоверений пула приложений длинный журнальный файл до веб-сайта, который выдает ошибку.

При разработке приложений ASP.NET на новом сайте или для проведения различий между приложениями, функционирующими на одном сайте, иногда полезно предусматривать анонимную учетную запись, отличную от `IUSR`. Для этого необходимо назначить выбранную учетную запись пользователя свойствам аутентификации данного сайта.

1. Запустите диспетчер IIS и раскройте узел сервера IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите элемент Oranges.

   По умолчанию центральная панель становится домашней страницей сайта, отображающей представление Features (Компоненты).
3. Дважды щелкните на значке Authentication (Аутентификация) и выделите элемент Anonymous Authentication (Анонимная аутентификация) в списке поставщиков.
4. Щелкните на гиперссылке Edit (Правка) в панели Actions (Действия).
5. В диалоговом окне Edit Anonymous Authentication Credentials (Редактирование анонимных учетных данных аутентификации) установите анонимные учетные данные либо для удостоверения конкретного пользователя, либо для удостоверения пула приложений (рис. 19.18).

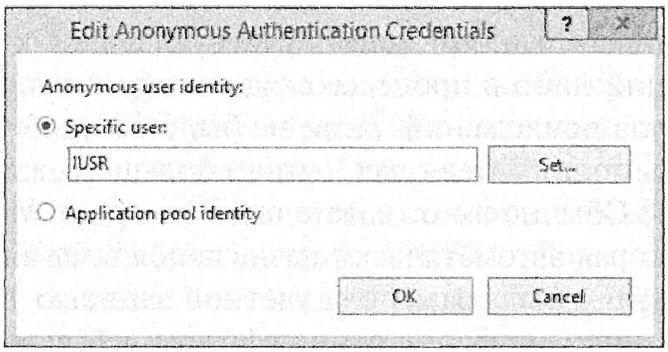


Рис. 19.18. Диалоговое окно Edit Anonymous Authentication Credentials

Переключатель Application pool identity (Удостоверение пула приложений) для анонимных учетных данных может пригодиться на веб-сайте, поддерживающем множество приложений, каждое из которых применяет уникальный пул приложений, сконфигурированный с уникальной учетной записью службы. После этого отчеты по аудиту точно покажут, какое приложение внутри сайта неправильно использовалось анонимными посетителями.

Делегирование компонентов

Делегирование компонентов живет и здравствует и является наилучшим решением для распределения администрирования IIS 8 между администраторами и другими пользователями, к примеру, разработчиками. По существу делегирование компонентов — это практика разблокирования определенных параметров конфигурации на уровне сервера в файле `applicationhost.config`, чтобы другие пользователи, такие как разработчики и администраторы сайтов, могли переопределять значения этих параметров на конкретных сайтах. Однако планирование эффективного делегирования можно сравнить с хождением по канату, натянутому высоко над землей: один неверный шаг — и ваша реализация IIS может остаться уязвимой для угроз безопасности. Когда дело доходит до конфигурирования параметра делегирования для каждого компонента, тщательно обдумайте, кому вы доверяете в достаточной степени, и только затем принимайте решения по утилизации и защите ресурсов на веб-сервере. Если вы делегируете компонент неопытному администратору сайта, он может неумышленно открыть весь сервер вредоносному коду или содержимому и скомпрометировать все веб-сайты на сервере. Регулирование и планирование подхода к делегированию компонентов должно быть в числе важнейших приоритетов.

В сущности, делегирование компонентов предусматривает разблокирование определенных разделов в файлах `web.config` для одного или нескольких сайтов. Разрешая указанной ограниченной группе пользователей чтение и запись определенных параметров конфигурации, вы разрешаете им вносить изменения в конфигурацию одного или нескольких веб-сайтов без связывания с вами, как администратором сервера, но это касается только разблокированных компонентов. Например, пусть вы делегируете компонент Digest Authentication, но не компонент ASP. Указанные пользователи смогут вносить в конфигурацию сайта изменения, влияющие на аутентификацию с помощью дайджеста, однако у них не будет возможности изменять параметры, которые воздействуют на поведение ASP. Делегирование компонентов может осуществляться либо на уровне сервера, чтобы идентифицировать стандартные параметры сайта, либо на уровне сайта, чтобы запретить наследование стандартных параметров сервера и конфигурировать уникальное делегирование сайт за сайтом. Другими словами, если возникает конфликт относительно того, какие компоненты кому делегированы, то предпочтение отдается параметру делегирования на уровне сайта.

Но это еще не все. Возможность внесения изменений в конфигурацию сайтов избранными пользователями зависит также от списков ACL для файлов `web.config`. Один лишь факт делегирования компонента совершенно не означает, что избранные пользователи имеют что-то сверх разрешения на чтение файла `web.config` сайта. Теперь вы должны выдать избранным пользователям разрешение на запись в файлы `web.config` их сайтов, чтобы позволить им изменять конфигурационные параметры разблокированного компонента. Для достижения максимальной безопасности при конфигурировании сайтов делегирование компонентов и списки ACL файловой системы NTFS должны поддерживаться согласованно.

Делегирование администрирования

В крупной среде IIS, поддерживаемой множеством администраторов, имеет смысл закрепить за разными администраторами ответственность за управление разными сайтами. На одиночном экземпляре IIS делегирование административных обязанностей на уровне сайтов требует, чтобы администратор серверного уровня разблокировал определенные аспекты более низких уровней сайтов.

Внутри файла applicationhost.config серверного уровня предпочтительный метод разблокирования интересующих конфигурируемых разделов в определениях веб-сайтов более низкого уровня предусматривает добавление дескриптора <location>. Например, если вы хотите управлять ведением журнала HTTP на уровне веб-сайта, можете изменить файл applicationhost.config следующим образом:

```
<location path="Default Web Site" overrideMode="Allow">
  <system.webServer>
    <httpLogging />
  </system.webServer>
</location>
```

Разблокирование конфигурируемых параметров можно также осуществлять с применением командлета PowerShell под названием Remove-WebConfigurationLock; однако на момент написания данной книги он не поддерживал удаление монопольной блокировки, поэтому приходилось сначала очищать весь раздел, а затем добавлять необходимые блокировки.

Разумеется, разрешение переопределения стандартных параметров серверного уровня на более низком уровне веб-сайтов вовсе не гарантирует, что администратор этого более низкого уровня действительно возьмется за управление собственными журналами. Успешное делегирование обязанностей требует хорошей подготовки и управления ответственностью. Но теперь, по крайней мере, файл applicationhost.config не препятствует редактированию параметров сайта с помощью диспетчера IIS.

Установка и конфигурирование SMTP

С выходом Windows Server 2012 в Microsoft решили объявить сервер SMTP не рекомендуемым. В версии Windows Server 2012 R2 служба SMTP по-прежнему работает, как это было в Windows Server 2008 R2, за исключением сценария управления, который был удален. Вы можете продолжать пользоваться этой службой, как делали это в прошлом, но администраторы и программисты должны перейти к применению System.Net.Smtp для отправки почты. Информация о System.Net.Smtp доступна по адресу http://tinyurl.com/MS2012SMTP.

Служба SMTP в IIS 8 не изменилась по сравнению с предыдущими версиями, но продолжает оставаться очень полезным инструментом. Она предназначена для отправки почты из сервера IIS другому серверу SMTP, и хотя она отправляет и принимает почтовые сообщения, она не предназначена для предоставления почтовых ящиков конечным пользователям. Функциональность подобного рода обеспечивает программное обеспечение Exchange Server или Office 365.

Начало работы

Компонент сервера SMTP при своей загрузке полагается на наличие успешно установленной консоли диспетчера Internet Information Services (IIS) 6.0 *и* модулей IIS 6 Metabase из службы роли IIS 6 Management Compatibility для IIS 8 (позже мы поговорим об установке подробнее). Эти модули IIS 6.0 используют конфигурационный файл IIS 8 по имени metabase.xml (из каталога %systemroot%\System32\inetsrv), который после установки SMTP получает несколько новых записей, наиболее важные из которых перечислены ниже.

<IISConfigObject Location="/LM.../DisplayName">
Устанавливает отображаемое имя компонента сервера SMTP в `SMTP Server`.

<IISConfigObject Location="/LM.../BindingManagerMoniker">
Устанавливает привязку событий для сервера SMTP в `smtpsvc1`.

<IISConfigObject Location="/LM.../Sources.../DisplayName">
Устанавливает отображаемое имя объекта ОС привязанной службы в `smtpsvc1`.

<IISSmtpService Location="/LM/SmtpSvc">
Содержит все параметры для службы SMTP (такие как тайм-ауты, максимальное количество подключений, поставщики аутентификации и опции).

<IISSmtpServer Location="/LM/SmtpSvc/1"...>
Содержит почтовые параметры для службы SMTP (такие как каталоги, TCP-порт и параметры маршрутизации).

Управлять службой SMTP Server можно, напрямую редактируя файл `metabase.xml`, но есть и более простой способ — консоль диспетчера Internet Information Services (IIS) 6.0, окно которой показано на рис. 19.19. По существу это та же самая консоль, которая применялась администраторами в прошлом для конфигурирования службы SMTP, поставляемой в составе IIS 6.0. Чтобы отобразить узел SMTP, в панели с древовидным представлением в левой части окна раскройте узел сервера для машины, на которой размещена служба SMTP. Первое, что вы заметите — служба SMTP установлена с запуском вручную. Для настройки параметров запуска вы должны сконфигурировать саму службу с помощью диспетчера IIS (рис. 19.20).

Если вы установили не только обязательные службы роли IIS 8, то поведение запуска службы SMTP после установки будет отличаться. В частности, если вы установили все службы роли IIS 8 Web Server, то служба SMTP будет запускаться немедленно после добавления компонента SMTP, несмотря на то, что она сконфигурирована на запуск вручную. И хотя это может быть удобно в начале, после первого перезагрузки веб-сервера будет непонятно, почему служба SMTP также не перезапускается самостоятельно. Таким образом, подумайте об изменении параметра запуска этой службы с ручного на автоматический.

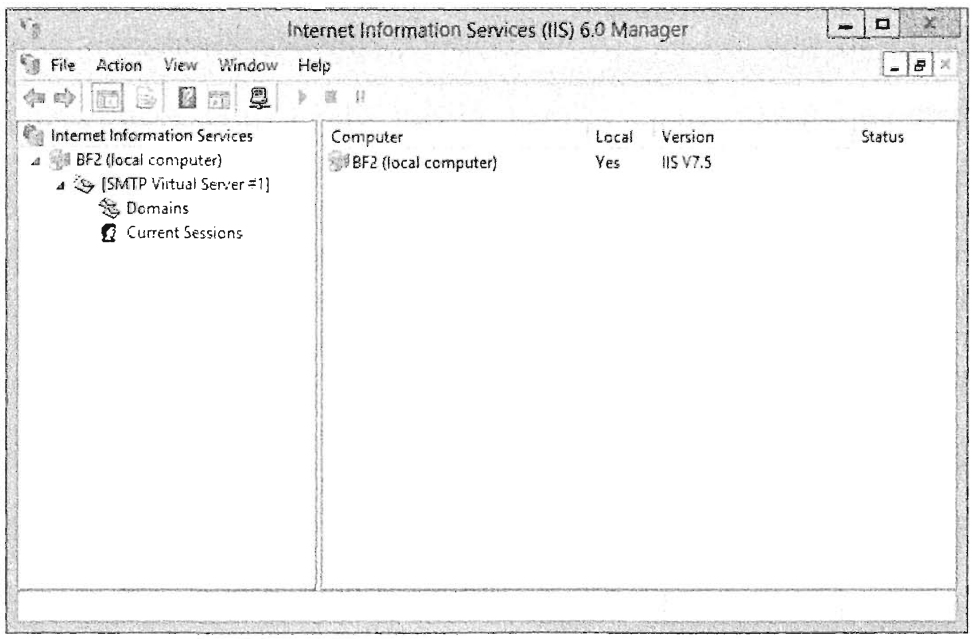


Рис. 19.19. Консоль диспетчера Internet Information Services (IIS) 6.0

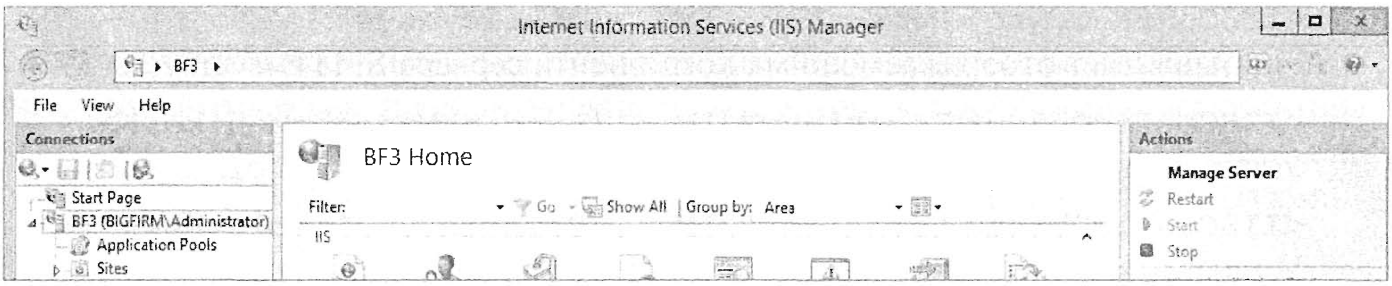


Рис. 19.20. Свойства службы SMTP

Добавление компонента SMTP Server

В дополнение к службам роли IIS 6 Metabase Compatibility и консоли диспетчера IIS 6.0 для IIS 8, компонент SMTP также требует использования компонента SMTP Server Tools (Инструменты сервера SMTP). Утилит диспетчера серверов, как с графическим пользовательским интерфейсом, так и работающие в командной строке, вполне достаточно для установки этих зависимостей в процессе установки службы SMTP. Компонент SMTP Server Tools предоставляет оснастку консоли диспетчера IIS 6.0, необходимую для администрирования службы SMTP. Чтобы установить этот обязательный компонент SMTP Server Tools с помощью графического пользовательского интерфейса, во время выполнения мастера добавления ролей и компонентов отметьте флажок для SMTP Server Tools в группе Feature Administration Tools (Инструменты администрирования компонентов), входящей в группу Remote Server Administration Tools (Инструменты дистанционного администрирования сервера). Интересно, могли ли в Microsoft упрятать это еще глубже?

Несколько слов о конфигурировании служб ОС

Стандартным именем ОС для службы SMTP является `SMTPSVC`, а отображаемым именем — Simple Mail Transfer Protocol (SMTP), и она зависит от службы IIS Admin. По умолчанию она аутентифицируется как учетная запись `Local System` (Локальная система), включена для всех профилей оборудования и не имеет сконфигурированных параметров восстановления. Чтобы обеспечить готовность службы SMTP на своих веб-сайтах, подумайте о настройке параметров восстановления при перезапуске, как вы бы делали это для любой другой службы, критически важной для системы.

Когда минимальных требований оказывается *действительно* недостаточно

Минимальной установки только служб роли IIS 6 Metabase Compatibility и консоли IIS 6.0 для IIS 8 будет недостаточно для развертывания на своих веб-сайтах компонента IIS 8 под названием SMTP E-mail. Фактически даже стандартная установка роли Web Server не предоставит достаточное количество служб роли для облегчения конфигурирования поддержки SMTP на сайтах.

Чтобы внедрить SMTP на веб-сайте, в Microsoft рекомендуют полностью установить все службы роли IIS 8. Но давайте подумаем о безопасности! К счастью, для укрепления защиты сервера можно отключить неиспользуемые компоненты сайта в файле `applicationhost.config`, в корневом файле `web.config` или в файлах `web.config`, специфичных для сайтов.

Чтобы установить компонент SMTP Server с помощью диспетчера серверов, просто выберите в меню Manage (Управление) пункт Add Roles and Features (Добавить роли и компоненты). Затем выберите SMTP Server в списке компонентов. Если же вы решили установить компонент SMTP Server посредством PowerShell, применяйте следующий синтаксис, чтобы установить и обязательные службы роли Web Server, и компоненты SMTP:

```
Add-WindowsFeature SMTP-Server
```

Настройка SMTP Server

После установки компонента SMTP Server можно настроить его конфигурацию и сформировать дополнительную поддержку доменов с применением консоли диспетчера Internet Information Services (IIS) 6.0. Хотя сама служба находится в данной консоли, встраивание службы SMTP внутрь веб-сайта IIS 8 осуществляется в другом месте (вскоре мы рассмотрим этот вопрос более детально). Навигация в консоли диспетчера Internet Information Services (IIS) 6.0 может вызвать прилив ностальгических воспоминаний, поскольку интерфейс является таким же, как у консоли из IIS 6 в Windows Server 2003.

Виртуальные серверы и домены

Компонент SMTP Server предлагает возможность передачи почты посредством конфигурационных параметров виртуального сервера SMTP. По умолчанию во время установки SMTP создается только один виртуальный сервер SMTP, но вы можете создать дополнительные виртуальные серверы, если будете размещать почту для разных доменных имен, которые должны быть сконфигурированы отдельно. Внутри каждого виртуального сервера SMTP должно существовать одно или несколько доменных имен, которые связывают соответствующий каталог файловой системы, предназначенный для доставки почты, с определенным полным доменным именем (Fully Qualified Domain Name — FQDN). По умолчанию первоначально созданный виртуальный сервер SMTP будет содержать только один домен, имеющий имя FQDN машины, где он находится.

Отличия в требованиях к безопасности и ограничениях доставки у дополнительных доменов могут обусловливать необходимость их обслуживания отдельными виртуальными серверами SMTP. Прежде чем принимать решение о том, какие домены должны обслуживаться тем или иным виртуальным сервером SMTP, необходимо изучить параметры виртуального сервера SMTP, которые оказывают влияние на домены. Каждый новый виртуальный сервер SMTP будет хранить свои конфигурационные параметры в совместимом с IIS 6 файле `metabase.xml` внутри отдельного элемента `IIsSmtpServer` с атрибутом `Location`, установленным в `/LM/SmtpSvc/{номер}`, где `{номер}` — последовательное целое число, которое назначается новым виртуальным серверам в порядке их создания. Допускается создавать столько виртуальных серверов, скольким можно назначить уникальную комбинацию IP-адресов и номеров TCP-портов, поддерживаемых сервером.

Если взамен вы обнаружите, что вся электронная почта подчиняется одним и тем же ограничениям и может обслуживаться единственным виртуальным сервером SMTP, тогда самым удобным способом будет использование стандартного сервера SMTP Virtual Server #1, построенного во время установки компонента. Просто до-

бавьте нужное количество доменов, которые должны поддерживаться для маршрутизации сообщений, в папку Domains (Домены), относящуюся к стандартному виртуальному серверу. В папке Domains можно создать новый домен, щелкнув на ней правой кнопкой мыши и выбрав в контекстном меню пункт для создания нового домена с помощью мастера создания домена SMTP (New SMTP Domain Wizard). Этот мастер идентифицирует следующие параметры:

- Domain Type (Тип домена) — удаленный или псевдоним;
- Domain Name (Имя домена) — полное адресное пространство, совместимое с протоколом x400, для почты, которая должна доставляться новым доменом (удостоверьтесь, что система DNS сконфигурирована на распознавание этого имени).

По завершении работы мастера откройте окно свойств нового домена, чтобы указать, должен ли он придерживаться ограничений квоты каталога входящих сообщений, установленных в конфигурационных параметрах виртуального сервера, на котором он размещен. Каждый новый домен будет формировать собственный элемент `IIsSmtpDomain` в конфигурационном файле `metabase.xml`.

Некоторые изменения требуют перезапуска служб

Добавление виртуальных серверов SMTP и/или доменов в Windows Server 2012 не вступит в силу до тех пор, пока службы SMTP не будут остановлены и перезапущены. Консоль диспетчера Internet Information Services (IIS) 6.0 предлагает быстрый метод перезапуска всех служб IIS, который предусматривает щелчок правой кнопкой мыши на имени компьютера в верхней части древовидной панели, выбор в контекстном меню пункта All Tasks (Все задачи) и затем пункта Restart IIS (Перезапустить IIS).

Аутентификация

В целях безопасности службу SMTP можно сконфигурировать так, чтобы она требовала аутентификации от других хостов SMTP, пытающихся передать ей сообщения. По умолчанию разрешен только анонимный доступ, что дает возможность любым серверам SMTP, которые хотят переместить сообщения электронной почты для поддерживаемых пространств имен домена, наводнять элементами каталог входящих сообщений. В безопасной среде, а также в целях аудита вам может понадобиться применить какой-то метод аутентификации, чтобы другие хосты SMTP были обязаны идентифицировать себя, прежде чем они получат разрешение передавать сообщения вашей службе SMTP.

Добавление компонента SMTP E-mail на веб-сайт IIS 8

После установки службы SMTP и всего набора служб роли Web Server в консоли диспетчера Internet Information Services (IIS) 6.0 для веб-сайтов IIS 8 появится компонент SMTP E-mail. Независимо от состояния виртуальных серверов SMTP, компонент SMTP E-mail можно включать или отключать для всего сервера IIS либо только для выбранных сайтов или веб-приложений. Глобальные параметры SMTP, определенные в файле `applicationhost.config` на серверном уровне, могут быть унаследованы одним или несколькими веб-сайтами.

Компонент SMTP E-mail указан на уровне сервера в области, озаглавленной как ASP.NET (рис. 19.21). В представлении Features (Компоненты) область Actions (Действия) для компонента SMTP E-mail, как и для любого другого компонента, предлагает быстрые ссылки, позволяющие открывать страницу параметров этого компонента, перезапускать/запускать/останавливать компонент, просматривать пулы приложений, сконфигурированные для обслуживания компонента, просматривать сайты, настроенные на использование этого компонента, а также получать справку по этому компоненту.

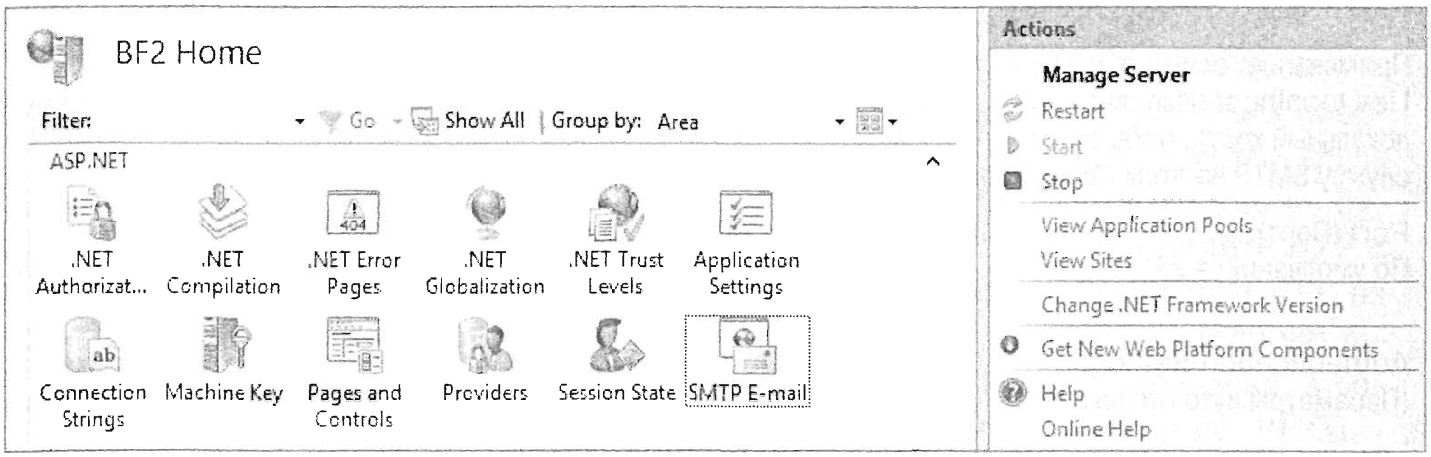


Рис. 19.21. Компоненты серверного уровня для сервера IIS 8 по имени `BF1`

После открытия страницы параметров компонента SMTP E-mail (рис. 19.22) вы можете устанавливать конфигурационные параметры, описанные в табл. 19.3.

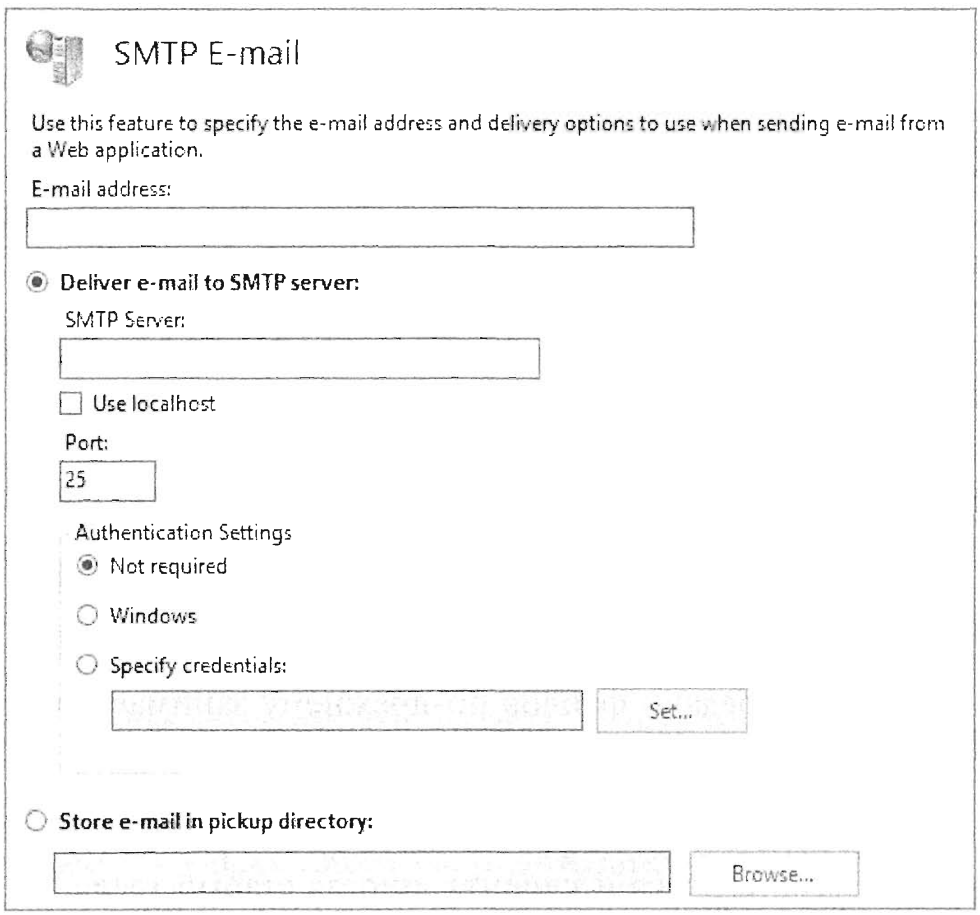


Рис. 19.22. Страница параметров компонента SMTP E-mail

Таблица 19.3. Параметры компонента SMTP E-mail

Параметр	Возможные значения	Описание
E-mail address (Адрес электронной почты)	Допустимый адрес почтового ящика из домена-отправителя	Указывает адрес электронной почты отправителя, который будет применяться при отправке сервером IIS почты из веб-приложения
Deliver email to SMTP server (Доставлять электронную почту серверу SMTP) SMTP Server (Сервер SMTP) Примечание: отметьте флажок Use localhost (Использовать локальный хост), чтобы применять службу SMTP на этом же сервере	Функционирующий сервер SMTP	Указывает сервер SMTP, обрабатывающий домен, который указан в параметре E-mail address
Port (Порт) По умолчанию = 25	Любой доступный номер TCP-порта	Указывает TCP-порт, на котором сервер SMTP будет прослушивать трафик SMTP
Authentication Settings (Параметры аутентификации)	Not required (Не требуются) Windows Specify credentials (Указать учетные данные)	Указывает метод аутентификации, поддерживаемый сервером SMTP. В поле, расположенном ниже переключателя Specify credentials, введите необходимые учетные данные
Store email in pickup directory (Сохранять электронную почту в выбранном каталоге)	Допустимый каталог файловой системы	Альтернатива доставке электронной почты серверу SMTP. Электронная почта сохраняется в указанном каталоге файловой системы для дальнейшей выборки приложением извлечения почты

После конфигурирования на серверном уровне индивидуальные веб-сайты и веб-приложения могут быть модифицированы для отправки электронной почты альтернативным серверам SMTP или поддержки других пространств имен доменов в их адресах электронной почты. Просто щелкните на значке компонента SMTP E-mail на уровне любого веб-сайта или веб-приложения, чтобы изменить поведение почты применительно к этой сущности.

Интеграция FTP в веб-страницы IIS 8

Во времена SkyDrive, Dropbox и всех прочих средств, ориентированных на облачные технологии, у вас может сложиться впечатление, что старый добрый протокол FTP остался в далеком прошлом. Однако этот хорошо опробованный и проверенный метод простой передачи файлов по-прежнему занимает сентиментальное, если только не функциональное, место в наших сердцах. И хотя верно утверждение о том, что во многих веб-приложениях, доступных на современном рынке, с помощью сложного кода ASP.NET маскируется всего лишь фактическое перемещение данных между системами сервера и клиента, иногда старый тезис "чем проще, тем лучше" звучит совершенно справедливо, когда дело доходит до управления передачей файлов в неоднородной сети.

Компания Microsoft сделала протокол FTP более универсальным, чем его предыдущая версия, и предоставила в ваше распоряжение новые инструменты обеспечения безопасности, которые помогут защитить доступ к данным и их транспортировку, сохраняя пользователю простоту работы. Например, FTP теперь поддерживает ограничения на число попыток входа, а также интеграцию дисковых квот Windows Server 2012 для усовершенствованного управления хранилищем. Более глубокие исследования службы FTP выходят за рамки данной главы, посвященной IIS, так что мы лишь бегло рассмотрим вопрос включения компонентов FTP в веб-сайты IIS 8.

Служба публикации FTP

Поскольку протокол FTP входит в состав IIS 8, вам понадобится только добавить службу роли FTP к роли Web Server, чтобы получить возможность пользоваться простой передачей файлов посредством своих веб-сайтов. Поскольку ранее в этой главе мы уже рассказывали о добавлении служб роли в IIS 8, то повторяться здесь не будем. Как и со всеми компонентами, ролями и службами ролей, не добавляйте FTP к своему веб-серверу, если отсутствует реальная необходимость в применении FTP на каком-то веб-сайте; в противном случае вы только внесете дополнительную уязвимость в плане безопасности. После того как служба роли FTP будет добавлена, в области FTP консоли диспетчера IIS появится множество новых значков (рис. 19.23).

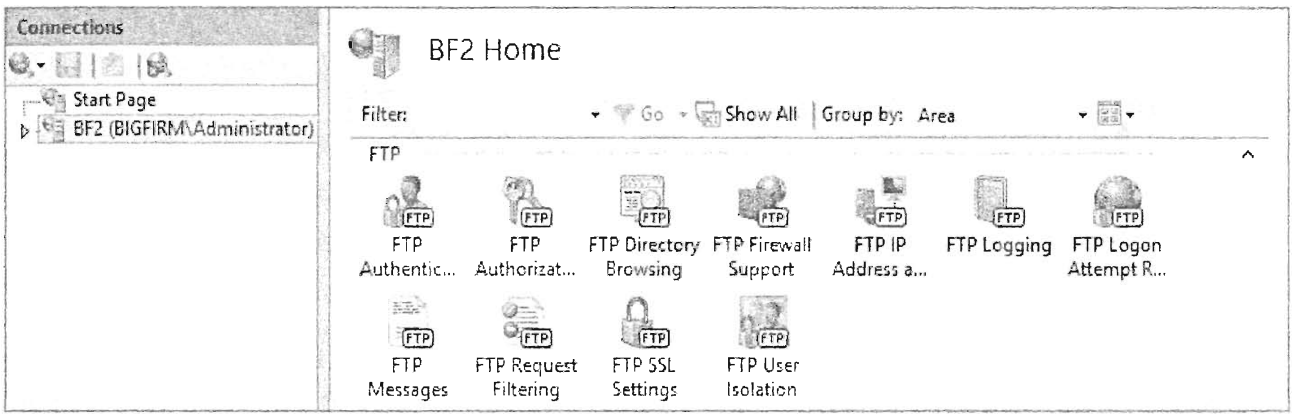


Рис. 19.23. Область FTP в консоли диспетчера IIS

Добавление FTP на веб-сайт IIS 8

Одно из преимуществ службы публикации FTP (FTP Publishing) связано с тем, что вы можете добавить функциональность FTP к существующему веб-сайту в IIS 8 непосредственно рядом с HTTP. В панели Actions (Действия) внутри консоли диспетчера IIS щелкните на ссылке Add FTP Publishing (Добавить публикацию FTP), чтобы получить конфигурацию FTP для сайта HTTP. Однако прежде чем добавлять передачу файлов, вы должны принять несколько предварительных решений.

Во-первых, т.к. FTP является отдельным протоколом, вы должны идентифицировать уникальный набор привязок для службы. Точнее говоря, необходимо запланировать IP-адрес, номер порта и виртуальный хост. Да, речь идет именно о *виртуальном хосте*. Подобно сайтам HTTP, служба FTP может функционировать со специальным именем заголовка, облегчая пользователям подключение к сайтам с дружественными именами. Кроме того, вы должны решить, будет ли FTP-сайт запускаться автоматически и следует ли задействовать SSL.

На рис. 19.24 показано диалоговое окно Add FTP Site (Добавление FTP-сайта) с вариантами, доступными для протокола SSL. Можно выбрать переключатель Require SSL (Требовать SSL) и таким образом отпугнуть клиентов, которые не могут работать с SSL. Можно смягчить требования к безопасности, выбрав переключатель Allow SSL (Разрешить SSL), который предлагает незащищенную передачу файлов для тех клиентов, которые не могут задействовать SSL. Наконец, можно выбрать переключатель No SSL (Без SSL), чтобы принять решение позже (это приведет к блокированию подключений SSL).

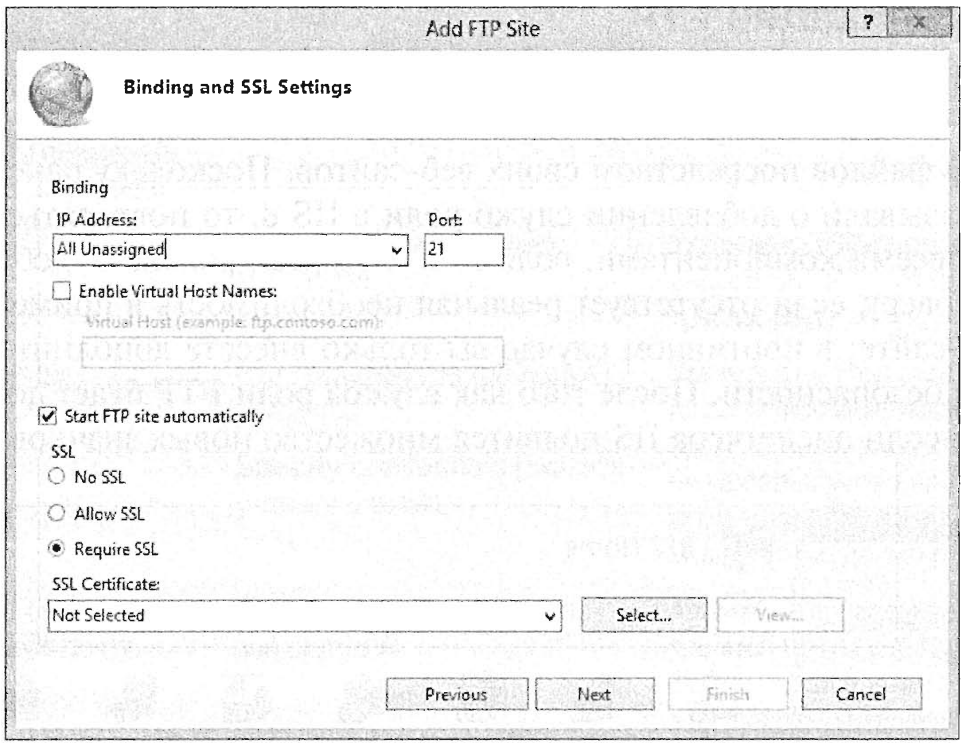


Рис. 19.24. Диалоговое окно Add FTP Site

Во-вторых, вы должны спланировать, следует ли разрешить встроенной службе FTP Publishing принимать анонимные подключения и поддерживать пароли в виде простого текста при базовой аутентификации. Вы можете также ограничить доступ только анонимными пользователями или определенными пользователями/группами (рис. 19.25). Вдобавок вы должны решить, могут ли разрешенные пользователи осуществлять запись или только чтение.

Для проверки, успешно ли была встроена служба FTP Publishing в веб-сайт, внутри панели Connections (Подключения) понадобится раскрыть хост, к которому была добавлена служба FTP. В представлении Features (Компоненты) теперь имеется новая группа значков, предназначенных для управления FTP; ниже описаны наиболее значимые возможности.

- Правила авторизации FTP позволяют конфигурировать дополнительные правила, которые либо предоставляют определенной группе пользователей конкретный уровень разрешений на доступ к службе FTP на этом сайте, либо отказывают в доступе.
- Ограничения на IP-адрес и домен FTP позволяют ограничивать службу FTP единственным IP-адресом, диапазоном подсетей или доменным именем.
- Изоляция пользователей FTP позволяет предотвращать пользователям доступ к каталогам других пользователей.

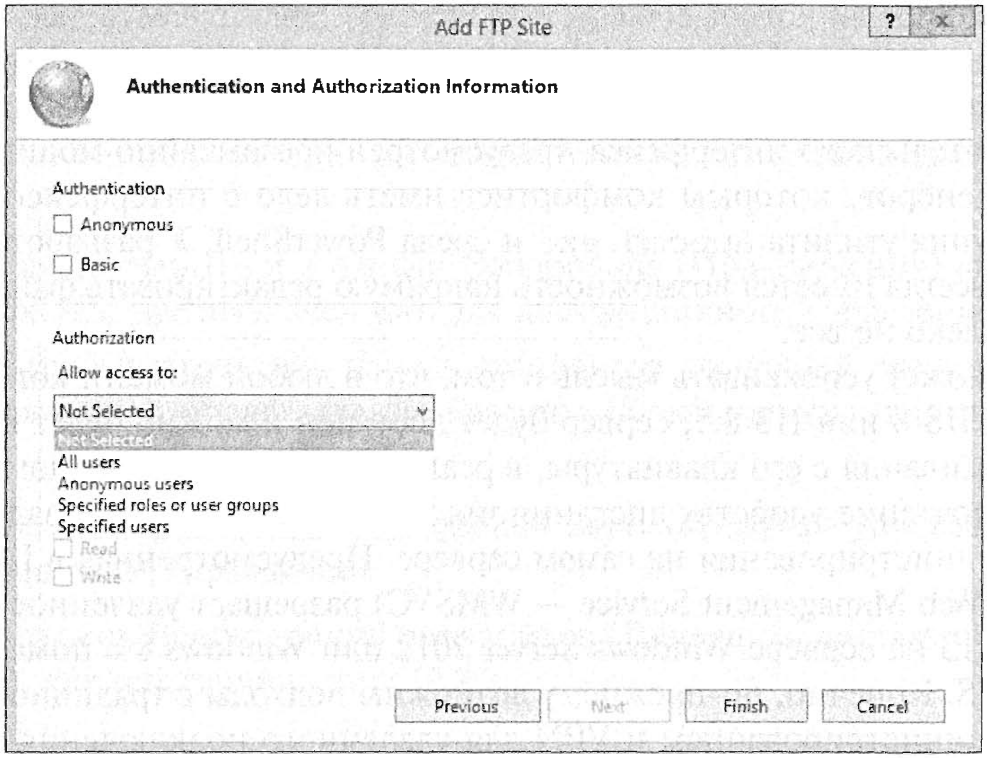


Рис. 19.25. Аутентификация и авторизация FTP-сайта

Одной из важных возможностей, которая не конфигурируется на основе веб-сайтов, является ограничение на количество попыток входа в FTP-сайт. Эта новая возможность позволит устанавливать порог для числа неудавшихся попыток входа, по достижении которого IP-адрес, откуда поступали эти попытки, блокируется, либо информация о таких попытках просто фиксируется в журнальном файле. Данный параметр можно конфигурировать только на уровне сервера.

В качестве альтернативного метода создания нового сайта службы FTP Publishing можно использовать PowerShell. Преимущества применения PowerShell как метода создания включают написание сценариев, автоматизацию и удаленное управление. Например, чтобы создать новый FTP-сайт по имени `FTPTest` со стандартными параметрами, который использует специальный порт номер 2121 и явно заданный физический каталог `D:\FTPTest`, можно ввести следующую команду:

```
New-WebFTPSite -Name FTPTest -Port 2121 -PhysicalPath D:\FTPTest
```

Имейте в виду, что этот новый FTP-сайт будет создан с очередным свободным идентификатором, т.к. в команде он не указан. Кроме того, будут сконфигурированы стандартные протоколы аутентификации и сущности авторизации.

Вспомните, что FTP — сама по себе мощная служба роли, и в случае ее применения на веб-сервере понадобится принять во внимание множество факторов. Описанию продукта FTP посвящены целые главы, и даже небольшие книги! Хотя детальное рассмотрение вопросов администрирования и безопасности FTP выходит за рамки этой главы, посвященной IIS, разумно подробнее ознакомиться с этим протоколом, чтобы неумышленно не сделать свои веб-сайты потенциально уязвимыми.

Расширенное администрирование

К этому моменту мы предоставили достаточный объем сведений об установке и конфигурировании IIS 8, а также о создании и управлении сайтами. Однако еще ос-

талась пара вопросов, которые следует прояснить. Преимущество администрирования IIS 8 кроется во всех инструментах, предлагаемых Microsoft, которые способны удовлетворить практически любые инженерные вкусы. Для поклонников графического пользовательского интерфейса предусмотрен чрезвычайно мощный диспетчер IIS. Для инженеров, которым комфортнее иметь дело с интерфейсом командной строки, доступна утилита `Appcmd.exe` и среда PowerShell. У разработчиков, знакомых с XML, всегда имеется возможность напрямую редактировать файлы `*.config`. И это еще далеко не все.

Хотя вас может успокаивать мысль о том, что в любой момент, когда понадобится управлять IIS 8 или IIS 8.5, сервер будет доступен и можно будет выполнять все задачи обслуживания с его клавиатуры, в реальности большинство администраторов отдают предпочтение удобству дистанционного управления перед надежностью локального администрирования на самом сервере. Предусмотренная в IIS служба веб-управления (Web Management Service — WMSVC) разрешает удаленное подключение к установке IIS на сервере Windows Server 2012 или Windows 8 с помощью консоли диспетчера IIS. Конечно, по-прежнему возможны подходы с традиционным дистанционным администрированием и VPN для удаленного подключения к операционной системе, но зачем излишне тратить полосу пропускания, если это не обязательно? Учитывая, что служба WMSVC использует статическое назначение TCP-порта, настройка брандмауэра для разрешения удаленного доступа извне представляется более легкой задачей, чем поддержка подключения VPN или RDP.

Но если во время дистанционного управления установкой IIS вы склонны иметь полный доступ к ОС, то в Microsoft предлагают надежную платформу дистанционного управления под названием Windows Remote Management (WinRM), которая предоставляет доступ на основе SOAP к системе Windows Server 2012 по всем портам, обычно разрешенным в брандмауэре. WinRM стала доступной в Windows Server 2003 R2, но требовала добавления посредством панели управления. Начиная с Windows Server 2012 платформа Windows Remote Management изначально установлена, включена и готова к применению.

Использование службы WMSVC

Прежде чем вы усядетесь за свой компьютер и запустите консоль диспетчера IIS, которая подключится к серверу IIS, находящемуся в другом крыле здания, потребуется выполнить определенную подготовительную работу. Ниже перечислены базовые задачи, которые вам предстоит выполнить для установки службы дистанционного управления.

1. Установка службы WMSVC.
2. Разрешение дистанционного подключения.
3. Конфигурирование дополнительных параметров.
4. Запуск службы WMSVC.

Хотя последняя задача представляется настолько очевидной, что ее не стоило и упоминать, порядок выполнения задач имеет первостепенное значение. Постарайтесь не переусердствовать, запустив только что установленную службу WMSVC до ее конфигурирования. Когда служба WMSVC функционирует, изменить ее невозможно.

Чтобы установить WMSVC на сервере IIS, добавьте роль Management Service (Служба управления) к роли Web Server в операционной системе. Ранее в этой главе были раскрыты другие методы добавления служб роли. Чтобы разрешить возможность дистанционного подключения в системе Windows Server 2012, выполните следующие шаги.

1. Запустите диспетчер IIS и в панели Connections (Подключения) щелкните на узле сервера IIS, предназначенного для дистанционного управления.

   По умолчанию центральная панель становится домашней страницей сервера, отображающей представление Features (Компоненты), как показано на рис. 19.26.

2. Дважды щелкните на значке Management Service (Служба управления) в разделе Management (Управление).

3. Отметьте флажок Enable remote connections (Разрешить дистанционные подключения), как показано на рис. 19.27.

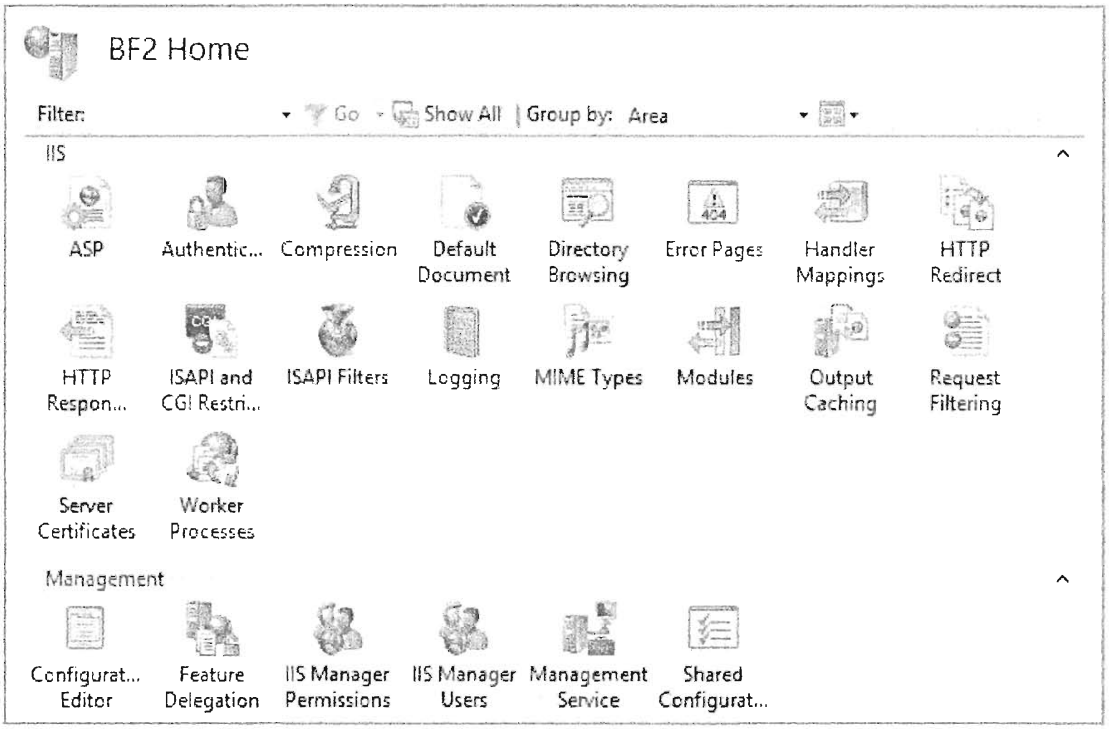


Рис. 19.26. Домашняя страница сервера в диспетчере IIS

Разрешить возможность дистанционного подключения можно также с помощью приведенной ниже команды PowerShell:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\WebManagement\Server
   -Name EnableRemoteManagement -Value 1
```

Дополнительные параметры WMSVC, которые может понадобиться сконфигурировать, включают привязку данной службы к специальной структуре IP-адресов или порта TCP. По умолчанию WMSVC прослушивает TCP-порт 8172 по всем IP-адресам на сервере. В качестве альтернативы можно явно перечислить IP-адреса, которым разрешено подключаться, а также указать, будет ли WMSVC принимать учетные данные Windows и учетные данные диспетчера IIS.

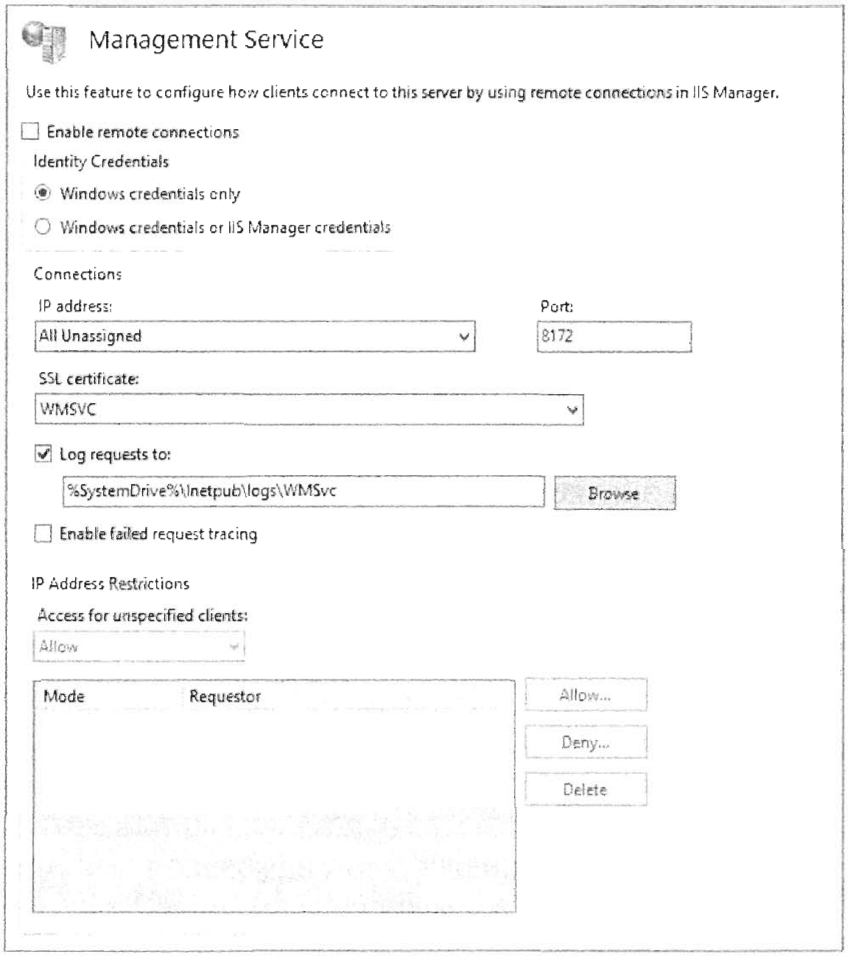


Рис. 19.27. Роль Management Service

Чтобы сконфигурировать дополнительные параметры, выполните описанную ниже последовательность действий.

1. Запустите диспетчер IIS и в панели Connections (Подключения) щелкните на узле сервера IIS, предназначенного для дистанционного управления.

   По умолчанию центральная панель становится домашней страницей сервера, отображающей представление Features (Компоненты).

2. Дважды щелкните на значке Management Service (Служба управления) в разделе Management (Управление).

Завершив настройку всех конфигурационных параметров, запустите WMSVC, как вы бы делали это с любой другой службой. Для удобства, когда диспетчер IIS нацелен на службу Management Service, в панели Actions (Действия) отображается гиперссылка Start (Запустить). Как только служба WMSVC начала функционировать на сервере IIS, консоль диспетчера IIS можно подключить к этому серверу IIS с помощью следующих шагов.

1. Запустите диспетчер IIS на удаленном компьютере.
2. На странице приветствия диспетчера IIS щелкните на гиперссылке Connect to a server (Подключиться к серверу) в разделе Connection tasks (Задачи подключения).
3. Укажите имя сервера IIS, к которому хотите подключиться.
4. Предоставьте учетные данные для подключения.

Остерегайтесь слишком большого количества подключений

Разрешение слишком большого числа одновременных подключений к WMSVC является верным способом обеспечить конфликты при администрировании. Позаботьтесь о том, чтобы к службе WMSVC подключались только машины определенных администраторов, и должным образом обучите этих администраторов.

Подключение, безопасность и ведение журнала

В общей схеме обеспечения защиты веб-сайта важную роль в обеспечении сохранности информационного содержимого играют многие факторы.

- Первым и наиболее очевидным фактором являются разрешения посетителей, пока они находятся на сайте.
- Вдобавок существуют параметры шифрования, защищающие данные во время их транспортировки, и службы, которые помогают уберечь IIS-сервер от перегрузки и возникновения аварийных ситуаций.
- Кроме того, предусмотрено ведение журнала событий на тот случай, когда вам понадобится знать о каждом посещении сайтов.
- Наконец, не следует забывать о необходимости создания резервных копий конфигурации и содержимого сайтов, которые могут пригодиться на случай, если произойдет авария.

В IIS 8.0 имеется ряд параметров аутентификации и трассировки сбойных запросов, которые помогают администраторам упреждать потребности пользователей. В Windows Server 2012 с помощью диспетчера системных ресурсов Windows (Windows System Resource Manager — WSRM) можно управлять потреблением ресурсов со стороны сервера IIS. Делегирование компонентов ограничивает повышенные привилегии для конфигурации сайтов, в то время как пользовательские разрешения регламентируют доступ к их содержимому.

Аутентификация

На веб-сайте IIS 8 доступно несколько возможных механизмов аутентификации. В табл. 19.4 кратко описаны отличия между методами аутентификации.

Обдумайте выбор метода аутентификации для своего сайта. Если вы выберете метод аутентификации, не обеспечивающий достаточной степени защиты, то на сайт могут проникнуть нежелательные посетители. Выбор излишне строгого метода аутентификации может попросту отпугнуть законных посетителей.

Разрешения

Вы можете воспользоваться страницей Permissions (Разрешения) диспетчера IIS, чтобы выдать объектам пользователей диспетчера, учетным записям пользователей Windows или объектам групп Windows разрешение на подключение к сайту или приложению в целях управления им. Имейте в виду, что только компоненты, которые были делегированы ("разблокированы") на уровне сервера, будут доступны держателям разрешений для администрирования на уровне сайта (рис. 19.28).

Таблица 19.4. Методы аутентификации

Метод аутентификации	Назначение
Аутентификация с помощью клиентских сертификатов AD (AD Client Certificate Authentication)	Отображает пользователей AD на клиентские сертификаты
Анонимная аутентификация (Anonymous Authentication)	Посетитель не обязан предоставлять учетные данные
Аутентификация с помощью заимствования полномочий ASP.NET (ASP.NET Impersonate Authentication)	Запускает приложения ASP.NET под альтернативным контекстом безопасности (вместо применения стандартной учетной записи ASP.NET)
Базовая аутентификация (Basic Authentication)	Посетитель должен указать имя пользователя и пароль (передаваемый простым текстом)
Аутентификация с помощью дайджеста (Digest Authentication)	Посетитель должен указать имя пользователя AD и пароль (требуется браузер, воспринимающий HTTP 1.1); пароль не передается
Аутентификация с помощью форм (Forms Authentication)	Перенаправление клиентской стороны прозрачным образом переносит пользователя на HTML-форму, в которой он вводит учетные данные, и затем прозрачно перемещает пользователя обратно на запрошенную страницу
Аутентификация Windows (Windows Authentication)	Диспетчер NTLM или протокол Kerberos проверяет подлинность пользователя Windows по его имени и паролю

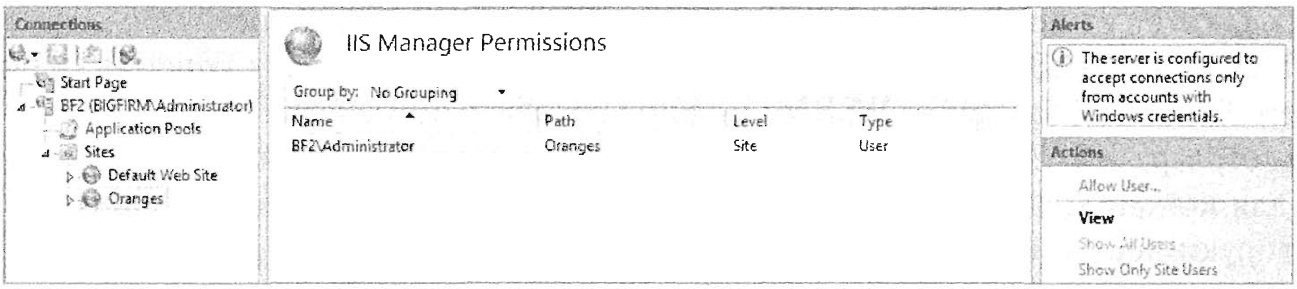


Рис. 19.28. Страница Permissions диспетчера IIS

Разрешение на доступ к сайту в целях просмотра или выгрузки вращается вокруг виртуальных каталогов приложений этого сайта. Вы можете управлять структурой разрешений отдельно взятого виртуального каталога с помощью следующих шагов.

1. Запустите диспетчер IIS и раскройте узел сервера IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите нужный сайт.

   По умолчанию центральная панель становится домашней страницей сайта, отображающей представление Features (Компоненты).
3. Щелкните на ссылке View Virtual Directories (Показать виртуальные каталоги) в панели Actions (Действия).
4. Выделите (с помощью обычного щелчка) выбранный виртуальный каталог и щелкните на гиперссылке Edit Permissions (Редактировать разрешения) в панели Actions.

5. Установите разрешения на вкладке Security (Безопасность) диалогового окна Properties (Свойства) для виртуального каталога.

Чтобы указать делегируемые компоненты и уровень делегирования, можно использовать либо PowerShell, либо диспетчер IIS. Для делегирования компонента с помощью диспетчера IIS выполните описанные ниже действия.

1. Запустите диспетчер IIS и раскройте узел сервера IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите нужный сайт.

   По умолчанию центральная панель становится домашней страницей сайта, отображающей представление Features (Компоненты).
3. Дважды щелкните на значке Feature Delegation (Делегирование компонентов) в области Management (Управление).
4. Щелкните на компоненте, подлежащем делегированию, и затем на гиперссылке в панели Actions (Действия), которая обозначает выбранный уровень делегирования (Read Only (Только чтение), Read/Write (Чтение/Запись), Reset to Inherited (Сбросить к унаследованным)).

Помните, что делегирование компонента на уровне сервера делает возможным изменение конфигурационных параметров этого компонента на любом или всех веб-сайтах внутри сервера, которые задействуют делегируемый компонент (в зависимости от разрешений `web.config` индивидуального сайта). Это может подвергать опасности некоторые сайты, так что применяйте делегирование в масштабах всего сервера с большой осторожностью. Ниже перечислены командлеты PowerShell, предназначенные для установки, удаления и отображения делегируемых компонентов:

```
Add-WebConfigurationLock
Remove-WebConfigurationLock
Get-ConfigurationLock
```

Безопасность доступа кода

Уровни доверия .NET можно сконфигурировать так, чтобы регламентировать определенный уровень доступа к базовому содержимому, который будут иметь приложения .NET на сайте. Уровни доверия .NET можно редактировать в диспетчере IIS, щелкнув на значке .NET Trust Level (Уровни доверия .NET), или же внести изменения непосредственно в файл `web.config`. Редактирование уровня полномочий кода .NET приведет к генерации записи в файле `web.config` соответствующего сайта. В табл. 19.5 перечислены возможные параметры для уровней доверия .NET и указано, что они обеспечивают.

Вызов SSL

Защита с помощью протокола SSL используется для многих поколений продукта IIS. К настоящему времени вы наверняка уяснили, что SSL применяется для защиты данных, которые передаются в и из сервера IIS. Чтобы инициировать SSL на веб-сайте IIS 8, вы должны сначала создать на сайте привязку HTTPS.

Таблица 19.5. Уровни доверия .NET

Уровень доверия	Назначение
Полный (внутренний)	Доступ ко всем ресурсам согласно параметрам безопасности ОС
Высокий (`web_hightrust.config`)	Не позволяет обращаться к коду или службам, записывать в журнал событий или получать доступ к MSMQ, ODBC, OleDb
Средний (`web_midtrust.config`)	Ограничения высокого уровня доверия плюс невозможность доступа к файлам за пределами иерархии каталогов приложения, обращение к реестру или выполнение вызовов сетевых служб и веб-служб
Низкий (`web_lowtrust.config`)	Ограничения высокого и среднего уровней плюс невозможность записи в файловую систему и невозможность вызова метода `Assert()`
Минимальный (`web_minimaltrust.config`)	По умолчанию только разрешения на выполнение

Чтобы добавить привязки к сайту, выполните следующие шаги.

1. Запустите диспетчер IIS и раскройте требуемый сервер IIS в панели Connections (Подключения).
2. Раскройте папку Sites (Сайты) и выделите сайт, требующий SSL.
3. В панели Actions (Действия) щелкните на ссылке Bindings (Привязки).
4. В открывшемся диалоговом окне Site Bindings (Привязки сайта) щелкните на кнопке Add (Добавить).
5. Измените тип привязки с HTTP на HTTPS и укажите сертификат, который должен использоваться.

Теперь, когда протокол SSL привязан к веб-сайту, вы можете провести точную настройку поведения SSL, дважды щелкнув на значке SSL Settings (Параметры SSL) на домашней странице этого сайта. Выберите нужное количество битов и укажите, обязательны ли сертификаты клиентской стороны.

Ведение журнала

Предыдущие версии ведения журнала IIS были ограниченными. В них предлагался фиксированный набор стандартных полей, и отсутствовал способ его расширения или настройки. К тому же не хватало возможности создания специального модуля для ведения журнала. С выходом версии IIS 8.5 ситуация изменилась. Чтобы расширить или настроить параметры ведения журнала IIS, выполните описанные ниже действия.

1. Запустите диспетчер IIS, выберите интересующий сайт или сервер в панели Connections (Подключения) и дважды щелкните на компоненте Logging (Ведение журнала).

   В дополнение к опции, применяемой по умолчанию, доступны семь стандартных опций ведения журнала.

2. В раскрывающемся списке Format (Формат) выберите W3C и щелкните на кнопке Select Fields (Выбрать поля).
3. В открывшемся диалоговом окне W3C Logging Fields (Поля журнала W3C) щелкните на кнопке Add Field (Добавить поле).
4. В поле Field Name (Имя поля) диалогового окна Add Custom Field (Добавление специального поля) введите имя специального поля внутри журнального файла.

   Имя поля не может содержать пробелы.
5. В раскрывающемся списке Source Type (Тип источника) можно выбрать один из следующих вариантов: Request Header (Заголовок запроса), Response Header (Заголовок ответа) или Server Variable (Серверная переменная).
6. В раскрывающемся списке Source (Источник) выберите имя HTTP-заголовка или серверной переменной, которая содержит значение, предназначенное для записи в журнал, или введите собственную исходную строку.
7. Щелкните на кнопке OK.
8. Щелкните на кнопке Apply (Применить) в панели Actions (Действия), чтобы применить новые параметры.

К имени нового журнального файла добавляется префикс `_x`, показывая, что этот файл содержит специальные поля. Полезно отметить, что общий объем данных, собранных со всех специальных полей, не может превышать 64 Кбайт, иначе IIS будет усекать данные.

Резервное копирование и восстановление данных

Никакое обсуждение IIS 8 не может считаться исчерпывающим без упоминания о восстановлении после аварий. В конце концов, никто не в состоянии предугадать, когда произойдет отказ системы или разрушение данных, но лучше иметь план на случай такой неизбежной ситуации. К счастью, архитектура сервера IIS 8 упрощает его резервное копирование. Мы уже рассматривали вопрос получения снимков сайтов для переноса; те же самые снимки можно использовать для восстановления сайта к его предыдущей версии. Кроме того, конфигурационные файлы XML находятся в файловой системе NTFS и, как таковые, нуждаются в резервном копировании только в рамках стратегии регулярного резервного копирования для подсистемы ввода-вывода. Следует подчеркнуть, что резервная копия состояния системы содержит лишь метабазу, но не конфигурационные файлы.

Таким образом, если речь идет только о резервном копировании файлов конфигурации и содержимого, то имеется ли какая-то особенность в резервном копировании IIS 8? Особенность одна — команды PowerShell, которые можно применять для создания, восстановления, удаления и вывода списка резервных копий.

- Чтобы сгенерировать резервную копию, выполните следующую команду:

  ```
  Backup-WebConfiguration -Name {имя_резервной_копии}
  ```

- Чтобы провести восстановление из резервной копии, выполните следующую команду:

  ```
  Restore-WebConfiguration -Name {имя_резервной_копии}
  ```

- Чтобы удалить (очистить) резервную копию, выполните следующую команду:

```
Remove-WebConfigurationBackup {имя_резервной_копии}
```

- Чтобы получить список резервных копий, выполните следующую команду:

```
Get-WebConfigurationBackup
```

Эти команды PowerShell могут быть помещены в сценарий и запланированы на выполнение по графику с помощью ОС. Но что, если в ОС возникнут какие-то проблемы, из-за чего администратор не будет знать о том, что в течение нескольких недель не удается получить достоверные резервные копии файла `applicationhost.config`? Не стоит переживать, т.к. в IIS ведется хронология конфигурации `applicationhost.config` в соответствии со стандартным графиком, находящимся в файле `%windir%\system32\inetsrv\config\schema\iis_schema.xml`. Эти автоматические резервные копии появятся в результатах выполнения команды `Get-WebConfigurationBackup` наряду с файлами резервных копий, сгенерированными вручную, и могут использоваться для восстановления с помощью команды `Restore-WebConfiguration`.

По умолчанию IIS 8 сохраняет автоматически генерируемые хронологические версии файла `applicationhost.config` в подкаталоге хронологии внутри `%systemdrive%\inetpub`. Это может быть не самым безопасным местом для таких важных файлов. Чтобы перенаправить будущие хронологические резервные копии `applicationhost.config` в другое место, например, в `D:\MyHistFiles`, выполните следующую команду PowerShell:

```
Set-WebConfigurationProperty -Filter //System.ApplicationHost/ConfigHistory
   -Name Path -Value "D:\MyHistFiles"
```

Резюме

Запланируйте использование IIS 8.5 и установите эту службу. Относительно экономный по умолчанию, сервер IIS 8.5 должен быть тщательно спланирован, чтобы не устанавливать большее количество модулей, чем в действительности необходимо. Даже если не принимать во внимание вопрос экономии ресурсов, устранение неиспользуемых служб ролей из сервера является также методом защиты веб-сайтов. Как всегда у Microsoft, существует несколько способов установки IIS 8.5, начиная с графического пользовательского интерфейса и заканчивая PowerShell.

> *Контрольный вопрос.* Вы собираетесь установить IIS 8.5 в системе Windows Server 2012 R2, из которой удален графический пользовательский интерфейс. Вы хотите установить только стандартные роли, а также роль ASP.NET и все, что она требует. Какая команда PowerShell нужна для этого?

Управляйте стандартными глобальными параметрами IIS 8. Модули IIS 8 — это лишь одно из свидетельств блочной структуры продукта. Веб-приложения и индивидуальные параметры конфигурации для каждого сайта также могут управляться независимым образом. Иерархическая структура глобальных параметров, веб-параметров, параметров приложений и параметров страниц допускает возможность детализированного администрирования несколькими специалистами.

Контрольный вопрос. Что такое делегирование компонентов?

Создавайте и защищайте веб-сайты в IIS 8. Проектирование и генерацию новых веб-сайтов в IIS 8 можно выполнять посредством графического пользовательского интерфейса или командной строки, что позволяет автоматизировать рутинную процедуру создания сайтов. Чтобы упростить выдачу разрешений, структуру разрешений можно копировать с одного сайта на другой или управлять ею на более высоких уровнях иерархии параметров. Задача генерации сайтов в IIS 8 облегчена за счет возможности пакетирования веб-сайта.

> *Контрольный вопрос.* Вам необходимо создать новый веб-сайт, который обладает всеми характеристиками Default Web Site, но должен также поддерживать страницы ASP.NET. Вы не хотите добавлять к Default Web Site поддержку ASP.NET, поскольку опасаетесь увеличить уязвимость существующего веб-содержимого. Как вы поступите на практике?

Управляйте IIS 8 с помощью расширенных приемов администрирования. Повседневное обслуживание сайтов и отправка содержимого могут отнимать основное время при администрировании IIS 8. Однако именно дополнительное высокоуровневое управление обеспечивает согласованное и бесперебойное обслуживание ваших веб-страниц. Важные задачи конфигурирования, в числе которых восстановление после сбоев, мониторинг производительности, настройка безопасности доступа кода и определение шифрования, могут выполняться либо локально, либо дистанционно.

> *Контрольный вопрос.* Из-за ограниченного пространства в хранилище вы пересматриваете план аварийного восстановления системы. Вы обдумываете возможность запаздывания резервного копирования файла `applicationhost.config` вплоть до месяца. Тем не менее, вас беспокоит, что небольшие изменения глобальной конфигурации, вносимые на протяжении месяца, могут быть утеряны, если сбой случится до момента создания ежемесячной резервной копии. Как бы вы восстанавливали изменение, сделанное в середине месяца?

Глава 20

Расширенный протокол IP: маршрутизация в Windows

Зачем маршрутизировать из среды Windows? Коротко ответить можно следующим образом: потому что такая возможность существует, и это откроет вам глаза на мир, которого вы ранее не замечали.

Более десятилетия тому назад маршрутизаторы были дорогостоящими устройствами, а компании, специалисты которых знали толк в сетях, зачастую использовали ненужные PC в качестве дешевых маршрутизаторов. Например, вставив в ПК пару сетевых карт и установив ОС Linux, инженер по сетям мог сэкономить своей компании немалые деньги на покупке внушительной груды металла у какого-то крупного поставщика сетевого оборудования. Даже в наше время в Интернете можно обнаружить оборудование подобного рода: оно до сих пор эксплуатируется у некоторых поставщиков услуг Интернета.

Маршрутизация является жизненно важной составляющей в поддержке любой сетевой инфраструктуры (только подумайте о том, сколько в вашей сети виртуальных локальных сетей, и каким образом трафик маршрутизируется между ними). Чтобы корректно управлять сетью и хостами в ней, важно понимать работу маршрутизации. Обычно это находится за пределами контроля администратора сервера, однако базовые знания о маршрутизации также помогут находить и устранять возникающие время от времени проблемы с подключениями на хостах и в сети.

В этой главе вы ознакомитесь с жизненным циклом IP-пакета в процессе его маршрутизации по сети, и узнаете об отличиях между маршрутизацией с учетом классов и маршрутизацией без учета классов (хотя это относительно старые концепции, анализ отличий между ними, несомненно, будет полезным). Мы объясним, как устройства трансляции сетевых адресов (network address translation — NAT) позволяют маршрутизировать TCP-трафик, а в ходе краткого исторического обзора покажем, каким образом появление Winsock способствовало наступлению бума Интернет.

Вы ознакомитесь с процессами установки роли Remote Access (Удаленный доступ) и узнаете, как конфигурировать маршрутизатор с NAT. (В следующей главе мы

еще возвратимся к роли Remote Access.) Мы расскажем о том, как конфигурировать компьютер с Windows Server 2012 R2 для маршрутизации IP-трафика, и обсудим туннелирование. Наконец, вы научитесь применять знания, полученные в этой главе, и ряд инструментов для устранения сложностей с сетевыми коммуникациями.

В этой главе вы изучите следующие темы:

- документирование жизненного цикла IP-пакета, маршрутизируемого по сети;
- объяснение точек зрения на IP-маршрутизацию с учетом классов и без учета классов;
- использование устройств NAT для маршрутизации TCP-трафика.

Жизненный цикл IP-пакета

Проектировщики первоначальной версии протокола Интернета (Internet Protocol) не просто добились поставленной перед ними цели: они создали то, что позволило достичь цели предельно простыми средствами. В результате вы заметите, что мы не собираемся рассказывать о том, как маршрутизировать UDP или TCP, поскольку обо всем этом позаботится протокол IP. Мы также не будем объяснять, каким образом выполнять маршрутизацию в сети Ethernet, т.к. Ethernet не маршрутизируется: коммуникации происходят в рамках одной подсети.

Но это означает, что для понимания маршрутизации в TCP/IP вы должны иметь представление о механизме движения IP-пакета через систему. С этой целью мы опишем жизненный цикл типового IP-пакета с применением модели сети, показанной на рис. 20.1.

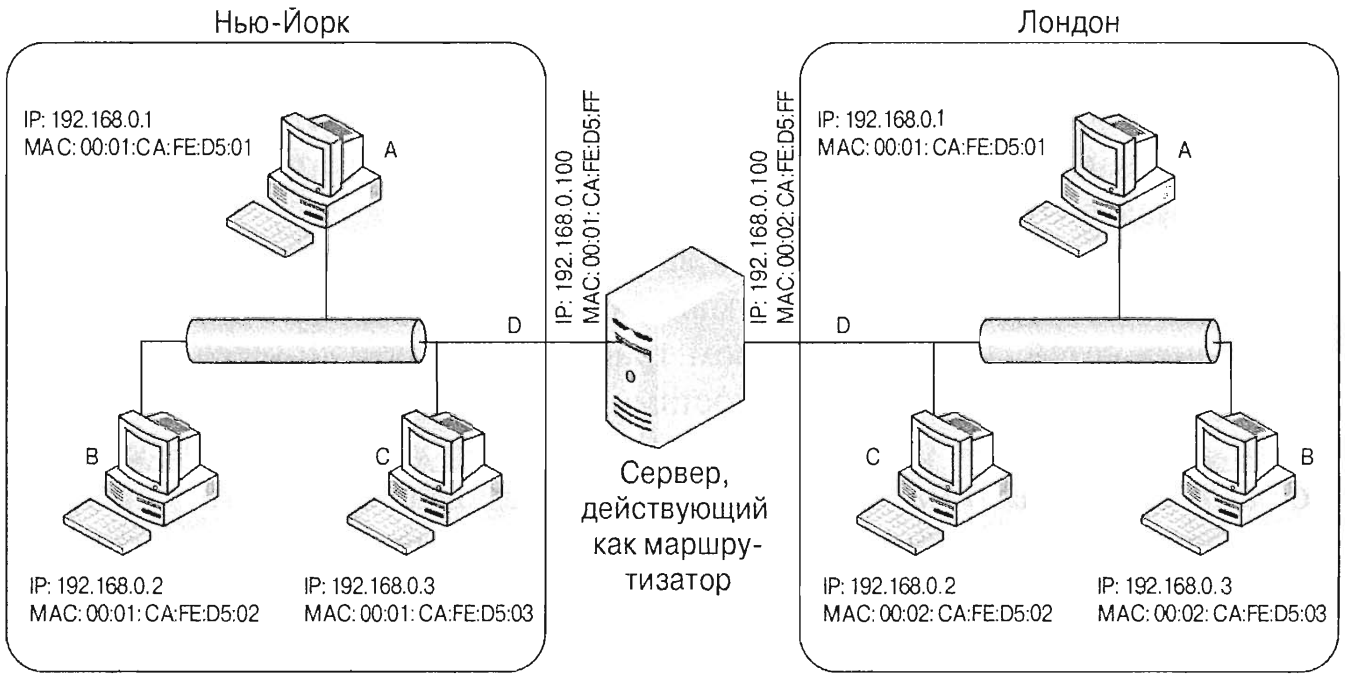


Рис. 20.1. Пример сети

В примере с жизненным циклом IP-пакетов в настоящем разделе мы будем использовать диаграмму сети, представленную на рис. 20.1 (предполагается, что маской подсети является 255.255.255.0, или /24, т.е. класс C).

Краткое повторение

Прежде чем погружаться в детали маршрутизации в Windows, мы начнем с краткого повторения того, что вы должны знать о протоколе TCP/IP, чтобы успешно усвоить материал данной главы.

- **IP-адреса идентифицируют индивидуальные интерфейсы.** Каждый активный интерфейс на TCP/IP-хосте (будь это ПК либо устройство вроде маршрутизатора или брандмауэра) владеет одним или несколькими IP-адресами; эти IP-адреса представляют собой 32-битовые числа для IPv4 и 128-битовые числа для IPv6. Адреса IPv4 обычно записываются с помощью десятично-точечной записи — четыре числа от 0 до 255, разделенные точками, например, 198.162.1.234. Адреса IPv6 группируются в виде шестнадцатеричных цифр. Каждая группа представляет 16 битов, а группы разделяются двоеточиями, например, 2001:db8::12af:d4f2:1cab:1002. (Два следующие подряд двоеточия представляют строку нулей, которая для краткости удаляется. В данном случае :: эквивалентно 0:0.)
- **В своей основе IP является ненадежным протоколом.** Он не прикладывает никаких усилий для гарантирования доставки или сообщения о том, что данные не удалось доставить по назначению.
- **UDP — ненадежный протокол, построенный поверх IP.** Этот протокол добавляет к IP концепцию портов — по одному для получателя и отправителя.
- **TCP — надежный протокол, построенный поверх IP.** За исключением размера адресов, нет никакой разницы между TCP поверх IPv6 и TCP поверх IPv4. Протокол TCP добавляет к IP следующие концепции: *порты* для получателя и отправителя, *подключение*, которое продолжается с момента начального приветствия до конца жизненного цикла, протокол *квитирования* (установления связи) для открытия и аккуратного закрытия подключения, упорядочивание для обеспечения правильного следования байтов в потоке подключения, а также способ разрыва подключения, когда на одном из концов обнаруживается состояние ошибки.

Простейший случай: маршрутизация не требуется

Простейший случай относится к ситуации, когда два компьютера, которые желают взаимодействовать друг с другом, находятся внутри одного сегмента Ethernet. Давайте возьмем сайт "Нью-Йорк" и начнем коммуникацию компьютера A (IP-адрес 192.168.0.1, MAC-адрес 00:01:CA:FE:05:01) с компьютером C (IP-адрес 192.168.0.3, MAC-адрес 00:01:CA:FE:05:03). Процедура описана ниже.

1. Приложение, или сетевой уровень, отправляет IP-пакет на уровень IP.
2. Уровень IP компьютера A просматривает заголовок на предмет IP-адреса получателя.
3. Уровень IP компьютера A находит MAC-адрес компьютера B с применением ARP (IPv4) или ND (IPv6).
4. Уровень IP компьютера A создает Ethernet-пакет и отправляет его.
5. Ethernet-карта компьютера C распознает этот адрес, читает пакет и пересылает его на уровень IP.
6. Уровень IP компьютера C просматривает заголовок и передает полезную нагрузку обработчику протокола.

К этому списку шагов мы будем возвращаться позже при поиске и устранении проблем с подключаемостью, но сейчас он нуждается в некоторых пояснениях.

Если бы IP-пакет имел *родителей*, то они были бы IP-адресами отправителя и получателя. Каждый IP-пакет должен знать, откуда он начинает свое движение и куда направляется. (Вообразите себе ситуацию, когда вы садитесь в автомобиль, и не знаете конечного пункта назначения.) В IPv4 пакету также требуется имя на тот случай, если какой-то промежуточный маршрутизатор разделит пакет на части. В таком случае получателю будет известно, какие части необходимо объединить вместе, чтобы восстановить пакет.

Наконец, ему нужна информация, которая сообщает получателю о том, каким образом трактовать данные этого пакета (т.е. полезную нагрузку), должен ли он передаваться стеку UDP или TCP либо, возможно, другому протоколу с аббревиатурами, подобными ICMP, IGMP, GRE и т.д. Для IP ими являются протоколы 1, 2, 47 и т.д. Большую часть времени вам не придется беспокоиться об этом, но при желании с помощью инструментов вроде Wireshark или Network Monitor можно заглянуть внутрь IP-пакета и просмотреть всю эту информацию.

При создании пакета вся информация — а также, возможно, дополнительные части — помещается в *IP-заголовок*, после чего этот заголовок и полезная нагрузка передаются на уровень IP сетевого стека для дальнейшей пересылки.

Уровень IP на любом компьютере или маршрутизаторе читает адреса отправителя и получателя и применяет их для определения, куда следует отправить пакет. В этом простейшем случае адреса отправителя и получателя находятся в одной и той же подсети, или локальном звене. В такой ситуации маршрутизация для пакета не требуется.

Уровень IP на компьютере-отправителе должен сообщить сетевому уровню (в большинстве случаев это будет драйвер Ethernet) о необходимости помещения пакета в правильную сетевую карту с подходящими сетевыми адресами получателя и отправителя, и чтобы сделать это, он должен знать Ethernet-адрес (MAC-адрес), соответствующий каждому IP-адресу.

На рис. 20.1 видно, что MAC-адресом для отправителя должен быть 00:01:CA:FE:D5:01, а MAC-адресом для получателя — 00:01:CA:FE:D5:03, но компьютер-отправитель не располагает такой диаграммой, и поскольку раньше он ни разу не общался с компьютером C, он не имеет представления о его MAC-адресе. Ему известно только то, что пакет должен проследовать по IP-адресу 192.168.0.3.

Примеры MAC-адресов

Обратите внимание, что выбранные нами примеры адресов являются гипотетическими. Адрес MAC (Media Access Control — управление доступом к среде передачи данных) — это глобально уникальный идентификатор, который выражен в форме длинной строки шестнадцатеричных цифр, обычно разделенных попарно дефисами. Как правило, пулы MAC-адресов выдаются поставщикам оборудования Институтом инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers — IEEE).

IPv4: протокол ARP

Именно здесь в игру вступает протокол распознавания адресов (Address Resolution Protocol — ARP), представляющий собой Ethernet-ретрансляцию. Формально все Ethernet-пакеты ретранслируются по всей подсети, но большинство из них сопровождаются MAC-адресом получателя и отсеиваются при приеме другими Ethernet-картами. Широковещательный Ethernet-пакет предназначен для принятия любой Ethernet-картой.

Пакет ARP содержит исходный MAC-адрес инициатора запроса и отыскиваемый IP-адрес. Каждая Ethernet-карта в данном сегменте получит этот запрос и должна будет передать его на свой уровень IP. Уровень IP проверит, принадлежит ли ему запрашиваемый IP-адрес. Затем интерфейс, который владеет данным IP-адресом, ответит утвердительно на запрос ARP с помощью одноадресного ответа, который идентифицирует сам интерфейс как владельца запрашиваемого IP-адреса.

Инициатор запроса принимает этот ответ и добавляет в свою *таблицу ARP* ассоциацию между этим IP-адресом и Ethernet-адресом. Просмотреть таблицу ARP в Windows можно в любой момент, используя один из многих методов. Простейший из них предусматривает запуск команды `arp -a`, которая отображает адреса, назначенные сетевым картам (рис. 20.2).

```
C:\Users\johm>arp -a

Interface: 192.168.1.2 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           cc-5d-4e-b7-f8-90     dynamic
  192.168.1.3           18-a9-05-db-a8-0a     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.12            01-00-5e-00-00-0c     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\johm>
```

Рис. 20.2. Отображение таблицы ARP

Как и большинство сведений о сети, отобразить эту таблицу можно также с помощью команды `netsh interface ipv4 show neighbors` (рис. 20.3).

В этом примере уровень IP на компьютере A создаст пакет, который гласит: "Я являюсь пакетом запроса ARP из машины с IP-адресом 192.168.0.1 и хочу знать MAC-адрес для интерфейса с IP-адресом 192.168.0.3". Затем компьютер A распространит это сообщение по всему нью-йоркскому сегменту, большая часть которого прекратит выполняемые в данный момент действия, проверит свой IP-адрес, чтобы выяснить, не является ли он 192.168.0.3, и только один компьютер (компьютер C) отправит обратно компьютеру A ответ следующего вида: "Я являюсь пакетом ARP ответа с машины с IP-адресом 192.168.0.3, а мой MAC-адрес выглядит как 00:01:CA:FE:D5:03".

Временами вы должны очищать устаревшую запись из таблицы ARP; это делается посредством команды `arp -d inet_addr` (где `inet_addr` — это IP-адрес, который вы хотите удалить из таблицы ARP), позволяющей повторить широковещательную рассылку. Чтобы ознакомиться с параметрами команды `arp`, укажите переключатель для получения справки: `arp -?`.

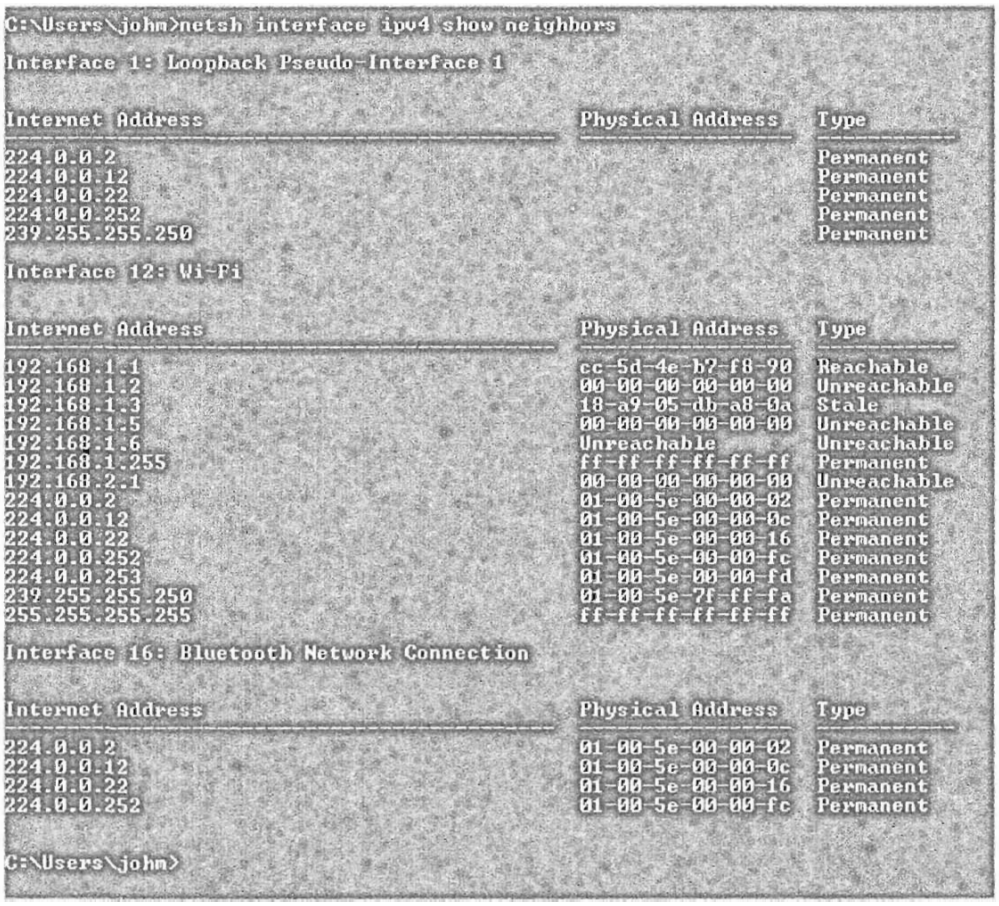


Рис. 20.3. Использование команды `netsh` для отображения таблицы соседей

IPv6: протокол Neighbor Discovery

В IPv4 уровень IP каждого компьютера внутри подсети должен приостанавливать свои действия для проверки входящих запросов ARP. Если вы можете представить себе, до какой степени раздражает необходимость прекращать свою работу каждый раз, когда кто-то звонит *любому* сотруднику компании, то вам нетрудно будет ощутить ситуацию, в которой постоянно пребывают хосты IPv4. Сейчас остроту этой проблемы помогают несколько смягчить коммутаторы, но если данному вопросу не уделять должного внимания, то сеть может по-прежнему подвергаться воздействию шквальных широковещательных рассылок, способных парализовать ее работу.

Разработчики IPv6 отказались от концепции протоколов на основе широковещательных рассылок, вместо которых теперь применяются протоколы групповой передачи. То же самое относится к протоколу обнаружения соседей (Neighbor Discovery — ND), который (среди прочего) берет на себя выполнение процесса распознавания адресов, за что ранее отвечал протокол ARP, не поддерживаемый в IPv6.

Поступая более разумно, уровень IPv6 будет брать последние 24 бита запрашиваемого IP-адреса и строить групповой адрес, известный как *групповой адрес запрашиваемого узла*, путем помещения этих 24 битов в X битов заполнителя внутри адреса получателя FF02:0:0:0:1:FFXX:XXXX. По этому адресу отправляется сообщение ходатайства соседа (Neighbor Solicitation). Поскольку для этих последних 24 битов существует свыше 16 миллионов разных вариантов, можно практически с полной уверенностью утверждать, что это групповое сообщение прервет работу только той Ethernet-карты и интерфейса, которые владеют данным IP-адресом.

Возвращаемое обратно сообщение объявления соседа (Neighbor Advertisement) говорит инициатору запроса о том, что MAC-адрес соответствует запрашиваемому IP-адресу; как и в ARP, это запоминается в специальной таблице, которая всегда проверяется при отправке IP-пакета, чтобы предотвратить повторение запросов одного и того же сообщения Neighbor Solicitation.

Можно ли воспользоваться командой `arp`, чтобы вывести таблицу соседей для IPv6? Нельзя, потому что протокол ARP предназначен исключительно для IPv4. Чтобы отобразить таблицу соседей, которая используется для вашего уровня IPv6, выполните команду `netsh interface ipv6 show neighbors`; пример такой таблицы для подключения по локальной сети (Local Area Connection) представлен на рис. 20.4.

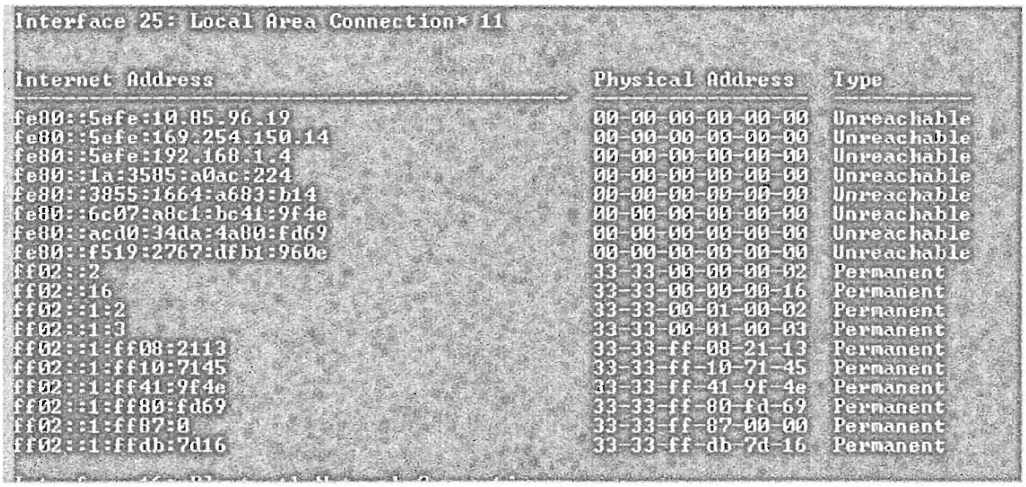


Рис. 20.4. Отображение таблицы соседей для IPv6

Наконец-то можно отправить пакет!

Теперь, когда вы знаете, с кем пытаетесь общаться, интерфейс компьютера A можно, наконец, отправить данные, построив Ethernet-пакет, полезной нагрузкой которого является IP-пакет (заголовок IP и полезная нагрузка IP), а заголовок содержит адреса отправителя и получателя, длину и тип протокола (в данном случае IP). Затем этот пакет передается Ethernet-карте, которая отправляет его дальше.

Кое-что об Ethernet

Известно ли вам, что невзирая на ненадежность протокола IP и его способность терять пакеты данных в силу множества причин, Ethernet сам по себе является надежным протоколом? Действительно, Ethernet использует электрические характеристики кабеля, принимающего участие в его функционировании, для отслеживания возможной путаницы между пакетом, который пытается передать Ethernet, и любым другим пакетом, передаваемым в то же самое время по тому же кабелю. Если выяснилось, что путаница имела место, Ethernet приостанавливает свою работу на случайно выбранный промежуток времени и повторяет попытку.

Сложный случай: с маршрутизацией

На самом деле этот случай не особенно сложен: дело в том, что из-за стремления максимально облегчить усвоение материала главы мы разнесли две части маршрутизации пакетов по разным разделам.

Каждый хост является в какой-то мере маршрутизатором

Каждый компьютер с IP-адресом является частично хостом и частично маршрутизатором. Он не может ретранслировать пакеты, полученные от других хостов, как это обычно делают маршрутизаторы, но ему почти наверняка приходится хранить таблицу маршрутов, исходящих из его собственных интерфейсов, к остальному миру — точно так же, как это делает маршрутизатор.

Как и в случае с таблицей ARP, вы всегда можете ознакомиться с содержимым этой таблицы, хотя обычно люди не горят желанием заниматься ее исследованием. Как и с таблицей ARP, можно применять две команды.

- **`route print`**. Эта команда давно используется как давний резервный инструмент для маршрутизации. В ней предусмотрен только один параметр `print`, который позволяет отобразить список интерфейсов и их MAC-адресов, за которым следует список маршрутов IPv4 и затем список маршрутов IPv6. Если вам нужны лишь маршруты IPv4, введите команду `route -4 print`, а если маршруты IPv6 — команду `route -6 print`.
- **`netsh`**. Команда `netsh` предназначена для работы со всеми конфигурационными параметрами и представлениями, которые имеют отношение к сети и могут появиться в будущем. Команда для отображения таблицы маршрутизации выглядит так: `netsh interface ipv4 show route` или `netsh interface ipv6 show route`.

Все команды отображают ту же самую таблицу маршрутизации, но информация и способ ее представления варьируются. Команда `route print` отображает таблицу маршрутизации, в большей степени базирующуюся на классах и знакомую многим пользователям. К концу этой главы вы должны чувствовать себя уверенно при анализе вывода, подобного представленному на рис. 20.5, который отображает пример таблицы маршрутизации IPv4.

Две команды `netsh interface ipv`*X* `show route` дают несколько более компактный вывод; если вас не интересует таблица индексов интерфейсов, то этот формат может подойти больше.

В обоих выводах `netsh` сетевые получатели представлены в более новом формате CIDR (Classless Inter-Domain Routing — междоменная маршрутизация без учета классов), который мы подробно опишем чуть позже. На рис. 20.6 показана таблица маршрутизации IPv4, а на рис. 20.7 — таблица маршрутизации IPv6. Между ними практически нет отличий, если не считать формата и размера префикса.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.1    192.168.1.4     25
        127.0.0.0        255.0.0.0         On-link     127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link     127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link     127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link     192.168.1.4    281
      192.168.1.4  255.255.255.255         On-link     192.168.1.4    281
    192.168.1.255  255.255.255.255         On-link     192.168.1.4    281
        224.0.0.0        240.0.0.0         On-link     127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.4    281
  255.255.255.255  255.255.255.255         On-link     127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.4    281
===========================================================================
Persistent Routes:
  None
```

Рис. 20.5. Отображение таблицы маршрутизации IPv4 с помощью команды `route print`

```
C:\Users\john>netsh interface ipv4 show route

Publish  Type      Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ---  ------------------------  ---  ------------------------
No       Manual    0    0.0.0.0/0                 12   192.168.1.1
No       System    256  127.0.0.0/8               1    Loopback Pseudo-Interface
1
No       System    256  127.0.0.1/32              1    Loopback Pseudo-Interface
1
No       System    256  127.255.255.255/32        1    Loopback Pseudo-Interface
1
No       System    256  192.168.1.0/24            12   Wi-Fi
No       System    256  192.168.1.2/32            12   Wi-Fi
No       System    256  192.168.1.255/32          12   Wi-Fi
No       System    256  224.0.0.0/4               1    Loopback Pseudo-Interface
1
No       System    256  224.0.0.0/4               16   Bluetooth Network Connect
ion
No       System    256  224.0.0.0/4               12   Wi-Fi
No       System    256  255.255.255.255/32        1    Loopback Pseudo-Interface
1
No       System    256  255.255.255.255/32        16   Bluetooth Network Connect
ion
No       System    256  255.255.255.255/32        12   Wi-Fi

C:\Users\john>
```

Рис. 20.6. Использование команды `netsh` для отображения таблицы маршрутизации IPv4

```
C:\Users\john>netsh interface ipv6 show route

Publish  Type      Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ---  ------------------------  ---  ------------------------
No       System    256  ::1/128                   1    Loopback Pseudo-Interface
1
No       Manual    256  2001::/32                 15   Teredo Tunneling Pseudo-I
nterface
No       System    256  2001:0:5ef5:7f48:304f:cde3:a683:b14/128   15   Teredo Tun
neling Pseudo-Interface
No       Manual    256  2001:4898::/33            28   fe80::f17b:d662:3e2:316c
No       Manual    256  2001:4898:8000::/33       28   fe80::f17b:d662:3e2:316c
No       Manual    256  2001:4898:dc05::/48       28   fe80::f17b:d662:3e2:316c
No       Manual    256  2a01:110::/33             28   fe80::f17b:d662:3e2:316c
No       Manual    256  2a01:110:8000::/33        28   fe80::f17b:d662:3e2:316c
No       Manual    256  2a01:110:8008:4005::/64   28   IPHTTPSInterface
No       System    256  2a01:110:8008:4005:3534:106f:a04c:cde8/128   28   IPHTTPS
Interface
No       System    256  2a01:110:8008:4005:403f:6e25:ce27:2cfd/128   28   IPHTTPS
Interface
No       Manual    256  fdda:dada:dada::/48       28   IPHTTPSInterface
No       Manual    256  fdda:dada:dada:dada::/96  28   fe80::f17b:d662:3e2:316c
No       System    256  fe80::/64                 16   Bluetooth Network Connect
ion
No       System    256  fe80::/64                 12   Wi-Fi
No       System    256  fe80::/64                 15   Teredo Tunneling Pseudo-I
nterface
No       System    256  fe80::/64                 28   IPHTTPSInterface
No       System    256  fe80::5efe:192.168.1.2/128   31   isatap.{51280017-DB4B-4
802-8458-5787828FEF72}
No       System    256  fe80::304f:cde3:a683:b14/128   15   Teredo Tunneling Pseu
do-Interface
No       System    256  fe80::3534:106f:a04c:cde8/128   28   IPHTTPSInterface
No       System    256  fe80::3962:9eb9:7d85:ae29/128   16   Bluetooth Network Co
nnection
No       System    256  fe80::5c25:fff7:db60:817a/128   12   Wi-Fi
No       System    256  ff00::/8                  1    Loopback Pseudo-Interface
1
No       System    256  ff00::/8                  15   Teredo Tunneling Pseudo-I
nterface
No       System    256  ff00::/8                  16   Bluetooth Network Connect
ion
No       System    256  ff00::/8                  12   Wi-Fi
No       System    256  ff00::/8                  28   IPHTTPSInterface

C:\Users\john>
```

Рис. 20.7. Использование команды `netsh` для отображения таблицы маршрутизации IPv6

Как видите, здесь присутствует немало данных, затрудняющих понимание.

Давайте выберем один из двух выводов и проанализируем его. Поскольку пользователи еще не успели привыкнуть к такому формату, остановимся на выводе команды `netsh`. Он содержит шесть столбцов: `Publish`, `Type`, `Met`, `Prefix`, `Idx` и `Gateway/Interface Name`. Ниже приведено описание каждого из этих столбцов.

- **`Publish`** (Публиковать). Указывает, отправляется ли эта запись таблицы маршрутизации другим компьютерам в объявлениях маршрутизатора. На машине, которая не действует как маршрутизатор, здесь будет находиться `No` (Нет) — только маршрутизаторы должны отправлять объявления о том, что они являются маршрутизаторами.

- **Type** (Тип). Здесь должно присутствовать Manual (Вручную) для маршрутов, которые были добавлены статически вручную или приложениями, либо System (Система) для маршрутов, добавленных автоматически уровнем IP. В любых наших таблицах маршрутизации мы видим вариант System.
- **Met** (Метрика). Это аббревиатура, означающая *metric* (метрика). Метрика представляет собой произвольное число, которое отражает относительную стоимость использования данного маршрута по сравнению с другим маршрутом, который приведет к тому же получателю. Когда несколько маршрутов удовлетворяют одному и тому же критерию получателя, всегда выбирается маршрут с самой низкой метрикой. Вскоре мы обсудим это более подробно.
- **Prefix** (Префикс). Это префикс сети, который будет сопоставляться с адресом получателя, чтобы найти кратчайший совпадающий префикс.
- **Idx** (Индекс). Это еще одна аббревиатура, которая означает *interface index* (индекс интерфейса). Индекс представляет собой число, отражающее интерфейс, на который ссылается данная запись маршрута для исходящего трафика. Индекс интерфейса часто можно использовать в командах netsh, чтобы указать интерфейс без упоминания его имени.
- **Gateway/Interface Name** (Имя шлюза/интерфейса). Для маршрутов, содержащих префиксы сети получателя за пределами локальной подсети, этот столбец содержит адрес в локальной подсети маршрутизатора, который может принимать пакеты и пересылать их дальше. Для маршрутов, сеть получателя которых относится к локальной подсети, в этом столбце описано имя интерфейса, на котором находится данная локальная подсеть.

Использование таблицы маршрутизации

Когда приложение собирает IP-пакет и отправляет его уровню IP, адрес его получателя сравнивается с адресом связи локальной подсети и маской каждого сетевого интерфейса, чтобы выяснить, является ли адрес получателя локальным. Вы уже видели, что происходит, если этот адрес действительно оказывается локальным: производится обращение к таблице ARP или ND и при необходимости эта таблица обновляется, а сам пакет помещается в подходящую сетевую интерфейсную плату для передачи требуемому получателю.

Если же адрес не является локальным, очевидно, вы должны отправить пакет через маршрутизатор. Вы найдете маршрутизатор, на который следует отправить пакет, и будете действовать так, как если бы MAC-адрес этого маршрутизатора в действительности был MAC-адресом, возвращенным запросом ARP по IP-адресу получателя. Вообще говоря, в некоторых довольно необычных средах маршрутизаторы сконфигурированы именно на такое действие — отвечать каждому запросу ARP, как если бы данный маршрутизатор на самом деле был искомым хостом. Однако это является признаком некорректно функционирующей сети, поэтому в дальнейшем его обсуждении нет смысла.

Как найти правильный маршрут в таблице маршрутизации? Существуют три простых критерия.

- *Сеть назначения для записи таблицы маршрутизации должна как можно точнее совпадать с адресом получателя пакета.*

В реальном мире это было бы аналогично ситуации, когда два курьера предлагают доставить ваш пакет по назначению, но вы отказываете тому из них, кто говорит: "Я могу доставить ваш пакет любому жителю Англии", и отдаете предпочтение курьеру, заявляющему: "Я могу доставить ваш пакет любому жителю города Хэдфилд в Англии" — второй курьер доставит пакет гораздо быстрее, т.к. сам является местным жителем.

- *Если имеются две возможных записи маршрутизации, из них выбирается та, которая имеет меньшую метрику.*

  Метрики представляют собой довольно-таки произвольные числа, и их единственное назначение — действовать в качестве схемы разрешения конфликтов на этапе поиска наиболее подходящего маршрута в таблице маршрутизации. Все, что требуется — это гарантировать, что маршруты к одному и тому же получателю можно отсортировать по метрике, чтобы отразить предпочтение проектировщика сети относительно того, какой маршрутизатор должен быть опробован первым.

- *Если в таблице маршрутизации по-прежнему остается несколько подходящих записей, то выбирается первая в списке.*

  Обратите внимание, что выбором "первой в списке" записи достаточно трудно в точности управлять. В результате вы должны тщательно выбирать подходящие метрики, чтобы иметь возможность всегда предсказывать, какой маршрут будет выбран.

Как упоминалось ранее, после выбора записи маршрутизации произойдет отправка IP-пакета маршрутизатору, который указан в этой записи в качестве шлюза. Разумеется, это означает, что уровень IP должен применять ARP для определения, какой MAC-адрес соответствует данному IP-адресу такого маршрутизатора. Обратите внимание, что IP-адрес получателя в IP-пакете, который в конечном итоге передается этому маршрутизатору, представляет собой IP-адрес исходного получателя, а не маршрутизатора.

Давайте снова пересмотрим пример сети, показанный на рис. 20.8.

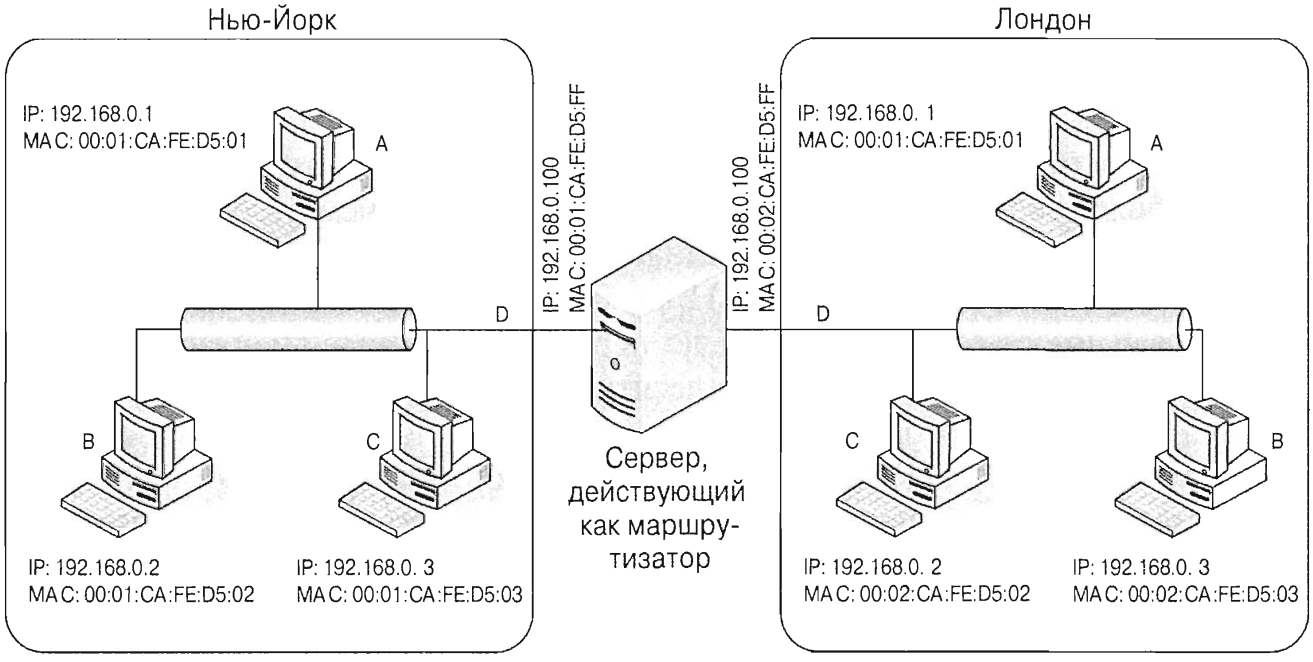


Рис. 20.8. Пример сети

Теперь вы видите, что IP-адреса машин, расположенных в Лондоне и Нью-Йорке, находятся в разных подсетях. Давайте задумаемся на минуту над тем, как хост из Нью-Йорка общался бы с хостом, находящимся в Лондоне, или каким образом он бы отправлял IP-пакет на этот лондонский хост. Чтобы определить это, вы должны иметь представление о масках сети.

От маршрутизации с учетом классов к маршрутизации без учета классов

Мы осознанно выбрали версию `netsh` таблицы маршрутизации, т.к. она использует более современный формат CIDR, в отличие от старого формата `netmask`, который был представлен как вывод команды `route print` на рис. 20.5.

Когда бы вы ни работали с сетями, вы будете встречать тех, кто знаком с новым форматом, и тех, кому известен старый формат; следовательно, лучше изучить оба формата, что также позволит вам выступать в роли толкователя между этими двумя группами. Приведенное ниже описание, возможно, не является совершенно точным с исторической точки зрения, но оно точное логически и поможет вам понять, почему Интернет стал таким, каким мы его видим в наши дни.

Вначале был класс

В ранние времена Интернета доступное адресное пространство казалось необъятным, а адреса раздавались пусть и не так щедро, как конфеты по праздникам, но все же не настолько скупо, как это происходит теперь. Пользователи Интернета были категоризированы по разным классам, и вместе с ними получали разные классы диапазонов адресов, соответствующие этим классам.

Классы именовались от A до C и различались между собой количеством битов, отведенных под сетевой адрес, и количеством битов, выделенных для адреса хоста. Располагая только 32 битами под IP-адрес, назначение класса A предполагало применение 8 битов для обозначения сетевого адреса (маска подсети 255.0.0.0), а оставшиеся 24 бита обозначали адрес хоста. Назначение класса B означало использование 16 битов для сетевого адреса (маска подсети 255.255.0.0) и 16 битов для адреса хоста. Наконец, назначение класса C предусматривало применение первых 24 битов для сетевого адреса (маска подсети 255.255.255.0) и оставшихся 8 битов для адреса хоста.

Классы идентифицируются путем чтения двоичной формы для выяснения, сколько наиболее значащих битов установлено в 1, прежде чем будет достигнут первый бит, равный 0. Адреса класса A начинаются с 0, поэтому первый октет находится в диапазоне от 0000 0000 до 0111 1111 (от 0 до 127 в десятичном представлении). Адрес класса B имеет единственную 1 до первого 0, поэтому диапазоном будет от 1000 0000 до 1011 1111 (от 128 до 191 в десятичном представлении). Адрес класса C начинается с двух 1, за которыми следует его первый 0, поэтому диапазоном является от 1100 0000 до 1101 1111 (от 192 до 223 в десятичном представлении).

Все это выглядит совершенно справедливым: пользователям класса A предоставлялась возможность иметь около 2^{24} (16 777 216) хостов, пользователи класса B получали в свое распоряжение примерно 2^{16} (65 536) хостов, а каждому пользователю класса C было доступно до 256 хостов.

Неиспользуемые адреса хостов

Почему было указано "около" или "примерно"? В каждом сетевом диапазоне определенное количество адресов недоступно для назначения хостам. Единственно абсолютные, "высеченные в камне" (или, во всяком случае, зафиксированные в документах RFC, которые являются эквивалентом каменных плиток в Интернете) требования заключаются в том, что в любой сети верхние и нижние границы диапазонов адресов являются зарезервированными.

Верхняя граница диапазона адресов — когда все биты хоста установлены в 1 (*адрес, состоящий из всех единиц*) — резервируется для направленной широковещательной передачи. Таким образом, например, если сети назначен класс B, а адреса начинаются с последовательности 192.168.*что-то.что-то*, то адрес направленной широковещательной передачи будет выглядеть как 192.168.255.255, где два октета 255 представляют двоичную последовательность 1111.1111, т.е. все единицы.

Пакет, отправленный по этому адресу, достиг бы каждого компьютера в сети 192.168.*что-то.что-то*. Каждый компьютер передал бы это сообщение на собственный уровень IP, где какое-то оборудование может прослушивать такой широковещательный трафик. (Вы встретите упоминания сети 192.168.*что-то.что-то* в разнообразной документации, и ниже мы посвятим несколько абзацев объяснению, почему так случилось.) Не пытайтесь опробовать это в своей производственной сети, поскольку вы очень легко утопите свою сеть в данных!

Нижняя граница адресного диапазона — когда все биты хоста установлены в 0 (*адрес, состоящий из всех нулей*) — формально резервируется для широковещательной передачи. Но минуточку, ведь только что было сказано, что адрес, состоящий из всех единиц, был зарезервирован для широковещательной передачи, не так ли? Да, это действительно так — и на сегодняшний день вы не найдете ни одной системы, которая бы применяла для широковещательной передачи все нули. Однако давным-давно, в "бронзовый век" Интернета, разработки в Интернет проводились сразу многими группами. По-видимому, широковещательная передача была изобретена одновременно несколькими компаниями. В компании Sun решили выполнять ее посредством всех нулей, а остальные выбрали для этого все единицы. К немалому удивлению Sun (в то время эта компания была основной движущей силой развития Интернета), победителями оказались остальные.

Но адрес, состоящий из всех нулей, не стал доступным для использования, т.к. он представляет еще и концепцию "адреса сети". В таблицах маршрутизации, а также в диаграммах сетей и другой документации адрес сети ссылается на сеть как единое целое, поэтому вместо того чтобы говорить о сети 192.168.*что-то.что-то*, сейчас можно вести речь о сети 192.168.0.0.

Концепция адресации Интернета в IPv4 сводится к тому, что адреса, состоящие из всех единиц, и адреса, состоящие из всех нулей, т.е. 255.255.255.255 и 0.0.0.0, что-то представляют. Адрес 192.168.0.0 теперь представляет сеть машин от 192.168.0.1 до 192.168.255.254, а что тогда представляет 0.0.0.0? Вообще говоря, он представляет сеть, состоящую из одного компьютера — "этого" компьютера. По аналогии адрес 255.255.255.255 представляет "широковещательную передачу на каждый из компьютеров в сети".

Сужение широковещательной передачи: первые немаршрутизируемые адреса

Когда сеть Интернет была невелика, упомянутые выше адреса широковещательной передачи были замечательными. Если вы хотели знать, какие компьютеры компании подключены к Интернету, то все, что нужно было сделать — выяснить, что их сетевым адресом является 192.168.0.0, а это означало, что вы могли определить количество компьютеров в сети компании, пропинговав адрес 192.168.255.255. Вы получили бы ответ от каждой машины компании (вы и сейчас можете поступать так, но будьте аккуратны). Затем вы могли бы попробовать подключиться к произвольно выбранным машинам и выяснить, какие из них представляют интерес.

Аналогично, если вы хотели определить количество компьютеров во всем Интернете, это также не составляло проблемы: вам просто нужно было воспользоваться командой `ping 255.255.255.255` и вы получили бы ответ от каждой существующей машины.

Поскольку каждое из этих действий связано с собственными рисками — во-первых, есть риск обнаружить себя и, во-вторых, риск наводнить свою сеть (или чью-то сеть, если бы вам удалось направить ответы на их адрес направленной широковещательной передачи) — то довольно скоро маршрутизаторы стали конфигурировать на запрет попадания в сеть пакетов с такими адресами получателя.

В результате адрес 192.168.255.255 теперь может применяться только изнутри сети 192.168.0.0; таким образом, передача по этому адресу стала направленной широковещательной передачей, которую вы можете направить только на самого себя, а передача по адресу 255.255.255.255 стала глобальной широковещательной передачей, которая могла бы достичь лишь машин на вашей стороне маршрутизатора. По существу это означало, что обе широковещательных передачи достигали одного и того же места — вашей локальной подсети — и поскольку адрес направленной широковещательной передачи 192.168.255.255 требовал вычисления, но адрес 255.255.255.255 можно было бы жестко закодировать, практически никто больше не использует форму направленной широковещательной передачи. К сожалению, это вовсе не означает, что вы можете заполучить этот адрес обратно и выдать его какому-то хосту.

Маршрутизация немаршрутизируемого, часть I: частные адреса

В документе, который определяет адреса, состоящие из всех нулей, и адреса, состоящие из всех единиц (RFC 1122, "Requirements for Internet Hosts — Communication Layers" ("Требования к хостам Интернета — уровни коммуникации")), также определен специальный адрес класса A как зарезервированный для целей коммуникации с *петлей обратной связи*. Это сеть 127.0.0.0, но из этого 16-миллионного диапазона адресов почти никто никогда не использует что-либо помимо единственного адреса 127.0.0.1, которому обычно присваивается псевдоним *localhost* (локальный хост).

Удобным соглашением, выработанным за прошедшие годы, является применение первого или последнего адреса в сети в качестве местоположения для стандартного маршрутизатора. Следует отметить, что это только соглашение, и ничто не заставляет вас поступать именно так, а не иначе (кстати, в нашем примере маршрутиза-

тор не следует этому соглашению: ему назначен адрес 192.168.0.100 для Нью-Йорка и адрес 192.169.0.100 для Лондона). Тем не менее, следование этому соглашению упростит поиск маршрутизатора тому, кто будет вас замещать. В качестве примера можно привести сеть 192.168.0.0: следуя указанному соглашению о первом адресе, для адреса стандартного маршрутизатора вы использовали бы 192.168.0.1.

Снова рассмотрим в качестве примера сеть 192.168.0.0. По какой причине мы продолжаем пользоваться этой сетью? Все объясняется просто: владельцы не обвинят нас в том, что мы случайно направили трафик по их маршруту. А почему мы уверены в этом? Дело в том, что этот адрес не является собственностью какого-то частного лица. В другом документе RFC (RFC 1918, "Address Allocation for Private Internets" ("Выделение адресов для частных сетей")) указан ряд диапазонов сетей, которые зарезервированы для частного использования. По умолчанию эти адреса не маршрутизируются — открытый маршрутизатор не пропустит дальше IP-пакет, получатель которого находится в следующих диапазонах:

10.0.0.0–10.255.255.255
172.16.0.0–172.31.255.255
192.168.0.0–192.168.255.255

Читатели, свободно оперирующие двоичными числами или хорошо запомнившие диапазоны классов, поймут, что диапазон 172.16.0.0–172.31.255.255 не является сетевым диапазоном, который соответствует какому-либо классу. По действительности он представляет собой *суперсеть* из 16 адресных диапазонов класса B между 172.16.0.0 и 172.16.255.255, а также между 172.31.0.0 и 172.31.255.255. Диапазон 192.168.*.* — это также суперсеть из 256 сетей класса C.

Конечно, если вы находитесь в одной из таких сетей, то обнаружите, что пакеты делают это за пределами маршрутизатора. Что вы можете не понять, так это то, что они делают это посредством трансляции сетевых адресов (NAT), которая изменяет исходный адрес так, чтобы маршрутизатор пропустил этот пакет.

Поначалу устройства NAT исходили из того, что в каждый момент времени к Интернету могло обращаться только определенное количество внутренних пользователей, поэтому устройству NAT назначалось соответствующее количество внешних адресов. При этом каждый раз, когда трафик пользователя нужно было переслать в Интернет, внутренний адрес этого пользователя отображался на свободный открыто маршрутизируемый внешний адрес. Для некоторых организаций это по-прежнему остается способом, посредством которого внутренние системы становятся доступными из внешней сети Интернет.

Определение подсетей и суперсетей

На ранних стадиях проектирования системы классов IP стало понятно, что даже крупная транснациональная корпорация, которая могла бы пожелать выделения адреса класса A, в действительности не располагала бы единственным Ethernet-кабелем, к которому присоединялись бы все 16 миллионов устройств. Поэтому была разработана схема, согласно которой крупную сеть можно было бы разделять на несколько *подсетей*.

Чтобы сделать это, необходимо было заявить, что различия между классами больше не играют настолько важной роли; у каждого хоста было бы собственное

представление о том, сколько битов его адреса определяют "сеть", и сколько битов описывают "данный хост в сети". Из-за того, что это разделяло двоичный адрес на две части не по границе октета, было решено позаимствовать термин из обработки графики — *маска*. В частности, появилось понятие *маска сети*. Маску сети можно представлять как лист бумаги с вырезанными в нем отверстиями (подобно театральной маске). Отверстия позволяют открывать сетевую часть вашего адреса и скрывать часть, относящуюся к хосту, заменяя эти биты нулями.

На рис. 20.9 показан результат применения маски сети 255.252.0.0 к адресу 192.168.143.8. Такая маска сети эквивалентна двоичной строке

1111 1111 1111 1100 0000 0000 0000 0000,

т.е. 14 битов установлены в 1, а 18 битов — в 0.

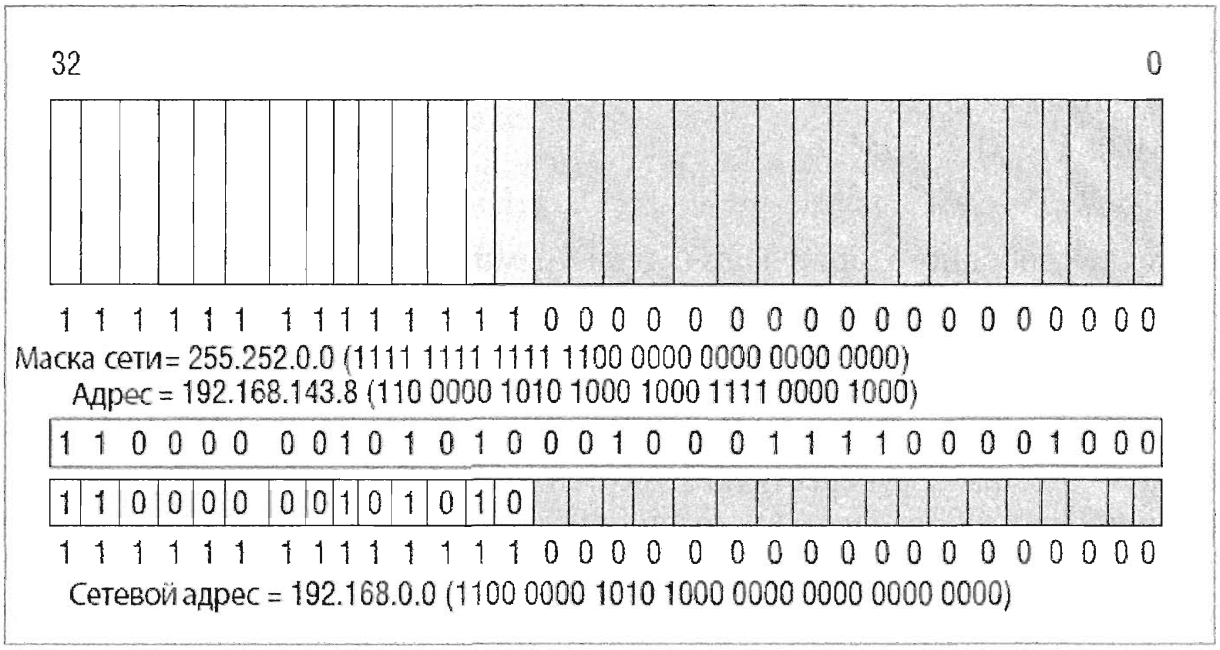


Рис. 20.9. Демонстрация работы маски сети

Адрес 192.168.143.8 является эквивалентом двоичной строки 1100 0000 1010 1000 1000 1111 0000 1000; выстроив эти биты под маской сети, можно увидеть, какие биты следует игнорировать при вычислении сетевого адреса, а какие принимать во внимание:

1111 1111 1111 1100 0000 0000 0000 0000: маска сети

1100 0000 1010 1000 1000 1111 0000 1000: адрес хоста

1100 0000 1010 1000 0000 0000 0000 0000: сетевой адрес

В двоичной математике это равносильно определению маски как числа, имеющего такую же ширину, как и адрес, с 1 в каждом бите части сети и 0 в каждом бите части хоста, после чего к маске и сетевому адресу применяется операция двоичного "И". Операция двоичного "И" сравнивает биты двух операндов, расположенные в соответствующих позициях: если оба бита установлены в 1, то битом результата будет 1; если какой-то из битов или оба установлены в 0, то битом результата будет 0. Вспомните двоичную математику и удостоверьтесь, что полученный результат корректен.

Как вы догадались из заголовка этого раздела, существовали также организации, которые приобрели себе класс C, а впоследствии обнаружили, что нуждаются в более чем 254 адресах. Разумеется, они могли бы приобрести еще один класс C, но если бы удалось заполучить класс C, смежный с уже имеющимся, то появилась бы возможность объединения двух сетей класса C в одну "суперсеть" с $2^9 - 2$ адресами (суммарно 510 адресов). Однако экономия в количестве адресов не была бы самым главным выигрышем: более существенным выигрышем от создания суперсети являются размеры таблиц маршрутизации на пути к этой сети.

Вы увидите эти маски сети в выводе команды `route -4 print`, но вычисление и уяснение того, какое количество битов представляет каждая из них, является настоящей головной болью. В этом случае важно иметь в виду, что в любом октете маски сети может появляться лишь девять значений: 255, 254, 252, 248, 240, 224, 192, 128, 0, т.е. 8, 7, 6, 5, 4, 3, 2, 1 и 0 битов, соответственно. Сложите количество битов в каждом октете — и вы получите общее количество битов в маске сети, в результате определив, сколько битов адреса вашего хоста привязано к этой сети.

Так как любая сеть может быть разделена на подсети в разных местах, маска сети для адреса зависит от того, где именно вы находитесь в этой сети. Например, адрес 10.1.2.3 может быть 3-м хостом в сети 10.1.2.0–10.1.2.255 или 66051-м хостом в сети 10.0.0.0–10.255.255.255.

Еще одной жертвой появления подсетей и суперсетей была направленная широковещательная передача: даже если конкретный маршрутизатор допускал прохождение направленной широковещательной передачи, откуда вам было знать, сколько битов нужно направить на вашу передачу? Это оказалось еще одним препятствием для направленной широковещательной передачи, которая в настоящее время существует лишь как досадная причина к тому, чтобы не использовать в сети адрес, состоящий из всех единиц.

Деление на подсети согласно RFC или в соответствии с реальностью

Многие из вас, возможно, уже сталкивались с диапазоном подсетей, выбранным из значений, которые указаны в документе RFC 1918 (`http://tools.ietf.org/html/rfc1918`). Каждый раз, когда вы подключаете к сети беспроводное устройство в местном кафе, вы получаете адрес из диапазона 10.0.0.0 класса A, который зарезервирован для частных сетей. Однако маской сети не является 255.0.0.0. В общем случае она имеет вид 255.255.255.0, допуская не более 253 устройств (один адрес занят маршрутизатором), которые пользуются беспроводной связью внутри кафе. Где бы вы ни находились, было бы несколько оптимистичным полагать, что указанный предел не будет достигнут.

Этот диапазон 10.* также часто применяется в домашних сетях, настраиваемых программами установки широкополосных систем или теми, кто следует инструкциям по созданию стандартной конфигурации из маршрутизаторов нескольких изготовителей. Если вы используете у себя дома сеть 10.0.0.0–10.0.0.255 с маской сети 255.255.255.0, то формально вы нарушаете положения документа RFC 950, которые гласят, что вы не должны применять подсеть, состоящую из всех нулей или всех единиц. Но не переживайте: Интернет-полиция не постучится к вам в дверь.

Если же вы сдаете экзамен по RFC 950 и RFC 1122, то вам следует исключить из своих расчетов две подсети: подсеть, состоящую из всех нулей, и подсеть, состоящую из всех единиц.

Междоменная маршрутизация без учета классов: сеть Интернет утрачивает свой класс

Как нетрудно заметить из приведенного выше обсуждения, использование адреса подсети, состоящего из всех нулей либо из всех единиц, не представляет серьезной проблемы, а широко распространенное применение суперсетей (которые не содержат в себе части подсети или, возможно, имеют часть подсети с отрицательной длиной) свидетельствует о том, что схема разделения сетевых адресов на классы, присущая Интернету, полностью утратила свою актуальность.

Добавьте к этому малоприятную необходимость вычислять маски сети. Маски сети всегда представляли собой строку из некоторого количества битов, установленных в 1, за которыми следовал ряд битов, установленных в 0, причем общее количество битов равнялось 32, т.е. размеру адреса IPv4. Чтобы сохранить написание сетевых адресов в форме "10.0.0.0–10.0.255.255" или "10.0.0.0 с маской сети 255.255.0.0", администраторы сетей использовали сокращенную систему записи, помещая косую черту после номера сети, а за ней указывая только количество битов, установленных в 1. Таким образом, "10.0.0.0–10.0.255.255" превращается в "10.0.0.0/16". Стандартное назначение адреса 10.0.0.0 как сети класса A с маской сети 255.0.0.0 в таком случае можно было бы описать как "10.0.0.0/8".

Как уже упоминалось, Интернет регулируется документами RFC, и эта новая сокращенная система записи не является исключением. В документе RFC 1519 первоначальное решение определено как междоменная маршрутизация без учета классов (Classless Inter-Domain Routing — CIDR) и данное название сохранилось.

В действительности сокращенная система записи CIDR была перенесена в IPv6; вы увидите, что префиксы сетей IPv6 повсюду в Windows Server 2012 R2 указываются точно в такой же форме.

Маршрутизация TCP: NAPT и PAT

Ранее в этой главе мы указывали, что IP является единственным маршрутизируемым уровнем. Мы говорили также о том, что Ethernet является системой широковещательной передачи, а TCP не нуждается в маршрутизации. Мы должны признаться, что это не совсем так.

Расшифровка таблицы маршрутизации

Есть ли у вас достаточно информации, чтобы прочитать таблицу маршрутизации на рис. 20.6? Давайте взглянем на таблицу маршрутизации компьютера A в Нью-Йорке еще раз.

Читая сверху вниз и не обращая внимания на поля `Publish`, `Met` и `Idx`, мы имеем следующие маршруты.

Записи маршрутизации компьютера A в Нью-Йорке

Префикс	Шлюз/интерфейс	Комментарии
0.0.0.0/0	192.168.1.1	Стандартный маршрут; это означает, что если не обнаруживается более точного соответствия ниже, пакет следует отправлять по IP-адресу 192.168.0.100, или компьютер D в Нью-Йорке. 0.0.0.0/0 — это специальное значение и не должно рассматриваться как что-то иное, чем заполнитель, означающий "по умолчанию"
127.0.0.0/8 127.0.0.1/32 127.255.255.255/32	Петля обратной связи	Даже адрес петли обратной связи должен маршрутизироваться! Первая запись указывает, что вся сеть петли обратной связи может быть достигнута посредством петлевого интерфейса; вторая запись определяет, что специфичный адрес 127.0.0.1 находится на этом интерфейсе; третья запись указывает, что направленные широковещательные передачи для этой сети могут отправляться сюда. Строго говоря, первая запись должна покрывать остальные
192.168.1.0/24 192.168.1.2/32 192.168.1.255/32	Wi-Fi	Это указывает, что любой адрес в Нью-Йорке, даже адрес маршрутизатора, можно достичь посредством интерфейса Local Area Connection (Подключение по локальной сети)
224.0.0.0/4	Петля обратной связи Подключение к сети с помощью Bluetooth Wi-Fi	Эти записи указывают, что групповой трафик может быть отправлен на любой из имеющихся интерфейсов
255.255.255.255/32	Петля обратной связи Wi-Fi Подключение к сети с помощью Bluetooth	Как и прежде, эти записи указывают, что широковещательные передачи данных могут направляться на любой из имеющихся интерфейсов

Нетрудно заметить, что эта таблица отображается в порядке от наименее конкретного маршрута к наиболее конкретному. Можете считать, что маршрутизатор внутри этого компьютера сравнивает получателя в столбце `Prefix` с получателем IP-пакета, рассуждая примерно так, как схематично описано ниже.

"Итак, у меня есть пакет для 192.168.0.2. Куда мне отправить этот пакет? Хорошо, 0.0.0.0/0 совпадает с чем угодно, так что если я не найду ничего другого, победителем станет эта запись. А что можно сказать о следующих нескольких записях? Все они начинаются с 127, и префикс не замаскировал это. Мой адрес получателя не начинается с 127, следовательно, этот вариант не подходит. Подходит 192.168.0.0/24, поскольку мой адрес получателя выглядит как 192.168.0.2, и если я обнулю все после первых 24 бит (а именно так мне следует поступить согласно данному префиксу), я получу 192.168.0.0, что совпадает с сетевым адресом префикса для этой записи. Именно этот совпадающий вариант я выберу вместо имеющегося у меня менее конкретного совпадения. Других совпадений нет, поэтому мне не остается ничего другого, как отправить свой пакет через Local Area Connection".

До тех пор, пока таблица маршрутизации завершена и корректна, компьютер всегда будет следовать описанной процедуре сопоставления префикса с адресом получателя, сначала маскируя этот адрес получателя соответствующим количеством битов в префиксе и всегда отбрасывая менее конкретное совпадение, когда удается найти более конкретное совпадение. Метрика используется лишь как схема для разрешения конфликтов в случае, если две записи имеют одинаковые префиксы, которые обеспечивают максимальное совпадение; в таком случае выбирается запись с самой низкой метрикой.

Заполнение таблицы маршрутизации

Каким образом исправить незавершенную таблицу маршрутизации? И еще: как узнать, что таблица маршрутизации не завершена?

Вы уже видели, что обращение к таблице маршрутизации происходит при поступлении каждого очередного IP-пакета. Поэтому корректная и завершенная таблица маршрутизации должна иметь возможность сообщить правильное место для отправки каждого пакета.

В таблице маршрутизации должен присутствовать, по меньшей мере, один стандартный маршрут с префиксом 0.0.0.0/0 (или ::/0 для маршрутов IPv6); в противном случае появятся пакеты, с которыми непонятно как поступить. Следует помнить, что в таблице маршрутизации может быть более одного стандартного маршрута; в таком случае имеется несколько маршрутизаторов, которые добровольно берут на себя выполнение этой задачи. Вспомните, что победителем оказывается маршрут с самой низкой метрикой.

Кроме того, таблица должна точно знать, как проложить маршрут к каждому адресу получателя, который не ведет к стандартному маршрутизатору. В большинстве домашних сред это не является проблемой. Стандартным маршрутизатором обычно является тот, который подключается к маршрутизатору DSL или кабельному маршрутизатору, и на него можно направлять все.

Однако в производственной среде внутри вашей непосредственной подсети часто предусмотрено несколько маршрутизаторов. Каждый из них ведет к своей части сети. Если перечислить эти маршрутизаторы и сети, к которым они ведут, то получится список, который соответствует всем записям в вашей таблице маршрутизации.

Если окажется, что вам необходимо добавить в свою таблицу маршрутизации какой-то маршрут, это без труда можно сделать из командной строки. Можно воспользоваться двумя базовыми командами: старой командой `route add` и хорошо знакомой командой `netsh`. Предположим, что вы хотите добавить маршрут к префиксу 192.168.0.0/16 с метрикой 100, который ведет к маршрутизатору с адресом 10.0.0.1. Это можно сделать с помощью любой из перечисленных ниже команд.

```
route add 192.168.0.0 mask 255.255.0.0 10.0.0.1 metric 100
route add 192.168.0.0/16 10.0.0.1 metric 100
netsh interface ipv4 add route 192.168.0.0/16 "Local Area Connection" 10.0.0.1
```

Команда `netsh` требует несколько большего объема ввода, чем `route`, даже если вы примените сокращенный способ записи:

```
netsh int ipv4 add ro 192.168.0.0/16 "Local" 10.0.0.1.
```

Аналогично, маршрут можно удалить — правда, если это маршрут, который добавляется автоматически вследствие объявления маршрутизатора, то он вернется следующим образом:

```
route del 192.168.0.0
netsh interface ipv4 delete route 129.0.0.0/8 "Local Area Connection"
```

Замысел первоначального проектного решения, несомненно, заключался в том, что протокол IP должен быть единственной точкой, которая требует маршрутизации, и это являлось исходной целью IP. Каким было первоначальное проектное решение для протокола TCP, что оно не требовало маршрутизации, и как оно изменилось с течением времени?

Почему понадобился TCP: чего не хватает в IP?

Итак, какие же недостатки IP привели к появлению TCP? В протоколе IP отсутствует концепция подключения: если бы нам нужно было выбрать для него аналогию из числа существующих и привычных систем, то это была бы традиционная почтовая служба. Каждый IP-пакет подобен почтовой открытке, которая проходит сквозь систему. Подобно почтовой службе, некоторые IP-пакеты по пути теряются, и если вы отправили два IP-пакета, один вскоре после другого, то они могут поступить в пункт назначения в обратном порядке. В отличие от почтовой службы, некоторые IP-пакеты могут быть доставлены дважды!

Почти как в случае почтовой открытки IP-пакет не может содержать простого сообщения вроде "Пожалуйста, проигнорируйте предыдущее сообщение", т.к. невозможно с полной уверенностью утверждать, что отправитель и получатель сходятся во мнении относительно "предыдущего" сообщения. Учитывая возможность случайного дублирования пакетов, получатель может даже полагать, что ему следует игнорировать само сообщение, предлагающее проигнорировать предыдущее сообщение — в общем, все очень запутанно!

Таким образом, чтобы обеспечить какую-то разновидность коммуникаций, необходимо преодолеть указанные ограничения и разработать такую систему коммуникаций с подключением, которая допускала бы обмен информацией, подобный привычному общению по телефону — начало связи, упорядоченный обмен информацией и конец связи. Именно это и обеспечивает протокол TCP.

Строго говоря, протокол TCP добавляет к IP перечисленные ниже атрибуты.

- **Квитирование** (подтверждение установления связи). Обмен сообщениями типа "Как поживаешь?", "Спасибо, хорошо. А ты как?", "Я тоже хорошо" в TCP известен как трехстороннее квитирование и состоит из очень коротких сообщений вида SYN, SYN/ACK и ACK. Сообщение SYN — это сокращение для "synchronize" ("синхронизировать"), а ACK — для "acknowledgment" ("подтверждение").

- **Упорядочение.** Счетчик отправленных и принятых байтов позволяет гарантировать, что никакие два байта не будут отправлены приложению дважды, а байты, принятые вне последовательности, могут быть переупорядочены. Эти последовательности (по одной на каждой стороне подключения) устанавливаются начальным сообщением SYN и подтверждаются каждым сообщением ACK.

- **Управление потоком.** Интеллектуальная система, которая называется *скользящими окнами*, поддерживает протекание трафика без необходимости в ожидании и без использования слишком большого объема памяти на стороне отправителя или получателя.

- **Индикация ошибок.** Приложение, которое неожиданно закрывается (подобно тому, как мы кладем трубку во время разговора по телефону), может сигнализировать об этом своему партнеру по коммуникациям с помощью пакета сброса (RST (от "reset" — "сброс")).
- **Порты.** Это немного напоминает коммутатор, наличие которого дает вам возможность позвонить в компанию по одному номеру и быть направленным на любой из тысяч дополнительных номеров, чтобы ваш разговор можно было отделить от других разговоров со служащими компании.

Сокеты, порты и Winsock

В действительности практически никто не создает приложения, которые взаимодействуют непосредственно с протоколом IP. Кое-кто по-прежнему разрабатывает приложения, которые напрямую управляют TCP, особенно в среде Windows, потому что разнообразные меры безопасности не разрешают создавать TCP-пакеты любому приложению кроме сетевого стека.

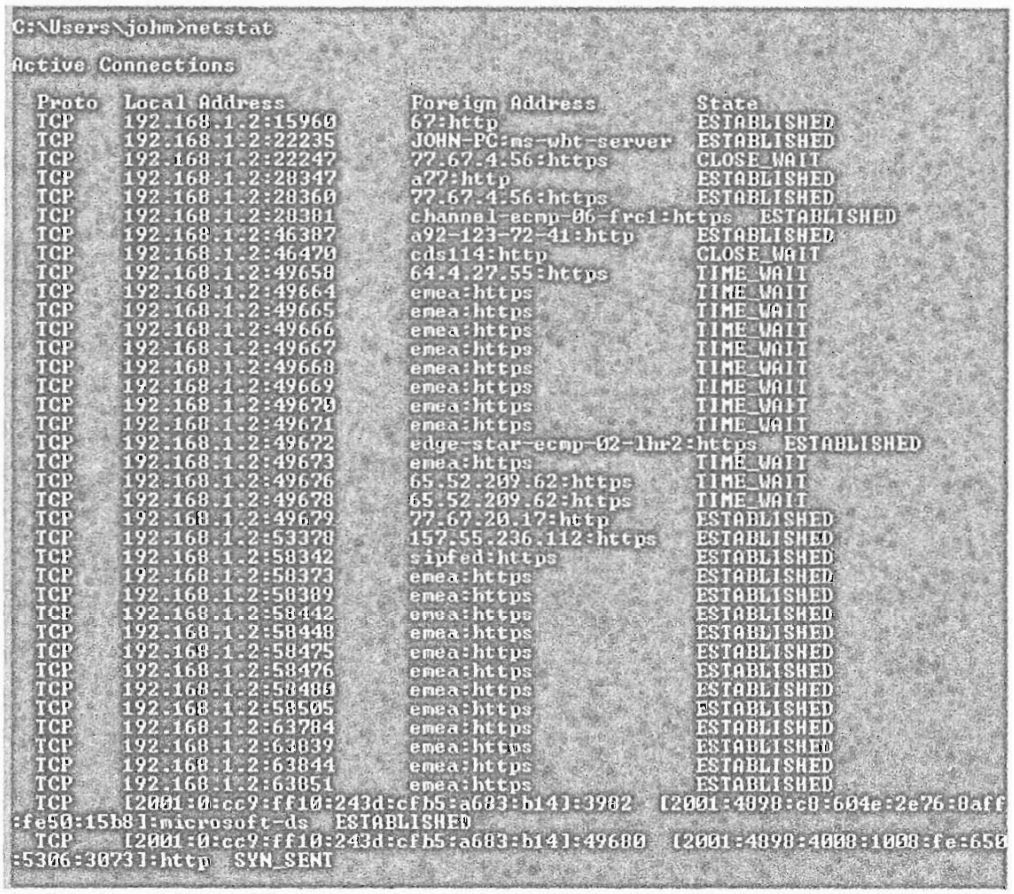
Вместо этого приложения взаимодействуют с уровнем TCP с применением так называемого *сокета*. Сокеты не уникальны для Windows, они существуют буквально с первых дней появления Интернета.

В терминах, принятых в Интернете, сокет состоит из пяти компонентов: адреса отправителя, адреса получателя, порта отправителя, порта получателя и протокола (в данном случае протоколом является TCP). Пара соответствующих друг другу сокетов (когда адрес отправителя и порт одного сокета совпадают с адресом получателя и портом другого сокета и наоборот) образуют подключение TCP. Сокет является *неподключенным*, если его порт и адрес получателя нулевые; сокет является *несвязанным*, если его порт и адрес отправителя нулевые. Несвязанный сокет также является неподключенным.

Хотя вы уже знаете, что собой представляет адрес, мы еще не объяснили, что такое порт. Все довольно просто: порт — это число от 1 до 65 535, выбираемое так, чтобы сокеты можно было отличать друг от друга. Порты ниже 1024 считаются зарезервированными в том смысле, что они могут быть назначены конкретному протоколу. Например, порты 21 и 20 назначены FTP.

Жизненный цикл подключения начинается в одном из двух состояний, что зависит от вида сокета — серверной стороны или клиентской стороны. Сокет серверной стороны начинается в состоянии LISTENING (Прослушивание), что требует привязки сокета к порту и адресу отправителя. Между тем, сокет клиентской стороны начинается в состоянии SYN-SENT (Синхронизирован—отправлен), когда он инициирует квитирование с серверным сокетом. Для этого необходимо, чтобы сокет был привязан и ассоциирован с адресом получателя и портом. Сервер отвечает своим состоянием SYN-ACK (Синхронизирован—подтвержден), создавая новый сокет с таким же портом и адресом получателя, что и у прослушивающего сокета, который переводится в состояние SYN-RECEIVED (Синхронизирован—принят). В завершение квитирования клиент отправляет сообщение ACK и переводит свой сокет в состояние ESTABLISHED (Установлено).

Чтобы получить представление о том, что именно подключается к вашей машине и в каком состоянии оно находится, можно воспользоваться командой `netstat`. На рис. 20.10 показан пример вывода этой команды.



```
C:\Users\john>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.2:15960      67:http                ESTABLISHED
  TCP    192.168.1.2:22235      JOHN-PC:ms-wbt-server  ESTABLISHED
  TCP    192.168.1.2:22247      77.67.4.56:https       CLOSE_WAIT
  TCP    192.168.1.2:28347      a77:http               ESTABLISHED
  TCP    192.168.1.2:28360      77.67.4.56:https       ESTABLISHED
  TCP    192.168.1.2:28381      channel-ecmp-06-frc1:https  ESTABLISHED
  TCP    192.168.1.2:46387      a92-123-72-41:http     ESTABLISHED
  TCP    192.168.1.2:46470      cds114:http            CLOSE_WAIT
  TCP    192.168.1.2:49658      64.4.27.55:https       TIME_WAIT
  TCP    192.168.1.2:49664      emea:https             TIME_WAIT
  TCP    192.168.1.2:49665      emea:https             TIME_WAIT
  TCP    192.168.1.2:49666      emea:https             TIME_WAIT
  TCP    192.168.1.2:49667      emea:https             TIME_WAIT
  TCP    192.168.1.2:49668      emea:https             TIME_WAIT
  TCP    192.168.1.2:49669      emea:https             TIME_WAIT
  TCP    192.168.1.2:49670      emea:https             TIME_WAIT
  TCP    192.168.1.2:49671      emea:https             TIME_WAIT
  TCP    192.168.1.2:49672      edge-star-ecmp-02-lhr2:https  ESTABLISHED
  TCP    192.168.1.2:49673      emea:https             TIME_WAIT
  TCP    192.168.1.2:49676      65.52.209.62:https     TIME_WAIT
  TCP    192.168.1.2:49678      65.52.209.62:https     TIME_WAIT
  TCP    192.168.1.2:49679      77.67.20.17:http       ESTABLISHED
  TCP    192.168.1.2:53378      157.55.236.112:https   ESTABLISHED
  TCP    192.168.1.2:58342      sipfed:https           ESTABLISHED
  TCP    192.168.1.2:58373      emea:https             ESTABLISHED
  TCP    192.168.1.2:58389      emea:https             ESTABLISHED
  TCP    192.168.1.2:58442      emea:https             ESTABLISHED
  TCP    192.168.1.2:58448      emea:https             ESTABLISHED
  TCP    192.168.1.2:58475      emea:https             ESTABLISHED
  TCP    192.168.1.2:58476      emea:https             ESTABLISHED
  TCP    192.168.1.2:58480      emea:https             ESTABLISHED
  TCP    192.168.1.2:58505      emea:https             ESTABLISHED
  TCP    192.168.1.2:63784      emea:https             ESTABLISHED
  TCP    192.168.1.2:63839      emea:https             ESTABLISHED
  TCP    192.168.1.2:63844      emea:https             ESTABLISHED
  TCP    192.168.1.2:63851      emea:https             ESTABLISHED
  TCP    [2001:0:cc9:ff10:243d:cfb5:a683:b141:3982  [2001:4898:c8:604e:2e76:8aff
:fe50:15b8]:microsoft-ds  ESTABLISHED
  TCP    [2001:0:cc9:ff10:243d:cfb5:a683:b141:49680  [2001:4898:4008:1008:fe:650
:5306:3073]:http  SYN_SENT
```

Рис. 20.10. Пример вывода команды `netstat`

Один порт на каждом конце означает два порта

Неправильно заявлять, что подключение к прослушивающему сокету создает подключение на другом порте. Это ошибочное утверждение высказывают многие, кто не понимает, что в данном случае задействовано два порта — по одному на каждой стороне. В качестве примера можно привести подключение к веб-серверу: скажем, клиент с адресом 192.168.1.2 желает подключиться к веб-серверу с адресом 10.20.30.40 и это первое подключение данного клиента с момента, когда он был запущен.

Для описания сокетов мы будем применять ряд сокращений. Каждый сокет будет описываться как {адрес отправителя, порт отправителя, протокол, адрес получателя, порт получателя}. Веб-сервер находится в состоянии LISTENING на порте 80; это означает, что у него есть сокет, привязанный к адресу отправителя 10.20.30.40, порту отправителя 80, протоколу TCP, адресу получателя 0.0.0.0, порту получателя 0 — т.е. {10.20.30.40, 80, TCP, 0.0.0.0, 0}. Клиент создает сокет {192.168.1.2, 1025, TCP, 10.20.30.40, 80}. Что? Откуда взялся 1025? Это первое число после 1024, следовательно, первый порт из незарезервированного диапазона, и оно будет использоваться в качестве номера порта отправителя для первого подключения. Следующее подключение будет исходить из порта 8700. Это число произвольно назначается приложениями и очень редко является последовательным. Считайте это мерой безопасности, усложняющей идентификацию трафика.

Клиент отправляет сообщение SYN на своем сокете, чтобы начать квитирование. Когда сокет LISTENING принимает SYN, уровень TCP создает копию сокета LISTENING и устанавливает порт и адрес получателя в соответствие с входящим

запросом подключения; таким образом, теперь существуют два сокета: {10.20.30.40, 80, TCP, 0.0.0.0, 0} в состоянии LISTENING и {10.20.30.40, 80, TCP, 192.168.1.2, 1025} в состоянии SYN-RECEIVED после отправки SYN-ACK. Этот сокет объединяется в пару с клиентским сокетом {192.168.1.2, 1025, TCP, 10.20.30.40, 80}, чтобы сформировать подключение. Когда клиент принимает SYN-ACK и отправляет в ответ сообщение ACK, оба сокета могут перейти в состояние ESTABLISHED. Таким образом, на сервере был создан новый сокет, но не новый порт.

С этого момента нет смысла называть один сокет сервером, а другой — клиентом: они оба равнозначны. Каждый из них может в любой момент отправлять и принимать данные. Несмотря на то что многие протоколы настаивают на соблюдении строгой синхронизации между командой и откликом, TCP является протоколом асинхронной связи; это означает, что любая сторона может отправлять данные в любой момент времени.

Чтобы аккуратно завершить подключение, одна сторона коммуникаций (назовем ее *инициатором закрытия*) отправит сообщение FIN и переведет свой сокет в состояние FIN-WAIT-1, чтобы указать, что она ожидает подтверждения своего FIN; она также ожидает, что другой конец подключения (назовем его *закрываемой стороной*) закроет сокет посредством FIN. Закрываемая сторона может продолжать отправку данных, однако после получения ею сообщения FIN она уже не будет принимать данные от инициатора закрытия.

В какой-то момент, обычно вскоре после получения FIN, закрываемая сторона отправит сообщение ACK, которое подтверждает FIN. Это заставит закрываемую сторону перейти в состояние CLOSE-WAIT, указывающее на то, что она знает, что уже не будет принимать данные, но все еще ожидает, пока приложение завершит прием данных и закроется. Когда инициатор закрытия примет ACK, он перейдет в состояние FIN-WAIT-2.

Со временем закрываемая сторона завершит отправку данных и отправит сообщение FIN, указывая на то, что приложение на ее конце также завершило работу. После отправки этого FIN закрываемая сторона перейдет в состояние LAST-ACK (она ожидает ACK — последнего ACK — от инициатора закрытия), и когда инициатор закрытия примет данное сообщение FIN, он перейдет в состояние TIME-WAIT и отправит ACK закрываемой стороне.

Получив этот ACK, закрываемая сторона закроет свой сокет, после чего она может забыть об этом подключении. Формально этот сокет находится в состоянии CLOSED (Закрыт). Однако инициатору закрытия приходится в течение примерно четырех минут поддерживать свой сокет в состоянии TIME-WAIT, прежде чем он также сможет перевести свой сокет в состояние CLOSED и забыть о подключении. (Это необходимо для того, чтобы предотвратить выдачу ответов на пакеты, по-прежнему путешествующие по сети, посредством сообщений RST.)

Winsock: почему мы можем пользоваться Интернетом

К счастью, даже разработчикам приложений не придется иметь дело со всеми этими деталями. Там, где есть сетевой стек, там доступен и интерфейс, применяемый для его программирования. Во времена “железного века” Интернета существовало столько разных интерфейсов, или интерфейсов программирования приложений (application programming interface — API), сколько было сетевых стеков. Тогда имелось более десятка сетевых стеков.

Для программистов сетевых приложений это означало либо необходимость в разработке более десятка разных версий своего ПО, либо выбор одного или двух сетевых стеков в надежде, что ставка сделана на правильный вариант. Между тем, нет никакой гарантии, что не появится очередное "убойное приложение", авторы которого выбрали другой сетевой стек — не тот, который был выбран вами.

В 1992 или 1993 году поставщики сетевых стеков поняли, что это сужает их рынок, поскольку никто не занимается разработкой приложений для сетей Windows. Они объединились вместе, назвав это "сотрудничеством конкурентов", и в течение нескольких месяцев разработали общий API-интерфейс, которого собирались придерживаться. Плод совместной разработки был назван Windows Sockets, поскольку он был очень похож на API-интерфейс BSD Sockets, используемый в системах Unix. Вскоре название Windows Sockets трансформировалось в Winsock, т.к. это совпадало с названием библиотеки, с которой компоновались программы, взаимодействующие с сетью.

Случайно или нет, в то же самое время Национальный центр суперкомпьютерных приложений (National Center for Supercomputing Applications — NCSA) выпустил веб-браузер NCSA Mosaic, ставший вскоре чрезвычайно популярным, который был доступен для Windows и других платформ.

Важность Winsock

Возьмем, к примеру, широко распространенную утилиту, которую можно найти в большинстве инструментальных наборов для сетевых администраторов — WFTPD, представляющую собой FTP-сервер, который до сих пор интенсивно применяется и доступен по адресу `http://www.wftpd.com/`. Без Winsock создать этот чрезвычайно популярный инструмент было бы нелегко! Благодаря этой утилите Winsock стал одним из ключевых факторов роста популярности Интернета во всем мире.

Графический веб-браузер от NCSA сыграл важную роль в популяризации Интернета, как это сделало появление America Online (AOL) и последующее использование этой службой API-интерфейса Winsock в качестве основного метода подключения приложений к стеку коммутируемых соединений.

Конечно, в наши дни нельзя говорить о "десятке сетевых стеков" для Windows. Для большинства из нас существует только один сетевой стек, создателем которого является Microsoft. Но он по-прежнему поддерживает Winsock, и разработчики по-прежнему могут писать сетевые программы, которые почти наверняка будут функционировать в любой системе Windows.

Спасибо, Winsock!

Маршрутизация немаршрутизируемого, часть II: NAPT и PAT

Теперь, когда вы знаете практически все о сокетах и портах, мы можем объяснить следующий большой скачок в технологии маршрутизации частных сетей в Интернет. Что касается обычного устройства NAT, то мы продемонстрировали, что у вас может быть столько подключенных извне клиентов, сколько имеется внешних IP-адресов — и это в то время, когда количество доступных IP-адресов неуклонно сокращается.

Таким образом, очередная блестящая идея заключалась в том, чтобы обеспечить возможность применения одного внешнего IP-адреса для нескольких внутренних IP-адресов. Поле зрения маршрутизатора NAT подобного рода должно было простираться за пределы уровня IP, достигая уровня TCP (или UDP); такой маршрутизатор должен использовать IP-адрес и порт для отображения подключений, а не целиком IP-адресов, на внешние подключения.

Такой вид маршрутизатора называется *транслятором сетевых адресов/портов* (network address/port translator — NAPT). Кое-кто может называть его *транслятором портов/адресов* (port/address translator — PAT). Мы предпочитаем применять термин NAPT, частично потому, что именно так этот маршрутизатор упоминается в документах RFC, но главным образом из-за того, что в обозначении NAPT сохранен "сетевой" компонент работы этого маршрутизатора, которым, по нашему мнению, не следует пренебрегать.

Поскольку маршрутизаторы NAPT пользуются гораздо большей популярностью по сравнению с маршрутизаторами NAT и аббревиатуру NAPT несколько труднее произносить, гораздо чаще приходится слышать о маршрутизаторах NAT, хотя речь, как правило, идет именно о маршрутизаторах NAPT. В некоторых производственных средах маршрутизатор NAT по-прежнему применяется в качестве маршрутизатора NAT уровня IP без трансляции портов, но в наши дни к этому следует относиться скорее как к причуде.

Когда на маршрутизатор NAPT поступает сообщение SYN от внутреннего адреса, он назначает этой попытке подключения внешний IP-адрес и порт (обычно с тем же самым номером, что и у внутреннего порта, но в случае конфликтов номер может назначаться случайным образом). Как только маршрутизатор NAPT видит внутренний IP-адрес и порт в IP-пакете, переданном TCP с его внутренней границы, он корректирует этот пакет и вставляет внешний IP-адрес и порт, прежде чем перенаправить этот IP-пакет в Интернет. Аналогично, когда маршрутизатор NAPT видит на своей наружной границе входящий IP-пакет, отправленный TCP, он отыскивает совпадающий внутренний IP-адрес и порт, чтобы выполнить замену, а затем направляет исправленный IP-пакет по соответствующему внутреннему адресу.

Непредвиденные последствия NAPT, часть I: случайный брандмауэр

Для большинства приложений NAPT работает действительно хорошо. Более того, NAPT обеспечивает неожиданные преимущества тем, кто испытывает потребность в устройствах защиты, которые сообщали бы об отказе и по умолчанию запрещали трафик. Каждое устройство NAPT действует как брандмауэр, потому что по умолчанию NAPT не будет известно, куда отправлять любой входящий пакет. Вместо того чтобы выдвигать предположение, NAPT либо отбросит такой пакет, либо выдаст ответ с индикацией отказа, такой как RST.

Большинство устройств NAPT позволяют конфигурировать отображения портов, например, сообщить NAPT о наличии веб-сервера, функционирующего по адресу 192.168.230.21 с портом 80; в этом случае устройство NAPT назначит статическое отображение своего внешнего IP-адреса с портом 80 на свой внутренний адрес 192.168.230.21 с портом 80.

Вы можете также сконфигурировать большинство устройств NAPT на пересылку любого неизвестного трафика по определенному IP-адресу, который иногда называют *хостом DMZ*. Не поддавайтесь искушению поступать так, поскольку это приведет к тому, что этот хост будет подвергаться всем мыслимым сетевым атакам. Интернет ведет себя несколько недружелюбно по отношению к тем, у кого нет брандмауэра.

Непредвиденные последствия NAPT, часть II: уничтожитель приложений

Тем не менее, для некоторых приложений устройства NAPT практически уничтожили протоколы, на которые полагались эти приложения. Есть несколько протоколов, такие как FTP (передача файлов), SIP (инициирование сеанса — для связи, подобной телефонной) и H.323 (для голосовых и видеофонов), которые во время коммуникации отправляют информацию об IP-адресах и портах своим партнерами по подключению. Даже IPSec, защищенный протокол для IP, который обеспечивает возможность аутентификации и шифрования трафика IP, будет временами нуждаться в сообщении своего IP-адреса.

Например, FTP-клиент предложит FTP-серверу соединиться с ним по его адресу 192.168.230.21 на порте 1025 с помощью команды `PORT 192.168.230.21,4,1`. Сервер не может подключиться к этому адресу и порту, т.к. адрес не является маршрутизируемым. Это обычно приводит к тайм-ауту при попытке передачи файла и чрезвычайно затрудняет использование FTP позади брандмауэра.

Маршрутизация немаршрутизируемого, часть III: шлюзы уровня приложений

Разработчики спецификации NAPT (RFC 3022, “Traditional IP Network Address Translator” (“Традиционный транслятор сетевых IP-адресов”)) были осведомлены о существовании подобной проблемы и предложили добавлять к любому маршрутизатору NAPT шлюзы уровня приложений (Application Layer Gateway — ALG).

Такой шлюз ALG должен проверять содержимое полезной нагрузки TCP на предмет распознаваемых протоколов и команд, редактируя сам поток TCP с целью изменения указанных там IP-адресов и номеров портов и открывая отображения, чтобы разрешить запрошенные входящие подключения.

Этот подход работает вполне приемлемо за исключением случая, когда протокол не распознан устройством NAPT как принадлежащий конкретному шлюзу ALG. Причина может быть проста, вроде применения другого порта, или сложна, например, использование шифрования (скажем, IPSec или FTP поверх SSL/TLS). В первом случае NAPT не знает о том, что вы отправляете трафик FTP, т.к. сервер не находится на порте 21; во втором случае устройство NAPT видит только зашифрованные данные, которые не может ни прочитать, ни модифицировать.

Устройства NAPT когда-нибудь утратят актуальность

Протокол IPv6 предлагает нам новую реальность. В IPv6 настолько много адресов, что проблема их исчерпания, которая создает немалые сложности в IPv4, никогда не возникнет.

Да, мы уже говорили об этом в отношении IPv4. Но сейчас хотим подчеркнуть: даже если вы назначите IPv6-адрес каждой травинке на газоне перед домом, то в вашем адресном пространстве IPv6 по-прежнему останется достаточно возможностей, чтобы назначить адреса всем предметам, хранящимся у вас в холодильнике, всем бытовым приборам и всем квадратным сантиметрам площади вашего дома. И даже после этого ваше адресное пространство отнюдь не будет исчерпано.

В результате наличия этого колоссального адресного пространства отпадет потребность в устройствах NAT или NAPT для IPv6. Если же вас интересует функция "случайного брандмауэра" устройств NAPT, то вам понадобится настроить более "предсказуемый" брандмауэр, действующий только как брандмауэр.

Установка NAT

Возможно, наиболее вероятной причиной превращения машины Windows Server 2012 R2 в маршрутизатор является потребность создать устройство NAT, которое обеспечило бы более точный контроль, чем можно получить от обычного устройства NAT. Установка NAT в Windows Server 2012 R2 относительно проста, хотя и предполагает выполнение множества шагов.

1. Установите роль Remote Access.

   Это включает в себя требуемые компоненты маршрутизации.

2. Откройте диспетчер серверов и выберите пункт меню Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты).

   Появится окно хорошо знакомого вам мастера добавления ролей и компонентов (рис. 20.11).

3. Щелкните на кнопке Next (Далее) на экране Before You Begin (Прежде чем начать).

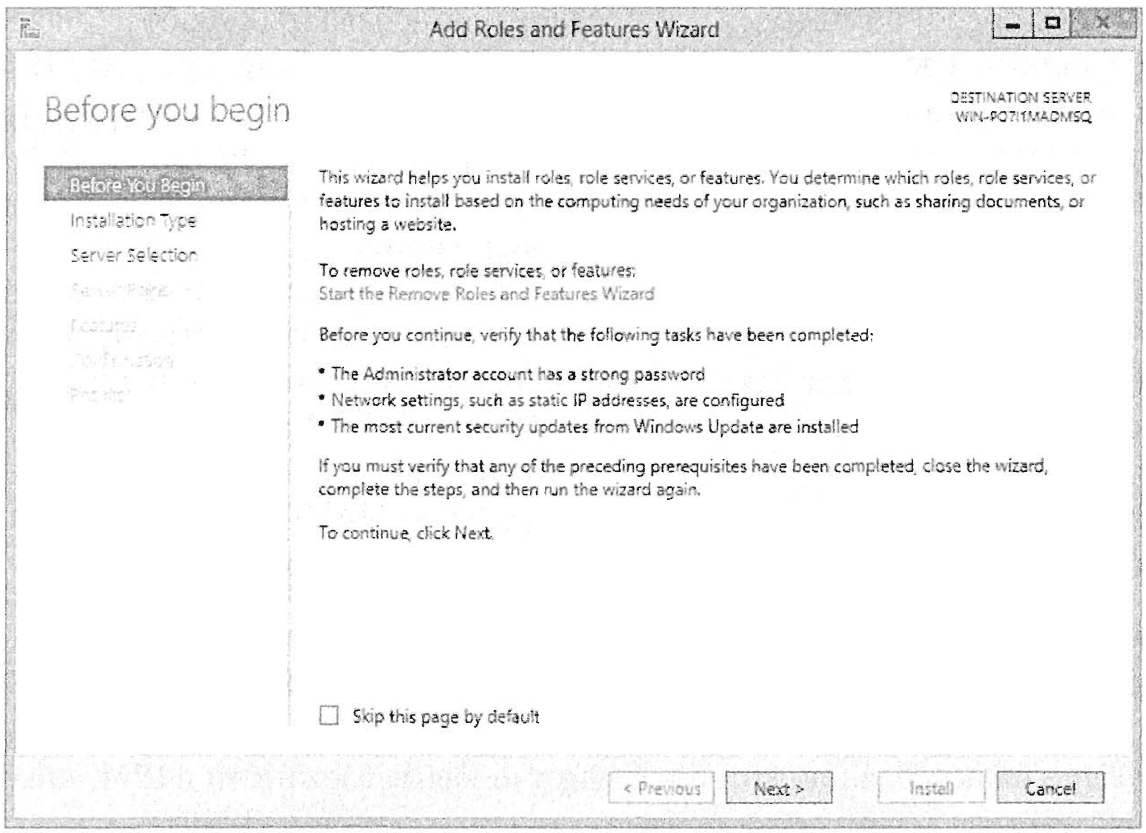


Рис. 20.11. Добавление серверной роли Remote Access

4. Выберите переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) и щелкните на кнопке Next, как показано на рис. 20.12.
5. Выберите в списке свой сервер и щелкните на кнопке Next. Вы окажетесь на экране Select Server Roles (Выбор серверных ролей).
6. Выполните прокрутку до тех пор, пока не увидите роль Remote Access. Отметьте флажок Remote Access (Удаленный доступ), как показано на рис. 20.13.

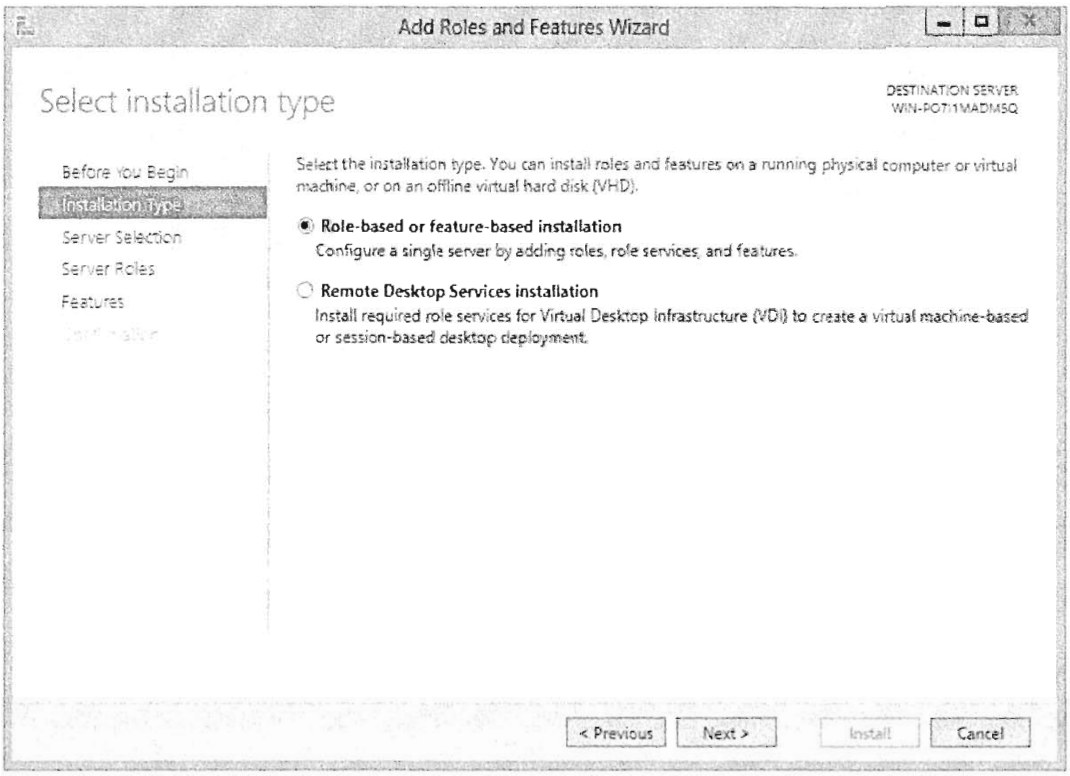


Рис. 20.12. Выбор переключателя Role-based or feature-based installation

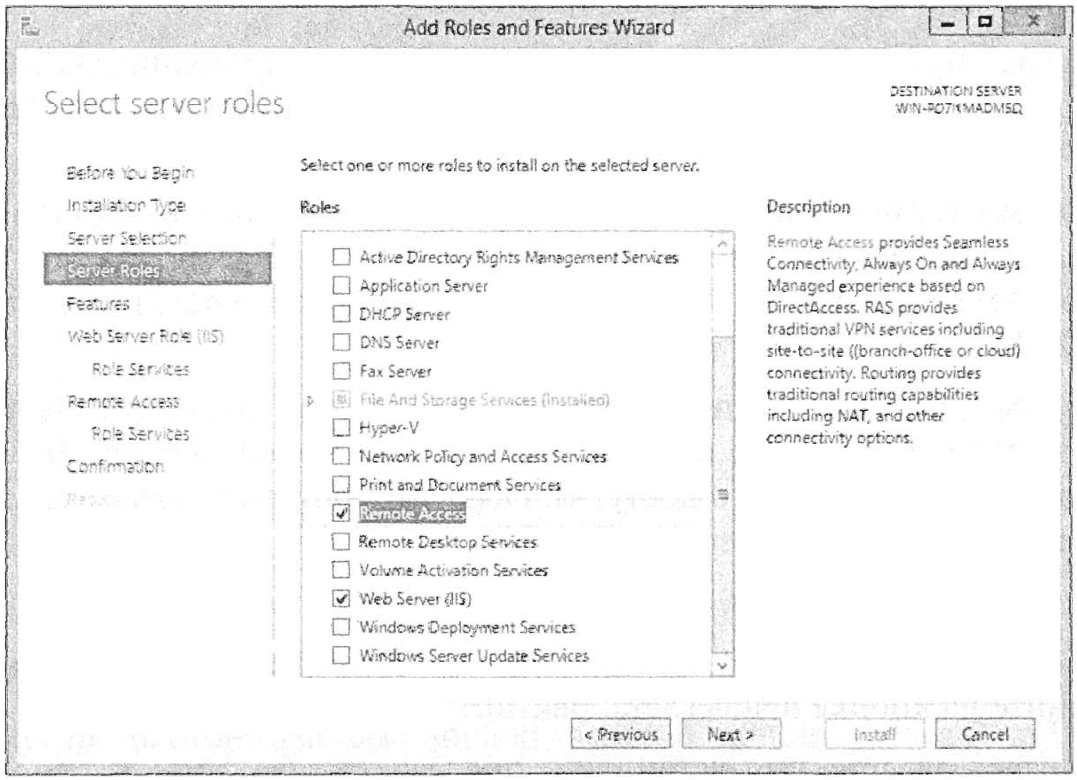


Рис. 20.13. Выбор роли Remote Access

Вам будет предложено установить дополнительные компоненты.

7. Щелкните на кнопке Add Features (Добавить компоненты), как показано на рис. 20.14.

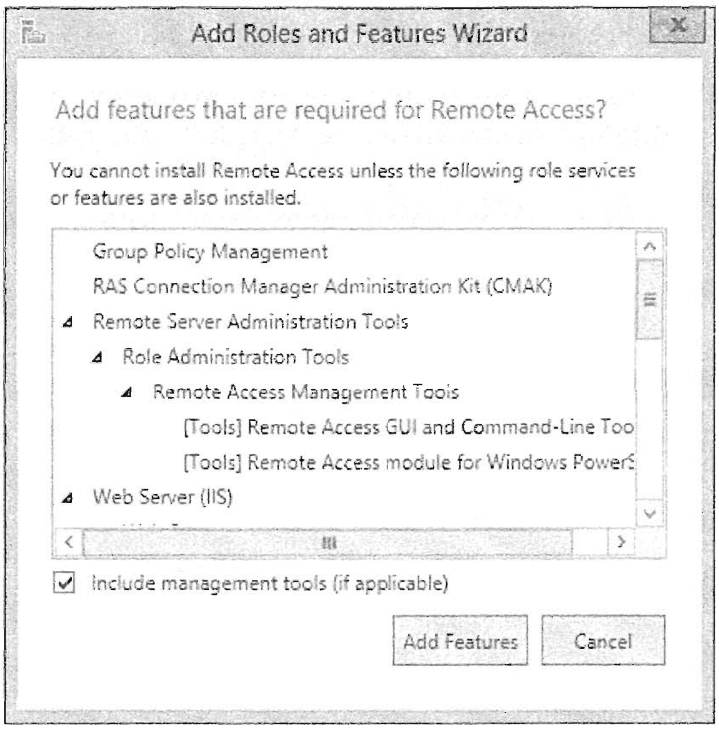


Рис. 20.14. Дополнительные компоненты роли Remote Access

Теперь, когда выбраны все необходимые элементы, можно продолжить установку.

8. Щелкните на кнопке Next.
9. На экране Select features (Выбор компонентов) щелкните на кнопке Next; ничего дополнительного больше не требуется.

   Вам будет предоставлена возможность установить дополнительные элементы ролей, которые формируют необходимые предпосылки для роли Remote Access, а также саму роль Remote Access.

10. Поскольку устанавливать дополнительные элементы для Web Server Role (IIS) (Роль веб-сервера (IIS)) не нужно, щелкайте на кнопке Next до тех пор, пока не попадете на экран Remote Access (Удаленный доступ), представленный на рис. 20.15.
11. Итак, вы добрались до подробностей. Щелкните на кнопке Next на экране Remote Access, и вы окажетесь на экране Remote Access Role Services (Службы роли удаленного доступа). Обратите внимание, что флажок Routing (Маршрутизация) не отмечен.
12. Отметьте флажок Routing, как показано на рис. 20.16.
13. Щелкните на кнопке Next, ознакомьтесь с информацией на итоговом экране и щелкните на кнопке Install (Установить).
14. Дождитесь завершения установки, после чего щелкните на кнопке Close (Закрыть).

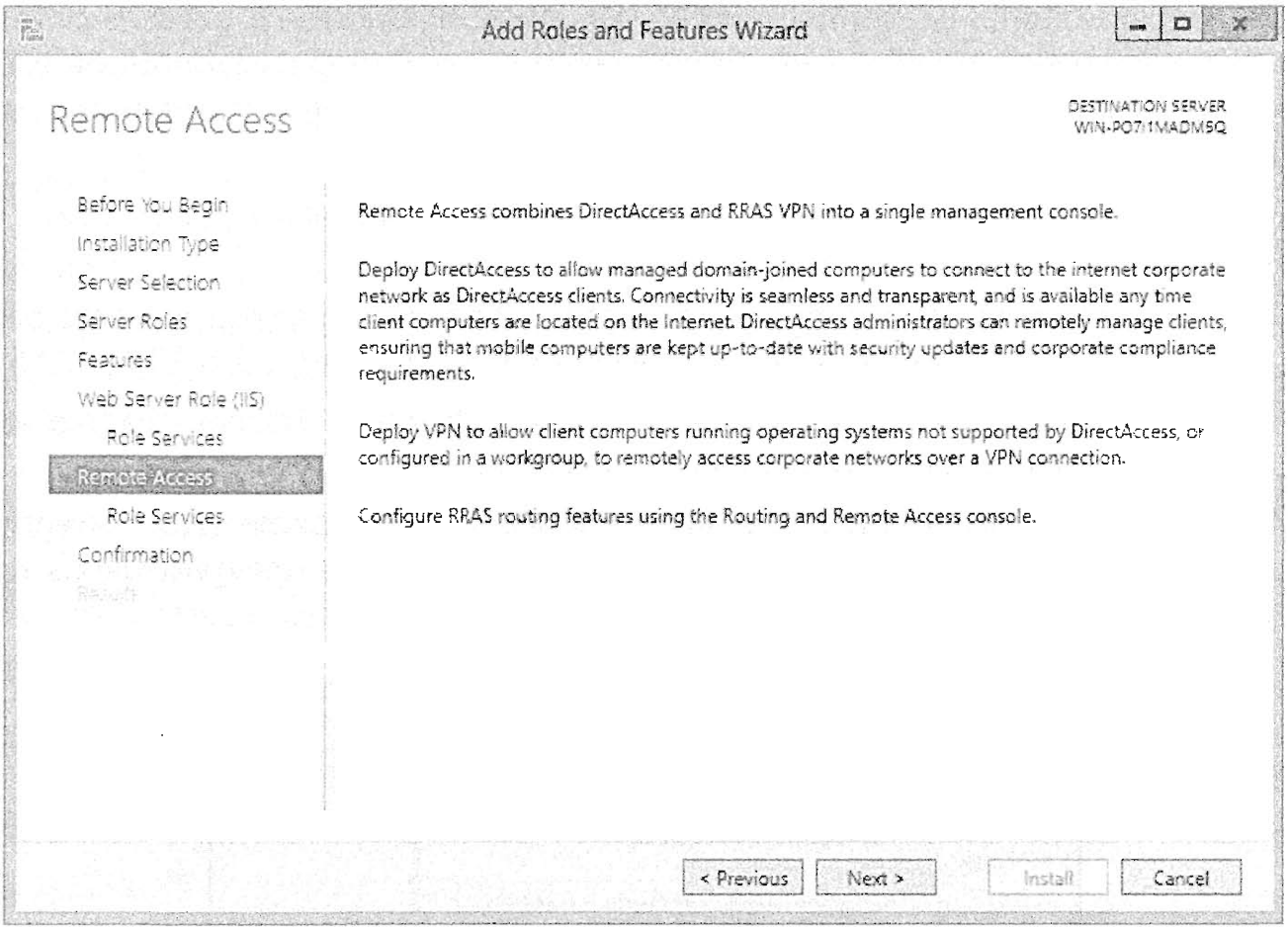


Рис. 20.15. Экран Remote Access

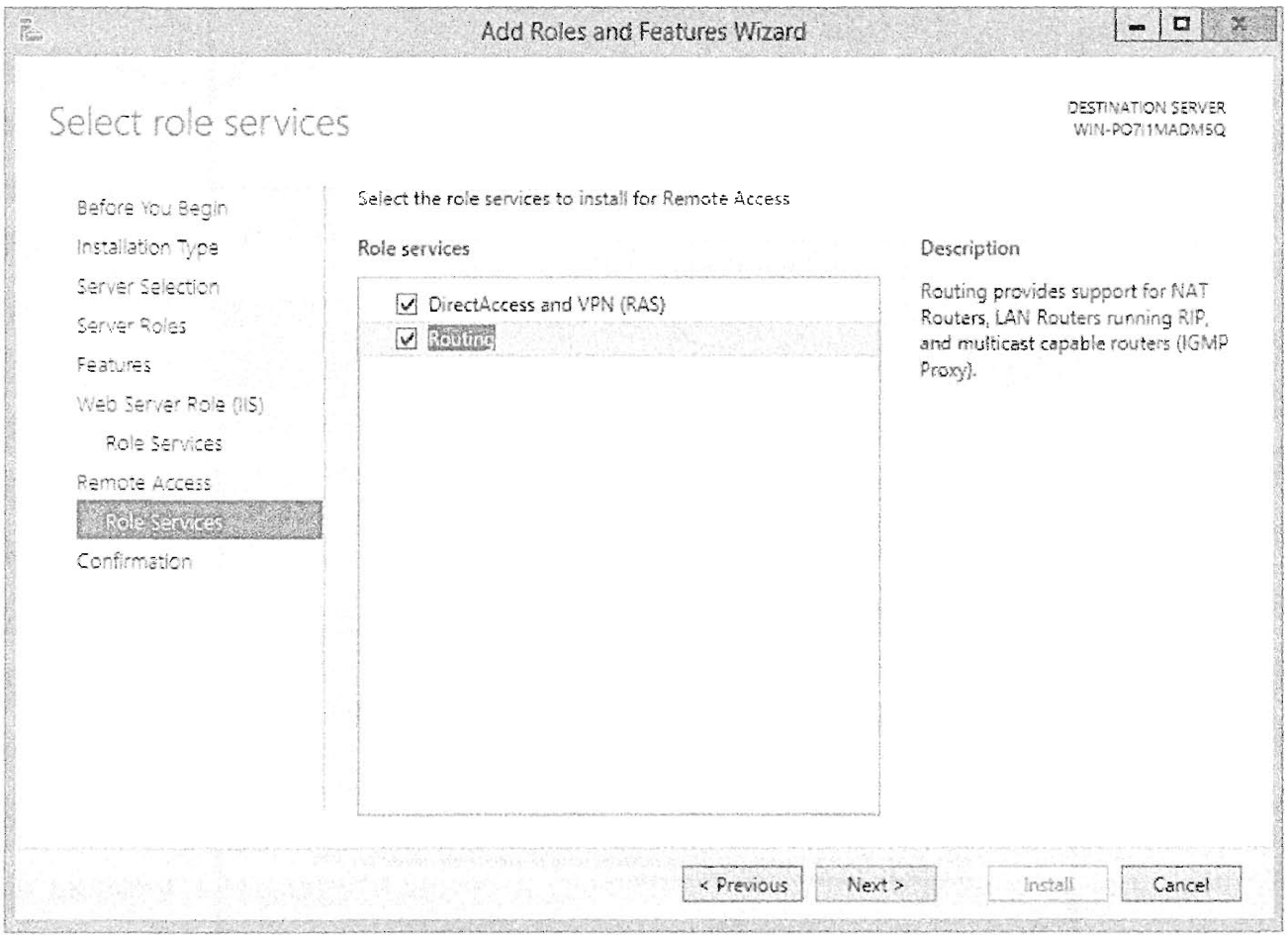


Рис. 20.16. Отметка флажка Routing на экране Remote Access Role Services

Одна из важнейших особенностей ОС Windows Server 2012 R2 связана с тем, что она напоминает вам о необходимости выполнения постконфигурационной работы, когда это требуется. В верхней части окна диспетчера серверов вы увидите символ флажка с восклицательным знаком желтого цвета.

1. Щелкните на значке с восклицательным знаком, и появится еще один экран (рис. 20.17).

   Вы увидите экран Post-deployment Configuration (Конфигурация после развертывания) для роли DirectAccess and VPN (RAS) (DirectAccess и VPN (RAS)).

2. Щелкните на ссылке Open the Getting Started Wizard (Открыть мастер начала работы), чтобы завершить конфигурирование.

   Это приведет к появлению экрана Configure Remote Access (Конфигурирование удаленного доступа). На рис. 20.18 видно, что здесь предусмотрены только опции для конфигурирования DirectAccess и VPN.

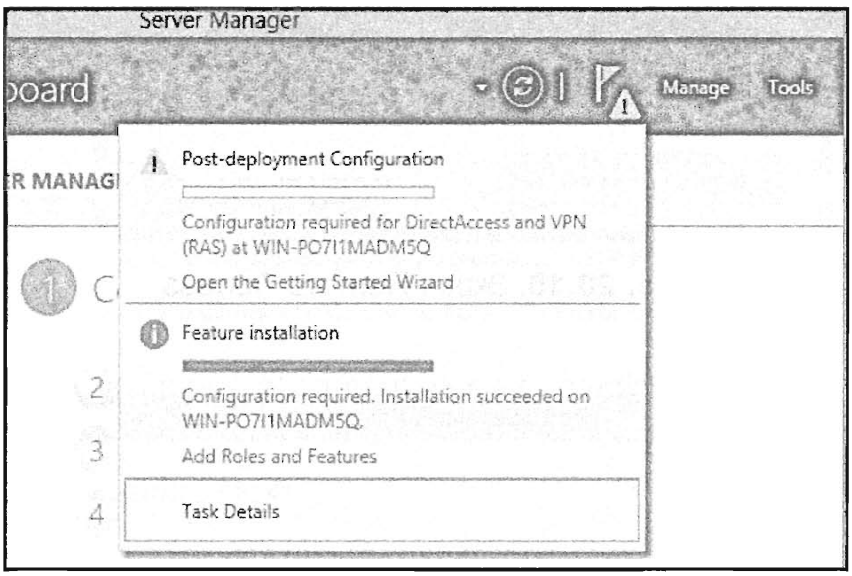


Рис. 20.17. Экран Post-deployment Configuration

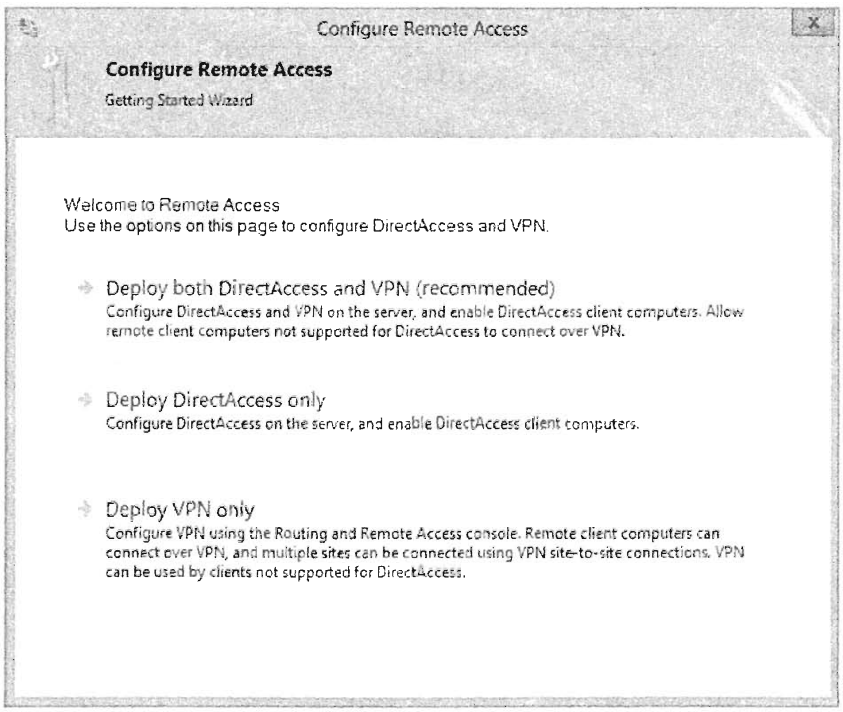


Рис. 20.18. Мастер начала работы для конфигурирования удаленного доступа

3. Поскольку вы не конфигурируете DirectAccess или VPN, просто закройте этот мастер. Вам будет предложено подтвердить закрытие мастера.
4. Получив окно с запросом на подтверждение, щелкните на кнопке OK.

   Чтобы завершить конфигурирование только для элементов маршрутизации и/или NAT, вам нужно воспользоваться традиционной консолью Routing and Remote Access (Маршрутизация и удаленный доступ).
5. Откройте диспетчер серверов и выберите в меню Tools (Сервис) пункт Routing and Remote Access (Маршрутизация и удаленный доступ), как показано на рис. 20.19.

   После запуска консоли Routing and Remote Access вы заметите, что она выглядит хорошо знакомой, если вам приходилось иметь с ней дело в Windows Server 2008 R2. Как видно на рис. 20.20, эта служба не функционирует (о чем говорит изображение стрелки, указывающей вниз, возле имени сервера).

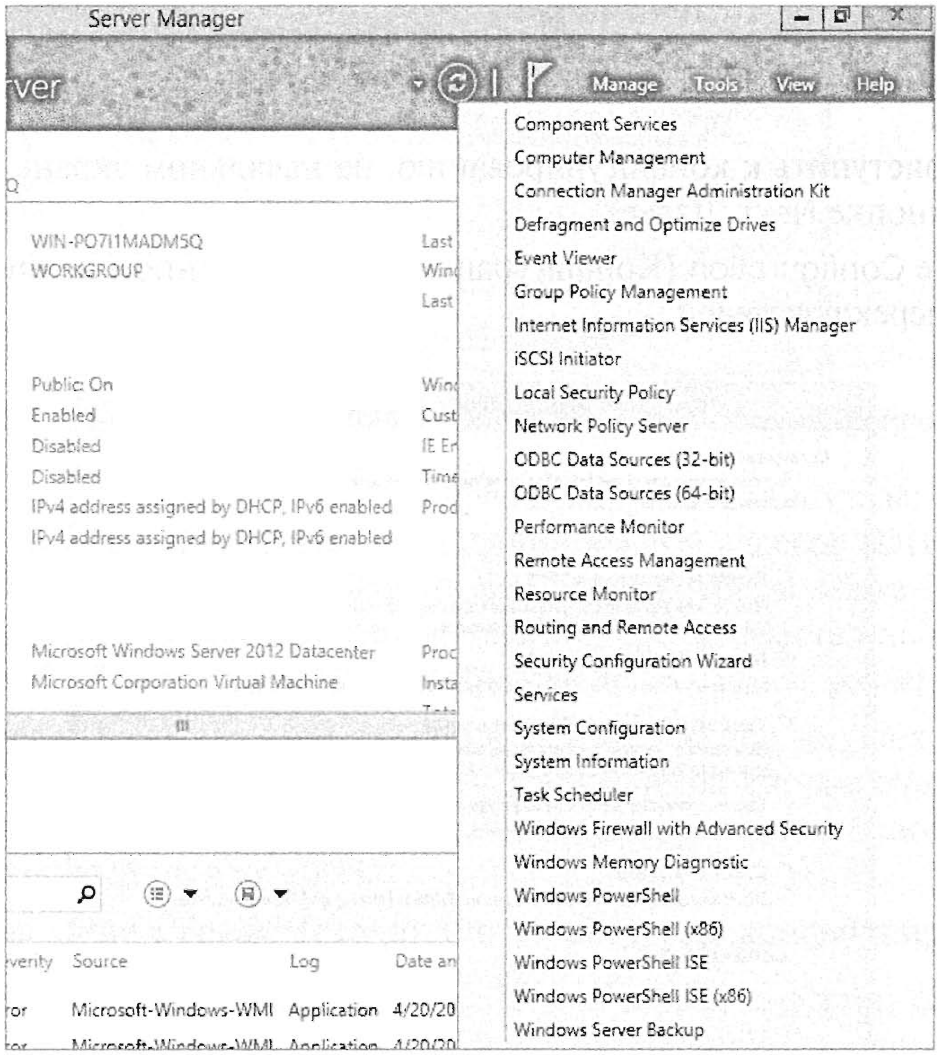


Рис. 20.19. Запуск консоли Routing and Remote Access

6. Щелкните правой кнопкой мыши на имени сервера и выберите в контекстном меню пункт Configure and Enable Routing and Remote Access (Конфигурировать и включить маршрутизацию и удаленный доступ), как показано на рис. 20.20.

   Это приводит к запуску мастера установки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). Все очень похоже на то, как это делалось в Windows Server 2008 R2.

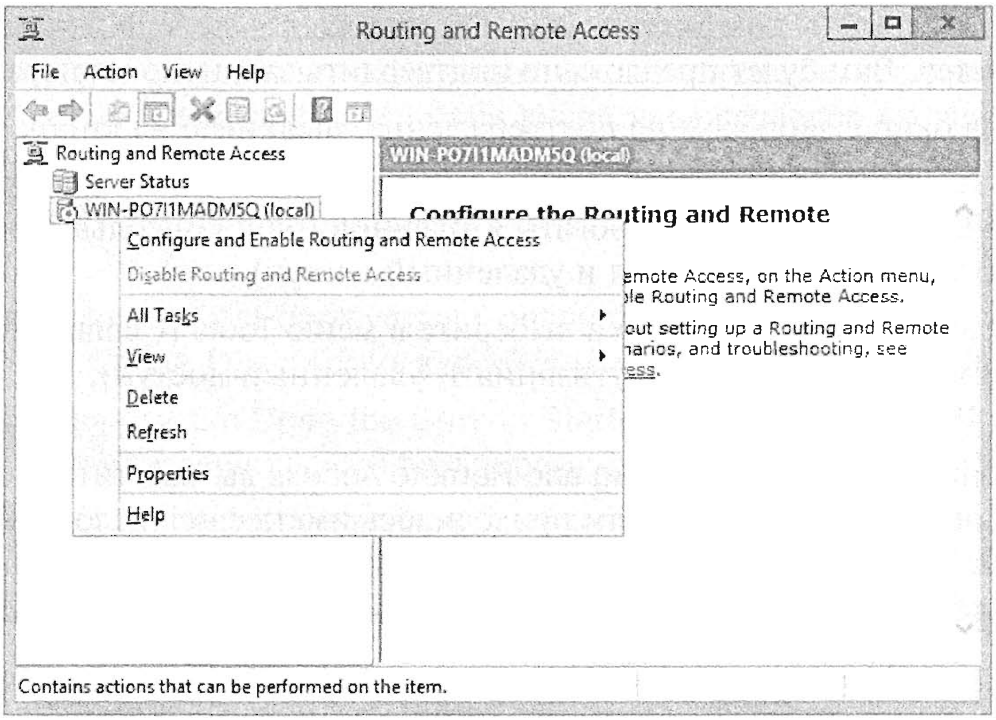


Рис. 20.20. Конфигурирование и включение маршрутизации и удаленного доступа

7. Чтобы приступить к конфигурированию, на начальном экране мастера щелкните на кнопке Next (Далее).

   На экране Configuration (Конфигурация), представленном на рис. 20.21, доступен ряд переключателей.

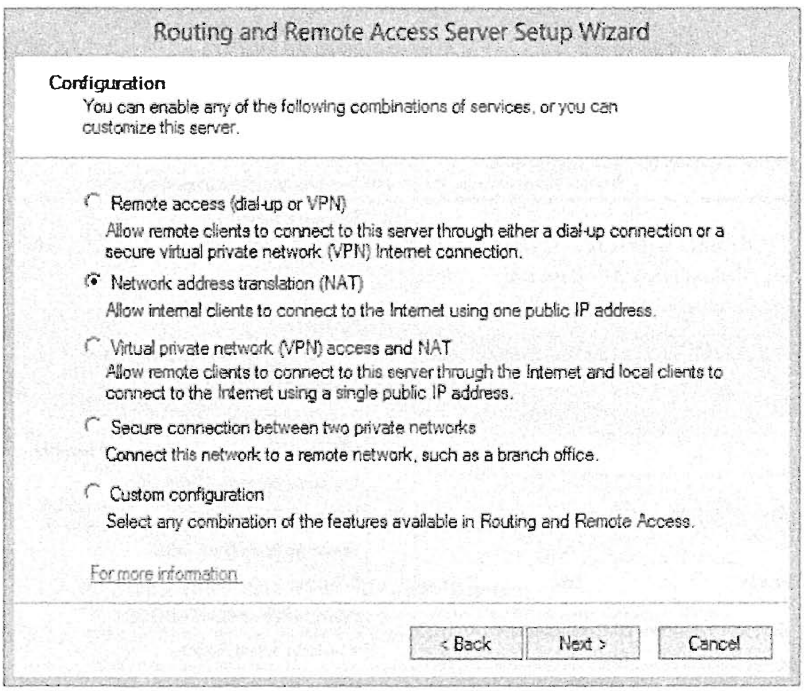


Рис. 20.21. Экран Configuration мастера установки сервера маршрутизации и удаленного доступа

8. Поскольку вы хотите конфигурировать NAT, выберите переключатель Network address translation (NAT) (Трансляция сетевых адресов (NAT)) и щелкните на кнопке Next.

   Вспомните, что назначением NAT в первую очередь является предоставление возможности маршрутизации в Интернете диапазонов IP-адресов, определен-

ных в частном порядке, через открыто маршрутизируемый "маскированный" IP-адрес. Следующий шаг конфигурирования предусматривает выбор сетевого интерфейса, который будет виден из Интернета. По нашему мнению, прежде чем продолжить работу, необходимо переименовать сетевые адаптеры так, чтобы облегчить себе в дальнейшем выбор подходящего интерфейса.

9. На экране NAT Internet Connection (Подключение NAT к Интернету) выберите интерфейс WAN (рис. 20.22).

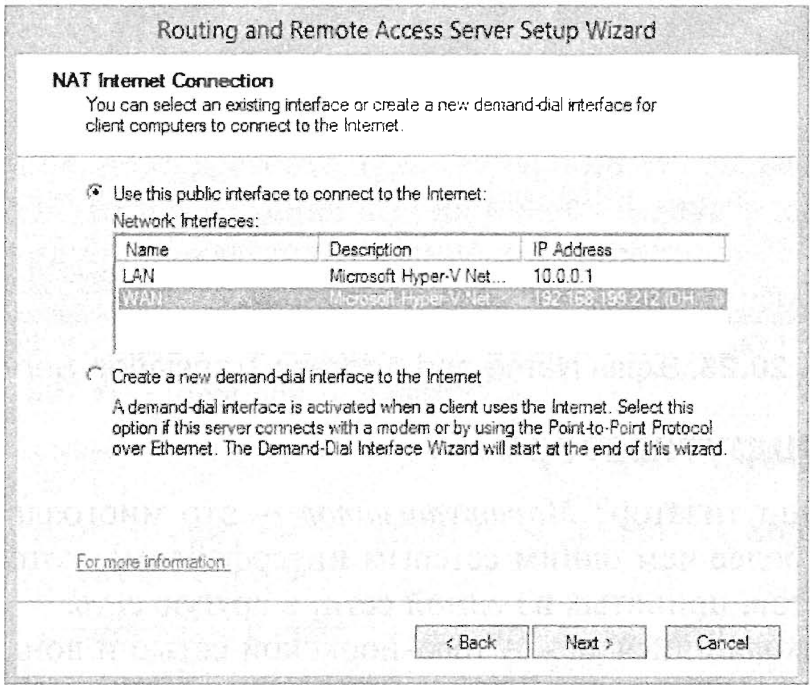


Рис. 20.22. Экран NAT Internet Connection — выбор интерфейса

Затем вам нужно указать, должны ли при маршрутизации и удаленном доступе быть включены базовые службы трансляции имен и адресов (DHCP и DNS). В большинстве ситуаций при наличии развернутой среды Active Directory эти службы являются составными частями данной среды. Мастер попытается обнаружить их. В общем случае эти службы уже должны быть развернуты.

10. Выберите переключатель I will set up name and address services later (Я настрою службы имен и адресов позже) и щелкните на кнопке Next. Появится экран Name and Address Translation Services (Службы трансляции имен и адресов), показанный на рис. 20.23.
11. Щелкните на кнопке Finish (Готово), чтобы завершить конфигурирование.

На этом конфигурирование завершено. Теперь любая система, сконфигурированная со стандартным шлюзом или статическим маршрутом в той же подсети внутри сети, которая подключена к интерфейсу, определенному как внутренний (в нашем примере это была подсеть Нью-Йорка), будет настроена на подключение к Интернету.

Возможно, вы уже догадались, что подобно многим другим устройствам NAT устройство NAT в Windows Server 2012 R2 в действительности представляет собой NAPT в том смысле, что оно будет транслировать и отображать порты необходимым образом. Имеется также ряд встроенных шлюзов ALG для поддержки применения FTP и PPTP.

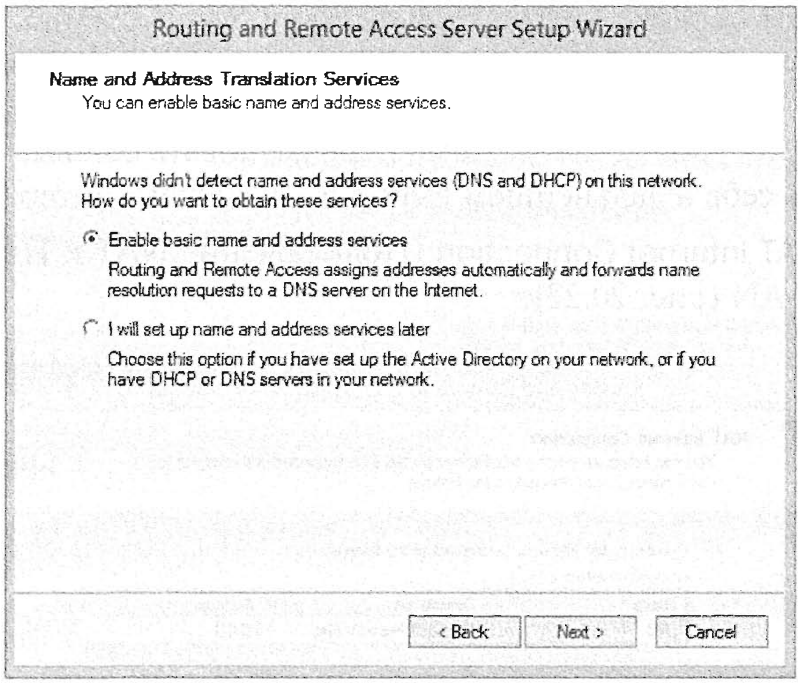


Рис. 20.23. Экран Name and Address Translation Services

Создание маршрутизатора

Что такое маршрутизатор? *Маршрутизатор* — это многоадресный компьютер (т.е. компьютер с более чем одним сетевым интерфейсом), который предназначен для передачи пакетов, принятых из одной сети, в другую сеть.

Компьютер, находящийся между нью-йоркской сетью и лондонской сетью, который мы будем называть компьютером шлюза, хорошо подходит для того, чтобы быть маршрутизатором: он является многоадресным, и каждый интерфейс подключен к своей сети. Но является ли он уже маршрутизатором? Нет — до тех пор, пока он не будет сконфигурирован на пересылку.

По умолчанию компьютеры Windows Server 2012 R2 не настроены на пересылку. Чтобы заставить компьютер Windows Server 2012 R2 пересылать пакеты IPv4, необходимо отредактировать один параметр реестра — `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter`, который должен существовать как значение dword, установленное в 0. Установите его в 1, чтобы включить IP-маршрутизацию, и перезагрузите компьютер.

Вот и все, что нужно было сделать для создания маршрутизатора между двумя локальными подсетями. Этот компьютер теперь будет автоматически пересылать пакеты, принятые на одном интерфейсе, интерфейсу, соответствующему сети, которая содержит адрес получателя этих пакетов. Как и ранее, вы можете использовать команду `route add` (или `netsh`, если вам нравится работать с клавиатурой), чтобы добавить любые маршруты, которые пока еще не представлены в маршрутизаторе.

Туннелирование: почти маршрутизация

Сетевое туннелирование — это форма маршрутизации, в которой сетевой трафик определенным способом инкапсулируется или трансформируется конечной точкой туннеля так, чтобы он мог достичь другой конечной точки туннеля, где он либо извлекается, либо преобразуется обратно.

В каком-то смысле NAT является формой туннелирования, при которой трансформация заключается в изменении IP-адреса и порта отправителя и/или получателя

по пути его следования. Как с другими методами туннелирования, между начальной и конечной точками следования пакета могут встречаться несколько устройств NAT.

Обход туннелирования с помощью portproxy

Последний туннель netsh, который вы посетите, чрезвычайно полезен и называется portproxy. Вы можете применять его, чтобы обойти ограничения портов путем переадресации "безопасного" порта, такого как 80 (для работы в веб с использованием HTTP), на "небезопасный" порт вроде 119 (протокол передачи сетевых новостей (Network News Transfer Protocol — NNTP), который часто блокируется в производственных средах с целью ограничения доступа сотрудников к этому источнику информации).

На другом конце, переадресовав порт 119 на порт 80, вы начинаете с инкапсуляции трафика NNTP из приложения чтения новостей внутрь подключения, которое выглядит для брандмауэра как подключение к веб-серверу.

Предполагая, что ваш домашний компьютер имеет адрес 10.20.30.40, а сервером новостей, на который вы хотите попасть, но не можете, является msnews.microsoft.com, вот команды для применения:

```
[На рабочем компьютере] netsh interface portproxy add v4tov4
119 10.20.30.40 80
[На домашнем компьютере] netsh interface portproxy add v4tov4
80 msnews.microsoft.com 119
```

Подключение к системам у себя дома с помощью этого метода, возможно, вызовет беспокойство, но для некоторых вариантов использования на работе такой метод вполне подойдет. Обратите внимание, что portproxy вообще не предусматривает аутентификации; кроме того, он не обеспечивает шифрования для защиты данных при передаче. Вы можете обнаружить, что виртуальная частная сеть (virtual private network — VPN) предлагает в этом отношении более широкие возможности. Обратитесь к главе 21, чтобы выяснить, каким образом сконфигурировать Windows Server 2012 R2 в качестве конечной точки VPN.

Команды туннелирования IPv6

При отсутствии собственной поддержки IPv6 от вашего поставщика услуг Интернета вы можете протестировать доступ в Интернет по протоколу IPv6 с применением службы туннелирования IPv6, такой как предлагаемая компанией Hurricane Electric (he.net). Мы поступили именно таким образом и настроили свой туннель — туннелирование IPv6 через IPv4 — описанным ниже способом.

```
netsh interface ipv6 add v6v4tunnel IP6Tunnel myIPv4Address 72.52.104.74
netsh interface ipv6 add address IP6Tunnel 2001:db8:1234:567:2
netsh interface ipv6 add route ::/0 IP6Tunnel 2001:db8:1234:567:1
publish=yes
netsh interface ipv6 set interface IP6Tunnel forwarding=enable
netsh interface ipv6 add route 2001:db8:fedc:ba98::/64 "Local Area Connection"
publish=yes
netsh interface ipv6 set interface "Local Area Connection"
forwarding=enable
advertising=enable
```

Первая команда создает сам туннель от данного сервера к машине, находящейся по адресу 72.52.104.74, а сервер, на котором запускается эта команда, теперь способен к коммуникациям IPv6 через этот туннель. Вторая команда создает адрес и назначает его интерфейсу туннеля. Третья команда создает маршрут, который пересылает трафик в туннель IPv6, если для него не определено что-то более конкретное — `::/0` представляет собой заполнитель IPv6 для стандартного получателя в записи маршрутизации.

Четвертая команда разрешает пересылку в туннеле IPv6, чтобы любой проходящий через этот туннель трафик для других машин в сети направлялся на эти машины. Пятая команда добавляет маршрут от этой машины к другим машинам в локальной сети. Шестая команда разрешает пересылку и объявление для трафика в этой локальной сети, чтобы была возможность направлять пакеты, принятые в данной сети, и компьютеры в этой сети знали, что мы хотим пересылать такой трафик дальше.

Еще одним вариантом использования `portproxy` является "включение IPv6" для приложения, которое способно работать только с трафиком IPv4. Мы снова выбираем NNTP в качестве интересующего протокола. Если вы располагаете программой чтения новостей, рассчитанной только на IPv4, и сервером новостей, рассчитанным только на IPv6, то можете соединить их друг с другом посредством следующей команды `portproxy`:

```
netsh interface portproxy add v4tov6 119 news6server.example.com 119
```

Затем просто настройте программу чтения новостей так, чтобы она указывала на `localhost:119`, и она подключится через прокси-сервер к серверу новостей IPv6.

Тестирование и устранение неполадок

Возможно, вам никогда не пригодится материал этого раздела, поскольку после изучения настоящей главы вы должны хорошо понимать маршрутизацию в контексте сервера Windows Server 2012 R2. Ладно, быть может, мы несколько преувеличиваем: некоторые базовые способы поиска и устранения неполадок позволят выяснить, на каких машинах из числа тех, что не входят в сферу вашей ответственности, производится администрирование неизвестными вам людьми, приводя к возникновению проблем.

Использование самого приложения

Для определения состояния сети можно применять многие инструменты. Какой из них и когда будет использоваться, зависит от проблемы, которую вы пытаетесь устранить. Первым инструментом, как и всегда, должен быть инструмент, который вы планируете в действительности применять. Давайте предположим, что вы пытаетесь создать подключение FTP; в этом случае сначала почитайте сообщения об ошибках, выдаваемые FTP-клиентом.

Если FTP-клиент сообщает о том, что запрос на подключение отклонен, то клиент по видимости получил TCP-сообщение RST от IP-адреса, который вы пытались достичь. Это может быть признаком наличия брандмауэра между вами и сервером или само серверное приложение может не функционировать.

Если FTP-клиент сообщает о тайм-ауте, то клиент не получил ничего в ответ на множество запросов на подключение. Это означает или присутствие "скрытого" брандмауэра между клиентом и сервером, или недосягаемость серверного компьютера в данный момент, по причине либо отсутствия сетевого маршрута к нему, либо из-за того, что компьютер в настоящее время не работает.

Избегайте скрытых брандмауэров

Несмотря на то что некоторые поборники безопасности рекомендуют пользоваться скрытыми брандмауэрами, мы не поддерживаем такую точку зрения. Скрытые брандмауэры не отвечают на неожиданные входящие запросы, предпочитая вместо этого хранить молчание. Соответствующим выражением в протоколе TCP для фразы "отойди и не разговаривай со мной" является сообщение RST; молчание по традиции означает "попытайся снова через некоторое время". Выдача сообщений RST не только ограничивает повторы для случайных подключений, но также предотвращает применение имитации подключения (IP-спуфинга) с целью выдать себя за сервер. При выполнении сеанса имитации подключения подлинный сервер будет по-прежнему получать SYN, а сообщение RST, отправляемое им в ответ, вызовет разрыв подключения клиента. Если RST отсутствует, клиент продолжит доверять ложному серверу, что порождает риск в отношении безопасности.

Пингование удаленного компьютера с помощью `ping`

Утилита `ping` — это классический инструмент, которым многие из нас пользуются не один десяток лет. Конструкция этого инструмента несколько изменилась, но базовый принцип заключается в отправке удаленному компьютеру пакета, на который предположительно этот удаленный компьютер ответит, и затем ожидание ответа с указанием, успешно ли он получен. В Windows Server 2012 R2 по-прежнему применяется классический метод `ping`, предусматривающий отправку удаленной машине эхо-запроса ICMP (с дополнительными данными, состоящими из "abcdefgh ijklmnopqrstuvwabcdefghi") и ожидание приема эхо-ответа ICMP.

Таким образом, важно помнить, что утилита `ping` тестирует только эхо-подключаемость ICMP; она не проверяет подключение TCP к серверному порту. Это будет делать только само подключение TCP к серверному порту (вот почему мы предлагали ранее использовать в качестве первого инструмента отладки приложение, которое вы пытаетесь отладить).

Многие брандмауэры блокируют эхо-службу ICMP, поэтому, как нетрудно продемонстрировать, выполнив сначала пингование удаленного компьютера и затем зайдя с помощью веб-браузера на сайт `www.microsoft.com`, неудавшийся результат применения `ping` вовсе не означает отсутствие возможности подключения.

Тем не менее, успешный результат тестирования с помощью `ping` указывает на то, что удаленная машина всего лишь отвечает на эхо-запросы. Вывод команды `ping` можно также использовать для определения корректности преобразования указанного имени в нужный IP-адрес. Инструмент `NsLookup` позволяет опрашивать DNS-сервер, что делает `NsLookup` лишь удобным инструментом для отладки DNS-сервера — для выяснения того, что DNS-клиент собирается делать с именем, `ping` оказывается ничуть не хуже любого другого инструмента.

Список аргументов ping может поставить вас в тупик. Наиболее полезные из них перечислены ниже.

- -t. Пингование хоста вплоть до принудительной остановки. Это полезно для определения момента, когда остановленный сервер возобновляет свою работу.
- -4 и -6. Используются для выбора между IPv4 и IPv6. Обратите внимание, что это повлияет на выбор преобразования имен DNS, а также на маршрут, применяемый для отправки пакетов ping.

Однако в большинстве ситуаций, связанных с поиском и устранением неполадок, оказывается вполне достаточно стандартных параметров, и чтобы получить грубую оценку распознаваемости и достижимости сервера, вы можете использовать команду ping сервер.домен.com.

Пингование удаленного компьютера с помощью traceroute

Утилита tracert, как в Microsoft сокращенно называют traceroute (интересно, помнит ли кто-нибудь сейчас те времена, когда можно было иметь имена файлов, соответствующие схеме "восемь-точка-три"?), представляет собой инструмент, предназначенный для детализации маршрута к получателю. Как и в случае ping, команда tracert отнюдь не обязательно свидетельствует о работоспособности подключения TCP к удаленному хосту. Но в целом tracert дает информацию, которой можно пользоваться.

Утилита tracert действует очень похоже на ping: она отправляет удаленному компьютеру эхо-запрос ICMP и ожидает приема эхо-ответа ICMP. Отличие заключается в том, что tracert устанавливает TTL (счетчик прыжков) на исходящих эхо-запросах. Для первых трех отправляемых пакетов счетчик прыжков устанавливается в 1, для следующих трех отправляемых пакетов — в 2 и так вплоть до указанного вами количества (по умолчанию оно равно 30).

Поскольку при прохождении маршрутизаторов пакетами счетчик прыжков уменьшается, первые три пакета столкнутся с ошибкой на первом же маршрутизаторе по пути к компьютеру-получателю. К счастью для tracert, этот маршрутизатор сообщает о том, что он отбросил этот пакет, а утилита tracert использует эту информацию для отображения адреса первого маршрутизатора. Аналогично, вторые три пакета покажут местонахождение второго маршрутизатора и т.д.

Некоторые маршрутизаторы не сконфигурированы на выдачу ответов, содержащих информацию такого рода, или они настолько загружены, что им просто не хватает для этого времени. В выводе tracert такие маршрутизаторы будут помечены как дающие тайм-аут. Это может произойти на одном или двух прыжках по маршруту. Когда вы видите несколько тайм-аутов в одной строке, это обычно указывает на то, что последний маршрутизатор перед строкой с тайм-аутами оказался неспособным пересылать пакеты в направлении вашего получателя или что получатель не отвечает.

В выводе команды tracert на рис. 20.24 видно, что хостом для www.microsoft.com в этой части мира является lb1.www.ms.akadns.net. Если вы воспроизведете этот тест у себя, картина может оказаться другой. По результатам пингования этого хоста нам уже известно, что он не отвечает на эхо-запросы ICMP, и по этой причине не приходят ответы (либо в виде эхо-ответов, либо в виде сообщений об ошибках) на пакеты со счетчиком прыжков, равным 14 и более.

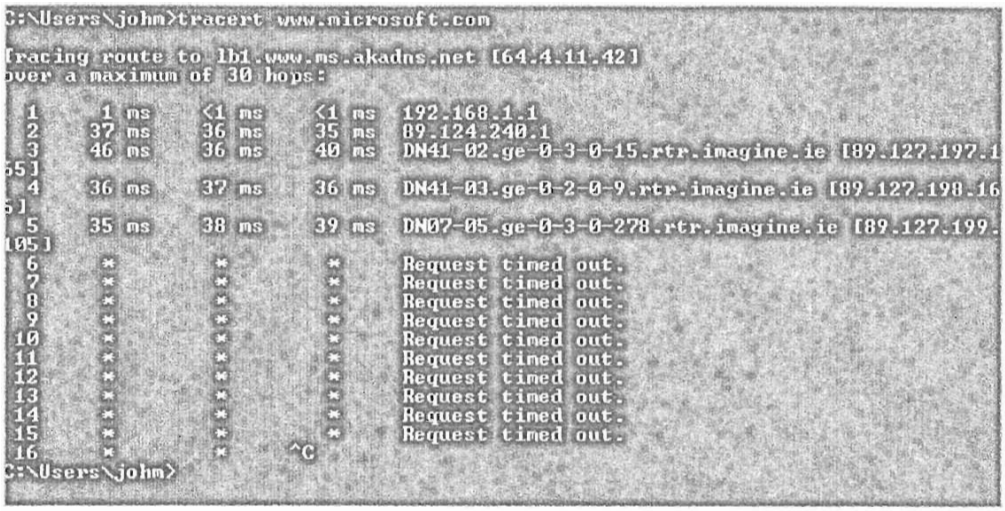


Рис. 20.24. Трассировка маршрута к веб-сайту Microsoft

Однако этот вывод команды `tracert` позволяет получить довольно неплохое представление о маршруте к веб-сайту Microsoft. Вас не должны смущать ответы *: блокирование трафика, основанного на ICMP, с целью предотвращения зондирования является вполне обычным делом.

Опять-таки, команда `tracert` имеет параметры `-4` и `-6`, которые можно применять для принудительной трассировки IPv4 и IPv6.

Проверка конфигурации с помощью `ipconfig`

Утилита `ipconfig` отображает информацию о конфигурации некоторых или всех имеющихся сетевых карт. С помощью `ipconfig /all` можно получить очень подробную информацию, а сама по себе команда `ipconfig` отображает ограниченное подмножество этой информации. Утилиту `ipconfig` лучше всего использовать для проверки, что конфигурация соответствует ожидаемой и, по меньшей мере, соответствует диаграммам сети, которые вы пытаетесь реализовать на практике.

Обратите внимание на наличие нескольких виртуальных интерфейсов в выводе команды `ipconfig`. Например, если вы выключили VPN-сервер или RRAS как точку коммутированного доступа, то для обеспечения возможности применения таким подключениям будет назначен интерфейс.

Для сетевых интерфейсов, которым выдаются адреса посредством DHCP, может быть полезно запустить команду `ipconfig /renew` или команду `ipconfig /release`, а за ней `ipconfig /renew`. Столь же быстро и с меньшими привилегиями можно отсоединить и снова подсоединить соответствующий сетевой кабель — это также приводит к освобождению и обновлению с DHCP-сервера.

Отображение сведений о маршрутизации и соседях

В этой главе мы уже рассказывали о таблице маршрутизации в Windows Server 2012 R2, и вы должны согласиться с тем, что за счет анализа таблицы маршрутизации так, как если бы вы сами были маршрутизатором, можно быстрее обнаружить причины неполадок в сети и локализовать их источник. Если же ваша таблица маршрутизации является очень большой, и разобраться в ней непросто, то уже сам этот факт может расцениваться как дефект, т.к. никто не в состоянии понять даже небольшой участок сети, чтобы с уверенностью заявлять о его корректном функционировании.

Помимо таблицы маршрутизации команда `arp -a or netsh interface ipv6 show neighbors` позволит узнать, с кем недавно обменивался информацией этот компьютер по каналу локальной сети. Если в этой таблице нет других записей за исключением тех, которые использовались групповыми адресами и адаптерами петли обратной связи, это указывает на то, что компьютер, возможно, не в состоянии достичь любого из своих соседей по каналу локальной сети. Часто это является признаком неисправного кабеля или порта коммутатора; в таком случае нужно попробовать заменить кабель или подсоединить его к другому порту коммутатора.

Отсутствие соседей может также указывать на невозможность согласования скорости передачи данных в сети с коммутатором. Недавно нам пришлось столкнуться с ситуацией несовместимости старого, но в целом работоспособного коммутатора 10/100 Мбит/с и нового компьютера с картой Gigabit Ethernet. Эта Ethernet-карта всегда понижала скорость передачи до 10 Мбит/с, а когда мы принудительно устанавливали скорость 100 Мбит/с, она переставала видеть любые другие системы в сети — ее таблица ARP просто опустошалась. Решить эту проблему удалось путем замены старого коммутатора новой моделью.

Использование Network Monitor

Монитор сети (Network Monitor), который ранее был зарезервирован исключительно за администраторами Windows Server, знающими, где он находится, а его самые ценные возможности были доступны только пользователям Microsoft System Management Server (Сервер управления системами Microsoft), теперь стал свободным продуктом, который можно загрузить из сайта Microsoft. Его текущая версия (Network Monitor 3.4) доступна по следующему адресу:

```
http://www.microsoft.com/en-ie/download/details.aspx?id=4865
```

Или же можно просто пройти по указанному ниже адресу и выполнить поиск по ключевым словам *Network Monitor*:

```
http://www.microsoft.com/downloads
```

Этот инструмент претерпел существенные изменения, и если в вашей организации есть разработчики, вы можете соблазнить их возможностью написания сценариев для анализа протоколов на собственном языке Network Monitor, который похож на C/JScript. Для анализа трафика в сети можно также воспользоваться существующими сценариями. Не забудьте дополнительно загрузить анализаторы из следующего сайта:

```
http://nmparsers.codeplex.com/
```

Они обеспечат дополнительные возможности декодирования для протоколов, что позволит лучше понимать сообщения, появляющиеся на экране.

На рис. 20.25 видно, что этот захват данных плюс простой фильтр `protocol.ICMP` дают возможность видеть трафик, сгенерированный в результате предыдущего выполнения команды `ping`.

Какая карта отслеживается?

Если вы хотите захватывать данные только с одной карты с применением Network Monitor, то на основании чего решать, какую именно карту использовать? В большинстве случаев сделать выбор относительно легко, поскольку во множестве систем установлена единственная сетевая карта, так что вариантов для выбора попросту нет.

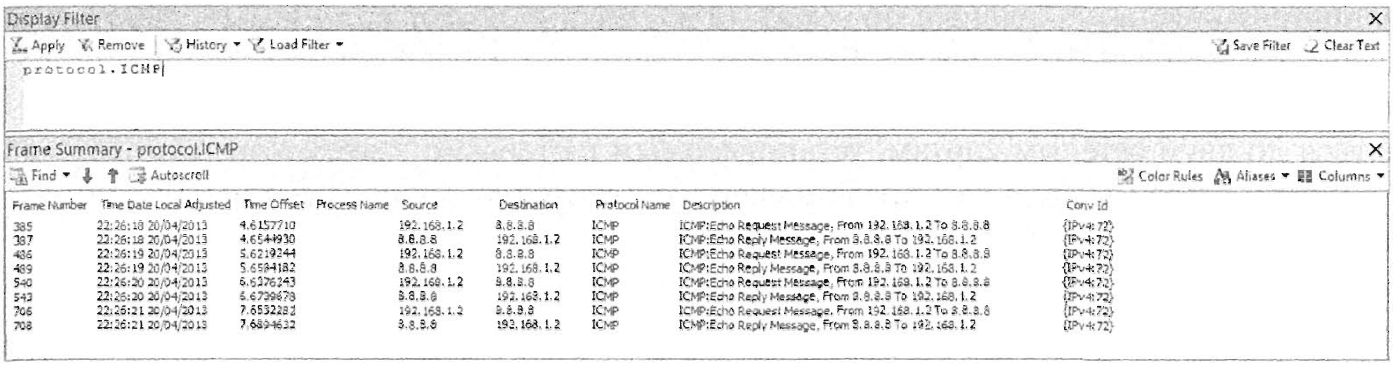


Рис. 20.25. Просмотр захвата данных `ping` в Network Monitor 3.4

Тем не менее, из-за отличий, имеющихся между IPv4 и IPv6, появляется одна особенность, которая касается темы слабых отправок и слабых получений.

- **Слабая отправка.** *Слабая отправка* — это такая отправка, когда IP-адрес отправителя пакета не соответствует IP-адресу, принадлежащему сетевому интерфейсу, на который он отправлен.
- **Слабое получение.** По аналогии со слабой отправкой *слабое получение* — это такое получение, когда IP-адрес получателя пакета не соответствует IP-адресу, принадлежащему сетевому интерфейсу, на котором он принят.

Уже не одно десятилетие IPv4 вносит своим поведением путаницу в умы сетевых администраторов. В интерфейсах IPv4 слабые отправки по умолчанию разрешены, а это значит, что интерфейс, выбранный для отправки IP-пакета, зависит от IP-адреса получателя, но не от IP-адреса отправителя. Выбирается интерфейс, ближайший к адресу следующего прыжка на маршруте к получателю.

Однако все это *не* имеет отношения к Windows Server 2012 R2 и Windows Server 2008 R2. В Windows Vista и Windows Server 2008 компания Microsoft предприняла решительный шаг, потребовав, чтобы IP-пакеты исходили из интерфейса, который соответствует адресу их отправителя, и подобным же образом — чтобы IP-пакеты отбрасывались, если адрес их получателя не совпадает с адресом интерфейса, на который они были приняты.

В отличие от этого в IPv6 по умолчанию слабые отправки не разрешены, поэтому пакет будет всегда отправляться интерфейсу, IP-адрес которого соответствует IP-адресу отправителя этого исходящего пакета. В Windows Server 2008 в этом отношении никаких изменений не произошло.

Тем не менее, перемены заключаются в том, что вы можете изменить данное поведение. Как и со всеми новыми командами конфигурирования сети, это можно сделать с помощью `netsh`:

```
netsh interface ipv4 set interface <имя_или_индекс> weakhostsend=enabled
netsh interface ipv4 set interface <имя_или_индекс> weakhostreceive=enabled
netsh interface ipv6 set interface <имя_или_индекс> weakhostsend=enabled
netsh interface ipv6 set interface <имя_или_индекс> weakhostreceive=enabled
```

Разумеется, любое из этих значений можно установить обратно в `disabled`, как принято по умолчанию, если вы предпочитаете именно такое поведение.

Отключение слабых получений для хоста является мерой защиты многоадресного компьютера, при которой пакеты будут отбрасываться, если они не были приняты на ожидаемом интерфейсе. Однако это может привести к отбрасыванию законного трафика, который действительно должен достичь вашего компьютера, если схема

маршрутизации и кабельные подключения отправили этот трафик не тому интерфейсу, на который было нужно. Если это именно тот случай, тогда конструкция вашей сети нуждается в пересмотре. Локальное звено, или подсеть, не должно разделяться по двум сетевым картам, установленным в отдельно взятом компьютере.

В этой главе мы дали вам представление о некоторых возможностях маршрутизации Windows Server 2012 R2. Из описания виртуальных частных сетей, приведенного в главе 21, вы узнаете об одной важной способности маршрутизации.

Резюме

Документируйте время жизни IP-пакета, маршрутизируемого по вашей сети. Понимание того, как компоненты маршрутизации действуют внутри хостов и маршрутизаторов, позволит вам предвидеть, по каким маршрутам сети будет проходить сетевой трафик. Такое понимание способствует обнаружению и устранению неполадок, временами возникающих в сети.

> *Контрольный вопрос.* Обратившись к сети Нью-Йорк/Лондон на рис. 20.1, воспользуйтесь своим пониманием маршрута, совершаемого IP-пакетом из хоста A на нью-йоркском сайте к хосту C на лондонском сайте, чтобы определить, какие адреса вы должны пропинговать для выявления проблем с маршрутизацией, которые препятствуют прохождению пакетов из пункта A в пункт C.

Объясняйте точки зрения на IP-маршрутизацию с учетом классов и без учета классов. При обсуждении маршрутизации со специалистами по сетям важно понимать старую терминологию, основанную на классах. Это существенно облегчит как обсуждение подобных вопросов, так и знакомство с документацией, в которой может использоваться старая терминология. Понимание работы IP-маршрутизации без учета классов позволит избежать неэффективности, являющейся результатом чрезмерно строгого соблюдения границ классов при адресации сети.

> *Контрольный вопрос.* Адрес 172.24.255.255 находится внутри класса B, для которого стандартной маской сети является 255.255.0.0. Он также относится к диапазону частных сетей 172.16/20 (RFC 1918), стандартная маска сети для которого выглядит как 255.255.240.0. С учетом этой информации укажите, чем является адрес 172.24.255.255 — адресом хоста или широковещательным адресом подсети?

Применяйте устройства NAT для маршрутизации трафика TCP. До тех пор, пока все мы не перейдем на использование протокола IPv6, нам придется применять устройства NAT для маршрутизации трафика TCP, который передается от множества хостов сети во внешний мир, используя для этого только несколько IP-адресов из сокращающегося резерва открытых IP-адресов. Понимание того, как устройства NAT изменяют адреса отправителя и получателя IP-пакетов, позволит отслеживать маршруты пакетов в сети и определять, какие системы следует рассматривать в качестве получателей данных.

> *Контрольный вопрос.* Пользователь жалуется, что когда он подключается к FTP-сайту, подключение поначалу устанавливается, но при первой же попытке получения списка файлов оно разрывается, а сервер сообщает, что не может подключиться к 192.168.0.10. Каковы вероятные причины возникновения этой проблемы и как ее можно решить?

Глава 21

Дистанционный доступ в офис: виртуальные частные сети

С ростом популярности мобильных вычислений все большее количество пользователей нуждаются в дистанционном доступе к своим данным, хранящимся на компьютере в их офисе. В частности, коммивояжерам, надомным работникам и консультантам по информационным технологиям во время их пребывания в пути или у себя дома должна быть предоставлена возможность безопасного подключения и непрерывающейся работы, как если бы они находились у себя в офисе. Для удовлетворения такой потребности часто используются виртуальные частные сети (virtual private network — VPN).

Сеть VPN — это частное подключение, которое создается в открытой сети, такой как Интернет. Если у пользователей есть доступ в Интернет (а в наши дни трудно найти кафе, аэропорт или общественное здание, где в той или иной форме не обеспечивалась бы возможность подключения к Интернету), то они могут обратиться в свой офис посредством VPN. После установки подключения пользователи могут обращаться к любым офисным ресурсам (к электронной почте, общим папкам и т.п.), как если бы они находились в самом офисе. Роль Remote Access в Windows Server 2012 R2 обеспечивает традиционные возможности службы маршрутизации и удаленного доступа (Routing and Remote Access Service — RRAS), которые стали привычными благодаря предыдущим версиям Windows Server. Однако опции дистанционного подключения были значительно модернизированы с помощью расширенной функциональности DirectAccess, которая также входит в состав этой роли. Это неклиентская, всегда включенная и управляемая посредством групповой политики альтернатива VPN, которая основана на протоколе шифрования IP Security (IPSec). Средство DirectAccess предоставляет поддержку для клиентов Windows 7 Enterprise и Windows 7 Ultimate или Windows 8 Enterprise. Тем не менее, для унаследованных клиентов по-прежнему нужно применять RRAS, чтобы обеспечить подключаемость через VPN.

В этой главе вы изучите следующие темы:

- добавление роли Network Policy and Access Services;
- сущность роли Remote Access;
- конфигурирование VPN-сервера;
- исследование DirectAccess.

Введение в VPN

Сеть VPN используется для предоставления доступа к частной сети через открытую сеть. Открытой сетью часто является Интернет, но это также могут быть арендованные линии связи, которые совместно применяются разными компаниями. На рис. 21.1 показан распространенный пример конфигурирования VPN-сервера.

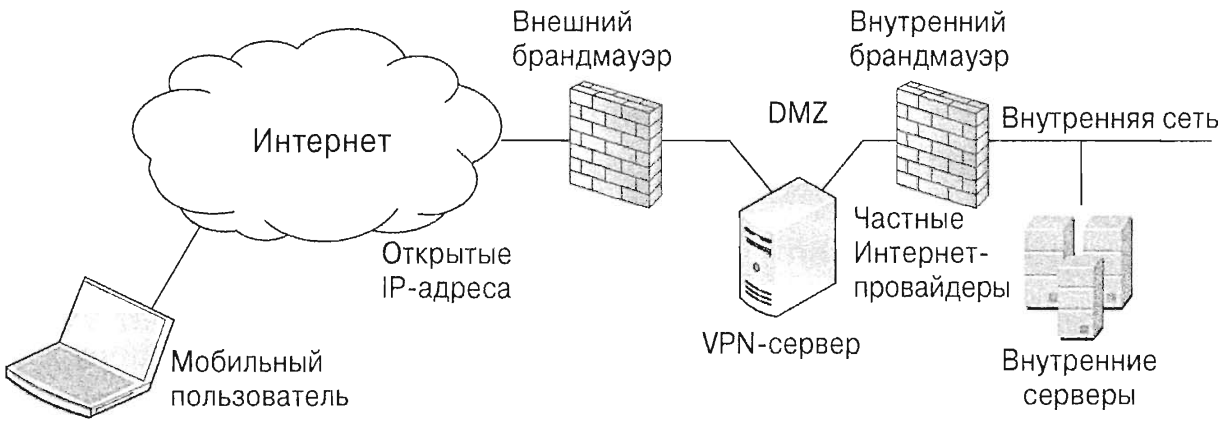


Рис. 21.1. Использование VPN для подключения мобильных пользователей

У VPN-сервера имеются, по меньшей мере, две сетевые интерфейсные карты (network interface card — NIC). Одной NIC назначен открытый IP-адрес, и она достижима любым пользователем, который располагает доступом в Интернет. Другой NIC назначен частный адрес, соединенный с внутренней сетью.

Как видно на этом рисунке, VPN-серверы часто размещаются в *демилитаризованной зоне* (demilitarized zone — DMZ). Как правило, у DMZ есть два брандмауэра. Один брандмауэр обеспечивает уровень защиты хостам в DMZ от потенциальных атак из Интернета, а второй, внутренний, брандмауэр предоставляет дополнительный уровень защиты внутренним клиентам. В других случаях DMZ может создаваться путем утилизации интерфейса на одном брандмауэре с последующим применением правил маршрутизации для создания сегментации между DMZ и локальной сетью. Хотя на рис. 21.1 с целью упрощения показан лишь VPN-сервер, DMZ можно сконфигурировать так, чтобы она содержала не только VPN-сервер.

Мобильный пользователь может использовать VPN-подключение для соединения с внутренней сетью, подключившись сначала к VPN-серверу. Установив подключение, пользователь получает возможность обращаться к внутренним ресурсам, как если бы он физически находился в этой внутренней сети. Один из недостатков состоит в том, что такое подключение зачастую оказывается довольно медленным.

Прежде всего, этому мобильному пользователю необходимо получить доступ в Интернет. Это можно сделать посредством широкополосного, коммутируемого или беспроводного подключения. Как именно пользователь соединен с Интернетом,

не так уж важно; важно лишь то, что он установил подключение. Затем VPN-сервер маршрутизирует трафик между мобильным пользователем и внутренней сетью.

Специфичной ролью, которая поддерживает сети VPN в Windows Server 2012 R2, является Remote Access. Служба RRAS внутри этой роли может применяться и для сетей VPN, и для подключений с прямым набором номера. Вы можете дополнить роль Remote Access использованием сетевой и клиентской безопасности, управляемой политиками, для чего развернуть роль Network Policy and Access Services (Службы сетевой политики и доступа). Позже мы обсудим обе роли более подробно.

Сеть VPN типа "шлюз-шлюз"

Хотя основное внимание в этой главе сосредоточено на предоставлении возможности подключения мобильным пользователям, сети VPN допускается также конфигурировать на поддержку подключаемости между двумя разными офисами. Этот вариант называется *сетью VPN типа "шлюз-шлюз"* и представлен на рис. 21.2.

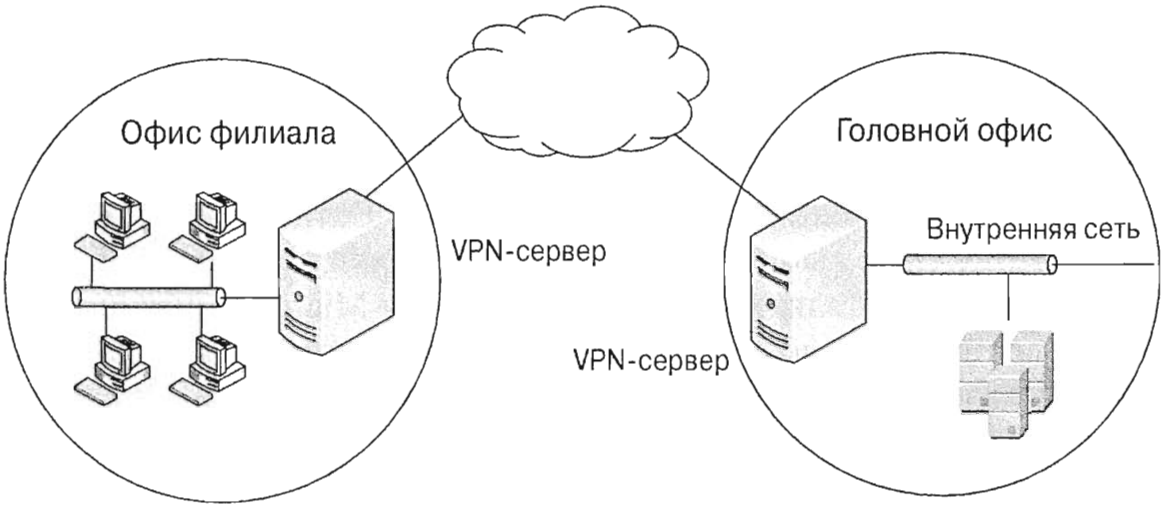


Рис. 21.2. Организация сети VPN типа "шлюз-шлюз"

В сети VPN типа "шлюз-шлюз" два VPN-сервера соединены через открытую сеть. В этой ситуации открытой сетью обычно оказываются получастные выделенные линии связи, но может применяться также Интернет. Это позволяет пользователям в офисе филиала легко подключаться к ресурсам головного офиса посредством VPN. Пользователи могут заметить, что такое подключение работает медленнее, но во всех остальных отношениях подключение ведет себя так, будто сервер находится в географически удаленном офисе.

Протоколы туннелирования

При конфигурировании VPN всегда должна приниматься во внимание безопасность. Данные не могут передаваться через Интернет в виде открытого текста без риска, что какой-то злоумышленник попытается перехватить их. Чтобы устранить такую опасность, в сетях VPN используются протоколы туннелирования.

В настоящее время для сетей VPN под Windows применяются три основных протокола туннелирования: протокол туннелирования уровня 2 (Layer 2 Tunneling Protocol — L2TP), протокол туннелирования с защищенным сокетом (Secure Socket Tunneling Protocol — SSTP) и протокол обмена ключами в Интернете версии 2 (Internet Key Exchange version 2 — IKEv2).

В прошлом использовался протокол туннелирования типа "точка-точка" (Point-to-Point Tunneling Protocol — PPTP), но из-за известных уязвимостей он применяется все реже, учитывая более высокую озабоченность администраторов вопросами безопасности.

Как VPN-сервер, так и VPN-клиент должны быть сконфигурированы на использование одного и того же протокола туннелирования.

Протокол Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol — это популярный протокол туннелирования, применяемый с сетями VPN. Обычно он шифрует трафик с помощью протокола IPSec (который подробно объясняется далее в главе); именно поэтому часто встречается обозначение L2TP/IPSec.

Когда L2TP используется в сочетании с IPSec, L2TP шифрует данные, обеспечивая их конфиденциальность, и подписывает данные, поддерживая их целостность. Однако у IPSec есть один недостаток, который не позволяет применять этот протокол все время — трафик IPSec не может проходить через сервер трансляции сетевых адресов (Network Address Translation — NAT).

NAT обычно служит для перевода частных IP-адресов в открытые IP-адреса и открытых IP-адресов обратно в частные. Однако из-за способа, которым пакеты IPSec собираются вместе, NAT безжалостно разрушает их. Если вам необходимо проходить через сервер NAT, то вы просто не сможете использовать L2TP/IPSec.

В прошлом, если для подключения к VPN-серверу Microsoft нужно было проходить через сервер NAT, вы должны были применять протокол PPTP. У этого протокола были выявлены серьезные проблемы с безопасностью, поэтому в наши дни он используется редко. Тем не менее, теперь для прохождения сервер NAT имеется другой вариант — Secure Socket Tunneling Protocol.

Протокол Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (SSTP) является более новым протоколом туннелирования, который появился в Windows Server 2008 и полностью поддерживается в Windows Server 2012 R2. Для защиты трафика VPN он применяет протокол защищенных сокетов (Secure Sockets Layer — SSL) на порте 443.

Действительно, появление SSTP было важным событием. Широко используемый протокол обеспечения безопасности SSL имеет превосходную репутацию и его хорошо понимают IT-специалисты. Именно поэтому профессионалы в области безопасности и администраторы доверяют этому протоколу гораздо больше, чем каким бы то ни было новинкам в данной области. Возможно, это кажется вам маловероятным, но если вы когда-либо пытались уговорить администратора брандмауэра открыть порт на брандмауэре предприятия, то неплохо знаете, что имеется в виду. Администраторы брандмауэров славятся (и по праву) тем, что согласны открывать только абсолютно необходимые порты. И даже если они убеждены в том, что порт должен быть открыт для выполнения конкретной задачи, их еще приходится всерьез убеждать в том, что открытие порта не несет в себе угрозы безопасности.

Однако поскольку протокол SSTP применяет SSL на порте 443, администратор брандмауэра проявляет бо́льшую готовность открыть такой порт (если только он еще не открыт). Безопасность SSL известна, так что если в рамках бизнес-модели

внедряется SSTP, это приемлемо для администратора брандмауэра. Вдобавок, если в производственной среде уже имеется веб-сервер, который использует HTTPS, то порт 443 уже открыт, и вам не придется долго упрашивать администратора брандмауэра открыть такой порт.

Сеанс SSTP начинается с создания сеанса HTTPS. Этот сеанс HTTPS шифруется с помощью SSL, что гарантирует безопасность сеанса еще до того, как любая информация или учетные данные аутентификации будут переданы по сети. После установления сеанса HTTPS сеанс SSTP отправляет учетные данные аутентификации и собственно данные по зашифрованному каналу.

Для поддержки SSL на VPN-сервере должен быть установлен сертификат, полученный от доверенного центра сертификации. Когда подключаются VPN-клиенты, этот сертификат отправляется клиентам и применяется для создания безопасного сеанса.

Протокол Internet Key Exchange version 2

Протокол Internet Key Exchange version 2 впервые появился в составе Windows Server 2008 R2 как новый тип VPN, а сейчас, с появлением Windows Server 2012 R2, он получил большие шансы на успех. Самым крупным преимуществом IKEv2 является способность поддержки средства VPN Reconnect (Восстановление подключения VPN).

Средство VPN Reconnect позволяет VPN-клиентам выдерживать непродолжительные разрывы подключения к сети, не теряя подключение в целом. После временной потери подключения к сети VPN-клиент может продолжить работу без повторной установки этого подключения с самого начала.

Протокол IKEv2 полезен в средах, где клиенты могут переходить от одного беспроводного клиента к другому или даже от беспроводного подключения к проводному подключению. IKEv2 требует получения сертификата от доверенного центра сертификации, но может пользоваться тем же самым сертификатом, что и SSTP.

Использование роли Network Policy and Access Services

Роль Network Policy and Access Services в Windows Server 2012 R2 позволяет создавать и вводить в действие политики, касающиеся сетевого доступа, аутентификации, авторизации и работоспособности клиентов в организации. Развертывание этой роли обеспечивает доступ к перечисленным ниже службам.

- **Network Policy Server (Сервер сетевой политики).** Служба Network Policy Server (NPS) — это реализация сервера RADIUS (Remote Authentication Dial-in User Service — служба дистанционной аутентификации пользователей, получающих доступ по дозвону) компанией Microsoft и включает политики доступа в сеть, учет, защиту доступа в сеть (Network Access Protection — NAP) и т.д. Технология NAP (иногда называемая защитой конечных точек (Endpoint Protection)) может применяться для оценки работоспособности клиентов, прежде чем им будет предоставлен доступ к сетевым ресурсам. Работоспособность определяется путем исследования клиентов с целью выяснения, удовлетворяют ли они определенным условиям, которые заранее установлены администратором, и могут включать такие пункты, как своевременно выполненные обновления, наличие

включенного брандмауэра и функционирование антивирусного ПО. Эти политики работоспособности могут применяться к любым клиентам — действующим в проводной сети, действующим в беспроводной сети или подключающимся дистанционно.

- **Health Registration Authority (Центр регистрации работоспособности).** Центр регистрации работоспособности (Health Registration Authority — HRA) входит в состав NAP и используется для выпуска сертификатов работоспособности, которые применяются для активизации NAP IPSec. Если клиент проводит проверку политики работоспособности, выполняемую NPS, то HRA выдаст чистую справку о работоспособности в форме сертификата работоспособности.
- **Host Credential Authorization Protocol (Протокол авторизации учетных данных хостов).** Протокол авторизации учетных данных хостов (Host Credential Authorization Protocol — HCAP) используется для объединения решения NAP от Microsoft с сервером управления сетевым доступом (Network Access Control Server) компании Cisco.

Является ли наличие этой роли обязательным требованием, если нужны только сети VPN?

Несмотря на то что развертывание роли Network Policy and Access Services не является обязательной предпосылкой для создания сетей VPN, наличие такой роли, установленной наряду с ролью Remote Access, обеспечивает несомненное преимущество при реализации безопасного и детализированного доступа в сеть, который большинство организаций требуют от сетей VPN. Следует также отметить, что все пользовательские учетные записи в Active Directory по умолчанию сконфигурированы на управление их коммутируемым доступом за счет применения сетевой политики NPS независимо от того, развернута эта роль или нет.

Установка роли Network Policy and Access Services

Прежде всего, мы будем предполагать, что у вас имеется среда с минимум одним контроллером домена Windows Server 2012 R2, сервером-членом и клиентом Windows 8. Перед тем, как пытаться развернуть удаленный доступ, обратитесь к предшествующим главам этой книги, если вам необходима помощь в установке упомянутых серверов.

1. Для начала войдите в систему Windows Server 2012 R2, присоединенную к домену, с помощью учетной записи, которая имеет административные разрешения на уровне домена. В окне диспетчера серверов (Server Manager) при выбранном пункте меню Local Server (Локальный сервер) щелкните на ссылке Add roles and features (Добавить роли и компоненты).
2. На экране Before you begin (Прежде чем начать) щелкните на кнопке Next (Далее).
3. На экране Select Installation Type (Выбор типа установки) проверьте, что выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов), и щелкните на кнопке Next.

4. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов), убедитесь, что ваш сервер выделен в разделе Server Pool (Пул серверов), и щелкните на кнопке Next.
5. На экране Select Server Roles (Выбор серверных ролей) выполните прокрутку экрана вниз до тех пор, пока не найдете в списке Roles (Роли) элемент Network Policy and Access Services (Службы сетевой политики и доступа), и отметьте флажок рядом с ним.
6. Затем вам будет предложено добавить некоторые требуемые здесь компоненты, такие как Remote Server Administration Tools (RSAT) (Инструменты дистанционного администрирования серверов (RSAT)), поэтому в открывшемся окне просто щелкните на кнопке Add Features (Добавить компоненты).
7. Для продолжения щелкните на кнопке Next.
8. На экране Select Features (Выбор компонентов) оставьте выбор компонентов в том виде, как есть, и два раза щелкните на кнопке Next.

   Когда вы доберетесь до экрана Select Role Services (Выбор служб ролей), в панели Role Services (Службы ролей) будут доступны три флажка (рис. 21.3).

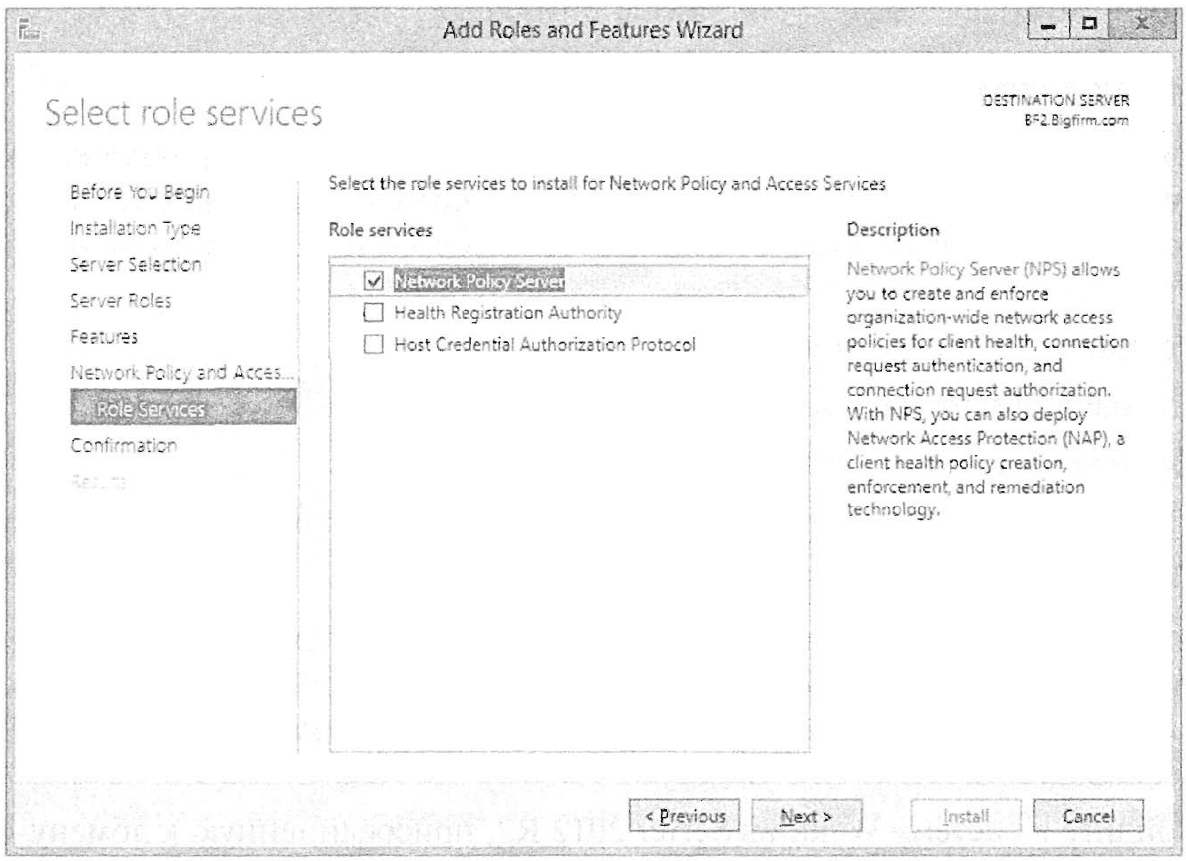


Рис. 21.3. Выберите службу роли

9. Отметьте флажок Network Policy Server (Сервер сетевой политики) и щелкните на кнопке Next.
10. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) просмотрите выбранные варианты и щелкните на кнопке Install (Установить), чтобы начать процесс установки.
11. После завершения установки щелкните на кнопке Close (Закрыть).

Использование роли Remote Access

Роль Remote Access включает значительно больше, чем просто возможность создания традиционного VPN-сервера. Ниже перечислены отдельные службы, предусмотренные в этой роли.

- **Remote Access Service (Служба удаленного доступа).** Служба Remote Access Service (RAS) применяется для подключения либо VPN-сервера, либо сервера коммутируемых подключений и предоставляет поддержку VPN для более старых клиентских компьютеров. Чтобы сервер можно было использовать в качестве VPN-сервера, он должен располагать, по меньшей мере, двумя NIC.
- **Routing (Маршрутизация).** Служба Routing обеспечивает программный маршрутизатор для оказания поддержки маршрутизаторам с такими возможностями, как Network Address Translation (NAT), Routing Information Protocol (RIP) и групповая передача.
- **DirectAccess.** Благодаря DirectAccess, пользователи прозрачно подключаются к корпоративной сети каждый раз, когда у их компьютеров, принадлежащих компании, имеется подключение к Интернету. Это возвращает организации более высокую степень контроля и управления мобильными компьютерами. Позже мы обсудим эту технологию подробнее.

Установка роли Remote Access

Поскольку вы уже развернули роль Network Policy and Access Services, ниже перечислены оставшиеся высокоуровневые шаги, которые вам придется выполнить, чтобы сконфигурировать свой сервер как VPN-сервер и установить подключение с клиентом.

1. Установите роль Remote Access.
2. Сконфигурируйте службу Routing and Remote Access Service.
3. Добавьте политики, чтобы разрешить подключения.
4. Сконфигурируйте разрешения на коммутируемые подключения пользователей.
5. Сконфигурируйте VPN-клиент и подключитесь.

В последующих разделах мы подробно пройдемся по этим шагам, чтобы помочь вам привести свой VPN-сервер в работоспособное состояние.

Далее описаны действия, которые понадобится выполнить, чтобы развернуть роль Remote Access.

1. Войдите в систему Windows Server 2012 R2, присоединенную к домену, с помощью учетной записи, которая имеет административные разрешения на уровне домена. В окне диспетчера серверов при выбранном пункте меню Local Server (Локальный сервер) щелкните на ссылке Add roles and features (Добавить роли и компоненты).
2. На экране Before you begin (Прежде чем начать) щелкните на кнопке Next (Далее).
3. На экране Select Installation Type (Выбор типа установки) проверьте, что выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов), и щелкните на кнопке Next.

4. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов), убедитесь, что ваш сервер выделен в разделе Server Pool (Пул серверов), и щелкните на кнопке Next.
5. На экране Select Server Roles (Выбор серверных ролей) выполните прокрутку экрана вниз до тех пор, пока не найдете в списке Roles (Роли) элемент Remote Access (Удаленный доступ) , и отметьте флажок рядом с ним.
6. Затем вам будет предложено добавить некоторые требуемые здесь компоненты, такие как RAS Connection Manager Administration Kit (CMAK) (Набор для администрирования диспетчера подключений RAS (CMAK)) и Web Server (IIS) (Веб-сервер (IIS)), поэтому в открывшемся окне просто щелкните на кнопке Add Features (Добавить компоненты).
7. Для продолжения щелкните на кнопке Next.
8. На экране Select Features (Выбор компонентов) оставьте выбор компонентов в том виде, как есть, и два раза щелкните на кнопке Next.

   Когда вы доберетесь до экрана Select Role Services (Выбор служб ролей), в панели Role Services (Службы ролей) будут доступны три флажка (рис. 21.4).

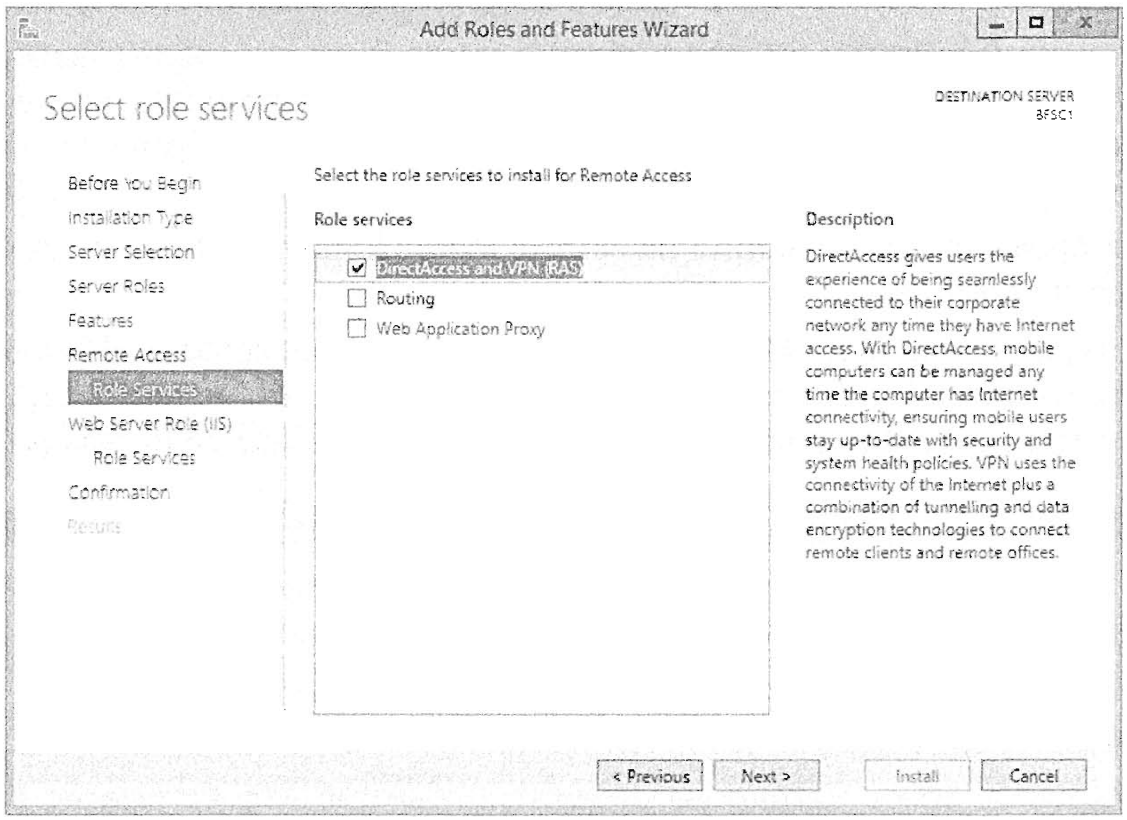


Рис. 21.4. Здесь также выберите службу роли

9. Отметьте флажок DirectAccess and VPN (RAS) (DirectAccess и VPN (RAS)) и три раза щелкните на кнопке Next, оставив стандартный выбор для параметров Web Server Role (IIS).
10. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) просмотрите выбранные варианты и щелкните на кнопке Install (Установить), чтобы начать процесс установки.
11. После завершения установки щелкните на кнопке Close (Закрыть).

Теперь, когда требуемая служба добавлена, ее еще предстоит сконфигурировать и либо добавить, либо модифицировать политики, прежде чем она сможет применяться в качестве VPN-сервера.

Совет относительно PowerShell: установка роли Remote Access

Используйте следующую простую команду PowerShell в качестве быстрой альтернативы развертывания роли Remote Access и связанных с нею инструментов дистанционного администрировании серверов (Remote Server Administration Tools):

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

Конфигурирование службы Routing and Remote Access Service

После установки роли Remote Access следующий этап заключается в конфигурировании службы Routing and Remote Access Service в качестве VPN-сервера. Управлять этой службой можно посредством диспетчера серверов или напрямую с помощью оснастки консоли MMC. Вы должны войти в систему компьютера Windows Server 2012 R2 с применением учетной записи, имеющей разрешения администратора домена, а не просто разрешения локального администратора.

1. В окне диспетчера серверов выберите меню Remote Access (Удаленный доступ) и обратите внимание на область с предупреждением, которое гласит Configuration required for DirectAccess and VPN (RAS) (Требуется конфигурирование для DirectAccess и VPN (RAS)).
2. Для продолжения щелкните на ссылке More (Дополнительно) в этой области предупреждения.
3. В открывшемся окне All Servers Task Details and Notifications (Подробности и уведомления обо всех серверных задачах), показанном на рис. 21.5, щелкните на ссылке Open the Getting Started Wizard (Открыть мастер начала работы).

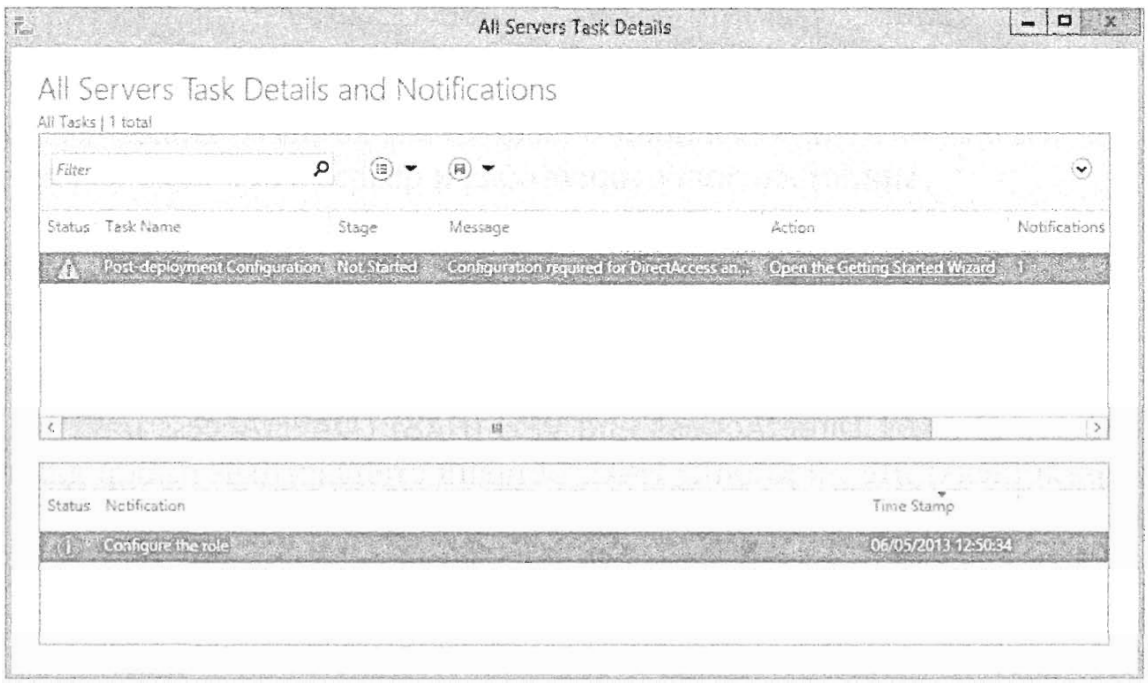


Рис. 21.5. Конфигурирование службы RRAS

Когда откроется мастер начала работы (Getting Started Wizard), вы получите на выбор три варианта развертывания: DirectAccess и VPN, только DirectAccess, только VPN.

4. Выберите переключатель Deploy VPN Only (Развернуть только VPN).

   Позже мы обсудим развертывание DirectAccess, но на данном этапе требуется только VPN.

5. В оснастке Routing and Remote Access (Маршрутизация и удаленный доступ) щелкните правой кнопкой мыши на имени вашего сервера и выберите в контекстном меню пункт Configure and Enable Routing and Remote Access (Конфигурировать и включить службу Routing and Remote Access), как показано на рис. 21.6.

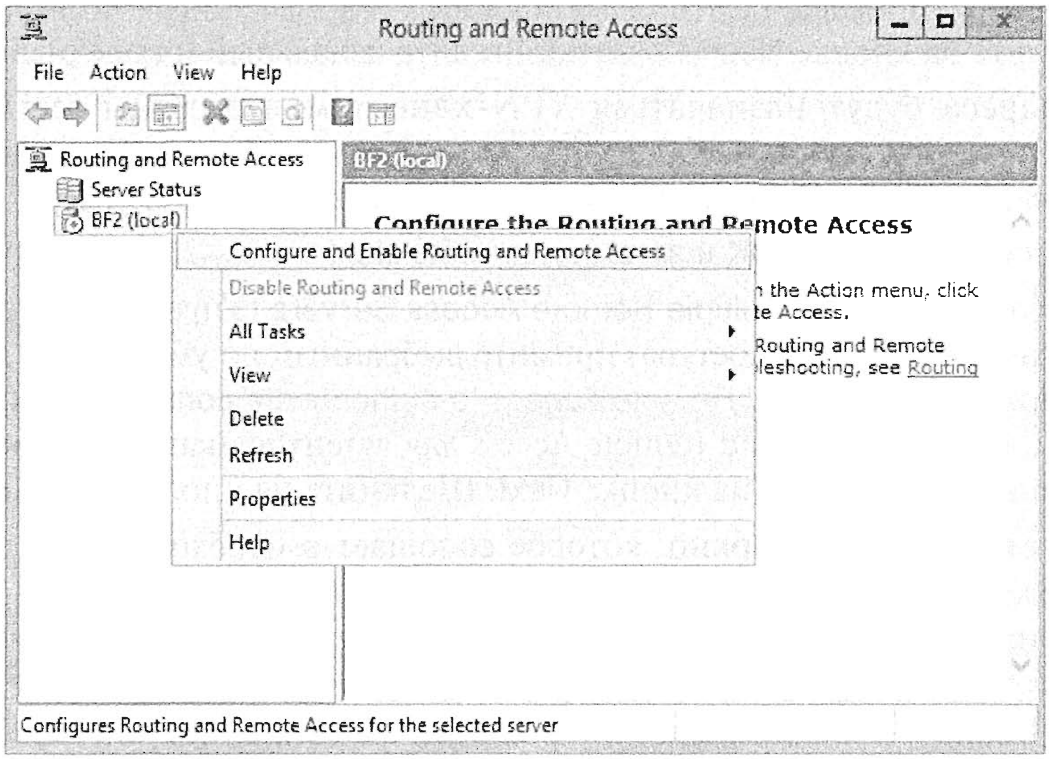


Рис. 21.6. Включение сервера RRAS

6. Это приведет к открытию мастера настройки сервера Routing and Remote Access (Routing and Remote Access Server Setup Wizard); щелкните на кнопке Next (Далее), чтобы продолжить.

Для VPN требуются две сетевые интерфейсные платы

Напоминаем, что для полного конфигурирования службы RRAS как VPN-сервера требуются две NIC. Тем не менее, если в наличии только одна NIC, вы все равно можете сконфигурировать RRAS так, чтобы можно было видеть и RRAS, и NPS. Вместо выбора на экране Configuration (Конфигурация) переключателя Virtual private network (VPN) access and NAT (Доступ к виртуальной частной сети (VPN) и NAT) выберите переключатель Custom configuration (Специальная конфигурация) и на появившемся экране Custom Configuration укажите варианты VPN access (Доступ к VPN) и NAT. После этого также понадобится открыть окно свойств сервера и на вкладке IPv4 добавить пул статических адресов.

---

7. На экране Configuration (Конфигурация) выберите переключатель Virtual private network (VPN) access and NAT (Доступ к виртуальной частной сети (VPN) и NAT) и щелкните на кнопке Next.
8. На экране VPN Connection (Подключение с VPN) выберите NIC, которая подключена к Интернету.

   В нашей системе мы переименовали NIC, видимую из Интернета, выбрали ее и эмулировали открытый IP-адрес, назначив ему 74.1.2.3.
9. Удостоверившись в правильности выбранных параметров, щелкните на кнопке Next.
10. На экране IP Address Assignment (Назначение IP-адреса) выберите переключатель From a specified range of addresses (Из указанного диапазона адресов) и щелкните на кнопке Next.
11. Щелкните на кнопке New (Создать). Введите начальный и конечный IP-адреса.

    Эти адреса будут назначаться VPN-клиентам и должны быть выбраны для разрешения доступа в сеть. В данном случае был выбран диапазон от 192.168.20.200 до 192.168.20.250, используемый в качестве примера.
12. Щелкните на кнопке OK и затем на кнопке Next.
13. На экране Managing Multiple Remote Access Servers (Управление несколькими серверами удаленного доступа) примите выбранный по умолчанию переключатель No, use Routing and Remote Access to authenticate connection requests (Нет, использовать Routing and Remote Access для аутентификации запросов на подключение) и щелкните на кнопке Next. Щелкните на кнопке Finish (Готово).

    Откроется диалоговое окно, которое сообщает о необходимости добавления промежуточного агента передачи DHCP, если для предоставления IP-адресов применяется DHCP. Это не имеет отношения к случаю использования статического диапазона IP-адресов, с которым мы здесь имеем дело.
14. Ознакомьтесь с информацией и щелкните на кнопке OK, чтобы закрыть это диалоговое окно.
15. При появлении уведомления о политике запросов на подключение NPS щелкните на кнопке OK, после чего щелкните на кнопке Start Service (Запустить службу) во всплывающем диалоговом окне, чтобы запустить службу RRAS.

С этого момента VPN-сервер будет присоединен к домену с установленной и сконфигурированной службой Routing and Remote Access Service. Однако клиенты не смогут подключаться до тех пор, пока не будет сконфигурирована политика доступа к сети.

Конфигурирование политик

Политики доступа к сети являются неотъемлемой составляющей обеспечения безопасного и контролируемого доступа к VPN. Если клиент не удовлетворяет условиям любой политики, он не сможет установить подключение. Если у VPN-сервера отсутствуют какие-либо политики, клиенты не смогут удовлетворять условиям несуществующих политик, следовательно, не смогут подключаться. Установленная ранее служба сервера сетевой политики (Network Policy Server — NPS) является тем самым местом в Windows Server 2012 R2, где производится управление такими политиками.

Службу NPS можно применять для создания и активизации политик доступа к сети в масштабах всей организации. Хотя эта глава сосредоточена на удаленном доступе, NPS можно использовать для создания дополнительных политик, позволяющих проверять любые компьютеры, в том числе и компьютеры во внутренней сети. Компьютеры, которые не удовлетворяют условиям, заранее определенным администратором, могут быть поставлены на карантин, и таким компьютерам может быть отказано в доступе к сети.

Политики конфигурируются внутри консоли NPS, обратиться к которой можно двумя разными методами. Однако возможности этой консоли зависят от того, каким способом к ней производится доступ.

- **Запуск из оснастки Routing and Remote Access.** В оснастке Routing and Remote Access вы можете щелкнуть правой кнопкой мыши на элементе Remote Access Logging & Policies (Ведение журналов и политики удаленного доступа) и выбрать в контекстном меню пункт Launch NPS (Запустить NPS). В случае запуска подобным образом консоль NPS отобразит только параметры, которые напрямую связаны со службой RRAS. Консоль в верхней части рис. 21.7 была запущена из RAS и в этой главе ей уделяется основное внимание.

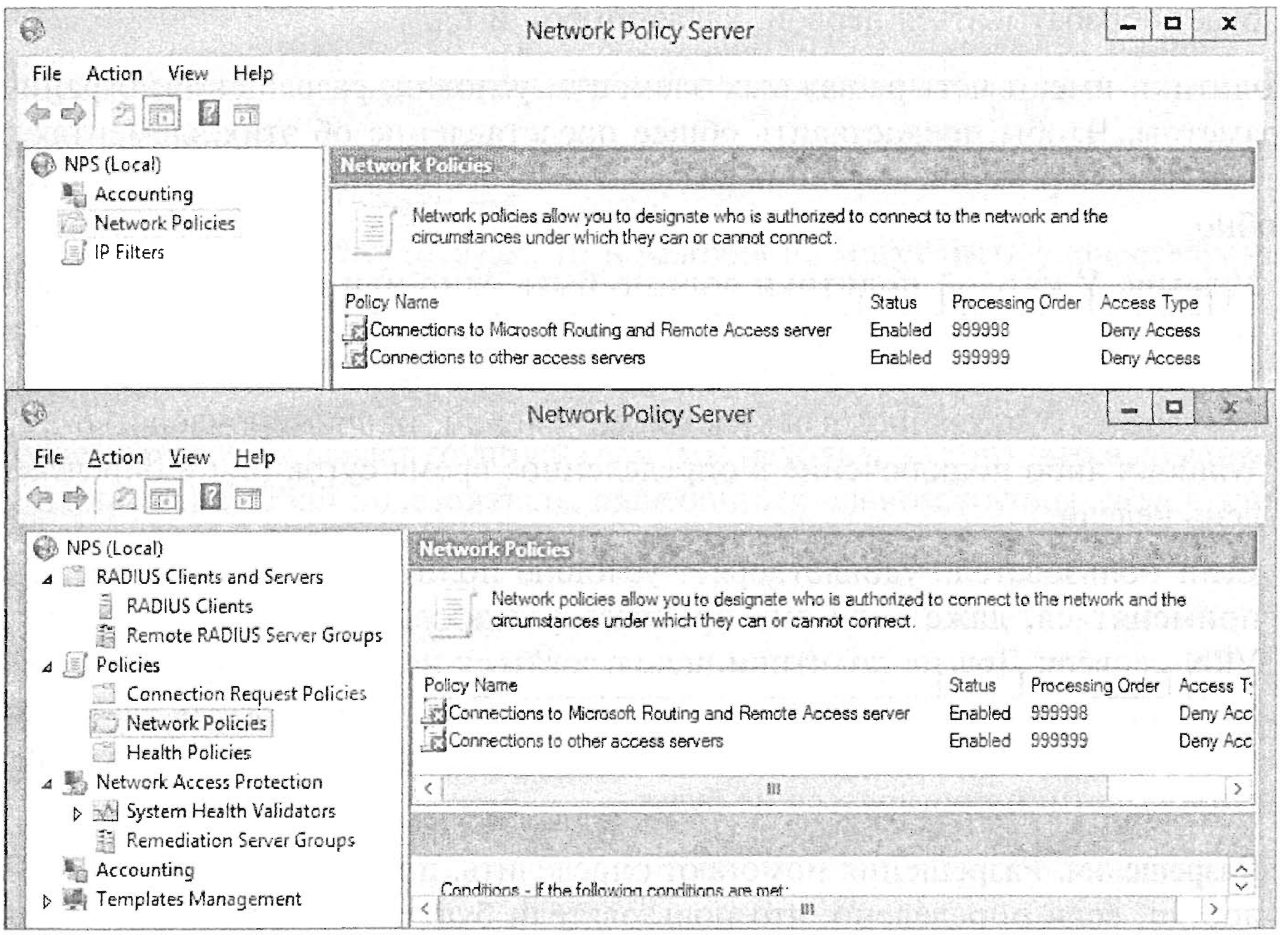


Рис. 21.7. Консоль Network Policy Server при запуске из RRAS (вверху) и при запуске из меню Tools (внизу)

- **Запуск через меню Tools (Сервис).** В случае запуска путем выбора в окне диспетчера серверов пункта меню Tools⇨Network Policy Server (Сервис⇨Сервер сетевой политики) становятся доступными многие дополнительные инструменты. Консоль в нижней части рис. 21.7 была запущена из меню Tools.

В узле Network Policies (Сетевые политики) консоли NPS содержатся две стандартные политики. Каждая из них при создании устанавливается в Deny Access (Отказать в доступе), но при желании это можно изменить. Эти две политики описаны ниже.

- **Connections to Microsoft Routing and Remote Access Server Policy (Подключения к Microsoft Routing и политика сервера удаленного доступа).** Включает единственное условие, согласно которому клиент RADIUS должен быть клиентом Microsoft (указанным как MS-RAS Vendor ^311$). Эта политика применима только к клиентам RADIUS.
- **Connections to Other Access Servers (Подключения к другим серверам доступа).** Включает единственное условие подключения в любое время суток и в любой день недели. Если никакие другие условия не удовлетворены предыдущими политиками, то будет использоваться именно эта политика. Обратите внимание, что порядок обработки начинается со стандартного 999999, представляющего собой наибольшее число, которое может быть назначено. Хотя у вас нет возможности назначить порядок обработки напрямую, этот порядок можно модифицировать, указывая подобным образом на то, какая политика будет обрабатываться первой, какая второй и т.д.

Политики имеют четыре важных элемента: условия, разрешения, ограничения и параметры. Чтобы предоставить общее представление об этих элементах, ниже приведен их обзор. В последующих разделах мы рассмотрим каждый элемент более подробно.

- **Условия.** У каждой политики должно быть одно или несколько условий, которые должны удовлетворяться, чтобы соответствующий клиент мог применять данную политику. Если условие не выполняется, политика не будет использоваться. Можно указывать много условий, например, членство в группе Windows либо подключение в определенное время суток или в определенный день недели.

  Если пользователь удовлетворяет условию политики, то эта политика будет применяться, даже если она препятствует доступу данного пользователя к VPN-серверу. Другие политики использоваться не будут. Рассмотрим для примера VPN-сервер, имеющий пять политик. Если пользователь удовлетворяет условию первой политики, а эта политика запрещает доступ, то остальные четыре политики проверяться не будут.

- **Разрешения.** Разрешения помогают определить, предоставлен ли пользователю доступ, если определено, что пользователи будут использовать эту политику (удовлетворяя условиям политики). На первый взгляд разрешения выглядят простыми, т.к. они могут быть установлены в Grant Access (Предоставить доступ) или Deny Access (Отказать в доступе). Тем не менее, параметры учетных записей индивидуальных пользователей могут переопределять разрешение политики, а политика может быть настроена на переопределение параметра учетной записи пользователя. По мере углубления в данную тему вы обнаружите, что разрешения не сводятся к одним лишь установкам Grant Access и Deny Access.

- **Ограничения.** Ограничения можно применять для обеспечения того, что клиенты следуют определенным правилам для подключения. Ограничения включают методы аутентификации, тайм-ауты для сеанса или время бездействия и т.д. Если пользователь выполняет условие и располагает разрешением, но не удовлетворяет одному из ограничений, в подключении ему будет отказано.
- **Параметры.** Параметры применяются, если пользователь удовлетворяет условиям и ограничениям политики. Параметры включают опции группы каналов передачи данных и выделения полосы частот, варианты шифрования, параметры IP-адресов и IP-фильтры.

Условия политики и порядок обработки политики

Установка и понимание условий играет очень важную роль для политик. Ниже перечислены основные правила, которые управляют политиками.

- Чтобы использовать политику, пользователь должен удовлетворять всем ее условиям.
- Пользователь будет использовать только первую политику, для которой удовлетворены все условия.
- Если пользователь получил отказ в доступе от политики, условия которой удовлетворены, дополнительные политики не оцениваются.
- Если пользователь не удовлетворяет условиям любой политики, доступ не может быть предоставлен.
- Если политики отсутствуют, то и условия не могут быть удовлетворены, а доступ не может быть предоставлен.

В качестве простого примера предположим, что вам нужно сконфигурировать политику для пользователей в группе `Sales`. Вы можете создать для этой политики условие, которое включает группу `Sales` (мы исходим из того, что в домене имеется группа `Sales`). Любой пользователь, являющийся членом группы `Sales`, удовлетворяет этому условию, и политика будет применена.

Понятие порядка обработки политики

Политики оцениваются в специфичном порядке, и при создании политик важно учитывать логику каждой из них, чтобы определить, какая политика будет использоваться. Представьте, что после создания политики для группы `Sales` у вас имеются три административно созданных политики с условиями и разрешениями, которые описаны в табл. 21.1.

Таблица 21.1. Оценка условий политики

Название политики	Условия	Разрешение
`Domain Users`	Член группы `Domain Users`	Deny Access (Отказать в доступе)
`IT Admins`	Член группы `IT Admins` в домене	Grant Access (Отказать в доступе)
`Sales`	Член группы `Sales` в домене	Grant Access (Отказать в доступе)

Эти политики показаны на рис. 21.8. Здесь следует обратить внимание на то, что каждая политика включает порядок обработки. Политика Domain Users находится в самом верху с порядком обработки 1, политика IT Admins имеет порядок обработки 2 и т.д. Подобным способом идентифицируется порядок, в соответствии с которым будут оцениваться данные политики, и это помогает выявить серьезный просчет в текущем проектном решении.

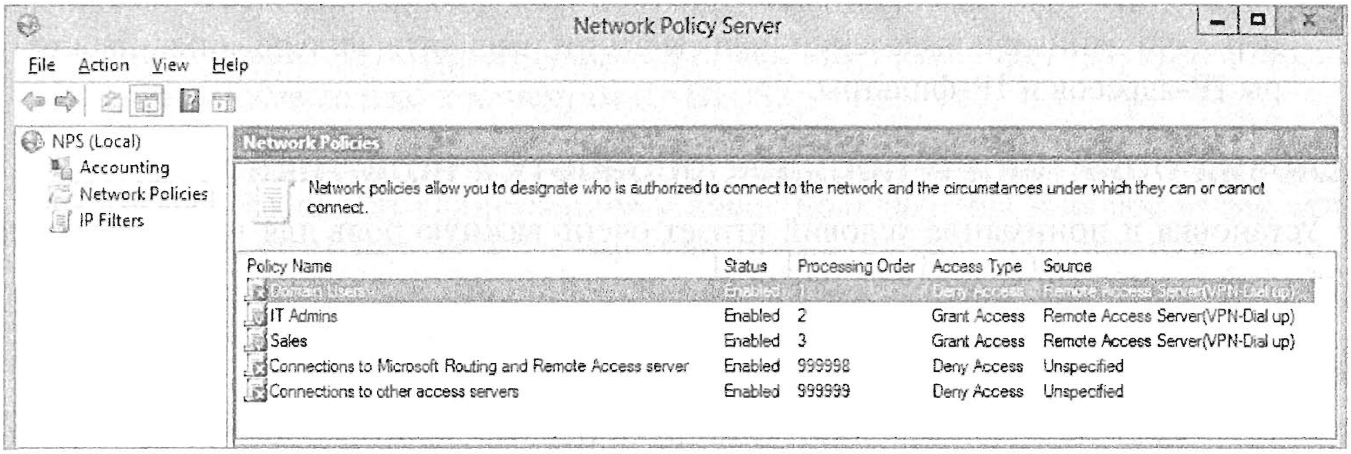


Рис. 21.8. Политики доступа к сети

В рассматриваемом примере всегда применялась бы только первая политика (Domain Users). Любой пользователь, входящий в состав либо группы IT Admins, либо группы Sales, является членом этого домена, и также был бы членом группы Domain Users. Из-за того, что эти пользователи являются членами группы Domain Users, они удовлетворяли бы условиям первой политики и использовали бы эту политику. В итоге политики IT Admins и Sales никогда бы не применялись, а поскольку политика Domain Users установлена в Deny Access, то никто из пользователей никогда не получил бы доступ в сеть.

Тем не менее, эта проблема легко разрешима. Щелкнув правой кнопкой мыши на любой из этих политик, вы можете выбрать в контекстном меню пункт Move Up (Переместить вверх) или Move Down (Переместить вниз) и изменить порядок обработки. В табл. 21.2 представлен более подходящий порядок обработки. Вообще говоря, политики должны быть упорядочены от наиболее специфичных к наименее специфичным, но соответствующую логику необходимо обдумать в любом случае.

Таблица 21.2. Изменение порядка обработки политик

Название политики	Условия	Разрешение	Порядок обработки политик
IT Admins	Член группы IT Admins в домене	Grant Access (Предоставить доступ)	1
Sales	Член группы Sales в домене	Grant Access (Предоставить доступ)	2
Domain Users	Член группы Domain Users	Deny Access (Отказать в доступе)	3

К политике можно добавлять более одного условия. Если политика включает несколько условий, то для ее использования должны быть удовлетворены все эти условия. Можно применять условия следующих категорий: Groups (Группы), Host Credential Authorization Protocol (HCAP) (Протокол авторизации учетных данных

хостов (HCAP)), Day and Time Restrictions (Ограничения дня и времени), Connection Properties (Свойства подключения), RADIUS Client Properties (Свойства клиента RADIUS) и Gateway (Шлюз).

Использование условия Groups

Условие Groups можно применять для ограничения доступа только определенными пользователями или компьютерами. Допускается добавлять любую действительную группу, которая поддерживается внутри домена, или любую локальную группу, поддерживаемую на индивидуальных системах. Здесь могут включаться группы Windows, группы компьютеров или группы пользователей.

Использование групп может быть эффективным способом идентификации пользователя, который пытается получить доступ к VPN-серверу. Например, если вы хотите, чтобы пользователи в группе `IT Admins` могли устанавливать подключение в любое время, а пользователи в группе `Sales` — только в определенные моменты, можете создать две политики с одним условием для каждой группы. После этого можно сконфигурировать ограничения, чтобы ограничить доступ указанным временем.

Использование условия Host Credential Authorization Protocol

Протокол HCAP можно применять для коммуникаций между NPS и серверами сетевого доступа от независимых разработчиков. Если все VPN-серверы произведены Microsoft, то использовать HCAP не следует. Тем не менее, HCAP позволяет поддерживать гибридную среду с разными типами VPN-серверов.

Использование условия Day and Time Restrictions

На рис. 21.9 представлен экран Day and Time Restrictions (Ограничения дня и времени). Предположим, что вы зарезервировали время от полуночи до 4 часов утра для проведения техобслуживания на сервере и хотите гарантировать, что в этот период сервер не будет принимать запросы на подключение. Настройки можно было бы сконфигурировать, как описано ниже.

Условие Day and Time Restrictions является наиболее часто используемым при управлении доступом к VPN-серверу. Позже вы увидите, что условие Day and Time Restrictions можно также применять в качестве ограничения.

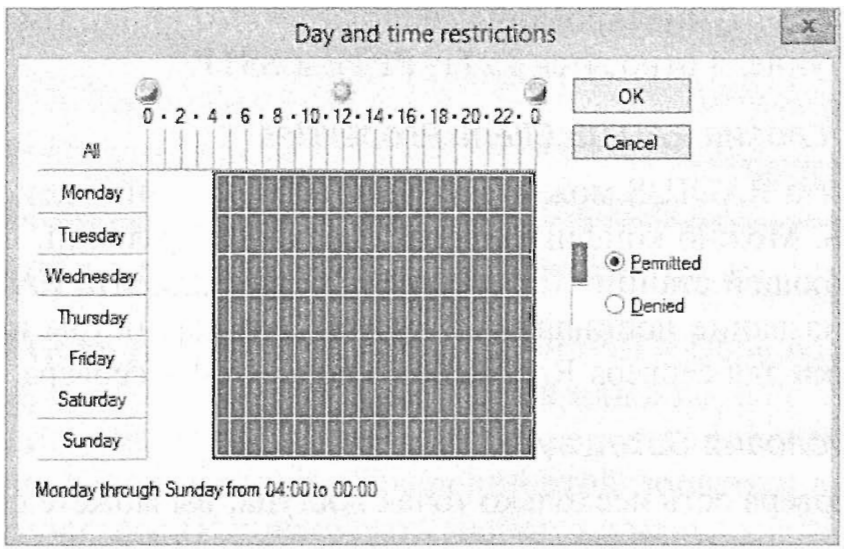


Рис. 21.9. Ограничение доступа с использованием условия Day and Time Restrictions

Использование условия Connection Properties

Категория Connection Properties включает несколько разных протоколов и деталей, касающихся протокола, который может быть затребован клиентом. Доступные настройки перечислены ниже.

- **Access Client IPv4 and IPv6 Addresses (Адреса IPv4 и IPv6 для доступа клиента).** Вы можете указать для клиента определенный IP-адрес или IP-подсеть. Это может быть полезно в сетях VPN типа "шлюз-шлюз", когда удаленный офис подключается к головному офису посредством VPN. Если удаленный офис имеет конкретный IP-адрес, остающийся неизменным, то условие может указывать этот IP-адрес.
- **Authentication Type (Тип аутентификации).** Протоколы аутентификации применяются для того, чтобы разрешить клиенту подтвердить свое удостоверение. Можно использовать множество разных типов аутентификации, и они могут быть заданы в разделе условия или в разделе ограничений.
- **Allowed EAP Types (Разрешенные типы EAP).** Расширяемый протокол аутентификации (Extensible Authentication Protocol — EAP) применяется для разрешения протоколов расширенной аутентификации. Это позволяет использовать смарт-карты и другие более надежные методы аутентификации.
- **Framed Protocol (Фреймовый протокол).** Фреймовые протоколы включают PPP (Point-to-Point Protocol — протокол типа "точка-точка") и SLIP (Serial Line Internet Protocol — межсетевой протокол для последовательного канала). Самым распространенным типом является PPP, который применяется клиентом для первоначального подключения к Интернету. Например, клиент мог бы войти в Интернет, а затем воспользоваться протоколом туннелирования, чтобы получить доступ к VPN-серверу через Интернет. Поддерживается также ряд других фреймовых протоколов, которые встречаются реже.
- **Service Type (Тип службы).** Вы можете указать, какой тип службы использует клиент, наподобие фреймового протокола с обратным вызовом (Callback Framed) или фреймового (Framed) протокола.
- **Tunnel Type (Тип туннеля).** Параметр Tunnel Type может применяться для указания протокола туннелирования, используемого клиентом. К поддерживаемым типам туннеля относятся L2TP, PPTP и SSTP.

Использование условия RADIUS Client Properties

Свойства клиента RADIUS можно применять для указания деталей, касающихся клиентов RADIUS. Можно конфигурировать несколько условий, в том числе идентификатор вызывающей станции, дружественное имя клиента RADIUS, адрес IPv4 или IPv6 и даже название поставщика клиента. Эти параметры используются при настройке политики для сервера RADIUS, но не для VPN-сервера.

Использование условия Gateway

Если у VPN-сервера есть несколько точек доступа, вы можете сконфигурировать шлюз, гарантировав таким образом, что клиенты будут обращаться к нему определенным способом. Условиями для шлюза могут быть вызываемый телефонный номер, имя сервера, адрес IPv4 или IPv6 и тип порта.

Предположим, что на VPN-сервере установлены две NIC с разными открытыми IP-адресами. В распоряжении одной NIC может быть достаточно широкая полоса пропускания, тогда как у другой NIC ее нет. Вы можете ограничить доступ к NIC с более широкой полосой пропускания избранной группой, комбинируя условие шлюза и условие группы Windows.

Установка разрешений политики

На разрешения политики могут влиять несколько разных элементов. На рис. 21.10 показана вкладка Overview (Обзор) окна свойств политики. Разрешения доступа находятся в ее центре.

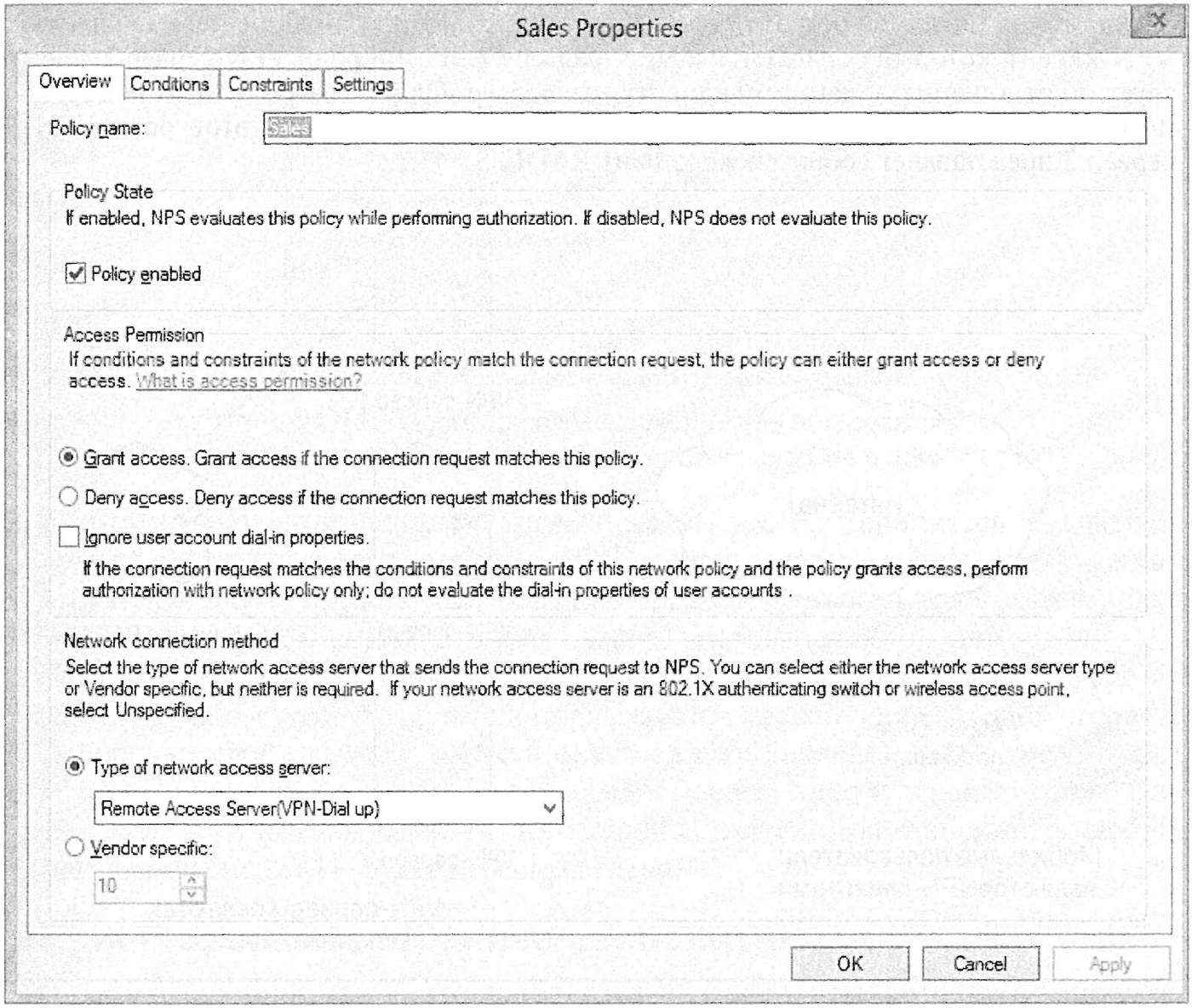


Рис. 21.10. Просмотр разрешений доступа внутри политики доступа

Разрешения Grant Access (Предоставить доступ) и Deny Access (Отказать в доступе) означают, что доступ будет предоставлен или в доступе будет отказано, когда условие политики удовлетворено, но только если учетная запись пользователя сконфигурирована на использование разрешений этой политики и флажок Ignore user account dial-in properties (Игнорировать свойства дозвона учетной записи пользователя) не отмечен. Свойства учетной записи пользователя устанавливаются для учетной записи Active Directory этого пользователя.

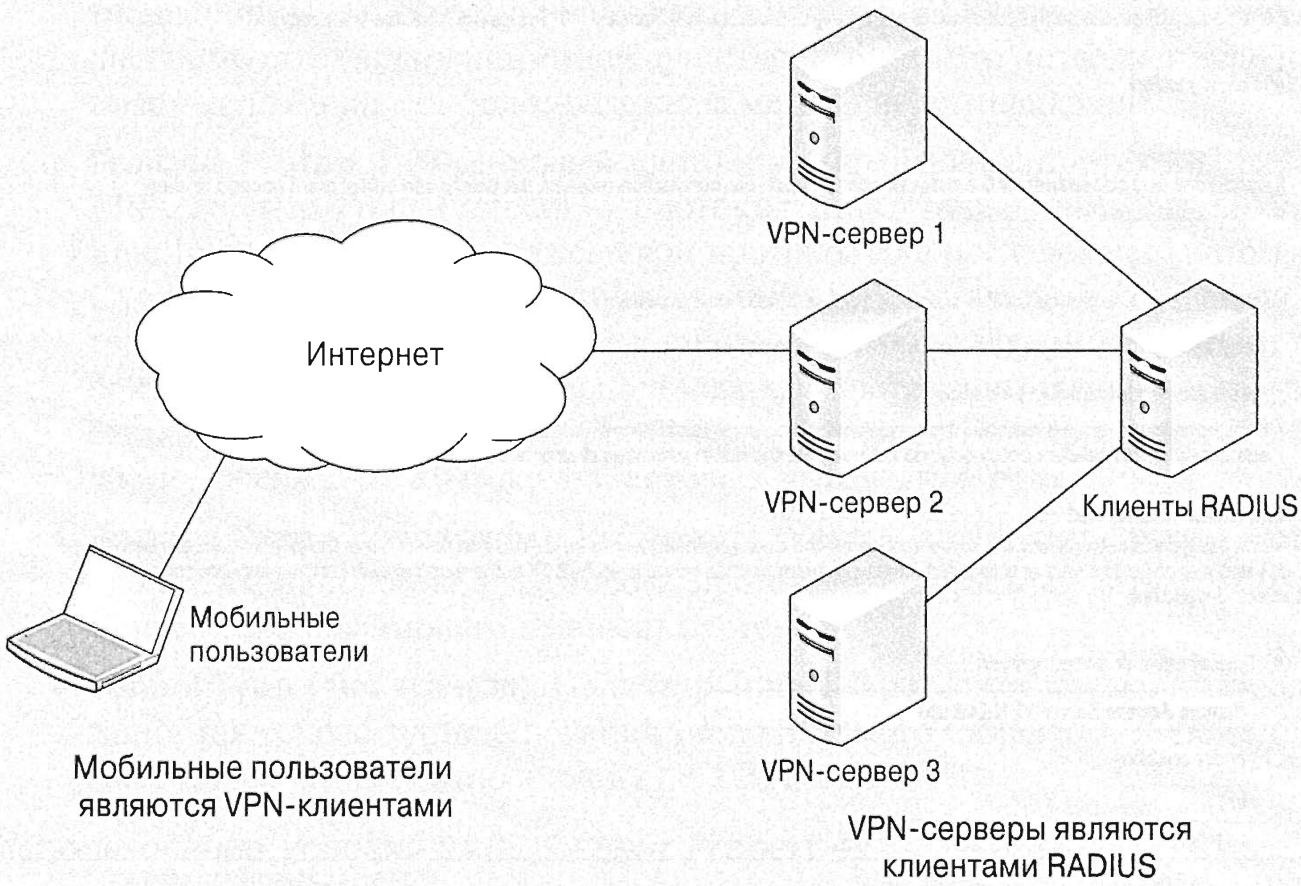
Пример из практики

Клиент RADIUS или VPN-клиент?

Термин *клиент RADIUS* иногда понимают неправильно. Когда используется RADIUS, конечным пользователем не является клиент RADIUS. Напротив, VPN-сервер является клиентом RADIUS.

Предположим, что у вас есть несколько VPN-серверов. Вы могли бы установить компонент NPS на другом сервере, чтобы он выступал в качестве сервера RADIUS и центральной точки аутентификации для всех VPN-серверов. Тогда вместо аутентификации клиента каждым VPN-сервером они могут передавать запросы аутентификации серверу RADIUS.

Взгляните на показанный в этой врезке рисунок. Конечным пользователем является VPN-клиент, который обращается к VPN-серверу 2. В этой роли VPN-сервер 2 действует по отношению к данному клиенту как сервер. Однако затем этот VPN-сервер передает учетные данные аутентификации серверу RADIUS, и в этой роли VPN-сервер 2 представляет собой также клиент RADIUS.



На рис. 21.11 показано окно свойств учетной записи пользователя с выбранной вкладкой Dial-in (Дозвон). Область Network Access Permission (Разрешение на доступ к сети) содержит три переключателя: Allow access (Разрешить доступ), Deny access (Отказать в доступе) и Control access through NPS Network Policy (Управлять доступом посредством сетевой политики NPS). Как видите, выбран переключатель Control access through NPS Network Policy, поэтому будут использоваться разрешения политики. Однако если выбрать здесь переключатель Allow access или Deny access, то разрешения политики не получат более высокий приоритет, если только не предпринять дополнительный шаг.

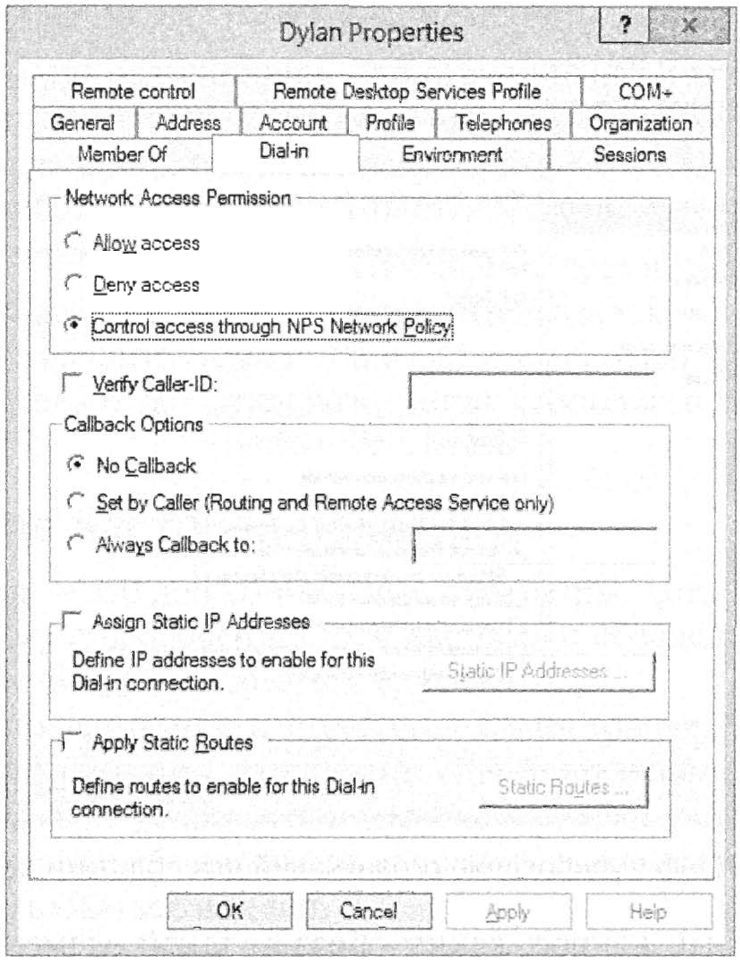


Рис. 21.11. Просмотр разрешений доступа пользователя к сети в оснастке Active Directory Users and Computers

Возможно, вам не дают покоя тревожные мысли. Не торопитесь. Вы должны установить разрешение на доступ для каждого пользователя в сети? В случае пяти пользователей это не представляет большой проблемы, но если пользователей 5000, это займет немало времени. К счастью, существует более простой способ.

Если вы снова взглянете на рис. 21.10, то заметите в разделе Access Permission (Разрешение на доступ) третий вариант: флажок Ignore user account dial-in properties (Игнорировать свойства дозвона учетной записи пользователя). Вы можете отметить его в дополнение либо к переключателю Grant Access, либо к переключателю Deny Access. Если этот флажок отмечен, то настройка для учетной записи пользователя, показанная на рис. 21.11, будет переопределена.

Конфигурирование ограничений политики

Ограничения политики — это дополнительные элементы, которые можно сконфигурировать для управления подключениями. Затем ограничения можно применять для отказа в доступе или отключения пользователей на основе других классификаций.

На рис. 21.12 показана вкладка Constraints (Ограничения) окна свойств политики доступа к сети. Возможно, вы заметили определенное пересечение с условиями и ограничениями. Следующие четыре элемента могут быть сконфигурированы либо как условия, либо как ограничения: Authentication Methods (Методы аутентификации), Called Station ID (Идентификатор вызывающей станции), Day and Time Restrictions (Ограничения дня и времени) и NAS Port Type (Тип порта NAS).

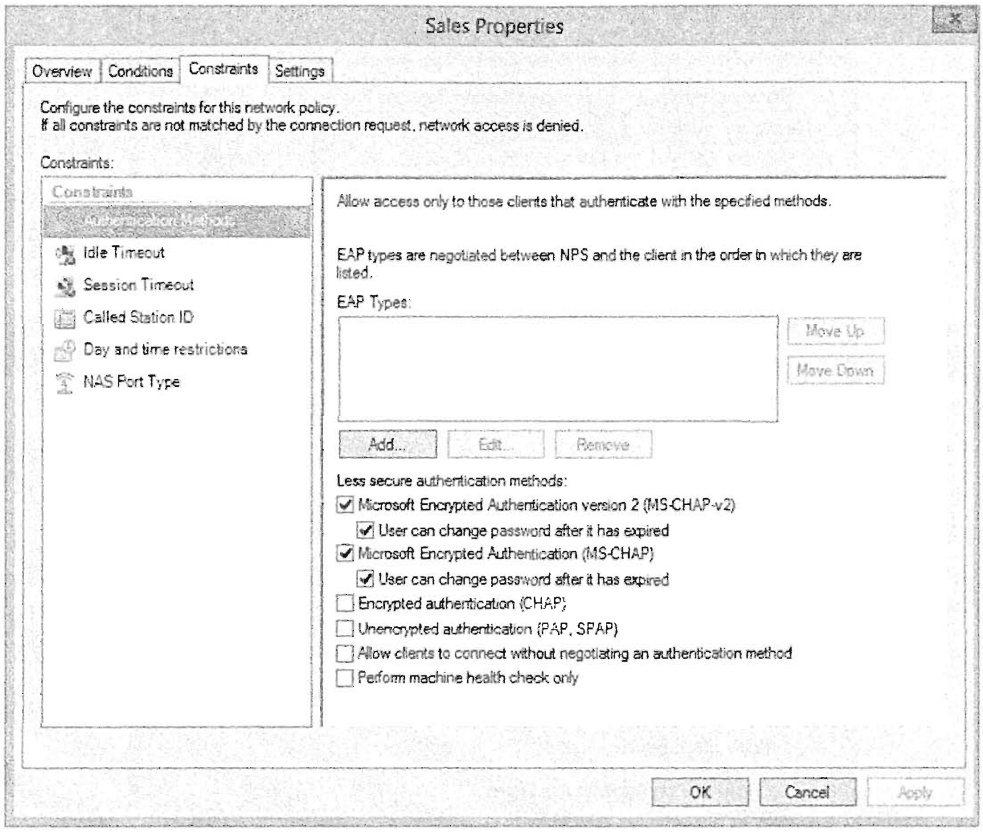


Рис. 21.12. Конфигурирование ограничений для политики доступа к сети

Возникает логичный вопрос, каким образом такой элемент должен использоваться — как условие или как ограничение? Ответ на него определяется назначением условия — условие предназначено для идентификации применяемой политики. Вспомните, что для использования политики должны быть удовлетворены все ее условия, а затем вы устанавливаете разрешения, ограничения и параметры, чтобы дополнительно ограничить или управлять подключением.

Предположим, что вы хотите предоставить пользователям группы `Sales` возможность подключения в любое время суток и в любой день недели, но членам группы Domain Users — только с 7 часов утра до 5 часов вечера, с понедельника по пятницу включительно. Для этого можно было бы создать две политики:

Политика 1

Условие: группа `Sales`, выбран переключатель Allow access

Ограничения: нет

Политика 2

Условие: группа `Domain Users`, выбран переключатель Allow access

Ограничения: с 7 утра до 5 вечера, с понедельника по пятницу

Если пользователи в группе `Sales` обращаются к серверу, они будут применять политику 1, основанную на условии группы `Sales`, а ограничения не лимитируют их доступ. Если к серверу обращается любой пользователь домена, который не входит в группу `Sales`, он будет использовать политику 2, основанную на условии группы `Domain Users`. Если пользователи группы `Domain Users` обращаются к серверу с 7 утра до 5 вечера с понедельника по пятницу, то подключение будет установлено. Однако если они обратятся к серверу в любое другое время, то по-прежнему будут применять политику 2, но ограничение предотвратит подключение.

Ниже указаны два дополнительных ограничения.

- Idle Timeout (Тайм-аут бездействия). Это ограничение можно сконфигурировать, чтобы закрывать подключение, если сеанс простаивает в течение определенного периода времени, точно так же, как хранитель экрана можно настроить на активизацию, когда система находится в состоянии бездействия.
- Session Time-out (Тайм-аут сеанса). Суммарное время подключения можно сконфигурировать для управления продолжительностью сеанса пользователя. Например, если разрешить Session Time-out и установить продолжительность в 60, то пользователь будет отключен, когда продолжительность его сеанса превысит 60 минут.

Конфигурирование настроек политики

Настройки политики — это дополнительные параметры, которые можно применить к соответствующему подключению. Эти настройки обеспечивают добавочные возможности, которыми могут пользоваться клиенты.

Разница между ограничениями и настройками очень тонкая. Ограничения применяются для гарантирования того, что клиент VPN будет использовать определенные элементы, и не позволят установить подключение, если клиент не задействует данные элементы. Настройки обеспечивают дополнительные возможности, которыми клиенты вольны пользоваться или нет.

На рис. 21.13 показана вкладка Settings (Настройки) окна свойств политики. Настройки в разделе RADIUS Attributes (Параметры RADIUS) применимы лишь в случае, если сервер используется как сервер RADIUS. К VPN-серверу применяются четыре настройки из раздела Routing and Remote Access (Маршрутизация и удаленный доступ).

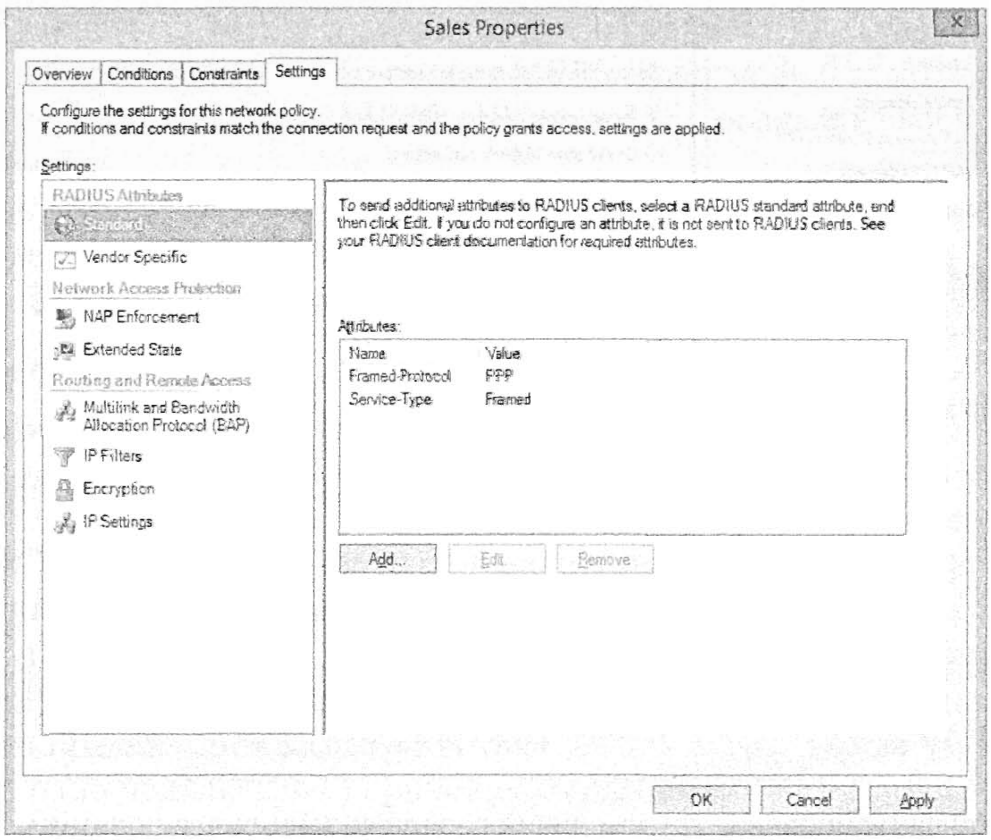


Рис. 21.13. Конфигурирование настроек для политики доступа к сети

Группа линий передачи данных и протокол распределения полосы пропускания

Группа линий передачи данных (Multilink) позволяет клиентам использовать для подключения несколько линий. Хотя это не является распространенной практикой применительно к сети VPN, такой подход может быть полезен в случае коммутируемых подключений. Если пользователь подключается посредством одной телефонной линии, он ограничен модемом 56 Кбит/с, но на телефонной линии даже такой модем ограничен скоростями менее 56 Кбит/с.

Если же в распоряжении клиента есть две телефонных линии и два модема, а у сервера также имеется, по меньшей мере, две телефонных линии и два модема, то этот клиент может установить одно совместно используемое подключение по двум телефонным линиям и двум модемам.

При существовании группы линий передачи данных также может применяться протокол распределения полосы пропускания (Bandwidth Allocation Protocol — BAP) для динамического закрытия неиспользуемых Multilink-подключений. Другими словами, если пользователь установил подключение с помощью двух Multilink-подключений, но задействовал только небольшую часть полосы пропускания, то BAP может рассоединить неиспользуемую линию, предоставив ее в распоряжение другого пользователя.

На рис. 21.14 показана вкладка Settings для Multilink и BAP со стандартными параметрами.

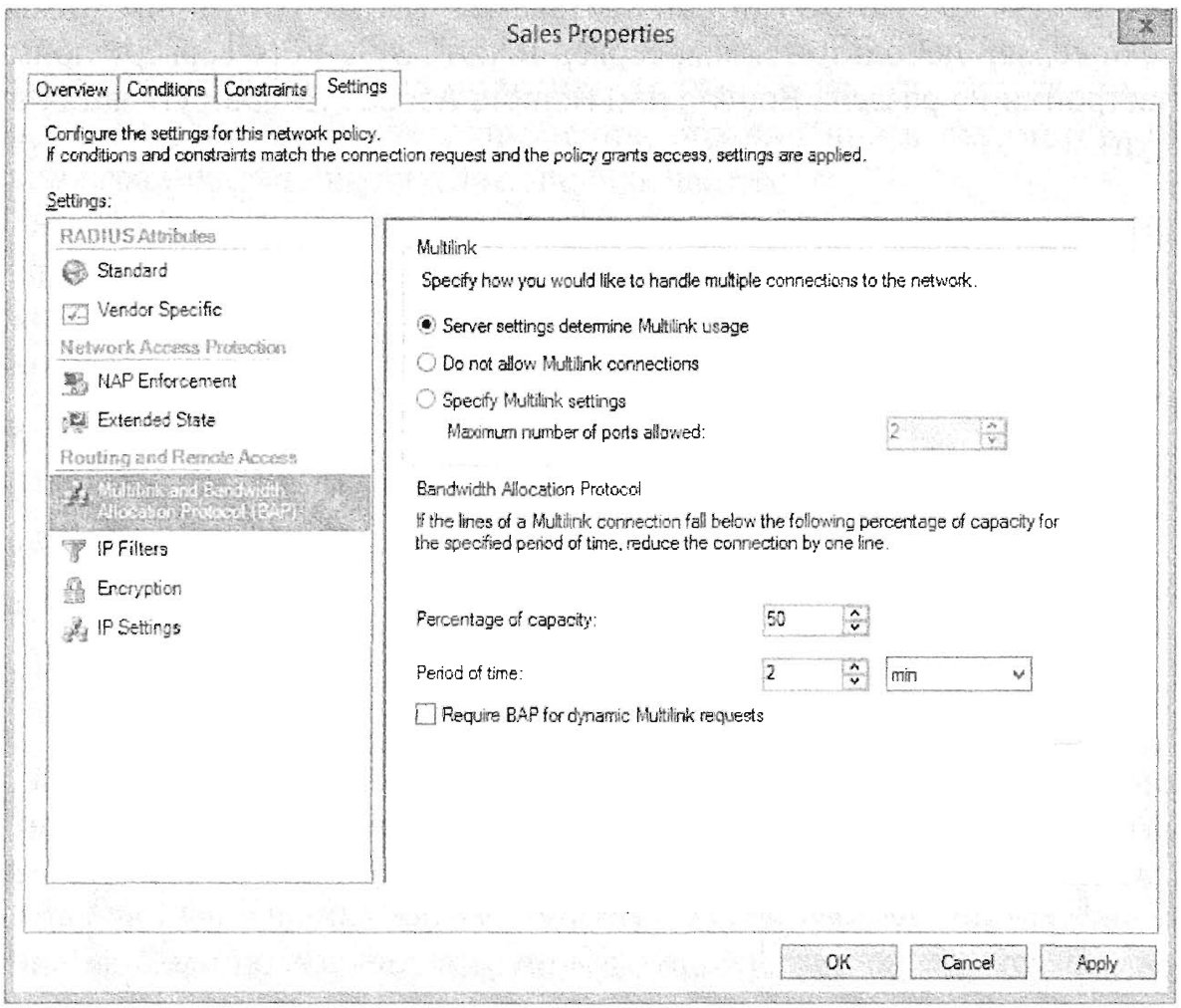


Рис. 21.14. Конфигурирование группы линий передачи данных для политики доступа к сети

IP-фильтры

Для управления трафиком, проходящим через подключение, можно использовать входные и выходные фильтры IPv4 и IPv6. Конфигурируемые настройки относятся к тому же типу, что и настройки базового маршрутизатора с фильтрацией пакетов.

Пакеты можно фильтровать на основе IP-адресов, подсетей, протоколов и портов. Если, например, предполагается, что VPN-клиенты должны иметь доступ только к одной подсети в рамках сети, можно было бы создать фильтр, обеспечивающий предоставление доступа к этой подсети, но не к другим. Аналогично, можно предусмотреть фильтр для блокирования доступа к конкретной подсети и предоставления доступа ко всем остальным подсетям.

Настройки шифрования

Настройки шифрования помогают определить, какой вид шифрования будет применяться для подключения. Шифрование будет кодировать данные таким образом, чтобы в случае перехвата максимально затруднить их декодирование. В разделе Encryption (Шифрование) предлагаются четыре варианта шифрования:

- Basic Encryption (MPPE 40-bit) (Базовое шифрование (MPPE с 40 битами))
- Strong Encryption (MPPE 56-bit) (Устойчивое шифрование (MPPE с 56 битами))
- Strongest Encryption (MPPE (128-bit) (Самое устойчивое шифрование (MPPE с 128 битами))
- No Encryption (Без шифрования)

Действительно используемое шифрование определяется другими протоколами. Например, если вы имеете дело с протоколом PPTP, то он будет применять шифрование MPPE (Microsoft Point-to-Point Encryption — двух точечное шифрование Microsoft) с указанным количеством битов. Тем не менее, если вы используете протокол L2TP, то вместо MPPE он будет применять IPSec, а в случае протокола Secure Socket Tunneling Protocol (SSTP) вместо MPPE будет использоваться SSL. Вдобавок каждый метод шифрования (MPPE, IPSec и SSL) обладает своей устойчивостью шифрования.

Когда выбраны все четыре настройки, клиент и сервер согласуют между собой наиболее устойчивый вид шифрования, который они могут применять оба. Настройку No Encryption использовать не рекомендуется.

Настройки IP-адресов

Настройки IP-адресов определяют, каким образом клиент получает IP-адрес, который применяется для внутренних подключений. Несмотря на то что VPN-клиент обычно имеет открытый IP-адрес, используемый для туннелирования через Интернет к VPN-серверу, после установления подключения ему также потребуется IP-адрес, локальный по отношению к внутренней сети.

Этот внутренний IP-адрес может быть выдан посредством диапазона адресов, выделенных VPN-сервером, запрошен у внутреннего DHCP-сервера или назначен статически. Для подключения к сети VPN типа “шлюз-шлюз” (когда VPN-сервер принимает только одно подключение) применяется статически назначенный адрес. Если вы следовали шагам по конфигурированию Routing and Remote Access, описанным в этой главе, то вы настроили диапазон IP-адресов, которые назначаются VPN-клиентам.

Создание политики доступа к сети

Уяснив элементы политики доступа к сети, вы сможете создать собственную такую политику. Описанные ниже действия отражают процесс создания политики доступа к сети, которая позволяет пользователям в группе `Domain Users` подключаться к вашему VPN-серверу. В этих шагах предполагается, что VPN-сервер является сервером-членом домена, что дает возможность использовать группу `Domain Users`.

1. Запустите консоль Routing and Remote Access Service (RRAS), выбрав в окне диспетчера серверов пункт меню Tools⇨Routing and Remote Access (Сервис⇨Маршрутизация и удаленный доступ).
2. Запустите консоль сервера сетевой политики (Network Policy Server), щелкнув правой кнопкой мыши на элементе Remote Access Logging and Policies (Ведение журнала и политики удаленного доступа) и выбрав в контекстном меню пункт Launch NPS (Запустить NPS).
3. Выберите в консоли Network Policy Server элемент Network Policies (Сетевые политики). Щелкните правой кнопкой мыши на этом элементе и выберите в контекстном меню пункт New (Создать).
4. Введите `Domain Users` для имени политики.
5. Выберите в раскрывающемся списке для типа сервера доступа к сети вариант Remote Access Server (VPN-Dial up) (Сервер удаленного доступа (VPN — вызов)).
6. Экран будет выглядеть примерно так, как показано на рис. 21.15. Щелкните на кнопке Next (Далее).
7. На экране Specify Conditions (Указание условий) щелкните на кнопке Add (Добавить). Выберите переключатель Windows Groups (Группы Windows), щелкните на Add и щелкните на кнопке Add Groups (Добавить группы).
8. Введите `Domain Users` в качестве имени объекта и щелкните на кнопке Check Names (Проверить имена).
9. По запросу введите учетные данные для этого домена. На экране Select Group (Выбор группы) щелкните на кнопке OK, чтобы принять группу. На экране Windows Groups (Группы Windows) щелкните на кнопке OK, а на экране Specify Conditions щелкните на кнопке Next.

   На экране Specify Conditions вы можете добавлять столько условий, сколько потребуется. Однако если вы предусмотрите несколько условий, то для использования политики должны быть удовлетворены *все* эти условия. Экран Specify Access Permission (Указание разрешений доступа) позволяет предоставить или отказать в доступе и переопределить свойства дозвона для пользователя.
10. Удостоверьтесь, что выбран переключатель Access granted (Доступ предоставлен). Отметьте флажок Access is determined by User Dial-in properties (which override NPS policy) (Доступ определяется свойствами дозвона для данного пользователя (которые переопределяют политику NPS)), чтобы гарантировать, что свойства дозвона данного пользователя не смогут переопределить данную политику. Щелкните на кнопке Next.

    На экране Configure Authentication Methods (Конфигурирование методов аутентификации) вы можете указать, какие методы аутентификации будут использоваться сервером и клиентами.

11. Щелкните на кнопке Add, чтобы просмотреть расширяемые протоколы аутентификации, которые можно добавить. Экран будет выглядеть подобно показанному на рис. 21.16.

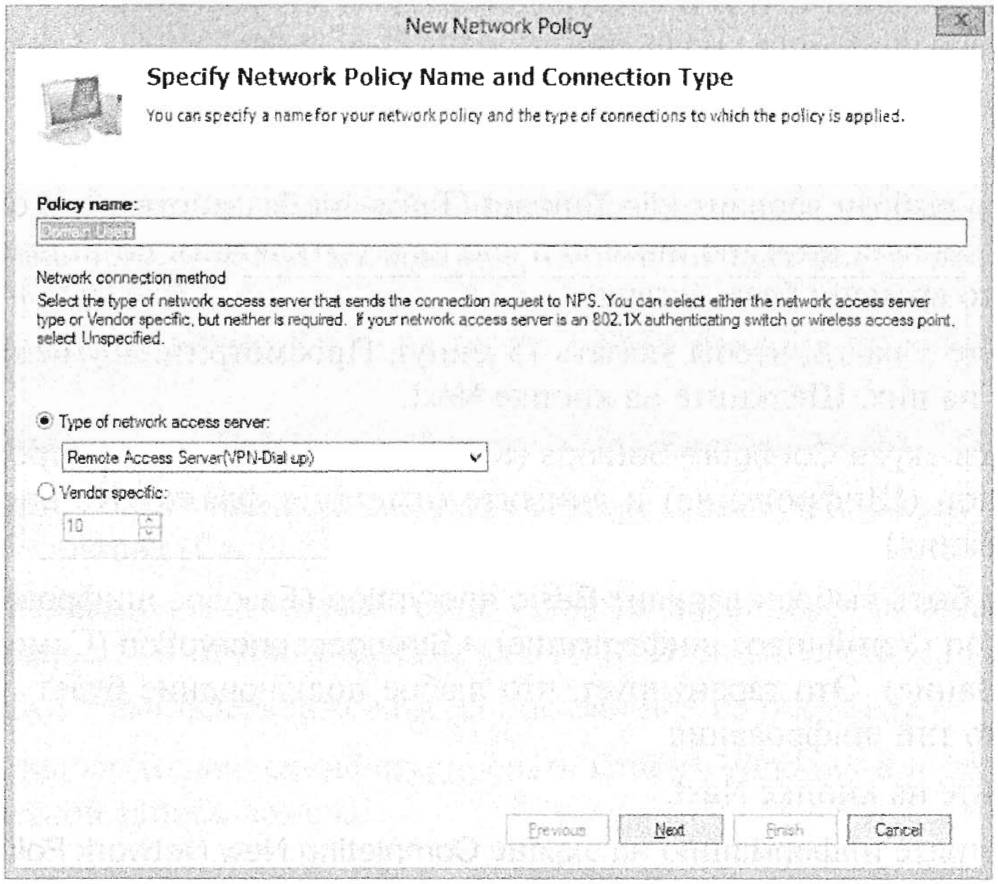


Рис. 21.15. Указание имени сетевой политики и типа подключения для политики

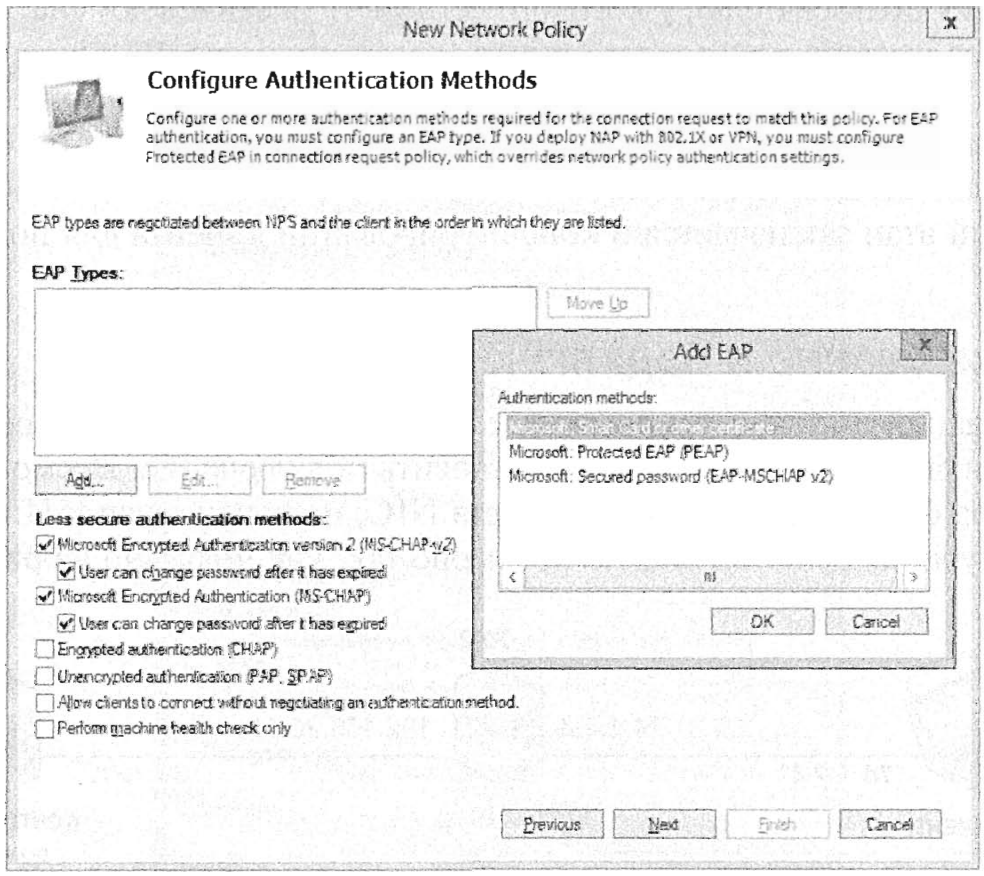


Рис. 21.16. Выбор из нескольких методов аутентификации

Вы можете добавить дополнительные методы EAP, но пока просто оставьте предлагаемое по умолчанию.

12. Щелкните на кнопке Cancel (Отмена), чтобы выйти из диалогового окна Add EAP (Добавление EAP). В следующем разделе мы рассмотрим разные методы аутентификации более подробно.
13. Щелкните на кнопке Next.
14. На экране Configure Constraints (Конфигурирование ограничений) удостоверьтесь, что выбран вариант Idle Timeout (Тайм-аут бездействия), и отметьте флажок Disconnect after the maximum idle time (Отключать по истечении максимального времени бездействия).
15. Измените `1` на `15`, чтобы указать 15 минут. Просмотрите другие ограничения, щелкая на них. Щелкните на кнопке Next.
16. Появится экран Configure Settings (Конфигурирование параметров). Выберите Encryption (Шифрование) и снимите отметку с флажка No encryption (Без шифрования).

    Должен быть выбран вариант Basic encryption (Базовое шифрование), Strong encryption (Устойчивое шифрование) и Strongest encryption (Самое устойчивое шифрование). Это гарантирует, что любое подключение будет использовать какой-то тип шифрования.
17. Щелкните на кнопке Next.
18. Просмотрите информацию на экране Completing New Network Policy (Завершение создания сетевой политики) и щелкните на кнопке Finish (Готово).

Итак, вы создали политику VPN, которую можно применять для предоставления доступа любому пользователю, у которого есть учетная запись домена.

Теперь у вас имеется контроллер домена (в этом примере `BF1`) и сервер-член (по имени `BF2`). На сервер были добавлены роли Network Policy and Access Services и Remote Access, а также сконфигурирована служба RRAS; кроме того, была создана связанная политика доступа к сети.

Следующий этап заключается в конфигурировании клиента для подключения к VPN-серверу.

Конфигурирование и подключение VPN-клиента

После создания и конфигурирования контроллера домена и VPN-сервера настало время сконфигурировать клиент и установить подключение. Несмотря на то что у VPN-сервера фактически будет одна карта NIC, подключенная к Интернету, тестовая конфигурация будет выглядеть примерно так, как показано на рис. 21.17.

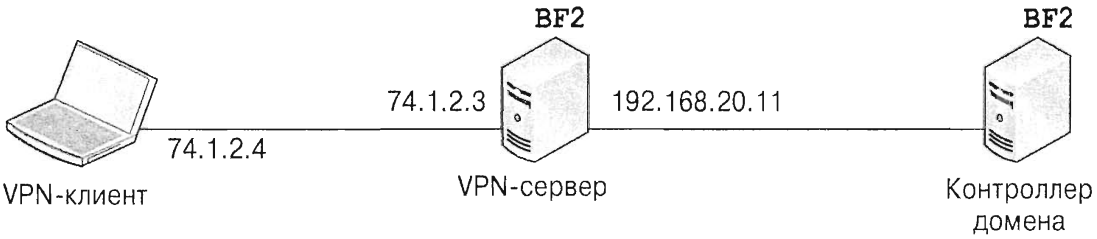


Рис. 21.17. Подключение к VPN-серверу

Обратите внимание, что у VPN-сервера есть две NIC. Вторичная NIC подключена к сети с IP-адресом 192.168.20.11/24, который относится к той же подсети, что и контроллер домена с IP-адресом 192.168.20.10/24.

Карта NIC, видимая из Интернета, имеет назначенный вручную открытый IP-адрес 74.1.2.3/8. Клиент будет получать от поставщика услуг Интернета любой открытый IP-адрес, но в нашей экспериментальной среде мы вручную назначаем IP-адрес 74.1.2.4/8, который находится в той же самой подсети, что и открытый IP-адрес.

Одной из самых серьезных задач является получение сертификата для работы и с сервером, и с клиентом, поэтому начальное тестирование мы проведем без сертификата. Позже мы покажем, как добавить сертификат и сконфигурировать сервер на использование L2TP/IPSec.

Сконфигурируйте сервер RRAS на работу с SSTP без SSL, выполнив следующие шаги.

1. Запустите консоль Routing and Remote Access Service (RRAS).
2. Щелкните правой кнопкой мыши на сервере и выберите в контекстном меню пункт Properties (Свойства).
3. В открывшемся диалоговом окне свойств перейдите на вкладку Security (Безопасность) и отметьте флажок Use HTTP (Использовать HTTP).

   Экран будет выглядеть похожим на показанный на рис. 21.18.

Теперь осталось только сконфигурировать клиент Windows 8 и подключиться с помощью учетной записи домена.

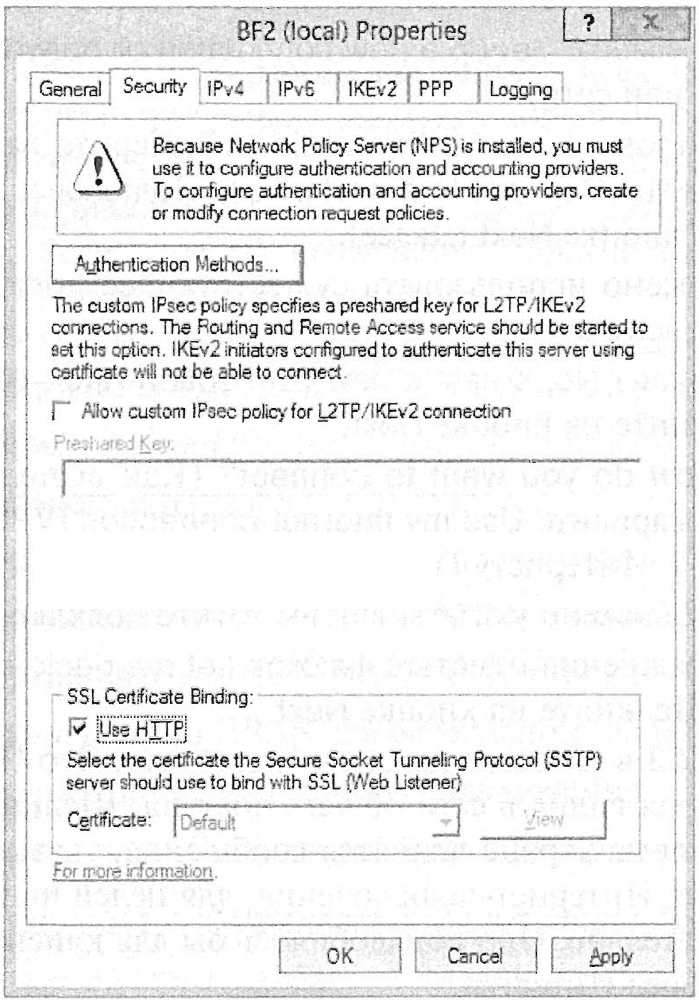


Рис. 21.18. Изменение параметров безопасности VPN

Для этого понадобится выполнить описанные ниже действия.

1. Назначьте своему клиенту Windows 8 IP-адрес 74.1.2.4/8 для эмуляции открытого IP-адреса, который сможет достичь VPN-сервера, выполнив следующие шаги.
   а. На стартовом экране в Windows 8 введите слово `Network`, щелкните на Settings (Параметры) и затем запустите центр управления сетями и общим доступом (Network and Sharing Center).
   б. Щелкните на ссылке Change Adapter Settings (Изменение параметров адаптера). Щелкните правой кнопкой мыши на элементе Local Area Connection (Подключение по локальной сети) и выберите в контекстном меню пункт Properties (Свойства).
   в. Выберите в списке элемент Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)) и щелкните на кнопке Properties.
   г. Введите IP-адрес **74.1.2.4** с маской подсети **255.0.0.0**.
   д. Щелкните на кнопке OK, чтобы закрыть окно IPv4 Properties (Свойства: Протокол Интернета версии 4 (TCP/IPv4)). Щелкните на кнопке Close (Закрыть), чтобы закрыть окно Local Area Connection Properties (Подключение по локальной сети — свойства).

   С этого момента у вас должна появиться возможность доступа к командной строке и пингования IP-адреса VPN-сервера 74.1.2.3. Если пропинговать сервер не удается, то установить VPN-подключение не получится.
2. Возвратитесь в центр управления сетями и общим доступом.
3. Создайте VPN-подключение, выполнив описанные ниже действия.
   а. Щелкните на ссылке Set up a new connection or network (Настройка нового подключения или сети).
   б. На экране Choose a connection option (Выберите вариант подключения) выберите вариант Connect to a workplace (Подключение к рабочему месту). Щелкните на кнопке Next (Далее).

      Будет предложено использовать существующее подключение или создать новое подключение.
   в. Выберите вариант No, create a new connection (Нет, создать новое подключение). Щелкните на кнопке Next.
   г. На экране How do you want to connect? (Как выполнить подключение?) щелкните на варианте Use my Internet connection (VPN) (Использовать мое подключение к Интернету (VPN)).

      Вам будет предложено указать, как вы хотите подключиться к Интернету.
   д. Для этого упражнения отметьте флажок Let me decide later (Принять решение позже). Щелкните на кнопке Next.
   е. Введите **74.1.2.3** в качестве адреса в Интернете. Это IP-адрес NIC на VPN-сервере, которая видна в сети общего доступа. Щелкните на кнопке Create (Создать). Хотя на экране появится сообщение, указывающее на необходимость создания Интернет-подключения, для целей нашего тестирования это делать необязательно. Оно понадобилось бы для клиента, устанавливающего соединение через Интернет.
   ж. Щелкните на кнопке Close (Закрыть).

4. Подключитесь к VPN-серверу, выполнив следующие шаги.
   а. В появившейся панели Networks (Сети) выберите только что созданное VPN-подключение и щелкните на кнопке Connect (Подключиться).
   б. Введите пароль учетной записи домена, который вы вводили при создании данного подключения. При желании можете также ввести новое имя пользователя и пароль. Экран будет выглядеть так, как показано на рис. 21.19.
   в. Щелкните на кнопке OK.

Рис. 21.19. Запуск VPN-подключения в Windows 8

Созданное вами подключение попытается соединиться с сервером. Сначала предпринимается попытка установить SSTP-подключение, а затем, если это не удастся, будут опробованы другие подключения.

Поскольку протокол SSTP активизирован без SSL, подключение произойдет. Обратите внимание, что и VPN-подключение Bigfirm, и домашняя сеть отображаются как активные.

Добавление сертификата

Теперь, когда вы убедились в работоспособности всех составных частей, можно добавить к серверу сертификат, чтобы защитить подключение. Существует несколько способов получения сертификата. Вы можете приобрести сертификат у доверенного центра сертификации или добавить службу сертификатов Active Directory (Active Directory Certificate Services), после чего бесплатно выпускать и устанавливать сертификаты самостоятельно.

Мы выберем бесплатный вариант, хотя для этого придется решить ряд дополнительных задач. Вам придется выполнить перечисленные ниже действия.

1. Установить службу Active Directory Certificate Services.
2. Создать сертификат аутентификации сервера.
3. Запросить и установить сертификат аутентификации сервера.
4. Установить сертификат компьютера на VPN-сервере.
5. Установить сертификат центра сертификации на клиенте.
6. Изменить конфигурацию RRAS для безопасного подключения.
7. Соединиться с помощью безопасного подключения.

Ниже описаны шаги, необходимые для выполнения этих задач.

Шаг 1: установка службы Active Directory Certificate Services

Выполните следующие шаги, чтобы установить службу Active Directory Certificate Services на VPN-сервер.

1. Войдите в систему Windows Server 2012 R2, присоединенную к домену, с помощью учетной записи, которая имеет административные разрешения на уровне домена. В окне диспетчера серверов (Server Manager) при выбранном пункте меню Local Server (Локальный сервер) выберите в меню Manage (Управление) пункт Add roles and features (Добавить роли и компоненты).
2. На экране Before you begin (Прежде чем начать) щелкните на кнопке Next (Далее).
3. На экране Select Installation Type (Выбор типа установки) проверьте, что выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов), и щелкните на кнопке Next.
4. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов), убедитесь, что ваш сервер выделен в разделе Server Pool (Пул серверов), и щелкните на кнопке Next.
5. На экране Select Server Roles (Выбор серверных ролей) отметьте флажок Active Directory Certificate Services (Службы сертификатов Active Directory) и в открывшемся окне щелкните на кнопке Add Features (Добавить компоненты).
6. Три раза щелкните на кнопке Next, чтобы перейти на экран Select Role Services (Выбор служб ролей).
7. На экране Select Role Services отметьте флажки Certification Authority (Центр сертификации) и Certificate Authority Web Enrollment (Веб-развертывание центра сертификации). Получив уведомление о добавлении дополнительных служб ролей, щелкните на кнопке Add Required Role Services (Добавить требуемые службы ролей). Щелкните на кнопке Next.
8. Примите все стандартные параметры, предлагаемые мастером. Просмотрите информацию на экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) и щелкните на кнопке Install (Установить).
9. После завершения установки щелкните на кнопке Close (Закрыть).

Шаг 2: конфигурирование службы Active Directory Certificate Services

Прежде чем можно будет пользоваться ролью Certificate Services, необходимо провести завершающие действия по конфигурированию.

1. В окне диспетчера серверов выберите меню AD CS и обратите внимание на область с предупреждением, которое гласит Configuration required for Active Directory Certificate Services (Требуется конфигурирование для Active Directory Certificate Services). Для продолжения щелкните на ссылке More (Дополнительно) в этой области предупреждения.
2. В открывшемся окне All Servers Task Details and Notifications (Подробности и уведомления обо всех серверных задачах) щелкните на ссылке Configure Active Directory Certificate Services on the destination server (Конфигурировать Active Directory Certificate Services на целевом сервере).

   Когда откроется мастер конфигурирования службы AD CS (AD CS Configuration Wizard), понадобится указать учетные данные для конфигурирования этой роли.

3. Введите учетную запись с административными разрешениями (или оставьте стандартную учетную запись администратора домена) и щелкните на кнопке Next (Далее).
4. На экране Select Role Services to Configure (Выбор службы ролей для конфигурирования) отметьте флажки Certification Authority (Центр сертификации) и Certificate Authority Web Enrollment (Веб-развертывание центра сертификации), после чего щелкните на кнопке Next.
5. На следующем экране выберите переключатель Enterprise CA (Центр сертификации предприятия) и щелкните на кнопке Next.
6. Если ранее вы не развертывали центр сертификации в своей среде или если проводите этот эксперимент в испытательной среде, на следующем экране выберите переключатель Root CA (Корневой центр сертификации) и щелкните на кнопке Next.
7. Выберите переключатель Create a Private Key (Создать секретный ключ) и для продолжения щелкните на кнопке Next.
8. На экране Cryptography for CA (Криптография для центра сертификации) оставьте стандартные параметры и щелкните на кнопке Next.
9. На экране CA Name (Имя центра сертификации) укажите имя для своего центра сертификации и щелкните на кнопке Next.
10. Укажите период допустимости для корневого сертификата или просто оставьте стандартный вариант 5 лет, после чего щелкните на кнопке Next.
11. На экране Confirmation (Подтверждение) проверьте, что были выбраны нужные параметры, и затем щелкните на кнопке Configure (Конфигурировать).

Изменение имени центра сертификации

Имейте в виду, что по завершении этой процедуры вы не сможете изменить имя центра сертификации. Единственная возможность предусматривает удаление и повторную установку данной роли, поэтому очень важно выбрать подходящее имя с первого раза.

---

12. Когда мастер завершит работу, щелкните на кнопке Close (Закрыть).

Шаг 3: создание сертификата аутентификации сервера

Выполните на VPN-сервере описанные ниже действия, чтобы создать сертификат аутентификации сервера.

1. В окне диспетчера серверов выберите в меню Tools (Сервис) пункт Certification Authority (Центр сертификации).
2. Щелкните правой кнопкой мыши на узле Certificate Templates (Шаблоны сертификата) и выберите в контекстном меню пункт Manage (Управлять).
3. Щелкните правой кнопкой мыши на шаблоне Web Server (Веб-сервер) и выберите в контекстном меню пункт Duplicate Template (Дублировать шаблон).
4. На вкладке Compatibility (Совместимость) окна свойств сертификата оставьте стандартную настройку Windows Server 2003 и перейдите на вкладку General (Общие).

5. В поле Template display name (Отображаемое имя сертификата) введите VPN IPSec.
6. Перейдите на вкладку Request Handling (Обработка запросов) и отметьте флажок Allow private key to be exported (Разрешить экспортирование секретного ключа).
7. Перейдите на вкладку Subject Name (Название темы) и отметьте флажок Supply in the request (Указывать в запросе).
8. Перейдите на вкладку Extensions (Расширения). Выберите элемент Application Policies (Политики приложений) и убедитесь, что в списке Application Policies присутствует элемент Server Authentication (Аутентификация сервера).

   Окно будет выглядеть похожим на показанное на рис. 21.20.

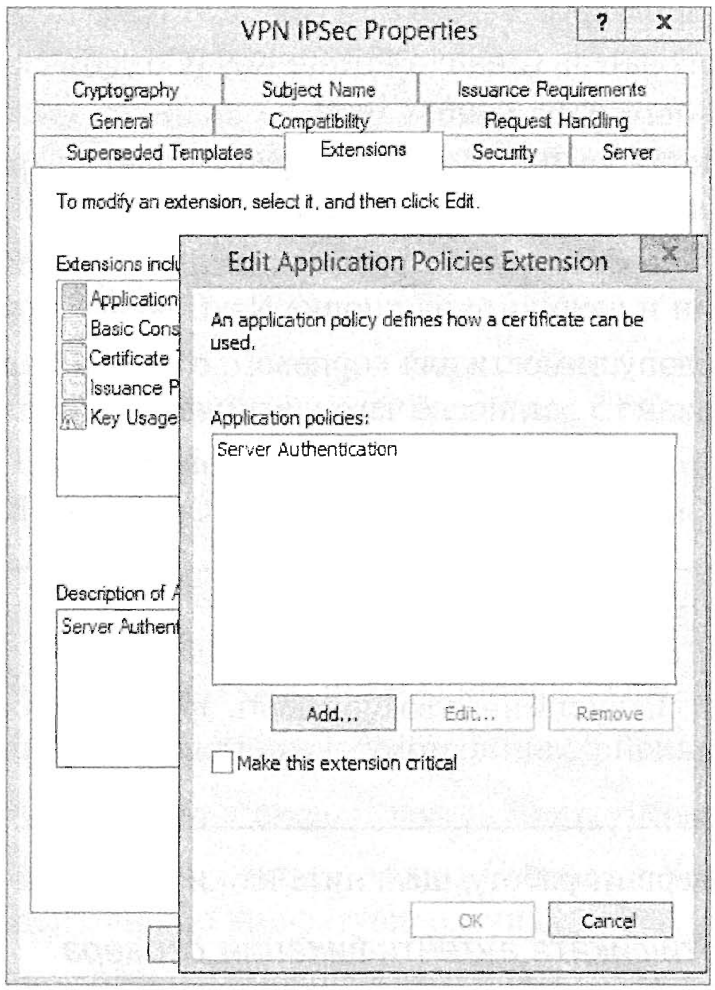


Рис. 21.20. Добавление расширения политики приложений Server Authentication для сертификата

9. Щелкните на кнопке OK или Cancel (Отмена), чтобы возвратиться на вкладку Extensions.
10. Щелкните на кнопке OK, чтобы сохранить шаблон.
11. Возвратитесь в окно консоли Certificate Authority.
12. Щелкните правой кнопкой мыши на узле Certificate Templates и выберите в контекстном меню пункт New⇨Certificate Template to Issue (Создать⇨Шаблон сертификата для выдачи).
13. Выберите VPN IPSec и щелкните на кнопке OK.

Шаг 4: запрос и установка сертификата аутентификации сервера

Выполните на VPN-сервере перечисленные далее шаги, чтобы установить сертификат аутентификации сервера.

1. С помощью описанных ниже действий сконфигурируйте параметры безопасности Internet Explorer так, чтобы его можно было использовать для добавления сертификата.
2. Запустите Internet Explorer с административными привилегиями (щелкнув на его значке правой кнопкой мыши и выбрав в контекстном меню пункт Run As Administrator (Запуск от имени администратора)).
3. Выберите в меню Tools (Сервис) пункт Internet Options (Параметры Интернета) и в открывшемся диалоговом окне перейдите на вкладку Security (Безопасность).
4. Выберите зону Local intranet (Местная интрасеть) и переместите ползунок уровня безопасности из положения Medium-low (Ниже среднего) в положение Low (Низкий). Щелкните на кнопке OK.
5. В поле адреса Internet Explorer введите **`http://localhost/certsrv`**, чтобы установить подключение с Certificate Services.
6. Щелкните на ссылке Request a Certificate (Запросить сертификат). Затем щелкните на ссылке Advanced Certificate Request (Расширенный запрос сертификата).
7. Щелкните на ссылке Create (Создать) и отправьте запрос этому центру сертификации. Когда будет предложено разрешить элемент управления ActiveX, щелкните на кнопке Yes (Да).
8. Просмотрите сообщение подтверждения и щелкните на кнопке Yes еще раз.
9. Выберите VPN IPSec в качестве шаблона сертификата. В поле Name (Имя) введите имя своего сервера и домена. В данном примере это будет `BF2.Bigfirm.com`.
10. Щелкните на кнопке Submit (Отправить).
11. Когда будет предложено разрешить элемент управления ActiveX, щелкните на кнопке Yes. Щелкните на кнопке Yes еще раз в диалоговом окне подтверждения. Нужный сертификат создан.
12. Щелкните на ссылке Install This Certificate (Установить этот сертификат); вам понадобится выполнить дополнительные шаги. Закройте Internet Explorer.

Шаг 5: установка сертификата компьютера на VPN-сервере

Ниже приведены действия по добавлению сертификата в хранилище сертификатов на VPN-сервере.

1. На стартовом экране в Windows Server 2012 R2 введите `MMC` и щелкните на опции MMC.
2. В окне консоли MMC выберите пункт меню File⇨Add/Remove Snap-in (Файл⇨Добавить ли удалить оснастку).
3. Выберите в списке слева оснастку Certificates (Сертификаты) и щелкните на кнопке Add (Добавить).

4. Щелкните на кнопке Finish (Готово), чтобы добавить оснастку при выбранном переключателе My user account (Моя учетная запись пользователя). Щелкните на кнопке Add еще раз, выберите переключатель Computer Account (Учетная запись компьютера) и щелкните на кнопке Next (Далее).
5. Щелкните на кнопке Finish. Щелкните на кнопке OK.
6. Перейдите к контейнеру Certificates — Current User \ Personal \ Certificates (Сертификаты — текущий пользователь \ Личное \ Сертификаты).
7. Экспортируйте сертификат сервера с помощью следующих шагов.
   а. Щелкните правой кнопкой мыши на сертификате сервера и выберите в контекстном меню пункт All Tasks⇨**Export** (Все задачи⇨Экспортировать).
   б. На экране приветствия мастера экспорта щелкните на кнопке Next (Далее).
   в. Выберите переключатель Yes, export the private key (Да, экспортировать секретный ключ) и щелкните на кнопке Next.
   г. Примите стандартный формат файла и щелкните на кнопке Next.
   д. На экране Password (Пароль) введите пароль в текстовых полях Password (Пароль) и Confirm Password (Подтвердить пароль) и щелкните на кнопке Next.
   е. Щелкните на кнопке Browse (Обзор) и перейдите в папку `C:\Certs` (при необходимости создайте ее).
   ж. Назначьте файлу имя **`VPNIPsec`** и щелкните на кнопке Save (Сохранить).
   з. Щелкните на кнопке Next, на кнопке Finish (Готово) и на кнопке OK.
8. Возвратившись в окно консоли MMC, импортируйте этот сертификат, выполнив описанные далее действия.
   а. Перейдите к контейнеру Certificates (Local Computer) \ Personal \ Certificates (Сертификаты (локальный компьютер) \ Личное \ Сертификаты).
   б. Щелкните правой кнопкой мыши на папке Certificates и выберите в контекстном меню пункт All Tasks⇨**Import** (Все задачи⇨Импортировать).
   в. На экране приветствия мастера импорта щелкните на кнопке Next (Далее).
   г. Щелкните на кнопке Browse (Обзор) и перейдите в папку `C:\Certs`.
   д. Измените расширение на All Files (*.*) (Все файлы (*.*)), чтобы появился экспортированный ранее файл.
   е. Выберите свой сертификат и щелкните на кнопке Open (Открыть).
   ж. На экране File to Import (Файл для импортирования) щелкните на кнопке Next.
   з. Введите пароль, который вы указывали для защиты сертификата, и щелкните на кнопке Next.
   и. Щелкните на кнопке Next, чтобы принять стандартное местоположение хранилища сертификатов, и щелкните на Next еще раз. Щелкните на кнопке OK.

9. Выполните перечисленные ниже шаги, чтобы сгенерировать доверенный корневой сертификат на VPN-сервере.
   а. Запустите Internet Explorer с административными привилегиями (щелкнув на его значке правой кнопкой мыши и выбрав в контекстном меню пункт Run As Administrator (Запуск от имени администратора)).
   б. В поле адреса Internet Explorer введите **`http://localhost/certsrv`**.
   в. Щелкните на ссылке Download a CA certificate, certificate chain, or CRL (Загрузить сертификат центра сертификации, цепочку сертификатов или CRL).
   г. Когда на экране появится предупреждение о разрешении элемента управления ActiveX, щелкните на кнопке Yes (Да).
   д. Щелкните на кнопке Yes еще раз во всплывающем диалоговом окне подтверждения.
   е. Щелкните на ссылке Download CA certificate (Загрузить сертификат центра сертификации) и щелкните на кнопке Save (Сохранить). Обратите внимание, что именем сертификата является `certnew`.
   ж. Перейдите в папку `C:\Certs`, щелкните на кнопке Save и затем на кнопке Close (Закрыть).

Далее вы установите этот корневой сертификат на клиенте.

Шаг 6: установка сертификата центра сертификации на клиенте

Когда клиент подключается к VPN-серверу, этот сервер передаст сертификат для использования в процессе установления сеанса. Однако по умолчанию клиент не считает этот сертификат достоверным. Чтобы клиент доверял сертификату данного сервера, на клиенте должен быть установлен корневой сертификат центра сертификации (CA).

Выполните описанные ниже действия, чтобы установить на клиенте корневой сертификат.

1. Скопируйте сертификат `certnew`, созданный на предыдущем этапе, из сервера в папку `C:\Certs` на клиенте.
2. На стартовом экране клиента Windows 8 введите `MMC`, щелкните на значке `MMC.exe` и нажмите <Enter>.
3. Если появится диалоговое окно User Account Control (Управление пользовательскими учетными записями), щелкните на кнопке Yes (Да), чтобы разрешить выполнение действия.
4. Выберите пункт меню File⇨Add/Remove Snap-in (Файл⇨Добавить или удалить оснастку).
5. Выберите в списке слева оснастку Certificates (Сертификаты) и щелкните на кнопке Add (Добавить).
6. Выберите переключатель Computer Account (Учетная запись компьютера) и щелкните на кнопке Next (Далее).
7. Оставьте выбранным переключатель Local Computer (Локальный компьютер) и щелкните на кнопке Finish (Готово). Щелкните на кнопке OK.

8. Перейдите к контейнеру Certificates (Local Computers)\Trusted Root Certification Authorities\Certificates (Сертификаты (локальный компьютер) \ Доверенные корневые центры сертификации \ Сертификаты).
9. Щелкните правой кнопкой мыши на контейнере Certificates и выберите в контекстном меню пункт All Tasks⇨Import (Все задачи⇨Импортировать).
10. На экране приветствия мастера импорта щелкните на кнопке Next (Далее).
11. Перейдите в папку `C:\Certs` и выберите файл сертификата `certnew.cer`. Щелкните на кнопке Open (Открыть). Щелкните на кнопке Next.
12. На экране Certificate Store (Хранилище сертификатов) щелкните на кнопке Next, чтобы принять стандартное местоположение хранилища сертификатов.

Шаг 7: изменение конфигурации RRAS для безопасного подключения

Теперь вы можете сконфигурировать RRAS-сервер на использование сертификата, выполнив следующие шаги.

1. Откройте консоль Routing and Remote Access Service, если она еще не открыта.
2. Щелкните правой кнопкой мыши на сервере и выберите в контекстном меню пункт Properties (Свойства).
3. В окне свойств сервера перейдите на вкладку Security (Безопасность).
4. Снимите отметку с флажка Use HTTP (Использовать HTTP) в разделе SSL Certificate Binding (Привязка сертификата SSL). Выберите созданный ранее сертификат.

Шаг 8: установка соединение с помощью безопасного подключения

С этого момента вы уже можете подключаться с помощью созданного ранее подключения в Windows 8. Вносить какие-либо изменения для Windows 8 не требуется. Подключение установится автоматически.

1. Обратитесь к панели Network (Сеть) в системе Windows 8.
2. Выберите созданное ранее VPN-подключение и щелкните на кнопке Connect (Подключиться).
3. Введите пароль учетной записи домена, который вы указывали при создании этого подключения.
4. Щелкните на кнопке Connect, и безопасное подключение будет установлено.

На описанных выше этапах вы принимали стандартные настройки для аутентификации. Тем не менее, вы можете использовать и другие методы аутентификации. Ниже приведено более подробное описание доступных методов аутентификации.

Аутентификация VPN-клиентов

Аутентификация позволяет клиенту доказать, что он именно тот, за кого себя выдает. По ее завершении политика доступа к сети способна определить, должен ли предоставляться этому клиенту доступ в сеть. Очевидно, что аутентификация очень важна. Вряд ли вы захотите, чтобы кто угодно мог подключаться к вашему VPN-серверу и получать доступ в сеть.

Если злоумышленнику удастся заполучить учетные данные законного пользователя, то он сможет выдать себя за этого пользователя и получить доступ к серверу. Именно поэтому аутентификация становится одним из значимых соображений безопасности и существует много способов аутентификации пользователей.

Поскольку методы, к которым прибегают злоумышленники, становятся все более изощренными, IT-специалисты создают более совершенные способы борьбы с незаконным проникновением в сети. Складывается впечатление, что совершенствованию методов незаконного проникновения в сети и ответному совершенствованию способов борьбы с этим явлением нет конца. Ниже мы ознакомим вас с разными методами аутентификации и покажем, как совершенствовались эти методы.

Старейшим методом аутентификации является протокол аутентификации с помощью пароля (Password Authentication Protocol — PAP). Этот метод предусматривал отправку паролей в виде открытого текста, поэтому его взлом особых усилий не требовал: достаточно было перехватить соответствующие пакеты. В наши дни на более безопасные методы аутентификации ссылаются как на методы расширяемого протокола аутентификации (Extensible Authentication Protocol). Они являются расширениями базовых методов аутентификации.

Когда выбрано несколько методов аутентификации, клиент и сервер договариваются о применении наиболее безопасного метода, который доступен им обоим. Серверу VPN нередко приходится поддерживать множество типов клиентов, поэтому каждый VPN-сервер, как правило, поддерживает несколько методов аутентификации. Вы должны убедиться в том, что ваш VPN-сервер располагает механизмами аутентификации для всех клиентов, которых вы решили поддерживать.

С другой стороны, вы можете принять решение использовать только самый надежный механизм аутентификации. В таком случае клиенты тоже должны применять этот метод, иначе они не смогут установить подключение.

Ранее в этой главе вы создали политику `Domain Users`, которая использовала стандартные методы аутентификации. Аутентификацию можно усилить путем добавления к этой политике метода аутентификации Microsoft: Secured password (EAP-MS-MSCHAP v2) (Microsoft: защищенный пароль (EAP-MS-MSCHAP v2)), щелкнув на кнопке Add (Добавить) и выбрав соответствующий элемент в списке (рис. 21.21). Этот метод требует добавления сертификата от центра сертификации. Если для ваших пользователей изготовлены специальные смарт-карты, то вы можете добавить вариант Microsoft: Smart Card or other certificate (Microsoft: смарт-карта или другой сертификат), обеспечив таким образом более надежную аутентификацию.

Ниже перечислены все доступные методы аутентификации в порядке от менее надежных к более надежным.

- Perform Machine Health Check Only (Выполнять только проверку работоспособности компьютера). Если сконфигурирован сервер сетевой политики, данный метод можно использовать для проверки работоспособности соответствующего клиента. В действительности это не является аутентификацией, поскольку проверяется только состояние работоспособности клиента; тем не менее, этот метод присутствует на экране аутентификации.
- Allow Clients to Connect without Negotiating an Authentication Method (Позволить клиентам устанавливать подключение без согласования метода аутентификации). Аутентификация не применяется. Любые клиенты могут устанавливать подключение без подтверждения своего удостоверения.

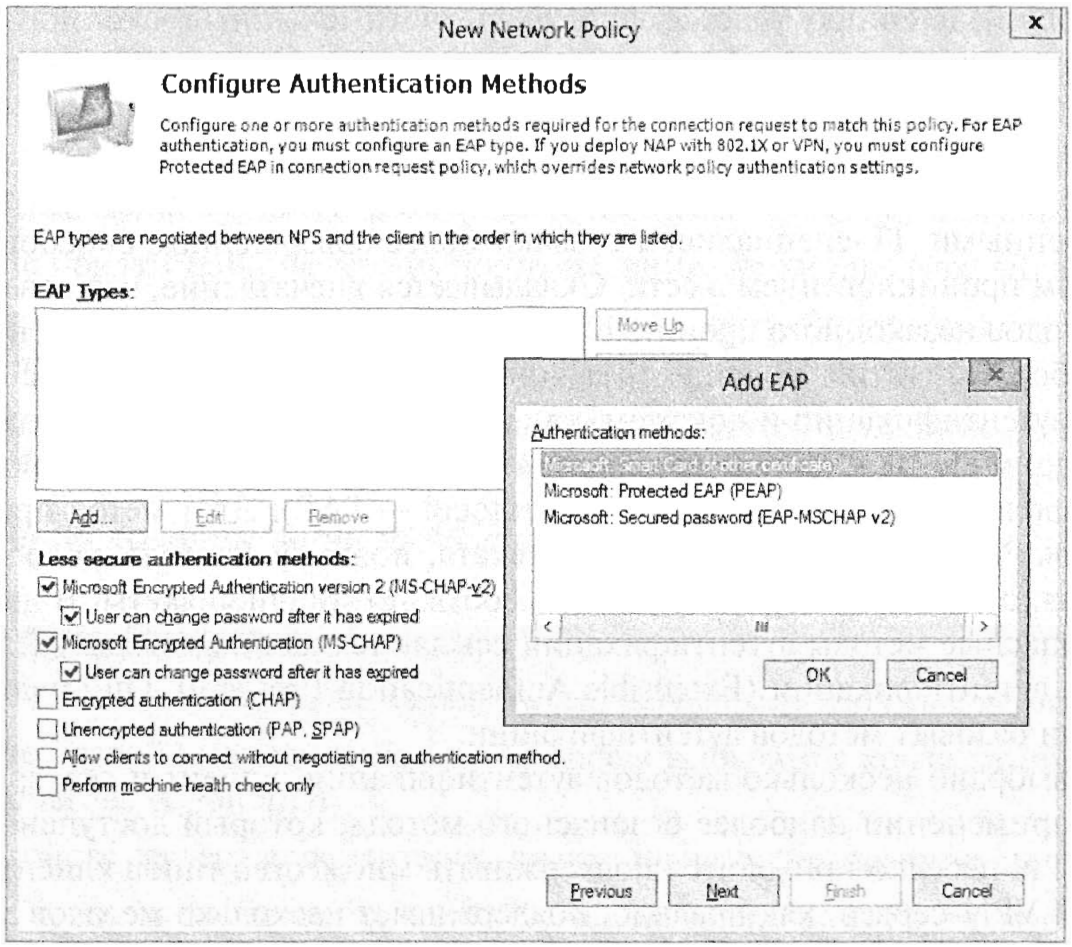


Рис. 21.21. Изменение методов аутентификации для политики

- **Unencrypted Authentication (PAP, SPAP) (Аутентификация без шифрования (PAP, SPAP)).** Данные аутентификации передаются по каналам связи в виде открытого текста. С помощью любого анализатора протокола (называемого *снифферо*м) можно перехватывать пакеты и выявлять учетные данные. К таким методам относятся Password Authentication Protocol и патентованный Shiva Password Authentication Protocol (SPAP). Мы были бы удивлены, узнав, что они используются сегодня в какой-то производственной среде.
- **Encrypted Authentication (CHAP) (Аутентификация с шифрованием (CHAP)).** Протокол аутентификации методом "вызов-приветствие" (Challenge Handshake Authentication Protocol — CHAP) был первым получившим широкое применение протоколом аутентификации с шифрованием. При установлении подключения у клиента запрашивалось однократно используемое число, которое объединялось с учетными данными, хешировалось, шифровалось и возвращалось серверу. Сервер периодически отправлял клиенту новое число подобного рода и инициировал очередной обмен "вызов-приветствие" в течение сеанса. Исторически протокол CHAP применялся на RRAS-серверах Microsoft для поддержки клиентов, отличных от Microsoft, но в наши дни вместо CHAP рекомендуются более надежные методы EAP.
- **Microsoft Encrypted Authentication (MS-CHAP) (Аутентификация с шифрованием Microsoft (MS-CHAP)).** Первое усовершенствование протокола CHAP, выполненное Microsoft. Этот метод работал только на клиентах Microsoft и был впоследствии заменен MS-CHAP v2. Чтобы воспрепятствовать попыткам анализа протокола, MS-CHAP также шифрует данные аутентификации.

- **Microsoft Encrypted Authentication version 2 (MS-CHAP v2) (Аутентификация с шифрованием Microsoft, версия 2 (MS-CHAP v2)).** Метод MS-CHAP v2 был разработан как усовершенствованный вариант MS-CHAP. По сравнению с MS-CHAP в MS-CHAP v2 реализовано несколько улучшений, в числе которых взаимная аутентификация. При использовании взаимной аутентификации сервер аутентифицирует себя по отношению к клиенту и лишь после этого клиент отправляет пользовательские учетные данные.

Ниже приведено описание трех методов аутентификации, которые называют методами расширяемого протокола аутентификации (Extensible Authentication Protocol — EAP). Следует отметить, что EAP является платформой безопасности, которая может применяться любым поставщиком. Эта платформа безопасности обеспечивает самую высокую защиту при максимальной гибкости.

- **Microsoft: Secured Password (EAP-MS-CHAP v2) (Microsoft: защищенный пароль).** Для повышения защиты EAP-MS-CHAP v2 использует сертификаты на VPN-сервере. Сертификат выпускается центром сертификации (CA), которому доверяет VPN-клиент, и предоставляется, когда этот VPN-клиент контактирует с VPN-сервером. Поскольку VPN-клиент доверяет CA, сертификат обеспечивает аутентификацию сервера по отношению к клиенту перед тем, как начинается процесс аутентификации клиента. Чтобы создать безопасный канал для процесса аутентификации MS-CHAP v2, с открытым и секретным ключами применяется TLS (Transport Layer Security — безопасность транспортного уровня).

  Метод EAP-MS-CHAP v2 легче в развертывании, чем EAP-TLS (аутентификация с помощью смарт-карты), но по-прежнему предлагает значительные усовершенствования по сравнению с MS-CHAP v2.

- **Microsoft: Protected EAP (PEAP) (Microsoft: защищенный EAP).** Версия PEAP не указывает какой-то метод аутентификации, а взамен обеспечивает дополнительную безопасность для любого используемого метода аутентификации. PEAP предоставляет защищенный канал, который препятствует внедрению злоумышленниками пакетов между клиентом и VPN-сервером.

- **Microsoft: Smart Card or Other Certificate (Microsoft: смарт-карта или другой сертификат).** Аутентификация на основе сертификатов считается самым надежным методом аутентификации из тех, которые могут применяться VPN-сервером. Смарт-карты обеспечивают многофакторную аутентификацию, поскольку пользователь должен что-то иметь (смарт-карту) и что-то знать (ассоциированный PIN-код). В смарт-карте есть встроенный цифровой сертификат, полученный от доверенного центра сертификатов (CA).

  Смарт-карты могут существенно увеличить затраты. Они требуют выпуска сертификатов CA, оборудования для изготовления смарт-карт со встроенными сертификатами и оборудования для считывания смарт-карт. Этот метод использует TLS, поэтому иногда на него ссылаются как на EAP-TLS.

Конфигурирование учета

Учет применяется на VPN-сервере для регистрации подробных сведений о том, кто обращается к серверу, а также о каждодневных действиях сервера. Все, что касается учета, конфигурируется посредством консоли NPS для VPN-сервера в среде Windows Server 2012 R2.

Консоль NPS включает мастер, который можно использовать для конфигурирования учета, и предлагает четыре варианта хранения данных учета:

- база данных SQL Server;
- текстовый файл;
- база данных SQL Server и локальный текстовый файл;
- база данных SQL Server с записью в текстовый файл для обхода отказа.

Лучше всего, когда ваша сеть включает SQL Server, и кто-то из сотрудников знаком с конфигурированием SQL Server для предоставления данных. Однако если функционирующий продукт SQL Server в сети отсутствует, то для регистрации данных вы должны выбрать текстовый файл.

Регистрировать можно разные типы данных:

- запросы учета;
- запросы аутентификации;
- периодическое состояние учета;
- периодическое состояние аутентификации.

Информация о запросах и состоянии аутентификации содержит все события аутентификации. В их число входят как неудачные, так и успешные попытки аутентификации. Хотя вполне очевидно, что аутентификация происходит при первом подключении пользователя, менее очевидно то, что сервер периодически требует от клиента подтвердить свое удостоверение. Для пользователя этот процесс является прозрачным, однако он гарантирует, что клиентский сеанс не будет похищен с целью несанкционированного использования злоумышленником. Успешная попытка такого похищения приведет к отключению первоначального пользователя и позволит злоумышленнику получить доступ к данным внутри сеанса.

Запросы учета и сведения о состоянии содержат такую часто применяемую при формировании счетов информацию, как момент установления подключения, его продолжительность и деятельность на протяжении периода подключения.

Чтобы сконфигурировать учет на VPN-сервере и сохранить информацию в локальном текстовом файле, выполните следующие шаги.

1. Запустите консоль Routing and Remote Access Service (RRAS), выбрав в окне диспетчера серверов пункт меню Tools⇨Routing and Remote Access (Сервис⇨ Маршрутизация и удаленный доступ).
2. Запустите консоль Network Policy Server (Сервер сетевой политики), щелкнув правой кнопкой мыши на узле Remote Access Logging and Policies (Протоколирование и политики удаленного доступа) и выбрав в контекстном меню пункт Launch NPS (Запустить NPS).
3. Выберите узел Accounting (Учет) в консоли Network Policy Server.
4. Щелкните на ссылке Configure Accounting (Конфигурировать учет) в панели, расположенной посередине.
5. Ознакомьтесь с информацией на экране Introduction (Введение) и щелкните на кнопке Next (Далее).

6. На экране Select Accounting Options (Выбрать параметры учета) выберите переключатель Log to a Text File on the Local Computer (Регистрировать данные в текстовом файле на локальном компьютере) и щелкните на кнопке Next.

   Экран Configure Local File Logging (Конфигурировать регистрацию в локальном файле) позволяет выбрать тип информации, которую необходимо регистрировать. На рис. 21.22 представлены стандартные параметры.

7. Если вы хотите выбрать другое местоположение, просто щелкните на кнопке Browse (Обзор) и перейдите в желаемое место.

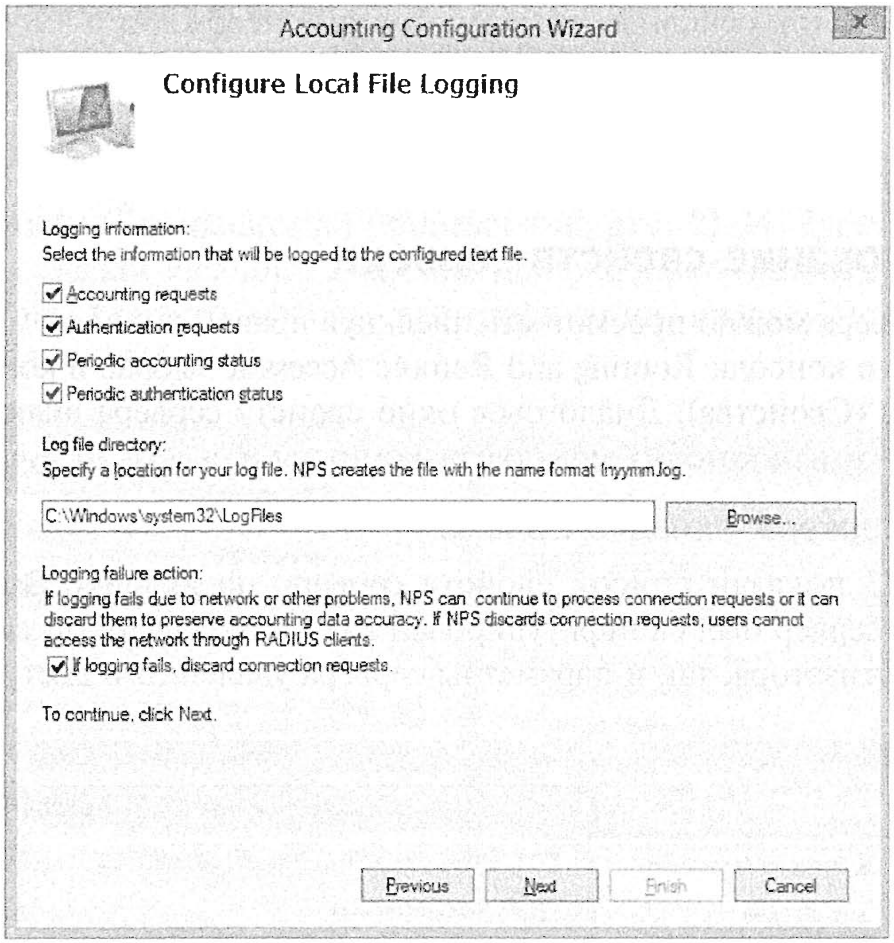


Рис. 21.22. Изменение методов аутентификации для политики

Важный выбор предстоит сделать в нижней части экрана — флажок If logging fails, discard connection requests (Если регистрация данных завершилась неудачно, игнорировать запросы подключения). Вы должны выяснить, что важнее для вас и вашей организации — регистрация данных учета или доступ к VPN-серверу. Когда более важной для всех является возможность регистрации данных, отметьте этот флажок; в таком случае, если регистрация данных завершится неудачно, VPN-сервер не разрешит устанавливать подключения. Когда более важным является доступ к VPN-серверу, снимите отметку с этого флажка. Тогда если регистрация данных завершится неудачно, пользователи по-прежнему смогут подключаться, но вы не сможете фиксировать данные об этих подключениях.

8. Примите параметры, выбранные по умолчанию, и щелкните на кнопке Next.
9. Просмотрите сведения на экране Summary (Сводка) и щелкните на кнопке Next. Щелкните на кнопке Close (Закрыть).

Итак, к этому моменту вы добавили сервер Routing and Remote Access Service, сконфигурировали его таким образом, чтобы он действовал в качестве VPN-сервера, добавили политику доступа к сети и настроили учет. Осталось только исследовать консоль Routing and Remote Access, чем мы и займемся в следующем разделе.

Исследование консоли Routing and Remote Access

После добавления и настройки службы Routing and Remote Access Service с помощью диспетчера серверов консоль Routing and Remote Access можно использовать для изменения параметров и просмотра информации о клиентах, установивших подключение. Есть три основных области, которые необходимо изучить:

- свойства сервера;
- порты;
- клиенты удаленного доступа.

Конфигурирование свойств сервера

Свойства сервера можно просмотреть, щелкнув правой кнопкой мыши на интересующем сервере в консоли Routing and Remote Access и выбрав в контекстном меню пункт Properties (Свойства). Диалоговое окно свойств сервера включает несколько вкладок, с содержимым которых можно ознакомиться и внести требуемые изменения.

Окно свойств сервера: вкладка General

На рис. 21.23 показан список свойств сервера на вкладке General (Общие). Поскольку этот сервер был сконфигурирован как VPN-сервер, он включает как параметры маршрутизатора, так и параметры сервера удаленного доступа.

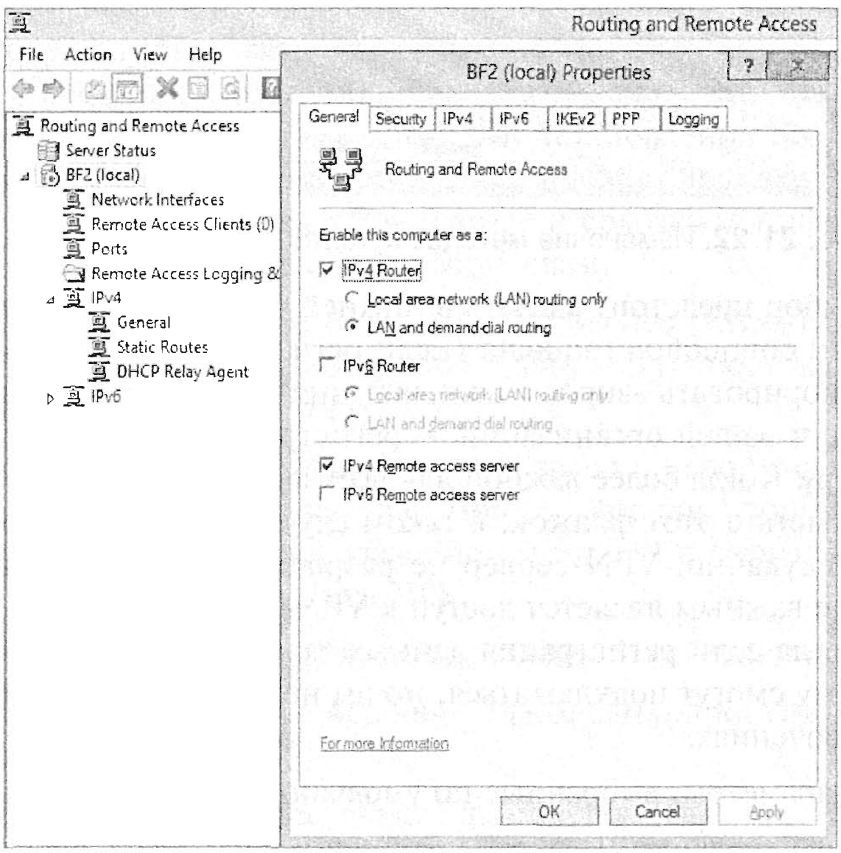


Рис. 21.23. Вкладка General для сервера RRAS

Флажок IPv4 Router (Маршрутизатор IPv4) и переключатель LAN and demand-dial routing (Маршрутизация в локальной сети и с дозвоном по требованию) позволяют VPN-серверу маршрутизировать пакеты от открытого IP-адреса (получаемого от VPN-клиентов) до внутренней локальной сети. На данный момент поддерживаются IPv4 и IPv6, т.к. Интернет постепенно переходит на IPv6, поэтому можно использовать либо IPv4, либо IPv6. В нижней части находится флажок IPv4 Remote access server (Сервер удаленного доступа IPv4), который указывает, что данный сервер применяется как сервер удаленного доступа, а во внутренней сети используются адреса IPv4. Глядя на эту вкладку, невозможно сказать, в каком качестве применяется сервер — как VPN-сервер или как сервер коммутируемых подключений. Но когда вы взглянете на доступные порты (показанные далее в главе), станет ясно, что сервер используется как VPN-сервер.

Окно свойств сервера: вкладка ***Security***

Вкладка Security (Безопасность) приведена на рис. 21.24. Здесь отражена ситуация, когда был сделан щелчок на кнопке Authentication Methods (Методы аутентификации), чтобы показать методы аутентификации, предусмотренные для этого сервера.

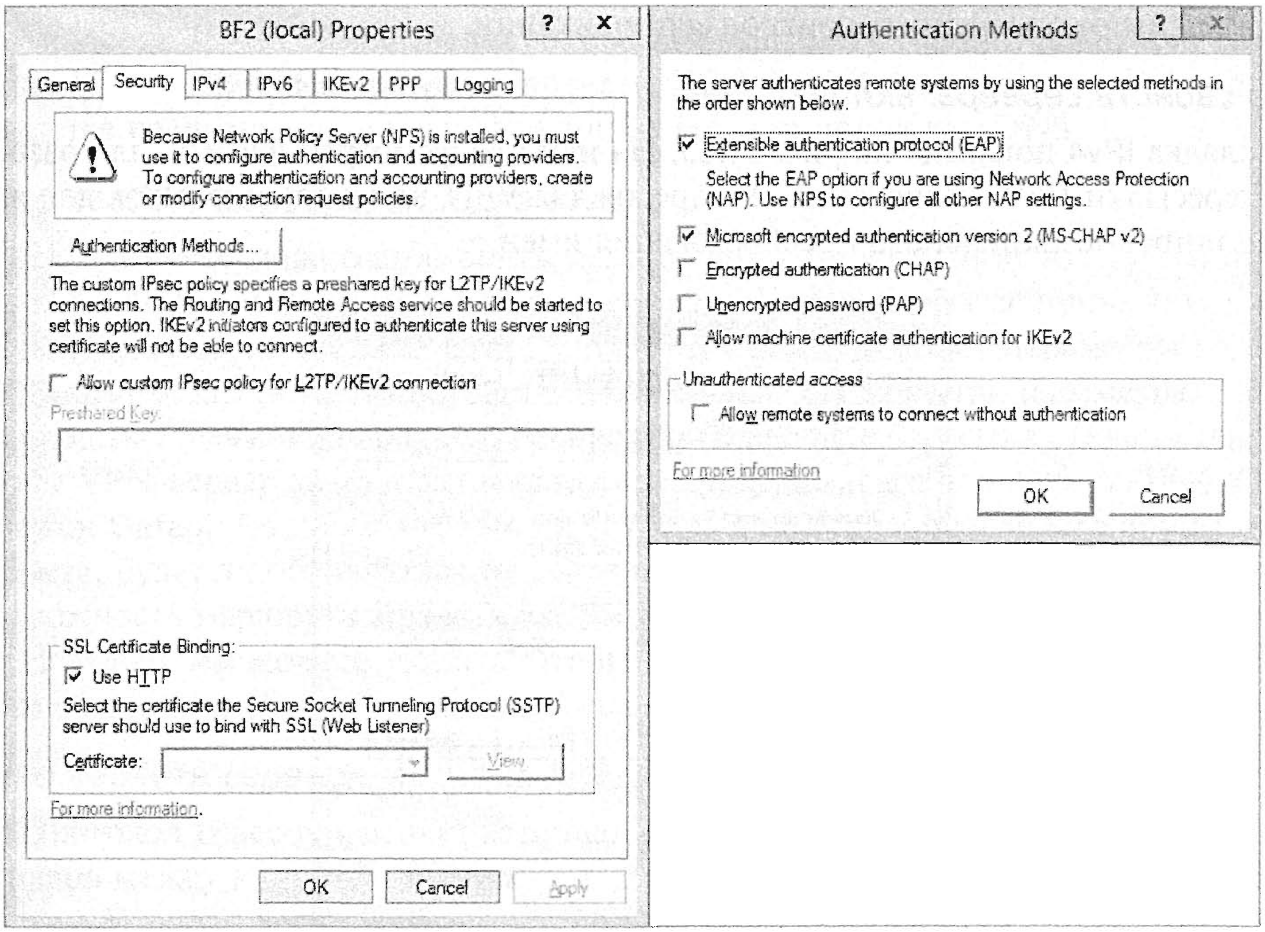


Рис. 21.24. Вкладка Security для сервера RRAS

На этой вкладке содержатся три основных параметра, включая аутентификацию; однако если вы развернули роль NPS, то управление параметрами аутентификации осуществляется этой ролью.

- **Authentication Methods (Методы аутентификации).** Если вы располагаете единственным VPN-сервером, то этот параметр будет установлен в Windows

Authentication (Аутентификация Windows). Это означает, что VPN-сервер будет аутентифицировать клиента с помощью типичных учетных данных Windows. Если же в организации существуют несколько VPN-серверов, то весьма вероятно наличие сервера RADIUS, поэтому можно выбрать RADIUS Authentication (Аутентификация RADIUS). После выбора RADIUS Authentication понадобится щелкнуть на кнопке Configure (Конфигурировать), чтобы предоставить информацию, которая позволит VPN-серверу подключаться к серверу RADIUS.

- **Allow Custom IPSec Policy (Разрешить специальную политику IPSec).** Протокол IPSec обычно используется с L2TP. В случае применения L2TP можно сконфигурировать специальную политику IPSec. Когда этот флажок отмечен, он требует совместно используемого ключа, который должен быть создан заблаговременно. Несмотря на возможность применения такого ключа, протокол Kerberos или сертификат обеспечивают более высокую безопасность.
- **SSL Certificate Binding (Привязка сертификата с использованием SSL).** В этой главе мы уже рассказывали об SSTP. Если вы намерены использовать этот протокол, то вам понадобится добавить к серверу сертификат, чтобы данные можно было шифровать с помощью SSL. После того как сертификат добавлен, его можно выбрать в раскрывающемся списке. Сертификаты должны быть получены от доверенных центров сертификации.

Окно свойств сервера: вкладка IPv4

Вкладка IPv4 показана на рис. 21.25. На ней предусмотрен флажок для разрешения пересылки IPv4, назначения IP-адресов для VPN-клиентов и флажок для включения широковещательного преобразования имен.

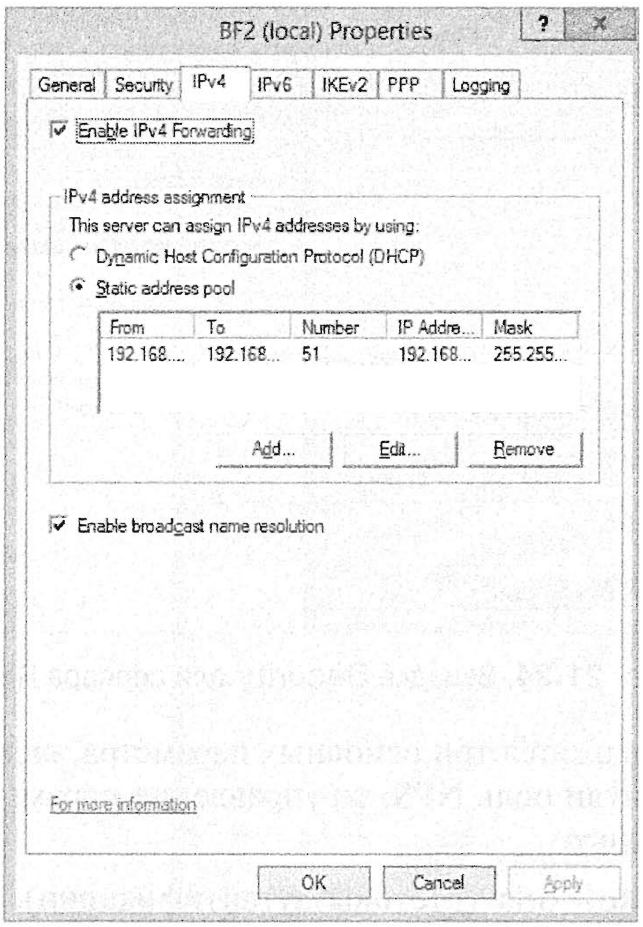


Рис. 21.25. Вкладка IPv4 для сервера RRAS

Если вы добавили серверную роль Routing and Remote Access Service и сконфигурировали ее с помощью процедуры, описанной в этой главе, то у вас имеется пул статических адресов, состоящий из 51 IP-адреса (от 192.168.10.200 до 192.168.10.250), которые можно назначать VPN-клиентам. Для назначения IP-адресов можно также применять существующий DHCP-сервер.

Сервер DHCP вовсе необязательно должен располагаться на том же сервере и даже в той же подсети, что и VPN-сервер. Он может быть любым DHCP-сервером, который достижим VPN-сервером. Тем не менее, поскольку VPN-сервер должен передавать DHCP-запросы из VPN-клиентов на DHCP-сервер, вы должны добавить агент пересылки DHCP (DHCP Relay Agent) в качестве дополнительной службы Routing and Remote Access Service.

Если флажок Enable broadcast name resolution (Включить широковещательное преобразование имен) отмечен, как предусмотрено по умолчанию, то клиенты могут преобразовывать имена во внутренней локальной сети, используя широковещательные передачи. Однако важно помнить, что такая передача не может проходить через маршрутизатор. Другими словами, широковещательные передачи будут преобразовывать имена только в той же внутренней подсети, которой принадлежит назначенный IP-адрес клиента.

Например, если клиент получает IP-адрес от VPN-сервера 192.168.10.101 с маской подсети 255.255.255.0, то широковещательные передачи будут преобразовывать лишь IP-адреса для клиентов в подсети 192.168.10.0. Клиентов в других подсетях придется распознавать с помощью других средств, таких как DNS.

Окно свойств сервера: вкладка IPv6

Вкладку IPv6 можно применять, если во внутренней сети используется протокол IPv6. Хотя применение IPv6 в Интернете становится все более привычным, его использование во внутренних сетях встречается реже, поэтому параметры на вкладке IPv6 могут остаться незатронутыми. Эта вкладка содержит три параметра.

Отметьте флажок Enable IPv6 Forwarding (Включить пересылку IPv6), если хотите, чтобы VPN-сервер действовал в качестве маршрутизатора для пакетов IPv6. Отмечая флажок Default Route Advertisement (Объявление стандартного маршрута), вы указываете, будет ли объявляться на сервере стандартный маршрут. Если у сервера есть возможность маршрутизировать пакеты IPv6, этот флажок должен быть отмечен.

Наконец, вы можете указать, чтобы назначение префикса IPv6 было совместимым с адресами IPv6 во внутренней сети.

Окно свойств сервера: вкладка IKEv2

Протокол IPSec применяет ассоциации безопасности для установки защищенных каналов между клиентом и сервером. Для определения таких ассоциаций безопасности в Windows Server 2008 R2 используется протокол IKEv2 (Internet Key Exchange version 2 — обмен ключами по Интернету версии 2). Кроме того, IKEv2 применяется для установки защищенного канала в случае, когда аутентификация осуществляется с помощью EAP-MS-CHAP v2.

На рис. 21.26 показана вкладка IKEv2 для сервера RRAS со стандартными параметрами. Эти параметры можно изменить для соответствия конкретным потребностям или средам.

Параметры перечислены ниже.

- **Idle Time-out (minutes) (Максимальное время бездействия (минут)).** Этот параметр задает продолжительность поддержания подключения в состоянии бездействия (в минутах), прежде чем IKEv2 прекратит сеанс. По умолчанию составляет 5 минут.
- **Network Outage Time (minutes) (Продолжительность перебоев в работе сети (минут)).** Этот параметр указывает, в течение какого времени (в минутах) может происходить повторная передача пакетов IKEv2 без получения ответа. Это может оказаться полезным, если в сети время от времени возникают перебои в работе из-за того, что в ней допускаются чересчур продолжительные подключения. По умолчанию составляет 30 минут.
- **Security Association Expiration Time (minutes) (Продолжительность действия ассоциации безопасности (минут)).** Когда продолжительность действия ассоциации безопасности подходит к концу, вырабатывается согласие относительно новой ассоциации безопасности и эта новая ассоциация создается до того, как будут переданы дополнительные данные. По умолчанию составляет 8 часов (480 минут).
- **Security Association Data Size Limit (MB) (Предел объема данных ассоциации безопасности (Мбайт)).** Когда достигается этот предел объема данных, вырабатывается согласие относительно новой ассоциации безопасности и эта новая ассоциация создается до того, как будут переданы дополнительные данные. По умолчанию составляет 100 Мбайт.

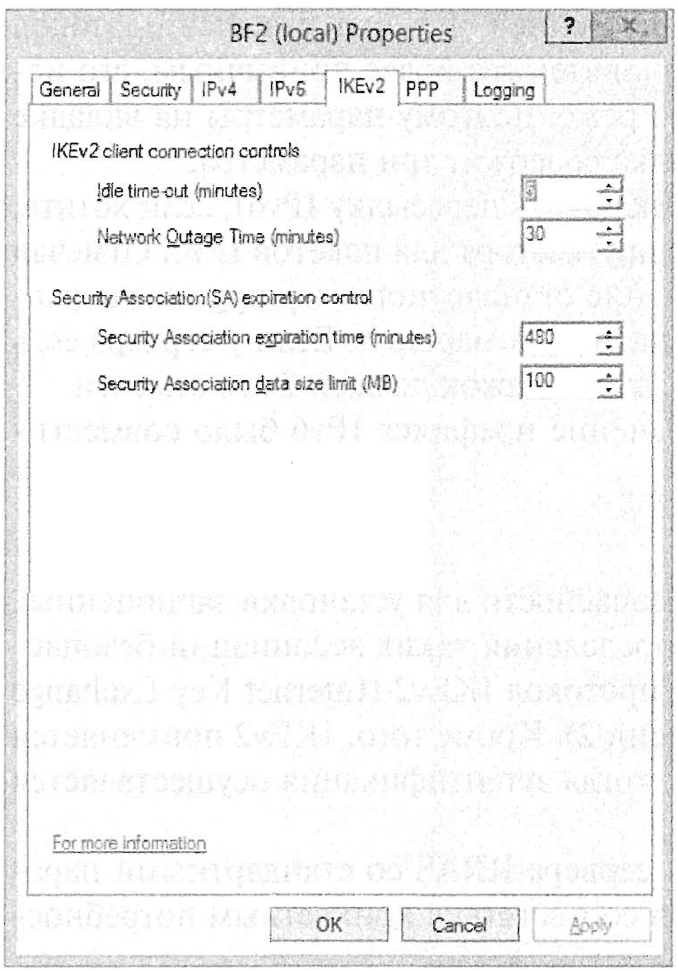


Рис. 21.26. Вкладка IKEv2 для сервера RRAS

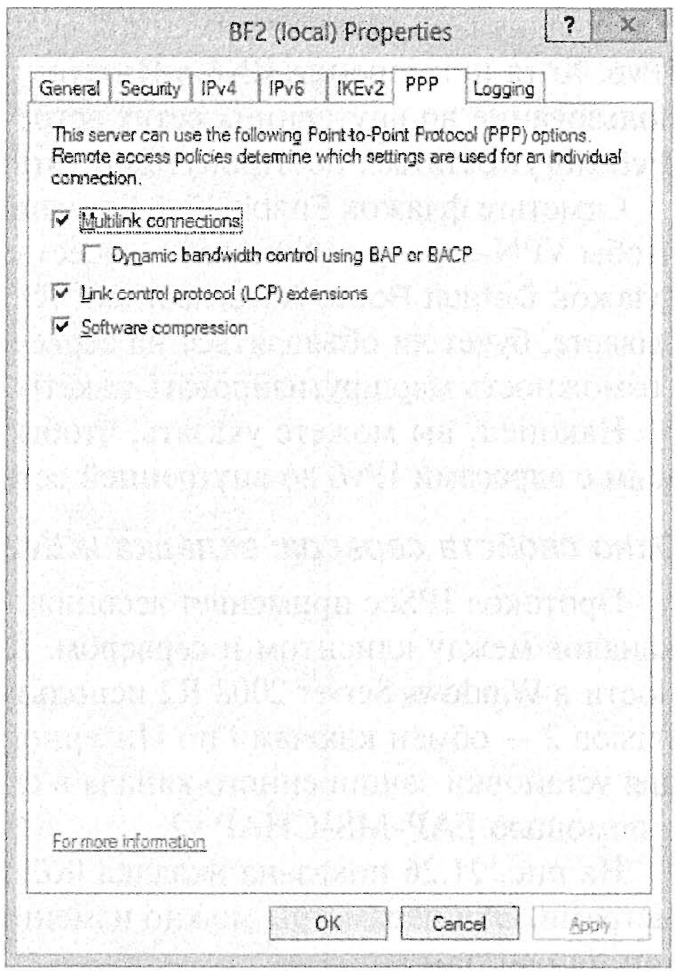


Рис. 21.27. Вкладка PPP для сервера RRAS

Окно свойств сервера: вкладка PPP

Протокол PPP применяется для коммутируемых подключений, а подключения подобного рода могут быть расширены с помощью разнообразных приемов, таких как использование подключений с группой линий передачи данных. На рис. 21.27 показаны параметры на вкладке PPP.

Параметры, конфигурируемые на данной вкладке, необязательно применяются ко всем пользователям. Вместо этого они определяют, что именно возможно на сервере, а параметры конкретной политики доступа к сети определяют, что может быть использовано для этой политики. Например, эти параметры можно было бы сконфигурировать так, чтобы разрешить применение на сервере подключений с группой линий передачи данных. С помощью политики, определенной для IT-администраторов, можно было бы разрешить использование таких подключений, тогда как посредством другой политики, ориентированной на рядовых пользователей, запретить им подобные подключения. Ниже перечислены доступные параметры.

- **Multilink Connections (Подключения, охватывающие группу линий передачи данных).** Когда этот флажок отмечен, клиенты дистанционного доступа могут объединять несколько подключений, чтобы увеличить доступную им полосу пропускания. Кроме того, это можно применять в подключениях маршрутизатора с дозвоном по требованию, используемых в VPN типа "шлюз-шлюз", которые соединяют офис филиала с головным офисом компании. Установив подключение с помощью двух линий, пропускная способность каждой из которых составляет 56 Кбит/с, можно обеспечить суммарную пропускную способность 112 Кбит/с.
- **Dynamic Bandwidth Control Using BAP or BACP (Динамическое управление полосой пропускания с помощью BAP или BACP).** Протоколы BAP и BACP разрешают динамическое добавление или изъятие линий исходя из интенсивности их применения. Например, если какой-то пользователь утилизировал две линии только на 10% их суммарной полосы пропускания, то вторая линия может быть автоматически изъята у пользователя и передана в распоряжение другим.
- **Link Control Protocol (LCP) Extensions (Расширения протокола управления каналом передачи данных).** Расширения LCP применяются для пересылки дополнительного трафика, связанного с данными об оставшемся времени и идентификации, которые используются для учета и регистрации событий. Если необходимости в таких данных нет, можно снять отметку с этого флажка, чтобы устранить дополнительный трафик на линии.
- **Software Compression (Программное сжатие).** Когда этот флажок отмечен, для сжатия данных применяется протокол Microsoft Point-to-Point Compression (MPPC).

Окно свойств сервера: вкладка Logging

Вкладка Logging (Регистрация) используется для указания, какие события и где регистрируются. Содержимое вкладки Logging показано на рис. 21.28. Хотя это не очевидно, параметры вкладки Logging на самом деле относятся к разным журналам событий. События, указываемые переключателями, заносятся в журнал событий и могут анализироваться с помощью программы просмотра событий (Event Viewer).

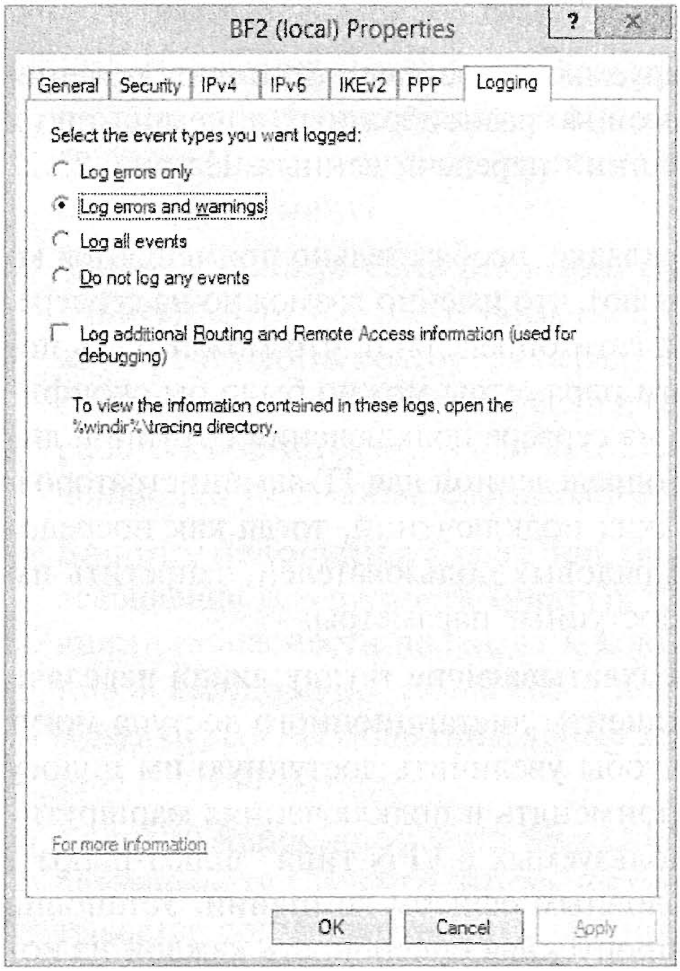


Рис. 21.28. Вкладка Logging для сервера RRAS

Предусмотрены следующие переключатели: Log errors only (Регистрировать только ошибки), Log errors and warnings (Регистрировать ошибки и предупреждения), Log all events (Регистрировать все события) и Do not log any events (Не регистрировать никаких событий). Более подробно о просмотре журналов событий будет рассказываться в главе 31.

Флажок Log additional Routing and Remote Access information (used for debugging) (Регистрировать дополнительную информацию Routing and Remote Access (используется для отладки)) совершенно не относится к журналам событий. Этот флажок применяется только при поиске и устранении специфичных проблем и может оказать большую помощь в локализации источника проблем.

Каждый раз, когда вы сталкиваетесь с журналами трассировки или отладки, имейте в виду одно важное обстоятельство: ведение таких журналов должно включаться только на период поиска и устранения проблемы и затем немедленно отключаться. Журналы трассировки и отладки потенциально потребляют значительные ресурсы, в том числе процессорное время, оперативную память и дисковое пространство. Действительно, все они полезны при поиске и устранении проблем, но если ведение журналов оставить включенным и далее, то это может повлиять на нормальное функционирование системы. Журналы трассировки хранятся в каталоге `%windir%\tracing`. По умолчанию этот каталог пуст, но когда вы выберете его, в нем будет создано несколько десятков файлов.

%WINDIR% ЧАСТО СООТВЕТСТВУЕТ C:\WINDOWS

`%windir%` — это переменная среды, которая указывает на место в системе, где установлена ОС Windows. Устанавливать Windows на диск C вовсе не обязательно, и в операционных системах предшествующих версий каталог для ОС Windows можно было называть по-другому. Тем не менее, операционная система всегда должна иметь возможность находить каталог, в котором она установлена, поэтому при загрузке ОС записывает в переменную `%windir%` фактический путь к каталогу Windows.

Значение переменной `%windir%` можно просмотреть, введя в командной строке **`%windir%`**. Командная строка будет интерпретировать эту переменную как `C:\Windows` (или другой каталог, где расположена ОС Windows). `C:\Windows` не является допустимой командой, поэтому будет выдано сообщение об ошибке, но первая часть этого сообщения говорит о том, как интерпретируется `%windir%`. Ту же процедуру можно повторить для любой переменной, такой как `%systemroot%` или `%programfiles%`.

Мониторинг клиентов удаленного доступа

После того как VPN-сервер начнет обслуживание VPN-клиентов, время от времени возникает потребность в наблюдении за его деятельностью. На рис. 21.29 показан узел Remote Access Clients (Клиенты удаленного доступа) с подключенным удаленным клиентом.

Это представление показывает, кто подключен в данный момент, насколько долго поддерживаются подключения (продолжительность), количество используемых портов (если подключение задействует несколько линий передачи данных) и текущее состояние подключений (активные или бездействуют). Здесь можно отключить любого пользователя, щелкнув правой кнопкой мыши на подключении и выбрав в контекстном меню пункт Disconnect (Отключить).

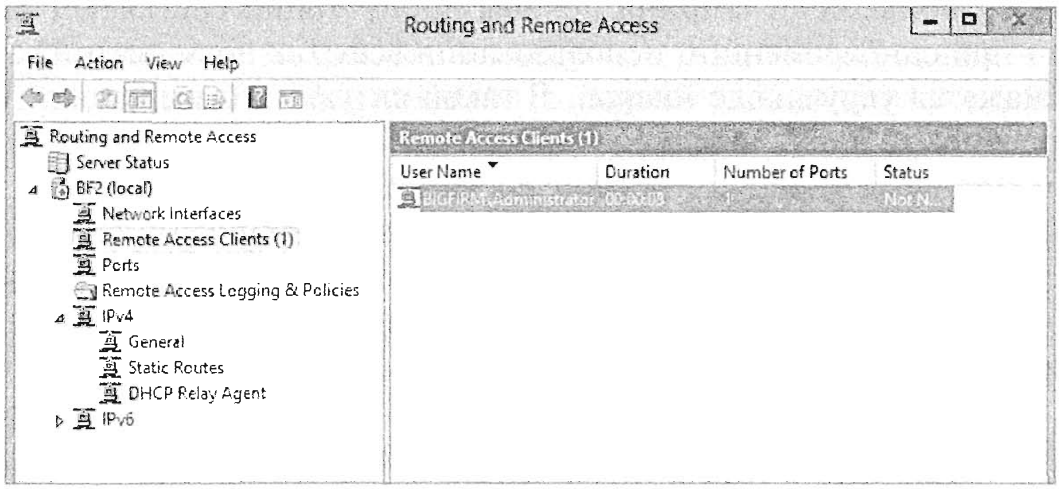


Рис. 21.29. Просмотр активных клиентов

Конфигурирование портов

В результате создания VPN-сервера автоматически создается множество портов — 128 портов PPTP, 128 портов SSTP, 128 портов IKEv2 и 128 портов L2TP. Созданные порты можно видеть на рис. 21.30.

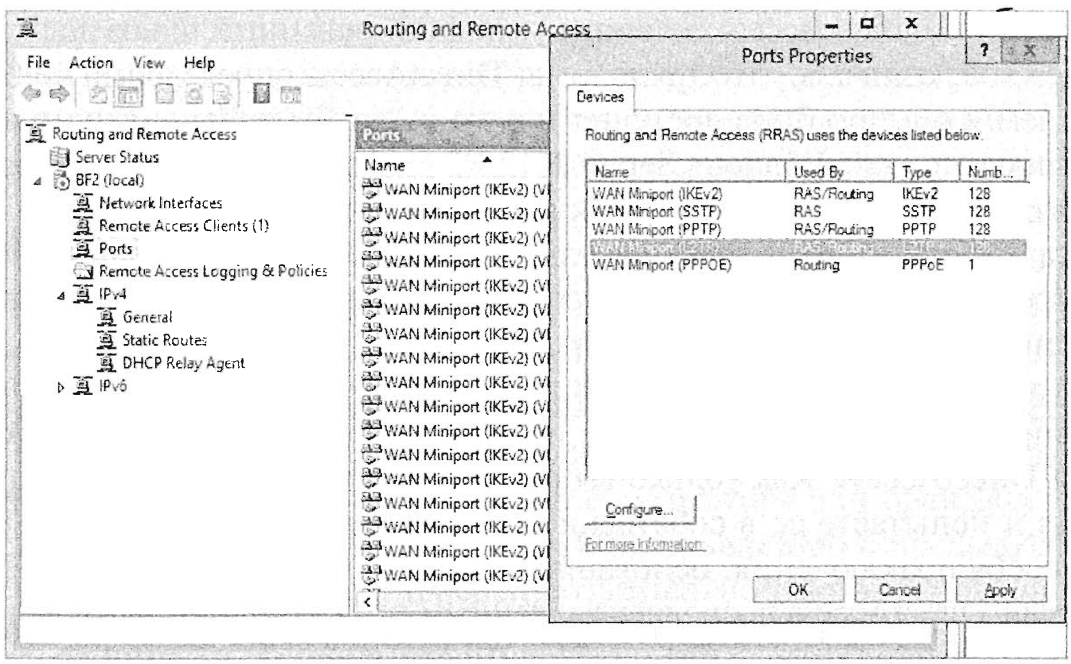


Рис. 21.30. Просмотр свойств портов на сервере RRAS

Обычно вы будете применять только один тип портов. Другими словами, если вы используете SSTP для VPN-подключений, то не будете иметь дело с портами PPTP и, скорее всего, не будете применять порты L2TP или IKEv2.

Количество используемых портов зависит от ширины полосы пропускания, требуемой каждому пользователю, и общей полосы пропускания, доступной для подключения к серверу. Если сетевая карта подключена к каналу WAN со скоростью 100 Мбит/с (большое везение), то для выбранного протокола можно поддерживать гораздо больше, чем 128 подключений, выполнив следующие действия.

1. Выберите порт.
2. Щелкните на кнопке Configure (Конфигурировать).
3. Измените число, чтобы разрешить большее количество подключений.

С другой стороны, если ширина полосы пропускания составляет лишь около 1 Мбит/с, то при одновременном использовании всех 128 подключений производительность окажется удручающе низкой. В такой ситуации имеет смысл уменьшить количество возможных подключений.

Итак, вы уже знаете, как добавить и настроить роль Network Policy and Access Services, а также роль Remote Access, и затем сконфигурировать сервер в качестве VPN-сервера. Далее мы приступим к обсуждению DirectAccess и преимуществ, которые можно получить в результате переноса клиентов и инфраструктуры удаленного доступа на DirectAccess.

Введение в DirectAccess

Технология DirectAccess представляет собой относительно новую функциональность удаленного доступа, которая впервые появилась в Windows Server 2008 R2. Внедрение DirectAccess продвигалось не слишком успешно, главным образом из-за того, что приведение DirectAccess в рабочее состояние было сопряжено с немалыми трудностями — для этого нужно было хорошо разбираться в IPv6 и знать все тонкости команды `netsh`. То обстоятельство, что подлинный опыт применения DirectAccess можно было приобрести лишь в случае запуска DirectAccess вместе с продуктом UAG (Unified Access Gateway — унифицированный шлюз доступа) производства Microsoft, означало, что технология DirectAccess определенно не была дешевым решением и обычно была доступна только крупным предприятиям.

Однако после выхода Windows Server 2012 R2 ситуация с DirectAccess изменилась. В Microsoft пересмотрели свой подход к развертыванию и управлению DirectAccess. В результате это поистине фантастическое решение в области удаленных подключений стало доступным гораздо более широкой аудитории.

Возможно, вы удивитесь формулировке “поистине фантастическое решение в области удаленных подключений”. В этом разделе мы объясним, почему именно так оцениваем DirectAccess, а позже пройдемся по процедурам развертывания и управления DirectAccess. Как только вы ознакомитесь с возможностями технологии DirectAccess и испытаете ее в собственной среде, вам будет трудно возвратиться к старому способу подключения, основанному на клиентах VPN.

Технология DirectAccess позволяет удаленным пользователям безопасно подключаться к корпоративной среде без необходимости в использовании традиционного клиента VPN. Иногда это называют “VPN с автоматической установкой соедине-

ния", поскольку такому решению присущи все привычные достоинства сетей VPN, но оно не влечет за собой административных накладных расходов для конечных пользователей и не заставляет IT-администраторов конфигурировать и управлять многочисленными методами аутентификации, которые сопровождают сторонние VPN-клиенты. Когда компьютер, который сконфигурирован на установление подключений с помощью DirectAccess, подключен к Интернету и удовлетворяет политикам, заданным администратором DirectAccess, он всегда будет автоматически подключаться к внутренней офисной сети — даже до того, как пользователь войдет в систему. Пользователям вообще нет нужды задумываться об установлении подключений, а с точки зрения IT-администратора эти удаленные компьютеры всегда находятся под его контролем и управлением.

Функционирование DirectAccess

После развертывания DirectAccess вы получаете постоянное, основанное на IPSec удаленное подключение к офисной сети, которым удобно управлять посредством групповой политики. Как лицо, отвечающее за управление решением дистанционного доступа в сеть вашей компании, вы наверняка хорошо знакомы с сотрудниками, постоянно жалующимися в службу поддержки на невозможность удаленного входа, забывающими имя пользователя или пароль и т.п.

Все эти проблемы исчезают сами собой, когда вы предоставляете тем же самым сотрудникам средства подключения DirectAccess. Тот факт, что шифрование данных, инкапсуляция пакетов и аутентификация происходят при инициализации стека протоколов TCP/IP на стороне клиента еще до входа пользователя в систему, приводит к ситуации, когда в выигрыше оказываются все стороны. При этом по-прежнему имеется возможность применения обновлений и групповых политик.

Возможности DirectAccess

Ниже приведен список возможностей DirectAccess, которыми вы можете воспользоваться при работе с Windows Server 2012 R2.

- **Отсутствие предварительных условий, касающихся PKI.** В предыдущей версии DirectAccess обязательным условием применения сертификатов для аутентификации было развертывание инфраструктуры открытых ключей (Public Key Infrastructure — PKI). В небольших средах конфигурирование и управление выделенной инфраструктурой PKI было настоящей головной болью для администраторов. В данном выпуске DirectAccess определенные сценарии попрежнему предполагают использование сертификатов для аутентификации, но сейчас появилась возможность применения самозаверяющего сертификата в мастере конфигурирования.
- **Поддержка позади устройства NAT.** Функциональность DirectAccess можно развернуть либо как пограничный сервер в DMZ, либо внутри основной сети позади устройства NAT наподобие маршрутизатора или брандмауэра. Это является приятным усовершенствованием по сравнению с предыдущей версией DirectAccess и означает, что теперь необязательно иметь под рукой множество сетевых карт и IP-адресов, если вы всего лишь хотите быстро привести среду в работоспособное состояние.

- **Поддержка балансировки нагрузки.** Для обеспечения высокой доступности и масштабируемости вместе с DirectAccess можно развернуть средство NLB (Windows Network Load Balancing — балансировка сетевой нагрузки Windows) или какое-то стороннее решение подобного рода.
- **Поддержка множества доменов.** Если нужно обеспечить пользователям возможность установления удаленных подключений через несколько доменов, то сейчас такая функциональность является интегрированной в DirectAccess.
- **Интеграция с NAP.** Чтобы гарантировать работоспособное состояние удаленных клиентов (когда установлены все обновления антивирусного ПО, включено средство BitLocker и т.д.) перед получением ими доступа во внутреннюю сеть, DirectAccess можно интегрировать с развертыванием NAP (Network Access Protection — защита сетевого доступа).
- **Мониторинг и диагностика.** Доступна удобная управляющая панель Monitoring (Мониторинг), которая отображает сводную информацию о подключенных клиентах, а также метрики входящего/исходящего трафика. С помощью представления Operations Status (Состояние операций) главной консоли можно также проверить работоспособность развертывания DirectAccess.
- **Улучшения производительности IP-HTTPS.** Одной из главных причин, по которым подключение к сети посредством DirectAccess обеспечивает более высокую производительность по сравнению с традиционными VPN-клиентами, является применение для коммуникаций IPv6 как основного стека протоколов. IPv6 представляет собой новейший и в итоге более быстродействующий стек, чем прежний хорошо знакомый стек IPv4. В число технологий перехода на IPv6 входит IP-HTTPS, где удалось добиться значительного выигрыша, касающегося масштабирования и снижения накладных расходов.
- **Поддержка Server Core и PowerShell.** Компонент DirectAccess в Windows Server 2012 R2 будет работать с установками Server Core операционной системы Windows Server 2012 R2 и также предоставляет полную поддержку Windows PowerShell — в отличие от своего предшественника, который не поддерживал ни то, ни другое.

Командлеты PowerShell для роли Remote Access

Теперь в вашем распоряжении имеется свыше 60 новых командлетов, которые обеспечивают поддержку PowerShell для роли Remote Access. С точки зрения DirectAccess эти новые командлеты позволяют добавлять и удалять элементы конфигурации, включать многосайтовое развертывание и даже предоставлять помощь при поиске и устранении проблем в клиентских системах. Полный список новых командлетов вместе с их описанием находится по адресу `http://tinyurl.com/ws2012racmdlets`.

- **Многосайтовая поддержка.** Если вы отвечаете за управление крупной производственной средой, которая охватывает несколько сайтов и географических площадок, то вас должна заинтересовать новая возможность DirectAccess — Multisite Support (Многосайтовая поддержка). Она позволяет развертывать в

сетях множество точек входа сервера DirectAccess, обеспечивая клиентам наилучшую производительность удаленного подключения независимо от их местоположения.

Поддержка клиентов

Чтобы подключаться к серверу DirectAccess, клиентский компьютер должен функционировать под управлением ОС Windows 7 Enterprise, Windows 7 Ultimate или Windows 8/8.1 Enterprise. Поскольку DirectAccess является составной частью роли Remote Access в Windows Server 2012 R2, не должно вызывать удивления то обстоятельство, что этот компонент может сосуществовать с конфигурациями RRAS в целях поддержки любых унаследованных клиентов, которые нуждаются в доступе к VPN, но не располагают операционной системой, обеспечивающей возможность подключения к DirectAccess.

Требования DirectAccess

Ниже перечислены минимальные требования, которые должны быть удовлетворены, чтобы можно было развернуть DirectAccess.

- **Active Directory.** Вы должны иметь функционирующую среду Active Directory, т.к. DirectAccess использует группы доступа и групповую политику (Group Policy) для помещения своих конфигурационных изменений на стороны клиентов.
- **Контроллеры домена.** Для поддержки DirectAccess должен быть развернут, по меньшей мере, один контроллер домена Windows Server 2012 R2 или последующей версии.
- **Группа доступа клиентов DirectAccess.** Создайте группу доступа Active Directory, используемую для хранения учетных записей компьютеров, которым вы предоставите возможность подключения с помощью DirectAccess. Можете назвать ее, например, `DirectAccess Clients`.
- **Сервер DirectAccess.** На виртуальном или физическом компьютере Windows Server 2012 R2 требуется включить роль Remote Access, которая входит в состав функциональности DirectAccess.
- **Один внутренний IP-адрес.** Если вы развертываете DirectAccess из внутренней сети (в отличие от сети Edge/DMZ), то вам необходимо гарантировать наличие на сервере DirectAccess хотя бы одной сетевой карты со статическим IP-адресом, а также сконфигурировать порт 443 и пересылку номера IP-протокола 41 через устройство NAT для этого IP-адреса.
- **Внешняя DNS-запись.** Вам понадобится сконфигурировать внешнюю DNS-запись A, сопоставляющую дружественное имя вроде `directaccess.bigfirm.com` с открытым IP-адресом, который будет соединять NAT-порт 443 с внутренним IP-адресом. В качестве альтернативы можно воспользоваться поставщиком динамической DNS, таким как Dyn DNS (`http://dyn.com/dns`) или FreeDNS (`http://freedns.afraid.org`).
- **Клиенты/рабочие станции.** Как упоминалось ранее, чтобы можно было работать с DirectAccess, клиентские компьютеры должны функционировать под управлением ОС Windows 7 Enterprise, Windows 7 Ultimate или Windows 8/8.1

Enterprise. Кроме того, они должны быть частью домена Active Directory, чтобы иметь возможность принимать обновления групповой политики от сервера DirectAccess.

- **Брандмауэр Windows клиентского компьютера.** Этот аспект совершенно очевиден, но в то же время является камнем преткновения для многих из тех, кто занимается развертыванием DirectAccess. У любых клиентов, которые вы хотите подключить к серверу DirectAccess, должна быть активизирована служба брандмауэра Windows с включенными параметрами для частной и общественной сетей. Когда параметры групповой политики переносятся на клиентов, они создают определенные правила и вносят определенные изменения в брандмауэр Windows, и если он отключен, то DirectAccess работать не будет. Это средство лучше всего сконфигурировать и заблокировать с помощью централизованной групповой политики для компьютеров всех пользователей.

Установка DirectAccess

В этом разделе вы ознакомитесь с процедурой установки и запуска DirectAccess внутри существующей среды. Мы будем развертывать топологию DirectAccess позади пограничного устройства с единственным сетевым адаптером. Такой подход позволит любому выполнить описанные шаги с минимальными усилиями и ресурсами в испытательной среде. Мы также будем предполагать, что вы успешно выполнили все задачи, описанные ранее в главе, располагаете развернутой ролью Remote Access с единственной сконфигурированной службой RRAS и обеспечили удовлетворение минимальных требований к развертыванию DirectAccess, которые обсуждались в предыдущем разделе.

1. Войдите в систему Windows Server 2012 R2, присоединенную к домену, с помощью учетной записи, которая имеет административные разрешения на уровне домена. В окне диспетчера серверов при выбранном пункте меню Local Server (Локальный сервер) выберите в меню Tools (Сервис) пункт Remote Access Management (Управление удаленным доступом).
2. В консоли управления удаленным доступом (Remote Access Management Console), окно которой показано на рис. 21.31, щелкните на элементе Configuration (Конфигурация) в навигационной панели слева.
3. Должно открыться окно мастера включения DirectAccess (Enable DirectAccess Wizard). Щелкните на кнопке Next (Далее), чтобы начать проверку предварительных условий и инициализацию конфигурации.
4. На экране DirectAccess Client Setup (Настройка клиента DirectAccess) щелкните на кнопке Add (Добавить), выберите группу доступа, сконфигурированную ранее в рамках одного из предварительных условий, и щелкните на кнопке Next.
5. На экране Remote Access Server Setup (Настройка сервера удаленного доступа), показанном на рис. 21.32, выполните следующие действия.
   а. Выберите переключатель Behind an edge device (with a single network adapter) (Позади пограничного устройства (с единственным сетевым адаптером)).
   б. Введите с открытое DNS-имя, которое клиенты будут использовать для подключения к серверу Remote Access (это должна быть внешняя DNS-запись

А или запись Dynamic DNS, созданная при выполнении минимальных требований к развертыванию DirectAccess).

в. Щелкните на кнопке Next.

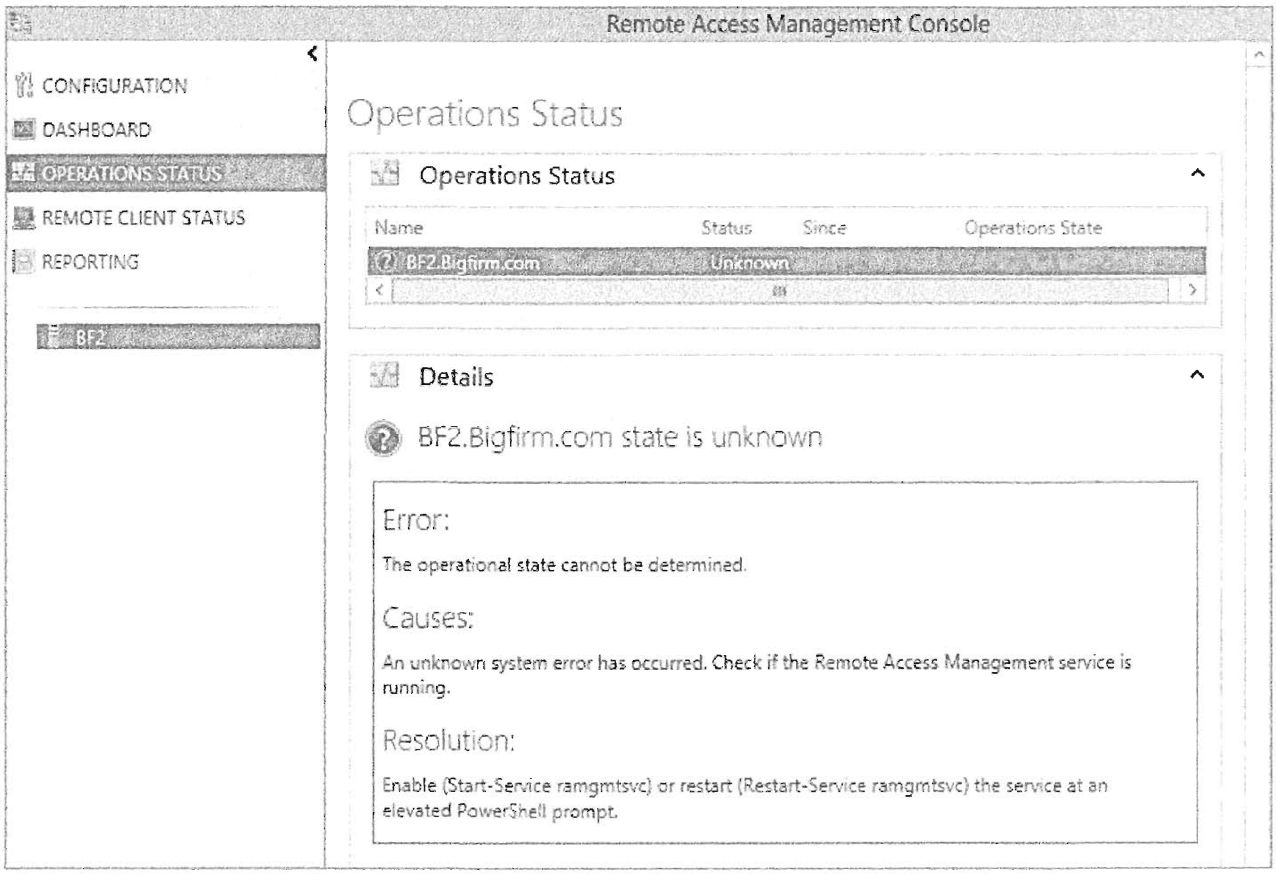


Рис. 21.31. Консоль управления удаленным доступом

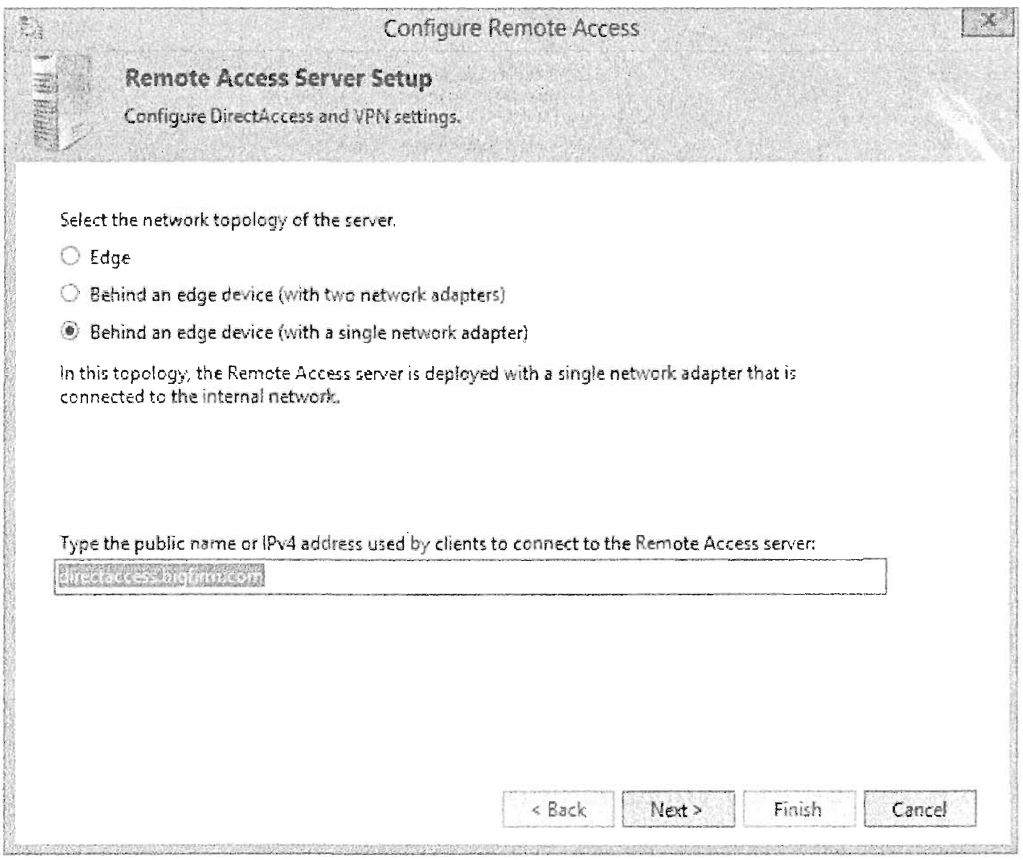


Рис. 21.32. Конфигурирование топологии и открытого имени DirectAccess

6. На экранах Infrastructure Server Setup (Настройка инфраструктурного сервера) и Configure Remote Access (Конфигурирование удаленного доступа) оставьте параметры, выбранные по умолчанию, и щелкните на кнопке Next, чтобы продолжить работу.
7. На последнем экране просто щелкните на кнопке Finish (Готово).

   На данном этапе не стоит беспокоиться о внесении каких-либо изменений в стандартную конфигурацию, т.к. вы будете делать это на более детальном уровне в управляющей панели Configuration по завершении начальной установки.
8. После того как сервер DirectAccess сконфигурирован, щелкните на кнопке Close (Закрыть), чтобы выйти из мастера.
9. Откройте консоль управления удаленным доступом (Remote Access Management Console) и снова щелкните на элементе Configuration (Конфигурация), находящемся в навигационной панели слева.

   На этот раз вы должны увидеть диаграмму, описывающую четыре шага, которые помогут сконфигурировать развертывание DirectAccess (рис. 21.33).

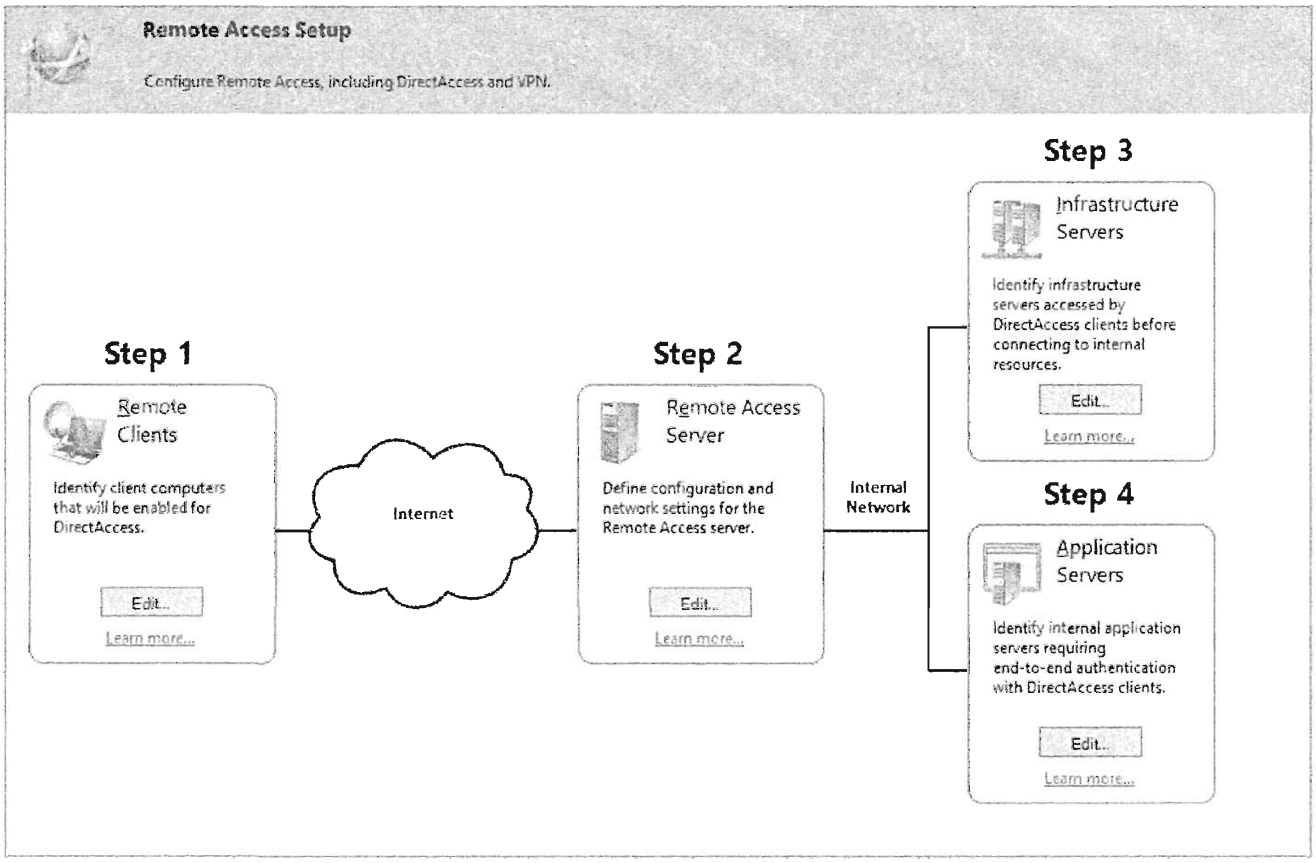


Рис. 21.33. Диаграмма конфигурации DirectAccess

10. Щелкните на кнопке Edit (Правка) в области Step 1, Remote Clients (Шаг 1, удаленные клиенты), чтобы открыть мастер настройки клиентов DirectAccess (DirectAccess Client Setup Wizard).
11. Оставьте выбранным переключатель Deploy full DirectAccess for client access and remote management (Развернуть полную версию DirectAccess для доступа клиентов и удаленного управления), как предложено по умолчанию, и щелкните на кнопке Next.

12. На экране Select Groups (Выбор групп), показанном на рис. 21.34, позаботьтесь о том, чтобы была представлена группа доступа Active Directory, созданная ранее в рамках выполнения минимальных требований к развертыванию DirectAccess, а любые другие группы, не относящиеся к делу, были удалены.

    Обратите внимание на флажок Enable DirectAccess for mobile computers only (Включить DirectAccess только для мобильных компьютеров). Если отметить его, выполнится запрос WMI для идентификации всех объектов компьютеров, которые представляют мобильные компьютеры, такие как ноутбуки. После идентификации для них включается DirectAccess, а любые немобильные компьютеры игнорируются.

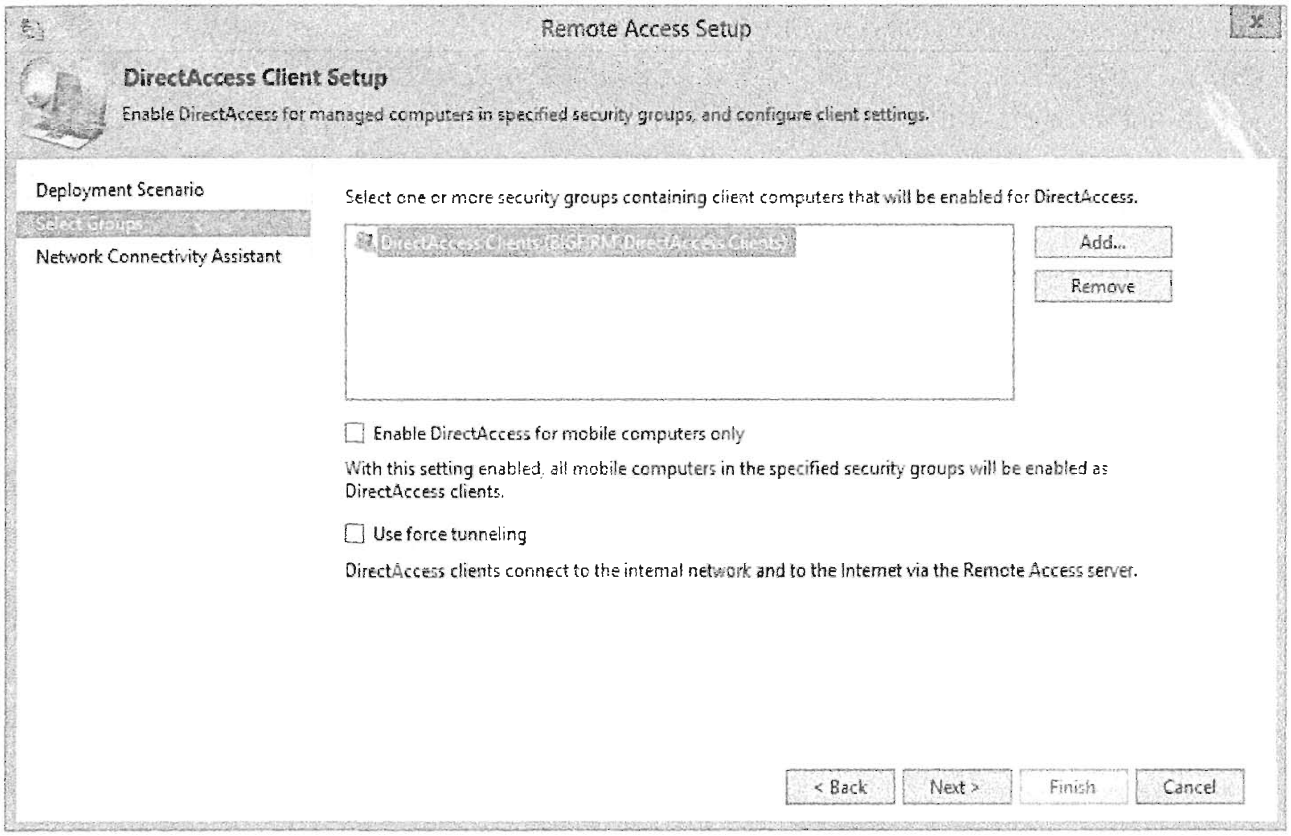


Рис. 21.34. Выбор группы доступа `DirectAccess Clients`

Однако будьте осторожны с этим флажком, поскольку если вы отметите его в процессе первоначального конфигурирования, а позже решите сделать DirectAccess доступным стационарным компьютерам в офисе филиала (т.е. не ноутбукам), то это не удастся до тех пор, пока не будет снята отметка с данного флажка.

13. Сделав выбор, щелкните на кнопке Next, чтобы продолжить.

    Финальный экран, относящийся к шагу 1, позволяет указать ресурсы, которые можно использовать в сочетании со средством NCA (Network Connectivity Assistant — помощник по подключению к сети), чтобы определить, подключен ли клиент к внутренней сети. При желании здесь можно оставить стандартный тип ресурса HTTP.

    Здесь следует также отметить чрезвычайно полезный параметр DirectAccess connection name (Имя подключения DirectAccess). Мы рекомендуем изменить его так, чтобы он соответствовал требованиям вашей организации, поскольк-

ку это будет идентификатором подключения, который отображается в сетевой панели каждого дистанционно подключаемого клиента DirectAccess.

14. Выбрав требуемые параметры, щелкните на кнопке Finish, чтобы завершить конфигурирование клиентов.
15. Теперь щелкните на кнопке Edit в области Step 2, Remote Access Server (Шаг 2, сервер удаленного доступа). Первым экраном, который вы увидите, будет Network Topology (Топология сети).
16. Подтвердите, что ваши параметры топологии и открытое DNS-имя сконфигурированы корректно, и для продолжения щелкните на кнопке Next.

    На экране Network Adapters (Сетевые адаптеры) вы можете видеть адаптер, который вы применяется для подключения DirectAccess к внутренней сети, а также сертификат, используемый для всех подключений IP-HTTPS. Именно здесь вы можете принять решение о применении либо открытого доверенного сертификата, либо базового самозаверяющего сертификата для аутентификации любых клиентов IP-HTTPS, которые используют DirectAccess.
17. Щелкните на кнопке Next, чтобы продолжить работу.

    Следующим экраном является Authentication (Аутентификация), как показано на рис. 21.35. Вам следует уделить особое внимание этому шагу, если хотите подключать к своему серверу DirectAccess устройства, функционирующие под управлением Windows 7.

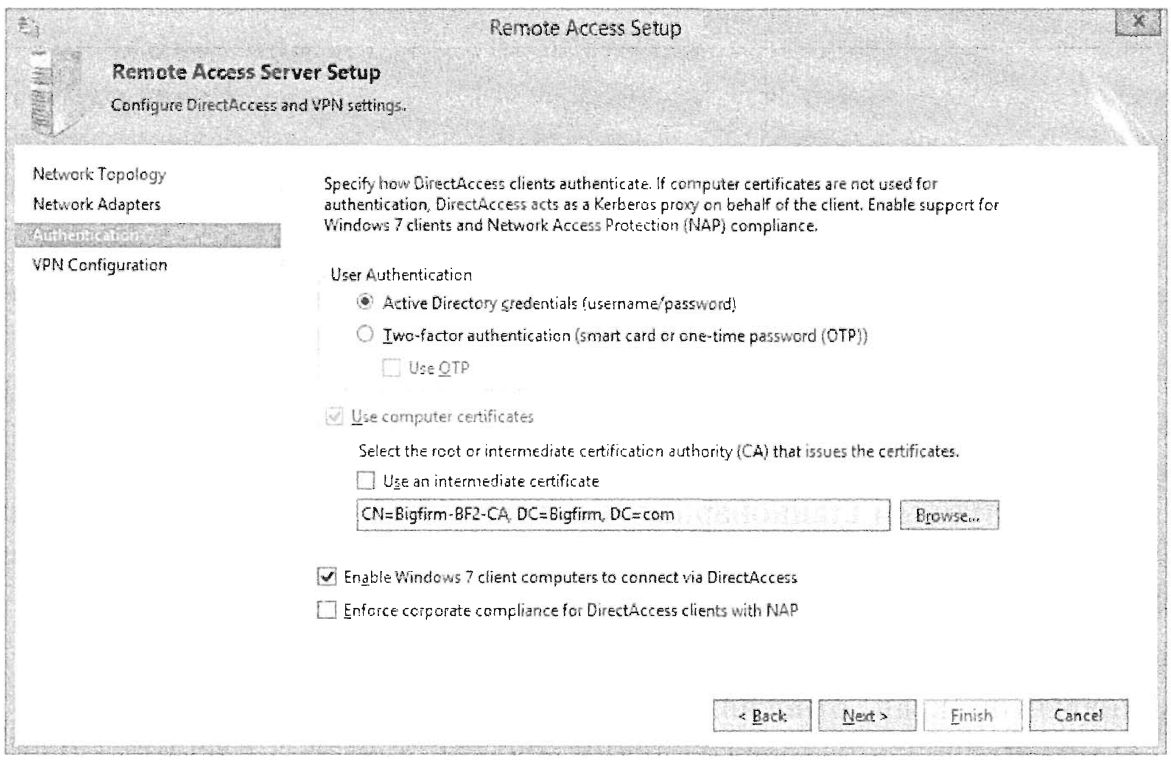


Рис. 21.35. Включение клиентов Windows 7

Обратите внимание на флажок Enable Windows 7 client computers to connect via DirectAccess (Разрешить клиентским компьютерам Windows 7 подключаться через DirectAccess). Предоставление такого разрешения по умолчанию не предусмотрено, и для многих это является еще одной ловушкой. Обязательно

отметьте этот флажок, если вы планируете задействовать клиентские компьютеры Windows 7.

18. Для продолжения щелкните на кнопке Next.

    На рис. 21.36 показан финальный экран мастера, VPN Configuration (Конфигурация VPN). Здесь задается способ назначения IP-адресов удаленным клиентам, подключающимся посредством VPN. Вы можете выбрать сервер DHCP или указать пул статических IP-адресов. Вкладка Authentication (Аутентификация) предоставляет возможность применения сервера RADIUS для аутентификации клиентов.

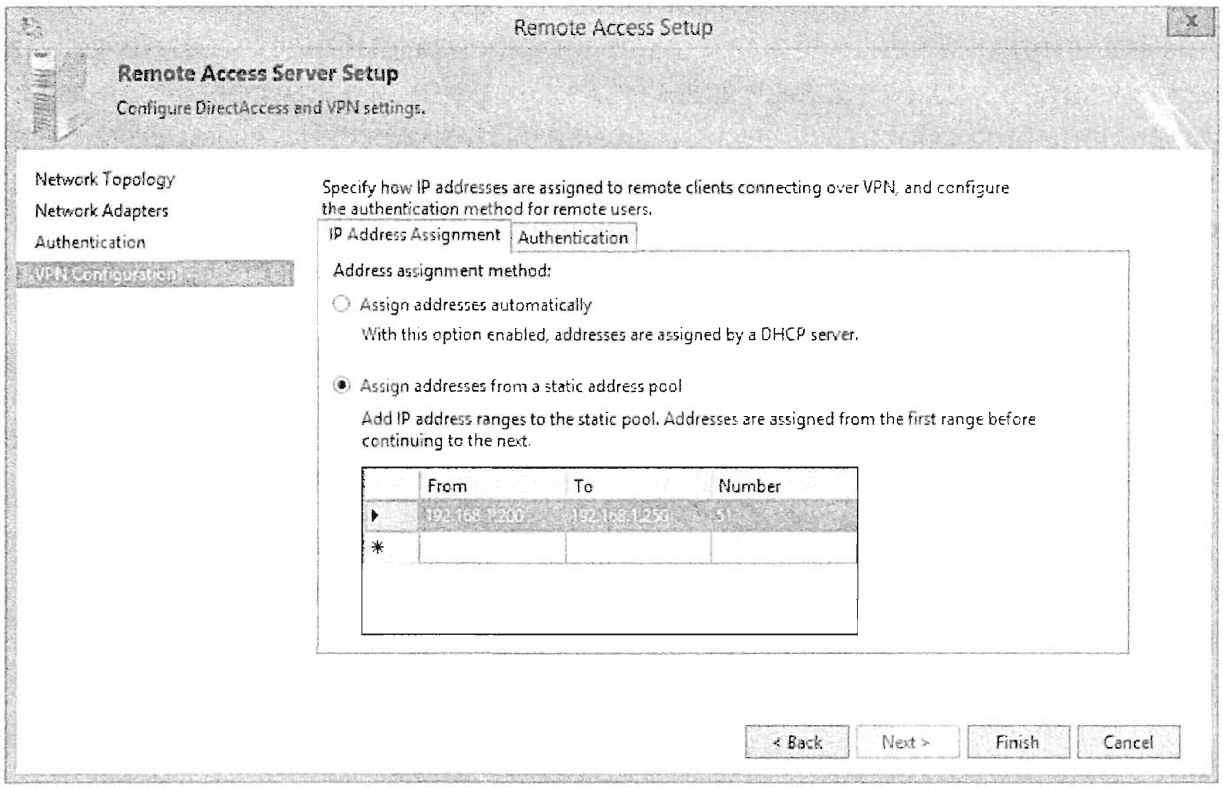


Рис. 21.36. Экран VPN Configuration

19. Сделав выбор, щелкните на кнопке Finish, чтобы завершить работу мастера.
20. Щелкните на кнопке Edit в области Step 3, Infrastructure Servers (Шаг 3, инфраструктурные серверы), чтобы открыть экран мастера Network Location Server (Сервер сетевых расположений). Здесь вы можете изменить сертификат, используемый сервером сетевых расположений для аутентификации клиентов. Мы оставим его в том виде, как предусмотрено по умолчанию, т.е. самозаверяющий сертификат.
21. Щелкните на кнопке Next.

    Экран DNS позволяет выбрать локальные параметры преобразования имен; и снова можно оставить стандартные установки без изменений.

22. Щелкните на кнопке Next.

    Экран DNS Suffix Search List (Список поиска DNS-суффиксов) позволяет указать дополнительные списки поиска DNS-суффиксов, которые будут применяться для клиентов DirectAccess. Это может пригодиться в многодоменных развертываниях, но в случае стандартных конфигураций здесь нет необходимости вносить изменения.

23. Щелкните на кнопке Next, чтобы продолжить работу.

    Экран Management (Управление) позволяет указать серверы управления, которые могут быть использованы для внесения обновлений и изменений в удаленно подключенные клиенты. Например, здесь можно было бы указать сервер System Center 2012 R2 Configuration Manager (Диспетчер конфигурации системного центра 2012 R2).

24. Завершив внесение изменений, щелкните на кнопке Finish.

25. Щелкните на кнопке Edit в области Step 4, Application Servers (Шаг 4, серверы приложений), чтобы открыть экран DirectAccess Application Server Setup (Настройка серверов приложений DirectAccess). Здесь вы можете принять решение расширить аутентификацию между клиентами DirectAccess и указанными серверами приложений. Вы также можете ограничить круг серверов, к которым разрешено подключаться пользователям DirectAccess, указав содержащие их группы доступа. В таком расширении нет необходимости, поэтому мы оставляем выбранный по умолчанию переключатель Do not extend authentication to application servers (Не распространять аутентификацию на серверы приложений).

26. Щелкните на кнопке Finish.

    Прежде чем завершить работу консоли, вы должны сохранить изменения, внесенные в конфигурацию, и обновить глобальные объекты групповой политики, которые DirectAccess применяет для конфигурирования клиентов.

27. Щелкните на кнопке Finish под диаграммой рядом с сообщением Some configuration changes have not yet been applied. Click Finish to apply the changes (Некоторые изменения в конфигурации еще не были применены. Щелкните на кнопке Finish, чтобы изменения вступили в силу).

Конфигурирование клиента DirectAccess

Теперь, когда компонент DirectAccess установлен на сервере, можно двигаться дальше и подключить клиентов. Возможность подключения будет проверяться на мобильном компьютере Windows 8 Enterprise. Ниже перечислены необходимые действия.

1. Добавьте в Active Directory учетную запись своего компьютера Windows 8 Enterprise в группу доступа, указанную при обработке шага “Step 1, Remote Clients” диаграммы конфигурации DirectAccess.
2. Удостоверьтесь, что брандмауэр Windows включен, как обсуждалось ранее в разделе “Требования DirectAccess”.
3. Подключив компьютер Windows 8 к корпоративной среде Active Directory, обновите групповую политику, для чего или откройте окно командной строки и введите команду `gpupdate /force`, или просто перезагрузите систему компьютера и снова войдите в домен.
4. Чтобы быстро проверить, действительно ли групповая политика была обновлена на вашем клиенте, откройте брандмауэр Windows и щелкните на элементе Connection Security Rules (Правила безопасности подключения).

   Вы должны увидеть, что обновленные правила DirectAccess применены, примерно так, как показано на рис. 21.37.

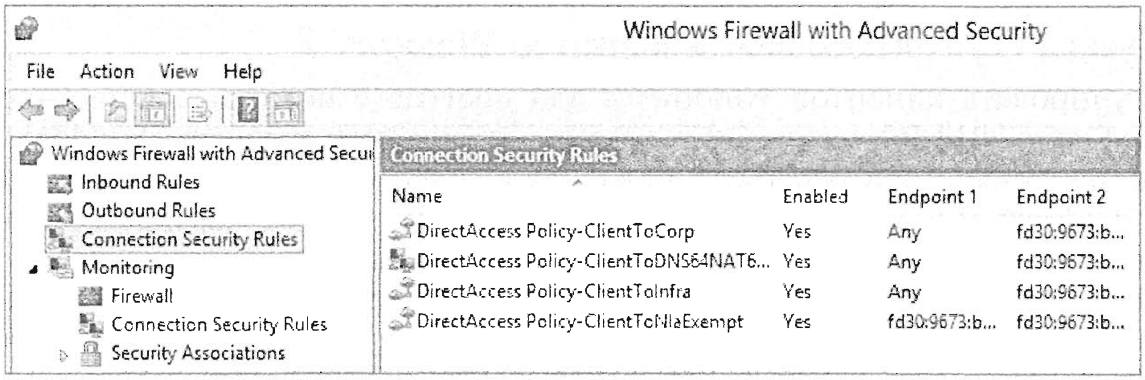


Рис. 21.37. Правила брандмауэра для DirectAccess

5. Если все требования удовлетворены, а объекты GPO на компьютере обновлены, щелкните на всплывающей панели в Windows 8, чтобы увидеть новое подключение DirectAccess, автоматически добавленное к обычному подключению Wi-Fi или подключению к локальной сети (рис. 21.38).

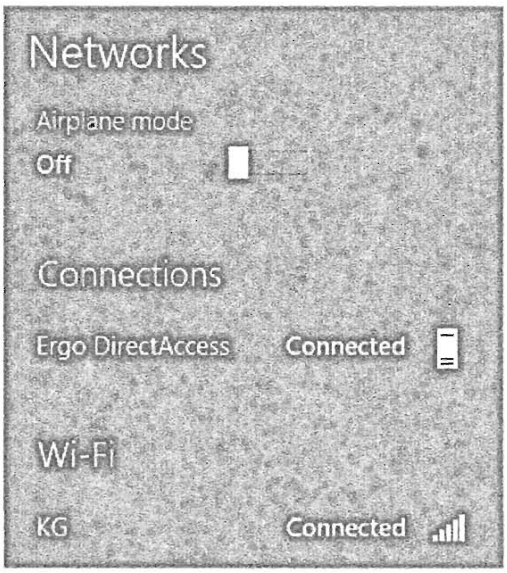


Рис. 21.38. Подключение DirectAccess в Windows 8

6. Если вы хотите просмотреть конфигурацию клиента DirectAccess в Windows 8, откройте окно Windows PowerShell и введите следующую команду:

```
Get-DAClientExperienceConfiguration
```

7. Чтобы подтвердить, что вы установили удаленное подключение с корпоративной средой посредством подключения DirectAccess, в окне PowerShell введите такую команду:

```
Get-DAConnectionStatus
```

Состояние `ConnectedRemotely` означает, что установлено подключение с помощью DirectAccess.

Вот и все, что необходимо сделать для активизации DirectAccess на клиенте, функционирующем под управлением Windows 8 Enterprise. Теперь вы должны иметь возможность просматривать ресурсы в удаленной сети, как если бы вы сидели в этом офисе и не заботились о накладных расходах, связанных с администрированием сторонних VPN-клиентов.

Обеспечение работоспособности клиентов Windows 7

Конфигурировать клиентов Windows 8 для доступа с помощью DirectAccess из Windows Server 2012 R2 всегда будет намного проще, чем клиентов Windows 7. Это объясняется наличием в Windows 8 новой возможности Kerberos Proxy, которая допускает двойную аутентификацию пользователя и клиентского компьютера посредством Kerberos. К сожалению, в Windows 7 такая возможность отсутствует и поэтому основным отличием настройки Windows 7 на работу с DirectAccess является необходимость получения сертификатов для рабочей станции от центра сертификации. Чтобы удовлетворить это требование, выполните следующие шаги.

1. Создайте новый центр сертификации либо воспользуйтесь существующим центром.
2. Создайте новый шаблон сертификата.
3. Включите автоматическое развертывание посредством групповой политики.
4. Отметьте флажок Enable Windows 7 client computers to connect via DirectAccess (Разрешить клиентским компьютерам Windows 7 подключаться через DirectAccess) при обработке области "Step 2, Remote Access Server" на диаграмме в консоли Remote Access Management Console.

Освоить этот процесс поможет статья в блоге по адресу `http://tinyurl.com/ws2012dawin7`.

Управление DirectAccess

Консоль Remote Access Management Console представляет собой центральный пользовательский интерфейс для DirectAccess. Получить доступ к ней можно из диспетчера серверов, выбрав в меню Tools (Сервис) пункт Remote Access Management (Управление удаленным доступом). Когда вы откроете эту консоль, то увидите пять разных навигационных представлений, которые можно исследовать. Ниже приведено краткое описание этих представлений.

- Configuration (Конфигурация). Это представление позволяет конфигурировать среду DirectAccess за четыре простых шага (см. раздел "Установка DirectAccess" ранее в этой главе). С помощью панели Tasks (Задачи), расположенной справа, можно также выполнять такие действия, как просмотр сводки по конфигурации, удаление параметров конфигурации, перезагрузка конфигураций, включение многосайтовой поддержки и балансировки нагрузки, а также запуск консолей управления RRAS и VPN.
- Dashboard (Управляющая панель). Представление Remote Access Dashboard (Управляющая панель удаленного доступа), показанная на рис. 21.39, предоставляет обзор состояний операций (Operations Status), конфигурации (Configuration Status) и удаленных клиентов (Remote Client Status).
- Operations Status (Состояние операций). Здесь вы можете просмотреть состояние работоспособности развертывания DirectAccess. При наличии проблем с подключением клиентов через DirectAccess именно сюда следует обращаться в первую очередь, чтобы проверить, не появились ли какие-то сообщения о предупреждениях или ошибках. По существу вас будет интересовать раздел подробностей, в котором должно отображаться сообщение Working Properly (Функционирует нормально).

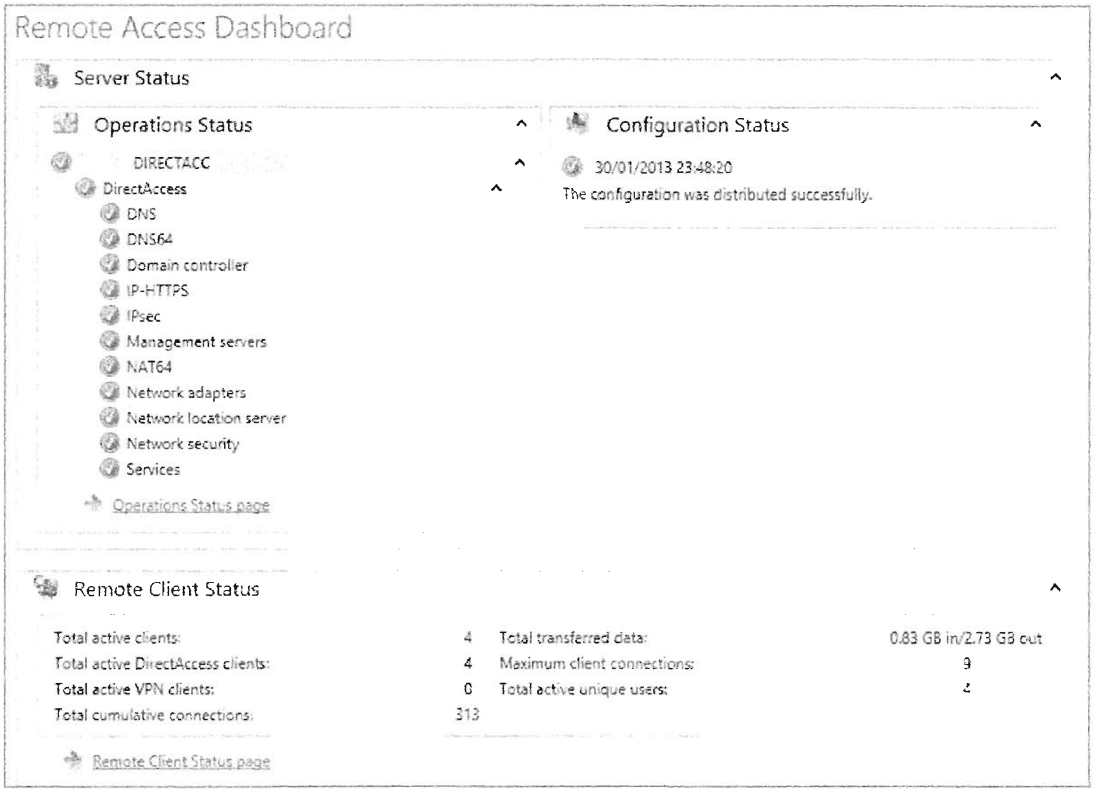


Рис. 21.39. Представление Remote Access Dashboard

Вы можете также запустить задачу View Performance Counters (Отобразить счетчики производительности) для компонентов IP-HTTPS, IPSec и Network Security, чтобы оценить метрики производительности на уровне пакетов.

- Remote Client Status (Состояние удаленных клиентов). Щелчок на этом представлении приводит к отображению списка подключенных клиентов DirectAccess, который содержит для каждого из них имя пользователя, имя хоста, протокол и продолжительность подключения. При желании можно щелкнуть правой кнопкой мыши на клиенте и выбрать в контекстном меню пункт Details (Подробности), чтобы ознакомиться с детальными статистическими данными.
- Reporting (Генерация отчетов). Раздел Remote Access Reporting (Генерация отчетов по удаленному доступу) консоли является особенно интересным и полезным, когда нужно сгенерировать отчеты по использованию DirectAccess. Все, что для этого необходимо — ввести начальную и конечную даты, а затем щелкнуть на ссылке Generate Report (Сгенерировать отчет). Вы можете также воспользоваться действием Configure Accounting (Конфигурировать учет) в панели Tasks (Задачи), чтобы сконфигурировать регистрацию данных учета Remote Access (рис. 21.40). Журналы учета могут храниться либо на удаленном сервере RADIUS, либо локально в базе данных Windows Internal Database.

Резюме

Добавьте роль Network Policy and Access Services. Первым шагом при создании VPN-сервера является добавление роли Network Policy and Access Services. После этого можно предпринимать дополнительные действия по конфигурированию VPN-сервера.

Контрольный вопрос. Чтобы создать VPN-сервер, вам необходимо добавить роль Network Policy and Access Services. Как вы решите эту задачу?

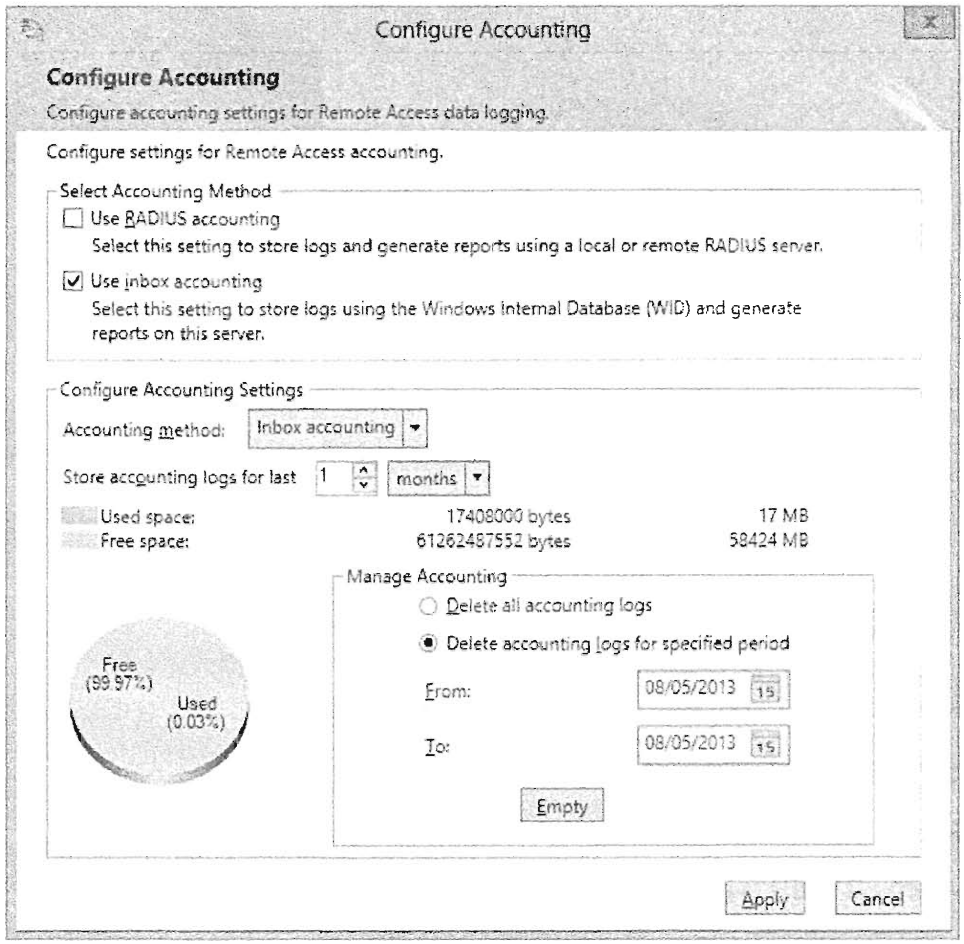


Рис. 21.40. Конфигурирование учета Remote Access

Освойте роль Remote Access. Роль Remote Access предусматривает гораздо больше, чем просто возможность создания традиционного VPN-сервера.

Контрольный вопрос. Назовите отдельные службы внутри этой роли (выберите три):

а. Remote Access Service

б. VPN Service

в. Routing

г. IPSec

д. DirectAccess

Сконфигурируйте VPN-сервер. Вы уже добавили роль Remote Access и теперь хотите сконфигурировать VPN-сервер, чтобы он мог принимать запросы на подключения от клиентов.

Контрольный вопрос. Что вы должны сделать для конфигурирования VPN-сервера?

Исследуйте DirectAccess. Технология DirectAccess позволяет удаленным пользователям безопасно подключаться к корпоративной среде без необходимости в использовании традиционного VPN-клиента.

Контрольный вопрос. Какие клиентские операционные системы поддерживаются для DirectAccess в Windows Server 2012 R2?

Глава 22

Добавление дополнительных размещений: сайты в Active Directory

Если все ваши контроллеры домена сосредоточены на одной физической площадке, можете пропустить эту главу. Однако если некоторые контроллеры домена находятся в других местах, то вы должны проинформировать Active Directory о каналах связи глобальной сети (wide area network — WAN), соединяющих между собой эти разные размещения. Для идентификации различных размещений в Active Directory используются сайты. Тем не менее, по умолчанию Active Directory известно только об одном сайте. Стандартный первый сайт называется `Default-First-Site-Name`. Если ваша организация располагается в одном месте, то все будет функционировать ожидаемым образом без возникновения проблем. Однако при наличии более одной площадки вам придется создать дополнительные сайты, подсети и связи сайтов. Сайты представляют размещения, объекты подсетей — действительные подсети, которые существуют в этих расположениях, а связи сайтов — каналы WAN, которые соединяют между собой разные площадки.

В этой главе рассказывается о создании сайтов и подсетей, конфигурировании межсайтовой репликации с помощью связей сайтов, оптимизации межсайтовой репликации за счет изменения свойств связей сайтов и конфигурировании ближайшего соседнего сайта для клиентов. В этой главе вы изучите следующие темы:

- создание сайтов;
- добавление подсетей к сайтам;
- конфигурирование связи сайта для репликации только в определенные моменты времени;
- конфигурирование групповой политики для ближайшего соседнего сайта.

Освоение концепций сайта

Многие организации размещены на нескольких физических площадках. Производственная, сбытовая и другие виды деятельности компании часто рассредоточены по городу, стране или даже по всему миру. Таким организациям приходится принимать дополнительные меры, чтобы повседневное функционирование Active Directory было оптимальным.

Взгляните на рис. 22.1. Здесь представлена организация под названием Bigfirm.com, которая имеет три физических площадки: штаб-квартиру, офис на другом конце города и удаленный офис.

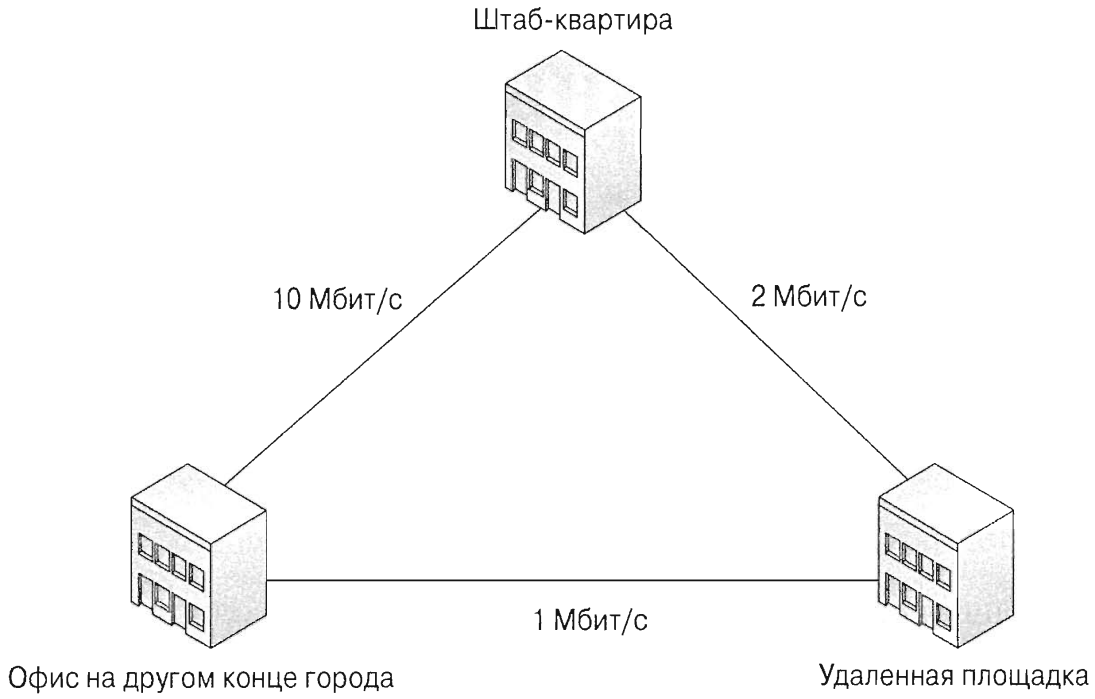


Рис. 22.1. Компания с несколькими площадками

Каждая физическая площадка обладает высокоскоростной подключаемостью. Другими словами, все маршрутизаторы, коммутаторы, сетевые карты и кабельные системы в штаб-квартире способны передавать данные со скоростью 1 Гбит/с, а все компоненты на двух других площадках поддерживают скорость передачи 100 Мбит/с. По существу это и есть базовое определение *сайта* как группы хостов или подсетей, соединенных между собой посредством высокоскоростных каналов связи.

Подключение между сайтами нельзя назвать таким же высокоскоростным, как внутри сайтов. На рис. 22.1 видно, что штаб-квартира компании соединяется с офисом на другом конце города с помощью канала WAN со скоростью 10 Мбит/с. Удаленный офис соединен со штаб-квартирой посредством еще более медленного канала связи 2 Мбит/с, а офис на другом конце города и удаленный офис располагают резервным соединением со скоростью 1 Мбит/с.

Предположим, что на каждой физической площадке присутствует, по меньшей мере, один контроллер домена. В такой ситуации возникают следующие вопросы.

- Когда пользователи входят в системы компьютеров удаленного офиса, то какой контроллер домена (domain controller — DC) должен аутентифицировать их?
- Если DC в удаленном офисе реплицирует данные Active Directory из DC в штаб-квартире, то какой путь он должен выбрать?

- Если снизится быстродействие канала связи 10 Мбит/с, то каким образом DC в штаб-квартире должен выполнять репликацию на DC в офисе на другом конце города?

Ответы на эти вопросы становятся очевидными, если обратиться к приведенному выше рис. 22.1.

- Пользователи удаленного офиса должны входить на DC в удаленном офисе.
- Репликация между штаб-квартирой и удаленным офисом должна осуществляться с использованием канала связи 2 Мбит/с.
- Если канал связи 10 Мбит/с становится перегруженным, то путь репликации от штаб-квартиры до офиса на другом конце города должен проходить через соединение 2 Мбит/с, а затем через соединение 1 Мбит/с.

Однако данные ответы совсем не очевидны для Active Directory. Вы должны обучить этому Active Directory, сконфигурировав объекты в оснастке Active Directory Sites and Services (Сайты и службы Active Directory).

Вспомните, что Active Directory — это огромная база данных объектов, представляющих пользователей, компьютеры и группы, которые относятся к сущностям реального мира. Когда вы создаете в Active Directory объект пользователя, то тем самым вы не создаете какое-то физическое лицо; вместо этого вы создаете объект, представляющий пользователя.

Аналогично, когда вы создаете в оснастке Active Directory Sites and Services сайт, то в действительности не создаете физическую площадку, а только объект, который ссылается на физическую площадку или физический сайт.

Сайты и репликация

В качестве напоминания, репликация Active Directory представляет собой процесс копирования всех добавлений, удалений и модификаций, произведенных в Active Directory. Когда добавляется учетная запись пользователя или пользователь изменяет свой пароль, это изменение должно реплицироваться по всей среде Active Directory.

Внутри сайта такая репликация происходит очень быстро и применяет процесс уведомлений. Рассмотрим для примера сайт с четырьмя контроллерами домена, имеющими имена `BF1`, `BF2`, `BF3` и `BF4` (рис. 22.2).

Если учетная запись пользователя добавляется на `BF1`, то `BF1` уведомит об этом изменении `BF2` и `BF3`. Контроллеры домена `BF2` и `BF3` не располагают этим изменением, поэтому они его запрашивают и в результате

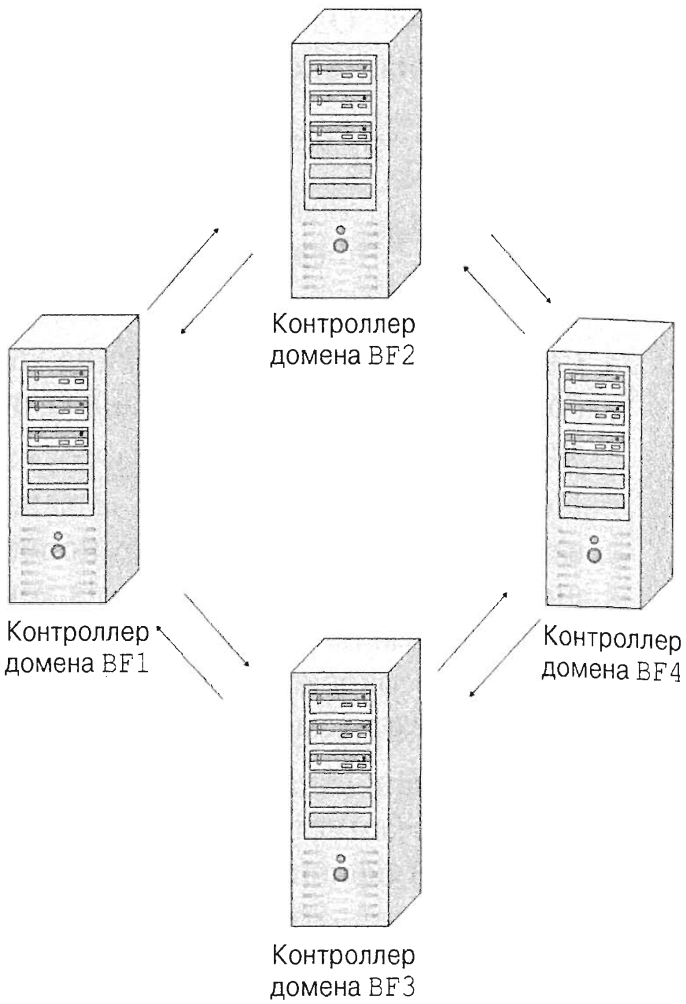


Рис. 22.2. Топология внутрисайтовой репликации

данные на всех трех контроллерах домена становятся актуальными. И BF2, и BF3 отправят уведомление об изменении контроллеру домена BF4, который запросит это изменение у первого DC, приславшего уведомление, но не у обоих контроллеров домена.

Представим, что первым было получено уведомление от BF2. Контроллер домена BF4 запросит изменение у BF2, а когда он получит уведомление от BF3, то обнаружит, что уже имеет такое изменение, поэтому проигнорирует уведомление от BF3. Такой процесс уведомления называется *погашением распространения*, и он предотвращает бесконечную репликацию изменения. Контроллеров домена вполне устраивает взаимодействие с другими контроллерами домена, но если DC внутри том же сайта отдален на более чем три прыжка, то средство проверки целостности знаний (Knowledge Consistency Checker — KCC) создаст прямую ссылку на этот DC. Средство KCC отвечает за создание и управление топологией репликации между сайтами. Оно проверяет Active Directory каждые 15 минут, чтобы создавать и удалять объекты подключения по всему лесу.

Репликация *между* сайтами оптимизирована за счет отказа от этого механизма уведомлений и сжатия реплицируемых данных.

- **Отсутствие уведомлений между сайтами.** Репликация между сайтами выполняется на основе расписания. Все реплицируемые данные, которые были собраны с момента последней репликации, передаются без использования процесса уведомления.
- **Сжатие реплицируемых данных между сайтами.** Реплицируемые данные предварительно сжимаются. Сайту с высокоскоростными подключениями сжатие не требуется. Однако поскольку каналы связи WAN имеют меньшую полосу пропускания, такое сжатие исключительно полезно.

Терминология, касающаяся сайтов

Прежде чем углубиться в детали, вы должны ознакомиться с рядом терминов и концепций. Ниже представлены некоторые ключевые концепции, имеющие отношение к сайтам.

- **Сайты.** Сайт (site) — это группа хостов или подсетей, соединенных между собой высокоскоростными каналами связи, которые размещены вместе на физической площадке.

  Понятие "высокоскоростные каналы связи" является относительным. Один сайт может включать все компоненты сетевой инфраструктуры, обеспечивающие скорость 10 Мбит/с, тогда как другой сайт может располагать скоростью 1 Гбит/с. Тем не менее, внутри каждого сайта все компоненты функционируют на базе высокоскоростной локальной сети, поэтому группа может называться сайтом даже несмотря на указанные различия в фактических скоростях.
- **Физические площадки.** Физической площадкой (physical location) называется местоположение локальной сети. Физической площадкой может быть один удаленный офис с 25 пользователями или целое здание, в котором работают тысячи пользователей. Если физическая площадка включает контроллер домена, то в Active Directory должен быть сконфигурирован объект сайта, представляющий эту физическую площадку.

Отключение сжатия

Иногда возникают ситуации, когда между сайтами имеется полоса пропускания, превышающая ту, которую можно обработать доступными вычислительными мощностями контроллеров домена, выполняющих межсайтовую репликацию. В таком случае вы можете рассмотреть вариант с отключением сжатия, чтобы контроллерам домена не приходилось тратить время на упаковку и распаковку реплицируемых данных.

В качестве альтернативы можно было бы добавить еще один DC, который принял бы на себя часть нагрузки, связанной с обработкой данных. Или же, если окажется, что интересующий DC является виртуальной машиной, то в целях повышения производительности можно было бы нарастить сокеты и процессорные ядра (конечно, при наличии доступных ресурсов). Если такие возможности отсутствуют, то отключение сжатия является единственным способом, который позволит снизить вычислительную нагрузку на DC.

Это сложная процедура, которая предусматривает изменение параметров Active Directory с помощью ADSI Edit. Ее следует выполнять, только при наличии надежной резервной копии среды Active Directory. Если вы тщательно взвесили все имеющиеся в вашем распоряжении варианты, то можете отключить сжатие, выполнив перечисленные далее шаги.

1. Запустите ADSI Edit из меню Administrative Tools (Администрирование).
2. Щелкните правой кнопкой мыши на ADSI Edit и выберите в контекстном меню пункт Connect to (Подключиться к).
3. Измените стандартный контекст именования на Configuration (Конфигурация).
4. Перейдите к контейнеру `CN=Sites,CN=Intersite Site Transport,CN=IP`.
5. Дважды щелкните на связи сайта, которую вы хотите модифицировать, чтобы получить доступ к ее свойствам.
6. Дважды щелкните на свойстве `options` (параметры).
7. Если это свойство имеет значение `<not set>` (не установлено), измените его на `4` и щелкните на кнопке OK. Вы увидите, что значением теперь стало `0x4 = (DISABLE_COMPRESSION)`.

   Если свойство `options` имело какое-то значение, к нему понадобится добавить 4. Например, если это свойство было установлено в 2, добавьте к нему 4, получив в итоге 6. Затем введите `6`.

- **Подсети.** Каждая локальная сеть будет включать одну или несколько подсетей (subnet). Эти подсети уже существуют на каждой физической площадке. Объекты сайтов добавляются в Active Directory для того, чтобы они представляли физические площадки, а объекты подсетей добавляются к объектам сайтов для представления действительных подсетей на этих площадках.
- **Связи сайтов.** Сайты соединяются с другими сайтами посредством более медленных WAN-подключений. Например, один сайт может соединяться с другим сайтом посредством быстрого WAN-канала T1. Два других сайта могут подключаться с применением более медленных (128 Кбит/с) каналов WAN. Объекты связей сайтов (site link) используются для информирования Active Directory об этих WAN-каналах, а свойства связей сайтов конфигурируются для предоставления подробных сведений о каналах, например, какую связь сайта задействовать и когда.

- **Мосты связей сайтов.** Мосты связей сайтов (site link bridge) создаются в Active Directory автоматически, разрешая репликацию между всеми сайтами. Даже если у какого-то сайта нет прямого пути к другому сайту, Active Directory связывает эти сайты *мостами*, предоставляя возможность подключения через одну или несколько связей другого сайта. Создание мостов на основе связей сайтов можно заблокировать, чтобы исключить применение определенных связей сайтов.

  Генератор межсайтовой топологии. Генератор межсайтовой топологии (Intersite Topology Generator — ISTG) решает задачи расширенного управления репликацией, назначая внутри сайта сервер-плацдарм и отслеживая его работоспособность. Если такой сервер-плацдарм перестает функционировать, ISTG назначает в качестве сервера-плацдарма другой контроллер домена.

- **Серверы-плацдармы.** Сервер-плацдарм (bridgehead server) — это специальный контроллер домена внутри сайта, который реплицирует данные Active Directory на контроллеры домена других сайтов. Каждый сайт имеет один сервер-плацдарм, назначенный ISTG. Назначение, выполненное ISTG, можно переопределить, указав предпочтительные серверы-плацдармы.

- **Предпочтительные серверы-плацдармы.** Предпочтительные серверы-плацдармы (preferred bridgehead server) можно указать вручную, чтобы предотвратить возможность назначения на роль сервера-плацдарма контроллеров домена, не располагающих необходимыми для этого ресурсами. После того как будет сконфигурирован один предпочтительный сервер-плацдарм, любые контроллеры домена, которые не сконфигурированы как предпочтительные серверы-плацдармы, не будут выбираться на эту роль.

Исследование сайтов

Построив инфраструктуру TCP/IP, вы должны проинформировать о ней Active Directory. После того как среда Active Directory будет располагать ключевой информацией о созданной инфраструктуре, она сможет принимать обоснованные решения относительно использования имеющейся полосы пропускания.

При выполнении репликации из одного DC на другой DC каждый из них должен знать, взаимодействует он через быстрый канал внутри сайта с высокоскоростными подключениями или же связывается с другим DC по каналу 256 Кбит/с, поэтому нуждается в дополнительном времени на предварительное сжатие данных. Данные межсайтовой репликации сжимаются по умолчанию.

Но контроллер домена не может знать вид канала передачи данных, если только вы не подскажете ему. Контроллеру домена известно, что он может связываться с другим DC на высокой скорости, если они оба находятся внутри одного и того же *сайта*. Однако контроллеры домена не знают, что они находятся внутри того же самого сайта, если вы не сообщите им об этом.

Как работают сайты

Возникает вполне очевидный вопрос: каким образом сообщить Active Directory о том, что контроллеры домена находятся на разных сайтах? Ответ: воспользоваться оснасткой Active Directory Sites and Services.

Контроллеры домена расположены в контейнере Servers (Серверы) одного из контейнеров Sites (Сайты) из Active Directory. Для каждого сайта предусмотрен отдельный контейнер. Вспомните, что сайт определяется как одна или больше подсетей, которые взаимодействуют друг с другом на относительно высоких скоростях передачи данных. Вы определяете сайты, а затем помещаете в них контроллеры домена.

Рабочие станции и серверы не добавляются в оснастке Active Directory Sites and Services. Тем не менее, в начале сеанса работы они все же используют имеющуюся здесь информацию для идентификации ближайших к ним контроллеров домена. Процесс под названием DC Locator Service (Служба локатора контроллеров домена) определяет, внутри какого сайта находится рабочая станция, базируясь на подсети хоста. Затем он определяет контроллер домена в том же сайте.

Но вас может интересовать, как среде Active Directory удалось выяснить, какие у нее есть сайты и подсети, а также то, какие подсети входят в тот или иной сайт? Здесь не обойтись без определенного администраторского труда, так что давайте посмотрим, как это делается посредством оснастки Active Directory Sites and Services.

Оснастку Active Directory Sites and Services можно открыть, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Sites and Services (Сервис⇨Сайты и службы Active Directory). Окно оснастки показано на рис. 22.3.

Обратите внимание, что имеется только один сайт с весьма "креативным" названием: `Default-First-Site-Name` (т.е. "имя первого стандартного сайта"). В настоящем примере присутствуют четыре контроллера домена (с именами `BF1`, `BF2`, `BF3` и `BF4`), и все они расположены внутри этого стандартного сайта.

Когда вы создаете лес Active Directory, среда AD создает этот стандартный сайт и предполагает, что в нем будет находиться все. При наличии единственного сайта вы можете открыть `Default-First-Site-Name` и увидеть, что внутри него присутствуют все ваши контроллеры домена.

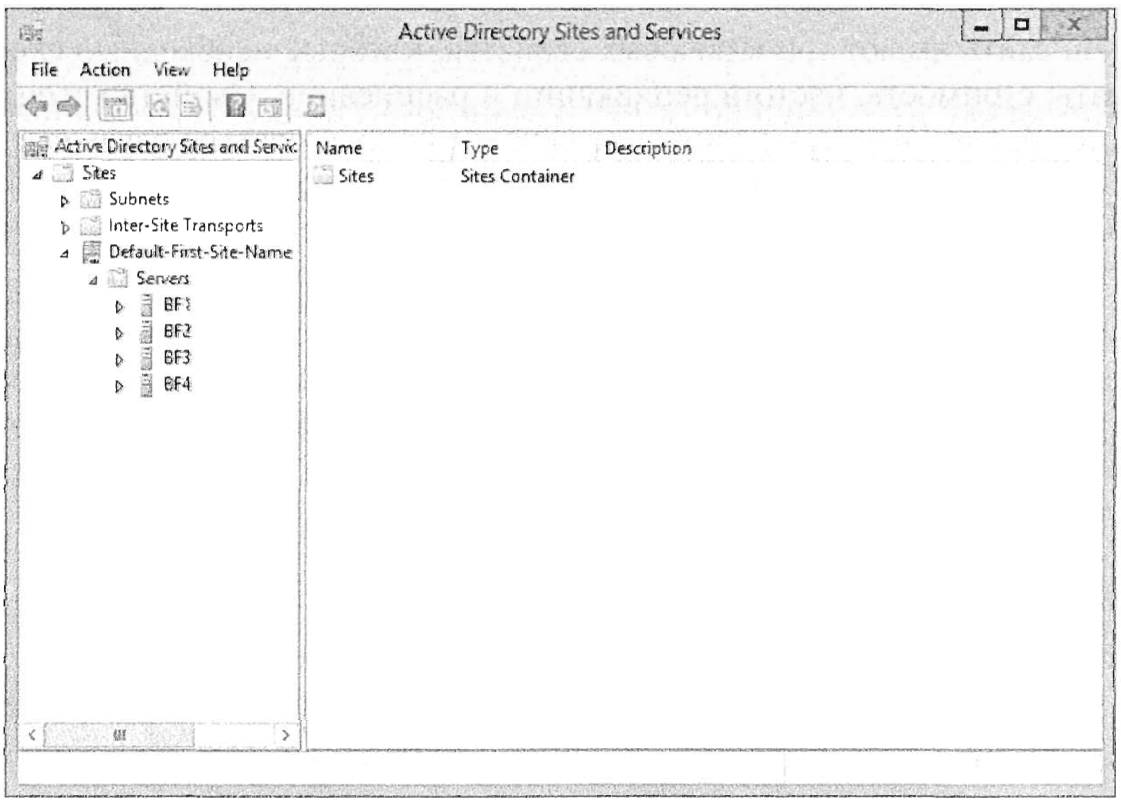


Рис. 22.3. Оснастка Active Directory Sites and Services

Автоматическое добавление серверов на подходящий сайт

Одним из действий, повышающих сервер до контроллера домена, является помещение объекта сервера внутрь сайта. По умолчанию он будет помещен в сайт `Default-First-Site-Name`. Тем не менее, если существует другой сайт с определенными подсетями, и повышаемый сервер имеет IP-адрес в какой-либо из определенных подсетей, то объект сервера будет помещен внутрь подходящего сайта.

Ниже описаны шаги и требования к настройке топологии сайтов Active Directory.

1. Определите каждый сайт.

   Под *сайтом* подразумевается площадка с высокоскоростной подключаемостью. Термины *сайт* и *площадка* часто применяются взаимозаменяемо. В рамках Active Directory сайт — это объект Active Directory, который относится к площадке с высокоскоростной подключаемостью.

2. Определите каждую подсеть.

   Для каждой подсети, которая создана в физической среде, в Active Directory необходимо создать соответствующий объект подсети.

3. Назначьте каждую подсеть сайту.

   Каждая подсеть связывается с фактической площадкой путем связывания объекта подсети с объектом сайта.

4. Создайте связи сайтов, чтобы соединить сайты.

   Физические площадки соединяются с помощью каналов WAN. Эти каналы WAN представлены объектами связей сайтов. Каждый такой объект включает два или большее число сайтов.

5. Сконфигурируйте свойства связей сайтов.

   Связи сайта имеют три ключевых свойства, которые необходимо сконфигурировать: стоимость, частота репликации и расписание. Свойство стоимости помогает Active Directory решить, должна ли использоваться связь сайта, с применением алгоритма определения наименьшей стоимости. Свойство частоты репликации указывает, насколько часто выполняется репликация. Свойство расписания отражает, когда следует инициировать репликацию.

Если вы определяете топологию после создания контроллеров домена, вам понадобится переместить контроллеры домена в подходящий сайт. Однако если топология определяется в оснастке Active Directory Sites and Services перед повышением серверов до контроллеров домена, то контроллеры домена будут автоматически добавлены к соответствующему сайту.

Переименование сайта `Default-First-Site-Name`

Вы можете переименовать свой первый сайт, избавившись от невыразительного `Default-First-Site-Name` и назначив ему более простое имя наподобие `HQ`.

1. Откройте оснастку Active Directory Sites and Services.
2. Откройте папку Sites (Сайты), чтобы отобразить папку Default-First-Site-Name.

3. Щелкните правой кнопкой мыши на папке Default-First-Site-Name и выберите в контекстном меню пункт Rename (Переименовать).
4. Имя `Default-First-Site-Name` будет выделено. Введите вместо него имя `HQ` и щелкните в каком-то другом месте экрана.

Это лучше всего сделать на раннем этапе процесса создания Active Directory. На самом деле сайт `Default-First-Site-Name` лучше всего переименовать при создании первого DC.

Определение сайта

Предположим, что вы создаете еще один сайт, расположенный на другом конце города. Вы должны проинформировать Active Directory об этом сайте. Щелкните правой кнопкой мыши на папке Sites (Сайты) и выберите в контекстном меню пункт New Site (Создать сайт); откроется окно, подобное показанному на рис. 22.4.

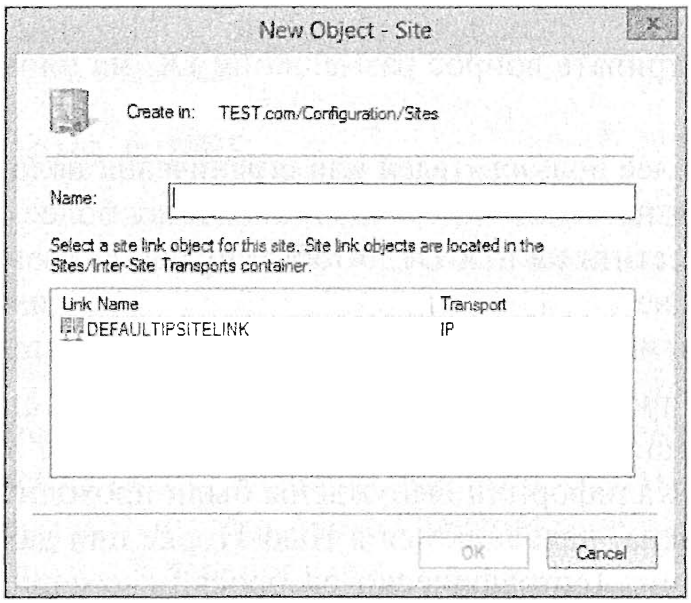


Рис. 22.4. Создание нового сайта

В поле Name (Имя) укажите имя нового сайта (например, **`Crosstown`**), щелкните на объекте `DEFAULTIPSITELINK` и затем на кнопке OK. После этого появится окно, представленное на рис. 22.5.

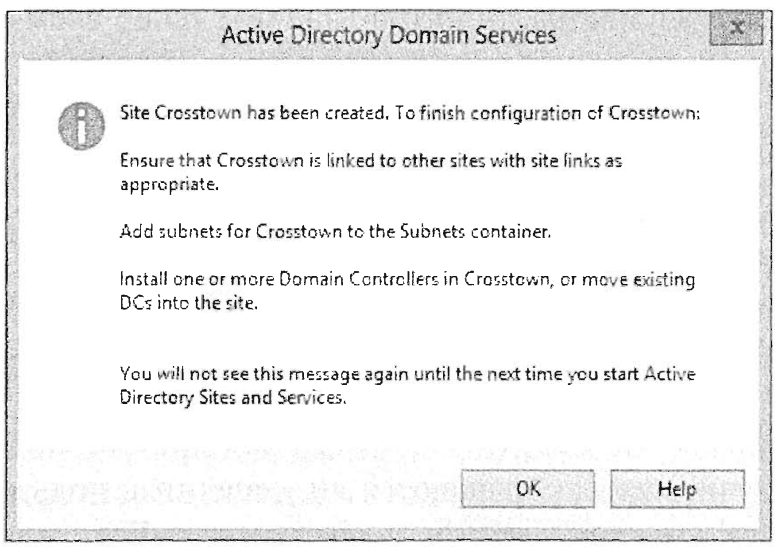


Рис. 22.5. Инструкции по завершению настройки нового сайта

Вы не обязаны создавать сайт для каждой площадки. Фактически единственная причина, по которой будет создаваться новый сайт, связана с намерением добавить на площадку контроллер домена. Если наличие контроллера домена на площадке не планируется, то создавать сайт не нужно.

Принятие решения относительно контроллеров домена на удаленных площадках

Если вы должны создавать сайт, только когда площадка будет содержать DC, то следует представлять себе, в каких случаях добавлять DC на площадку. Хороший вопрос!

Наличие отдельной площадки вовсе не означает, что ей понадобится контроллер домена. Например, если на площадке работают всего пять пользователей, подключенных через канал WAN, то вряд ли вы захотите идти на дополнительные расходы по установке контроллера домена. Эти пользователи могут открывать сеансы посредством канала WAN.

Вы должны рассматривать вопрос размещения DC на площадке в одной из следующих ситуаций.

- **Наличие 100 и более пользователей или ограничения полосы пропускания.** В общем случае, если на какой-то площадке имеется более 100 пользователей, то вы должны разместить на ней DC, чтобы управлять всеми запросами аутентификации. Допускается размещать DC в сайте с меньшим количеством пользователей, но когда их больше 100, то наличие DC обязательно.

  Недостаточно широкая полоса пропускания является еще одной веской причиной для размещения DC на удаленном сайте. Вряд ли вы захотите, чтобы пользователи из Калифорнии вынуждены были проходить аутентификацию на контроллере домена, находящемся в Нью-Йорке или даже где-нибудь дальше, скажем, в Лондоне. Географически разбросанные офисы компании должны предоставлять своим пользователям возможность локальной аутентификации. Высокоскоростные линии связи, пересекающие всю страну и, тем более, разные континенты, могут оказаться весьма дорогостоящими.

- **Неприемлемо медленный канал WAN.** Если вход в систему пользователями отнимает значительное время, то наличие DC внутри сайта значительно сократит время входа. Разумеется, понятие "значительное время" является относительным. В одной среде неприемлемым может считаться период в 10 минут, тогда как в другой среде даже 2 минуты могут расцениваться как неприемлемое время входа.

- **Канал WAN является ненадежным для входа, когда это необходимо.** Если пользователи не могут надежно войти в систему, когда в этом возникает необходимость, рассмотрите возможность размещения DC на площадке. Например, если пользователям требуется входить в промежутке с 9 до 18:00, с понедельника по пятницу, но в эти часы канал WAN загружен на 100%, то пользователи не смогут пройти аутентификацию в домене.

  Следует также учитывать, обращаются ли удаленные пользователи к таким ресурсам на удаленном сайте, как файловый сервер. Если пользователи не могут аутентифицироваться посредством DC, то они не смогут получить доступ к

ресурсам, которые требуют их учетных данных Active Directory. В разделе "Кешированные учетные данные" далее в этой главе приведено более подробное объяснение такого сценария.

- **Интенсивный трафик LDAP.** Если пользователи или приложения часто запрашивают Active Directory, то наличие DC в рамках сайта предотвратит использование этими запросами каналов WAN. Для запрашивания и/или модификации данных в Active Directory применяется протокол LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам), а приложения часто инициируют запросы к глобальному каталогу. Интенсивный трафик LDAP нередко требует превращения контроллера домена в сервер глобального каталога (global catalog — GC).

ОС Windows Server 2012 R2 продолжает предлагать возможность развертывания контроллера домена только для чтения (read-only domain controller — RODC) на площадках с небольшим числом пользователей. Контроллеры RODC хранят меньший объем данных и могут применяться на удаленных площадках. Более подробно RODC рассматриваются в главе 23.

Контроллер домена и DNS

Если вы помещаете DC внутрь какого-то сайта, то должны всерьез обдумать вопрос о том, чтобы сделать его DNS-сервером. Если это единственный DC, тогда у вас обязательно должен быть DNS-сервер. Когда пользователь входит в систему, служба `netlogon` запрашивает у службы DNS местоположение контроллера домена на сайте пользователя. Если DNS-сервер на сайте отсутствует, то для обращения к службе DNS придется применять канал WAN. Обычно используется служба DNS, интегрированная в Active Directory (Active Directory integrated — ADI). ADI DNS обновляется посредством обычной репликации Active Directory и не требует большого объема администрирования для зон и переноса зон.

Кешированные учетные данные

Возможно, вы помните, что если пользователь входил в какую-то систему ранее, то он может войти в ту же систему с теми же самыми учетными данными домена, даже если контроллер домена не доступен. При этом используются кешированные учетные данные.

Рассмотрим пользователя с мобильным компьютером. Он подключает свой ноутбук к базовой станции у себя на работе и входит в домен. Позже, ожидая самолет в аэропорту, он желает воспользоваться тем же ноутбуком для работы над отчетом. Для входа в систему пользователь может применить ту же самую учетную запись. Однако контроллер домена его компании в аэропорту не доступен. Вместо этого вход в систему происходит с участием учетных данных, которые были кешированы на ноутбуке.

С точки зрения пользователя процесс входа ничем не отличается: пользователь вводит то же самое имя и пароль, после чего на экране появляется рабочий стол.

Это работает таким же образом для пользователей на удаленных площадках, не располагающих контроллером домена и надежными каналами WAN. Если пользователь входил в систему своего компьютера на удаленной площадке через WAN-канал ранее, то он может войти снова с применением тех же учетных данных.

Когда пользователь открыл сеанс с помощью кешированных учетных данных, система периодически пробует обратиться к контроллеру домена. Как только канал WAN становится доступным, система открывает сеанс и пользователь сможет обращаться к ресурсам обычным способом.

Кешированные учетные данные и GC

Кешированные учетные данные работают несколько по-другому, если какой-то контроллер домена доступен, но не доступен контроллер домена, размещающий глобальный каталог. Глобальный каталог является единственным местом, где хранится информация о членстве в универсальных группах, а для успешного входа членство в универсальных группах должно быть идентифицировано.

Когда пользователь открывает сеанс, формируется маркер, который включает идентификаторы SID всех групп, членом которых он является, а также SID самого пользователя. Однако если GC отсутствует, членство в универсальных группах идентифицировать невозможно.

Причина в том, что членам какой-то универсальной группы может быть явно запрещен доступ. Тем не менее, если членство в универсальных группах идентифицировать не удалось, но вход в систему был разрешен, то вполне возможно, что члены этой универсальной группы получат доступ к ресурсам, к которым он должен быть запрещен.

Взгляните на рис. 22.6. Пользователь входит в систему в удаленном офисе. Канал WAN в данный момент не доступен, но пользователь может получить доступ к контроллеру домена `BF2` в этом удаленном офисе. Обратите внимание, что контроллер домена `BF1` является сервером глобального каталога, но BF2 — нет.

Служба `netlogon` способная проверить достоверность учетных данных пользователя на `BF2`, но поскольку глобальный каталог не может быть достигнут, и членство в универсальных группах идентифицировать не получилось, то вход пользователю запрещается. Он не сможет войти даже с помощью кешированных учетных данных.

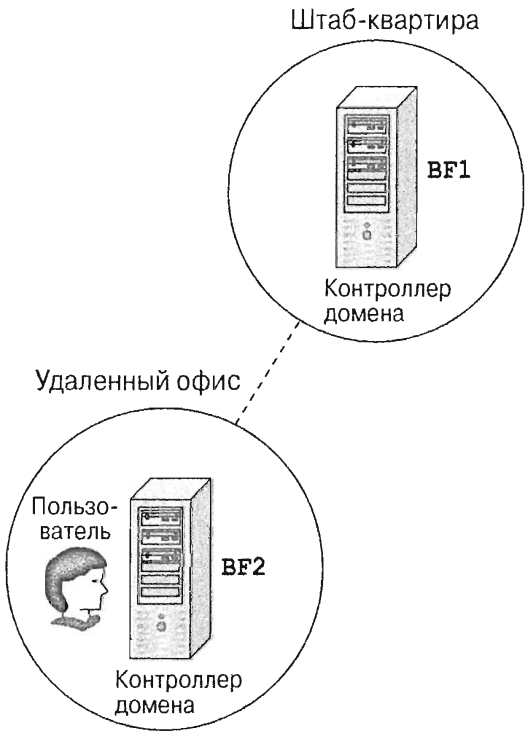


Рис. 22.6. Открытие сеанса без доступа к GC

Во избежание такой проблемы вы должны либо сделать DC на удаленном сайте сервером глобального каталога, либо включить кеширование членства в универсальных группах.

Сервер глобального каталога или кеширование членства в универсальных группах

Решив развернуть контроллер домена внутри сайта, вам также нужно принять решение, хотите ли вы сделать этот DC сервером глобального каталога. На сервере глобального каталога будет размещаться глобальный каталог.

Если вы не сделаете DC сервером глобального каталога, то должны включить на данном сайте кеширование членства в универсальных группах. Когда это сделано, контроллер домена будет кешировать данные членства в универсальных группах пользователя, когда он в пер-

вый раз откроет сеанс, и использовать эти данные для создания маркера пользователя при последующих входах в систему.

Данные членства в универсальных группах для любых пользователей, которые входили в систему контроллера домена, обновляются каждые восемь часов. Контроллер домена может хранить кешированные данные членства в универсальных группах для максимум 500 пользователей.

Главной причиной, по которой вы можете отказаться от варианта сделать DC сервером глобального каталога на удаленном сайте, связана с тем, что репликация глобального каталога будет потреблять слишком большую долю полосы пропускания. Скажем, если использование полосы пропускания уже составляет 80%, то превращение DC в сервер глобального каталога может привести к скачку утилизации полосы пропускания до 100%.

Чтобы сделать любой DC сервером глобального каталога, понадобится модифицировать параметры в диалоговом окне NTDS Settings Properties (Свойства настроек NTDS) для сервера. Это окно с отмеченным флажком Global Catalog (Глобальный каталог) показано на рис. 22.7.

Для открытия диалогового окна NTDS Settings Properties сервера найдите в оснастке Active Directory Sites and Services объект сервера внутри нужного сайта. Щелкните правой кнопкой мыши на элементе NTDS Settings (Настройки NTDS) и выберите в контекстном меню пункт Properties (Свойства).

Включить кеширование членства в универсальных группах на сайте можно, внеся изменения в диалоговом окне свойств NTDS Site Settings Properties (Свойства настроек сайта NTDS). Это окно с отмеченным флажком Enable Universal Group Membership Caching (Включить кеширование членства в универсальных группах) представлено на рис. 22.8.

Рис. 22.7. Превращение контроллера домена в сервер глобального каталога

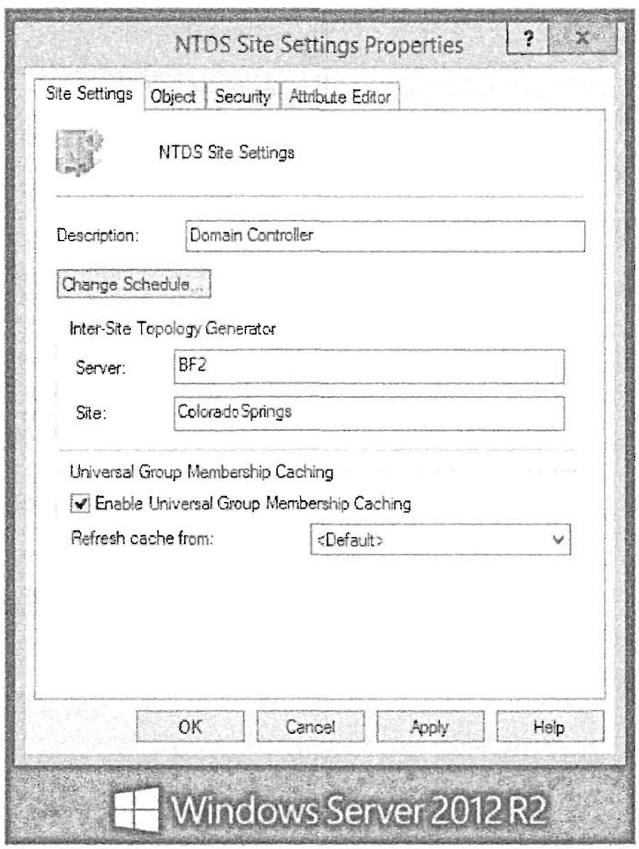


Рис. 22.8. Включение кеширования членства в универсальных группах

Чтобы открыть окно NTDS Site Settings Properties для сайта, найдите в оснастке Active Directory Sites and Services объект сайта внутри контейнера Sites (Сайты). Щелкните правой кнопкой мыши на элементе NTDS Settings для требуемого сайта и выберите в контекстном меню пункт Properties (Свойства).

Определение подсети и размещение ее в сайте

Далее вам необходимо описать подсети в производственной среде. Предположим, что сайт `HQ` содержит единственную подсеть 192.168.20.0/24, а сайт `Crosstown` — подсеть 192.168.1.0/24. Вы должны сообщить Active Directory об этих подсетях: всегда помните о том, что подсети должны назначаться сайтам, поэтому сначала создавайте сайты, а затем подсети.

1. Щелкните правой кнопкой мыши на папке Subnets (Подсети) и выберите в контекстном меню пункт New Subnet (Создать подсеть).
2. Введите `192.168.20.0/24`, чтобы идентифицировать эту подсеть.
3. Выберите сайт `HQ`, чтобы ассоциировать с ним эту подсеть.

   Окно будет выглядеть примерно так, как показано на рис. 22.9.
4. Добавьте подсеть 192.168.1.0/24 и ассоциируйте ее с сайтом `Crosstown`.

   Окно оснастки Active Directory Sites and Services будет похоже на показанное на рис. 22.10.

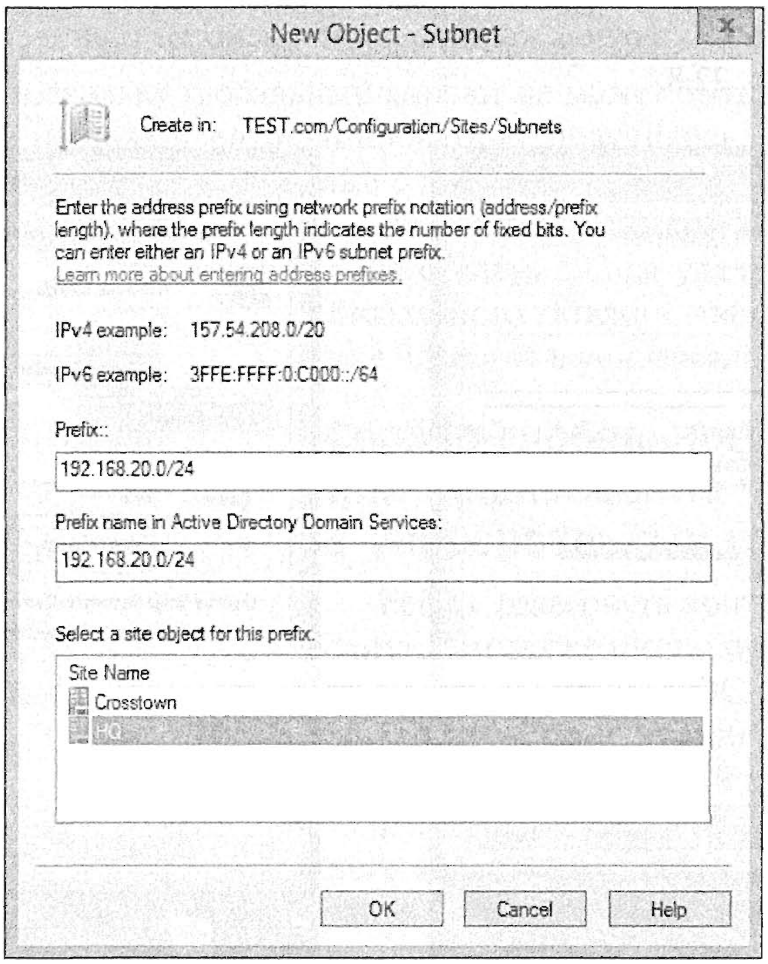


Рис. 22.9. Создание новой подсети

IPv4 или IPv6

В оснастке Active Directory Sites and Services можно добавлять подсети как IPv4, так и IPv6, но только по одной за раз. При добавлении подсетей вы должны идентифицировать маску подсети, используя форму записи CIDR (Classless Inter-Domain Routing — междоменная маршрутизация без учета классов). В формате CIDR указывается количество битов, равных 1, в маске подсети. Запись /24 означает, что первые 24 бита в маске подсети установлены в 1; другими словами, маска подсети выглядит как 255.255.255.0.

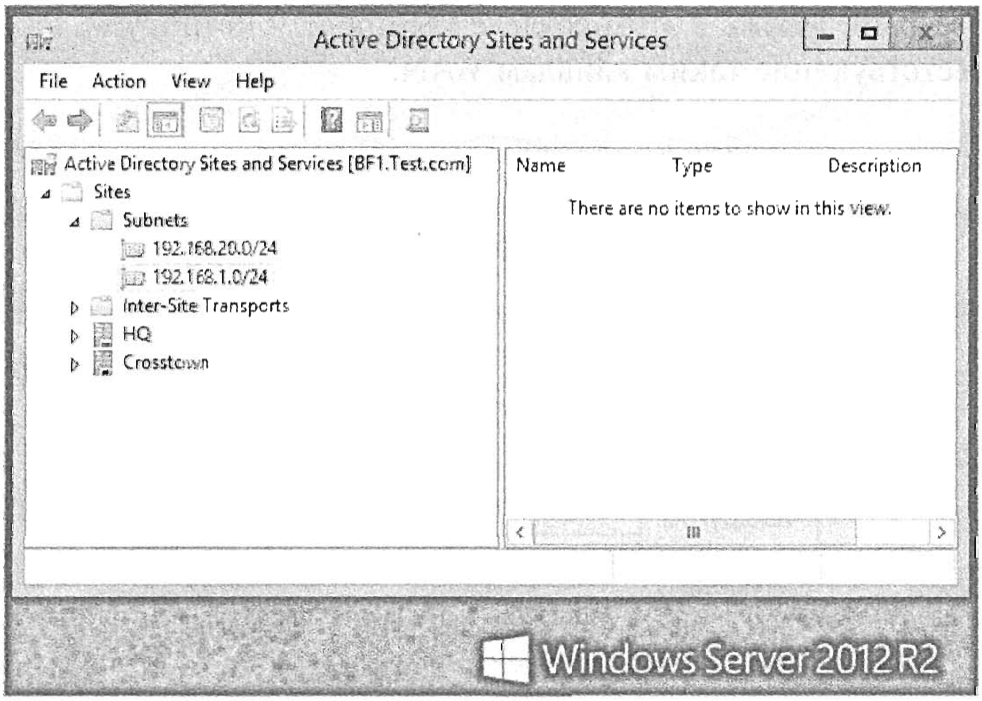


Рис. 22.10. Окно оснастки Active Directory Sites and Services после добавления подсетей

Помещение сервера внутрь сайта

К этому моменту все четыре контроллера домена производственной среды находятся внутри сайта `HQ`. Предположим, что `BF3` принадлежит сайту `Crosstown`. Чтобы сообщить Active Directory о том, что `BF3` физически находится на сайте `Crosstown`, можно переместить его туда. Перейдите к папке Sites⇨HQ⇨Servers (Сайты⇨HQ⇨Серверы), щелкните правой кнопкой мыши на `BF3` и выберите в контекстном меню пункт Move (Переместить); откроется диалоговое окно Move Server (Перемещение сервера), представленное на рис. 22.11.

Рис. 22.11. Перемещение сервера

Конечно, это дополнительная работа, но правильная организация серверов в Active Directory Sites and Services окупится сполна, если производственная среда включает несколько площадок, соединенных каналами WAN.

Добавление связей сайта

Связи сайта применяются для идентификации действительных каналов WAN. Оснастка Active Directory Sites and Services начинает со стандартной связи сайта, имеющей очередное "креативное" имя — `DefaultIPSiteLink`. Точно так же, как вы можете переименовать стандартный сайт и добавить новые сайты, у вас есть возможность переименовать стандартную связь сайта и создать другие связи сайта.

Взгляните на рис. 22.12. На нем показаны три сайта, входящие в состав производственной среды: головной офис, офис на другом конце города и удаленный офис. На этой диаграмме три сайта соединены между собой тремя каналами WAN с разными скоростями. Позже в этом разделе мы продемонстрируем, как создать связи сайта, соответствующие таким каналам WAN.

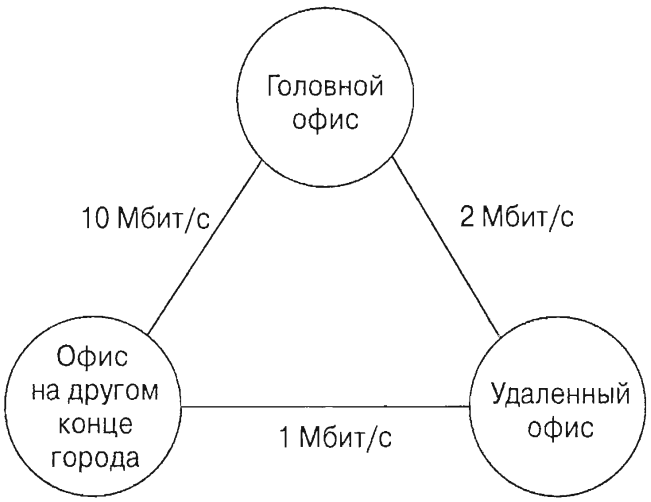


Рис. 22.12. Три сайта и три связи сайтов

При создании связей сайта на выбор есть два варианта: IP-связи сайта и SMTP-связи сайта. Почти всегда вы будете использовать IP-связи сайта.

IP-связь сайта

IP-связи сайта применяют вызов удаленных процедур (remote procedure call — RPC) через подключение IP-транспорта. Практически все время вам придется использовать именно IP-связи сайта. Одно из основных требований заключается в наличии IP-подключения между сайтами. Если пингование между сайтами проходит успешно, значит, вы располагаете IP-подключением и должны применять IP-связь сайта.

SMTP-связь сайта

Если прямое IP-подключение не доступно, и вы не реплицируете данные домена, то можете сконфигурировать SMTP-связь сайта. На первый взгляд SMTP *выглядит* как идеальное решение: этот протокол не обязательно должен функционировать постоянно, канал не должен слишком часто быть активным и — что особенно впечатляет — у вас даже есть возможность отправлять обновления репликации через почтовую службу Hotmail!

К сожалению, пользы от всего этого не так уж много. Прежде всего, вы можете реплицировать только схему уровня леса и контексты назначения имен в конфигурации, поэтому вам не удалось бы применять SMTP для репликации обновлений между контроллерами домена в том же домене. Другими словами, с помощью SMTP

невозможно реплицировать такие простые задачи, как добавление либо изменение пользователей, компьютеров или групп внутри домена.

Кроме того, вы не можете использовать практически ни один из старых почтовых серверов. Чтобы среда Active Directory, имеющая высокие требования к безопасности, позволила применять для репликации почтовый сервер, вам понадобится сертификат, выданный центром сертификации предприятия, который гарантирует защищенную доставку почты.

Создание связей сайта

Ниже перечислены шаги, которые необходимо выполнить в оснастке Active Directory Sites and Services для получения конфигурации, отражающей диаграмму на рис. 22.12.

1. Откройте оснастку Active Directory Sites and Services.
2. Добавьте сайт по имени `RemoteOffice` с использованием процедуры, описанной ранее в этой главе.
3. Добавьте подсеть 192.168.30.0/24 к сайту `RemoteOffice` с применением процедуры, описанной ранее в этой главе.
4. Перейдите к папке Sites⇨Inter-Site Transports⇨IP (Сайты⇨Межсайтовые транспорты⇨IP). Щелкните правой кнопкой мыши на `DEFAULTIPSITELINK` и выберите в контекстном меню пункт Rename (Переименовать).
5. Введите `CrossHQ` в качестве имени. К этой связи сайта добавляются `Crosstown`, `HQ` и `RemoteOffice`. Вскоре вы удалите из нее сайт `RemoteOffice`.
6. Щелкните правой кнопкой мыши на элементе IP, выберите в контекстном меню пункт New Site Link (Создать связь сайта) и назначьте этой новой связи сайта имя `CrossRemote`.
7. Выберите сайты `Crosstown` и `RemoteOffice` и щелкните на кнопке Add (Добавить). Окно будет выглядеть примерно так, как показано на рис. 22.13. Щелкните на кнопке OK.

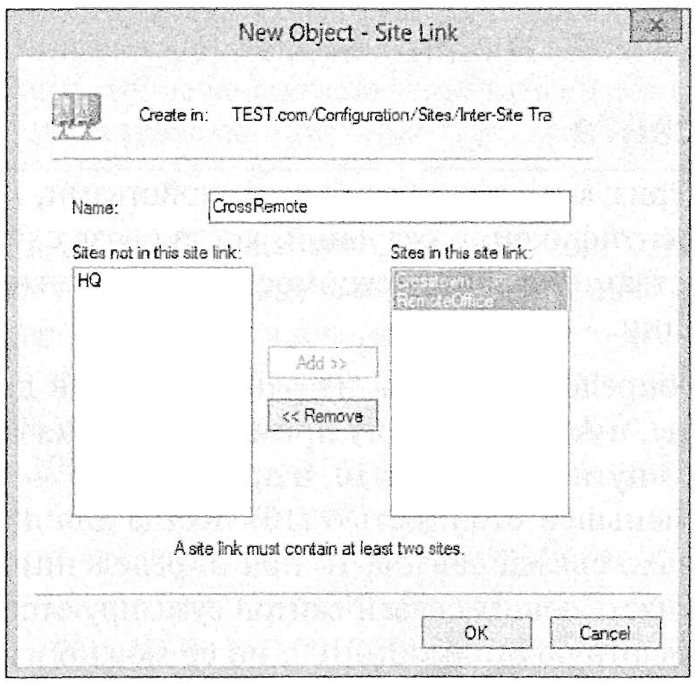


Рис. 22.13. Добавление связи сайта

8. Щелкните правой кнопкой мыши на элементе IP и выберите в контекстном меню пункт New Site Link еще раз.
9. Назовите новую связь сайта `HQRemote`.
10. Выберите сайты `HQ` и `RemoteOffice` и щелкните на кнопке Add. Щелкните на кнопке OK.

    Когда вы создали сайт `RemoteOffice`, единственной доступной связью сайта была `DEFAULTIPSITELINK`, которую вы затем переименовали в `CrossHQ`.
11. Щелкните правой кнопкой мыши на связи сайта `CrossHQ` и выберите в контекстном меню пункт Properties (Свойства).
12. Выберите сайт `RemoteOffice` и щелкните на кнопке Remove (Удалить). Окно должно выглядеть подобным показанному на рис. 22.14. Щелкните на кнопке OK.

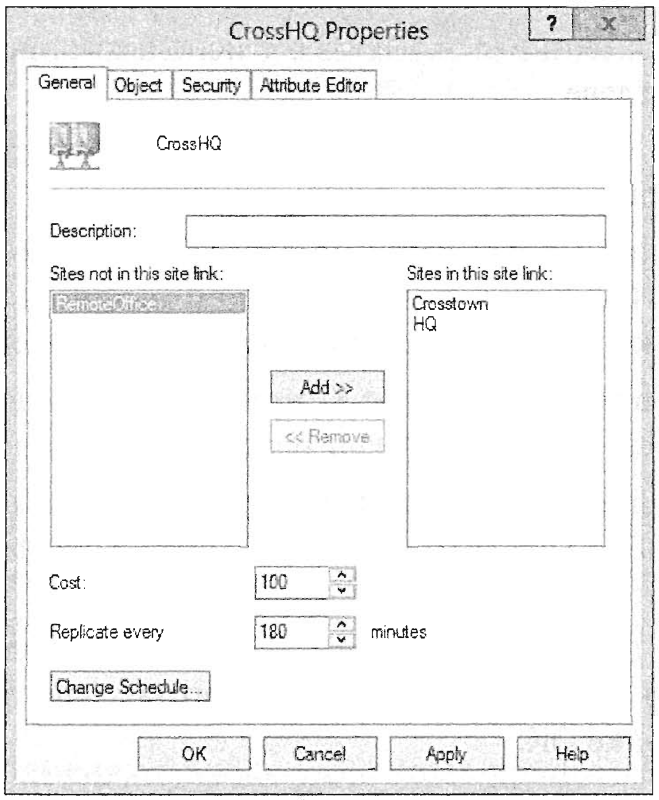


Рис. 22.14. Удаление сайта из связи сайта

Свойства связи сайта

Связи сайта характеризуются тремя важными свойствами, которые используются Active Directory для идентификации ситуаций, когда связь сайта будет задействована. Этими тремя свойствами являются стоимость, частота выполнения репликации и расписание репликации.

- **Стоимость.** Для определения пути из одного сайта в другой, имеющего наименьшие затраты, в Active Directory применяется показатель стоимости. Если стоимость одного пути составляет 10, а другого пути — 100, то будет использоваться путь с меньшей стоимостью (10). Когда для достижения сайта применяется несколько связей сайтов, то при определении минимальных затрат стоимости всех участвующих связей сайтов суммируются. При создании связь сайта имеет стандартную стоимость 100, но ее можно изменить, указав любое значение из диапазона 1–99 999.

- **Частота репликации.** Это свойство отражает то, насколько часто происходит репликация между сайтами. Начальная репликация внутри сайта выполняется каждые 15 секунд между контроллерами домена. Однако проведение репликации каждые 15 секунд по каналу WAN представляется слишком частым. По умолчанию репликация по каналам WAN происходит каждые 180 минут. Данное значение можно изменить на любое другое из диапазона 15–10 080.
- **Расписание.** Расписание указывает, когда будет использоваться канал. Стандартное расписание предусматривает применение канала 24 часа в сутки 7 дней в неделю. Тем не менее, изменив это расписание, вы можете ограничить время использования канала для репликации. Например, если в период с полуночи до 6 часов утра интенсивность применения канала невысока, но приближается к максимуму в рабочее время, можете сконфигурировать репликацию между сайтами так, чтобы она происходила только между 00:00 и 6:00.

Подсчет стоимости

Для назначения стоимости IP-связям сайтов имеется широкий диапазон значений (от 1 до 99 999). Вспомните, что эти значения будут использоваться Active Directory при выборе канала, применяемого для попадания на другой сайт.

Пример из практики

Стоимость является относительной

При назначении стоимости важно гарантировать как можно более точное отражение скорости канала. Например, если одна линия 10 Мбит/с имеет стоимость 10, то все линии 10 Мбит/с должны иметь стоимость 10. Аналогично, если линия 10 Мбит/с имеет стоимость 10, то для линии 1 Мбит/с должно быть выбрано достаточно высокое число (такое как 100); тогда скорости подключений между 1 Мбит/с и 10 Мбит/с получат стоимости из промежутка 10–100. Можно также использовать разные числа и разные диапазоны чисел. Скажем, вы могли бы назначить стоимость 1000 подключению 1 Мбит/с и стоимость 100 подключению 10 Мбит/с. Однако мы не рекомендуем применять небольшие числа из очень узкого диапазона вроде стоимости 1 для линии 10 Мбит/с и стоимости 10 для линии 1 Мбит/с. Если когда-то в будущем добавится линия 20 Мбит/с, то вы не сможете назначить ей стоимость меньше 1, поэтому придется заново перестраивать и переназначать все стоимости.

Взгляните на рис. 22.15. Здесь показаны три сайта со связями сайтов и скоростями каналов WAN. Вдобавок каждой связи назначена стоимость.

Поскольку связь `CrossHQ` реализована с помощью самого быстрого канала (линия 10 Мбит/с), ей назначена стоимость 10 — наименьшая среди всех связей. Связь `CrossRemote` является самой медленной (1 Мбит/с), поэтому ей назначена наивысшая стоимость 100. Связь `CrossHQ` располагает каналом WAN со скоростью 2 Мбит/с, и этой связи назначена стоимость 25.

Когда сайт `HQ` желает провести репликацию с офисом на другом конце города, он видит, что прямой путь, использующий CrossHQ, обладает наименьшей стоимостью, равной 10, по сравнению с затратами, которые составят 125 (100+25), если проложить путь через удаленный офис.

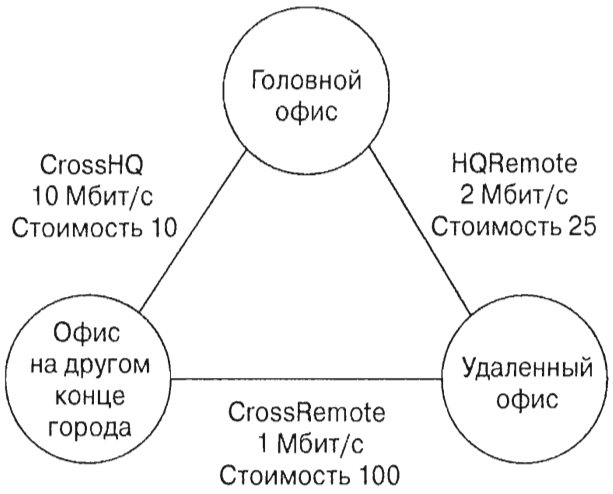


Рис. 22.15. Три сайта, соединенные с помощью трех связей сайтов

Однако когда удаленный офис желает выполнить репликацию с офисом на другом конце города, то наименее затратный путь проходит через сайт HQ; его стоимость составляет 35 (10+25). Прямой путь с применением связи `CrossRemote` имеет стоимость 100, поэтому им следует пользоваться лишь в случае недоступности других путей.

Конфигурирование межсайтовой репликации

Теперь, когда вы видели, как создаются подсети, сайты и связи сайтов, вам необходимо узнать, каким образом сконфигурировать для согласования с сетевой инфраструктурой. Вам уже известно, что внутри сайта репликация Active Directory выполняется за счет построения топологии репликации между контроллерами домена.

Но та же самая топология через каналы WAN была бы неэффективной, поэтому взамен AD создает минимальное остовное дерево, что означает создание набора межсайтовых путей репликации, который минимизирует нагрузку на полосу пропускания глобальной сети. Взгляните на оснастку Active Directory Sites and Services, показанную на рис. 22.16. Здесь видны три сайта с тремя IP-связями сайтов.

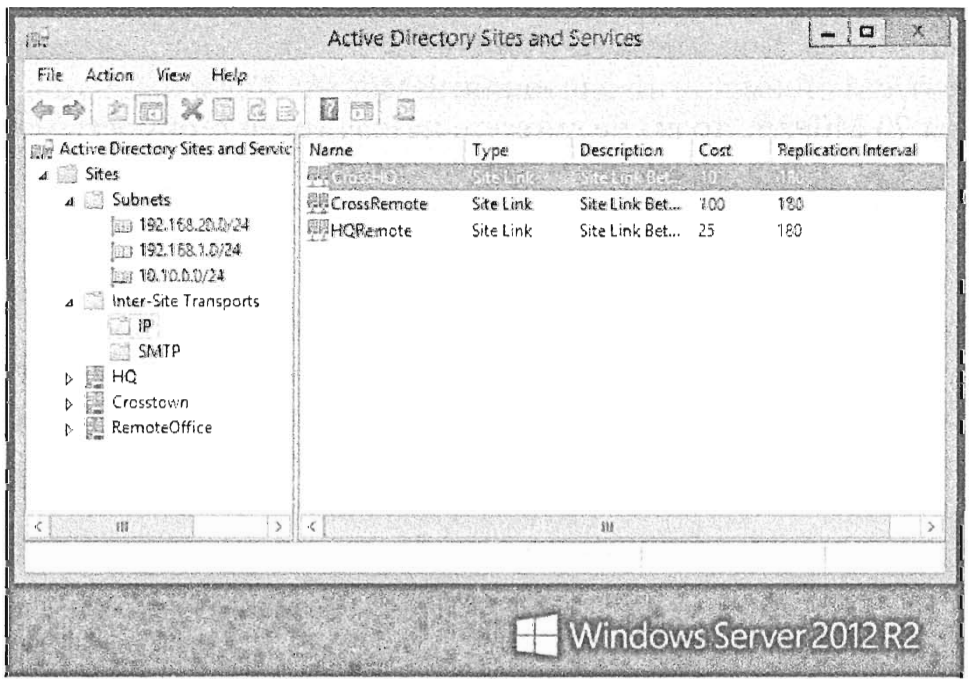


Рис. 22.16. Оснастка Active Directory Sites and Services с тремя сайтами и тремя связями сайтов

Обратите внимание, что стоимость каждой связи сайта была модифицирована в Active Directory Sites and Services. Вскоре вы узнаете, как это делать.

Хотя это простое предприятие, оно служит хорошей иллюстрацией проблем в многосайтовой среде. Вы видите, что после настройки сайтов контроллеры домена самостоятельно выясняют, как выполнять репликацию между ними *внутри сайта*. Однако при выходе за пределы сайта им требуется небольшая помощь.

Вы сообщаете AD о соединениях между сайтами, создавая связи сайтов. Конфигурируя свойства связей сайтов, вы помогаете Active Directory идентифицировать путь, используемый для репликации, определять, когда репликация должна выполняться, и выяснять, насколько часто она требуется.

Если дважды щелкнуть на любом объекте связи сайта, откроется диалоговое окно свойств, подобное приведенному на рис. 22.17.

Рис. 22.17. Диалоговое окно свойств связи сайта

Это диалоговое окно *чрезвычайно* важно по трем причинам.

- Поле со счетчиком Cost (Затраты) применяется для того, чтобы помочь AD определить, какую связь использовать. Служба Active Directory отдаст предпочтение путям с меньшими затратами. По умолчанию в этом поле указана стоимость 100.
- Поле со счетчиком Replicate Every XX Minutes (Выполнять репликацию каждые XX минут) предназначено для управления частотой репликации через эту связь. По умолчанию в этом поле установлено значение 180 минут.
- Наконец, кнопка Change Schedule (Изменить расписание) позволяет модифицировать моменты времени, когда будет происходить репликация, основываясь на расписании.

Щелчок на кнопке Change Schedule приводит к открытию диалогового окна, похожего на показанное на рис. 22.18.

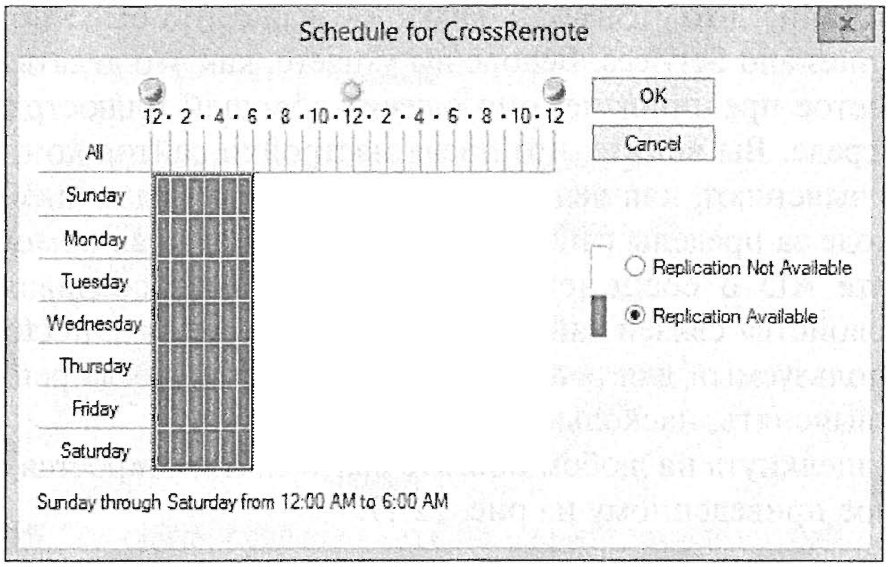


Рис. 22.18. Настройка расписания репликации

Расписание для этой связи сайта было изменено, чтобы разрешить проведение репликации только в часы, когда отсутствует пиковая нагрузка — с полуночи до 6 часов утра.

Связь между сайтами `HQ` и `Crosstown` может интенсивно использоваться в рабочее время, и вы хотите, чтобы репликация происходила лишь в нерабочие часы. Настройка расписания сообщает AD о том, что не следует пытаться проводить репликацию до 6 часов вечера.

Выполняйте репликацию, по крайней мере, раз в 180 дней

Репликация сайтов Active Directory должна выполняться, по крайней мере, раз в 180 дней. Active Directory отбрасывает объекты, которые были неактивными на протяжении 180 дней, так что если какие-то два сайта не общались между собой в течение нескольких месяцев, то из копий AD данных сайтов начинают удаляться объекты, которые ими не использовались, хотя контроллеры домена в других сайтах продолжают работать с этими объектами. Проблема возникает только в случае, когда контроллер домена долгое время не функционирует. Не подключайте DC к сети заново, если он не выполнял репликацию Active Directory в течение более 180 дней.

В предыдущих версиях операционной системы этот срок составлял 60 дней и был основан на стандартной продолжительности существования объектов. Однако в Windows Server 2003 с SP1 и последующих версиях, включая Windows Server 2012 R2, продолжительность существования была изменена на 180 дней.

Как только вы сообщите Active Directory всю информацию о сайтах, усовершенствованная версия KCC под названием ISTG (Inter-Site Topology Generator — генератор межсайтовой топологии) определит, какие связи и когда применять. На каждом сайте один контроллер домена автоматически назначается как ISTG.

Выяснить, какой сервер является ISTG, можно в диалоговом окне NTDS Site Settings Properties (Свойства настроек сайта NTDS) для сайта. Чтобы открыть его, выберите интересующий сайт и дважды щелкните на элементе NTDS Site Settings (Настройки сайта NTDS). Тем не менее, имейте в виду, что ISTG практически не нуждается в контроле.

Важная функция ISTG связана с назначением серверов-плацдармов. Кроме того, вы можете переопределить назначение, выполненное ISTG, указав предпочтительные серверы-плацдармы.

Серверы-плацдармы

Сервер-плацдарм — это контроллер домена внутри сайта, который будет выполнять репликацию на контроллеры домена на других сайтах. В любой момент времени на каждом сайте будет существовать только один активный сервер-плацдарм.

Генератор ISTG выбирает контроллер домена в качестве сервера-плацдарма и периодически проверяет, функционирует ли он. Если этот контроллер домена вышел из строя или переведен в автономный режим, ISTG автоматически назначит на роль сервера-плацдарма другой DC.

По крайней мере, именно так этот механизм функционирует в обычных обстоятельствах, если предположить, что вы не переопределили назначение, сделанное ISTG, указав предпочтительный сервер-плацдарм.

Предпочтительные серверы-плацдармы

Иногда может понадобиться исключить возможность, чтобы какой-то DC становился сервером-плацдармом. Например, какой-то DC вплотную приблизился к пределу своих возможностей, имея загрузку процессора почти 80% и чрезмерно высокий коэффициент использования файла подкачки. Когда ISTG выберет этот DC в качестве сервера-плацдарма, загрузка его процессора может подскочить до 100%, что значительно повлияет на производительность других функций на данном сервере.

Используйте предпочтительные серверы-плацдармы для управления исключениями

С предпочтительными серверами-плацдармами связана одна тонкость. Вы выбираете контроллер домена в качестве предпочтительного сервера-плацдарма не столько из-за того, что хотите, чтобы он был сервером-плацдармом, сколько потому, что не хотите, чтобы сервером-плацдармом стал *какой-то другой* контроллер домена. Другими словами, предпочтительные серверы-плацдармы выбираются, чтобы исключить из процесса выбора один или несколько DC. После назначения любого DC предпочтительным сервером-плацдармом ISTG будет выбирать на эту роль только сервер из состава предпочтительных серверов-плацдармов.

Вы не можете напрямую исключить какой-то контроллер домена из числа предпочтительных серверов-плацдармов. Однако у вас есть возможность назначить *другие* контроллеры домена в качестве предпочтительных серверов-плацдармов. Например, если есть четыре DC, и вы не хотите, чтобы `BF4` становился сервером-плацдармом, вы должны назначить `BF1`, `BF2` и `BF3` предпочтительными серверами-плацдармами.

Из этого следует дополнительное соображение. Если вы когда-либо назначаете одиночный контроллер домена предпочтительным сервером-плацдармом, то должны также назначить на эту роль, по меньшей мере, еще один контроллер домена. В случае если был назначен только один контроллер домена, и он выходит из строя, то ISTG не сможет автоматически передать эту роль другим контроллером домена.

Чтобы назначить сервер в качестве предпочтительного сервера-плацдарма, выполните перечисленные ниже шаги.

1. Откройте оснастку Active Directory Sites and Services.
2. Перейдите в контейнер Servers (Серверы) на интересующем сайте.
3. Щелкните правой кнопкой мыши на сервере, который хотите добавить, и выберите в контекстном меню пункт Properties (Свойства).
4. В списке Transports available for inter-site data transfer (Транспорты, доступные для межсайтовой передачи данных) выберите IP и щелкните на кнопке Add (Добавить).

   Диалоговое окно свойств сервера будет выглядеть примерно так, как показано на рис. 22.19.

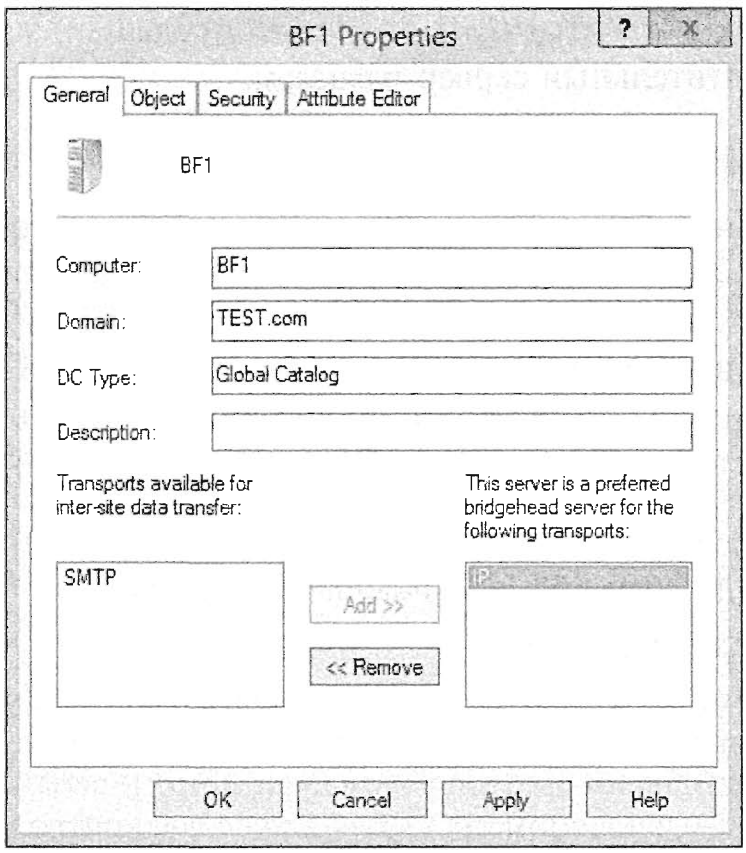


Рис. 22.19. Назначение сервера на роль предпочтительного сервера-плацдарма

5. Щелкните на кнопке OK, чтобы закрыть окно свойств.
6. Повторите эти шаги для каждого сервера, который хотите сделать предпочтительным сервером-плацдармом.

Принудительное выполнение репликации

Инструмент командной строки `repadmin` поддерживает возможность, которой вы можете воспользоваться для выполнения репликации данных между двумя контроллерами домена, даже если это происходит вне расписания. Это может быть полезно при поиске и устранении проблем с репликацией между сайтами. Переключатель `repadmin` является `/replsingleobj`.

Репликация в командной строке

В предыдущих редакциях Windows переключатель `replsingleobject` применялся для репликации объектов между контроллерами домена даже при отсутствии подключения. Однако в Windows Server 2012 R2 он был сокращен до `replsingleobj` (`obj` вместо `object`). Эта сокращенная версия была также доступна в Windows Server 2003 наряду с длинной версией, но в Windows Server 2012 и Windows Server 2008 допускается пользоваться только сокращенной версией. На основании собственного опыта мы можем сообщить, что сколько бы раз вы ни пытались вводить команду, не сократив `object` до `obj`, ничего у вас не выйдет — она просто не заработает.

Вот базовый синтаксис для инструмента `repadmin`:

```
repadmin <команда> <аргументы>
```

С переключателем `replsingleobj` синтаксис выглядит так:

```
repadmin /replsingleobjc sourceDC destinationDC ObjectDN
```

Исходный и целевой контроллеры домена могут быть идентифицированы по именам (таким как `BF1`) или полным доменным именам (вроде `BF1.Bigfirm.com`). Отличительное имя (distinguished name — DN) объекта следует правилам, принятым для таких имен в LDAP. Например, компьютер по имени `TestCPU`, созданный в организационной единице `Sales` домена `Bigfirm.com`, имел бы отличительное имя:

```
CN=TestCPU,OU=Sales,DC=bigfirm,DC=com
```

Если имя DN содержит пробелы, оно должно быть заключено в кавычки.

Чтобы реплицировать объект `TestCPU` из `BF1` в `BF2`, можете воспользоваться приведенной ниже командой. Обратите внимание, что хотя в книге эта команда разнесена на две печатных строки, она должна вводиться в одной командной строке:

```
repadmin /replsingleobj BF1.bigfirm.com BF2.bigfirm.com
CN=TestCPU,OU=Sales,DC=bigfirm.DC=com
```

Конфигурирование клиентов для доступа к ближайшему соседнему сайту

Одним из великолепных средств Windows Server 2012 R2 является возможность обучения клиентов тому, к какому сайту обращаться, если контроллер домена на их сайте вышел из строя. Рассмотрим производственную среду Bigfirm.com на рис. 22.20.

Каждый сайт имеет, по меньшей мере, один контроллер домена, и пользователи обычно входят в систему контроллера домена своего сайта. Но что, если контроллер домена, находящегося внутри сайта офиса на другом конце города, выйдет из строя?

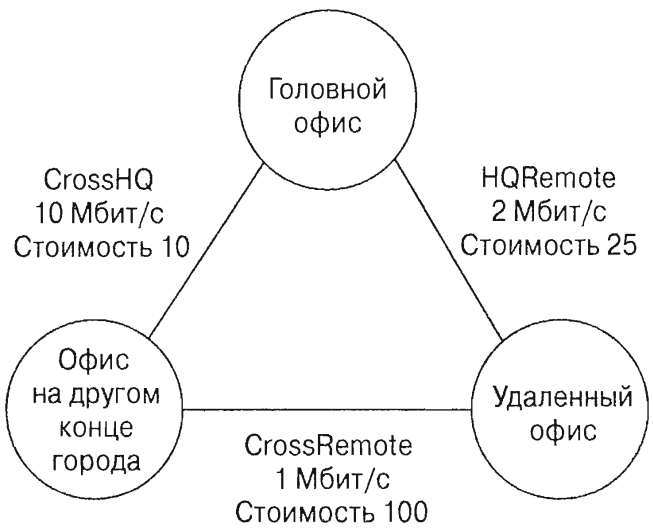


Рис. 22.20. Ближайший соседний сайт

Вряд ли вас устроит ситуация, когда пользователям придется задействовать более медленное подключение и входить в системы контроллеров домена на сайте удаленного офиса. Однако именно это может произойти, если не включен параметр обнаружения ближайшего соседнего сайта. Сначала служба DC Locator попытается найти контроллер домена на том же сайте, к которому относится клиент. Если попытка оказывается безуспешной, служба DC Locator ищет любой контроллер домена независимо от площадки, если только не включен параметр обнаружения ближайшего соседнего сайта.

Термин *ближайший сайт* не совсем точен. В Active Directory отсутствует концепция расстояния, но известно о стоимости, сконфигурированной в свойствах связей сайта. Хотя, скорее всего, ближайшие сайты будут иметь самые быстрые каналы WAN, поэтому настроены с наименьшей стоимостью, организация может быть сконфигурирована по-другому.

Например, удаленный офис может находиться на расстоянии пары километров от офиса на другом конце города, но на расстоянии десятка километров от головного офиса компании. Стоимость связи между удаленным офисом и головным офисом составляет 25, а стоимость связи между офисом на другом конце города и удаленным офисом равна 100. Если бы принималось во внимание расстояние, то ближайшим считался бы сайт офиса на другом конце города, но поскольку учитывается стоимость, то в качестве ближайшего соседнего сайта идентифицируется головной офис компании, т.к. стоимость связи с ним является наименьшей.

Средство ближайшего соседнего сайта является недоступным в клиентах, которые функционируют под управлением операционных систем, предшествующих Windows Vista

Средство ближайшего соседнего сайта будет работать только для клиентов и серверов, функционирующих под управлением Windows 7, Windows 8 и Windows Server 2008 или последующих версий операционных систем. Это средство не оказывает влияния на поведение клиентов с Windows XP, Windows Server 2003 или более ранними версиями ОС.

Вы можете сконфигурировать серверы Windows 7, Windows 8 и Windows Server 2012 R2 на использование при поиске ближайшего соседнего сайта критерия стоимости связи. Есть два метода, которые можно применять для конфигурирования этого средства:

- групповая политика;
- модификация реестра.

Конфигурирование средства ближайшего соседнего сайта с помощью групповой политики

Если вы хотите сконфигурировать множество клиентов так, чтобы для определения ближайших сайтов использовался критерий стоимости, можно внести изменения в групповую политику (Group Policy).

Сайт, домен или организационная единица

Приведенная ниже процедура проведет вас по шагам конфигурирования всех клиентов в домене за счет изменения стандартной политики домена. Тем не менее, вы можете слегка модифицировать шаги, чтобы создать либо изменить любой объект GPO и связать его с сайтом, доменом или организационной единицей в зависимости от того, на какие компьютеры вы хотите воздействовать.

Чтобы сконфигурировать всех клиентов в домене, выполните описанные ниже шаги.

1. Запустите консоль управления групповой политикой (Group Policy Management Console), выбрав в окне диспетчера серверов пункт меню Tools⇨Group Policy Management (Сервис⇨Управление групповой политикой).
2. Перейдите к объекту Default Domain Policy (Стандартная политика домена) внутри папки Forest⇨Domains⇨*Имя домена* (Лес⇨Домены⇨*Имя домена*).
3. Щелкните правой кнопкой мыши на элементе Default Domain Policy и выберите в контекстном меню пункт Edit (Правка).
4. Перейдите в папку Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Вход в сеть⇨Записи DNS средства обнаружения контроллеров домена).
5. Дважды щелкните на параметре Try Next Closest Site (Пробовать ближайший соседний сайт) и в открывшемся окне выберите переключатель Enabled (Включено). Окно консоли будет выглядеть примерно так, как показано на рис. 22.21. Щелкните на кнопке OK.

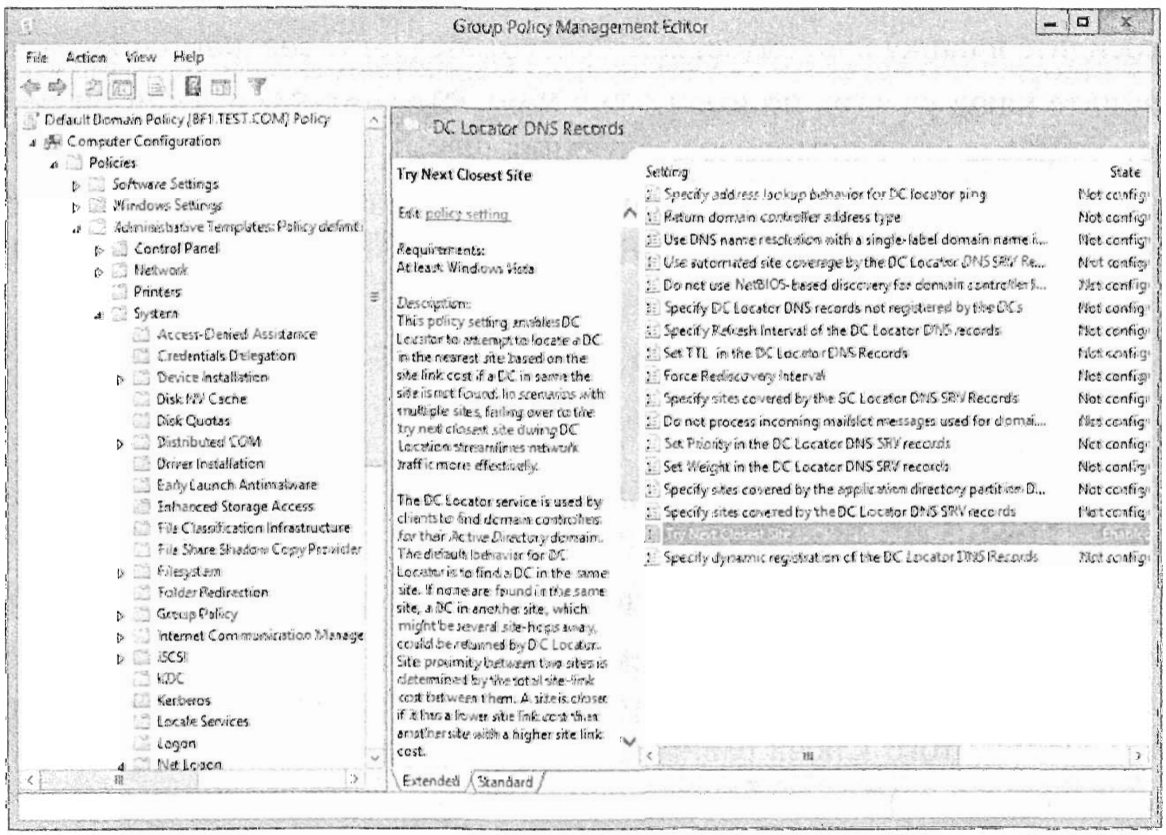


Рис. 22.21. Конфигурирование параметра Try Next Closest Site посредством групповой политики

6. Закройте редактор управления групповыми политиками и консоль управления групповой политикой.

   Вы можете подождать, пока групповая политика применится в результате обычного цикла обновления или воспользоваться командой `gpupdate /force`, чтобы выполнить обновление всех индивидуальных клиентов.

Конфигурирование средства ближайшего соседнего сайта с помощью реестра

Групповая политика позволяет один раз сконфигурировать параметр и повлиять на множество клиентов. Но если вы хотите, чтобы средство ближайшего соседнего сайта применялось только определенным клиентом, можете модифицировать реестр.

Будьте осторожны при работе с реестром

Внося изменения в реестр, нужно действовать очень осторожно. Некорректное редактирование реестра может серьезно нарушить работу вашей системы. Прежде чем модифицировать реестр, рекомендуется создать резервную копию всех ценных данных на компьютере.

Чтобы включить параметр `Try Next Closest Site` для клиента Windows 7 или Windows 8, выполните перечисленные ниже действия.

1. Запустите редактор реестра, для чего щелкните на кнопке Start (Пункт), введите в поле поиска `regedit` или `regedit32` и нажмите <Enter>. Обе команды запускают один и тот же редактор реестра.
2. Выберите раздел `HKEY_LOCAL_MACHINE (HKLM)`.
3. Перейдите в папку `System\CurrentControlSet\Services\Netlogon\Parameters`.
4. Найдите ключ реестра по имени `Try Next Closest Site`. Если он не существует, создайте его с помощью следующих шагов.
5. Щелкните правой кнопкой мыши в области параметров и выберите в контекстном меню пункт New⇨DWORD (32-bit) Value (Создать⇨Параметр DWORD (32 бита))
6. Назначьте новому ключу имя **`Try Next Closest Site`**, разделяя слова пробелами.
7. Дважды щелкните на ключе `Try Next Closest Site`. Измените его значение на `1`. Окно редактора реестра будет выглядеть примерно так, как показано на рис. 22.22.
8. Щелкните на кнопке OK. Закройте редактор реестра.

В качестве напоминания: этот параметр вступает в игру, только если не удается связаться с контроллером домена внутри того же сайта, где находится клиент.

Если значение этого ключа равно `1`, служба DC Locator будет использовать при поиске контроллера домена на ближайшем соседнем сайте величину стоимости связей сайта. Когда значение ключа равно `0`, служба DC Locator не будет применять величину стоимости и может обратиться к любому контроллеру домена независимо от площадки.

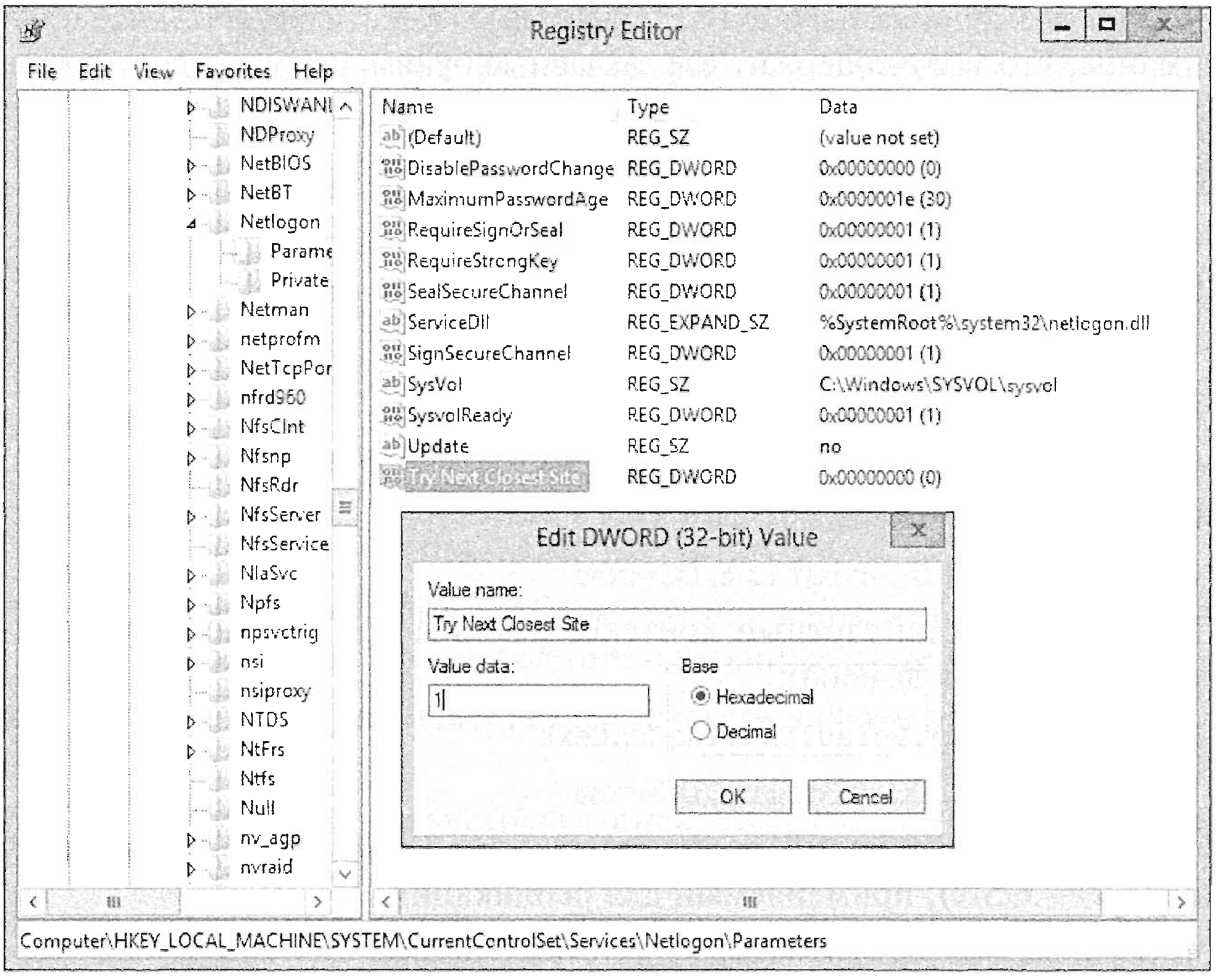


Рис. 22.22. Изменение реестра

Использование PowerShell

Командлеты PowerShell раскрывались во многих главах этой книги, так что вы видели многие из них. В настоящем разделе рассказывается о нескольких командлетах, которые можно применять как по отдельности, так и в сочетании друг с другом для извлечения информации из Active Directory.

Использование отличительных имен

В описанных ниже шагах речь идет об отличительных именах (DN), которые освещались более подробно в главе 7 и упоминались ранее в этой главе. Прежде чем вы сможете создавать DN на лету, необходимо немного попрактиковаться, но возможность создания и идентификации имен DN наверняка пригодится вам в работе, особенно при написании сценариев или анализе подробностей Active Directory.

Здесь изложены основы инструментов поиска в Active Directory, встроенных в PowerShell, которые могут оказаться чрезвычайно полезными, если организация достаточно велика, чтобы поддерживать несколько сайтов.

1. Запустите экземпляр Windows PowerShell.
2. Получите определенную информацию о своей среде, создав сначала с помощью указанного ниже командлета переменную, которая будет представлять

домен. Этот командлет заносит в переменную $dom имя DN домена. Обратите внимание, что LDAP содержит все заглавные буквы.

```
$dom=[adsi]"LDAP://RootDSE"
```

3. Теперь вы можете запросить информацию о домене, используя переменную $dom, с помощью указанных ниже команд.

   а. Просмотрите контекст именования корневого домена:

   ```
   Write-Host $obj.RootDomainNamingContext
   ```

   Наш результат: DC=bigfirm,DC=com

   б. Просмотрите контекст именования всех доменов в лесе:

   ```
   Write-Host $obj.NamingContexts
   ```

   Наш результат: DC=bigfirm,DC=com

   в. Просмотрите стандартный контекст именования по умолчанию (или частичное имя DN домена):

   ```
   Write-Host $obj.DefaultNamingContext
   ```

   Наш результат: DC=bigfirm,DC=com

   г. Определите наивысший порядковый номер обновления (update sequence number — USN), применяемый для репликации:

   ```
   Write-Host $obj.HighestCommittedUSN
   ```

   Наш результат: 86051

Бывают ситуации, когда отличительное имя пользователя неизвестно, поскольку вы не знаете, в какой организационной единице он находится. Если вы знаете какие-то подробности об учетной записи (такие как отображаемое имя), вы можете извлечь отличительное имя, воспользовавшись встроенным в Active Directory поисковым механизмом. В этом примере предполагается, что учетные записи применяют отображаемое имя в формате "имя, точка, фамилия" (например, John.Smith). Таким образом, все, что вам требуется знать для поиска — это имя и фамилия пользователя.

1. Сначала создайте переменную для фильтра (элемент поиска) с помощью такой строки:

   ```
   $filter = "(&(ObjectCategory=User)(DisplayName=John.Smith*))"
   ```

   Символ подстановки * используется для поиска всех экземпляров (таких как John.Smith.2 и John.Smith.3).

2. Затем создайте экземпляр поискового механизма, применяющего фильтр, посредством следующей строки:

   ```
   $Searcher = New-Object System.DirectoryServices.DirectorySearcher($Filter)
   ```

3. Наконец, найдите все экземпляры с помощью такой команды:

   ```
   Searcher.Findall()
   ```

   Будут выведены имена DN всех учетных записей, которые соответствуют этому отображаемому имени.

   Предыдущий код можно даже вставить в сценарий, предназначенный для приема параметра (такого как имя пользователя).

4. Введите следующие строки в любом текстовом редакторе (например, Notepad) и сохраните результат в файле **FindUser.ps1** внутри папки C:\Scripts.

   Первая строка идентифицирует параметр, который будет приниматься, а вторая строка использует этот параметр в фильтре. Остальные строки были описаны выше.

```
Param($filterName)
$filter = "(&(ObjectCategory=User)(DisplayName=$filterName))"
$Searcher = New-Object System.DirectoryServices.
DirectorySearcher($Filter)
Searcher.Findall()
```

5. Запустите этот сценарий с помощью такой строки в PowerShell:

```
C:\Scripts\FindUser.ps1 John.Smith*
```

Вам может понадобиться извлечь список групп, членом которых является пользователь. Если вы знаете имя DN, выполните описанные ниже шаги.

1. Создайте переменную для объекта пользователя в своем домене с применением имени DN.

   В этом коде мы используем учетную запись Administrator, но можно указать любую другую учетную запись (в том числе учетные записи компьютеров):

```
$user=[adsi]"LDAP://CN=Administrator,CN=Users,Dc=bigfirm,DC=com"
```

2. Извлеките данные о членстве в группах для пользователя, выполнив следующую команду:

```
Write-Host $user.memberof -separator " >>> "
```

   В результате выводится список групп в формате DN. Переключатель separator облегчает определение, где заканчивается одна группа и начинается другая.

Резюме

Создайте сайт. Объекты сайтов добавляются в Active Directory для представления физических площадок с высокоскоростными подключениями, на которых будут размещаться контроллеры домена. После принятия решения о размещении контроллера домена на физической площадке вы должны добавить сайт.

Контрольный вопрос. Создайте сайт для представления новой площадки в Вирджиния-Бич.

Добавьте подсети к сайтам. Подсети клиентов в Active Directory используются для определения, на каком сайте они находятся. Чтобы это работало, необходимо создать объекты подсетей и ассоциировать их с сайтами.

Контрольный вопрос. Создайте объект подсети для представления подсети 10.15.0.0/16, которая существует на площадке Вирджиния-Бич. Ассоциируйте этот объект подсети с сайтом VB (Вирджиния-Бич).

Сконфигурируйте связь сайта для выполнения репликации только в определенные периоды времени. Часто желательно ограничить время выполнения репликации между сайтами. Если используются стандартные параметры, то репликация будет про-

исходить каждые 180 минут. Если в определенные периоды канал WAN интенсивное используется, вы можете сконфигурировать расписание так, чтобы репликация проводилась только в определенные периоды времени.

Контрольный вопрос. Сконфигурируйте сайт `Default-First-Site-Name` (или другой сайт) для выполнения репликации только в промежутке между полуночью и 5 часами утра.

Сконфигурируйте групповую политику для использования средства ближайшего соседнего сайта. Если на сайте клиента контроллер домена оказывается недостижимым, то клиент будет искать любой контроллер домена безотносительно того, насколько близко он находится. Это может отрицательно сказаться на времени открытия сеанса для предприятий с несколькими площадками, соединенными между собой каналами WAN с разными скоростями. Вы можете сконфигурировать клиентов Windows Vista (и более новых) так, чтобы они находили и входили в систему контроллера домена на ближайшем соседнем сайте, если контроллер домена на их сайте не доступен. Это можно сделать с помощью групповой политики или редактора реестра.

Контрольный вопрос. Какой из перечисленных ниже параметров групповой политики должен быть изменен, чтобы включить средство ближайшего соседнего сайта?

1. Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Logon⇨DC Locator DNS Records (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Вход⇨Записи DNS средства обнаружения контроллеров домена).
2. Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Вход в сеть⇨Записи DNS средства обнаружения контроллеров домена).
3. User Configuration⇨Policies⇨Administrative Templates⇨System⇨Logon⇨DC Locator DNS Records (Конфигурация пользователя⇨Политики⇨Административные шаблоны⇨Система⇨Вход⇨Записи DNS средства обнаружения контроллеров домена).
4. User Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records (Конфигурация пользователя⇨Политики⇨Административные шаблоны⇨Система⇨Вход в сеть⇨Записи DNS средства обнаружения контроллеров домена).

Глава 23

Третий контроллер домена: контроллеры домена только для чтения

Большинство контроллеров домена хранят полную копию Active Directory, включая все учетные записи администраторов и их пароли. Кроме того, контроллеры домена наслаждаются безопасной жизнью за запертыми дверьми серверного помещения или шкафа. До тех пор, пока обеспечивается надежная физическая защита контроллеров домена, все они функционируют великолепно.

Тем не менее, иногда контроллеры домена приходится развертывать на других площадках для поддержки пользователей, работающих в офисах филиалов или в удаленных офисах предприятия. В идеальной ситуации в офисах филиалов обеспечивается та же физическая защита, что и в головном офисе, но в реальности это далеко не так. В прошлом администраторам приходилось сопоставлять риск похищения или взлома контроллера домена, размещенного в удаленном офисе, и выгоду от обеспечения более высокой производительности для пользователей удаленного офиса. В наши дни администраторы располагают еще одной возможностью.

Благодаря появлению в Windows Server 2008 контроллеров домена только для чтения (read-only domain controller — RODC), у администраторов есть возможность достичь с их помощью двух целей. Они могут размещать контроллеры RODC на удаленной площадке для поддержки пользователей и в то же время значительно снизить риски, связанные с их похищением или взломом. Использование RODC в Windows Server 2012 R2 упростилось еще больше за счет усовершенствования мастеров развертывания, а также автоматизации и управления посредством Windows PowerShell.

В этой главе вы изучите следующие темы:

- подготовка леса и домена для RODC;
- подготовка домена;
- разрешение кеширования паролей на любом RODC;
- разрешение кеширования паролей на одиночном RODC.

Введение в контроллеры домена только для чтения

Контроллеры домена только для чтения являются контроллерами домена нового типа, который впервые появился в Windows Server 2008. Они специально спроектированы для применения в удаленных офисах предприятия, где невозможно гарантировать физическую защиту.

Третий контроллер домена

Любой домен начинается с одиночного контроллера домена с возможностью записи. Компании часто добавляют второй DC с целью повышения отказоустойчивости на случай, если произойдет отказ первого DC. Хотя перед созданием RODC наличие двух контроллеров домена не является требованием, большинство компаний все-таки располагают двумя контроллерами домена. Контроллер домена только для чтения не может использоваться для повышения отказоустойчивости. Если установлен только один контроллер домена с возможностью записи, и он выходит из строя, то RODC нельзя применять для подхвата ролей FSMO, к тому же на нем нельзя хранить большинство паролей.

В главе 22 вы узнали, как добавлять сайты в Active Directory для различных географически удаленных друг от друга площадок предприятия. Представьте для примера, что головной офис компании соединен с удаленным офисом с помощью медленного канала, как показано на рис. 23.1.

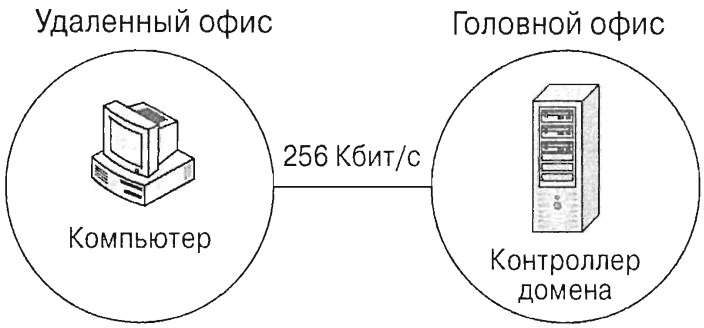


Рис. 23.1. Компания с удаленным сайтом

Для входа в систему своего компьютера любому пользователю из удаленного офиса придется использовать медленный WAN-канал (256 Кбит/с). Время входа в систему можно было бы сократить, разместив в удаленном офисе контроллер домена и сконфигурировав сайт внутри Active Directory.

Перемещение DC в удаленный офис определенно улучшит показатели времени входа в систему у пользователей. Однако это привносит серьезный риск безопасности, связанный с возможностью похищения DC из удаленного офиса или его компрометации. Злоумышленник, владеющий навыками социальной инженерии, вряд ли достиг бы своей цели, если бы явился в головной офис компании и заявил, что забирает контроллер домена для проведения ежегодной профилактики. Однако тот же самый пройдоха, явившись в удаленный офис, вполне мог бы убедить местных сотрудников в том, что их контроллер домена действительно должен быть изъят для “чистки”.

Если бы злоумышленнику удалось получить неограниченный физический доступ к DC, он смог бы узнать пароли ключевых учетных записей, в том числе учетных записей администраторов. Однако если в удаленном офисе разместить RODC вместо обычного DC, то у злоумышленника не будет возможности доступа ко всем паролям в домене, т.к. RODC хранит только ограниченный объем данных, которыми можно воспользоваться в злонамеренных целях.

Благодаря применению BitLocker, диски сами по себе будут бесполезными для того, кто не располагает надлежащим доступом. Обязательно зашифруйте диски на контроллерах RODC с помощью BitLocker, чтобы сократить возможные проблемы на случай их физического похищения. Известно, что во многих мелких филиалах предприятий с ограниченным числом сотрудников, решающих задачи и исполняющих должностные обязанности, которые не связаны с информационными технологиями, вопросам обеспечения физической безопасности уделяется недостаточное внимание. Нам приходилось видеть полнофункциональные контроллеры домена и файловые серверы, установленные на полках в кладовых, куда все сотрудники имели свободный доступ. Контролируйте свою среду, когда только возможно. Ограничьте доступ в помещения с IT-инфраструктурой только по специальным пропускам или карточкам с кодом, шифруйте данные на своих машинах и применяйте RODC вместо полнофункциональных контроллеров домена, когда это позволяет ситуация.

Еще одним важным средством RODC является разделение административных ролей (Administrative Role Separation — ARS), которое предоставляет администраторам домена возможность делегировать права, подобные имеющимся у администратора домена, любому пользователю или группе домена в среде. Это становится удобным в ситуации, когда в удаленном офисе или удаленной зоне DMZ отсутствует IT-персонал, который мог бы помочь с установкой или управлением RODC. Наличие на сайте суперпользователя или соответствующей группы делает возможным локальное управление RODC. Данное лицо (или лица) может проводить обслуживание, а также применение исправлений и обновлений к индивидуальному контроллеру RODC. Одна из важных особенностей ARS заключается в том, что пользователь, которому делегированы более высокие разрешения, имеет права на проведение процедур административного уровня только на данном RODC. Он не располагает правами администратора домена повсюду в среде, поэтому вам не придется беспокоиться о том, что этот пользователь имеет слишком много контроля в рамках предприятия.

Внесение изменений на контроллере домена только для чтения

Что же на самом деле означает понятие *только для чтения*, когда речь идет о контроллере домена только для чтения? Оно вовсе не значит, что на контроллере RODC никогда не происходят изменения; вместо этого оно означает, что изменения не могут исходить из контроллера домена только для чтения. Изменения могут порождаться контроллером домена с возможностью записи и реплицироваться на RODC.

Контроллером домена с возможностью записи может быть любой нормальный DC, на котором могут фиксироваться добавления, удаления и изменения, вносимые в Active Directory. Обычно, когда в Active Directory происходят изменения, такие как добавление учетной записи либо изменение пароля, они могут случаться на любом DC в домене. Затем эти изменения реплицируются на другие DC.

Контроллер RODC не является контроллером домена с возможностью записи. Это означает, что любые изменения, которые пытается внести пользователь, будучи подключенным к RODC, на данном RODC не делаются. Вместо этого производится обращение к DC с возможностью записи, и на нем фиксируется соответствующее изменение после проверки учетных данных. При необходимости изменение реплицируется обратно на RODC.

Такой подход не позволяет злоумышленнику завладеть RODC на удаленной площадке, внести изменения в Active Directory и добиться, чтобы эти изменения реплицировались на все DC с возможностью записи.

Несмотря на то что контроллер RODC будет получать реплицированные данные от DC с возможностью записи, он не хранит все содержимое, находящееся на DC с возможностью записи.

Пример из практики

Похищенный контроллер домена

У одной известной нам компании был удаленный офис, в котором работало около 15 человек. Головной и удаленный офисы компании были разделены железнодорожным путем, компания-владелец которого не разрешала прокладывать кабель под рельсами. Пользователи подключались посредством телефонного модема 256 Кбит/с с созданием сети VPN между головным и удаленным офисами.

Неудивительно, что пользователи часто жаловались на чересчур большое время входа в систему. Со временем администраторы домена создали контроллер домена и поместили его в удаленном офисе. К сожалению, в этом офисе была очень слабая физическая защита.

Спустя примерно месяц контроллер домена пропал. Пользователи даже не могли точно сказать, когда контроллер исчез, хотя за счет анализа журналов администраторам удалось сузить временной интервал. Вскоре было выявлено немало свидетельств, указывающих на причастность к этой пропаже одного из сотрудников, имеющего доступ в офис в нерабочее время, но неопровержимые доказательства отсутствовали.

Поскольку на пропавшем контроллере домена хранилась полная копия Active Directory, включая все административные учетные записи вместе с паролями, в IT-отделе компании довольно быстро началась паника. Было потрачено немало времени на смену паролей и переименование учетных записей. Всерьез подумывали даже о том, не удалить ли их однодоменный лес и начать все заново.

Руководство компании посвятило приличное время оценке риска в случае отказа от перестройки леса. Они провели сравнение этого риска с последствиями для бизнеса, которые могло повлечь за собой удаление леса и воссоздание его с нуля. В конце концов, было решено рискнуть. Риск оказался оправданным: свидетельств того, что кому-то удалось воспользоваться результатами пропажи для нанесения компании ущерба, в итоге так и не было обнаружено.

Если бы вместо DC использовался RODC, то единственной потерей компании оказалась бы стоимость похищенного сервера, зато удалось бы избежать дополнительных рисков, которые вызвали столь сильные переживания у администраторов и руководства.

Содержимое RODC

На контроллере RODC хранятся все учетные записи Active Directory и *большинство* атрибутов, которые можно найти на DC с возможностью записи. Существенная разница между RODC и DC с возможностью записи заключается в том, что на RODC хранится совсем незначительное количество паролей.

Более конкретно, на RODC обычно хранятся только пароли пользователей, не являющихся администраторами, которые входят в системы в этом удаленном офисе. Сохранение на RODC других паролей целенаправленно блокируется.

На рис. 23.2 представлен процесс при наличии RODC в удаленном офисе. Представьте, что пользователь Салли впервые входит на RODC. Ее система связывается с RODC. На RODC учетная запись Салли пока еще не кеширована, поэтому RODC отправит запрос контроллеру домена, находящемуся в головном офисе компании.

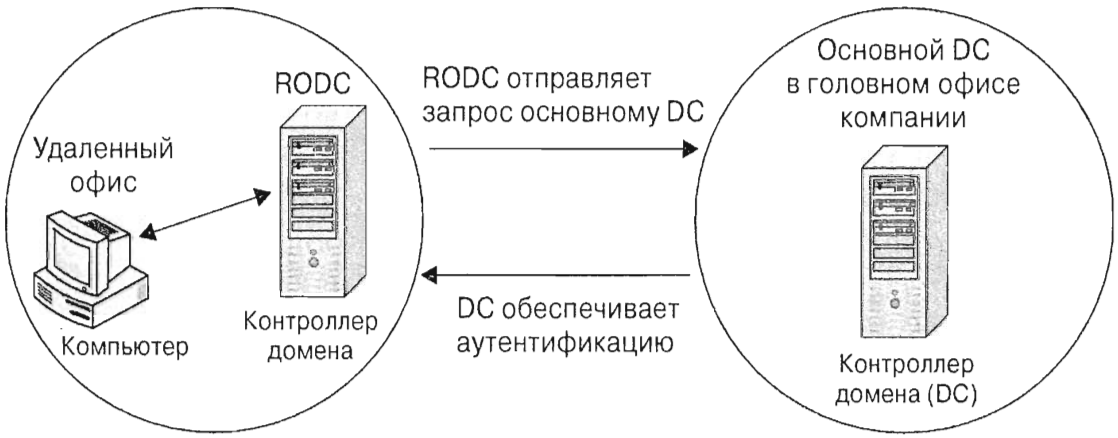


Рис. 23.2. Процесс входа в RODC

Контроллер домена в головном офисе компании проверяет учетные данные Салли и обращается к политике репликации паролей, чтобы определить, можно ли кешировать на этом RODC учетные данные Салли. По умолчанию никакие пароли на RODC не кешируются. Однако, как правило, разрешено кешировать учетные данные пользователей, которые не являются администраторами и работают в удаленном офисе. На RODC не кешируются любые пароли, которые явно запрещено кешировать.

Когда Салли в следующий раз будет входить в систему на удаленном сайте, указанные ею учетные данные сравниваются с кешированными учетными данными на RODC. Термин *кешированные учетные данные* означает, что они хранятся во временном месте на жестком диске сервера.

Кеширование на жестком диске RODC

Если вы — специалист по компьютерному оборудованию, то можете подумать о *кеше*, который представляет собой память, используемую для улучшения производительности. Например, кеш уровня L1 и L2 — это дополнительная память, предназначенная для повышения производительности процессора. Память является изменчивой, и ее содержимое будет утеряно в результате завершения работы или перезагрузки системы. Тем не менее, учетные данные, кешированные на RODC, хранятся на жестком диске контроллера RODC. Эти учетные данные останутся незатронутыми даже после выключения питания RODC или перезагрузки системы.

Самая важная особенность связана с тем, что пароли пользователей в домене, которые еще не входили в системы на удаленной площадке, в RODC не сохраняются и не реплицируются.

А что произойдет, если в систему RODC войдет какой-то администратор с применением административной учетной записи? Контроллер RODC предназначен для защиты от физической атаки, что достигается отказом от сохранения паролей администраторов на сервере. Но если администратор вошел в систему и его пароль кешируется, то RODC не может исполнить свое предназначение.

Чтобы решить такую проблему, политика репликации паролей конфигурируется для запрета кеширования на контроллере RODC паролей учетных записей администраторов. Политику репликации паролей можно изменять и также указывать конкретные группы, которым разрешена или запрещена репликация паролей.

Политика репликации паролей

Политика репликации паролей была добавлена в Windows Server 2008 для поддержки RODC и остается одним из дополнительных преимуществ Windows Server 2012 R2. Она указывает, какие пароли будут кешироваться на RODC. По умолчанию пароли на RODC вообще не кешируются, поэтому вы должны понять, как это работает, чтобы при необходимости модифицировать данную политику.

На рис. 23.3 показано диалоговое окно свойств RODC с выбранной вкладкой Password Replication Policy (Политика репликации паролей). Каждый контроллер RODC имеет собственную политику репликации паролей.

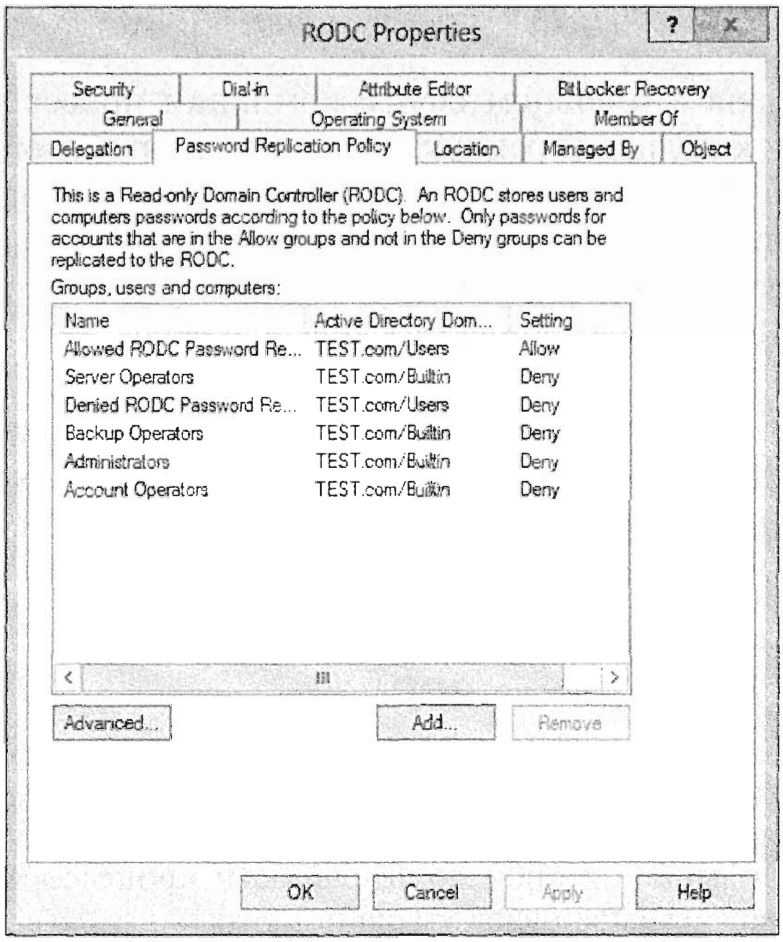


Рис. 23.3. Вкладка Password Replication Policy

Репликация или кеширование

Вы могли заметить, что мы используем и термин *репликация,* и термин *кеширование.* Поскольку пароль кеширован на RODC, он будет реплицироваться обратно на этот RODC, когда изменения распространяются посредством обычной репликации. Кроме того, допускается указывать отдельных пользователей для репликации их паролей на RODC даже до входа этих пользователей в систему. После того как пароль реплицирован на RODC, он считается кешированным на этом RODC.

Обратите внимание, что настройку Deny (Запретить) имеют следующие группы:

- Account Operators (Операторы учетных записей)
- Administrators (Администраторы)
- Backup Operators (Операторы резервного копирования)
- Denied RODC Password Replication (Репликация запрещенных паролей RODC)
- Server Operators (Операторы сервера)

Пользователи, являющиеся членами любой из перечисленных групп, могут входить в систему RODC, но их учетные данные не будут кешироваться на этом RODC. Единственной группой, для которой по умолчанию задана настройка Allow (Разрешить), является Allowed RODC Password Replication (Репликация разрешенных паролей RODC). Пароли пользователей этой группы могут кешироваться.

ОС Windows Server 2012 R2 модифицирует схему Active Directory с целью включения нескольких дополнительных атрибутов Active Directory, поддерживающих политику репликации паролей. Ниже приведено краткое описание этих атрибутов.

- msDS-Reveal-OnDemandGroup. Этот атрибут также называется *разрешенным списком.* Он указывает учетные записи, пароли которых могут кешироваться на RODC. По умолчанию он включает единственное значение — группу Allowed RODC Password Replication. Другими словами, только пользователи из группы Allowed RODC Password Replication (которая является локальной группой домена), могут иметь пароли, кешированные на RODC. Изначально группа Allowed RODC Password Replication пуста, поэтому по умолчанию ни один из паролей не будет кешироваться на RODC.
- msDS-NeverRevealGroup. Этот атрибут также называется *запрещенным списком.* Он указывает учетные записи, пароли которых не могут кешироваться на RODC, и в дополнение к членам группы Denied RODC Password Replication включает группы Account Operators, Server Operators, Backup Operators и Administrators.

  Если учетная запись является членом msDS-NeverRevealGroup и msDS-Reveal-OnDemandGroup, то предпочтение получает msDS-NeverRevealGroup. Это значит, что если учетная запись находится и в разрешенном, и в запрещенном списке, то приоритет получает запрещенный список.
- msDS-RevealedList. Это список учетных записей, которые имеют учетные данные, кешированные на RODC. Чтобы просмотреть данный список, щелкните на кнопке Advanced (Дополнительно) внутри вкладки Password Replication Policy диалогового окна свойств RODC.

- msDS-AuthenticatedToAccountList. Этот список содержит все учетные записи, которые пытались пройти аутентификацию на RODC. Администраторы могут время от времени просматривать этот список, чтобы определить, кто аутентифицируется посредством RODC и кого, возможно, следует добавить в разрешенный список. Чтобы просмотреть этот список, щелкните на кнопке Advanced внутри вкладки Password Replication Policy диалогового окна свойств RODC.

Политика репликации паролей работает в сочетании с группами Allowed RODC Password Replication и Denied RODC Password Replication. Ниже указаны два важных аспекта, которые должны приниматься во внимание при настройке политики и групп.

- **Политика репликации паролей специфична для каждого RODC.** Любой отдельно взятый контроллер RODC может располагать своими пользователями или группами, разрешенными либо запрещенными, в то время как другой RODC может иметь дело с другими пользователями или группами, которым разрешено или запрещено кеширование паролей.
- **Группы применяются ко всем RODC повсюду.** Группы Allowed RODC Password Replication и Denied RODC Password Replication применяются ко всем RODC. Например, если какой-то пользователь добавляется в группу Denied RODC Password Replication, то его учетные данные не будут кешироваться ни на одном RODC в рамках домена.

Группа Denied RODC Password Replication

Группа Denied RODC Password Replication автоматически добавляется в Active Directory. Пароли любых пользователей, помещаемых в эту группу, или пользователей, которые являются членами группы, добавленной в эту группу, не будут кешироваться ни на одном RODC внутри домена.

К примеру, если учетная запись пользователя Джо добавлена в эту группу, то пароль его учетной записи не может быть кеширован ни на одном RODC. Если пользователь Салли является членом группы IT Admins и эта группа добавляется в Denied RODC Password Replication, то пароль учетной записи Салли не может кешироваться ни на одном RODC в домене.

На рис. 23.4 показано диалоговое окно свойств группы Denied RODC Password Replication с выбранной вкладкой Members (Члены).

Эта группа является локальной группой доступа домена и по умолчанию включает следующие члены:

- Cert Publishers (Издатели сертификатов)
- Domain Admins (Администраторы домена)
- Domain Controllers (Контроллеры домена)
- Enterprise Admins (Администраторы предприятия)
- Group Policy Creator Owners (Владельцы создателей групповой политики)
- krbtgt
- Read-only Domain Controllers (Контроллеры домена только для чтения)
- Schema Admins (Администраторы схемы)

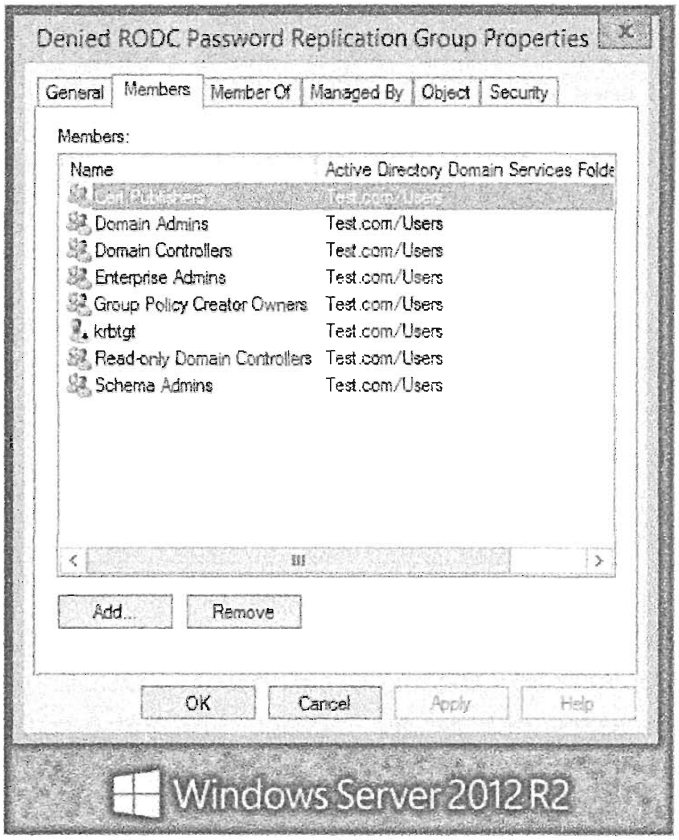


Рис. 23.4. Члены группы `Denied RODC Password Replication`

KRBTGT и KRBTGT123

Контроллеры домена с возможностью записи применяют учетную запись `krbtgt` с протоколом Kerberos. Ее можно считать учетной записью билета для получения билета Kerberos, и ее пароль известен всем контроллерам домена с возможностью записи. Когда требуется создать билеты для аутентификации, они шифруются с помощью симметричного ключа, который выводится из пароля. Поскольку все DC используют для этой учетной записи один и тот же пароль, то все они могут расшифровать билеты, выданные другими DC.

На контроллерах RODC учетная запись билета для получения билета Kerberos работает по-другому. Во-первых, она имеет отличающееся имя, такое как `krbtgt123` (после `krbtgt` может также применяться другая полупроизвольная строка цифр). Во-вторых, с ней связан другой пароль. Контроллерам домена с возможностью записи известен пароль RODC; однако контроллеры RODC не знают пароля учетной записи `krbtgt`, используемой контроллерами домена с возможностью записи.

Пользователи с учетными записями, входящими в состав любой из этих групп, по-прежнему могут входить в систему RODC. Единственное отличие заключается в том, что их учетные данные не будут кешироваться, устраняя риск в плане безопасности в случае похищения RODC.

Группа `Allowed RODC Password Replication`

Группа `Allowed RODC Password Replication` также представляет собой локальную группу доступа домена, находящуюся в контейнере Users (Пользователи). Диалоговое окно свойств группы `Allowed RODC Password Replication` показано на рис. 23.5.

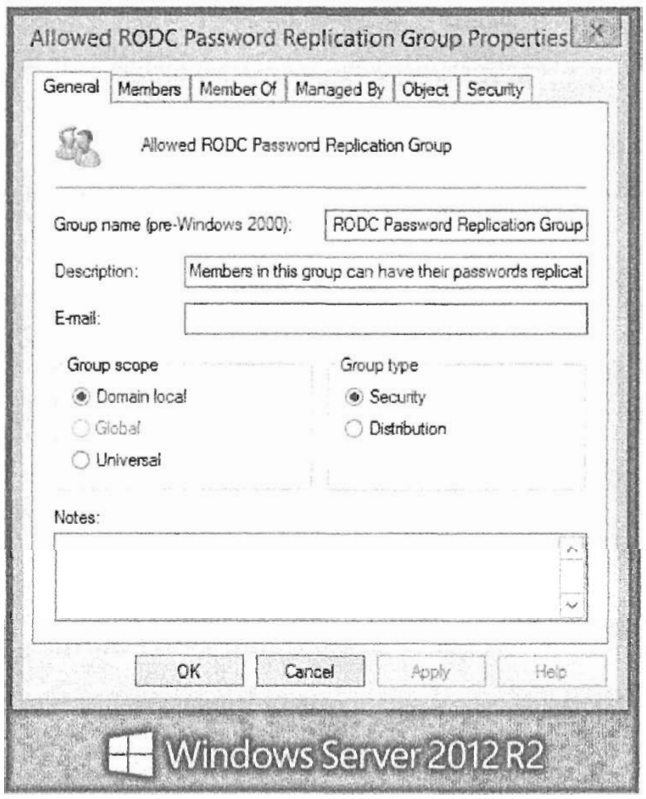


Рис. 23.5. Диалоговое окно свойств группы `Allowed RODC Password Replication`

В отличие от группы `Denied RODC Password Replication`, которая по умолчанию содержит несколько членов, группа `Allowed RODC Password Replication` изначально является пустой. Пароли членов этой группы могут реплицироваться или кешироваться на любом RODC в домене.

Если пользователь является членом этой группы, а также `Denied RODC Password Replication`, то преимущество получит группа `Denied RODC Password Replication`.

Делегирование задач администрирования RODC

Когда вы повышаете сервер до контроллера домена только для чтения, будет предложено указать пользователя или группу, которые будут заниматься администрированием этого RODC или могут завершить повышение этого RODC. Если задачи администрирования будет выполнять какой-то пользователь из удаленного офиса, то это является наилучшим способом делегирования данному пользователю подходящих разрешений.

Когда только возможно, выдавать разрешения или привилегии рекомендуется группам, а не отдельным пользователям, и рассматриваемый случай не является исключением. Вы должны создать группу и добавить в нее пользователя или пользователей, которые будут проводить администрирование RODC.

Пользователи в этой группе получат возможность при необходимости завершить установку RODC на удаленном сайте, и вдобавок будут располагать нужными разрешения для администрирования RODC. Тем не менее, они не имеют административных разрешений на уровне домена, находясь в этой группе.

Несмотря на то что такой группе предоставляются специфичные разрешения для RODC, по умолчанию она не добавляется в группу `Allowed RODC Password Replication`. Однако, возможно, имеет смысл добавить ее учетную запись в разрешенную группу, чтобы учетные данные пользователя кешировались на DC и этот

пользователь мог выполнять локальные задачи администрирования даже в случае недоступности канала WAN.

Требования к развертыванию RODC

Прежде чем контроллер RODC может быть развернут, среда Active Directory должна удовлетворять ряду базовых требований.

- **По меньшей мере, один контроллер домена должен функционировать под управлением Windows Server 2008 или Windows Server 2012.** Контроллер RODC должен проводить репликацию с контроллером домена Windows Server 2008 или Windows Server 2012, имеющим возможность записи. Если ни один из контроллеров домена не работает под управлением хотя бы Windows Server 2008, то установить RODC не удастся. Если вы повышаете до контроллера домена первый сервер Windows Server 2008 в давно существующем домене (например, функционирующем под управлением Windows Server 2003), то сначала должны подготовить домен и лес с помощью команд `adprep /forestprep` и `adprep /domainprep`. Если же лес был построен на серверах Windows Server 2008 или Windows Server 2012, то в запуске `adprep /forestprep` и `adprep /domainprep` нет необходимости. Администраторам, проводящим модернизацию Windows Server 2008 до Windows Server 2012, при установке контроллеров RODC не придется беспокоиться о подготовке домена или леса. Служба Active Directory Domain Services сама позаботится о выполнении задач предварительного конфигурирования `adprep`.
- **Функциональным уровнем домена должен быть, по меньшей мере, Windows Server 2003.** Функциональный уровень домена Windows Server 2003 предоставляет делегирование, ограниченное Kerberos. Это обеспечивает необходимую безопасность для RODC.
- **Функциональным уровнем леса должен быть, по меньшей мере, Windows Server 2003.** Контроллер RODC требует репликации связанных значений, которая доступна, когда функциональный уровень был поднят до Windows Server 2003.
- **Лес должен быть подготовлен за счет выполнения `adprep`.** Прежде чем устанавливать первый контроллер RODC, вы должны запустить команду `adprep`.

Функциональный уровень домена

Разные функциональные уровни домена предоставляют разные возможности. Когда все контроллеры в домене модернизируются до более новых версий операционных систем, вы можете поднять функциональный уровень домена, чтобы получить преимущество от этих новых возможностей.

Ниже перечислены разные функциональные уровни домена.

- **Windows Server 2003.** Используется, когда все контроллеры домена работают под управлением, по меньшей мере, Windows Server 2003. Не забывайте, что это минимальный функциональный уровень домена, который будет поддерживать контроллеры RODC.
- **Windows Server 2008.** Применяется, когда все контроллеры домена функционируют под управлением, по меньшей мере, Windows Server 2008.

- **Windows Server 2008 R2.** Используется, когда все контроллеры домена работают под управлением, по меньшей мере, Windows Server 2008 R2.
- **Windows Server 2012.** Применяется, когда все контроллеры домена функционируют под управлением, по меньшей мере, Windows Server 2012.
- **Windows Server 2012 R2.** Используется, когда все контроллеры домена работают под управлением, по меньшей мере, Windows Server 2012 R2.

Функциональные уровни понижать невозможно

Хотя есть возможность повысить функциональный уровень домена, после повышения пути назад не будет. Это относится к функциональному уровню и домена, и леса. Поскольку более высокие функциональные уровни обеспечивают дополнительные возможности, возникает вполне логичный вопрос: почему бы всегда не выбирать наивысший уровень? Ответ заключается в том, что функциональный уровень домена предписывает минимальную версию ОС, под управлением которой должны функционировать контроллеры домена.

В качестве примера, если у вас есть домен с контроллерами домена Windows Server 2008, то вы можете добавить контроллер домена Windows Server 2012 R2, но поднять уровень выше Windows Server 2008 не удастся. Аналогично, если вы построили домен путем повышения сервера Windows Server 2012 R2 до контроллера домена и выбрали Windows Server 2012 R2 для функциональных уровней домена и леса, то никогда не сможете повысить до контроллера домена сервер, на котором функционирует ОС ниже версии Windows Server 2012.

Вы можете выяснить (и при необходимости модернизировать) текущий функциональный уровень домена, выполнив следующие шаги.

1. Войдите в систему контроллера домена.
2. Откройте оснастку Active Directory Users and Computers, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Users and Computers (Сервис⇨Пользователи и компьютеры Active Directory).
3. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт Raise Domain Functional Level (Поднять функциональный уровень домена). Появится окно, похожее на показанное на рис. 23.6.

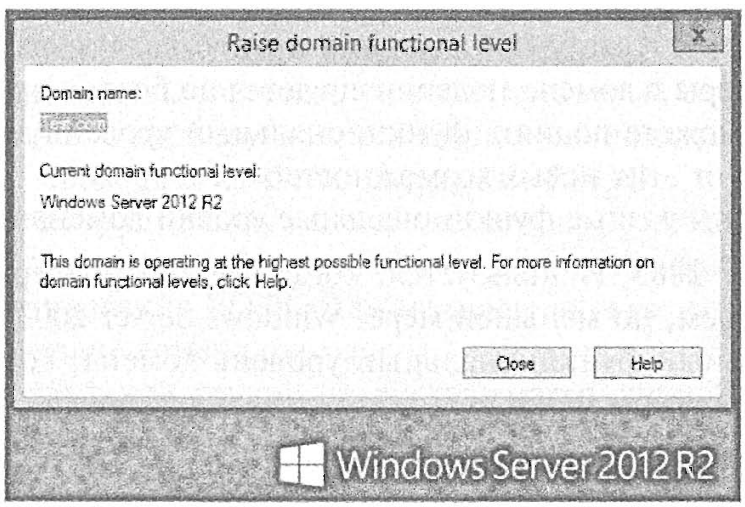


Рис. 23.6. Проверка функционального уровня домена

Здесь текущим функциональным уровнем домена является Windows Server 2012 R2, и домен действует на максимально возможном функциональном уровне, во всяком случае, до появления следующего выпуска Windows Server.

4. Если функциональный уровень домена не соответствует, по меньшей мере, Windows Server 2003, поднимите его до Windows Server 2003, выбрав Windows Server 2003 и щелкнув на кнопке Raise (Поднять).

   Как вы помните из описанных ранее предварительных условий для RODC, функциональным уровнем домена должен быть хотя бы Windows Server 2003, чтобы можно было использовать контроллеры RODC.

Поднять функциональный уровень домена необходимо только на одном контроллере в домене. В пределах короткого промежутка времени он выполнит репликацию на все контроллеры домена.

Если не все контроллеры домена функционируют под управлением, по меньшей мере, Windows Server 2012 R2, то поднять функциональный уровень домена до Windows Server 2012 R2 невозможно. В этом случае после щелчка на кнопке Raise выдается сообщение об ошибке. Контроллеры домена, которые работают под управлением более старых версий ОС, понадобится удалить из домена или модернизировать.

Функциональные уровни леса

Подобно тому, как функциональные уровни домена предлагают разные возможности, различные функциональные уровни леса также обеспечивают разные возможности. Функциональные уровни леса перечислены далее.

- **Windows Server 2003.** Применяется, когда все домены работают на функциональном уровне домена не ниже Windows Server 2003. Не забывайте, что это минимальный функциональный уровень леса, требуемый для поддержки контроллеров RODC.
- **Windows Server 2008.** Используется, когда все домены работают на функциональном уровне домена не ниже Windows Server 2008.
- **Windows Server 2008 R2.** Применяется, когда все домены работают на функциональном уровне домена не ниже Windows Server 2008 R2.
- **Windows Server 2012.** Используется, когда все домены работают на функциональном уровне домена не ниже Windows Server 2012.
- **Windows Server 2012 R2.** Применяется, когда все домены работают на функциональном уровне домена не ниже Windows Server 2012 R2.

Вы не можете сделать функциональный уровень леса выше самого низкого функционального уровня домена. Чтобы можно было модернизировать функциональный уровень домена, сначала потребуется выполнить модернизацию всех контроллеров в этом домене. Затем можно поднять функциональный уровень леса.

Вы можете выяснить (и при необходимости модернизировать) текущий функциональный уровень леса, выполнив описанные ниже шаги.

1. Войдите в систему контроллера домена.
2. Откройте оснастку Active Directory Domains and Trusts (Домены и доверительные отношения Active Directory), выбрав в окне диспетчера серверов пункт

меню Tools⇨Active Directory Domains and Trusts (Сервис⇨Домены и доверительные отношения Active Directory).

3. Щелкните правой кнопкой мыши на элементе Active Directory Domains and Trusts и выберите в контекстном меню пункт Raise Forest Functional Level (Поднять функциональный уровень леса).

   Появившееся окно будет выглядеть примерно так, как показано на рис. 23.7. Здесь текущим функциональным уровнем леса является Windows Server 2012 R2, и это самый высокий уровень, доступный в настоящее время.

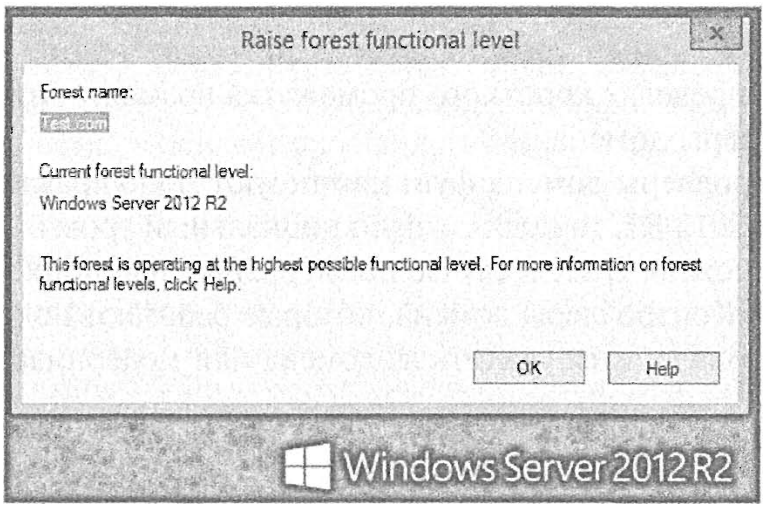


Рис. 23.7. Проверка функционального уровня леса

4. Если функциональный уровень леса не соответствует, по меньшей мере, Windows Server 2003, поднимите его до Windows Server 2003, выбрав Windows Server 2003 и щелкнув на кнопке Raise (Поднять).

Если какой-то из доменов не будет поднят до выбранного уровня леса, он окажется неработоспособным. Другими словами, если любой из доменов в лесе в текущий момент действует на функциональном уровне домена Windows Server 2008 R2, и вы попытаетесь поднять функциональный уровень леса до Windows Server 2012, то эта попытка успеха не принесет.

После того как функциональные уровни домена и леса подняты, по меньшей мере, до Windows Server 2003, можете запустить команду `adprep`, чтобы при необходимости подготовить среду к добавлению контроллеров домена только для чтения.

Запуск `adprep`

Инструмент командной строки `adprep` позволяет подготовить Active Directory для разных сред. Он модифицирует схему Active Directory и обновляет разрешения, чтобы подготовить лес и домен к предоставлению других возможностей.

Вспомните, что для поддержки RODC вы должны иметь хотя бы один контроллер домена Windows Server 2008, но другие контроллеры домена могут функционировать под управлением Windows Server 2003. Поскольку функциональным уровнем домена должен быть, по меньшей мере, Windows Server 2003, необходимо, чтобы все контроллеры домена работали под управлением минимум Windows Server 2003.

Если лес начинался с контроллеров домена, на которых были установлены операционные системы более ранних версий, чем Windows Server 2008 или Windows

Server 2012 (например, Windows Server 2003), то вам придется запустить обе команды — adprep /forestprep и adprep /domainprep. Однако если лес начинал свое существование с контроллеров домена Windows Server 2008 или выше, то выполнять указанные две команды не нужно, но запуск команды adprep /rodcprep по-прежнему необходим.

Для достижения лучшей производительности команда adprep должна выполняться на компьютерах с определенными ролями.

- **adprep /forestPrep**. Эту команду следует запускать на контроллере домена, содержащем роль Schema Master (Хозяин схемы). Чтобы иметь возможность выполнить эту команду, вы должны быть членом групп Schema Admins *и* Enterprise Admins.
- **adprep /domainPrep**. Эту команду следует запускать на контроллере домена, содержащем роль Infrastructure Master (Хозяин инфраструктуры). Чтобы иметь возможность выполнить эту команду, вы должны быть членом группы Domain Admins.
- **adprep /rodcPrep**. Эту команду следует запускать на контроллере домена, содержащем роль Infrastructure Master. Чтобы иметь возможность выполнить эту команду, вы должны быть членом группы Enterprise Admins.

Идентификация хозяина схемы

Если вам неизвестно, какой контроллер домена содержит роль Schema Master или Infrastructure Master, можете воспользоваться одним из следующих простых запросов командной строки: dsquery server -hasfsmo schema или dsquery server -hasfsmo infr. Команда dsquery возвратит отличительное имя сервера, содержащего запрошенную роль. Отличительное имя — это имя, которое применяется для уникальной идентификации объектов с использованием протокола Lightweight Directory Access Protocol (LDAP). Например, контроллер домена по имени BF1 в организационной единице Domain Controllers домена TEST.com имел бы отличительное имя CN=BF1,OU=Domain Controllers,DC=TEST,DC=Com.

Инструмент adprep доступен на установочных DVD-дисках Windows Server 2008 и Windows Server 2012 в указанных ниже папках.

- **Windows Server 2008.** Инструмент adprep находится в папке x:\Sources\Adprep на установочном DVD-диске Windows Server 2008.
- **Windows Server 2008 R2.** Инструмент adprep находится в папке x:\Support\Adprep на установочном DVD-диске Windows Server 2008 R2. Эта папка включает как 64-разрядную версию (adprep.exe), так и 32-разрядную версию (adprep32.exe) этого инструмента.
- **Windows Server 2012 и Windows Server 2012 R2.** Инструмент adprep находится в папке x:\Support\Adprep на установочном DVD-диске Windows Server 2012. В отличие от предыдущих редакций сервера, в данном выпуске 32-разрядная версия adprep отсутствует.

Так как вы будете модифицировать схему леса, для выполнения команды adprep /forestprep понадобится войти в систему с применением учетной записи, явля-

ющейся членом в группах Schema Admins и Enterprise Admins. Чтобы запустить команду adprep /domainprep, вам придется войти в систему от имени учетной записи, которая находится в группе Domain Admins. Выполнение команды adprep /rodcprep требует членства в группе Enterprise Admins.

Для подготовки леса к установке RODC выполните следующие шаги.

1. Войдите в систему контроллера домена, который также является хозяином схемы, с использованием административной учетной записью из группы Enterprise Admins.
2. Вставьте установочный DVD-диск Windows Server 2012 R2.
3. На начальном экране введите **cmd**, щелкните правой кнопкой мыши на элементе Command Prompt (Командная строка) и выберите в контекстном меню пункт Run as administrator (Запуск от имени администратора).
4. Введите букву дисковода DVD, затем символ двоеточия (:) и нажмите <Enter>.

   Например, если DVD-диск находится в дисководе D, введите **D:** и нажмите <Enter>.
5. Перейдите в каталог x:\support\adprep, где x — фактическое имя дисковода DVD, для чего введите команду **cd \support\adprep** и нажмите <Enter>.
6. Подготовьте лес, выполнив описанные ниже действия.
   а. Введите **adprep /forestprep** и нажмите <Enter>. Если необходимо запустить adprep в среде 32-разрядной версии Windows Server, вместо adprep укажите adprep32.
   б. Откроется диалоговое окно ADPREP Warning (Предупреждение ADPREP), запрашивающее подтверждения, что все контроллеры домена в лесе функционируют под управлением, по меньшей мере, Windows Server 2003. Введите **C** и нажмите <Enter>, чтобы продолжить.

На контроллерах домена Windows Server 2008 и Windows Server 2012 лес уже обновлен

Если первый контроллер домена в лесе работает под управлением Windows Server 2008 или более новой версии ОС, то когда этот сервер повышался до контроллера домена, информация уровня леса была приведена в актуальное состояние. Если вы запустите adprep еще раз и удостоверитесь в том, что все актуально, никакого вреда от этого не будет. (В таком случае adprep уведомит, что информация уровня леса уже была обновлена.)

   в. Инструмент adprep выполнит несколько команд импортирования, отображая на экране ход работ. Это займет несколько минут. Когда adprep завершится, вы увидите сообщение Adprep successfully updated the forest-wide information (Adprep успешно обновил информацию уровня леса), после чего появится приглашение на ввод.
7. Подготовьте домен с помощью команды adprep, выполнив приведенные далее действия.

а. Введите **adprep /domainprep** и нажмите <Enter>.

Если необходимо запустить adprep в среде 32-разрядной версии Windows Server, вместо adprep укажите adprep32. Обратите внимание, что 32-разрядная версия adprep в Windows Server 2012 отсутствует. ОС Windows Server 2012 R2 является 64-разрядной.

б. Инструмент adprep обновит домен и выведет сообщение Adprep successfully updated the domain-wide information (Adprep успешно обновил информацию всего домена).

8. Подготовьте домен к созданию контроллеров домена RODC с помощью следующих действий.

а. Введите **adprep /rodcprep** и нажмите <Enter>.

Если необходимо запустить adprep в среде 32-разрядной версии Windows Server, вместо adprep укажите adprep32. Обратите внимание, что 32-разрядная версия adprep в Windows Server 2012 отсутствует. ОС Windows Server 2012 R2 является 64-разрядной.

б. Инструмент adprep обновит раздел ForestDnsZones, раздел DomainDnsZones и раздел домена.

Вы должны увидеть сообщение Adprep completed without errors (Выполнение adprep завершено без ошибок).

Репликация изменений по всему лесу потребует некоторого времени. Как только изменения будут реплицированы, вы сможете успешно повысить контроллер домена до RODC.

Контроллер RODC и серверные приложения

Хотя некоторые серверные приложения будут нормально работать на контроллере RODC, как если бы они выполнялись на обычном контроллере домена, возникнут проблемы с приложениями, которые нуждаются в большем взаимодействии с Active Directory. Учитывая то обстоятельство, что контроллер RODC развертывается в удаленном офисе, где находится минимум квалифицированных IT-специалистов, вполне возможно, что будут присутствовать только приложения, заведомо совместимые с RODC.

Тем не менее, если у вас все же есть серверные приложения, установленные в удаленном офисе, или вы хотите установить их на RODC, то придется провести небольшие исследования.

По адресу http://technet.microsoft.com/library/cc732790.aspx опубликована статья "Приложения, заведомо совместимые с контроллером домена только для чтения", в которой рассказывается о том, что необходимо сделать для обеспечения работоспособности таких приложений. Перечисленные ниже серверные приложения будут работать без проблем или потребуют только минимальной подготовки:

- Microsoft Internet Security and Acceleration (ISA) Server
- Microsoft Office Live Communications Server
- Microsoft Office Outlook

- Microsoft Systems Management Server (SMS)
- Microsoft Operations Manager (MOM)
- Windows SharePoint Services
- Microsoft SQL Server 2005

Серьезная проблема возникает, когда Exchange Server пытается взаимодействовать с глобальным каталогом (global catalog — GC) на RODC. Контроллер RODC может действовать в качестве GC, но этого далеко не достаточно для обслуживания глобальным каталогом локального экземпляра Exchange Server.

Значительные проблемы возникают и в случае, если вы пытаетесь развернуть RODC в удаленном офисе, где используются другие приложения; в такой ситуации не обойтись без дополнительного тестирования. Одни приложения не создадут проблем, с другими придется немного повозиться, а третьи вообще откажутся функционировать на контроллере RODC.

Установка RODC

Повысить сервер Windows Server 2012 R2 до контроллера домена только для чтения можно с помощью описанных далее шагов.

1. Для начала удостоверьтесь, что все перечисленные ниже условия удовлетворены.
   - Сервер присоединен к домену.
   - На сервере установлена роль AD DS.
   - Домен работает, по меньшей мере, на функциональном уровне домена Windows Server 2003.
   - Лес обладает, по меньшей мере, функциональным уровнем леса Windows Server 2003.
   - При необходимости лес и домен были подготовлены посредством следующих команд:

     ```
     adprep /forestprep
     adprep /domainprep
     adprep /rodcprep
     ```

   - Изменения, внесенные командами `adprep`, были реплицированы по всему лесу.

Когда необходимы команды adprep?

В некоторых ситуациях в командах `adprep` нет нужды. Если домен построен с применением серверов Windows Server 2008 или Windows Server 2012, то схема уже актуальна, и `adprep` не требуется.

Однако если вы имеете дело с доменом Windows Server 2003, то перед повышением первого сервера Windows Server 2012 до контроллера домена (что требуется до создания RODC) вам придется выполнить команды `adprep /domainprep` и `adprep /forestprep`. Затем необходимо запустить команду `adprep /rodcprep` и только после этого приступать к созданию RODC.

---

2. Создайте в существующем домене сайт для контроллера RODC, выполнив следующие действия.
   а. Войдите в систему контроллера домена и откройте оснастку Active Directory Sites and Services, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Sites and Services (Сервис⇨Сайты и службы Active Directory).
   б. Щелкните правой кнопкой мыши на контейнере Sites (Сайты) и выберите в контекстном меню пункт New Site (Создать сайт).
   в. Назначьте сайту имя `RemoteOffice` и выберите подходящую связь сайта, если они уже создавались внутри домена. Если специальные связи сайта еще не были сконфигурированы в домене, выберите `DefaultIPSiteLink`. Окно создания нового сайта будет выглядеть примерно так, как показано на рис. 23.8. Щелкните на кнопке OK.
   г. Просмотрите информацию, отображаемую в диалоговом окне, и щелкните на кнопке OK.

      Конфигурирование связи сайта обсуждалось в главе 22.
   д. Закройте оснастку Active Directory Sites and Services.

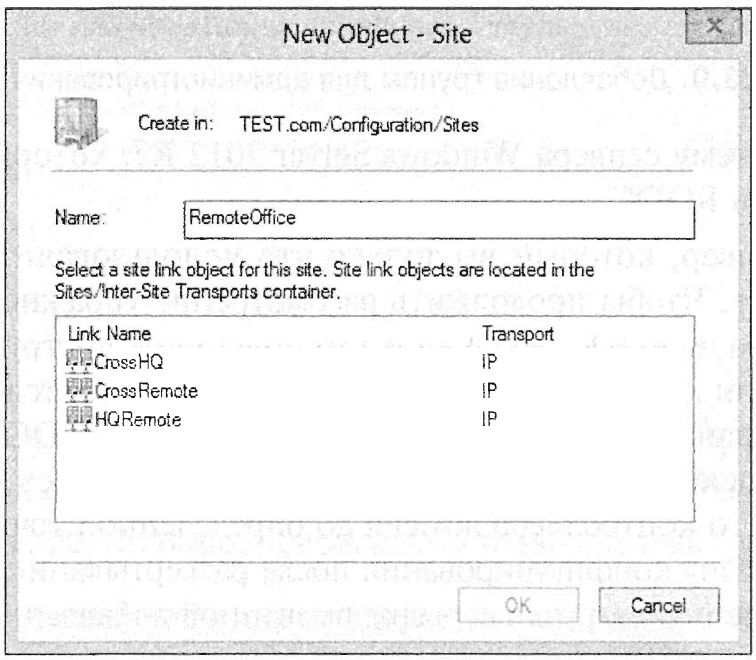


Рис. 23.8. Добавление сайта в оснастке Active Directory Sites and Services

3. Создайте группу, которая будет использоваться для администрирования контроллеров RODC, выполнив описанные ниже шаги.
   а. Откройте оснастку Active Directory Sites and Services, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Sites and Services (Сервис⇨Сайты и службы Active Directory).
   б. Щелкните правой кнопкой мыши на контейнере Users (Пользователи) и выберите в контекстном меню пункт New⇨Group (Создать⇨Группа).
   в. В диалоговом окне New Object — Group (Создать объект — Группа) введите **`Remote Office Admins`** (Администраторы удаленного офиса) для имени создаваемой группы. Удостоверьтесь, что в разделе Group scope (Область дейс-

твия группы) выбран переключатель Global (Глобальная), а в разделе Group type (Тип группы) — переключатель Security (Доступа). Диалоговое окно New Object — Group будет похоже на показанное на рис. 23.9. Щелкните на кнопке OK.

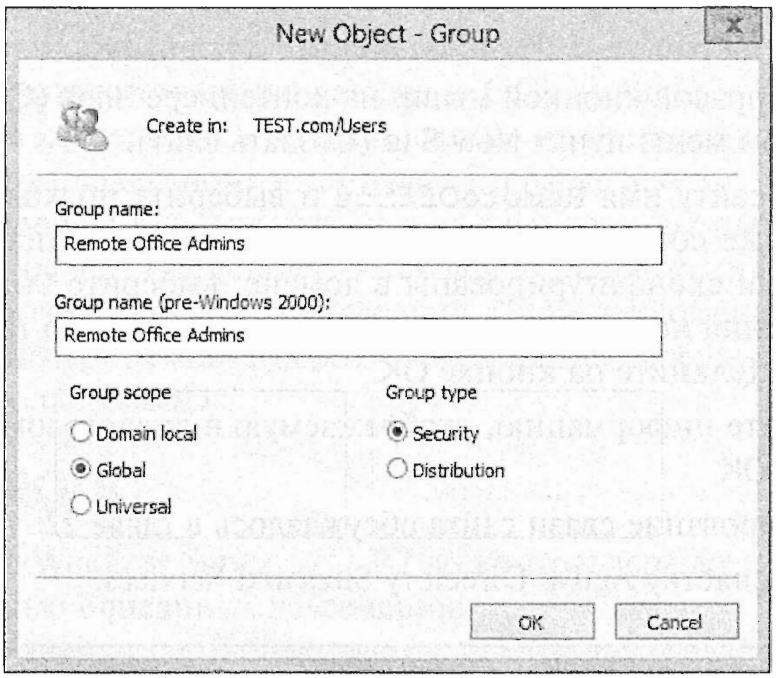


Рис. 23.9. Добавление группы для администрирования RODC

4. Войдите в систему сервера Windows Server 2012 R2, который хотите повысить до контроллера RODC.

   Это не тот сервер, который вы только что использовали для создания сайта `RemoteOffice`. Чтобы продолжить рассмотрение упражнения по повышению данного сервера до RODC, мы пропустим пошаговые инструкции, описывающие добавление роли AD DS на данный сервер. Предполагается, что такая процедура была проделана. Для повышения до контроллера RODC применяются те же самые шаги (раскрытые в главе 7), которые использовались для повышения первого или второго контроллера домена до определенной точки. Вместо этого мы рассмотрим задачу конфигурирования после развертывания, которая инициируется сразу после перезагрузки сервера, вызванной добавлением роли AD DS.

5. После завершения перезагрузки откройте диспетчер серверов и щелкните на кнопке Notifications (Уведомления).

   Вы заметите значок предупреждения, сообщающий о том, что доступна задача повышения этого сервера до контроллера домена, выполняемая после развертывания.

6. Щелкните на ссылке Promote this server to a domain controller (Повысить этот сервер до контроллера домена), чтобы запустить мастер конфигурирования службы доменов Active Directory (Active Directory Domain Services Configuration Wizard).

7. На экране Choose a Deployment Configuration (Выбор конфигурации развертывания) выберите домен, в котором желаете повысить сервер до RODC, и удостоверьтесь в том, что выбран переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен).

Вам также понадобится изменить учетные данные, которые будут применяться при подключении этого сервера к домену.

8. Щелкните на кнопке Change (Изменить) и выберите пользователя, который имеет права повышения сервера до контроллера домена. Окно мастера будет выглядеть примерно так, как показано на рис. 23.10. Щелкните на кнопке Next (Далее). Появится диалоговое окно Windows Security (Безопасность Windows). Поле в этом окне будет автоматически заполнено именем домена, к которому вы присоединились.
9. Введите данные учетной записи, которая имеет разрешение на повышение сервера до контроллера домена внутри домена. Диалоговое окно Windows Security представлено на рис. 23.11. Щелкните на кнопке OK.

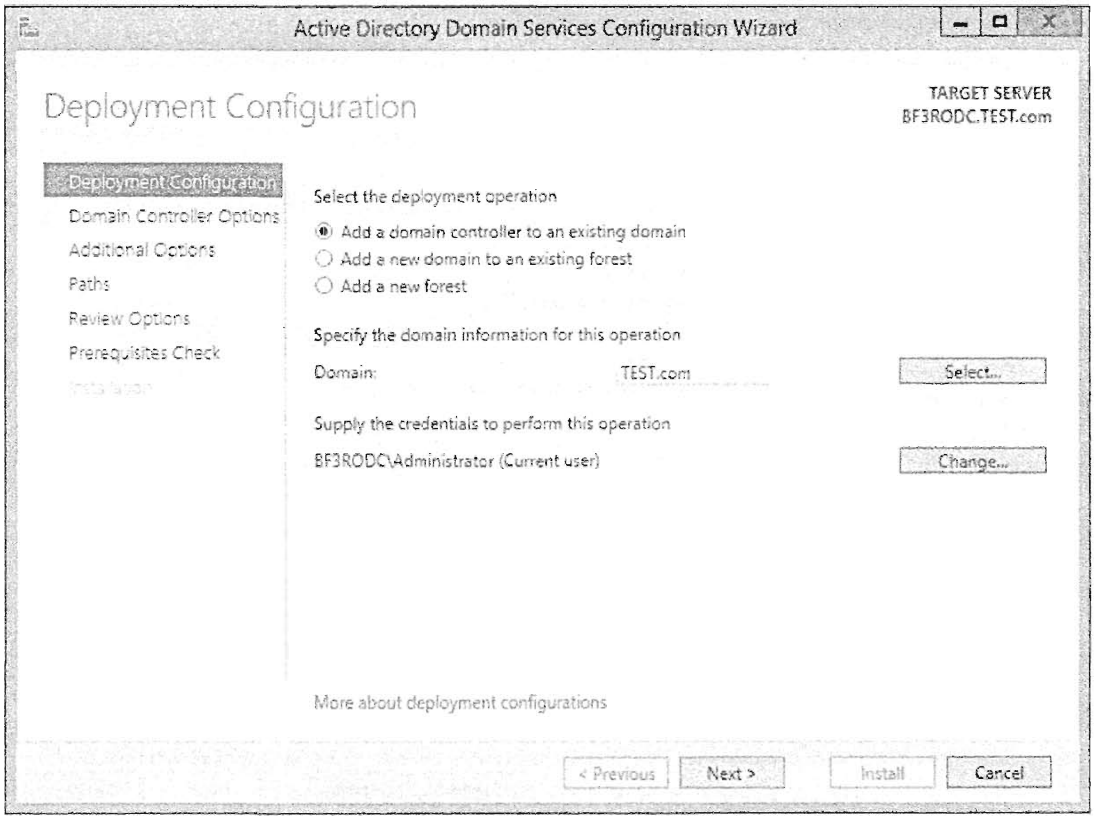


Рис. 23.10. Выбор конфигурации развертывания

Рис. 23.11. Ввод учетных данных для доступа в сеть

10. Появится экран Domain Controller Options (Параметры контроллера домена). Отметьте флажки Domain Name System (DNS) server (Сервер системы доменных имен (DNS)) и Read-only domain controller (RODC) (Контроллер домена только для чтения (RODC)).
11. Снимите отметку с флажка Global Catalog (Глобальный каталог).
12. В раскрывающемся списке Site name (Имя сайта) выберите сайт `RemoteOffice`, созданный ранее в этом упражнении.

    В качестве последнего конфигурационного параметра на этом экране вы должны задать пароль Directory Services Restore Mode (DSRM) (Режим восстановления служб каталогов (DSRM)). Щелкните на кнопке Next. Изображение на вашем экране будет примерно таким, как показано на рис. 23.12.

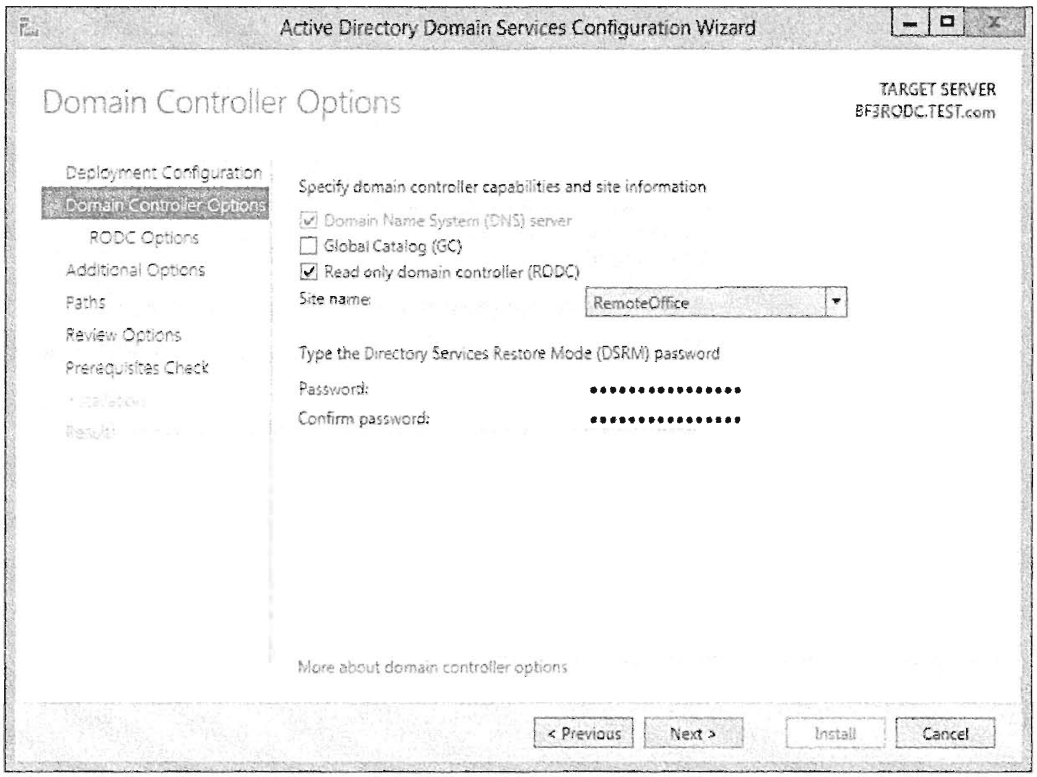


Рис. 23.12. Экран Domain Controller Options

13. Щелкните на кнопке Next.

Глобальный каталог или кеширование членства в универсальных группах

При конфигурировании RODC внутри сайта вам понадобится решить, делать его сервером глобального каталога или включить кеширование членства в универсальных группах. В главе 22 обсуждались детали, которые помогут решить, что именно использовать на производственном сайте, но в испытательной среде вы можете выбрать любой вариант.

Появится экран RODC Options (Параметры RODC), который позволяет выбрать делегированную административную учетную запись или группу для RODC.

14. Выберите и примените группу `Remote Office Admins`, созданную ранее в этом упражнении.

    Обратите внимание на учетные записи, которым разрешено реплицировать пароли, и на учетные записи, которым запрещено реплицировать пароли в RODC. Если вы хотите внести какие-то изменения в эти стандартные политики, просто щелкните на кнопке Add (Добавить), чтобы либо разрешить, либо запретить репликацию паролей. Вспомните, что настройка Deny (Запретить) всегда имеет преимущество, поэтому если учетная запись или группа присутствует в обоих списках, то для нее репликация паролей в RODC выполняться не будет. Изображение на вашем экране будет примерно таким, как показано на рис. 23.13.

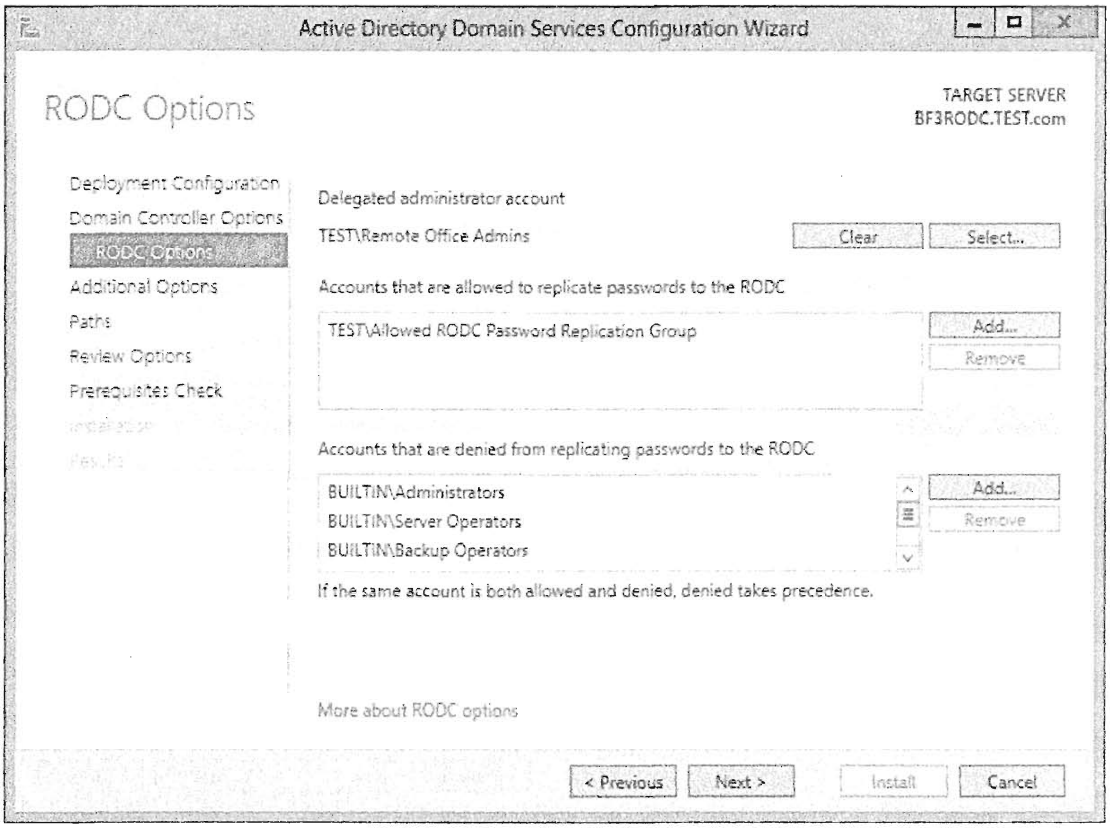


Рис. 23.13. Экран RODC Options

15. Щелкните на кнопке Next.

    Появившийся экран Additional Options (Дополнительные параметры) будет заполнен, предоставляя возможность при желании указать путь для установки с носителя и выбрать конкретный контроллер домена, с которого будет выполняться репликация.

16. Оставьте стандартные параметры и щелкните на кнопке Next.

    На экране Paths (Пути) предусмотрены стандартные местоположения папок для базы данных AD DS, журнальных файлов и `SYSVOL`. Здесь предоставляется возможность выбрать другие местоположения для папок, но в данном упражнении вполне подойдут стандартные местоположения.

17. Оставьте настройки, предложенные по умолчанию, и щелкните на кнопке Next, чтобы продолжить. На экране Review Options (Просмотр параметров) отображаются все конфигурационные параметры, выбранные в мастере конфигурирования служб домена Active Directory.

18. Просмотрите всю информацию на предмет корректности и щелкните на кнопке Next, чтобы начать проверку предварительных условий.

    Мастер запустит проверку необходимых предварительных условий в отношении выбранных параметров конфигурации, чтобы убедиться в их совместимости для завершения надлежащей установки RODC в домене. На рис. 23.14 показан экран Prerequisites Check (Проверка предварительных условий) с успешными результатами проверки. Если любое предварительное условие не удовлетворено, в панели View results (Просмотреть результаты) отобразится сообщение об ошибке, описывающее суть возникшей проблемы. Прежде чем процесс установки может быть продолжен, все проблемы должны быть устранены.

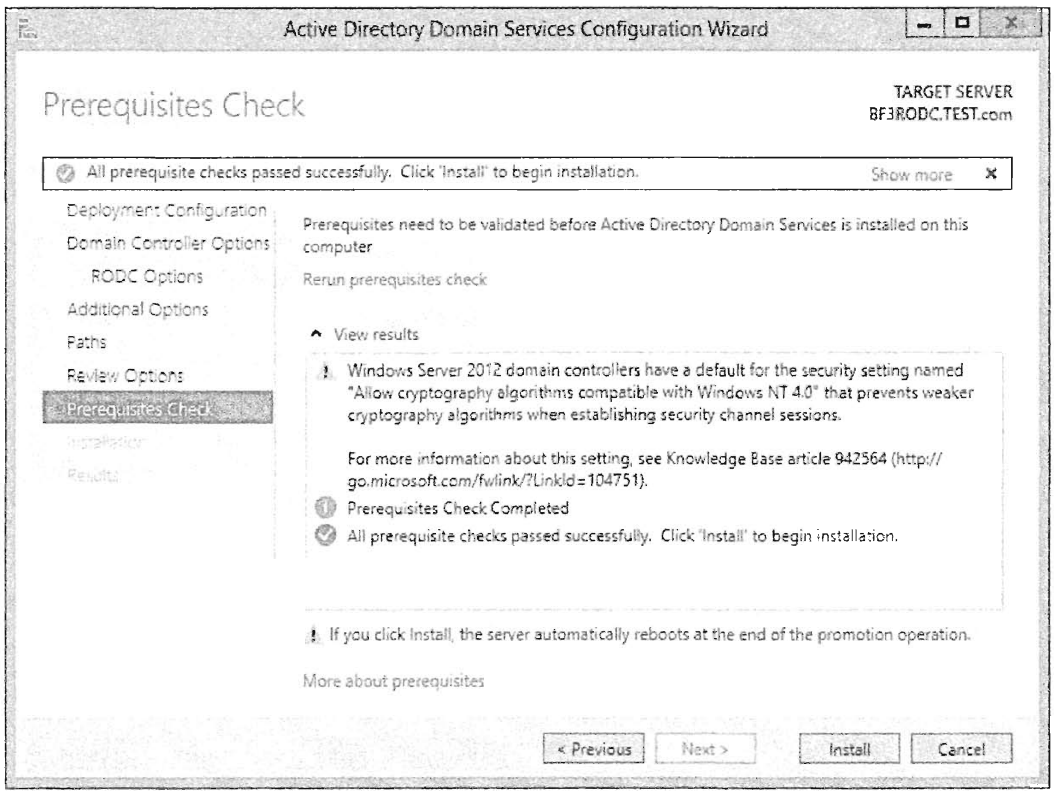


Рис. 23.14. Экран Prerequisites Check

19. Щелкните на кнопке Install (Установить), чтобы создать контроллер RODC.

    Установка может занять несколько минут. После ее успешного завершения появится экран Results (Результаты), подтверждающий выполненную установку.

20. Просмотрите любые сообщения об ошибках или предупреждения, которые могли поступить, и щелкните на кнопке Close (Закрыть), чтобы завершить работу мастера.

Установка RODC на Server Core

Версия Server Core поддерживает установку RODC. В Windows Server 2012 R2 появилась новая возможность, которая заключается в том, что контроллер RODC можно построить с использованием графического пользовательского интерфейса, а затем этот интерфейс можно удалить, преобразовав сервер из полнофункционального экземпляра Windows Server 2012 R2 в Server Core. То же самое применимо к серверам, на которых функционирует исключительно Server Core. Такие машины могут

быть модернизированы до полного графического пользовательского интерфейса, если вам действительно необходима дополнительная функциональность. Если вы решили установить RODC, используя только Server Core, то помните, что в вашем распоряжении будет лишь командная строка, поэтому вам придется запускать задачи конфигурирования AD DS с помощью файла автоматических ответов.

Создать файл автоматических ответов можно двумя способами.

- Выполните задачи конфигурирования AD DS на другом сервере-члене с полной установкой Windows Server 2012 R2. Когда вы доберетесь до итогового экрана, щелкните на кнопке Export Settings (Экспортировать параметры) и следуйте указаниям мастера для сохранения файла. (Этот процесс описан в главе 7.)
- Создайте текстовый файл с помощью редактора Notepad (Блокнот). Вот пример:

```
[DCInstall]
InstallDNS=Yes
ConfirmGc=Yes
CriticalReplicationOnly=No
DisableCancelForDnsInstall=No
Password=P@ssw0rd
RebootOnCompletion=Yes
ReplicaDomainDNSName=DomainDNSName
ReplicaOrNewDomain=ReadOnlyReplica
ReplicationSourceDC=bf1.test.com
SafeModeAdminPassword=P@ssw0rd
SiteName=RemoteOffice
UserDomain=test.com
UserName=Administrator
```

  Создав файл автоматических ответов, вы можете повысить сервер до RODC в окне командной строки Server Core.

Просмотр свойств RODC

После повышения сервера до контроллера RODC можно просматривать и модифицировать свойства этого сервера с помощью оснастки Active Directory Users and Computers. Это допускается делать на самом RODC или на любом другом DC внутри домена.

Посредством следующих шагов можно просмотреть различные свойства контроллера RODC.

1. Войдите в систему контроллера домена от имени учетной записи с административными привилегиями.
2. Откройте оснастку Active Directory Users and Computers, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Users and Computers (Сервис⇨Пользователи и компьютеры Active Directory).
3. Перейдите к контейнеру Domain Controllers (Контроллеры домена) в домене и выберите его. Найдите созданный ранее контроллер RODC. Щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства).

4. В открывшемся диалоговом окне свойств RODC перейдите на вкладку Password Replication Policy (Политика репликации паролей).

   Обратите внимание, что группе `Allowed RODC Password Replication` (Репликация разрешенных паролей RODC) было выдано разрешение на репликацию паролей, тогда как другим группам это запрещено.

5. Щелкните на кнопке Add (Добавить).

6. В открывшемся окне выберите переключатель Allow passwords for the account to replicate to this RODC (Разрешить репликацию паролей для учетной записи на этом RODC).

   Окно будет выглядеть примерно так, как показано на рис. 23.15.

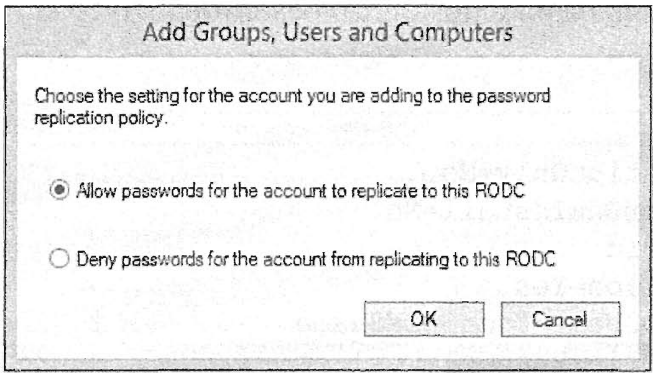


Рис. 23.15. Разрешение репликации паролей для учетной записи

7. Щелкните на кнопке OK.

8. Введите `Remote Office Admins` в текстовом поле. Это имя группы, созданной ранее в этой главе. При желании можете также щелкнуть на кнопке Advanced (Дополнительно), найти нужную группу и добавить ее.

9. После добавления группы щелкните на кнопке OK. Вы увидите, что ваша группа добавилась с настройкой Allow (Разрешить).

   Обратите внимание, что с помощью этого диалогового окна можно добавлять или удалять любые группы. Тем не менее, настройку Allow или Deny (Запретить) можно сконфигурировать только при добавлении группы. Модифицировать эту настройку напрямую невозможно. Чтобы изменить ее, придется удалить группу и затем снова добавить ее, указав другую настройку.

10. Вы должны возвратиться на вкладку Password Replication Policy диалогового окна свойств RODC. Щелкните на кнопке Advanced. Открывшееся диалоговое окно Advanced Password Replication Policy (Расширенная политика репликации паролей) будет подобным приведенному на рис. 23.16, где показана вкладка Policy Usage (Использование политики).

    В этом окне предусмотрено два выбора. Вы можете просмотреть любые учетные записи, которые были кешированы на RODC, а также любые учетные записи, которые применялись для входа в систему RODC.

    Здесь можно идентифицировать любых обычных пользователей, которые входят в систему контроллера RODC и, возможно, нуждаются в добавлении их учетных записей в политику репликации паролей или в группу `Allowed RODC Password Replication`.

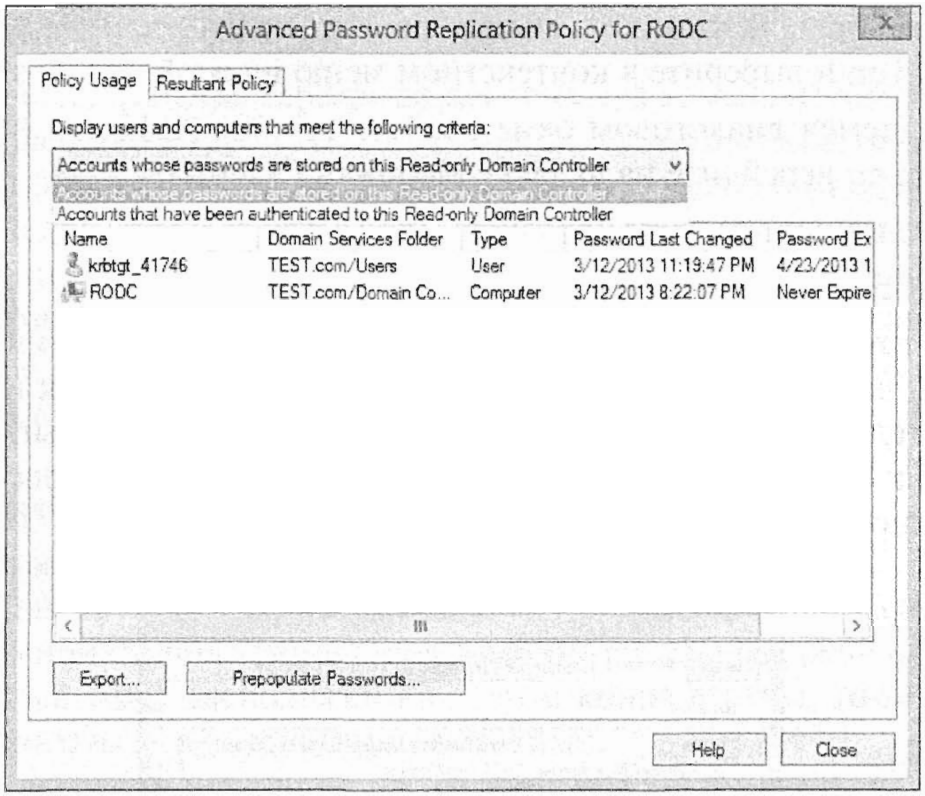


Рис. 23.16. Просмотр вкладки Policy Usage

11. Щелкните на кнопке Prepopulate Passwords (Предварительно заполнить пароли).

    Обратите внимание, что это приводит к активизации инструмента поиска Active Directory. Вы можете идентифицировать любые учетные записи пользователей или компьютеров, чьи пароли хотите реплицировать на RODC до того, как пользователь действительно войдет. Это может пригодиться, если удаленный офис связан с головным офисом посредством ненадежного канала WAN, и необходимо обеспечить кеширование учетных записей пользователей на RODC перед тем, как они впервые войдут в систему.

12. Щелкните на кнопке Cancel (Отмена), чтобы закрыть окно поиска Active Directory, щелкните на кнопке Close (Закрыть) для закрытия диалогового окна Advanced Password Replication Policy и щелкните на кнопке OK, чтобы закрыть диалоговое окно свойств RODC.

Пользователи или группы, добавленные в этом окне, будут иметь возможность репликации или кеширования своих паролей на данном RODC. Тем не менее, если вы хотите, чтобы пользователь или группа получили возможность реплицировать или кешировать свои пароли на любом RODC, то необходимо модифицировать группу `Allowed RODC Password Replication`.

Изменение списка разрешенных паролей

Если вы хотите разрешить пользователям реплицировать или кешировать свои пароли на любом контроллере RODC, а не на каком-то определенном, измените свойства группы `Allowed RODC Password Replication` с помощью перечисленных ниже шагов.

1. Откройте оснастку Active Directory Users and Computers.
2. Перейдите в контейнер Users (Пользователи).

3. Щелкните правой кнопкой мыши на группе `Allowed RODC Password Replication` и выберите в контекстном меню пункт Properties (Свойства).
4. В открывшемся диалоговом окне свойств группы `Allowed RODC Password Replication` перейдите на вкладку Members (Члены).
5. Щелкните на кнопке Add (Добавить).
6. Введите `Remote Office Admins` в текстовом поле.

   Это имя группы, созданной ранее в этой главе. При желании можете также щелкнуть на кнопке Advanced (Дополнительно) и перейти к интересующему пользователю или группе. Диалоговое окно свойств будет выглядеть примерно так, как показано на рис. 23.17. Обратите внимание, что посредством этого окна можно добавлять и удалять группы.

Рис. 23.17. Добавление группы в группу `Allowed RODC Password Replication`

7. Щелкните на кнопке OK, чтобы закрыть диалоговое окно свойств группы `Allowed RODC Password Replication`.

Аналогичную процедуру можно применять для изменения членов группы `Denied RODC Password Replication`. По умолчанию группа `Denied RODC Password Replication` содержит несколько групп. В диалоговом окне ее свойств можно добавлять и удалять группы.

Предупреждение, касающееся безопасности

Хотя удалять члены из группы `Denied RODC Password Replication` допускается, в Microsoft рекомендуют не модифицировать предварительно заполненные группы. Эти группы помогают гарантировать, что пароли для учетных записей с повышенными разрешениями не будут кешироваться на сервере. Если удалить одну из таких групп, а член этой группы войдет в систему контроллера RODC, то вполне вероятно, что его учетные данные сохранятся на этом RODC и станут мишенью для компрометации в случае похищения или взлома RODC.

Поэтапная установка

Обычно для повышения сервера до контроллера домена необходимо, по меньшей мере, иметь членство в группе `Domain Admins`. Однако весьма маловероятно, чтобы члена группы `Domain Admins` отправили работать в удаленный офис. Во многих сценариях это не представляет серьезной проблемы, но могут возникать ситуации, когда члену группы `Domain Admins` довольно трудно физически попасть в удаленный офис. С учетом этого в вашем распоряжении есть несколько вариантов действий.

- **Построить контроллер RODC в головном офисе и доставить его на удаленную площадку.** Такой вариант может оказаться дорогостоящим и затратным в плане времени. Если сервер как раз покупается, было бы дешевле доставить его прямо в удаленный офис и построить RODC на месте.
- **Организовать прибытие кого-то из администраторов домена на удаленную площадку для проведения установки.** Если удаленный офис находится на противоположной стороне улицы, это было бы идеальным решением. Однако если удаленный офис расположен на другом конце страны, то затраты на поездку могут оказаться необоснованно высокими.
- **Повысить сервер дистанционно.** В главе 17 раскрыты многочисленные технологии дистанционного администрирования, которые можно использовать для удаленного администрирования сервера. Тем не менее, поскольку повышение сервера до контроллера домена требует перезагрузки, здравый смысл подсказывает, что без физического присутствия специалиста не обойтись.
- **Выполнить поэтапную установку.** Поэтапная установка проводится в две стадии. Администратор домена предварительно настраивает учетную запись (как описано в разделе "Предварительная настройка учетной записи RODC" далее в этой главе), после чего администратор с ограниченными привилегиями на удаленной площадке сможет повысить сервер.

Использование установочного носителя

База данных Active Directory может быть очень большой, и если полоса пропускания канала WAN недостаточно широка, то повышение сервера до контроллера домена может занять длительное время и препятствовать нормальной работе других пользователей, которые работают с этим же каналом.

Один из способов избежать такой проблемы предусматривает создание установочного носителя, который включает Active Directory. Необходимые данные можно записать на компакт-диск и отправить его на удаленную площадку.

Чтобы создать установочный носитель, понадобится запустить утилиту `ntdsutil` в окне командной строки на контроллере домена с возможностью записи и выполнить в ней команду `ifm` (от installing from media — установка с носителя). Ниже перечислены шаги для создания установочного носителя.

1. Войдите в систему контроллера домена в том же домене, где будет установлен RODC.
2. Откройте окно командной строки с административными разрешениями.
3. Создайте пустой каталог с помощью команды `md c:\ifm`.

   Этому каталогу можно назначить любое желаемое имя и сохранить его на любом другом диске по вашему выбору.

4. Введите в командной строке **ntdsutil** и нажмите <Enter>. Появится приглашение на ввод команд утилиты ntdsutil.
5. Введите команду **Activate instance ntds** и нажмите <Enter>.

   Утилита ntdsutil подключится к экземпляру Active Directory на контроллере домена и выведет сообщение Active instance set to ntds (Активный экземпляр установлен в ntds).
6. Введите команду **ifm** и нажмите <Enter>. Появится приглашение ifm.
7. Введите команду **Create rodc c:\ifm** и нажмите <Enter>.

Внутри папки ifm будет создана папка по имени Active Directory с единственным файлом ntds.dit. Вы можете скопировать этот файл на установочный носитель, такой как компакт-диск, и доставить носитель в удаленный офис.

После создания установочного носителя вы можете установить его на удаленном сервере с помощью мастера конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard). На экране Paths (Пути) этого мастера выберите переключатель Install from media (Установить с носителя) и перейдите в нужную папку.

Предварительная настройка учетной записи RODC

Предварительная настройка учетной записи RODC — это всего лишь другой способ назвать процедуру создания учетной записи для RODC перед его повышением. Предварительная настройка учетной записи RODC требует членства в группе Domain Admins.

Для предварительной настройки учетной записи RODC выполните описанные ниже действия.

1. Откройте оснастку Active Directory Users and Computers, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Users and Computers (Сервис⇨Пользователи и компьютеры Active Directory).
2. Перейдите к контейнеру Domain Controllers (Контроллеры домена). Щелкните на ней правой кнопкой мыши и выберите в контекстном меню пункт Pre-create Read-only Domain Controller account (Предварительно создать учетную запись контроллера домена только для чтения), как показано на рис. 23.18.

   Запустится мастер установки служб домена Active Directory (Active Directory Domain Services Installation Wizard).
3. Ознакомьтесь с информацией на экране приветствия и щелкните на кнопке Next (Далее).
4. На экране Network Credentials (Учетные данные для доступа в сеть) щелкните на кнопке Alternate Credentials (Изменить учетные данные) и введите данные учетной записи в группе Domain Admins, если текущих учетных данных для входа недостаточно. Щелкните на кнопке Next.
5. На экране Specify the Computer Name (Указание имени компьютера) введите имя контроллера RODC. Окно мастера будет выглядеть примерно так, как показано на рис. 23.19. Щелкните на кнопке Next.

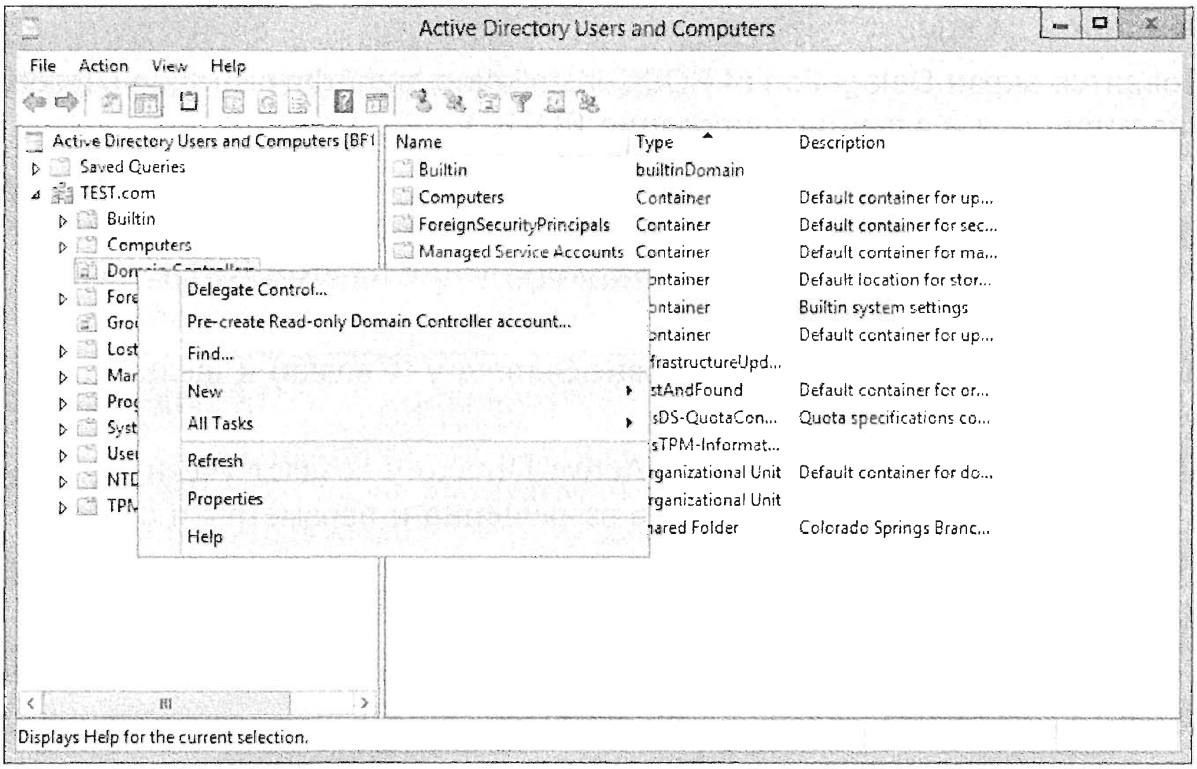


Рис. 23.18. Предварительное создание учетной записи RODC в оснастке Active Directory Users and Computers

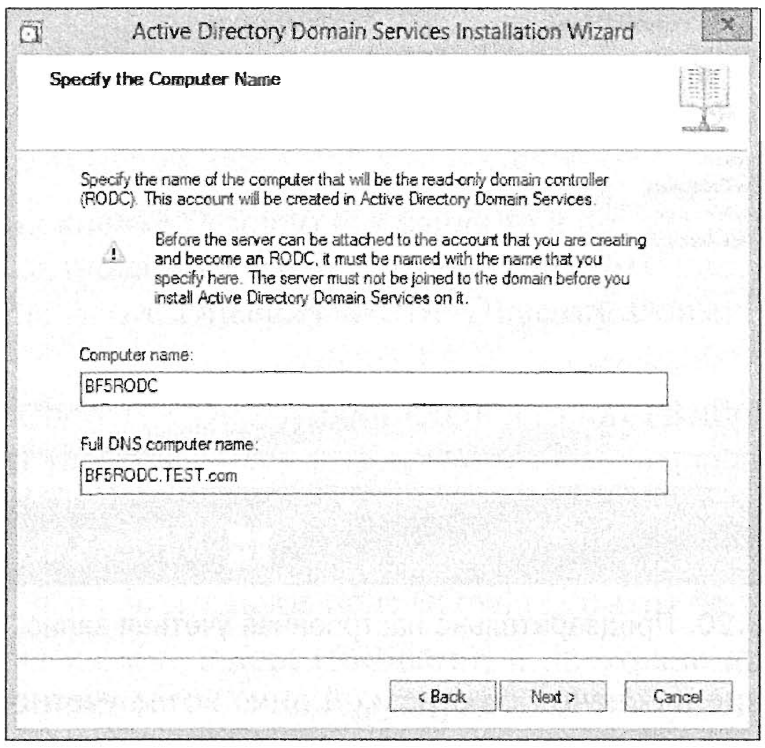


Рис. 23.19. Указание имени контроллера RODC

6. На экране Select a Site (Выбор сайта) выберите сайт, на котором будет размещаться RODC. Щелкните на кнопке Next.

   Появится экран Additional Domain Controller Options (Дополнительные параметры контроллера домена) с отмеченными флажками DNS Server (DNS-сервер), Global Catalog (Глобальный каталог) и Read-only Domain Controller (RODC) (Контроллер домена только для чтения (RODC)). При желании можете снять отметку с флажка DNS Server или Global Catalog, однако отмеченный флажок Read-only Domain Controller (RODC) для выбора не доступен.

7. Щелкните на кнопке Next.

   Появится экран Delegation of RODC Installation and Administration (Делегирование установки и администрирования RODC).

8. Введите имя группы или пользователя, который будет повышать сервер до контроллера RODC на удаленной площадке. Указанная учетная запись будет иметь локальные административные разрешения на этом RODC. Щелкните на кнопке Next.

9. Просмотрите информацию на экране Summary (Сводка) и щелкните на кнопке Next.

   Мастер установки служб домена Active Directory создаст учетную запись для RODC, назначит соответствующие разрешения и параметры и сообщит об успешном выполнении работ.

10. Щелкните на кнопке Finish (Готово).

    Оснастка Active Directory Users and Computers отобразит учетную запись этого RODC в контейнере Domain Controllers (рис. 23.20).

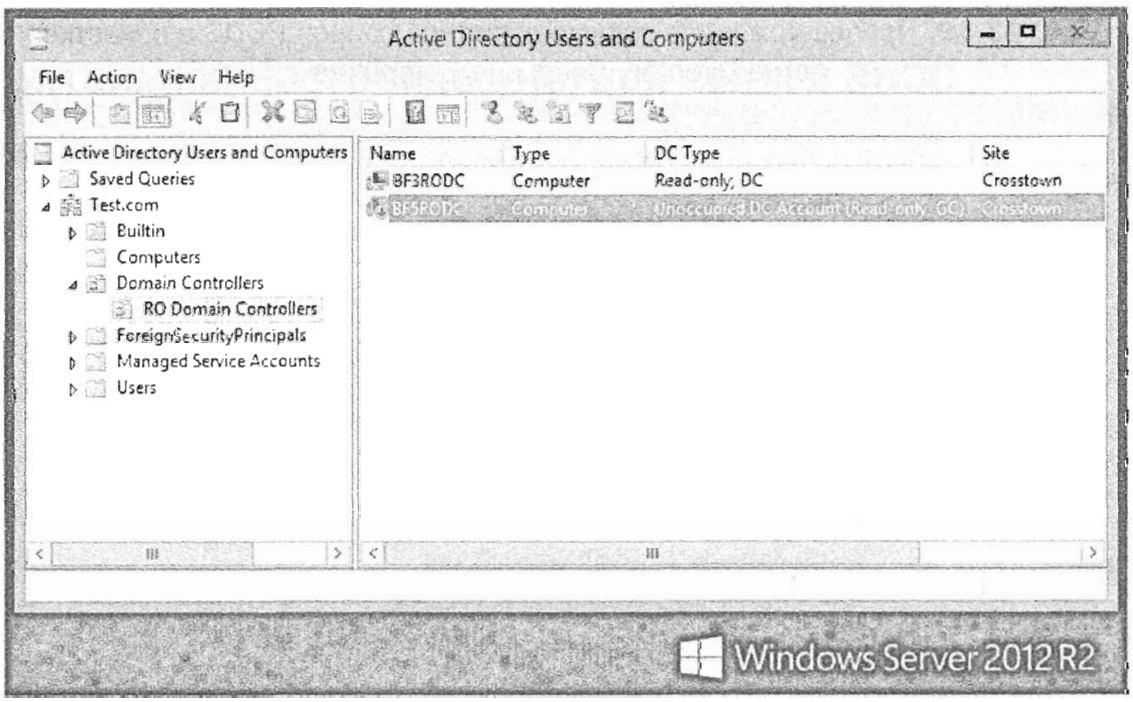


Рис. 23.20. Предварительно настроенная учетная запись RODC

Обратите внимание на значок со стрелкой вниз возле учетной записи `BF5RODC`; он указывает на то, что эта учетная запись еще не включена. Она включится, когда будет запущен мастер конфигурирования служб домена Active Directory для повышения сервера до контроллера RODC. Кроме того, в столбце DC Type (Тип контроллера домена) для этой учетной записи отображается Unoccupied DC Account (Read-only, GC) (Незанятая учетная запись контроллера домена (только для чтения, глобальный каталог)); это указывает на то, что она является предварительно настроенной учетной записью.

Имея предварительно настроенную учетную запись RODC, локальный администратор на удаленной площадке теперь может запустить мастер конфигурирования служб домена Active Directory, чтобы выполнить повышение до RODC.

Вторая стадия установки предварительно настроенного контроллера RODC

С помощью описанных ниже шагов локальный администратор может завершить установку предварительно настроенного контроллера RODC. Имя компьютера, на котором запускается утилита `DCPromo`, должно совпадать с именем, указанным для предварительно настроенной учетной записи.

Не присоединяйтесь к домену

Предварительно настроенная учетная запись создает в контейнере Domain Controllers действительную учетную запись компьютера. Поскольку любой компьютер может иметь только одну учетную запись, предварительно настроенный RODC не может быть членом домена до его повышения. Вместо этого он начинает как член рабочей группы и добавляется в домен в ходе процесса конфигурирования AD DS.

---

1. Войдите в систему сервера под учетной записью локального администратора.
2. Если роль AD DS еще не установлена, добавьте ее и перезагрузите систему сервера.
3. После завершения перезагрузки запустите диспетчер серверов и щелкните на кнопке Notifications (Уведомления).

   Вы заметите значок предупреждения, сообщающий о доступности задачи повышения этого сервера до контроллера домена, выполняемой после развертывания.
4. Щелкните на кнопке Promote this server to a domain controller (Повысить этот сервер до контроллера домена), чтобы запустить мастер конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard).
5. На экране Choose a Deployment Configuration (Выбор конфигурации развертывания) удостоверьтесь в том, что выбран переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен).

   Вы увидите, что обязательное поле Domain (Домен) не заполнено.
6. Щелкните на кнопке Select (Выбрать), и на экране появится окно Windows Security (Безопасность Windows), запрашивающее учетные данные для операции развертывания.
7. Введите имя и пароль пользователя, находящегося в группе, которой были делегированы разрешения на завершение установки, и для продолжения щелкните на кнопке Next (Далее).

   На экране Domain Controller Options отобразится уведомление о том, что была создана предварительно настроенная учетная запись RODC, которая соответствует имени хоста. По умолчанию в мастере для этого выбирается переключатель Use existing RODC account (Использовать существующую учетную запись RODC), как показано на рис. 23.21.

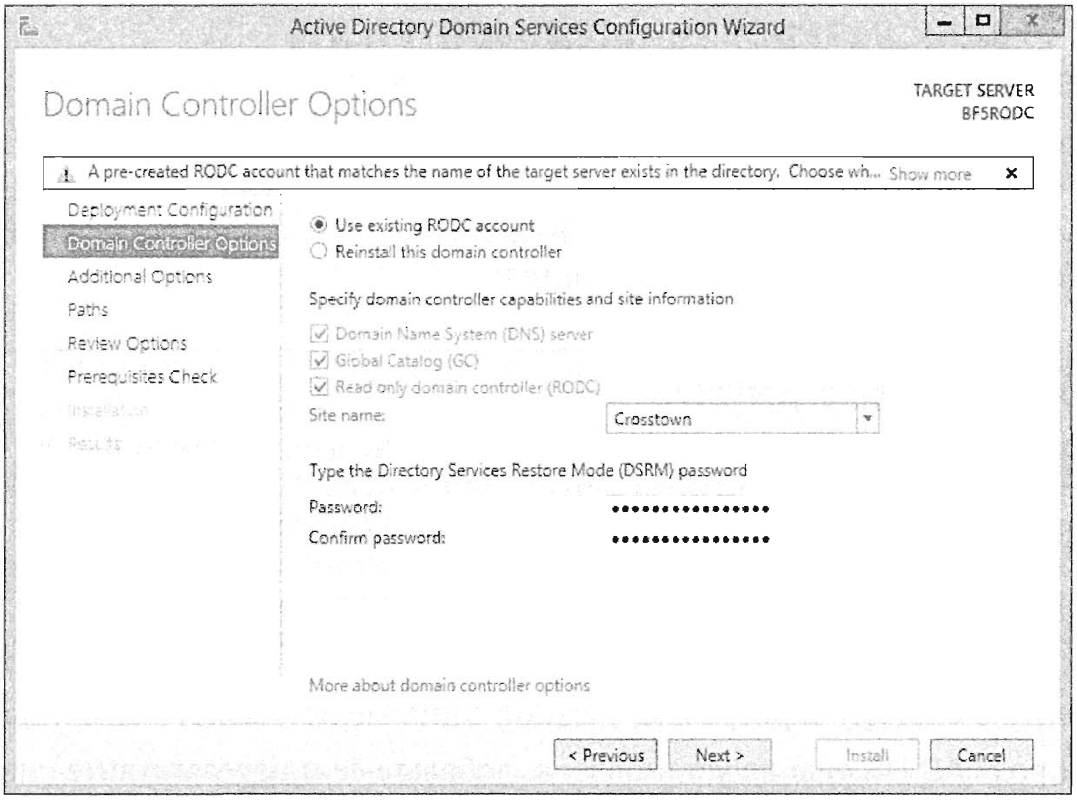


Рис. 23.21. Мастер конфигурирования служб домена Active Directory обнаружил предварительно настроенный RODC

8. Оставьте без изменений параметры, выбранные по умолчанию, и щелкните на кнопке Next, чтобы продолжить.
9. Продолжайте следовать инструкциям мастера, как было указано в предыдущих упражнениях, выбирая необходимые параметры на каждом его экране.

Повышение сервера до контроллера RODC может занять несколько минут и по завершении требует перезагрузки. Отметив флажок Reboot on completion (По завершении перезагрузиться), вы разрешаете автоматическое выполнение перезагрузки. После успешного завершения установки сервер будет повышен до контроллера RODC, добавлен в домен и готов к использованию.

Служба DNS на контроллере RODC

Настоятельно рекомендуется установить на контроллере RODC службу DNS. В пошаговых процедурах, описанных в этой главе, служба DNS выбиралась каждый раз. Она сопровождается совсем небольшими накладными расходами, но обеспечивает значительные выгоды. Если в офисе филиала отсутствует сервер DNS, но есть контроллер домена, то для обнаружения этого контроллера домена пользователям по-прежнему придется передавать запросы к DNS по каналу WAN. Кроме того, в удаленном офисе все равно потребуется обычное преобразование имен DNS.

Взгляните на рис. 23.22, где представлен процесс обычного входа в систему. Когда пользователь входит в систему, выполняются следующие действия.

1. Пользователь вводит свои учетные данные и активизируется служба `netlogon`.
2. Процесс `netlogon` отправляет службе DNS запрос для нахождения имени и IP-адреса контроллера домена, находящегося на той же площадке, что и пользователь. Должны быть извлечены записи SRV и хоста этого сервера.

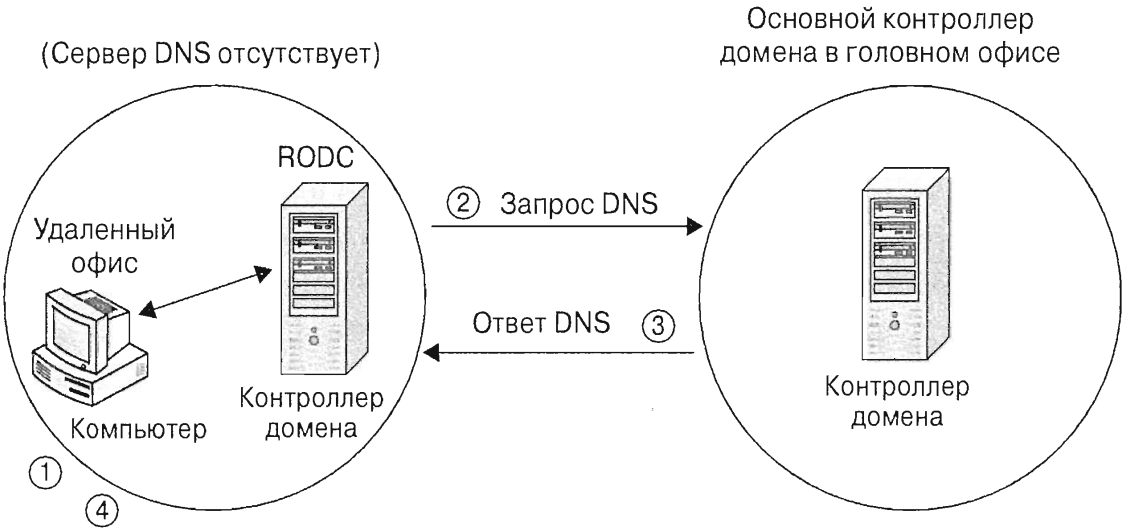


Рис. 23.22. DNS и процесс входа в систему

3. Служба DNS отправляет ответ.
4. Служба `netlogon` передает учетные данные пользователя контроллеру RODC, размещенному на площадке.

За счет конфигурирования службы DNS на контроллере RODC можно избежать передачи запросов к DNS по каналу WAN. Служба `netlogon` опрашивает службу DNS на RODC и затем передает учетные данные контроллеру RODC.

Сервер DNS, интегрированный с Active Directory

Если другие серверы DNS сконфигурированы как интегрированные с Active Directory (Active Directory integrated — ADI), то контроллер RODC будет также настроен как зона, интегрированная с Active Directory. Сервер DNS, интегрированный с Active Directory, реплицирует данные зоны посредством репликации Active Directory и его наличие в доменах Windows настоятельно рекомендуется.

Когда сайты сконфигурированы надлежащим образом, репликация Active Directory значительно оптимизируется.

- Весь трафик репликации сжимается до примерно 10–15% от его первоначального объема.
- Можно запланировать график репликации, чтобы она происходила в нерабочее время или в часы, в которые отсутствует пиковая нагрузка.

Сервер DNS только для чтения

Когда служба DNS добавляется на контроллер RODC, получается DNS-сервер только для чтения. В действительности это новый тип зоны, впервые появившийся в Windows Server 2008 и известный как *основная зона только для чтения*.

Обычно запись SOA (Start of Authority — начало зоны) для DNS-сервера ADI перечисляет себя как основной сервер. Другими словами, обновления могут происходить на этом сервере. Однако DNS-сервер ADI на контроллере RODC будет содержать копию записи SOA из DNS-сервера с возможностью записи.

Традиционная система DNS имеет дело с единственным DNS-сервером, хранящим данные основной зоны. Затем можно добавить несколько DNS-серверов, ко-

торые хранят дополнительные зоны. Эти дополнительные DNS-серверы допускают только чтение и получают свои обновления из основного DNS-сервера.

DNS-сервер ADI только для чтения, установленный на контроллере RODC, действует подобно конфигурации основного и дополнительных DNS-серверов. Обновления не могут происходить на контроллере RODC, как они не могут происходить на дополнительном DNS-сервере. Однако самое большое отличие заключается в том, что у вас нет необходимости управлять переносами зон DNS, что пришлось бы делать в случае традиционных DNS-серверов. Переносы зон управляется посредством репликации Active Directory.

Резюме

Подготовьте лес и домен для контроллеров RODC. В Windows Server 2012 R2 контроллеры RODC являются великолепным инфраструктурным активом, и их невозможно добавить до тех пор, пока не будут подготовлены лес и домен. Эта подготовка модифицирует используемую схему и разрешения.

Контрольный вопрос. Укажите команду, которую нужно выполнить, чтобы подготовить лес к поддержке контроллеров RODC.

Подготовьте домен. Прежде чем можно будет добавлять контроллеры RODC, в дополнение к подготовке леса вы должны также подготовить домен.

Контрольный вопрос. Укажите две команды, которые необходимо выполнить, чтобы подготовить домен к поддержке контроллеров RODC.

Разрешите кеширование паролей на любом RODC. Контроллер RODC может кешировать пароли для пользователей на основе того, каким образом он сконфигурирован. Когда пароль пользователя кешируется на RODC, процессу аутентификации нет необходимости обращаться к каналу WAN, поэтому он протекает быстрее. Тем не менее, кешированные пароли могут быть похищены злоумышленниками, поэтому привилегированные учетные записи не должны кешироваться на контроллере RODC.

Контрольный вопрос. Что понадобится модифицировать, чтобы разрешить кеширование паролей для пользователей на любом RODC в домене?

- группу `Allowed RODC Password Replication`;
- группу `Denied RODC Password Replication`;
- политику репликации паролей.

Разрешите кеширование паролей на отдельно взятом RODC. Среду можно сконфигурировать так, чтобы пароли членов определенной группы реплицировались и кешировались на любом RODC в соответствующем домене. Среду также можно сконфигурировать для репликации или кеширования этих паролей только на одиночном RODC.

Контрольный вопрос. Что понадобится модифицировать, чтобы разрешить кеширование паролей для пользователей на отдельном RODC в домене?

- группу `Allowed RODC Password Replication`;
- группу `Denied RODC Password Replication`;
- политику репликации паролей.

Глава 24

Создание более крупных сред Active Directory: за пределами одного домена

До сих пор в этой книге мы имели дело с простейшими реализациями Active Directory (AD) одного домена. Несмотря на то что Active Directory может поддерживать крупные предприятия с единственным доменом, IT-отделы в силу разных причин сталкиваются с необходимостью администрирования многих доменов. Иногда это является частью первоначального плана, однако временами этим приходится заниматься из-за реструктуризации компании или поглощения ею других компаний.

Администраторы должны понимать последствия использования в организации нескольких доменов. Они должны знать точки принятия решений, которые заставляют организацию рассматривать возможность перехода к применению нескольких доменов. Как правило, любая жизнеспособная организация проявляет тенденцию к росту. Всегда заранее планируйте время на построение масштабируемого инфраструктурного фундамента и будьте готовы к расширению и оценке возможных ограничений ресурсов вашей среды в будущем.

В этой главе вы изучите следующие темы:

- объяснение фундаментальных концепций Active Directory;
- выбор между использованием в проектном решении Active Directory одного домена, нескольких доменов или нескольких лесов;
- добавление доменов в среду Active Directory;
- управление функциональными уровнями, доверительными отношениями, ролями FSMO и глобальным каталогом.

Основы проектных решений с несколькими доменами

Прежде чем мы рассмотрим вопрос добавления в среду Active Directory нескольких доменов, вам необходимо уяснить ряд важных концепций. В частности, вы должны понимать логические и физические компоненты Active Directory, что поможет планировать проектное решение Active Directory. Знание преимуществ и отличий между использованием единственного домена, нескольких доменов в единственном лесу и множества лесов способствует принятию решения о подходящей реализации, которая удовлетворит потребности вашей организации.

Процессы, происходящие "за кулисами", такие как репликация с несколькими хозяевами, протокол аутентификации Kerberos и программные ограничения Active Directory, в дальнейшем определяют структуру реализации Active Directory. Необходимо принимать во внимание достоинства и недостатки каждого варианта.

Домены

Обычно домен AD представляют как границу безопасности для пользователей и компьютеров в деле совместного использования, внутри которой для распространения информации об этих пользователях и компьютерах применяется репликация с несколькими хозяевами. Это верно, но не особенно проясняет суть, так что давайте посмотрим, что имеется в виду.

Граница безопасности

Каждая сеть, в которой реализована хотя бы какая-то система безопасности, должна хранить список со сведениями о пользователях — именами, паролями и другой информацией о людях, которым разрешено пользоваться системой. Вам также известно, что при наличии более чем одной машины возникает проблема: как обеспечить совместное использование упомянутым списком всеми машинами в компании? Вспомните, что это делается путем установки небольшого количества серверов, называемых *контроллерами домена*, с базой данных пользователей, которая называется `NTDS.DIT`. Имя для этого важного файла базы данных было выбрано согласно аббревиатуре от "new technology directory services" (службы каталогов новой технологии), а расширение — в соответствие с аббревиатурой от "directory information tree" (дерево информации каталога), что является форматом, закрепленным отраслевыми стандартами.

Серверы-члены и рабочие станции по-прежнему имеют свои списки учетных записей *локальных* пользователей, поддерживаемые в базах данных управления учетными данными безопасности (Security Account Management — SAM), но в большинстве случаев локальные учетные записи применяются не особенно широко. Вместо этого вы конфигурируете рабочие станции и серверы-члены на *доверие* списку пользователей на контроллерах домена. Когда кто-то пытается усесться за рабочей станцией и утверждает, что является членом вашего домена, эта рабочая станция принимает имя и пароль, введенные этим пользователем, и передает их контроллеру домена (DC), спрашивая, присутствуют ли такое имя и пароль в базе данных домена. Если DC отвечает, что комбинация имени пользователя и пароля действительно допустима, рабочая станция *доверяет* тому, что сообщает DC.

Домен определяет границу безопасности. Домен предоставляет границу для администрирования учетных записей и доступа к ресурсам. Членам группы `Domain Admins` выдается полный доступ к объектам домена. Домен также управляет применением объектов GPO к своим пользователям и компьютерам.

В ранних версиях Windows Server домен также служил границей для политик паролей и параметров блокировки учетных записей. Замечательной возможностью Windows Server 2012 R2 являются детализированные политики паролей. Они позволяют применять разные политики паролей в пределах одного домена. Хотя Windows Server 2012 R2 предоставляет эту возможность, существующие реализации Active Directory могут включать несколько доменов, что обеспечивало применение отличающихся политик паролей в средах, предшествующих Windows Server 2008.

При наличии одного домена доступ к ресурсам управляется посредством групп и учетных записей домена. Если же доменов несколько, то потребуется доверительное отношение, которое позволяет распознавать пользователей и группы другого домена компьютерами данного домена. Доверительное отношение похоже на калитку в заборе, через которую пользователи могут входить и выходить.

Чтобы спроектировать безопасную реализацию Active Directory, вы должны хорошо понимать границы безопасности домена, леса и физических контроллеров домена.

Репликация с несколькими хозяевами

Вторая часть определения домена — *репликация* — относится к процессу, который гарантирует, что каждая копия базы данных домена будет совпадать с любой другой ее копией. Другими словами, если вы находитесь в офисе Топики (штат Канзас) и создали учетную запись пользователя, то поначалу эта новая запись — учетная запись пользователя — существует только на контроллере домена Active Directory в Топике. Одна из задач механизма базы данных Active Directory заключается в том, чтобы как можно быстрее передать эту новую информацию на другие контроллеры домена, т.е. выполнить репликацию. Часть определения домена, касающаяся *нескольких хозяев*, происходит из того факта, что изменение можно внести в базу данных AD из любого контроллера домена.

Когда вы создали свой первый домен с помощью мастера конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard), была создана база данных Active Directory, которая должна реплицироваться с помощью процесса репликации с несколькими хозяевами. Структура этой базы данных включает три основных части, или раздела.

- **Раздел домена.** Содержит информацию о пользователях, группах и компьютерах, которые ассоциированы с доступными ресурсами.
- **Раздел конфигурации.** Содержит параметры репликации и другие конфигурационные настройки среды Active Directory наподобие информации Exchange Server.
- **Раздел схемы.** Содержит определение объектов. Оно сообщает Active Directory о том, как формировать учетную запись пользователя или группу, и указывает, какие данные могут быть назначены пользователю.

Не единственная граница безопасности

Домен предоставляет границу безопасности для доступа и управления ресурсами. Тем не менее, это не *единственная* граница безопасности. Домен не является непроницаемой стеной, за которой информация полностью защищена. Сведения о домене совместно используются другими контроллерами домена внутри леса Active Directory, а группа доменов имеет встроенное отношение между своими членами. Таким образом, еще одной границей безопасности является лес, который защищает информацию, совместно используемую контроллерами домена.

Информация о пользователях и группах домена может быть обнаружена на серверах глобального каталога, которые могут находиться в других доменах. Контроллеры домена леса реплицируют дополнительную информацию, такую как конфигурационные данные Active Directory.

Физической границей безопасности Active Directory являются контроллеры домена. Контроллер домена содержит базу данных на своих физических дисках и реплицирует изменения на другие контроллеры домена.

Если любая из упомянутых границ безопасности компрометируется, вся среда Active Directory оказывается под угрозой и зависит от прихотей злоумышленника, которого обычно изображают в виде черного силуэта в шерстяной шапке и длинном пальто.

Когда разработчики в Microsoft начали добросовестно относиться к безопасности, они обнаружили, насколько большой ущерб среде Active Directory способен нанести такой злоумышленник. Получив административные привилегии, он мог бы изменить конфигурацию в другом домене, и эти изменения реплицировались бы на остальные контроллеры домена. Что касается физического контроллера домена, злоумышленник мог бы расшифровать пароли для доступа. Это стало главным стимулом к добавлению таких возможностей Windows Server, как контроллеры домена только для чтения и политик репликации паролей для кеширования паролей. Если бы злоумышленнику удалось запустить свои руки в контроллер домена в незащищенной области, то, по крайней мере, этот контроллер домена не смог бы реплицировать изменения на другие контроллеры домена и на нем хранился бы только ограниченный набор паролей.

Раздел домена является самой крупной порцией базы данных и реплицируется только на контроллеры домена внутри того же самого домена. Кроме того, он представляет собой растущую порцию базы данных, т.к. организации будут намного чаще создавать дополнительные объекты пользователей и компьютеров, а также другие объекты домена, чем добавлять данные в разделы конфигурации и схемы.

Если вы хотите ограничить объем репликации по каналам глобальной сети (WAN), вам следует подумать о разделении пользователей и групп, находящихся в разных расположениях, путем определения для каждого расположения отдельного домена.

Именно так в основном структурирован домен. Он представляет собой границу безопасности, администрирующую доступ к ресурсам и аутентифицирующую пользователей. Домен также является единицей репликации в том, что его информация совместно используется контроллерами домена внутри одного и того же домена. А теперь давайте посмотрим, какие есть возможности по расширению Active Directory на большее число доменов.

Леса

Рассматривая возможность создания дополнительных доменов в Active Directory, мы возвращаемся обратно к природе, применяя такие хорошо знакомые понятия, как *леса* и *деревья*. И хотя невозможно получить лес, не имея дерева, мы начнем с концепции леса.

После создания первого домена вы можете создать дополнительные контроллеры домена для того же самого домена или создать контроллеры домена для новых доменов, связанных с первым доменом. Когда дополнительные домены создаются относительно первого домена, как вы поступите позже в разделе "Создание нескольких доменов", не вся информация базы данных Active Directory реплицируется на их контроллеры домена. Раздел домена не реплицируется на контроллеры новых доменов. Разделы конфигурации и схемы будут реплицироваться на каждый контроллер домена в лесе. Формулировка "в лесе" означает группу доменов, которые реплицируют разделы конфигурации и схемы.

Кроме того, принадлежность к лесу указывает на то, что домены связаны друг с другом. Такой связью является доверительное отношение, построенное между доменами, когда в лес добавляется несколько доменов. Между новым доменом и другим доменом в лесе автоматически создается не поддающееся конфигурированию двунаправленное транзитивное доверительное отношение. Это означает, что пользователи и группы одного домена могут обращаться к ресурсам, таким как файлы и принтеры, в другом домене, и наоборот. В действительности пользователи в любом домене могли бы иметь доступ к ресурсам в любом другом домене внутри леса.

Возвратимся обратно к природе. Когда вы создали первый домен на первом контроллере домена, то тем самым получили лес, состоящий из одного домена и одного дерева. Важно понимать, что построение домена с нуля, как это делалось в главе 7, приведет к созданию автономного чистого леса, который ни с чем другим не взаимодействует. Примерно то же самое мы наблюдаем в природе. Лес представляет собой совокупность деревьев. Он является своего рода границей безопасности для населяющей его живности, которая может укрыться в нем и чувствовать себя в безопасности. Лесные обитатели могут спокойно заниматься поисками пропитания под сенью деревьев, ветви и корни которых тесно переплетены между собой. Они вовсе не стремятся перебраться в другие леса. ("Не выходи на луг, Бэмби. Это опасно".) Таким образом, отдельные леса не обмениваются информацией друг с другом, если только вручную не сконфигурировать такую возможность, а пользователи не осмеливаются заходить в другие леса по собственному желанию. Кроме того, вы можете только добавлять дополнительные деревья в лес. Корни деревьев не распространяются на другие леса. Вы не можете пересадить один лес вплотную к другому лесу в надежде объединить их. Аналогия "обратно к природе" соблюдается в полной мере.

Границы безопасности, создаваемые доменами и лесами, помогают управлять доступом и безопасностью объектов внутри среды. Каждый домен и лес действуют как пост безопасности для объектов, которые желают перемещаться между сущностями и делиться информацией. Такие проверки и сопоставления помогают поддерживать безопасность среды. Лес играет роль защитного зонтика для находящихся в нем объектов. Если вы хотите блокировать доступ к части своей сети, вам следует рассмотреть возможность применения отдельного леса, чтобы предотвратить совместное использование ресурсов с другими частями сети.

Деревья

При создании нового домена в лесе Active Directory ему должно быть назначено имя. В общем случае *дерево* — это группа доменов в лесе с одинаковым пространством имен.

Корень леса

Возможно, вы решили, что мы закончили с аналогией "обратно к природе". Тем не менее, нам придется ее модифицировать. Корень дерева — это новое пространство имен для группы доменов, такое как Test.com. Корневым доменом леса доменов Active Directory является первый домен, который был установлен в этом лесе лесу. Временами на него ссылаются как на *корень леса*. Обычно его изображают на вершине дерева.

Например, первый домен или домен корня леса был назван Test.com. Следующему дочернему домену можно назначить имя Ecoast.Test.com. Таким образом, дочерний домен входит в то же самое пространство имен Test.com и является частью того же дерева. Если вы создадите другой домен по имени Consolidated.com, он не будет иметь такое же пространство имен. Ecoast.Test.com считается дочерним доменом Test.com, а Consolidated.com является новым деревом в том же лесе. Вдобавок Consolidated.com представляет собой корень дерева, несмотря на то, что у него нет дочерних доменов.

В лесе Active Directory, имеющем лишь пару доменов, это не имеет большого значения, особенно когда речь идет о доступе к ресурсам через доверительные отношения. Разница несущественна. При наличии нескольких доменов способ их именования влияет на доверительные отношения. Это обусловлено особенностями функционирования протокола аутентификации Kerberos.

Протокол Kerberos и доверительные отношения

Аутентификация Kerberos подобна тому, как знакомятся в средней школе. Опытные парни понимают, что для знакомства простых подмигиваний и улыбок далеко не достаточно; они подключают круг своих знакомств. Они хотят заставить кого-то за них поручиться.

Допустим, вы присмотрели в школьном коридоре симпатичную девчонку, с которой еще не знакомы. Вы не можете прямо с ходу заговорить с ней; к тому же, существует "устройство защиты" под названием Ее Мама, которая начнет ужасно нервничать и волноваться, если вы попытаетесь позвонить к ним в дом. Однако ваше собственное "устройство защиты", которое называется Ваша Мама, знакомо с "устройством защиты" по имени Ее Мама; более того, они — хорошие подруги. Поэтому вы просите свою маму поговорить с ее мамой, чтобы положить начало общению между пользователем (вами) и ресурсом (симпатичной девчонкой).

Когда ваша мама не является подругой "устройства защиты" по имени Ее Мама, выясняется, что она знакома с одной женщиной, которая является хорошей подругой Ее Мамы. Эта женщина является "корнем леса" в данном квартале — она дружит со всеми. Таким образом, ваша мама вступает в переговоры с этой женщиной, а та разговаривает с Ее Мамой. Пусть и окольным путем, но задача решена!

С логической точки зрения доверительные отношения между доменами представляют собой либо отношения "родительский–дочерний", либо отношения "корень леса–корень дерева". Как упоминалось ранее, Ecoast.Test.com является дочерним доменом для Test.com, поэтому они связаны отношением "родительский–дочерний". Consolidated.com имеет отношение "корень леса–корень дерева". Доверительные отношения внутри леса показаны на рис. 24.1.

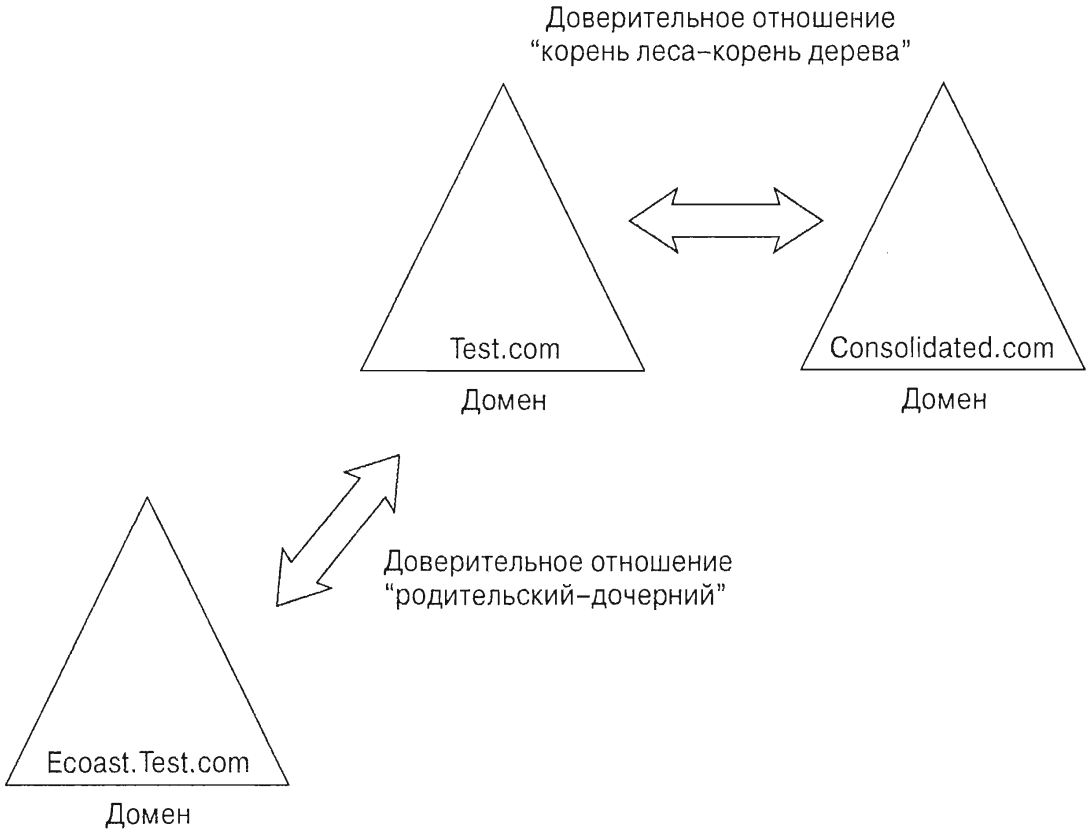


Рис. 24.1. Пример леса Active Directory

Протокол Kerberos воспринимает в подобной манере доверительные отношения между доменами. Учетная запись пользователя начинает с получения поручительства (*билета*) у своего контроллера домена. Если необходимый ресурс находится в другом домене, она должна проследовать через доверительные отношения в домен, содержащий этот ресурс. Понадобится подняться вверх по доверительному отношению "родительский–дочерний", пересечь доверительное отношение "корень леса–корень дерева" и при необходимости спуститься вниз по пути доверительного отношения "родительский–дочерний" другого дерева. Если пользователь находится в Ecoast.Test.com, это значит, что он должен контактировать с контроллером домена Ecoast.Test.com. Если ресурс размещается в Consolidated.com, то контроллер домена Ecoast.Test.com взаимодействует с контроллером домена в Test.com. Затем контроллер домена Test.com должен обратиться к контроллеру домена в Consolidated.com. Таким образом, чтобы добраться до требуемого ресурса, придется выполнить три прыжка, поскольку именно такой путь предоставляют создаваемые автоматически доверительные отношения. Более высокие деревья означают большее количество прыжков, более интенсивный трафик и большую задержку. Если вы работаете в крупной организации, включающей много доменов, то вместо последовательных прыжков по доверительным отношениям доменов вы всегда можете создать доверительное отношение, установленное напрямую, которое обеспечит непосредственную ссылку между двумя доменами, отстоящими далеко друг от друга в рамках иерархии доменов.

Вы должны строить деревья и леса вместе

Поддержка нескольких доменов является великолепной возможностью, которая стала значительным усовершенствованием по сравнению с более ранними версиями Windows Server. Но вы не можете присоединять существующие домены к дереву. Вспомните, что в живой природе вы не можете пересадить какой-то лес рядом с другим лесом. К тому же не удастся поместить в лес существующие деревья; пересадка деревьев — задача не из легких. Точно так же, как могучий дуб вырастает из маленького желудя, сформировать лес можно единственным способом — с нуля. Вы начинаете с одного домена, корня леса. Затем вы можете добавить домен в существующее дерево (дочерний домен) или добавить дерево в существующий лес (корень дерева). Другие домены навсегда останутся за пределами вашего леса.

Вы не можете прививать или подрезать

Предположим, что вы создали в одной сети домен AD по имени Test.com. Затем в совершенно другой сети, не связанной с первой, вы создали домен AD под названием Ecoast.Test.com. Вы не сможете затем связать эти две сети друг с другом, получив долгожданное воссоединение родительского и дочернего доменов. Аналогично вы не сможете построить AD-деревья Consolidated.com и Test.com изолированно и впоследствии соединить их, чтобы создать лес. Присоединение существующих доменов к существующим деревьям или лесам называется *прививанием*, но сделать это невозможно — во всяком случае, с помощью инструментов, поставляемых Microsoft. Таким образом, например, если компания Exxon приобретает компанию Mobil и у Exxon уже есть домен по имени Exxon.com, а у Mobil — домен Mobil.com, то объединить их в дерево с помощью имеющихся инструментов Active Directory от Microsoft не получится.

Но не стоит тревожиться, если вам не удалось найти сторонние инструменты для прививания. Microsoft просто не поддерживает их. Одним из самых серьезных обстоятельств, сдерживающих создание инструмента, который позволил бы привить домен к лесу, является *схема*. Схема, которая определяет объекты в Active Directory, допускает модификацию, как будет показано в разделе "Роли FSMO и GC" далее в главе. Если две компании изменяют свои схемы по-разному, то разработать метод, обеспечивающий объединение таких различий, не представляется возможным. Еще одна очень важная причина, препятствующая прививанию домена к лесу, связана с соображениями безопасности. В рассмотренном ранее примере в именах домена присутствует Test.com, но поскольку они не создавались вместе, идентификаторы защиты не совпадают. Если разрешить прививание Test.com к Ecoast.Test.com, возникла бы значительная брешь в безопасности.

Подрезание также не допускается. Если Consolidated.com является частью леса и его компания выходит из Test.com, то этот домен не сможет функционировать независимо от остальных доменов. В нашем распоряжении нет флажка, который бы позволил этому случиться, к тому же безопасность дерева и иерархии была бы полностью утрачена.

Вы должны быть администратором предприятия

Необходимо также помнить об еще одном факторе — для добавления доменов в лес недостаточно быть обычным администратором домена. Возможно, вы полагали, что учетные данные администратора домена дают вам безраздельную власть,

но это ошибка. Вы должны быть членом группы администраторов предприятия (`Enterprise Admins`).

Если вы создали домен AD по имени Test.com и хотите создать в его дереве дочерний домен Ecoast.Test.com, то должны войти в систему сервера, который планируется сделать первым контроллером домена в Ecoast.Test.com, и создать дочерний домен Ecoast.Test.com. Процесс создания нового дочернего домена очень похож на способ построения первоначального домена. При этом по-прежнему применяется мастер конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard), но в ходе работы с ним будут выбираться несколько отличающиеся параметры.

Прежде чем этот мастер позволит добавить еще один домен, он потребует указать имя и пароль всемогущего администратора предприятия для домена Test.com. Конфигурация AD DS откажется создать дочерний домен, если только она тотчас же не сможет установить контакт с родительским доменом и получить разрешение. Аналогично, если вы хотите создать второе дерево в лесе, мастер потребует предоставить имя и пароль учетной записи администратора предприятия для первого дерева. (А как насчет третьего или четвертого дерева — какая учетная запись потребуется для *них*? Начиная со второго и заканчивая миллионным деревом в лесе, вы должны указывать имя и пароль учетной записи администратора предприятия для первого дерева в лесе.)

Планирование среды Active Directory

Перед повышением сервера до первого контроллера домена необходимо составить общее представление о сети Active Directory. В дополнение к структуре организационных единиц, пространству имен DNS, размещению контроллеров домена и репликации, которые являются частью плана с единственным доменом, вы должны принять во внимание потребность в нескольких доменах. Чтобы получить правильное решение по этому вопросу, следует учесть множество факторов. Ниже приведено более подробное их обсуждение.

Удовлетворение политических потребностей

"Это *мои* данные, поэтому я хочу, чтобы они находились на *моих* серверах!" Поскольку во многих фирмах информация стала самым важным активом, временами часть управленческих подразделений отказываются передавать контроль над этой информацией центральной IT-группе. И это нельзя считать неразумным: если бы вы отвечали за поддержку списка рассылки для пяти миллионов человек, обеспечивающего фирме половину объема продаж, то наверняка предпочли бы, чтобы данные находились на компьютерах, за которыми работают люди, отчитывающиеся непосредственно перед вами.

Конечно, в этой истории присутствует и другая сторона — руководитель IT-отдела, который желает иметь полный контроль над всеми серверами в здании, и такое его желание вполне законно. В конце концов, если неустойчиво функционирующий сервер выйдет из строя и отказ повлияет на работу остальной сети, то отвечать за это придется именно ему.

Таким образом, начальник отдела или вице-президент желает контролировать оборудование, где размещены его данные, но руководитель IT-отдела, который от-

вечает за безопасность всех данных и корректное функционирование сети в целом, стремится контролировать данные и сеть. Кто из них окажется победителем? Когда как — в этом и состоит "политический" аспект.

Что делает Active Directory, чтобы помочь в решении таких политических проблем? Увы, не так много, как хотелось бы: в вашем распоряжении нет мастера, который заставил бы вице-президентов выработать приемлемое для вас решение. Однако разнообразие параметров, относящихся к доменам, в Active Directory предоставляет проектировщикам сети гибкость, необходимую для построения любой желаемой структуры сети. Вы работаете в относительно небольшой организации, которой было бы достаточно одного домена, но одному из вице-президентов хочется владеть сервером? Нет проблем, предоставьте ему собственную организационную единицу внутри домена. Вы работаете в компании с двумя довольно большими офисами и независимыми IT-подразделениями? Решить проблему можно было бы путем создания двух доменов и доверительного отношения между ними. Поскольку контроллерам домена Active Directory, функционирующим под управлением Windows Server 2012 R2, требуется не так много полосы пропускания WAN, как в более ранних версиях, может обнаружиться, что имеет смысл располагать только одним доменом, т.к. его легче администрировать, нежели два. Тем не менее, это невозможно с точки зрения полосы пропускания. Итак, степень использования полосы пропускания является следующим аспектом.

Вопросы подключаемости и репликации

Растет количество компаний, занимающих более одного места. Компания может поглотить другую фирму, офис которой находится на другом конце страны, и то, что когда-то было двумя отдельными *локальными* сетями, теперь стало одной организацией с потребностью в канале WAN. На проектное решение Active Directory влияет доступная пропускная способность канала WAN. Решение относительно использования одного или нескольких доменов зависит от скорости канала WAN. *Скорость* — понятие относительное. Для одних решений вполне достаточно каналов с полосой пропускания 10 Мбит/с, тогда как для других такой полосы мало. В первую очередь это зависит от размеров раздела домена и от частоты его модификации.

Если ширина полосы WAN позволяет, вы можете связать два офиса вместе и создать только один домен. Структура с единственным доменом предпочтительна в том отношении, что ее будет легче администрировать. Каждый сайт будет содержать, по крайней мере, один контроллер домена, который управляет всеми пользователями и компьютерами. Если канал WAN выходит из строя, то контроллер домена в каждом офисе может управлять входом пользователей в систему.

Но такие контроллеры домена должны взаимодействовать друг с другом каждый раз, когда происходят какие-то изменения, такие как смена пароля у пользователя или создание администратором учетной записи для нового пользователя. Эта репликация должна происходить через канал WAN.

Если канал не в состоянии поддерживать трафик репликации, вы должны обдумать возможность создания нескольких доменов. Таким образом, раздел домена, который является самым крупным разделом в базе данных Active Directory, будет ограничен местоположением офиса, в котором он размещен. Разделы конфигурации и схемы будут реплицироваться по каналу WAN, однако они меняются не особенно часто. Это позволит существенно сократить объем трафика репликации.

Среда Active Directory позволяет указывать, как должна реплицироваться ее информация, но репликации должны подвергаться все части базы данных Active Directory. В результате в организациях с несколькими площадками необходимо выяснять, способна ли доступная полоса пропускания поддерживать трафик репликации.

Глобальный каталог (GC), который содержит объекты из всех доменов, получает изменения от доменов по всему лесу. Глобальный каталог важен для процесса входа пользователя в систему и Exchange Server, поэтому он должен находиться близко к пользователям. Следовательно, каждый домен будет также реплицировать информацию глобального каталога по каналам WAN на другие сайты. Доступная полоса пропускания может не справиться с этим трафиком, поэтому, возможно, придется рассмотреть вариант с отдельными лесами.

Несколько доменов: когда это имеет смысл

Когда вы должны применять один домен, разделенный на организационные единицы, а когда иметь несколько доменов или даже лесов? Общее эмпирическое правило таково: используйте несколько доменов, только если нет другого выхода. В таком случае возникает реальный вопрос: когда наличие множества доменов имеет смысл? Это имеет смысл в нескольких случаях, которые описаны ниже.

- **Проблемы с репликацией из-за недостаточной ширины полосы пропускания.** Пожалуй, это самая убедительная причина. Все контроллеры домена в домене действительно должны находиться в онлайновом режиме и постоянно быть доступными друг другу. Репликация между контроллерами домена должна быть согласованной, иначе произойдет отказ в их работе. Если канал WAN не в состоянии поддерживать трафик репликации, лучше реализовать несколько доменов. Представьте себе следующую ситуацию. Один из офисов находится в Чикаго, а другой — в Сиднее (Австралия), и они связаны между собой дорогостоящим каналом. Предположим также, что в чикагском офисе работают 20 000 человек, а в сиднейском — 150 человек. Каждый раз, когда чикагские пользователи изменяют свои пароли, весь трафик должен реплицироваться по дорогостоящему каналу WAN на контроллеры домена в Сиднее. Такое использование канала WAN не является эффективным. Лучше просто построить два домена.

- **Юридические требования.** Иногда возникают соображения юридического характера, которые требуют создания отдельных доменов и возможно отдельных лесов. Хотя изначально вы могли не считать, что необходимо использовать несколько лесов, есть ситуации, когда без этого не обойтись.

  Поскольку вы не можете убрать дерево из леса, вам придется задуматься над возможностью реструктуризации вашей организации. В случае отсечения потребовалось бы создать отдельный лес, чтобы обеспечить четкое отмежевание от главного леса Active Directory.

  Некоторые национальные законы могут запрещать совместное использование информации по разные стороны национальной границы. Роль Global Catalog указывает закрытую информацию для каждого пользователя в лесе. Она также включает контакты с их информацией. В некоторых странах с этим могут возникать проблемы. Следовательно, потребуются отдельные леса.

Организации могут располагать похожими правилами для пользователей. Возможно, должен быть предусмотрен контроль специфических пользовательских учетных записей внутри определенного здания. Может быть, должны изолироваться ресурсы, требующие более жесткой проверки безопасности. Учитывая юридические требования, может понадобиться отдельный домен или лес. Отдельные леса могут также потребоваться из-за риска потенциального вмешательства внутрь леса.

- **Политика.** Об этом шла речь в разделе "Удовлетворение политических потребностей".
- **Слияние двух организаций.** Ваша фирма приобрела другую фирму, и вы должны скомбинировать две организации. Инструменты сторонних разработчиков помогают приспособить новый домен к существующему домену, но это крупная задача. Возможно, в данный момент у вас просто нет времени, чтобы сделать это. В таком случае вам придется некоторое время провести в мире с множеством доменов — скорее всего, в мире из нескольких *лесов*. Однако мы рекомендуем рассмотреть возможность слияния двух доменов с помощью инструмента, подобного Active Directory Migration Tool (Инструмент миграции Active Directory), который раскрывается в главе 25.

Некоторые требования к множеству доменов смягчены усовершенствованиями в Windows Server 2008 и Windows Server 2012 R2. Теперь имеется возможность устанавливать разные политики паролей для разных пользователей внутри домена. В прошлом для этого приходилось создавать отдельные домены. Офисы филиалов требовали создания отдельных доменов. Например, угроза границам безопасности возникала из-за того, что контроллер домена находился у кого-то под столом. В случае похищения контроллера домена мог быть скомпрометирован целый домен. Наличие отдельного домена ограничивало объем информации, подверженной угрозе. Контроллер домена только для чтения и политики кеширования паролей устраняют такие угрозы.

Случай с пустым корнем

Вернемся к рис. 24.1. На этом рисунке помимо Test.com и Ecoast.Test.com (дочернего домена Test.com) вы видите дополнительный домен корня дерева Consolidated.com. Мы сделали так, чтобы диаграмма "выглядела" правильно, но мы привыкли иметь дело с иерархиями, сходящимися в одной точке.

В дереве легко заметить, какой домен является корневым или доменом верхнего уровня: домен Consolidated.com находится на вершине дерева Consolidated.com, а Test.com — на вершине дерева Test.com. Но когда вы встраиваете два дерева (Consolidated.com и Test.com) в один лес, попробуйте ответить, какой домен является верхним, или корневым? Может быть, корня вообще нет и все деревья равноценны?

В лесе Active Directory, образованном из нескольких деревьев, *существует* единственный корневой домен леса. Просто неочевидно, какой из них является таким корнем.

Итак, предположим, что вам встретился лес AD, который содержит три домена — Test.com, Apex.com и Consolidated.com. Какой из этих доменов представляет собой корень леса? Ответ на этот вопрос не лежит на поверхности, т.к. все три домена выглядят находящимися на одном и том же уровне. Нам неизвестен быстрый метод выяснения, какой из доменов является корнем леса, но есть несколько более

медленный способ. Вспомните, что только домен корня леса содержит группу по имени Enterprise Admins; именно так можно найти корень.

Откройте оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory), выбрав в окне диспетчера серверов пункт Tools⇨Active Directory Users and Computers (Сервис⇨ Пользователи и компьютеры Active Directory). В левой панели этой оснастки MMC вы увидите значок, представляющий домен; на нем схематически изображены три системных блока рядом. Щелкните правой кнопкой мыши на этом значке и выберите в контекстном меню пункт Find (Найти). В появившемся диалоговом окне имеется раскрывающийся список, помеченный In (В), который позволяет указать, в каком домене должен быть произведен поиск. Щелкните на списке, и вы увидите, что есть возможность поиска в любом домене леса. Выберите один из доменов верхнего уровня. Затем обратите внимание на поле, помеченное Name (Имя); введите в нем **enterprise*** и нажмите <Enter>. Если в результате поиска будет найдена группа под названием Enterprise Admins, то вы нашли корень. Если же нет, откройте раскрывающийся список In и проверьте еще один домен — и так до тех пор, пока не найдете домен, содержащий группу Enterprise Admins.

Представим, что в рассматриваемом примере с Test/Ecoast/Consolidated корневым доменом является Test.com. Существуют три домена, поскольку имеются (или когда-то были) три разных бизнес-сущности, которые по ряду причин оказались в одном предприятии. А кого заботит, что пользователи Test.com стали корнем леса?

Пользователям Consolidated и Ecoast есть до этого дело — знают они об том или нет. Причина связана с тем, что члены группы Enterprise Admins, которые волею случая попали в домен Test, обладают высокими правами в *каждом домене леса.* Они не являются членами группы Domain Admins в этих доменах, но вполне могут быть, т.к. группа Enterprise Admins обладает практически такими же правами, как и группа Domain Admins, во всех доменах.

Это означает, что хотя *теоретически* Test, Ecoast и Consolidated имеют отдельные домены с четкими и удобными границами безопасности, *на практике* пользователям Ecoast и Consolidated остается лишь надеяться, что в один прекрасный день пользователи Test не поддадутся искушению сделать что-нибудь неожиданное в доменах Ecoast или Consolidated. Как поступить? Не создавайте три домена; создайте четыре домена.

Первым доменом — корневым — должен быть домен, который вы не собираетесь когда-либо использовать (e-gobbledygook.com или что-то вроде того). Создайте в этом домене одну административную учетную запись, включив ее в группу Enterprise Admins. Позвольте создать такую учетную запись директору по информационным технологиям. Попросите его записать на листке бумаги ее имя и пароль, поместить листок в сейф и воспользоваться процедурой ликвидации персонала из сериала "Клан Сопрано" по отношению к тем, кому известен этот пароль, исключая вас и самого директора. (Понятно, что это всего лишь шутка. Но учтите, что речь идет о чрезвычайно важной учетной записи, доступ к которой посторонним лицам должен быть категорически запрещен.)

В то же самое время создайте еще три домена. Вам опять понадобятся услуги директора по информационным технологиям, который должен ввести имя пользователя и пароль для учетной записи Enterprise Admins, чтобы можно было создать эти три домена. Затем вы можете забыть об учетной записи Enterprise Admins, т.к. пользоваться ею придется нечасто.

Идея создания первого домена и помещения в него только одной или двух учетных записей, после чего с ним никакие действия не предпринимаются, называется построением структуры AD *с пустым корнем*.

Некоторые фирмы создают домен с пустым корнем, даже когда предприятие имеет единственный домен, на тот случай, если в будущем будут приобретены другие компании. Мы считаем это похвальной предусмотрительностью и рекомендуем рассмотреть такую возможность. Разумеется, недостаток такого подхода связан с тем, что вам понадобится контроллер домена (а еще лучше два), который будет функционировать, ничего не делая для поддержки корневого домена, и каждому из них потребуется копия Windows Server 2012 или предыдущей редакции сервера в зависимости от функционального уровня леса. Но это может оказаться неплохой инвестицией: пустой корень — тот самый случай, когда мы готовы отказаться от предпочтения, отдаваемого нами системам с единственным доменом.

Пример из практики

Случай с двумя контроллерами домена

В любой среде рекомендуется обеспечить высокий коэффициент готовности и возможность аварийного восстановления для служб и систем. Модель репликации с несколькими хозяевами, предоставляемая Active Directory, существенно упрощает решение этих задач. Все, что от вас требуется — это установить еще один контроллер домена внутри сайта для поддержания постоянной готовности или в каком-то другом сайте для обеспечения аварийного восстановления либо сделать то и другое.

Однако *лучше всего* добавить, по крайней мере, два контроллера домена в пустой домен корня леса. Несмотря на отсутствие в таком домене пользователей или ресурсов, он по-прежнему является незаменимой (в буквальном смысле) частью среды Active Directory. Он должен обладать высоким коэффициентом готовности и устойчивости к отказам. Если такой домен поддерживается только одним контроллером домена, этому контроллеру придется выполнять очень большой объем работы. Если вы потеряете и не сможете восстановить его, возможно, вам придется обратиться в службу поддержки Microsoft и заодно подкорректировать свое резюме.

Рассмотрим влияние одиночного контроллера домена пустого корня.

- Весь трафик аутентификации Kerberos проходит через этот домен корня леса. Запомните: он является дружественным по отношению ко всем, в частности к корню каждого дерева.
- Синхронизация времени централизована на эмуляторе PDC (primary domain controller — основной контроллер домена) корня леса, который по умолчанию является первым контроллером домена.
- Две роли FSMO, Domain Naming Master (Хозяин именования доменов) и Schema Master (Хозяин схемы), находятся в этом домене и на этом одиночном контроллере домена.

Таким образом, если одиночный контроллер домена пустого корня выйдет из строя, это скажется на остальных частях леса. Вы не можете создать контроллер домена реплики без контроллера домена, из которого выполняется репликация, поэтому вам не останется ничего другого, как провести восстановление с нуля. Возможно, вам придется заново перестроить среду Active Directory и перенести в нее пользователей и компьютеры, если восстановление окажется недоступным.

Указания по проектированию структуры Active Directory

Цель этой главы заключается в том, чтобы дать общее представление о работе отдельных компонентов Active Directory. Ранее мы обсуждали основные области решения, касающиеся структуры Active Directory. Мы настоятельно рекомендуем прочитать книгу до конца, прежде чем приступать к построению структуры Active Directory, т.к. AD буквально *пронизывает* сети, базирующиеся на Windows. Однако в последующих разделах приводится несколько рекомендаций относительно того, как приступить к проектированию собственной структуры Active Directory.

Проанализируйте топологию доступной глобальной сети

Контроллеры домена в том или ином домене должны выполнять репликацию между собой, чтобы поддерживать информацию в согласованном состоянии по всему домену. Контроллеры домена не нуждаются в наличии подключения 24 часа в сутки 7 дней в неделю. Вы *могли бы* устанавливать подключения между офисами филиалов и головным офисом каждый день или немного чаще, и затем предпринимать попытку принудительной репликации, хотя это не просто и может приводить к проблемам по ходу дела. Однако в целом вы обнаружите, что домены работают эффективнее всего, когда в них поддерживается постоянное сквозное подключение. При наличии области, которая недостаточно или нерегулярно обслуживается существующими подключениями WAN, возможно, лучше сделать ее отдельным доменом или отдельным лесом.

Спланируйте будущие сайты

Когда вы будете знать, где находятся подключения WAN, подготовьте список будущих сайтов, назначьте им имена и спланируйте, какие машины на какие сайты последуют. Кроме того, документируйте природу их подключений, т.е. скорость и стоимость, чтобы помочь Active Directory разумно использовать межсайтовую полосу пропускания.

Определите, какие из существующих доменов целесообразно объединить, и объедините их

Возможно, вы хотите сократить количество доменов в своем предприятии. Одним из способов достижения этой цели является объединение ресурсных доменов в главный домен. Идея заключается в том, что вы сначала модернизируете главный домен до Windows Server 2012, а затем объединяете другие домены с этим главным доменом как организационные единицы с помощью инструмента миграции Active Directory (Active Directory Migration Tool — ADMT) или любого другого инструмента подобного рода, который вы могли приобрести. Объединение доменов и применение ADMT подробно обсуждаются в главе 25.

Когда необходима организационная единица, а когда нужен домен?

Как указывалось ранее, предприятие можно представить в виде нескольких доменов. Кроме того, вы можете создать единственный домен и использовать орга-

низационные единицы, чтобы распределить административный контроль, или же применять любое их сочетание.

В какой-то мере это политический вопрос, но для начала вы можете проанализировать предполагаемые потребности организации. Централизовано или децентрализовано администрирование? Кто управляет учетными записями пользователей? Кто управляет такими ресурсами, как файловые серверы? Насколько тесно сотрудничают между собой подразделения компании?

Выбор организационных единиц или нескольких доменов предусматривает разделение сети между контролирующими силами, чтобы они могли администрировать ее. Организационные единицы позволяют определенным администраторам управлять учетными записями компьютеров, пользователей или групп, за которые они несут ответственность. Таким образом, если администраторам необходимо только это, отдавайте предпочтение организационным единицам. Выбор варианта с несколькими доменами зависит от того, кто будет управлять контроллерами домена. При наличии отдельной группы администраторов, которые будут управлять контроллерами домена, не считая домена корня леса, создание дополнительного домена будет вполне оправданным.

С технической точки зрения, как упоминалось выше, на самом деле существует только несколько причин для использования более одного домена. Основной причиной является трафик репликации. Если у вас есть два крупных домена, соединенных между собою медленным каналом WAN, то вы можете прийти к выводу о целесообразности их сохранения как отдельных доменов. Но хорошо обдумайте свое решение: Active Directory чрезвычайно эффективно задействует каналы WAN для трафика репликации доменов.

Разработайте имена для своих доменов/деревьев

Active Directory допускает широкое разнообразие имен доменов, но иногда в нашем распоряжении оказывается слишком много хорошего с очень *многими* вариантами. Если вы решили применять структуру с несколькими доменами, то насколько удачно эти домены подойдут друг другу? По какому принципу вы проводите разделение: по географическому расположению, по подразделениям или по функциям? Где сейчас проходят линии контроля в организации?

Важно понимать, что имена доменов выбираются, главным образом исходя из политических соображений. За исключением доверительного отношения "родительский–дочерний" вряд ли существует какой-то другой технический фактор влияния на имена. Имя будет периодически отражаться на пользователях посредством такой технологии, как основанные на доменах распределенные файловые системы (Distributed File System — DFS), и зависит на то, как они входят в систему компьютеров. Таким образом, поскольку пользователи видят это имя, руководство может заботить то, как назван домен.

Приведите в готовность инфраструктуру DNS

После того как вы определитесь с именами своих доменов, вам необходимо спланировать инфраструктуру DNS. Выясните, какие серверы будут ее поддерживать. Подумайте над тем, как клиенты будут распознавать внутренние и внешние имена. Запомните перечисленные ниже рекомендации.

- Запланируйте зону DNS, имя которой соответствует имени вашего домена Active Directory, и не бойтесь использовать фиктивный домен верхнего уровня.
- Не рекомендуется применять внешне зарегистрированные имена DNS.
- Хотя Windows Server 2012 R2 настраивает инфраструктуру DNS автоматически, вам редко придется начинать все с нуля. Если пространства имен DNS уже имеются, удостоверьтесь в том, что DNS-сервер поддерживает динамические обновления DNS и записи ресурсов служб. Вы вовсе не обязаны использовать DNS-сервер Microsoft, но это неплохая идея, особенно с зонами, интегрированными с Active Directory.
- Если вам приходится применять зарегистрированные DNS-имена вашей компании, то разделенная DNS является *самым подходящим* способом защиты ваших зон от посторонних глаз для 99% содержимого Active Directory.

Рекомендации по общей структуре AD

При построении структуры AD приходится учитывать очень много факторов, но только вам известны конкретные потребности и желания вашей организации — мы не можем предложить проектное решение AD, которое годилось бы на все случаи жизни. Но в целом важно иметь в виду следующие рекомендации.

- Используйте сайты для управления полосой пропускания и репликацией.
- Применяйте организационные единицы для создания изолированных участков пользователей и/или компьютеров, куда вы сможете затем делегировать функции административного управления.
- Используйте домены для решения задач репликации, безопасности, а также соответствия законодательным и политическим нормам.

Применяйте леса для создания полностью отдельных сетевых систем. Например, если у вашего предприятия есть дочерняя компания, которая не пользовалась полным доверием (в человеческом смысле, а не в смысле Active Directory), и вы опасались, что автоматические доверительные отношения (в смысле Active Directory), созданные совместным членством в лесе, могут привести к появлению нежелательных каналов доступа, то сделайте их отдельными лесами. Ценность отдельных лесов заключается в том, что между двумя лесами вообще не существует отношений безопасности, если только вы явно не создадите их с помощью механизма доверительных отношений.

Создание нескольких доменов

После того как вы тщательно обдумаете структуру и убедите начальство в правильности выбранного вами способа реализации Active Directory, следует приступать к практическому воплощению ваших идей. Если вы не рискуете проверить эффективность желаемой структуры Active Directory в производственной среде, то, по крайней мере, можете сделать это в испытательной среде. Таким образом, вы должны знать процедуру построения нескольких доменов.

Процесс создания нового домена похож на процесс создания первого домена. Прежде всего, нужно определиться с именем домена. Поскольку изменение имени домена влечет за собой многочисленные последствия, его следует по возможности

избегать. Подобно первоначальному домену, новый контроллер домена понадобится подготовить к поддержке Active Directory. Он должен также иметь возможность распознавать имена доменов корня леса посредством DNS. Затем вы повысите первый сервер до контроллера домена, создав новый домен.

Назначение имен в структурах с несколькими доменами

Реальная практика показывает, что иерархия доменов лучше всего работает на крупных предприятиях. В Active Directory мы называем ее *древовидной структурой*, невзирая на тот факт, что корни компьютерных деревьев обычно висят в воздухе, а их "листья" располагаются внизу. (Действительно, приходится признать, что аналогия "обратно к природе" не во всем последовательна.) В Microsoft спроектировали AD так, чтобы в качестве системы назначения имен применялась DNS, а система DNS сама по себе носит иерархический характер, поэтому Active Directory использует это счастливое стечение обстоятельств и поощряет построения предприятий с несколькими доменами в виде иерархий.

Пространства имен с несколькими доменами должны поддерживаться DNS. Предпочтительный метод предполагает предоставление такой поддержки AD DS через мастер конфигурирования. Поскольку дочерние домены имеют последнюю часть имени, совпадающую с именем существующего родительского домена, они располагают пространством имен DNS. Тем не менее, мастер автоматически настроит новые контроллеры домена на поддержку пространства имен дочернего домена. Вам не придется также создавать пространство имен для нового дерева, т.к. процесс повышения до контроллера домена автоматически сконфигурирует DNS для его поддержки. Однако чтобы безошибочно создать новое дерево, будущему контроллеру домена необходимо распознавать имена домена корня леса.

Если среда DNS была установлена заблаговременно, ей понадобится поддерживать записи ресурсов служб и динамические обновления DNS.

Невозможно всегда получать именно то, что вы хотите

Несмотря на уменьшившуюся важность NetBIOS-имени домена, вы по-прежнему будете встречать такие имена в сети. Прежде чем создавать домен, тщательно проверьте, доступно ли NetBIOS-имя, с помощью соответствующей утилиты. Если NetBIOS-имя отсутствует, утилита сгенерирует какое-то другое имя. Если вы не осведомлены о доступности такого имени, дело может застопориться из-за неправильно именованного домена.

Нам приходилось видеть тестовые домены, которым были назначены желаемые NetBIOS-имена. В результате, когда построен реальный домен, конфликтующие имена практически сразу станут очевидными и приведут к остановке процесса.

Подготовка контроллера домена для второго домена

В рамках рассматриваемого примера нам предстоит создать первый контроллер домена в другом домене — Ecoast.Test.com. Как упоминалось ранее, крупным изменением в Windows Server 2012 R2 по сравнению с предшествующими редакциями сервера является требование настройки DNS для домена. В ранних версиях Windows необходимо было подготовить DNS еще до построения домена. Мастер конфигурирования AD DS

идентифицирует потребность в установке DNS и проведет вас по соответствующим шагам. После создания дочернего домена вы обнаружите следующие компоненты:

- зона, интегрированная с Active Directory, на новом контроллере домена для имени дочернего домена, такого как Ecoast.Test.com;
- список DNS-серверов пересылки на этом контроллере домена для DNS-серверов Test.com;
- делегированный поддомен DNS на Test.com, указывающий на новый контроллер домена.

Прежде всего, настройте машину, которая будет контроллером домена для Ecoast.Test.com. Назначьте серверу имя **EC1**, напоминающее название первого контроллера домена в дочернем домене Ecoast.Test.com. Он должен будет поддерживать Active Directory для указанного количества пользователей и компьютеров в вашей организации. В производственной среде вам следует планировать построение, по меньшей мере, двух контроллеров домена для такого домена. Второй контроллер домена будет копией первого, обеспечивая отказоустойчивость базы данных домена.

Для применения Active Directory необходимо установить роль Active Directory Domain Services. Как и в случае первого контроллера домена для Test.com, мастер добавления ролей и компонентов (Add Roles and Features Wizard) позволяет включить эту роль. Он установит все двоичные сборки, требуемые для настройки контроллера домена, в том числе .NET Framework и службу DNS.

Имейте в виду, что теперь, когда утилита `DCPromo` была объявлена устаревшей, роль AD DS берет на себя выполнение процесса повышения сервера до контроллера домена. Это происходит в два этапа: добавление роли AD DS на сервер и, как постконфигурационная задача, проводимая после перезагрузки, повышение сервера до контроллера домена в новом домене с помощью мастера конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard).

Перед повышением сервера до контроллера домена удостоверьтесь в наличии учетных данных для учетной записи из группы `Enterprise Admins`.

Создание второго домена

После того как роль AD DS установлена, вы можете заняться установкой нового дочернего домена. Войдите в систему как администратор `EC1`, запустите постконфигурационную задачу для повышения сервера до контроллера домена. Этого можно достичь, либо выбрав нужный элемент в области Notifications (Уведомления) окна диспетчера серверов, либо перейдя в панель AD DS Management (Управление AD DS) в диспетчере серверов и запустив данную задачу.

Откроется окно мастера конфигурирования служб домена (рис. 24.2); на экране Deployment Configuration (Конфигурация развертывания) вы сообщаете мастеру, что хотите создать новый домен в существующем лесу, но не создавать новое дерево. В раскрывающемся списке Select domain type (Выбор типа домена) по умолчанию предлагается вариант Child Domain (Дочерний домен). В поле Parent domain name (Имя родительского домена) выберите имя родительского домена для присоединения (Test.com), а в поле New domain name (Имя нового домена) введите имя нового домена (Ecoast). После выбора имени родительского домена для присоединения в окне Windows Security (Безопасность Windows) будут запрошены данные учетной за-

писи, входящей в группу Enterprise Admins. Введите требуемую информацию и щелкните на кнопке Next (Далее), чтобы продолжить работу.

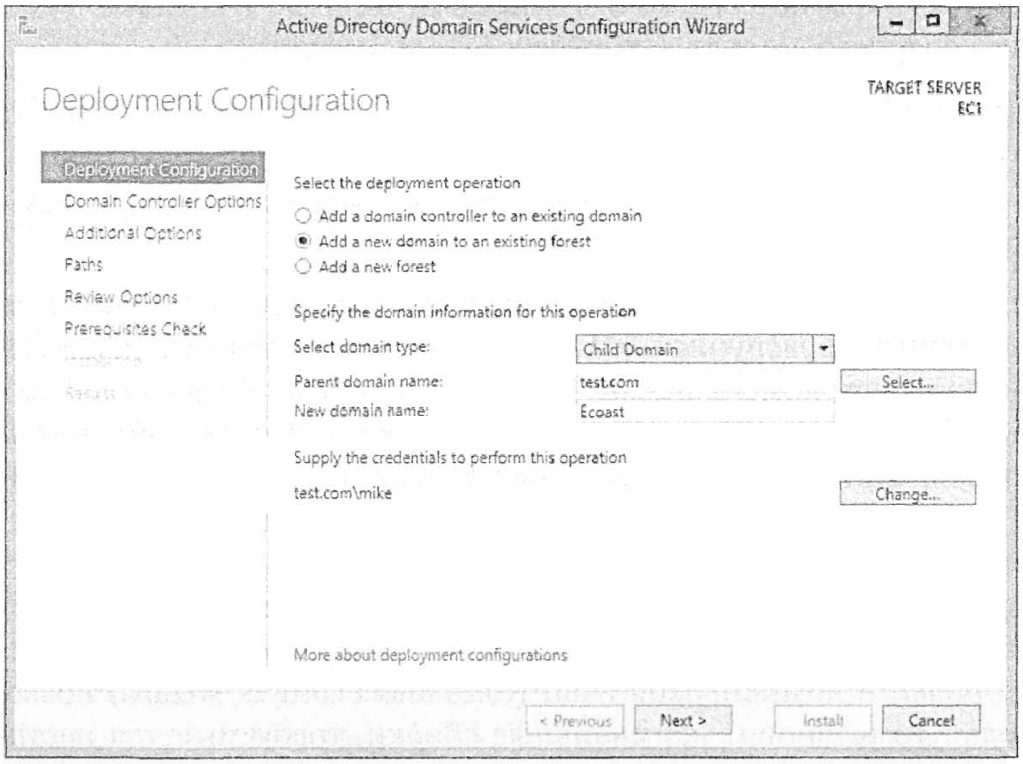


Рис. 24.2. Выбор конфигурации развертывания для нового домена в существующем лесу

На экране Domain Controller Options (Параметры контроллера домена) по умолчанию предлагается операционная система, используемая для развертывания этого основного контроллера домена для нового домена. В раскрывающемся списке Domain functional level (Функциональный уровень домена) выбран вариант Windows Server 2012 R2. Функциональные уровни домена мы обсудим в следующем разделе. На данном экране мастера доступны и другие параметры. Удостоверьтесь в том, что отмечен флажок Domain Name System (DNS) server (Сервер системы доменных имен (DNS)). Укажите, нужно ли сделать этот контроллер домена сервером GC, отметив флажок Global Catalog (GC) (Глобальный каталог (GC)). Поместите этот контроллер домена внутрь ранее созданного сайта, выбрав в раскрывающемся списке Site name (Имя сайта) соответствующее имя. Наконец, установите пароль для режима восстановления служб каталогов (Directory Services Restore Mode — DSRM). Экран мастера должен выглядеть примерно так, как показано на рис. 24.3. Для продолжения щелкните на кнопке Next.

На экране DNS Options (Параметры DNS) проверьте, отмечен ли флажок Create DNS delegation (Создать делегирование DNS) и предоставлены ли требуемые учетные данные. Затем щелкните на кнопке Next, чтобы перейти на экран Additional Options (Дополнительные параметры). Это очень важный экран. Здесь вы назначаете новому дочернему домену NetBIOS-имя (рис. 24.4). По умолчанию в качестве данного имени выбирается имя, введенное ранее на экране Deployment Configuration. В нашем случае оно выглядит как ECOAST. Вспомните, что поскольку это дочерний домен, имя получит суффикс родительского домена. Несмотря на то что здесь присутствует только ECOAST, полным именем домена будет Ecoast.Test.com, а полным доменным именем (FQDN) этого контроллера — Ec1.Ecoast.Test.com.

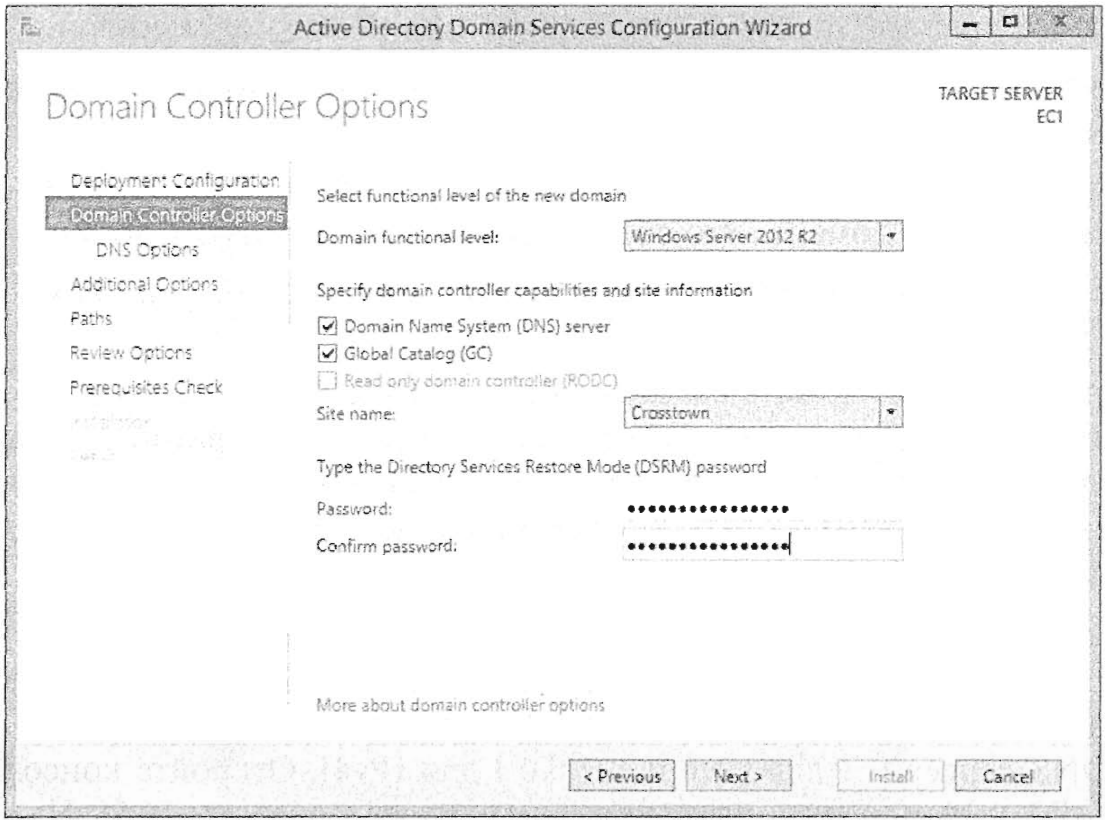


Рис. 24.3. Экран Domain Controller Options

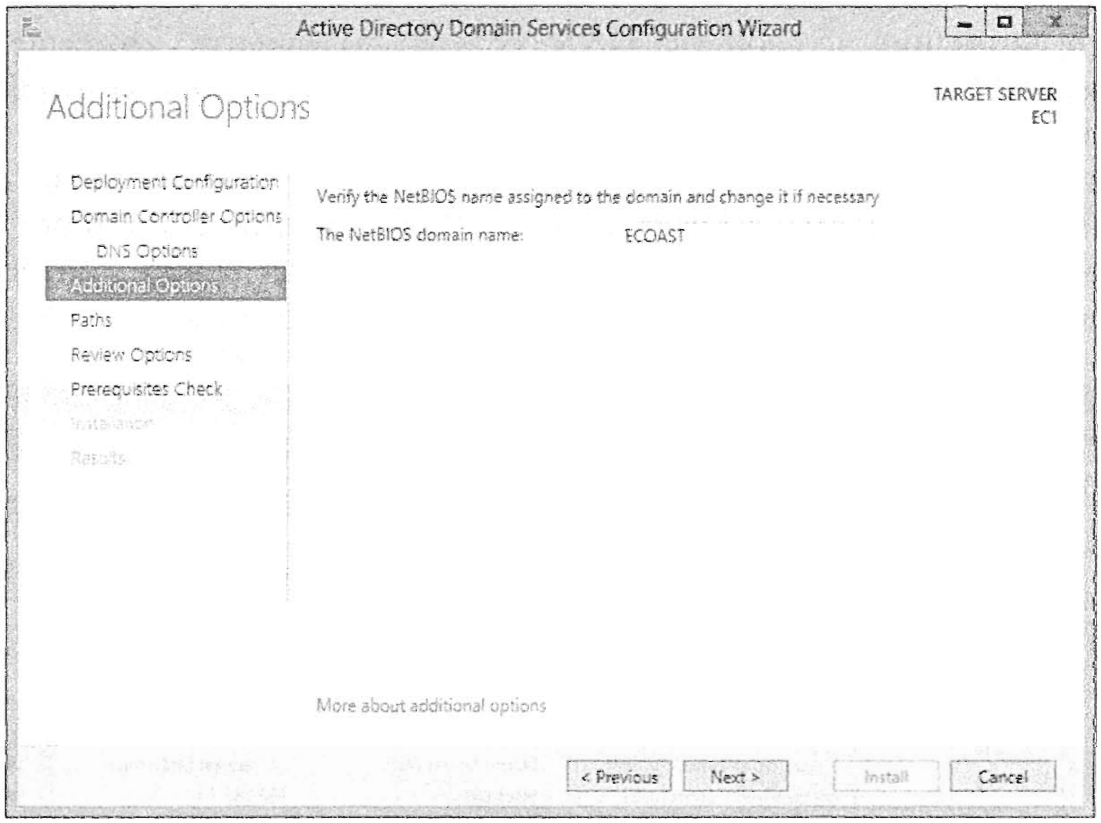


Рис. 24.4. NetBIOS-имя домена

Начиная с этого момента, вам придется только отвечать на вопросы мастера, как вы уже поступали ранее для первого домена, поэтому мы не будем здесь снова описывать остальные экраны.

Прежде чем оставить эту тему, мы приведем несколько замечаний, касающихся использования AD DS для построения доменов.

Роль AD DS требует достаточно жесткой последовательности создания доменов.

1. Первый домен, который вы создаете в лесе, является доменом корня леса; никакие изменения в этот домен не вносятся.
2. Для нового домена вы должны создать, по меньшей мере, один дополнительный контроллер домена. Это обеспечит отказоустойчивость домену.
3. Добавление доменов осуществляется путем их создания в AD DS по отношению к существующему домену.

   Например, вы не можете создать домен по имени Green.com и отдельно еще один домен под названием Yellow.com, а после этого принять решение об их объединении в лес. Взамен вы должны сначала создать Green.com как первый домен в лесе и затем создать Yellow.com как первый домен в новом дереве, но в существующем лесу.

После перезагрузки вы должны исследовать свой полностью сформированный и укомплектованный контроллер домена Ec1.Ecoast.Test.com. Проверьте его IP-конфигурацию с помощью `ipconfig /all` и убедитесь в том, что он перечисляет себя как DNS-сервер (::1 для IPv6 и 127.0.0.1 для IPv4). Откройте консоль диспетчера DNS (DNS Manager) на новом контроллере домена (рис. 24.5). Найдите зону Ecoast.Test.com, в которой контроллер домена Ec1 указан в качестве сервера имен. В зоне Ecoast.Test.com должны быть зарегистрированы запись A контроллера домена и записи SRV самого домена.

Обратите внимание на свойства DNS-сервера; вы увидите, что существует, по крайней мере, один DNS-сервер пересылки для BF1.Test.com или контроллеров домена родительского домена (рис. 24.6).

Также запустите консоль DNS Manager для BF1, чтобы удостовериться в добавлении делегирования поддомена Ecoast (рис. 24.7). Дополнительные проверки включают те же проверки, которые проводятся при построении любого контроллера домена, вроде создания файлов базы данных, папки и служб.

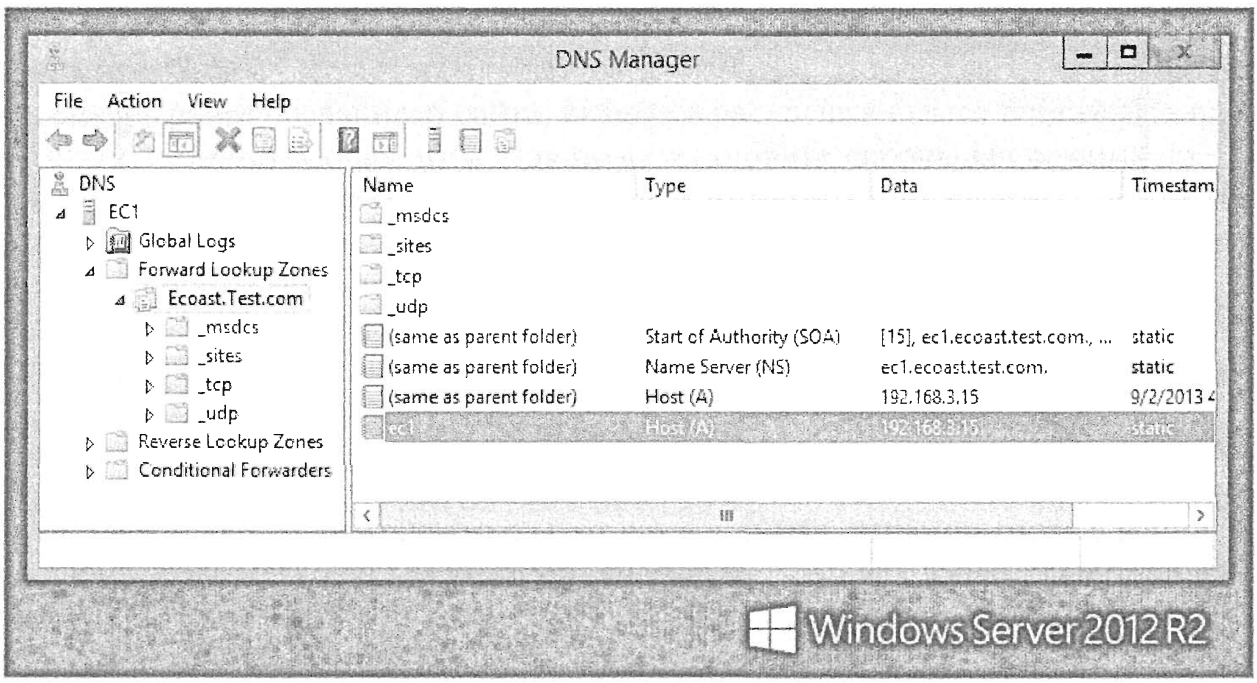


Рис. 24.5. Зона DNS для нового домена

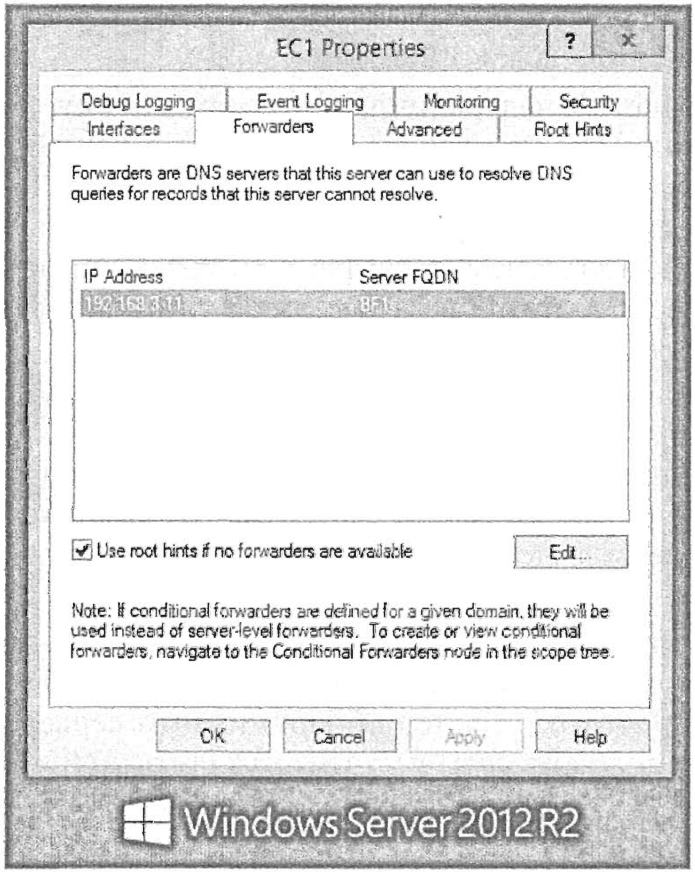


Рис. 24.6. DNS-серверы пересылки на новом контроллере домена

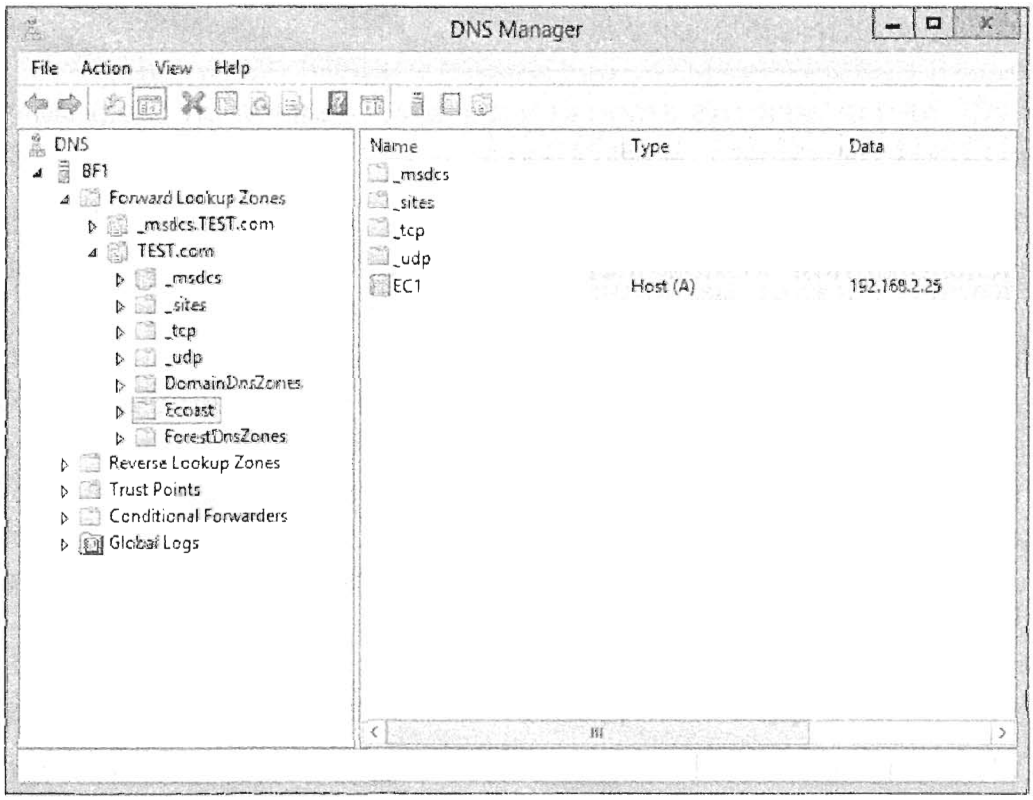


Рис. 24.7. Делегирование поддомена

Подчеркнем еще раз: инфраструктура DNS для поддержки новых доменов в Windows Server 2012 R2 конфигурируется автоматически. Если что-то ведет себя не так, как ожидалось, интеграцию DNS может понадобиться настроить вручную. Информация о том, как это сделать, а также каким образом выявить и устранить неполадки в DNS, приведена в главе 6.

Неправильное написание имен доменов

В ходе описанной выше процедуры вполне возможно допустить неправильное написание имени домена. При подготовке этой книги в нашей виртуальной испытательной среде мы создали домены Ecoast.Test.com и Ecoast.Test.com.com. Мы проявили невнимательность, но мастер принял набранные имена за чистую монету, что в результате привело к проблемам. Поэтому при создании нового домена в производственной среде обеспечьте, чтобы за экраном монитора следили хотя бы две пары глаз, и дважды проверяйте то, что ввели, на экране сводки.

Обратите внимание на существование отличия между переименованием неправильно написанного домена во время его создания и переименованием домена, который уже развернут и успешно функционирует в производственной среде. Намного проще сделать все правильно с первого раза. Если позже вам придется изменять имя домена, вы столкнетесь с весьма утомительным и трудоемким процессом запуска команд `rendom` для полного изменения имени.

Если после создания первого контроллера домена имя по-прежнему указано неправильно, можете еще раз запустить мастер AD DS Configuration Wizard на том же самом сервере. На этот раз мастер обнаружит, что сервер является контроллером домена. Он предположит, что вы хотите удалить Active Directory из сервера. Единственный вариант, который вам предстоит выбрать, связан с тем, является ли этот контроллер домена последним в домене. В данном случае это так. Затем мастер полностью удалит экземпляр Active Directory из сервера и среды.

Любое другое решение будет либо трудоемким в отношении Active Directory, такое как процесс переименования домена, либо деструктивным наподобие прекращения работы и удаления операционной системы.

Функциональные уровни

Функциональные уровни — это параметры конфигурации, используемые для управления унаследованной возможностью взаимодействия, а также контроля над тем, какие компоненты доступны в домене или лесе. Они также применяются для обеспечения совместимости между многочисленными версиями Windows Server во время выполнения миграций и модернизаций операционной системы на контроллерах домена. Каждая ОС Windows Server обладает своими специфичными расширенными средствами и уникальным функциональным уровнем, который интегрируется между разными операционными системами для обеспечения гладкой работы служб AD DS повсеместно в среде. Мы рассмотрим типы функциональных уровней и соображения по их изменению.

Функциональные уровни домена

В Active Directory на основе Windows 2000 Server существовало только два возможных варианта: либо совокупность контроллеров домена, которые все базировались на Windows 2000 Server, либо совокупность контроллеров домена, включающих и Windows 2000 Server, и Windows NT 4 — именно поэтому были возможны лишь два режима. Однако Active Directory в составе операционных систем, начиная с Windows Server 2003 и заканчивая Windows Server 2012 R2, может существовать несколько комбинаций контроллеров домена, каждая со своим режимом. Предпочтительным термином является *функциональный уровень*; иногда мы называем его *функциональ-*

ным уровнем домена, чтобы отличить от функциональных уровней *леса*, с которыми вы вскоре ознакомитесь.

Функциональный уровень домена можно изменить, открыв оснастку Active Directory Users and Computers и щелкнув правой кнопкой мыши на значке, который представляет необходимый домен. Выберите в контекстном меню пункт Raise Domain Functional Level (Поднять функциональный уровень домена); появится диалоговое окно, подобное показанному на рис. 24.8.

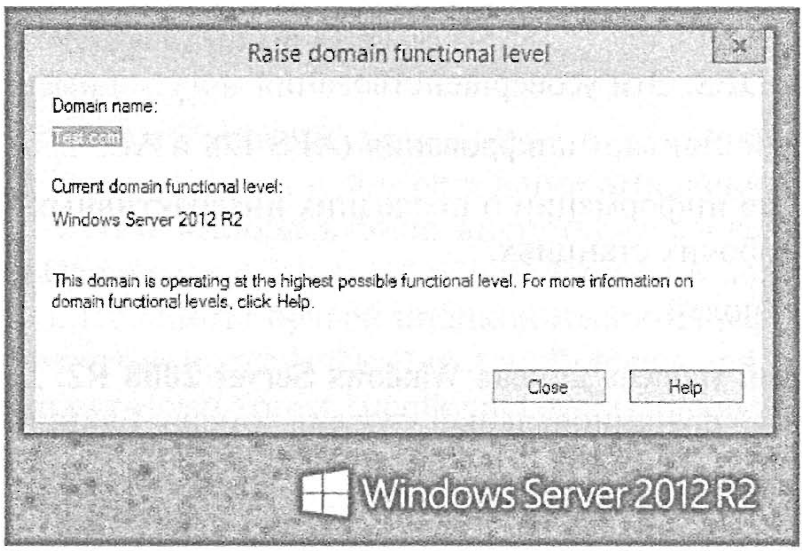


Рис. 24.8. Просмотр функционального уровня домена

В этом случае домен находится на функциональном уровне Windows Server 2012 R2, который является наивысшим из доступных на сегодняшний день. Кроме того, в диалоговом окне не предлагается возможность его изменения. Функциональные уровни домена можно изменять в направлении повышения, но не понижения. В данной ситуации это все, что мы можем сделать с этим доменом.

Изменение функционального уровня домена должно выполняться осторожно и обдуманно. Так как это односторонняя операция, вы должны удостовериться в том, что все контроллеры домена внутри домена могут удовлетворять требованиям желаемого функционального уровня. В противном случае унаследованный контроллер домена может просто утратить нормальную работоспособность. Он не будет должным образом участвовать в репликации, в результате чего его база данных станет содержать устаревшие или несовместимые данные.

Ниже описано, что можно получить от каждого функционального уровня.

- **Функциональный уровень домена Windows Server 2003.** Для его обеспечения все контроллеры домена в домене должны работать под управлением Windows Server 2003. Здесь предусмотрено несколько экзотических возможностей. Эти изменения не оказывают существенного влияния на работу. Вы даже можете никогда не увидеть их в действии.
  - Переименование домена; см. главу 25.
  - Можно выполнять перенаправление контейнеров пользователей и компьютеров.
  - Делегирование с ограничениями.
  - Избирательная авторизация; это связано с доверительными отношениями.
  - Обновление меток времени входа.

- **Функциональный уровень домена Windows Server 2008.** Для его обеспечения все контроллеры домена в домене должны работать под управлением Windows Server 2008. Однако в справочной системе Windows Server 2008 R2 дается важное предостережение. В частности, если вы планируете добавить в качестве контроллеров домена серверы с более ранними версиями ОС, такими как Windows Server 2008 или Windows Server 2003, то можете выбрать этот функциональный уровень домена. Ниже перечислены некоторые возможности данного функционального уровня.
  - Поддержка репликации DFS. В главе 14 вы читали об усовершенствованной репликации DFS. Эти усовершенствования могут применяться и здесь.
  - Расширенный стандарт шифрования (AES 128 и AES 256).
  - Отслеживание информации о последних интерактивных входах для пользователей на рабочих станциях.
  - Политики паролей.
- **Функциональный уровень домена Windows Server 2008 R2.** Даже у этой версии есть собственный функциональный уровень домена. Единственной его особенностью является предоставление механизма аутентификации. Это модифицирует маркер безопасности для пользователей, передаваемый серверам-членам с целью получения доступа к ресурсам. По существу он уведомляет о том, что пользователь был аутентифицирован посредством сертификата, а не учетных данных в виде имени пользователя и пароля. Затем можно сконфигурировать приложения и ресурсы для выдачи разрешения на основе этой информации.
- **Функциональный уровень домена Windows Server 2012 и Windows Server 2012 R2.** Функциональный уровень домена Windows Server 2012 R2 включает все замечательные возможности, предоставляемые предыдущими функциональными уровнями домена. Кроме того, он предлагает несколько дополнительных возможностей, которые заслуживают упоминания. Сейчас, когда в Windows Server 2012 имеется динамическое управление доступом (Dynamic Access Control — DAC), аутентификация Kerberos 5 несколько изменилась. Используя новую поддержку центра распределения ключей Kerberos (Kerberos Key Distribution Center — KDC) для утверждений, комплексную аутентификацию и защиту Kerberos, параметры политики административных шаблонов KDC обеспечивают контроллерам домена возможность поддержки утверждений и комплексной аутентификации для защиты Kerberos и DAC. Этот новый параметр политики также доступен на клиентском уровне для Windows 8. Аутентификация Kerberos и DAC более подробно обсуждались в главе 15.

Существует еще одна важная причина для перехода на функциональный уровень минимум Windows Server 2003 или выше. Вы не сможете модернизировать функциональный уровень *леса* до тех пор, пока все домены в лесе не окажутся на функциональном уровне домена Windows Server 2003. Если среда не находится на функциональном уровне домена хотя бы Windows Server 2003, вы не сможете извлечь преимущества от применения контроллеров домена только для чтения.

Функциональные уровни леса

При модернизации контроллеров домена или доменов в существующем лесе либо при создании нового леса ради безопасности ОС Windows Server 2012 предполагает, что не все контроллеры домена основаны на Windows Server 2012. Поэтому полный набор новых возможностей не будет задействован, если не все контроллеры домена в лесе работают на функциональном уровне домена Windows Server 2012. Если только не создается совершенно новый лес с использованием Windows Server 2012 R2, то в большинстве организаций придется пройти через процесс модернизации от Windows Server 2008 до Windows Server 2012 R2. Частью этого процесса будет поднятие функционального уровня леса.

Поднять функциональный уровень леса можно с помощью оснастки Active Directory Domains and Trusts (Домены и доверительные отношения Active Directory), которая открывается путем выбора в окне диспетчера серверов пункта меню Tools⇨Active Directory Domains and Trusts (Сервис⇨Домены и доверительные отношения Active Directory). Щелкните правой кнопкой мыши на расположенном в левой панели значке, помеченном как Active Directory Domains and Trusts, и выберите в контекстном меню пункт Raise Forest Functional Level (Поднять функциональный уровень леса). Откроется диалоговое окно, представленное на рис. 24.9. Будьте внимательными, чтобы не щелкнуть правой кнопкой мыши на значке домена. В таком случае внутри контекстного меню будет доступен только пункт Raise Domain Functional Level.

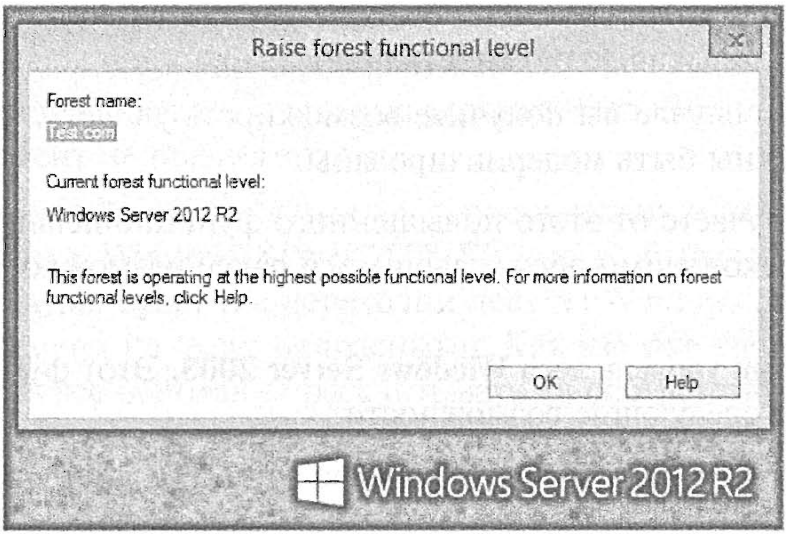


Рис. 24.9. Просмотр функционального уровня леса

На рис. 24.9 видно, что в данном примере функциональный уровень леса высок настолько, насколько это возможно при текущем функциональном уровне домена. Кроме того, понизить этот функциональный уровень нельзя.

Замечательная особенность заключается в том, что в лесе можно иметь домены, работающие под управлением операционных систем с более низким функциональным уровнем, чем функциональный уровень леса. Нередко приходится встречать домен Windows Server 2008 R2 в лесе Windows Server 2012 R2. Они работают вместе и оперируют на разных уровнях, оставляя пространство для миграций и возможности взаимодействия между операционными системами. До тех пор, пока функциональным уровнем домена является Windows Server 2003 или выше, такой домен может быть частью леса Windows Server 2012 R2.

Вы не сможете перейти на функциональный уровень леса Windows Server 2012 R2, пока каждый отдельно взятый контроллер домена в каждом домене этого леса не будет работать под управлением Windows Server 2012 R2 или выше. Однако подумайте вот над чем: не означает ли это, что все домены должны находиться на функциональном уровне домена Windows Server 2012 R2, прежде чем оснастка Active Directory Domains and Trusts позволит поднять функциональный уровень леса? Нет, оказывается, что не должны.

1. Когда вы открываете диалоговое окно, показанное на рис. 24.9, отображаемое в нем сообщение зависит от текущего состояния среды. Поскольку этот экспериментальный лес был построен на Windows Server 2012 R2, вы увидите такое сообщение: This forest is operating at the highest possible functional level (Этот лес действует на самом высоком функциональном уровне). Если бы вы попытались поднять функциональный уровень леса до Windows Server 2012 R2 при наличии контроллеров домена, продолжающих работать под управлением Windows Server 2008, то получили бы сообщение You can't go to 2012 R2 level (Вы не можете перейти на уровень Windows Server 2012 R2). Вдобавок было бы указано, какие контроллеры домена необходимо модернизировать перед тем, как можно будет перейти на функциональный уровень леса Windows Server 2012 R2.
2. Когда вы щелкаете правой кнопкой мыши на значке Active Directory Domains and Trusts, лес предоставляет краткие сведения о своих контроллерах домена:
   - если все контроллеры домена базируются на Windows Server 2012 R2, вам будет предоставлена возможность поднять функциональный уровень леса;
   - в противном случае вы получите возможность увидеть, какие контроллеры домена должны быть модернизированы.

Итак, что вы получаете от этого повышенного функционального уровня? Вы будете располагать несколькими обсуждавшимися ранее возможностями, которые подытожены ниже.

- **Функциональный уровень леса Windows Server 2003.** Этот функциональный уровень включает следующие возможности.
  - **Транзитивные доверительные отношения между лесами.** Одно доверительное отношение позволяет каждому домену в каждом из двух лесов доверять друг другу — но только в случае, если оба леса находятся на функциональном уровне Windows Server 2003.
  - **Более гибкая репликация членства в группах.** Старая проблема Windows 2000 Server, когда один пользователь изменял членство в группе и практически одновременно с ним членство в той же самой группе изменял другой пользователь, в результате чего одно из изменений терялось, на функциональном уровне леса Windows Server 2003 устранена.
  - **Улучшенная межсайтовая маршрутизация.** Значительная часть кода Windows Server 2003, отвечающего за межсайтовую репликацию, переписана заново. В то время как леса, основанные на Windows 2000 Server, разрушаются при количестве сайтов около 200, леса Windows Server 2003 способны поддерживать вплоть до 5000 сайтов.

- **Исправления в глобальном каталоге.** Любое изменение в структуре глобального каталога, вроде происходящего в результате установки приложения, управляемого AD, вызывает настоящую панику у глобального каталога в лесе уровня Windows 2000 Server; он сбрасывает свои базы данных и создает их заново, что приводит к интенсивному трафику репликации в сети. Леса уровня Windows Server 2003 намного более интеллектуальны, т.к. их глобальный каталог сосредоточен только на внесении изменений в базу данных вместо полной ее перестройки.
- **Переопределения схемы.** Недостаточно гибкую структуру схемы AD удалось сделать чуть более гибкой в лесе уровня Windows Server 2003. Удаление или откат изменений схемы по-прежнему невозможны, но схема организована так, чтобы исключать случаи, когда одно приложение, управляемое AD, случайно становится препятствием для внесения изменений в схему со стороны другого приложения, управляемого AD.

- **Функциональный уровень леса Windows Server 2008.** Этот функциональный уровень не привносит ничего специфического, поэтому в переходе на него нет особого смысла.
- **Функциональный уровень леса Windows Server 2008 R2: корзина AD DS.** Этот функциональный уровень предоставляет удобную возможность восстановления объектов Active Directory во время работы служб AD DS. Значительная экономия времени!
- **Функциональные уровни леса Windows Server 2012 и Windows Server 2012 R2.** Эти функциональные уровни включают все замечательные возможности из всех предшествующих функциональных уровней леса. Дополнительные средства на данный момент не предусмотрены.

Как известно каждому, кто пережил первоначальную версию AD под Windows Server 2003, дорога к Windows Server 2008 R2 иногда бывала долгой. Мы уверены, аналогичная ситуация будет и с переходом леса на Windows Server 2012 R2. Однако затраты сил и времени не будут напрасными. Как мы уже упоминали, вы *заплатили* за это, и у вас есть все основания рассчитывать на соответствующую отдачу.

Роли FSMO и GC

К этому моменту вы видели, как настраивать несколько доменов AD, но планирование AD предполагает не только это. Для обеспечения функционирования AD необходимо знать следующие аспекты.

- **Хозяева операций и глобальные каталоги.** Это особые функции, которые должны выполняться некоторыми контроллерами домена. Размещение этих ролей позволяет гарантировать надлежащее функционирование Active Directory.
- **Синхронизация времени.** Верите или нет, но AD просто не заработает до тех пор, пока все члены AD и контроллеры домена не согласуют показания времени в рамках пяти минут. Это управляется одним из хозяев операций, а именно — эмулятором PDC корневого домена леса.

В нескольких последующих разделах мы рассмотрим этот вид промежуточного планирования и функционирования AD. Для начала мы поговорим о хозяевах операций.

Репликация с несколькими хозяевами и с одним хозяином

Как упоминалось ранее, одним из признаков, которые отличают домены и контроллеры домена AD от доменов NT 4 и предшествующих версий, является применение репликации с *несколькими хозяевами*, а не с *одним хозяином*. При репликации с несколькими хозяевами *любой* контроллер домена может принимать изменения, касающиеся учетной записи пользователя. Это значит, что какой-то локальный администратор может запустить инструмент администрирования вроде оснастки Active Directory Users and Computers и внести изменения в учетную запись пользователя на доступном контроллере домена. Поскольку принимать изменения может любой контроллер домена, то любой контроллер домена является "хозяином" — отсюда и название репликации с несколькими хозяевами.

Не все компоненты поддерживают несколько хозяев

Вообще говоря, Active Directory пытается распространить идею децентрализованного управления на всю свою структуру. В целом все контроллеры домена равны между собой, однако, перефразируя Джорджа Оруэлла, некоторые контроллеры домена "более равны, чем другие". К ним относятся контроллеры домена, обслуживающие любую из пяти ролей, которые называются либо ролями *Operations Master* (Хозяин операций), либо ролями *Flexible Single Master of Operations* (Гибкие операции с одним хозяином), сокращенно FSMO. Строго говоря, аббревиатурой FSMO пользовались специалисты Microsoft при разработке Windows 2000 Server, однако позже, во время бета-тестирования, они переименовали FSMO в Operations Master. В результате некоторые пользуются термином *Operations Master*, но многие успели привыкнуть к аббревиатуре FSMO и применяют ее даже в наши дни, когда появилась версия Windows Server 2012 R2, возможно, из-за того, что она короче. Таким образом, понятия *Domain-Naming Operations Master* и *Domain-Naming FSMO* обозначают одно и то же — хозяина операций именования доменов.

Определенные работы в AD должны быть централизованными, поэтому мы и пришли к FSMO. Возьмем, к примеру, работу по созданию новых доменов. Предположим, что имеется домен Test.com и кто-то решил установить новый контроллер домена и посредством этого создать дочерний домен Ecoast.Test.com. Создание нового домена заставляет AD формировать множество структур данных, т.е. домен для Ecoast.Test.com, вызывая дополнительную работу для глобального каталога, изменения в базе данных AD всего леса и т.д. Теперь представим, что два человека приблизительно в одно и то же время пытаются создать новый домен по имени Ecoast.Test.com. Это могло бы стать настоящим кошмаром: родительский домен принимал бы конфликтующие запросы на модификацию базы данных AD, могли бы возникнуть потенциальные проблемы с безопасностью, а лес в целом мог бы прекратить функционирование.

Именование доменов: пример FSMO

Чтобы избежать ситуации дублирования имен и контролировать структуру леса, в Microsoft предложили, чтобы при создании нового домена один контроллер домена действовал как своего рода центральный информационный центр. Каждый раз, когда вы пытаетесь создать новый дочерний домен или новое дерево домена, AD DS

останавливается и находит в целом лесе один контроллер домена, который является "хранителем имен доменов". Говорят, что такой контроллер домена представляет собой роль FSMO именования доменов или хозяина операций именования доменов. Если служба AD DS на новом предполагаемом контроллере домена не может установить контакт с FSMO именования доменов, она категорически отказывается от любых дальнейших действий.

Запомните, что даже если вы имеете дело с предприятием мирового масштаба, имеющим десятки доменов, сотни офисов по всему миру, тысячи контроллеров доменов и сотни тысяч рабочих станций, в нем есть один и только один компьютер, который служит в качестве FSMO именования доменов. Если бы такой компьютер находился, скажем, в окинавском офисе, а вы сидели бы за сервером в нью-йоркском офисе и пытались создать новый домен в лесе, то ваш компьютер не мог бы продолжить работу до тех пор, пока не связался бы с компьютером в Окинаве и получил от него разрешение на создание нового домена.

Почему администраторы должны знать о ролях FSMO

В общем случае вам не придется постоянно помнить о контроллерах домена, которые исполняют функции FSMO внутри леса. Однако вам все же придется провести небольшое планирование того, какие контроллеры домена получат роли FSMO, и вы должны знать, как назначить конкретную роль FSMO отдельному контроллеру домена.

Это напоминает о том, что вам *придется* управлять ролями FSMO вручную. Среда AD автоматически выбирает конкретный контроллер домена, который должен исполнять каждую роль FSMO (первый установленный вами DC), однако не обладает достаточными возможностями найти его, если эти роли были перемещены. Рассмотрим, к примеру, такой сценарий. В вашей компании решили поэкспериментировать с AD и установить первый контроллер домена на заброшенном компьютере в испытательной среде — скажем, старой системе с процессором 1 ГГц и оперативной памятью 1 Гбайт. Они увидели, что AD работает довольно хорошо, и инициировали приобретение серьезного оборудования для контроллеров домена в производственной среде. После развертывания таких контроллеров домена складывается впечатление, что все работает просто замечательно.

Однажды эта идиллия закончилась: явившись на работу в какой-то из понедельников, сотрудники обнаружили, что выходные у AD, похоже, не закончились — среда AD не функционирует. Администраторы выяснили, что они не в состоянии создавать новые учетные записи пользователей или присоединять машины к домену. Кто-то пытается установить Exchange Server, но получает сообщение об отсутствии прав на изменение того, что называется *схемой*. Согласно плану, для кливлендского офиса требовалось создать новый дочерний домен, но это действие также было отклонено. Остальные контроллеры домена жалуются, что не могут найти PDC, а изменения в учетных записях вроде переустановки паролей не попадают на резервные контроллеры домена.

Что случилось? Как оказалось, в выходные кто-то экспериментировал в испытательной среде, и в ходе экспериментов ему понадобилась еще одна машина. Под руку ему подвернулся старенький компьютер с процессором 1 ГГц, который работал под управлением Windows Server 2003 и, похоже, функционировал в качестве конт-

роллера домена AD. Однако, по мнению воскресного простака, этот компьютер не должен был играть важной роли в сети, ведь фирма теперь располагала несколькими десятками крупных контроллеров домена, работающих в сети. В итоге экспериментатор очистил жесткий диск этой системы и установил на нем Linux.

Между тем по умолчанию AD назначает роли FSMO контроллеру домена, который был установлен первым. В этой небольшой истории система с процессором 1 ГГц на самом деле играла очень важную роль. И вот ее не стало. А среда AD недостаточно интеллектуальна, чтобы выявить данный факт и предложить на эту роль новый компьютер. Можно сказать, что наш "блистательный" лес утратил FSMO. Теперь задача заключается в том, чтобы перенести роли FSMO на другие контроллеры домена.

Важно знать, где именно в среде находятся и функционируют роли FSMO. Мы можем предложить несколько общих рекомендаций относительно того, где в домене и лесе должны находиться конкретные роли. Старайтесь, когда это только возможно, не разносить роли по нескольким контроллерам домена. По большей части основной контроллер корневого домена леса должен содержать роли PDC Emulator, Schema Master, Domain Naming Master и RID Master. При централизованном размещении этих ролей задача управления ими существенно облегчается. Формально роль хозяина инфраструктуры (Infrastructure Master) может функционировать на любом контроллере домена в среде, где каждый контроллер домена представляет собой также и сервер GC. Если вы работаете в среде с несколькими доменами, в которой не все контроллеры доменов являются серверами GC, то должны поместить роль Infrastructure Master на контроллер домена, где не хранится глобальный каталог. В последующих разделах мы рассмотрим каждую из ролей более подробно.

Глобальные каталоги

В данной главе мы повсеместно упоминали о глобальных каталогах. В итоге вы могли бы предположить, что глобальные каталоги относятся к категории FSMO. На самом деле это не так, поскольку глобальные каталоги не являются "одиночными". Хотя вы начинаете с одного глобального каталога, вы можете позволить другим контроллерам домена исполнять эту роль. Тем не менее, подобно ролям FSMO, важно знать, какие из контроллеров домена располагают этой ролью и где они находятся.

Для начала отметим, что первым является контроллер домена, созданный вами в начале. Поскольку все необходимые роли требуются изначально, роли FSMO и Global Catalog помещаются на этот первый сервер. Таким образом, возвращаясь к предыдущему примеру, призрак рабочей станции с процессором 1 ГГц снова возникнет перед нами, когда в процессе входа в систему понадобится глобальный каталог. Ошибки на других контроллерах домена и журналы событий рабочей станции, возможно, намекнут вам на такое обстоятельство.

Глобальный каталог содержит всего понемногу. Он хранит подмножество свойств или атрибутов для каждого объекта в лесе. Вспомните, что объектами могут быть пользователи, контакты, группы, компьютеры и другие сущности, описанные в Active Directory. Следовательно, все контроллеры домена, являющиеся серверами глобального каталога, содержат персональную информацию для каждого пользователя в лесе, даже если этот глобальный каталог относится не к тому же самому домену, которому принадлежит пользователь.

Пример из практики

Вывод из эксплуатации с помощью DCPROMO и AD DS

Рассказанная выше история о контроллере домена на базе машины с процессором 1 ГГц вовсе не фантастична. Нам приходилось сталкиваться с ситуациями, когда неосведомленный администратор очищал жесткие диски вышедшего из строя контроллера домена, т.к. у него было в запасе пара контроллеров домена с репликой, способных поддержать функционирование домена, под предлогом "все равно он уже устарел". Просто так случалось, что этот контроллер домена оказывался первым в домене.

Возможна одна ситуация, при которой AD автоматически переносит роль FSMO — когда вы используете `DCPROMO` или AD DS для понижения контроллера домена, удерживающего одну или несколько ролей FSMO, до сервера-члена. Это средство находит другой подходящий контроллер домена и переносит на него роли FSMO. В таком случае вывод из эксплуатации старого контроллера домена не приводит к возникновению проблем. Таким образом, полезной оказывается следующая рекомендация: когда вы хотите избавиться от какого-то контроллера домена, всегда применяйте `DCPROMO` или AD DS для вывода его из эксплуатации и только после этого запускайте утилиту `fdisk`.

Если происходит авария, и у вас нет возможности восстановить систему, помните о методах, обсуждаемых ниже, которые предназначены для переноса ролей FSMO из отказавшего контроллера домена.

Сколько необходимо глобальных каталогов? Обычно это зависит от количества имеющихся сайтов. Существует много вариантов применения GC. Наиболее заметным является содействие процессу входа в систему. Если всем пользователям внутри леса с несколькими доменами назначаются основные имена пользователей (user principal name — UPN), такие как `bdavis@test.com`, то контроллеры домена должны быть способны определять, какому домену эти имена в действительности принадлежат. Информацию подобного рода обеспечивает глобальный каталог. Поэтому было бы неплохо, если бы глобальный каталог находился в сайте, где пользователи входят в домен.

Поскольку глобальный каталог содержит всю нужную информацию, приложениям, управляемым Active Directory, например, Exchange Server, необходим глобальный каталог. Exchange Server использует глобальный каталог для нахождения всех получателей и членов групп рассылки в организации. Было бы хорошо, если экземпляры Exchange Server располагали бы GC на том же сайте.

Вы должны сопоставить наличие этой возможности с потенциальным трафиком репликации, который серверы будут принимать от других доменов. Все домены будут реплицировать свою доменную информацию в каждый глобальный каталог. Как правило, важность глобального каталога для входа и функционирования Exchange Server значительно перевешивает соображение, касающееся трафика репликации.

Приняв решение по необходимому количеству GC, вам понадобится войти в систему как администратору предприятия и включить контроллеры домена внутри леса. Это делается с помощью консоли Active Directory Sites and Services. Пройдя через контейнер Sites (Сайты) до конкретного сайта и далее до объекта Servers

(Серверы), вы увидите, что в диалоговом окне NTDS settings Properties (Свойства параметров NTDS) отмечен флажок Global Catalog (Глобальный каталог), как показано на рис. 24.10.

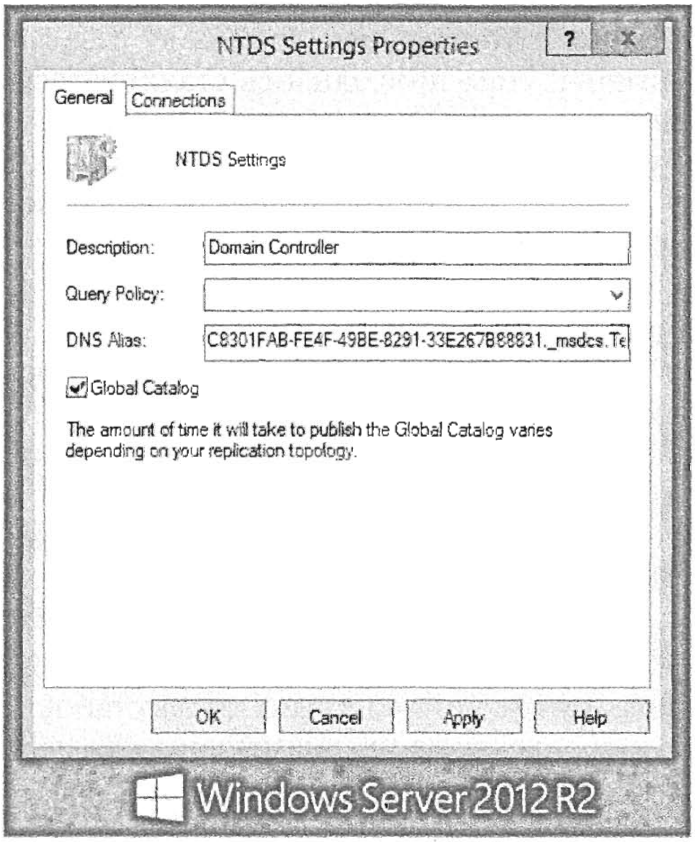


Рис. 24.10. Включение глобального каталога

Роли FSMO

В Active Directory предусмотрено пять ролей FSMO:

- Schema Master (Хозяин схемы)
- Domain Naming Master (Хозяин именования доменов)
- Relative Identifier (RID) Master (Хозяин относительных идентификаторов (RID))
- PDC Emulator (Эмулятор основного контроллера домена)
- Infrastructure Master (Хозяин инфраструктуры)

Во всем лесе имеется только одна FSMO-роль Schema Master и, аналогично, только одна FSMO-роль Domain Naming Master. Однако у каждого домена в лесе есть собственные роли RID Master, PDC Emulator и Infrastructure Master.

Мы рассмотрим функции каждой из этих ролей, а также требования, связанные с их назначением контроллерам домена.

Роль Schema Master

Схема является термином для описания структуры базы данных AD, т.е. полей. Она служит определением таких элементов в базе данных, как имена пользователей, пароли и т.д. В каком-то смысле схема представляет собой справочник для Active Directory.

Анализ схемы с помощью оснастки Active Directory Schema

Схему можно просмотреть с помощью оснастки Active Directory Schema. Однако она не входит в состав меню Administrative Tools (Администрирование); чтобы запустить ее, придется выполнить описанные ниже шаги.

1. Откройте окно командной строки и введите **`regsvr32 schmmgmt.dll`**. Отобразится сообщение DllRegisterServer in schmmgmt.dll succeeded (Служба `DllRegisterServer` в `schmmgmt.dll` успешно запущена). Чтобы очистить его, щелкните на кнопке OK.
2. Откройте диалоговое окно Run (Выполнить), введите **`mmc /a`** и нажмите <Enter>, чтобы запустить консоль управления Microsoft (Microsoft Management Console) в авторском режиме.
3. Выберите в меню File (Файл) пункт Add/Remove Snap-in (Добавить или удалить оснастку).
4. Выберите оснастку Active Directory Schema, щелкните на кнопке Add (Добавить) и затем на кнопке OK. Оснастка Active Directory Schema сейчас загружена и готова к использованию.

   Вы увидите окно, подобное показанному на рис. 24.11.

   Здесь выделена часть схемы, которая говорит о наличии атрибута под названием `userPrincipalName`, представляющего собой одно из доступных пользователю имен входа.

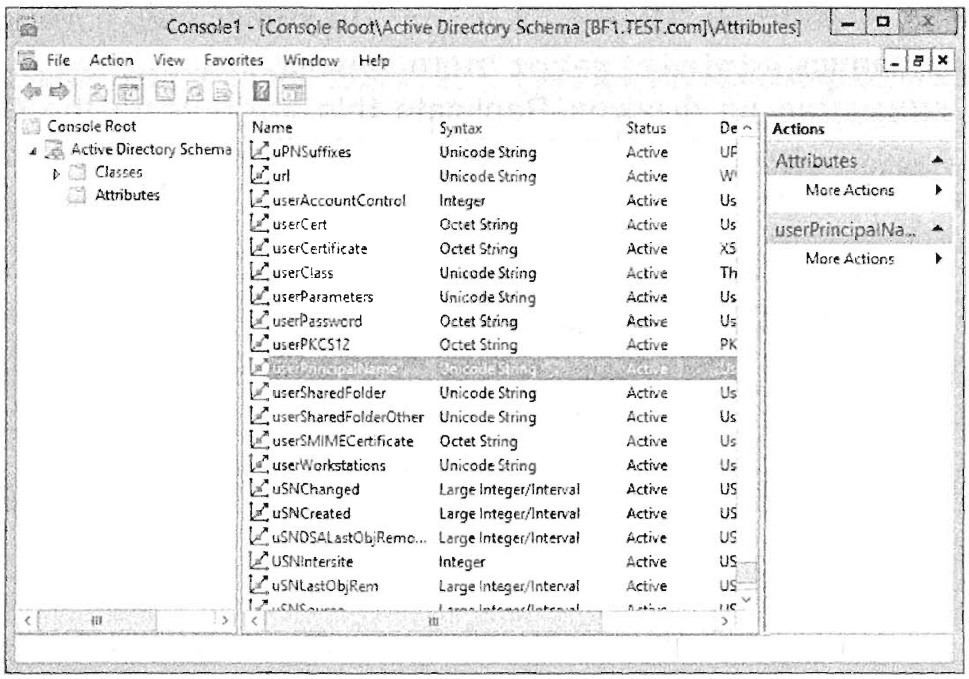


Рис. 24.11. Оснастка Active Directory Schema

5. Дважды щелкните на атрибуте `userPrincipalName`, в результате чего откроется диалоговое окно с его свойствами, но они, скорее всего, будут недоступными для изменения, даже если вы являетесь членом группы `Enterprise Admins`. Вспомните, что даже администраторы предприятия не могут модифицировать схему — для этого необходимо быть членом группы `Schema Admins`. Но если вы администратор схемы, то увидите диалоговое окно свойств, где все свойства доступны (рис. 24.12).

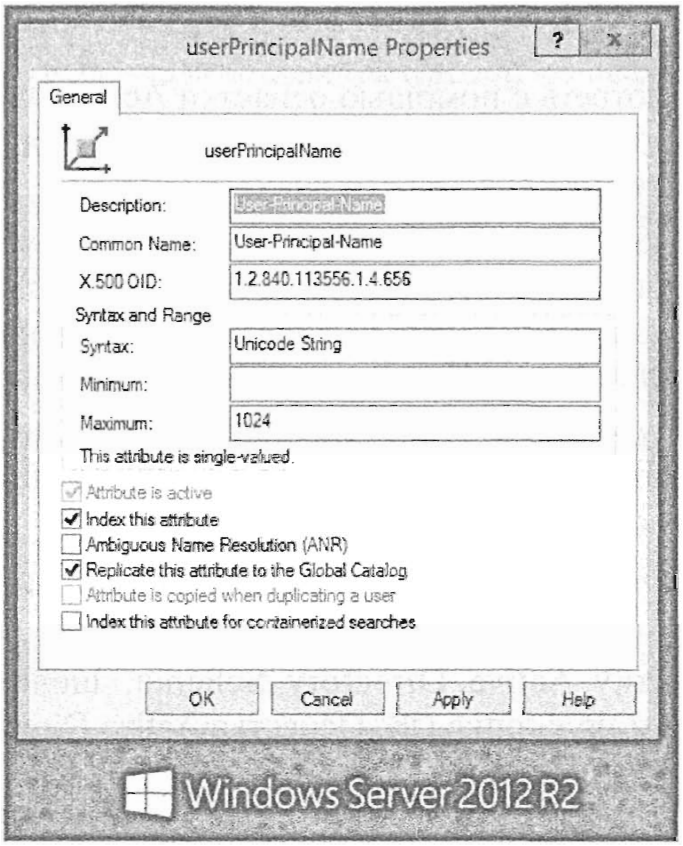


Рис. 24.12. Диалоговое окно свойств атрибута `userPrincipalName`

Подобно администратору предприятия, администратор схемы — это учетная запись пользователя, которая является членом определенной группы в корневом домене леса. Группа называется `Schema Admins`. По умолчанию в данной группе находится учетная запись `Administrator` этого домена.

Обратите внимание на флажок Replicate this attribute to the Global Catalog (Реплицировать этот атрибут в глобальный каталог). Этот флажок позволяет управлять тем, какие атрибуты можно реплицировать в GC.

Отмена регистрации DLL-библиотеки

Чтобы удалить оснастку Active Directory Schema из сервера по причинам, связанным с безопасностью, выполните следующую команду:

```
REGSVR32 /u C:\Windows\System32\schmmgmt.dll
```

Схема и Active Directory

Часто ли вы будете изменять схему? Значительными ли будут изменения? Вероятно, нет. Но есть ряд моментов, которые вы должны иметь в виду.

Во-первых, вспомните, что для всего леса существует только одна схема; бессмысленно говорить об изменении схемы для отдельного домена, т.к. любые изменения в схеме являются изменениями схемы всего леса. Таким образом, внесение даже незначительного изменения в схему повлияет на каждый контроллер домена во всех доменах внутри леса, поскольку все контроллеры доменов должны быть уведомлены об изменениях и, следовательно, должны зарезервировать в своей копии схемы место для новых элементов схемы, что потребует определенного времени работы центрального процессора и дисков.

Во-вторых, когда вы будете изменять схему? Обычно единственным действием, приводящим к изменению схемы, будет добавление новых серверных приложений, таких как Exchange Server 2013 или других приложений подобного рода, которые разрабатывались с учетом Active Directory. Продукты Microsoft будут самостоятельно управлять обновлением схемы в ходе установки. Делать это вручную не придется. В главе 25 вы ознакомитесь с использованием утилиты `adprep` с целью подготовки доменов предшествующих версий для Windows Server 2012 R2. Это также будет модифицировать схему.

Поддержка упорядоченного внесения изменений в схему

Ввиду того, что изменения схемы влияют на лес в целом, можно обоснованно утверждать, что схема *меняется*. Желательно, чтобы эти изменения носили как можно более упорядоченный характер. Нет ничего хуже, когда два человека пытаются модифицировать схему в одно и то же время.

Рис. 24.13. Просмотр роли хозяина схемы

По этой причине, а также потому, что для целого леса предусмотрена только одна схема, во всем лесу существует лишь один компьютер, который может утвердить изменения в схеме. Говорят, что такой компьютер играет роль *хозяина схемы*. По умолчанию AD помещает роль хозяина схемы на первый контроллер домена, который вы установили в первом домене леса. Таким образом, первый создаваемый контроллер домена должен быть очень хорошо защищен!

Посмотреть, какой компьютер является мастером схемы, можно следующим образом.

1. Щелкните правой кнопкой мыши на объекте Active Directory Schema (Схема Active Directory).
2. Выберите в контекстном меню пункт Schema Master (Хозяин схемы), чтобы открыть диалоговое окно, подобное приведенному на рис. 24.13.

Для перемещения роли хозяина схемы вы должны быть администратором схемы.

Планирование изменений и конфликтов схемы

Прежде чем завершить рассмотрение схемы, мы изложим свои соображения относительно того, как она повлияет на вашу организацию. Приложений, управляемых AD, совсем немного. Но сейчас давайте посмотрим, что случится, если внутри схемы возникнут конфликты. Предположим, что вы работаете в крупном университете с большим количеством независимых факультетов. Лес этого университета состоит из многих доменов (Chemistry, English, Microbiology, Astronomy, Music, Geology и других), причем все они входят в состав единственного леса и, следовательно, имеют только одну схему. А теперь представим, что домен Astronomy получил в свое

распоряжение замечательное новое приложение, которое поможет профессорам, присоединенным к этому домену, успешно проводить исследования, и они решили поместить его в AD. Это приложение добавляет в схему несколько десятков новых элементов, в числе которых поле Magnitude, где хранится яркость звезды. Далее предположим, что сотрудники из домена Geology позже приобрели не менее замечательное новое приложение, которое содействует в проведении сейсмологических исследований и также добавляет в схему несколько элементов, в частности, поле Magnitude, в котором хранится информация о силе землетрясения. Что произойдет, когда в домене Geology попытаются установить приложение, которое желает создать в схеме поле с уже существующим именем? Если в двух словах, то результат такого конфликта зависит от обстоятельств и не все возможные последствия будут положительными.

Наше мнение таково: при первой установке своего приложения сотрудники домена Geology *должны были знать*, что оно будет конфликтовать с существующим приложением. Но как они могли узнать об этом? Вообще говоря (и это может вам не понравиться), для каждого леса должна быть предусмотрена постоянно действующая экспериментальная среда с одним или двумя контроллерами домена, на которых функционирует рабочая, но независимая версия леса. Прежде чем вводить в эксплуатацию какие-либо серверные приложения, они должны быть проверены в этой экспериментальной среде, чтобы выяснить, не создают ли они такие изменения в схеме, которые приводят к возникновению проблем в AD.

Что об этом можно сказать? Домены Astronomy и Geology привыкли действовать независимо друг от друга, не спрашивая друг у друга разрешения на запуск приложений? Да, в это легко поверить: у исследовательских и образовательных учреждений действительно существует такая традиция. Но после того как вы приняли решение объединить все составные части организации в единый лес, вашим организационным компонентам придется более тесно взаимодействовать друг с другом, чтобы все работало нормально. Кроме того, кто-то должен отвечать за обеспечение постоянного функционирования экспериментальной среды, а это означает ее комплектование кадрами, помещением, оборудованием и программным обеспечением. Теперь утверждение о том, что Windows снижает совокупную стоимость владения, не выглядит особенно убедительным. Но, по крайней мере, операционная система Windows Server 2012 R2 предлагает гипервизор Hyper-V. Экспериментальная среда вполне заслуживает того, чтобы приобрести ее и выполнять проверки с ее помощью.

По существу в этом случае AD является просто еще одной порцией программного обеспечения, которая сообщает о том, что если вы хотите ею пользоваться, то вам придется изменить подход к работе. Это представляется шагом назад, как если бы изготовитель мышей заявил: “Да, мы сожалеем о том, что наша революционная конструкция мыши не соответствует анатомическому строению вашей ладони. Может вам прибегнуть к хирургической операции?”

Роль Domain Naming Master

Вы уже сталкивались с этой ролью FSMO — она применялась ранее в качестве примера при объяснении, для чего необходим хозяин операций. Во всем лесе имеется только одна такая роль. Как и в случае с хозяином схемы, AD помещает роль Domain Naming Master на первый контроллер домена в первом домене.

Размещение Domain Naming Master

Роль Domain Naming Master должна помещаться только на контроллер домена, который также является сервером глобального каталога. По-видимому, разработчики AD проявили здесь некоторую лень и решили, что поскольку глобальному каталогу известна информация со всего леса, роль Domain Naming Master могла бы воспользоваться этим знанием.

Роль RID Master

Одной из функций, которые должен выполнять любой контроллер домена AD, работающий в собственном режиме, является создание новых учетных записей (пользователей и компьютеров) без обращения к какому-то "центральному" или "основному" контроллеру домена. В мире Windows Server все что угодно имеет уникальный идентификатор, который называется *идентификатором безопасности* (security ID — SID). Идентификаторы SID выглядят следующим образом:

S-1-5-21-*D1-D2-D3-RID*

Конструкция 1-5-21 применима ко всем SID. Что же касается *D1*, *D2* и *D3*, то это в действительности три генерируемых случайным образом 32-битовых числа. Когда среда AD впервые создает домен, она генерирует эти три уникальных 32-битовых числа, и они остаются постоянными для любого SID, формируемого в данном домене. Речь идет не только об отдельном сочетании D1/D2/D3 для домена — локальный диспетчер учетных записей безопасности (Security Account Manager — SAM) на рабочей станции или сервере-члене также имеет собственный набор из трех уникальных 32-битовых чисел.

Таким образом, например, если вы создали домен по имени Bigfirm.com и оказалось, что для него были сгенерированы D1=55, D2=1044 и D3=7, то каждый SID в Test.com будет выглядеть так: S-1-5-21-55-1044-7-*значение,* где *значение* — это 32-битовое число. Другими словами, все идентификаторы SID в домене идентичны за исключением последних 32 битов. Последние 32 бита отражают только *относительное* отличие между идентификаторами SID, поэтому их назвали *относительными идентификаторами* (relative identifier — RID). Некоторые идентификаторы RID являются фиксированными, например, SID для стандартной учетной записи `Administrator` на компьютере.

Как бы то ни было, если контроллер домена нуждается в генерации нового SID, то ему *известно*, какой будет первая часть этого SID. Контроллеру домена необходим лишь уникальный RID. Следовательно, в каждом домене имеется один контроллер домена, который поддерживает пулы, состоящие из 500 идентификаторов RID. После этого каждый контроллер домена сможет создавать до 500 учетных записей, прежде чем ему придется снова обратиться к этому центральному контроллеру домена, который выделит еще 500 идентификаторов RID. Компьютер, который выдает такие пакеты по 500 идентификаторов RID, называется хозяином RID, или RID FSMO. По умолчанию им будет первый контроллер домена, установленный *в домене*. Обратите внимание, что хозяин RID предусмотрен в каждом домене, а не один на весь лес.

Назначение роли RID Master можно просмотреть в оснастке Active Directory Users and Computers. В окне этой оснастке щелкните правой кнопкой мыши на объекте домена и выберите в контекстном меню пункт Operations Masters (Хозяева операций). В диалоговом окне на рис. 24.14 видно, что роль RID Master назначена BF1.Test.com. На вкладках PDC и Infrastructure (Инфраструктура) отображаются назначения ролей PDC Emulator и Infrastructure Master для данного домена.

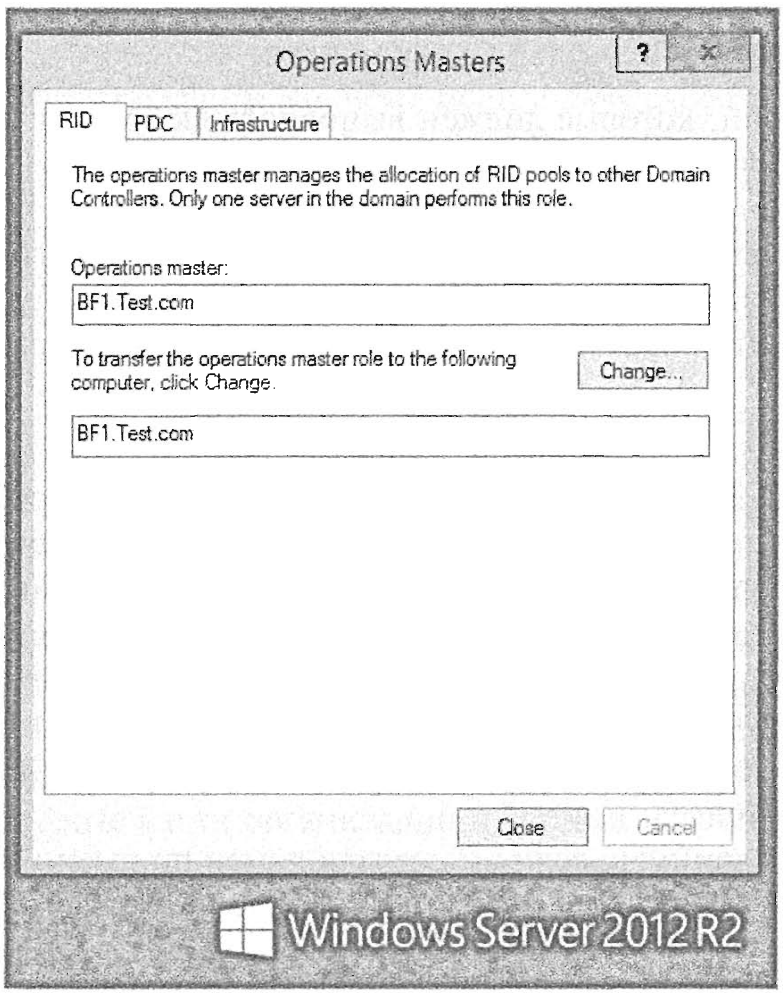


Рис. 24.14. Просмотр ролей RID Master, PDC Emulator и Infrastructure Master

Роль Infrastructure Master

По мнению специалистов из Microsoft, в сети с несколькими доменами трудно быстро отразить изменения в учетных записях групп и пользователей по всем доменам. Так, вы могли переименовать пользователя или поместить пользователя в группу внутри администрируемого вами домена, но в течение какого-то времени это изменение может быть не видно в других доменах. Период времени основан на репликации между контроллерами домена. В случае единственного сайта с парой контроллеров домена период может составлять всего пять минут. Внутри одного сайта с большим количеством контроллеров домена этот период может достигать 15 минут. Если репликация происходит между сайтами, она зависит от таких параметров репликации связей сайтов, как интервал и график проведения. Данный процесс ускоряется так называемым *хозяином инфраструктуры* (Infrastructure Master). Его роль можно изменить таким же способом, каким изменялась роль RID Master. Предусмотрен один хозяин инфраструктуры на домен.

Размещение роли Infrastructure Master

Для роли Infrastructure Master характерна одна странность: ее нельзя помещать на контроллер домена, который является сервером глобального каталога, если только лес не содержит единственный домен. Вполне нормально, если все контроллеры домена в домене являются глобальными каталогами. Самый первый настроенный контроллер домена принимает на себя все пять ролей Operations Master, а это значит, что изначально хозяин инфраструктуры находится на сервере глобального каталога. Это хорошо до тех пор, пока имеется один домен, и, конечно же, справедливо и при наличии только *одного* контроллера домена. В лесе с единственным доменом глобальный каталог будет содержать ту же самую информацию, что и этот единственный домен. Когда появляется несколько доменов, самое время переназначить роль Infrastructure Master другому контроллеру домена.

Роль PDC Emulator

Наконец, есть еще роль PDC Emulator. Она очень важна.

Произвольно выбранный из числа контроллеров домена AD принято считать "основным" контроллером домена. И хотя домен AD функционирует в смешанном режиме, роль PDC Emulator — это нечто большее, чем просто эмулятор; это единственный контроллер домена, который может принимать изменения в учетных записях.

Но не значит ли это, что эмулятор PDC утрачивает свою актуальность, как только вы переходите в собственный режим, и уже нет компьютеров с версиями ОС, предшествующими Windows 2000 Server? Ничуть. Эмулятор PDC по-прежнему выполняет две чрезвычайно важные функции. Поскольку репликация уже обсуждалась ранее в книге, вам наверняка известно, что репликация изменений в AD занимает определенное время — иногда весьма значительное. Предположим, что вы работаете в Сент-Луисе и хотите изменить свой пароль. Вы звоните в службу технической поддержки компании, которая находится в Оттаве (что вам неизвестно). Сотрудник службы технической поддержки изменяет ваш пароль, и, кажется, все должно быть хорошо.

Но на каком контроллере домена этот сотрудник изменил ваш пароль? Вероятно, он сделал это на контроллере домена, который был к нему физически ближе, т.е. на контроллере домена, находящемся в Оттаве. Таким образом, контроллеру домена в Оттаве известен ваш новый пароль. Но сколько времени пройдет до того, как локальные контроллеры домена в Сент-Луисе узнают ваш новый пароль? Речь может идти о нескольких часах. Значит ли это, что вам придется в течение нескольких часов философски созерцать потолок, ожидая, пока ваш новый пароль доберется до Сент-Луиса? Действительно, если бы речь шла о каком-то другом атрибуте помимо пароля, то ответ был бы утвердительным, но пароли являются особым случаем.

Когда администратор изменяет пароль на каком-то контроллере домена, этот контроллер домена немедленно связывается с системой, действующей в качестве эмулятора PDC для данного домена. Таким образом, эмулятору PDC почти всегда известны наиболее актуальные пароли. Когда вы пытаетесь войти в домен, то на самом деле входите в систему локального контроллера домена. Когда вы сообщаете свой новый пароль, локальный контроллер домена поначалу склонен отказать во входе, потому что указанный вами пароль не соответствует тому, которым располагает контроллер домена. Но прежде чем отказать во входе, локальный контрол-

лер домена подключается к эмулятору PDC для этого домена и повторяет проверку пароля; если пароль, который вы предоставили локальному контроллеру домена, совпадает с новым паролем, имеющимся у эмулятора PDC, то вы сможете войти в домен.

Такая "высокоприоритетная репликация" также проводится для еще одного пользовательского атрибута — разблокировок учетных записей. Когда пользователь забывает свой пароль и пытается войти с указанием неправильного пароля снова и снова, он не только нуждается в новом пароле; возможно, действия этого пользователя привели к блокированию его учетной записи. Таким образом, кроме переустановки пароля для пользователя администратору может потребоваться разблокировать его учетную запись. Немедленная репликация нового пароля без репликации разблокировки учетной записи вряд ли окажется особенно полезной.

Это одна важная задача роли PDC Emulator. А в чем заключается другая задача? Об этом речь пойдет в разделе "Синхронизация времени" далее в главе.

Передача ролей FSMO

Если вы хотите переместить назначение FSMO на другой контроллер домена, то должны выполнить передачу роли. Процесс довольно прост. Как было показано выше, назначение FSMO можно просмотреть в трех разных оснастках консоли MMC:

- оснастка Active Directory Domains and Trusts управляет ролью Domain Naming Master;
- оснастка Active Directory Schema управляет ролью Schema Master;
- оснастка Active Directory Users and Computers управляет ролями PDC Emulator, RID Master и Infrastructure Master.

Таким образом, для передачи роли вы можете выполнить описанную ниже процедуру.

1. Откройте оснастку для желаемой роли.
2. Укажите целевой контроллер домена, который примет назначение этой роли.
   а. Просто откройте соответствующую оснастку.
   б. Щелкните правой кнопкой мыши на верхнем объекте в оснастке MMC.
   в. Выберите в контекстном меню пункт Connect to Domain Controller (Подключиться к контроллеру домена).

      На экране появится диалоговое окно, показанное на рис. 24.15. В нем вы можете выбрать целевой контроллер домена и щелкнуть на кнопке OK.
3. Просмотрите роль, щелкнув правой кнопкой мыши на верхнем объекте дерева в левой панели и выбрав в контекстном меню пункт Operations Masters (Хозяева операций).

   Новое диалоговое окно отобразит текущее назначение FSMO. На представленном ранее рис. 24.14 показаны вкладки для ролей, относящихся к доменам (RID Master, PDC Emulator и Infrastructure Master). На рис. 24.13 можно видеть роль Schema Master. В каждом из этих диалоговых окон нижнее поле отражает целевой контроллер домена.

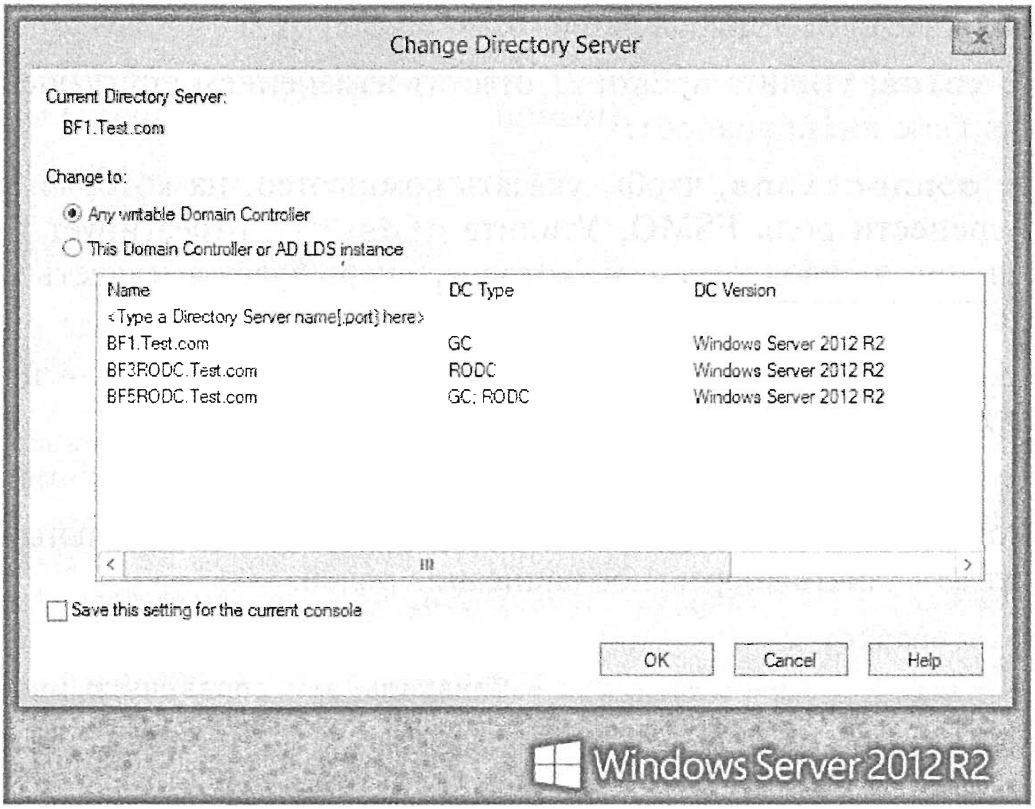


Рис. 24.15. Изменение целевого контроллера домена

4. Чтобы перенести роль на целевой контроллер домена, щелкните на кнопке Change (Изменить).

Чтобы перенести роль RID Master, PDC Emulator или Infrastructure Master для заданного домена, вы должны быть администратором этого домена. Чтобы перенести роль Domain Naming Master, вы должны быть администратором предприятия, а для переноса роли Schema Master — администратором схемы.

Как видите, передавать роли FSMO посредством графического пользовательского интерфейса чрезвычайно просто. Однако есть одно условие: вы можете применять графический пользовательский интерфейс для передачи роли FSMO, *если функционирует текущий компьютера FSMO*. Если вы обработали с помощью `fdisk` жесткий диск компьютера, который действовал в качестве хозяина именования доменов, то некому будет "утвердить" передачу роли на другой компьютер. В таком случае вы не просто *переносите* роль Operations Master — вы должны, выражаясь языком пиратов, "захватить хозяина".

Если эмулятор PDC или хозяин инфраструктуры переходит в автономный режим, вы можете совершенно безопасно перенести роли FSMO на другой компьютер, причем действительно это сделать посредством инструмента с графическим пользовательским интерфейсом. Он сообщит о том, что хозяин операций находится в автономном режиме, поэтому вы не можете перенести роль, но смело игнорируйте это сообщение и щелкайте на кнопке Change (Изменить).

Но чтобы захватить роль RID Master, Domain Naming Master или Schema Master, вам придется использовать инструмент командной строки `ntdsutil`. С помощью `ntdsutil` можно также переносить роли FSMO, но графический пользовательский интерфейс намного проще. Командную строку можно применять для администрирования установленных копий Server Core. Начните с ввода **`ntdsutil`** в командной строке.

Затем выполните следующие действия.

1. Введите **roles**; утилита ntdsutil ответит изменением приглашения на ввод на такое: fsmo maintenance:.
2. Введите **connections**, чтобы указать компьютер, на который вы собираетесь перенести роль FSMO. Утилита ntdsutil отреагирует изменением приглашения на ввод команды, которое теперь будет выглядеть так: server connections:.
3. Введите **connect to server** ***имя_сервера***, где *имя_сервера* — целевой контроллер домена, на который вы хотите перенести роль FSMO.
4. Введите **quit**, чтобы возвратиться к приглашению fsmo maintenance:.
5. Чтобы отобразить возможные команды, введите вопросительный знак. Это позволит вам узнать корректное написание ролей.

```
fsmo maintenance: ?
?                                - Показать эту справочную информацию
Connections                      - Подключиться к определенному
                                   экземпляру AD DC/LDS
Help                             - Показать эту справочную информацию
Quit                             - Возвратиться в предыдущее меню
Seize infrastructure master      - Переопредлить роль инфраструктуры на
                                   подключенном сервере
Seize naming master              - Переопредлить роль Domain Naming
                                   Master на подключенном сервере
Seize PDC                        - Переопредлить роль PDC Emulator на
                                   подключенном сервере
Seize RID master                 - Переопредлить роль RID Master на
                                   подключенном сервере
Seize schema master              - Переопредлить роль Schema Master на
                                   подключенном сервере
Select operation target          - Выбрать сайты, серверы, домены, роли
                                   и контексты именования
Transfer infrastructure master   - Сделать подключенный сервер хозяином
                                   инфраструктуры
Transfer naming master           - Сделать подключенный сервер хозяином
                                   именования
Transfer PDC                     - Сделать подключенный сервер
                                   эмулятором PDC
Transfer RID master              - Сделать подключенный сервер хозяином RID
Transfer schema master           - Сделать подключенный сервер хозяином
                                   схемы
```

6. Введите **transfer** ***хозяин_роли_fsmo***. Если утилита ntdsutil обнаружит, что не может связаться с текущим компьютером FSMO для получения одобрения, откроется диалоговое окно с запросом подтверждения. Подтвердите, что вы действительно хотите выполнить перенос.
7. Если не появились какие-то сообщения об ошибках, то вы свою задачу выполнили. Но если перенос роли не удался, введите **seize** ***хозяин_роли_fsmo***. Такое действие является чуть более радикальным, однако оно всегда приводит к требуемому результату.
8. Два раза введите **quit**, чтобы завершить работу.

Ниже приведен пример сеанса, в ходе которого мы захватили роль RID Master из компьютера Bf2.Test.com и перенесли ее на компьютер Bf1.Test.com (вводимые с клавиатуры команды выделены полужирным).

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server bf1.test.com
Binding to bf1.test.com ...
Connected to bf1.test.com using credentials of locally logged on user.
Привязка к bf1.test.com ...
Подключение к bf1.test.com с применением учетных данных пользователя,
локально вошедшего в систему.
server connections: quitfsmo maintenance: transfer rid master
ldap_modify_sW error 0x34(52 (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-03210CB1, problem 5002
(UNAVAILABLE), data 1722

Win32 error returned is 0x20af(The requested FSMO operation failed.
The current FSMO holder could not be contacted.)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Server "bf1.test.com" knows about 5 roles
Schema - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
Naming Master - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,
DC=comPDC - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
RID - CN=NTDS Settings,CN=BF2,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
Infrastructure - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com

Ошибка ldap_modify_sW с кодом 0x34(52 (Не доступно).
Расширенным сообщением об ошибке ldap является 000020AF:
SvcErr: DSID-03210CB1, проблема 5002
(НЕ ДОСТУПНО), данные 1722
Возвращена ошибка Win32 с кодом 0x20af(Отказ запрошенной операции FSMO.
Не удается связаться с текущим компьютером FSMO.)
В зависимости от кода ошибки это может указывать на ошибку подключения,
ldap или переноса роли.
Серверу bf1.test.com известно о 5 ролях
Хозяин схемы - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
Хозяин именования доменов - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=comPDC -
CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,
CN=Configuration,DC=test,DC=com
Хозяин RID - CN=NTDS Settings,CN=BF2,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
Хозяин инфраструктуры - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com

fsmo maintenance:
```

Похоже, что перенос не удался. Давайте попробуем выполнить захват.

```
fsmo maintenance: seize rid master
Attempting safe transfer of RID FSMO before seizure.
ldap_modify_sW error 0x34(52 (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-03210CB1, problem 5002
(UNAVAILABLE), data 1722
Win32 error returned is 0x20af(The requested FSMO operation failed.
The current FSMO holder could not be contacted.)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of RID FSMO failed, proceeding with seizure ...
Searching for highest rid pool in domain
Server "bf1.test.com" knows about 5 roles
Schema - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,
CN=Configuration,DC=bigfirm,DC=com
Naming Master - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
PDC - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
RID - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=bigfirm,DC=com
Infrastructure - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
```

Попытка безопасного переноса роли RID перед захватом.
Ошибка ldap_modify_sW с кодом 0x34(52 (Не доступно).
Расширенным сообщением об ошибке ldap является 000020AF:
SvcErr: DSID-03210CB1, проблема 5002
(НЕ ДОСТУПНО), данные 1722
Возвращена ошибка Win32 с кодом 0x20af(Отказ запрошенной операции FSMO.
Не удается связаться с текущим компьютером FSMO.)
В зависимости от кода ошибки это может указывать на ошибку подключения,
ldap или переноса роли.
Перенос роли RID не удался, выполнение захвата ...
Поиск наибольшего пула индексов rid в домене
Серверу bf1.test.com" известно о 5 ролях
Хозяин схемы - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,
CN=Configuration,DC=bigfirm,DC=com
Хозяин именования доменов - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
PDC - CN=NTDS Settings,CN=BF1,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com
Хозяин RID - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,CN=Sites,
CN=Configuration,DC=bigfirm,DC=com
Хозяин инфраструктуры - CN=NTDS Settings,CN=BF1,CN=Servers,
CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=test,DC=com

```
fsmo maintenance:
```

Захват и приведение в порядок

Если вы захватили хозяина RID, именования доменов или схемы, позаботьтесь о том, чтобы старый хозяин никогда больше не появлялся в сети, иначе будет нарушена нормальная работа AD. Если этот контроллер домена снова станет доступным, он будет считать, что по-прежнему располагает той или иной ролью FSMO. Таким образом, неизбежно возникнет конкуренция между старым и новым хозяином.

Настоятельно рекомендуется изъять сетевой кабель и очистить жесткий диск. Мы рекомендуем загрузиться с установочного компакт-диска, чтобы удалить системный раздел для последующей чистой установки ОС.

Синхронизация времени

Когда речь идет о репликации и доверительных отношениях, среда AD нуждается в том, чтобы все ее контроллеры доменов согласовали текущее время и дату. *Точное* соответствие не требуется, но они должны быть достаточно близки — протокол Kerberos не сможет работать, если расхождение в показаниях времени между контроллером домена и системой, пытающейся использовать этот контроллер домена для аутентификации, окажется бо́льшим пяти минут. Серверы Windows включают службу под названием Windows Time (Время Windows), которая обеспечивает синхронизацию времени на всех рабочих станциях и серверах Windows.

Машины в AD остаются в синхронизированном состоянии следующим образом. Эмулятор PDC корня леса, т.е. первый контроллер первого созданного домена, представляет собой главный сервер времени (Master Time Server Dude). Все другие серверы автоматически создают иерархию, похожую на "телефонное дерево", для распространения информации о синхронизации времени. Каждый, кто находится в этой иерархической структуре ниже самого высокого уровня, автоматически получает сигналы синхронизации времени от вышестоящего уровня в иерархии, как описано ниже.

- Серверы-члены и рабочие станции синхронизируются с контроллером домена, который обеспечил их вхождение в систему.
- Контроллеры домена синхронизируются с контроллером домена в их домене, на котором находится роль PDC Emulator.
- Если в лесе имеется более одного домена, то в нем будет несколько эмуляторов PDC, т.к. каждый домен располагает своим эмулятором PDC.

  Эмуляторы PDC должны согласовывать между собой показания времени, для чего они выбирают один эмулятор PDC в качестве "источника" — эмулятор PDC для *первого* домена в лесе, т.е. корень леса. Таким образом, окончательным центром синхронизации времени является именно эмулятор PDC для корневого домена леса.

А кто синхронизирует время для верхнего уровня этой иерархии, т.е. эмулятора PDC корневого домена леса?

Прежде всего, как ни странно, синхронизировать этот эмулятор PDC нет нужды. Главное для AD — чтобы все серверы имели одно и то же показание времени. Конечно, было бы неплохо, чтобы они располагали *действительным* временем, но это не обязательно. Если все предприятие начинает работу на 10 минут раньше, то в AD не возникнет никаких проблем, если *все* серверы также начнут работу на 10 минут раньше.

Часовые пояса и синхронизация времени

Однако *очень важно* правильно установить часовые пояса на всех системах! Среда AD хранит и синхронизирует время в показаниях "универсального времени" — в основу основ AD положено гринвичское время. Операционные системы Windows используют часовые пояса для понимания времени системных часов и отображения времени, которое будет понятно вам. Таким образом, если оставить везде тихоокеанское поясное время и затем установить системные часы в показания местного времени, то с точки зрения каждой из систем расхождения в универсальном времени достигали бы нескольких часов, и синхронизация оказалась бы невозможной. Ситуация подобного рода поставила бы вас в тупик, т.к. показания времени на контроллере домена и рабочей станции выглядели бы идентичными (вы ведь не знаете, что у них установлены разные часовые пояса), но взаимодействовать они отказываются. Этого бы не случилось, если бы вы могли просмотреть, каковы в действительности представления контроллера домена и рабочей станции об *универсальном* времени. Быстро выяснить часовой пояс системы можно, открыв окно командной строки и введя команду **w32tm /tz**.

Но поскольку мы имеем именно такую иерархию, давайте сделаем все как надо и синхронизируем эмулятор PDC корневого домена от какого-то надежного источника. Вы могли бы приобрести устройство с протоколом сетевого времени (Network Time Protocol — NTP), которое синхронизирует свое время с системой глобального позиционирования (Global Positioning System — GPS). С другой стороны, вовсе необязательно приобретать дорогостоящие устройства: вы можете всего лишь позволить Интернету установить время.

Набор стандартов Интернета включает способ распространения информации о времени, который называется простым протоколом сетевого времени (Simple Network Time Protocol — SNTP) и описан в документе RFC 1769, доступном по адресу `www.faqs.org/rfcs/rfc1769.html`. Очень многие машины в Интернете служат NTP-серверами, и будут предоставлять актуальную информацию о времени любой машине с выполняющимся NTP-клиентом. К счастью, в системах Windows Server предусмотрен такой NTP-клиент; по сути, он представляет собой протокол, применяемый AD для синхронизации своих членских систем. С помощью команды `w32tm` вы можете сообщить компьютеру Windows Server 2012 R2 о необходимости синхронизации своих часов с заданным сервером времени Интернета:

```
w32tm /config /computer:bf1 /update /manualpeerlist:time.windows.com
  /syncfromflags:manual /reliable:yes
```

Давайте разберем некоторые из этих странных параметров.

- **/computer**. Имя компьютера. В данном случае мы использовали имя компьютера с эмулятором PDC корня леса.
- **/reliable**. Да, это действительно *надежный* источник информации о времени для других компьютеров.
- **/manualpeerlist**. Список конкретных серверов времени, с которыми необходимо провести синхронизацию.
- **/syncfromflags**. Устанавливается в `manual` (вручную), т.к. синхронизация нужна только с серверами из списка `manualpeerlist`.

Можно указывать несколько серверов времени, разделяя их пробелами и заключая список в двойные кавычки, например:

```
w32tm /config /computer:bf1 /update
/manualpeerlist:"time.windows.com AnotherTimeServer.com StillAnotherOne.com"
/syncfromflags:manual /reliable:yes
```

Если вы забыли, какой именно сервер времени предложили применять для синхронизации, то можете вспомнить это посредством следующей команды:

```
w32tm /query /computer:bf1 /source
```

По умолчанию эмулятор PDC корневого домена леса будет пытаться выполнить синхронизацию со своим источником времени каждые шесть минут до тех пор, пока он успешно не подключится к этому источнику. Затем через шесть минут он делает это снова и спустя шесть минут еще раз. Он производит повторную синхронизацию каждые шесть минут до тех пор, пока успешно не проведет синхронизацию три раза подряд. После этого эмулятор PDC сокращает частоту синхронизации до каждых 100 минут. Изменить это можно с помощью ключа реестра, хотя не совсем понятно, зачем это может понадобиться. (Все параметры службы времени находятся в разделе `HKLM\System\CurrentControlSet\Services\W32Time\Config`.) В качестве альтернативы для просмотра конфигурации можно запустить следующую команду:

```
C:\Users\Administrator> w32tm /query /computer:bf1 /configuration
[Configuration]

EventLogFlags: 2 (Local)
AnnounceFlags: 10 (Local)
TimeJumpAuditOffset: 28800 (Local)
MinPollInterval: 6 (Local)
MaxPollInterval: 10 (Local)
MaxNegPhaseCorrection: 172800 (Local)
MaxPosPhaseCorrection: 172800 (Local)
MaxAllowedPhaseOffset: 300 (Local)

FrequencyCorrectRate: 4 (Local)
PollAdjustFactor: 5 (Local)
LargePhaseOffset: 50000000 (Local)
SpikeWatchPeriod: 900 (Local)
LocalClockDispersion: 10 (Local)
HoldPeriod: 5 (Local)
PhaseCorrectRate: 7 (Local)
UpdateInterval: 100 (Local)
```

Но где найти SNTP-сервер? Как ни странно, SNTP-серверов более чем достаточно. Крупные DNS-серверы большинства поставщиков услуг Интернета обычно действуют в качестве SNTP-серверов. Вы можете выяснить, является ли отдельная машина SNTP-сервером, с помощью небольшого бесплатного инструмента под названием `ntpquery.exe`, доступного по адресу `www.bytefusion.com/products/fs/fs.htm`. Вы просто указываете ему DNS-имя или IP-адрес, и если эта машина является сервером времени, то экран заполняется малопонятными длинными числами.

Может показаться, что включить фиксацию успешных и неудачных попыток в журнале событий не представляется возможным. Однако есть диагностическая программа, с помощью которой вы можете выяснить, установили ли вы соединение

с действительно полезным сервером времени. Эта программа называется `w32tm` и присутствует на всех машинах Windows. Хотя она не настолько замечательна, как `ntpquery.exe`, она бесплатна и интегрирована со службой времени.

Чтобы определить, работает ли сервер времени системы, откройте окно командной строки и введите **`w32tm /resync`**. Это будет выглядеть примерно так:

```
c:\> w32tm /resync
Sending resync command to local computer...
The command completed successfully.
```

Отправка команды resync локальному компьютеру...
Команда выполнилась успешно.

Или, если сервер времени не функционирует, вы увидите следующее сообщение:

```
The computer did not resync because no time data was available.
```

Компьютер не синхронизирован, поскольку данные времени не доступны.

Эта служба требует, чтобы порт 123 был открыт внешнему миру, поэтому настройте свои брандмауэры подходящим образом.

Доверительные отношения

Как обсуждалось ранее в этой главе, компьютеры внутри домена разрешают пользователям аутентифицироваться посредством контроллеров домена для доступа к их ресурсам. Эти компьютеры доверяют контроллерам домена. Для пользователей за пределами домена между контроллерами домена были созданы явные доверительные отношения, чтобы авторизовать пользователям доступ к ресурсам компьютеров. В настоящем разделе мы более подробно рассмотрим концепции, лежащие в основе этих явных доверительных отношений, и покажем, как их администрировать.

Доверительные отношения обладают характеристиками, которые можно сконфигурировать, когда они созданы. Доверительные отношения могут иметь одно или два направления. Они могут быть транзитивными или нетранзитивными. Каждая характеристика рассматривается в контексте типа доверительного отношения, которое будет создаваться.

Создавать и администрировать доверительные отношения можно с помощью оснастки Active Directory Domains and Trusts. Кроме того, те же самые операции можно выполнять посредством утилиты `netdom`.

Определение домена: доверительное отношение

Итак, у вас есть сервер, который может аутентифицировать пользователя, т.е. контроллер домена. Но для кого он будет проводить эту аутентификацию? Не для любой системы. Персональный компьютер (рабочая станция или сервер) может использовать контроллер домена для аутентификации, если этот персональный компьютер присоединяется к домену, чтобы стать его членом. Системы, которые не являются членами любого домена, могут выполнять аутентификацию с применением учетных записей пользователя в их локальной базе данных SAM. Системы, которые являются членами домена, могут либо аутентифицировать пользователя с помощью своих локальных учетных записей SAM, либо запросить его аутентификацию у одного из контроллеров домена. В мире сетей Microsoft мы говорим о том, что системы,

не состоящие в доменах, *доверяют* только своим локальным базам данных SAM, но системы, принадлежащие домену, *доверяют* своей базе данных SAM и контроллерам домена в своем домене. Присоединение к домену создает *доверительное отношение* между компьютером и контроллерами домена. Прежде чем рабочая станция будет доверять контроллеру домена для предоставления ей услуг по входу и до того, как контроллер домена станет в достаточной степени доверять рабочей станции, чтобы *предлагать* такие услуги, программное обеспечение Microsoft требует получения согласия со стороны администратора домена и администратора рабочей станции.

Когда вы присоединяете машину к домену, то обычно входите в систему с использованием учетной записи, которую рабочая станция распознает как локального администратора, но когда вы попытаетесь присоединить эту машину к домену, домен сообщит, что ему нужно видеть учетную запись администратора, распознаваемую самим *доменом*. Точно так же, как договор между двумя странами требует его подписания главами *обеих* стран, доверительное отношение между машинами и доменами требует авторизации со стороны локального администратора и администратора уровня домена.

Но доверительные отношения могут распространяться еще дальше. Как упоминалось ранее, доверительные отношения возникают между доменами в лесе. Вы можете также создавать доверительные отношения между доменами леса и другими доменами. Таким образом, если ваш компьютер является членом домена Test.com, а домен Test.com доверяет домену Apex.com, то локальные контроллеры домена могут аутентифицировать информацию, касающуюся не только учетных записей пользователей в Test.com, но и учетных записей пользователей в Apex.com.

Более подробно о доверительных отношениях

Если вы хотите соединить старый и новый домены для выполнения чистой миграции, если после слияния корпораций необходимо, чтобы домены в одном лесе доверяли доменам в другом лесе, или если просто нужно обеспечить совместное использование данных разными доменами, то придется создать доверительное отношение. Когда один домен доверяет другому, то первый домен утверждает, что ранее он принимал аутентификацию только от собственных контроллеров домена, но теперь он будет принимать аутентификацию также от контроллеров домена во втором домене.

Но как построить одно из таких доверительных отношений? В случае доверительных отношений между доменами можно применять графический пользовательский интерфейс либо инструмент командной строки под названием `netdom`.

Доверительные отношения имеют направление

Чтобы лучше понять доверительные отношения, прежде всего, следует уяснить, что они имеют направление. Доверительные отношения могут быть построены для перемещения либо в одном направлении, либо в двух. Терминология, принятая в Windows Server для описания доверительных отношений, несколько запутывает основные концепции. На рис. 24.16 приведена иллюстрация, которая поможет уловить суть этих концепций и хорошо усвоить терминологию, используемую в дальнейшем.

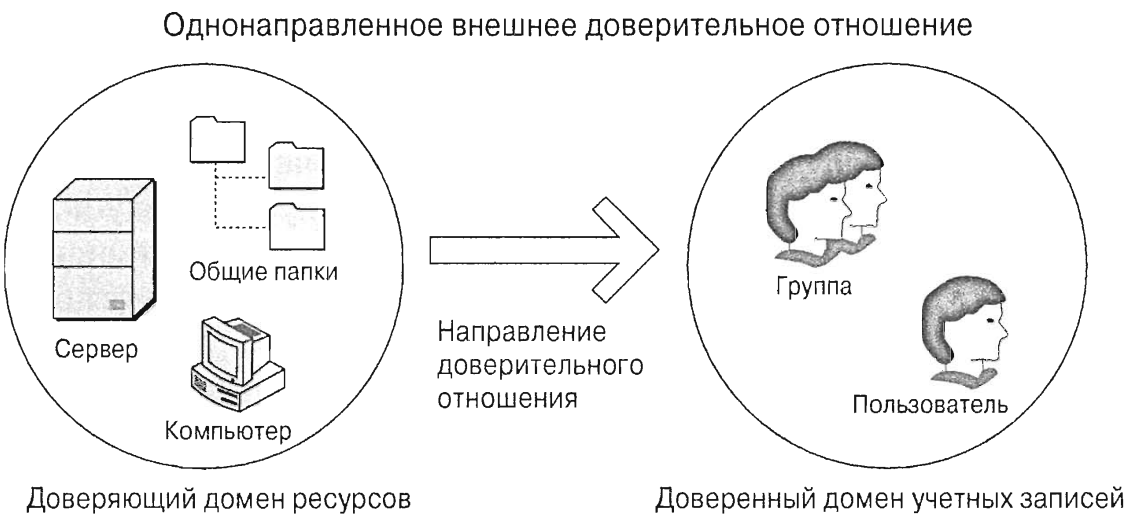


Рис. 24.16. Доверительные отношения

В любом доверительном отношении между двумя доменами участвуют доверяющий домен и доверенный домен. *Доверяющий* домен готов принимать информацию для входа, а также аутентификацию от *доверенного* домена. Предположим для примера, что есть два домена — Factory.com и Workers.com. Пусть Factory.com является доменом, который содержит совсем незначительное количество учетных записей пользователей, но зато набор учетных записей компьютеров для нескольких сотен серверов. Людям с учетными записями пользователей в Workers.com необходимо получать доступ к данным на серверах в домене Factory.com.

Или, другими словами, нужно, чтобы домен Factory.com *доверял* домену Workers.com. "Ресурсы" доверяют "учетным записям".

Если вы не до конца уяснили сущность доверительных отношений, прочитайте предшествующие разделы, чтобы не осталось каких-либо вопросов. Основная цель здесь в том, чтобы предоставить пользователям из домена Workers.com доступ к данным в домене Factory.com. Но серверы Factory.com, конечно же, не позволят обращаться к этим данным произвольным пользователям, если только они не смогут аутентифицировать этих пользователей. Однако домен Factory.com не может аутентифицировать таких пользователей — это могут делать только контроллеры их собственного домена. Следовательно, домен Factory.com должен начать принимать аутентификацию от Workers.com. Именно это в данном случае является определением доверительного отношения: принятие аутентификаций от контроллеров другого домена. Таким образом, пользователи домена Workers.com получают доступ к данным домена Factory.com, поскольку Workers.com является *доверенным* доменом, а Factory.com разрешает им доступ, потому что он представляет собой *доверяющий* домен.

Автоматически создаваемые доверительные отношения между доменами внутри одного леса являются двунаправленными. Один домен доверяет другому и наоборот. Доверительные отношения, создаваемые вручную, не обязательно разрешают доверие в обоих направлениях, так что по-прежнему есть возможность установки однонаправленных доверительных отношений.

Некоторые доверительные отношения являются транзитивными

Примечательная особенность леса связана с тем, что из-за транзитивной природы этих доверительных отношений все его домены доверяют друг другу — даже если

домен A не доверяет домену B *напрямую*, может оказаться, что A доверяет D, D доверяет C, а C доверяет B.

Работа доверительных отношений была проиллюстрирована в разделе "Протокол Kerberos и доверительные отношения" ранее в этой главе. Там применялась аналогия со знакомством с симпатичной девчонкой. Если бы у этой симпатичной девчонки был брат, подобно вам помешанный на компьютерах и к тому же увлекшийся вашей сестрой, то доверительное отношение между Вашей Мамой и Ее Мамой действовали бы в противоположном направлении. Они работали бы в случае существования корня леса для местного квартала или даже большего количества родительских "устройств защиты", формирующих сеть отношений. Когда образуются цепочки таких доверительных отношений, возникает своего рода игра "Шесть шагов до Кевина Бэйкона" [1], когда каждый доверяет каждому.

В этом и заключается транзитивная природа некоторых доверительных отношений. Автоматически построенные доверительные отношения "родительский–дочерний", а также доверительные отношения "корень леса–корень дерева" являются транзитивными. Установленные напрямую доверительные отношения и доверительные отношения леса также транзитивны, но они создаются вручную. Транзитивная природа сокращает количество доверительных отношений, которые необходимо формировать.

Доверительные отношения не устраняют все меры безопасности

Иногда люди опасаются создавать доверительные отношения между двумя доменами, полагая, что если домен A и домен B доверяют друг другу, то любой пользователь с учетной записью в домене A может нанести ущерб домену B и наоборот. Между тем это не имеет ничего общего с действительностью. Установление доверительных отношений между двумя доменами означает лишь то, что система в домене A может распознавать пользователя из домена B, а система в B — пользователя из A. Чтобы удостовериться в этом, подумайте над таким вопросом: может ли какой-то пользователь в домене A делать все, что ему вздумается, на любой системе в этом домене A? Конечно же, нет — все действия контролируются групповыми политиками, правами доступа пользователя и разрешениями.

Подобные опасения возникают у людей потому, что они привыкли работать в сетях с более старыми версиями Windows Server, которые были сконфигурированы со стандартными правами и разрешениями. Поскольку более ранние версии разрешений Windows Server представляли собой что-то вроде "заходите к нам все, кто пожелает", соединение доменов A и B действительно означало, что любой пользователь из A мог делать все, что угодно, на любом компьютере в B (а также наоборот). Но современные сети являются более строгими в этом отношении по двум причинам. Во-первых, стандартные права и разрешения, которые пользователь имеет в сети, состоящей из рабочих станций Windows 7 и выше, а также доменов

[1] Шесть шагов до Кевина Бэйкона (Six Degrees of Kevin Bacon) — это игра, участники которой должны за максимум 6 переходов найти связь между загаданным актером и Кевином Бэйконом через актеров, с которыми они вместе снимались. Игра основана на теориях тесного мира и шести рукопожатий. Кевин Бэйкон — американский актер, продюсер, режиссер. (*Прим. перев.*)

Windows Server 2008/2012, гораздо более ограничены, чем права и разрешения для сети с рабочими станциями и контроллерами домена Windows XP или Windows 2003. Во-вторых, теперь администраторы уделяют намного больше внимания вопросам безопасности и гораздо больше заботятся о защите своих серверов. Если сервер в домене A хорошо защищен от пользователей, принадлежащих этому домену, то этот сервер автоматически будет намного сильнее защищен от пользователей из любого другого доверяющего домена.

В доверительные отношения вовлечены администраторы с обеих сторон

Решение о том, чтобы позволить домену A принимать аутентификацию от домена B (для реализации однонаправленного доверительного отношения), не может быть принято доменом A в одностороннем порядке; оно также не может быть навязано со стороны домена B. Создание доверительного отношения сродни заключению договора между двумя странами: чтобы он обрел юридическую силу, обе стороны должны скрепить его подписями. Мы отдаем себе отчет, что во многих случаях администратором домена на обеих сторонах оказывается одно лицо (возможно, вы), но, тем не менее, ему придется предъявить свои учетные данные обоим доменам, прежде чем можно будет создать доверительное отношение.

Четыре вида доверительных отношений

В мире Windows Server 2012 R2 существуют четыре вида доверительных отношений, которые можно создавать вручную: внешние отношения, отношения, установленные напрямую, отношения леса и отношения области. Эти доверительные отношения были также доступны в Windows Server 2008. В редакциях сервера, предшествующих Windows Server 2003, были реализованы только внешние и установленные напрямую доверительные отношения. Скорее всего, вам придется иметь дело лишь с внешними и в редких случаях с доверительными отношениями леса, но давайте кратко рассмотрим все четыре вида.

- **Внешние доверительные отношения.** Внешние доверительные отношения по существу являются той их разновидностью, о которой в основном идет речь при обсуждении доверительных отношений между доменами. Поскольку они вытекают непосредственно из технологии доверия NT, их иногда называют *доверительными отношениями NT*. Если вы хотите, чтобы какой-то домен в лесе доверял домену, находящемуся *за пределами* этого леса, или в терминологии Microsoft — *внешнему* домену, то строите *внешнее* доверительное отношение. Оно будет использоваться при проведении миграции. Например, во время миграции домена в новый пустой домен AD, основанный на Windows Server 2012 R2, между этими двумя доменами сначала должно быть создано внешнее доверительное отношение, чтобы затем можно было копировать в новый домен учетные записи пользователей и прочие данные.
- **Доверительные отношения, установленные напрямую.** Доверительные отношения, установленные напрямую, помогают ускорить процесс аутентификации в крупных лесах. Помните ли вы обсуждение, касающееся протокола Kerberos и организации знакомств между старшеклассниками? Было бы неплохо изба-

виться от лишних звеньев связи между вами и понравившейся вам симпатичной девчонкой. Именно это и имеется в виду, когда речь идет об установленных напрямую доверительных отношениях. В рассмотренном ранее примере с помощью такого отношения домен Ecoast.Test.com мог бы обойти Test.com и соединиться напрямую с Consolidated.com. Правда, это не особо впечатляющий пример. Действительный выигрыш от применения установленных напрямую доверительных отношений мог бы получить только лес с несколькими деревьями или с многоуровневой иерархией доменов.

- **Доверительные отношения леса.** Доверительные отношения леса впервые были реализованы в Windows Server 2003 и позволяют формировать одно доверительное отношение между двумя лесами. После этого каждый домен в первом лесе будет доверять каждому домену из второго леса.
- **Доверительные отношения области.** Доверительные отношения области делают возможными доверительные отношения с системами Unix, которые используют для аутентификации протокол Kerberos. (То, что мы называем доменами, пользователи Unix и Kerberos называют *областями*.)

По большей части мы будем применять внешние доверительные отношения, но также покажем, как строить доверительные отношения леса.

Транзитивные доверительные отношения леса

Поскольку у нас нет возможности пересаживать реальные леса так, чтобы они росли вместе, мы не можем добавить один лес к другому. Самое большее, что мы можем сделать — это создать доверительное отношение. Внешнее доверительное отношение подходит для совместного использования ресурсов в пределах одного домена. Доверительное отношение леса лучше всего подходит для нескольких доменов. Доверительные отношения леса могут применяться только доменами, которые работают, по меньшей мере, на функциональном уровне леса Windows Server 2003.

Подобно автоматическим транзитивным доверительным отношениям, доверительное отношение леса предоставляет всем доменам в одном лесе шлюз для доверия доменам из другого леса. Предположим, что компания Test.com приобретает Apex.com, причем обе они располагают своими лесами. В компании Test.com желают, чтобы ее лес беспрепятственно взаимодействовал с лесом Apex.com, поэтому создают между лесами единственное доверительное корневое отношение, которое является универсальным.

Тем не менее, существуют причины, по которым это может быть далеко не всем тем, что хотелось бы Test.com и Apex.com. Эти причины указаны ниже.

- Во-первых, это возможно, только если Test.com и Apex.com модернизированы минимум до функционального уровня леса Windows Server 2003. В идеальном случае следовало бы модернизировать все домены и контроллеры доменов до Windows Server 2012 R2, чтобы можно было воспользоваться всеми замечательными возможностями, предоставляемыми этой самой современной технологией.
- Во-вторых, когда речь идет о некотором программном обеспечении, управляемом AD, два доверяющих друг другу леса — это не в точности то же самое, что один лес. (Здесь имеется в виду Exchange Server. Хотя это не единствен-

ное приложение подобного рода, но оно является наиболее важным.) Причина связана с существованием еще одного очень важного элемента, объединяющего леса, в дополнение к их транзитивным доверительным отношениям — глобального каталога.

Приложение Exchange Server воспринимает предприятие как одну большую фирму независимо от количества доменов в ней, поскольку Exchange Server полагает, что все домены, совместно использующие глобальный каталог, эквивалентны одному предприятию. Следовательно, возникает проблема: два отдельных доверяющих друг другу леса *по-прежнему имеют два отдельных глобальных каталога*.

- В-третьих — хотя это, пожалуй, менее важная проблема — как ни странно, доверительные отношения "лес-лес" не транзитивны *между лесами*. Под этим мы понимаем тот факт, что если лес 1 доверяет лесу 2, то все домены леса 1 доверяют всем доменам леса 2 и наоборот.

  Но давайте предположим, что вы установили транзитивное доверительное отношение между лесом 2 и лесом 3. Теперь все домены леса 2 доверяют всем доменам леса 3 (и наоборот). А что можно сказать о лесе 1 и лесе 3 — какое доверительное отношение существует между ними? Оказывается, что доверительное отношение между упомянутыми лесами отсутствует. Доверительные отношения "лес-лес" не являются сквозными. Чтобы каждый из этих лесов доверял друг другу, вы должны построить полностью отдельное доверительное отношение между лесом 1 и лесом 3.

С подробностями настройки доверительных отношений вы ознакомитесь в следующем разделе.

Создание доверительных отношений вручную

Основным инструментом для управления доверительными отношениями является консоль Active Directory Domains and Trusts (ADDT). Хотя суровые администраторы старой школы полагают, что мастера предназначены в основном для слабаков-администраторов нового поколения, мастер создания нового доверительного отношения (New Trust Wizard), доступный в ADDT, окажется весьма кстати, когда вы оцените сложность работы с командой `netdom`.

Доверительные отношения для домена можно найти на вкладке Trusts (Доверительные отношения) в диалоговом окне свойств любого из доменов, перечисленных в консоли ADDT (рис. 24.17). Здесь показано однонаправленное исходящее внешнее доверительное отношение для домена Apex.com. Даже при использовании терминологии, связанной с доверительными отношениями, понять то, о чем говорит эта вкладка, довольно сложно.

Возвратившись к рис. 24.16, можно заметить, что Apex.com является доменом с компьютерами, принтерами и файлами. Исходящая из него стрелка обращена в сторону домена Test.com. В области Domains trusted by this domain (outgoing trusts) (Домены, которым доверяет этот домен (исходящие доверительные отношения)) вкладки Trusts на рис. 24.17 перечислены домены с пользователями и группами. В данном случае пользователи в Test.com могут обращаться к файлам и принтерам в Apex.com.

Вы можете проверить это, создав локальную группу домена Apex.com в оснастке Active Directory Users and Computers. При добавлении в эту группу членов можно выбирать пользователей и группы из домена Test.com. Затем этой локальной группе домена можно назначить разрешение на доступ к ресурсам.

На рис. 24.18 показаны входящие доверительные отношения для Test.com. Это такие же доверительные отношения, которые обсуждались ранее и отображались на контроллерах домена Test.com. Домен Apex.com присутствует в области Domains that trust this domain (incoming trusts) (Домены, которые доверяют этому домену (входящие доверительные отношения)). Домен ресурсов Apex.com доверяет домену Test.com, который является доменом учетных записей.

Создание доверительных отношений с помощью мастера New Trust Wizard

Давайте обсудим доверительные отношения леса. Насколько мы видим, вы не можете прибегнуть к утилите `netdom` для создания по-настоящему интересных транзитивных доверительных отношений между лесами. Для этого вам понадобится оснастка Active Directory Domains and Trusts (ADDT). Тем не менее, в собственной практике мы полагались на внешние доверительные отношения. Они эффективны в деле формирования доверительных отношений между двумя доменами, что является превалирующим требованием в средах Active Directory. Доверительное отношение леса применимо к гораздо более крупным организациям, чем типовое IT-предприятие.

Создание доверительных отношений с помощью мастера New Trust Wizard, входящего в состав ADDT, выполняется посредством одной и той же процедуры для любого вида доверительных отношений, и все они требуют того же самого конфигурирования и информации.

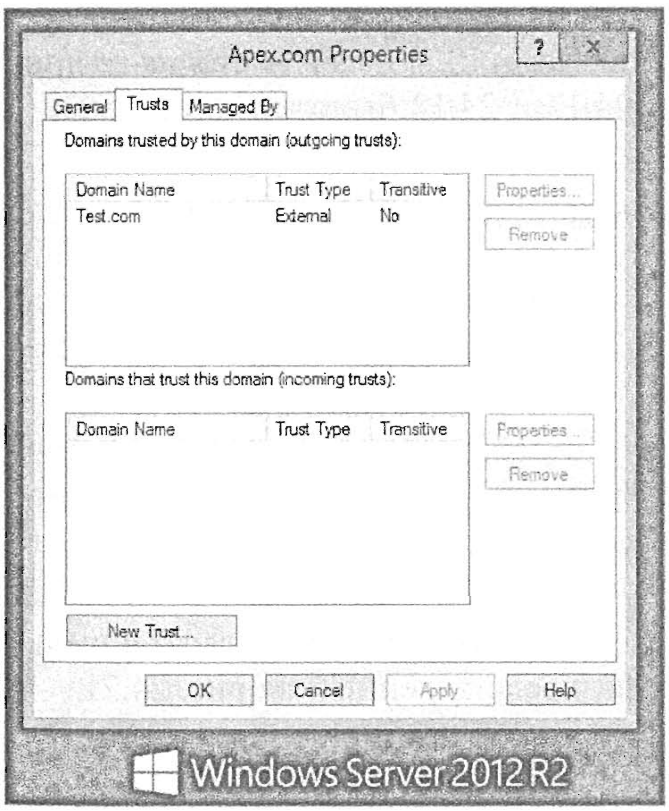


Рис. 24.17. Исходящее доверительное отношение

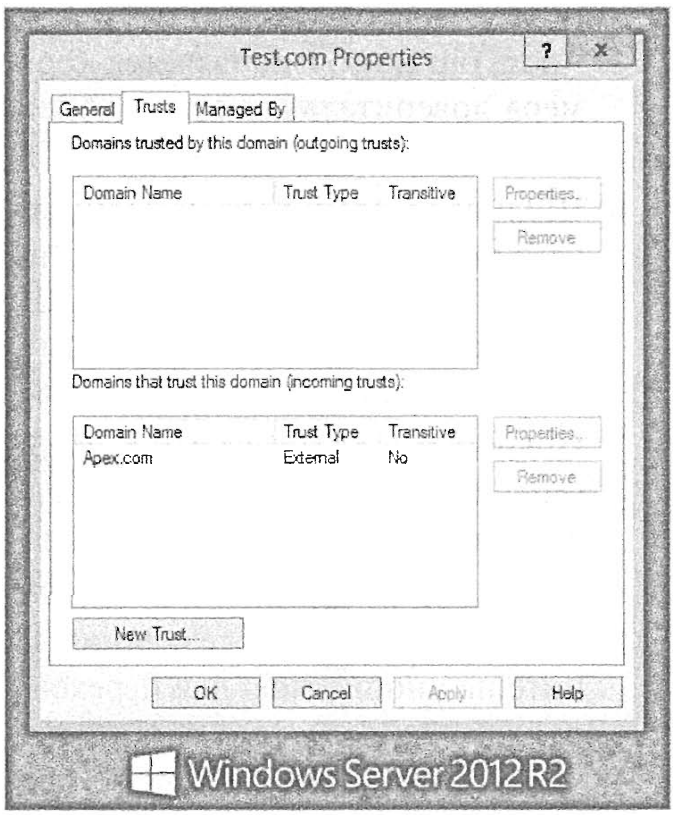


Рис. 24.18. Входящее доверительное отношение

1. Первым делом, как обычно, проверьте DNS с помощью нескольких команд `NsLookup`, чтобы убедиться в возможности пользователей в каждом лесу, области или домене находить контроллеры домена в другом лесу.

   Хотя существуют разные способы настройки преобразования имен внутри другого домена, мы предпочитаем устанавливать зоны-заглушки DNS. Зону-заглушку можно сконфигурировать как интегрированную с Active Directory, в результате чего она будет автоматически реплицироваться на другие контроллеры домена в домене. Это не требует модификаций основной зоны, что пришлось бы делать в случае дополнительной зоны. Та же цель достигается посредством серверов условной пересылки.

2. Затем удостоверьтесь в том, что оба леса находятся на функциональном уровне леса Windows Server 2012 R2.

3. Наконец, убедитесь в том, что вы располагаете именем и паролем учетной записи, которая является членом либо группы `Enterprise Admins`, либо группы `Domain Admins` для корневого домена леса, причем учетная запись подобного рода необходима для каждого леса.

4. Откройте оснастку Active Directory Domains and Trusts, выбрав в окне диспетчера серверов пункт меню Tools⇨Active Directory Domains and Trusts (Сервис⇨Домены и доверительные отношения Active Directory).

5. Щелкните правой кнопкой мыши на значке, представляющем корневой домен леса (вы не можете создать доверительное отношение леса из любого другого домена), выберите в контекстном меню пункт Properties (Свойства) и в открывшемся диалоговом окне перейдите на вкладку Trusts (Доверительные отношения), которая показана на рис. 24.17.

   Здесь видно, как создать доверительное отношение леса между Test.com (представляющим собой, как вы наверняка помните, корневой домен леса) и Apex.com (который является корнем другого леса). Для целей настоящего примера доверительное отношение на рис. 24.17 и 24.18 было заблаговременно удалено посредством щелчка на кнопке Remove (Удалить).

6. Щелкните на кнопке New Trust (Создать доверительное отношение), после чего появится экран с приветствием мастера создания нового доверительного отношения (New Trust Wizard). Щелкните на кнопке Next (Далее), и вы увидите экран, подобный показанному на рис. 24.19. В поле Name (Имя) мы указали **`Apex.com`**. (Мастер не чувствителен к регистру символов.)

7. Щелкните на кнопке Next, чтобы перейти к действительно *важному* выбору (рис. 24.20). Вспомните, что внешнее доверительное отношение — это простое доверительное отношение "домен-домен", а доверительное отношение леса является транзитивным доверительным отношением, которое вас интересует.

8. Выберите переключатель Forest trust (Доверительное отношение леса) и щелкните на кнопке Next для перехода на экран, представленный на рис. 24.21.

   Вы уже видели, что в доверительном отношении присутствуют две стороны — домен, который доверяет, и домен, которому доверяют. Этот экран позволяет выбрать, кто кому доверяет, и должны ли доверительные отношения быть двунаправленными.

9. Выберите переключатель Two-way (Двунаправленное) и щелкните на кнопке Next, чтобы перейти на экран, показанный на рис. 24.22.

   Здесь получается действительная экономия времени. Как говорилось ранее, один администратор не может создать доверительное отношение для двух доменов; должны быть задействованы администраторы с обеих сторон. Обычно это означает, что вы должны сначала настроить одну сторону доверительного отношения на одном домене, после чего перейти на контроллер домена в другом домене и завершить настройку на другой стороне.

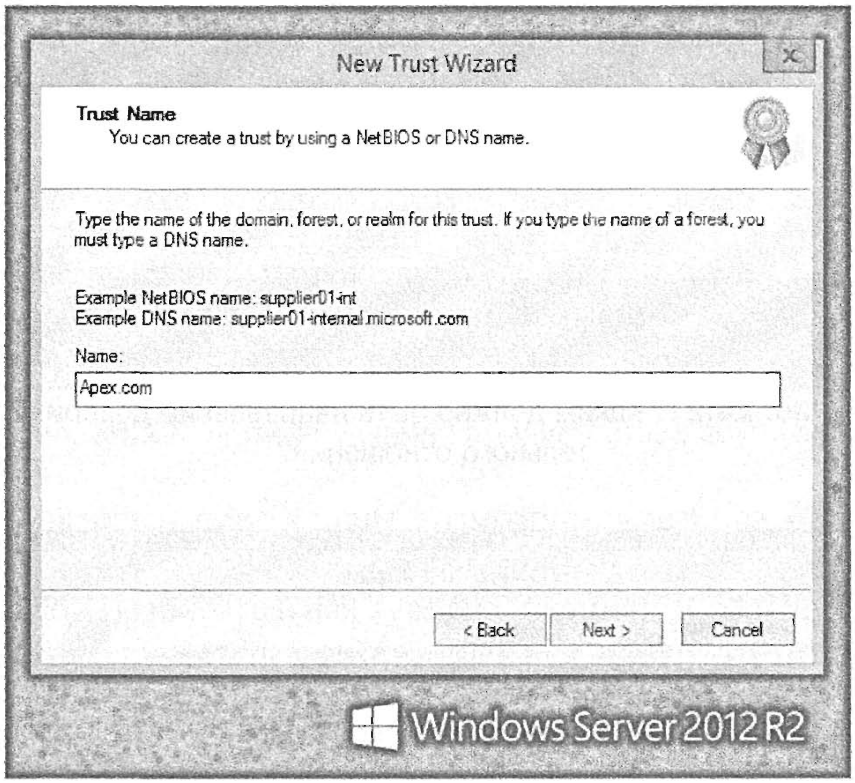


Рис. 24.19. Кому вы будете доверять?

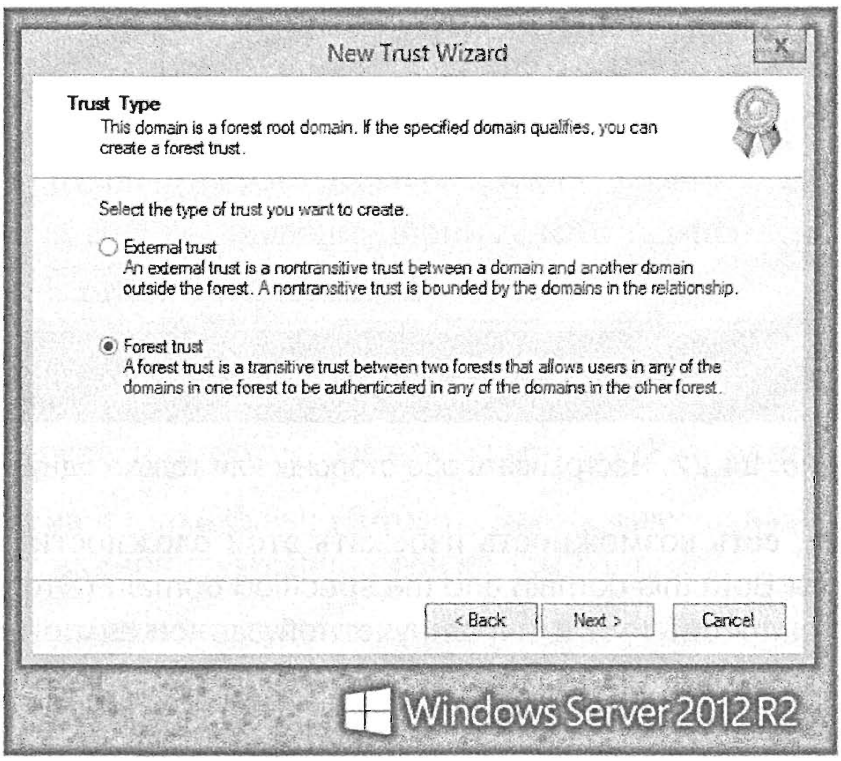


Рис. 24.20. Доверительное отношение какого типа требуется?

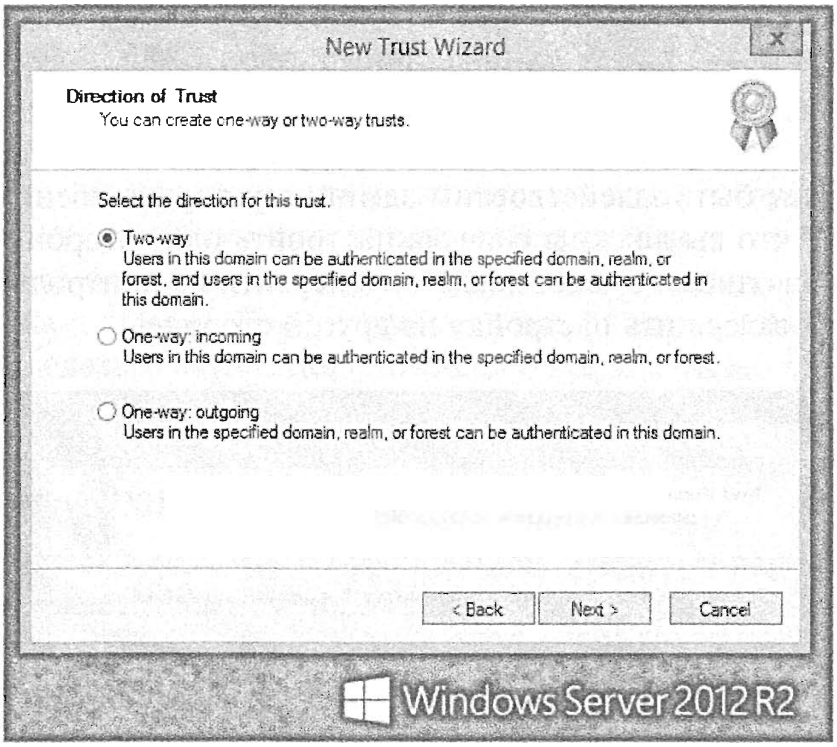


Рис. 24.21. Каким должно быть направление доверительного отношения?

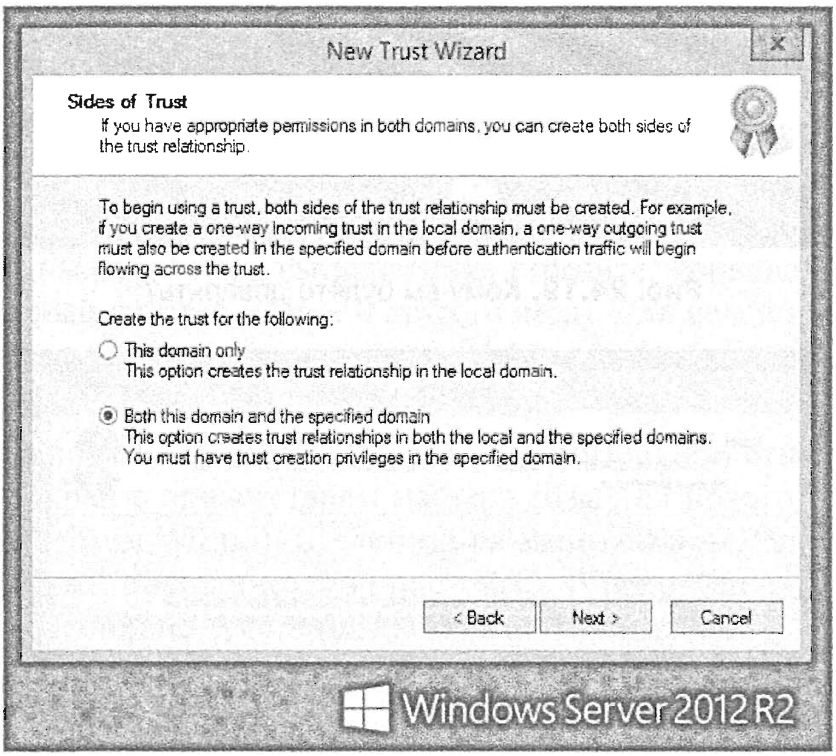


Рис. 24.22. Настраивать обе стороны или только одну?

Тем не менее, есть возможность избежать этой сложности. В случае выбора переключателя Both this domain and the specified domain (Этот и указанный домен) мастер запросит имя и пароль учетной записи администратора другого домена.

10. Заполните поля User name (Имя пользователя) и Password (Пароль) данными административной учетной записи (рис. 24.23) и щелкните на кнопке Next.

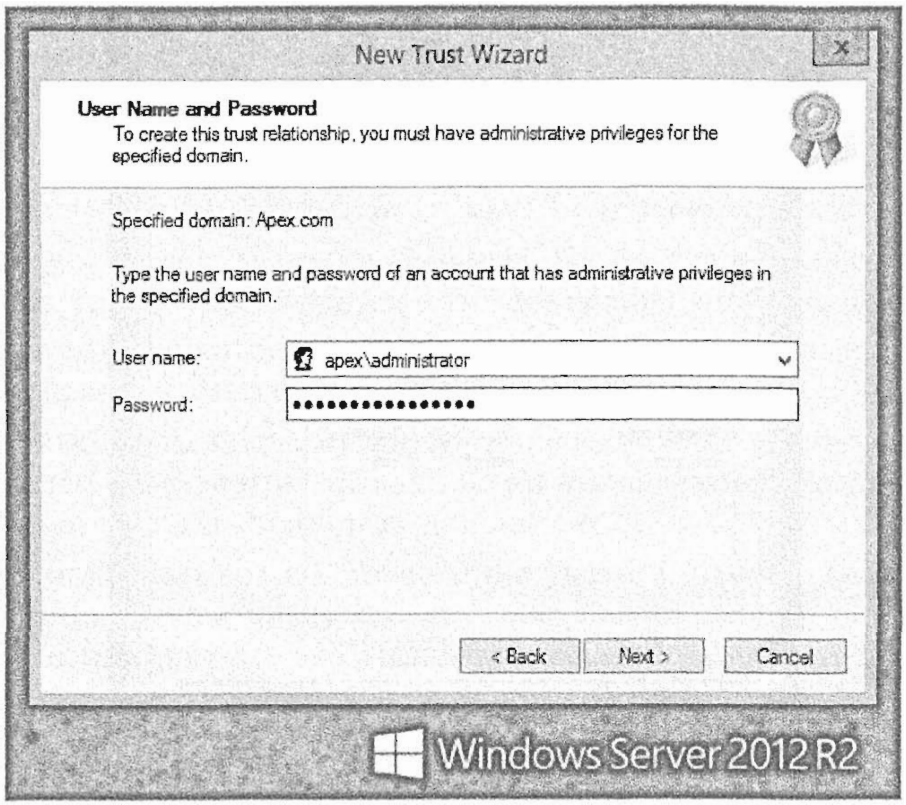


Рис. 24.23. Учетные данные администратора другого домена

Следующий экран предоставит возможность выбора между переключателями Forest-wide Authentication (Аутентификация в масштабах леса) и Selective Authentication (Избирательная аутентификация). В большинстве случаев вы создаете доверительное отношение леса из-за того, что хотите, чтобы все домены одного леса доверяли всем доменам другого леса. Если это так, выберите переключатель Forest-wide Authentication. С другой стороны, если вы желаете более точно настроить информацию аутентификации, передаваемую между лесами, то выберите переключатель Selective Authentication. Однако в этом случае вам предстоит выполнить намного больше работы!

11. Щелкните на кнопке Next, и мастер предложит выбрать вид аутентификации со стороны другого леса.
12. Выберите предпочитаемый переключатель и щелкните на кнопке Next.

    Вы получите еще две информационные панели, подтверждающие сделанный выбор.
13. Для продолжения щелкните на кнопке Next.

    Мастер запросит, желаете ли вы подтвердить связь между лесами. После этого появится последний экран This is what you did (Результаты вашей работы).
14. Щелкните на кнопке Finish (Готово). Задача завершена — домены Apex.com и Test.com функционируют практически как один.

На рис. 24.24 показаны результаты проделанной работы, отображаемые на вкладке Trusts. Домен Apex.com добавлен в обе области. Если вы решите просмотреть свойства доверительного отношения, то сможете выполнить процедуру проверки его достоверности. Это полезно при поиске и устранении неполадок.

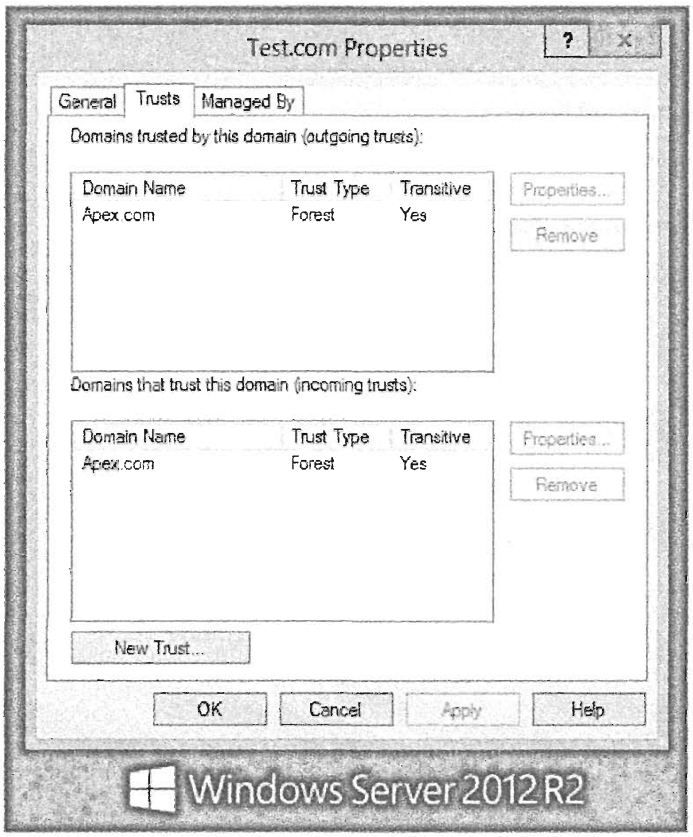


Рис. 24.24. Вкладка Trusts после завершения работы мастера

NETDOM: универсальный инструмент для работы с доверительными отношениями

Как уже упоминалось, подлинный, лежащий в основе смысл доверительного отношения распространяется за рамки доверительных отношений "домен-домен": он включает связь между членами домена и их контроллерами домена, а это значит, что иметь дело с доверительными отношениями приходится даже внутри предприятия с единственным доменом. Однако у административных инструментов прослеживается тенденция к обработке либо доверительных отношений "домен-домен", либо доверительных отношений между членами домена. Нам известен только один инструмент, который представляет доверительные отношения во всей их полноте — утилита `netdom`. Впервые появившаяся на заре развития Windows Server, утилита `netdom` становилась все более мощной и удобной в каждой новой версии, включая Windows Server 2012 R2. Приятной особенностью Windows Server 2012 R2 является то, что `netdom` устанавливается по умолчанию. Вам не придется заниматься поиском инструментов поддержки.

Большинство параметров `netdom` влияют на доверительные отношения между членами домена. Мы не хотим здесь уделять слишком много внимания этому аспекту, т.к. нас интересует главным образом обсуждение доверительных отношений типа "домен-домен", но некоторые параметры `netdom` все же перечислим.

`netdom add` добавляет в домен учетную запись компьютера. Это не приводит к присоединению данного компьютера к домену — на целевом домене лишь создается учетная запись компьютера и если этот домен является доменом AD, вы можете даже указать `netdom` организационную единицу, в которую должна быть помещена учетная запись. Это удобно, поскольку локальный администратор компьютера может присоединить его к домену, только *если* администратор домена уже создал учетную запись для этого компьютера в домене.

Вот как выглядит синтаксис netdom add:

```
netdom add машина /domain:имя_домена
/userd:учетная_запись_администратора_целевого_домена
/passwordd:пароль_администратора_целевого_домена
/server:имя_контроллера_домена /ou:целевая_организационная_единица /DC
```

Давайте рассмотрим составные части команды. Чтобы создать учетную запись компьютера в домене, вам должна быть известна следующая информация.

- Имя компьютера, для которого нужно создать учетную запись в домене. Именно это указывается в параметре *машина*.
- Вам необходимо знать, к какому домену присоединяется компьютер. Именно это предоставляется в параметре /domain. Если этот параметр не указан, то учетная запись компьютера создается в текущем домене.
- Этот домен может позволить добавление учетной записи компьютера, только если вы относитесь к числу тех, кому разрешено делать подобные операции в домене. Учетные данные указываются в параметрах /userd и /passwordd. Разумеется, если вы уже вошли в систему от имени учетной записи с такими разрешениями, то еще раз их предоставлять не понадобится.
- Возможно, вы хотите, чтобы эта операция была выполнена на конкретном контроллере домена. Его можно задать с помощью параметра /server.
- Возможно, вы хотите поместить новую учетную запись компьютера в конкретную организационную единицу; для этого предусмотрен параметр /ou. К сожалению, указывать организационную единицу придется в терминологии LDAP.
- Наконец, учетные записи компьютеров для контроллеров домена несколько отличаются от прочих учетных записей компьютеров; именно для этой цели в netdom предусмотрен параметр /DC.

Таким образом, если вы хотите создать учетную запись компьютера Matterhorn в домене Apex.com и поместить ее в организационную единицу Workstations, то должны ввести следующую команду:

```
netdom add Matterhorn /domain:apex.com
  /ou:"ou=Workstations,dc=apex,dc=com"
```

Опять-таки, это не означает присоединение Matterhorn к домену — для этого даже не понадобится система по имени Matterhorn. Но теперь локальный администратор в системе Matterhorn сможет присоединить компьютер к Apex.com, и ему не понадобится предоставлять имя/пароль учетной записи в домене. Но что, если вы хотите создать учетную запись компьютера *и* присоединить компьютер к домену? Для этого предназначена команда netdom join:

```
netdom join машина /domain:имя_домена
/userd:учетная_запись_администратора_целевого_домена
/passwordd:пароль_администратора_целевого_домена
/usero:учетная_запись_администратора_локальной_системы
/passwordo:пароль_администратора_локальной_системы
/ou:организационная_единица /reboot
```

Большинство параметров выглядят довольно знакомыми. Как и ранее, вы должны указать netdom присоединяемый компьютер и домен, а также возможно организационную единицу, в которую необходимо поместить учетную запись компьютера. Поскольку эта команда создает учетную запись компьютера в домене, необходимо предоставить учетные данные администратора уровня домена.

Однако теперь, поскольку осуществляется также присоединение компьютера к домену, понадобится разрешение этого *компьютера*; следовательно, вам нужно продемонстрировать наличие учетной записи, которую компьютер распознает как относящуюся к локальному администратору — именно для этого предусмотрены параметры passwordo и usero. (Символ o в конце параметров можно трактовать как начальную букву в object (объект), т.е. мы присоединяем этот объект к домену. То же самое можно сказать о d в параметрах userd и passwordd — они представляют пользовательскую учетную запись с административными привилегиями в *целевом* (destination) домене.) Наконец, параметр /reboot сообщает рабочей станции или серверу-члену о необходимости выполнить перезагрузку, чтобы внесенные изменения вступили в силу. Интересно отметить, что для выполнения этой команды вам вовсе необязательно работать за целевым компьютером — она может быть запущена дистанционно. Предположим для примера, что вы хотите переместить систему Saturn в домен Planets.com. Учетная запись администратора на компьютере Saturn называется satadmin и имеет пароль hi, а в Planets.com есть администратор домена по имени planadmin с паролем so. Тогда команда будет иметь такой вид:

```
netdom join Saturn /domain:planets.com
/usero:satadmin /passwordo:hi
/userd:planadmin /passwordd:so
/reboot
```

Мы уже упоминали, что netdom может помочь при выполнении миграции, позволяя перемещать компьютер из одного домена в другой; для этого используется команда netdom move. Ей потребуется три набора, состоящих из имени учетной записи и пароля, потому что для перемещения компьютера из домена A в домен B понадобится предъявить учетные данные администратора в домене A, в домене B и на самом перемещаемом компьютере. Как и ранее, вы указываете userd, passwordd, usero и passwordo. Но теперь необходимо указать также userf и passwordf — имя пользователя и пароль в *предыдущем* домене. К этому моменту все параметры должны быть знакомы:

```
netdom join машина /domain:имя_домена
/userd:учетная_запись_администратора_целевого_домена
/passwordd:пароль_администратора_целевого_домена
/usero:учетная_запись_администратора_локальной_системы
/passwordo:пароль_администратора_локальной_системы
/userf:учетная_запись_администратора_предыдущего_домена
/passwordf:пароль_администратора_предыдущего_домена
/ou:организационная_единица /reboot
```

Предположим, что вы хотите переместить компьютер по имени saturn.planets.com из домена Planets.com в домен Cars.org. Допустим, что у вас есть в Saturn административная учетная запись satadmin, в Planets.com — учетная запись администратора домена planadmin, а в Cars.org — учетная запись администратора домена caradmin. Пусть каждая административная учетная запись имеет пароль hi. Тогда команда выглядела бы следующим образом:

```
netdom move saturn.planets.com /domain:cars.org
/usero:satadmin /passwordo:hi
/userf:planadmin /passwordf:hi
/userd:caradmin /passwordd:hi
/reboot
```

Прежде чем перейти к обсуждению возможностей netdom, касающихся доверительных отношений "домен-домен", мы должны упомянуть о том, что эта утилита способна помочь при выполнении других задач, связанных с обслуживанием доверительных отношений между членами домена.

- **netdom reset**. Сбрасывает учетную запись компьютера. Иногда, находясь в системе, вы не можете войти в домен из-за того, что, как сообщается, компьютер потерял свою доменную учетную запись. Временами сброс учетной записи компьютера исправляет ситуацию.
- **netdom resetpwd**. Сбрасывает пароль доменной учетной записи компьютера. Для выполнения этой команды вы должны находиться непосредственно за компьютером. Если компьютер не подключался к домену на протяжении нескольких недель, срок действия пароля его учетной записи истекает. Эта команда может устранить проблему.
- **netdom remove**. Удаляет систему из домена.
- **netdom renamecomputer**. Переименовывает компьютер и его учетную запись. Будьте аккуратны с этой командой на серверах с сертификатами, т.к. они устанавливались с учетом имен.

Создание доверительных отношений между доменами с помощью netdom

Далее вы узнаете, как строить доверительные отношения с помощью netdom. Вспомните, что вы будете работать с двумя видами доверительных отношений: внешними доверительными отношениями (нетранзитивными типа "домен-домен") и доверительными отношениями леса (транзитивными типа "лес-лес"). С помощью netdom можно создавать внешние доверительные отношения. Сейчас вам будет легко представить, как это делается с помощью netdom. Вы должны указать, кто кому доверяет, и предоставить учетные данные администратора домена в каждом домене.

Синтаксис выглядит следующим образом:

```
NETDOM TRUST имя_доверяющего_домена /Domain:имя_доверенного_домена
    [/UserD:пользователь] [/PasswordD:[пароль | *]]
    [/UserO:пользователь] [/PasswordO:[пароль | *]]
```

Вспомните, что в наиболее базовых доверительных отношениях фигурируют *доверяющий* и *доверенный* домены. Доверяющий домен принимает аутентификацию от доверенного домена. Вы можете сделать доверительное отношение двунаправленным, но даже в этом случае netdom требует, чтобы один домен назывался доверяющим, а другой — доверенным. (Конечно, если вы строите двунаправленное доверительное отношение, то не имеет значения, какой из двух доменов вы сделаете доверяющим, а какой — доверенным.) Как и ранее, вы предъявляете учетные данные, но на этот раз используете параметры /uo и /po для указания имени пользователя и пароля для администратора домена из доверяющего домена "ресурсов", а параметры /ud и /pd для указания имени пользователя и пароля для администратора домена из доверенного домена "учетных записей". Параметр /add говорит о том, что нужно создать доверительное отношение, а /twoway — о том, что оно должно быть двунаправленным. Если вам необходимо однонаправленное доверительное отношение, параметр /twoway можно опустить. Параметр /enablesidhistory формирует доверительное отношение, которое может поддерживать инструменты миграции, создающие хронологии SID. Эта тема более подробно обсуждается в главе 25.

Итак, чтобы Apex.com и Test.com доверяли друг другу, предположим, что именем администратора домена Apex.com является `apexAdmin` с паролем `@pex.c0m`, а именем администратора домена Test.com — `testAdmin` с паролем `T3$t.c0m`. На контроллере домена Test.com выполняется следующая команда:

```
netdom trust apex.com /domain:test.com
/UserD:testAdmin /PasswordD:T3$t.c0m
/UserO:apexAdmin /PasswordO:@pex.c0m
/add /twoway /EnableSIDHistory
```

Доверительные отношения могут разрушаться по разным причинам. Если вы создали доверительное отношение, в течение нескольких месяцев не задействовали его, а затем пытаетесь применить это доверительное отношение для миграции, то может оказаться, что оно не работает. Утилита `netdom` позволяет "обновить" доверительное отношение с помощью параметра `/reset`:

```
netdom trust apex.com /domain:Test.com
/UserD:testAdmin /PasswordD:T3$t.c0m
/UserO:apexAdmin /PasswordO:@pex.c0m
/reset
```

Это похоже на команду, которая создает доверительное отношение, но вместо параметров `/add /twoway /enablesidhistory` в конце указывается просто `/reset`. Вместо `/reset` можно использовать `/verify`, чтобы проверить работоспособность доверительного отношения; если оно не работает, попробуйте применить `/reset`. *Настоятельно* рекомендуется проверять состояние доверительных отношений, чтобы убедиться в их работоспособности. Кроме того, доверительное отношение Apex.com можно проверить так:

```
netdom query /d:apex.com
/ud:apexAdmin /pd:@pex.c0m
/verify trust
```

Когда доверительное отношение больше не требуется, его можно разорвать с помощью следующей команды:

```
netdom trust apex.com /domain:test.com
/UserD:testAdmin /PasswordD:T3$t.c0m
/UserO:apexAdmin /PasswordO:@pex.c0m
/remove /twoway
```

После создания необходимых доверительных отношений посредством Windows PowerShell довольно легко отобразить все доверенные объекты внутри леса. Воспользуйтесь приведенной ниже командой, чтобы просмотреть существующие доверительные отношения в AD:

```
C:\PS>Get-ADTrust -Filter *
```

Резюме

Четко сформулируйте фундаментальные концепции Active Directory. Лес и деревья возвращают среду Active Directory "обратно к природе". Лес — это коллекция доменов, построенных относительно друг друга посредством AD DS. Деревья — это домены внутри иерархического пространства имен DNS с одинаковой последней частью имени. Ключом к отношениям между доменами являются автоматические

и не поддающиеся конфигурированию двунаправленные транзитивные доверительные отношения.

Контрольный вопрос. Когда создается первый контроллер домена для первого домена, в базе данных Active Directory формируются три раздела. Как называются эти три раздела, что в них содержится и какие из них реплицируются на другие контроллеры домена в лесе?

Выберите между использованием в структуре Active Directory одного домена, нескольких доменов или нескольких лесов. При выборе структуры Active Directory вы можете решить, что требуется несколько доменов, а не один домен с несколькими организационными единицами внутри. Ограничения репликации, юридические требования и политические факторы — вот главные причины, которые могут обусловить выбор структуры с множеством доменов.

Контрольный вопрос. Какие средства Windows Server 2012 R2 устраняют две причины применения структуры с несколькими доменами, которые связаны с безопасностью?

Добавьте домены в среду Active Directory. При построении нового домена или контроллера домена с репликой в лесе Active Directory вы будете использовать мастер конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard). В предыдущих версиях Windows Server структура DNS должна была быть на месте еще до установки. В Windows Server 2012 R2 все необходимое выполняется автоматически.

Контрольный вопрос. Поскольку все необходимые действия, связанные с DNS, теперь обрабатываются Windows Server 2012 R2, полезно знать, правильно ли они выполнены. Какие четыре изменения вы должны увидеть после добавления нового дочернего домена?

Управляйте функциональными уровнями, доверительными отношениями, ролями FSMO и глобальным каталогом. Мы обсудили несколько конфигураций, связанных с лесом, которые будут управляться администраторами предприятия. Функциональные уровни для леса и доменов обеспечивают доступность возможностей, предусмотренных в самой последней версии Windows Server. Чтобы получить в свое распоряжение эти возможности, все контроллеры домена должны быть модернизированы до этого уровня. Функциональные уровни можно поднимать, но не опускать. Пять ролей FSMO представляют собой особые роли, назначаемые контроллерам домена внутри доменов, а также лесу. Ролями, связанными с доменом, являются PDC Emulator, RID Master и Infrastructure Master. К ролям, связанным с лесом, относятся Domain Naming Master и Schema Master. Чтобы домены, не являющиеся частями одного и того же леса, могли совместно пользоваться определенными ресурсами, необходимо создавать доверительные отношения. Исключением являются установленные напрямую доверительные отношения, которые позволяют сократить путь доверия между двумя доменами внутри того самого леса.

Контрольный вопрос. Размещение роли FSMO диктуется доменом, которому она назначена, и ролью Global Catalog. В каких двух ролях предусмотрены правила, связанные с размещением, в том, что касается глобального каталога?

Глава 25

Миграция, слияние и модификация Active Directory

В большинстве крупных организаций Active Directory стала стандартной и наиболее распространенной службой каталогов и аутентификации. Служба Active Directory управляет доступом к серверам, компьютерам, файловым и принтерным ресурсам, а также к электронной почте, базам данных и приложениям в масштабах всей организации. Служба Active Directory впервые появилась в версии Windows 2000 Server. Потребовалось более десяти лет, чтобы она прижилась в организациях. В Windows Server 2012 предлагается пятый крупный выпуск Active Directory. Будучи важной частью бизнес-операций, информационная технология и инфраструктура становятся предметом обсуждения при планировании слияний, поглощений и ответвлений в организациях. Структура Active Directory не поддерживает пересадку или отсечение доменов. Другими словами, вы не можете добавить домен в лес либо изъять из леса существующий домен. Следовательно, разделение или добавление бизнес-операций будет влиять на среду Active Directory, заставляя вас вручную переносить пользователей, компьютеры и данные с обеспечением непрерывности ведения бизнес-деятельности. Важно всесторонне обсудить эти операции в кругу лиц, ответственных за принятие решений внутри организации.

С выходом Windows Server 2008 обеспечиваются значительные обновления функций Active Directory. Большая часть времени при разработке Active Directory в Windows Server 2012 была потрачена на совершенствование существующих возможностей продукта. Например, корзина Active Directory (Active Directory Recycle Bin) была оснащена графическим пользовательским интерфейсом. Ранее она была доступна только посредством PowerShell. Кроме того, группа `gMSA` (Managed Service Accounts — учетные записи управляемых служб) расширяет возможность Windows Server 2008 R2, включив поддержку учетных записей управляемых служб в кластеризацию и балансировку нагрузки.

Не обошлось и без внесения простых изменений в интерфейс, а также оптимизации производительности; вам наверняка понравятся обновления базовых элементов

Active Directory. После модернизации своего контроллера домена вы можете клонировать его с помощью Hyper-V и затем воспользоваться безопасным восстановлением.

В этой главе вы изучите следующие темы:

- внедрение в сеть новых версий Active Directory;
- миграция доменных учетных записей из одного домена в другой.

Стратегии модернизации и миграции

До сих пор наши обсуждения строились так, словно вы создавали совершенно новую сеть, однако в наши дни подобная ситуация случается редко. Вместо этого мы будем предполагать, что у вас уже существует домен Active Directory, и вы хотите перейти к домену Active Directory, основанному на Windows Server 2012. Или же, как вариант, вы хотите объединить две инфраструктуры AD. В любом случае работа такого рода относится к категории *миграции*.

Приступив к рассмотрению стратегий миграции, мы представим базовый обзор ряда элементов и другие соображения. Если вы выполняете миграцию, то, скорее всего, имеете действующий домен и хотите преобразовать или модернизировать его до домена AD, функционирующего на основе Windows Server 2012.

Больше всего IT-администраторы опасаются, удастся ли им успешно провести процедуру миграции. Домен, прекращающий (полностью или частично) функционирование во время миграции, нельзя рассматривать как приемлемый вариант. Абсолютно необходим подходящий план тестирования миграции и ее проверка в экспериментальной среде. Обычно компании создают виртуальную инфраструктуру в производственной или экспериментальной среде. Преимущество использования такой виртуальной инфраструктуры для тестирования заключается в том, что с помощью процесса P2V (Physical to Virtual — физический в виртуальный) вы можете поместить контроллер домена в частную сеть для проверки процесса модернизации.

Чтобы успешно пройти через этот процесс, настоятельно рекомендуется создать экспериментальную среду из своей производственной среды; дополнительные сведения приведены в статье по адресу `http://tinyurl.com/ch25p2v`. В статье показано, как построить экспериментальную среду на основе текущей среды Windows Server 2003, Windows Server 2008 или Windows Server 2008 R2. Несмотря на то что материал кажется устаревшим, он по-прежнему актуален и ему можно спокойно следовать.

К миграции на домен Windows Server 2012 применимы три базовых философии.

- **Модернизация домена на месте.** Процесс предусматривает установку операционной системы Windows Server 2012 поверх существующего контроллера домена Windows.
- **Постепенная миграция.** Сервер-член Windows Server 2012 повышается до контроллера домена с репликой существующего домена. Иногда это называют модернизацией Active Directory.
- **Миграция домена (требует нового леса или домена).** Некоторые организации предпочитают устанавливать новую среду AD в качестве способа построения чистого домена. Такой тип миграции предусматривает настройку нового пространства имен и перемещение всех объектов. Это весьма масштабное мероприятие, которое требует тщательного планирования и точного исполнения. Данная тема в настоящей главе не обсуждается.

Возможности модернизации

Прежде чем мы углубимся в рассмотрение процесса миграции и тестирования, необходимо уяснить, какие версии могут быть модернизированы.

Функциональный уровень леса Windows Server 2003 является минимальным требованием для выполнения модернизации на месте. Если вы планируете модернизировать Windows Server 2003 до Windows Server 2012, то сначала должны модернизировать домен до Windows Server 2008 или Windows Server 2008 R2. Непосредственный переход от Windows Server 2003 Active Directory к Windows Server 2012 R2 Active Directory невозможен.

Модернизации поддерживается для следующих версий:

- Windows Server 2008 (только 64-разрядная версия)
- Windows Server 2008 R2
- Windows Server 2012

Для перечисленных ниже версий модернизация не поддерживается:

- Windows Server 2008 (32-разрядная версия)
- Windows Server 2003 (любая версия)
- Windows 2000 Server (любая версия)

При модернизации до Windows Server 2012 в домене не допускается существование контроллеров домена Windows 2000 Server. Вы должны понизить контроллеры домена Windows 2000 Server до рядовых серверов и позволить выполниться обычной репликации. (В их удалении можно убедиться, проведя проверку допустимости домена.)

Миграция посредством модернизации на месте

Перенос домена Active Directory из предыдущих (поддерживаемых) версий Windows Server на Windows Server 2012 обычно производится как стандартная модернизация. Производственный домен может содержать очень мало контроллеров домена или пребывать в чистом изначальном виде. Модернизация на месте может представляться довольно быстрым и легким процессом.

При модернизации на месте вы предоставляете программе установки Windows Server 2012 возможность преобразовать базу данных Active Directory домена в базу данных Active Directory на основе Windows Server 2012. Процесс является относительно безболезненным и предусматривает установку Windows Server 2012 поверх одной из предыдущих поддерживаемых версий Windows Server. Сначала вы выполняете пару подготовительных процедур, а затем запускаете программу установки на контроллере домена.

После завершения процесса установки в домене все выглядит в основном, как и прежде. Пользователи и группы остаются теми же самыми. Компьютеры остаются такими же. В учетные записи пользователей также не изменяются, и к этому моменту основные преимущества связаны только с инструментами, доступными для IT-специалиста. Это вариант типа “все или ничего”. Модернизация приложений и операционных систем ничем не примечательна. Разработчики изо всех сил стремились к тому, чтобы вносимые изменения не приводили к сбоям и не вызывали до-

рогостоящих обращений клиентов в службу технической поддержки. Тем не менее, что-то может пойти не так. Если в ходе модернизации контроллера домена возникла проблема, откат может оказаться весьма болезненным и требовать немалых затрат времени.

Пути модернизации

Возможные пути модернизации до Windows Server 2012 по существу подчиняются следующему правилу: Windows Server 2008 x64 или последующая версия и та же самая редакция или лучше (т.е. Datacenter или Standard Edition) Windows Server 2012 не рассчитаны на процессор x86, поэтому для многих организаций модернизация на месте может не подойти. Поскольку в подавляющем большинстве организаций для Active Directory по-прежнему применяется Windows Server 2003, весьма маловероятно, что они используют 64-разрядную версию Windows Server 2003.

Если организация располагает Active Directory на основе Windows 2000 Server , в ней придется сначала провести модернизацию до Windows Server 2008 x64.

Подготовка к модернизации

Прежде чем начать модернизацию, вы должны быть абсолютно уверены в наличии инфраструктуры DNS — выполните проверку записей ресурсов службы с помощью `NsLookup` и `DcDiag`, как было показано в главе 6.

Чтобы обеспечить себе возможность возврата к исходному состоянию, обойдите все контроллеры домена, синхронизируйте их и создайте их резервные копии. Если модернизация завершится неудачно, вы сможете выполнить процедуру восстановления на контроллере домена с помощью данных исходного состояния системы. (Но давайте будем надеяться, что до этого не дойдет.)

Переводить контроллер домена в автономный режим, как это нужно было делать в прежние времена, не понадобится, поскольку процедуре модернизации необходим доступ ко всем контроллерам домена и ролям.

Удостоверьтесь, что функциональные уровни вашего леса и доменов соответствуют, по меньшей мере, Windows Server 2003.

Выполнение модернизации на месте для AD на основе Windows Server 2008 R2 (x64)

Модернизация на месте предполагает выполнение следующих базовых шагов.

1. Подготовка схемы леса для обеспечения совместимости с Windows Server 2012.
2. Подготовка домена для Windows Server 2012.
3. Запуск программы установки для модернизации контроллера домена.

Эти шаги подробно описаны в последующих разделах.

Подготовка схемы леса и домена

При выполнении модернизации на месте вовсе необязательно, чтобы на всех контроллерах домена была установлена одна и та же версия Windows Server: допускается сочетание Windows Server 2008 R2 и 64-разрядной версии Windows Server 2008 (модернизация поддерживается только для 64-разрядных версий). Тем не менее, на

определенных контроллерах домена Windows Server 2008 R2 или Windows Server 2008 должны располагаться некоторые роли FSMO. Хозяином именования доменов данного леса, которым по умолчанию является первый контроллер домена в лесе, должна быть как минимум машина с 64-разрядной версией Windows Server 2008. Эмуляторы PDC каждого домена внутри леса также должны находиться на машине с этой минимальной версией ОС. По умолчанию, эмулятор PDC располагается на первом контроллере домена в каждом домене.

Даже если вы собираетесь модернизировать до Windows Server 2012 только один домен в лесе, базирующемся на Windows Server 2008, понадобится изменить схему леса и домена, прежде чем ОС Windows Server 2012 сможет быть установлена на целевом контроллере домена. Все домены в лесе разделяют одну и ту же схему, поэтому вы должны изменить схему всего леса. Эта задача выполняется на компьютере с ролью хозяина схемы данного леса.

В Microsoft внесли ряд базовых изменений в инструмент `adprep`, которые главным образом касаются областей, где этот инструмент хранит данные и указывает, какие объекты опубликованы. Ниже перечислены ссылки на статьи TechNet, где можно ознакомиться с организацией всех записей. Мы рекомендуем просмотреть эти материалы, прежде чем запускать команду `adprep` в производственной среде.

- **Обновления в масштабах всего леса.** `http://tinyurl.com/c25AdPrepFW`
- **Обновления в масштабах всего домена.** `http://tinyurl.com/c25AdPrepDW`
- **Обновления контроллеров домена только для чтения.** Обновления контроллеров домена только для чтения (RODC) не предусмотрены.
- **Обновления схемы.** `http://tinyurl.com/c25AdPrepSC`

Выполнение `adprep`

Команда `adprep` встроена в операционную систему Windows Server 2012. При выполнении других типов миграций (постепенной миграции или миграции доменов) добавление роли Active Directory Domain Services приводит к запуску команды `adprep` должным образом. В случае модернизации на месте для старта этого процесса необходимо обратиться к установочному компакт-диску или ISO-образу. Чтобы успешно выполнить команду `adprep`, вы должны располагать подходящими учетными данными.

Запуск команды `adprep /forestprep` требует членства в перечисленных ниже группах:

- `Schema Admins` (Администраторы схемы)
- `Enterprise Admins` (Администраторы предприятия)
- `Domain Admins` (Администраторы домена)

Выполнение команды `adprep /domainprep` (включая `/gpprep`) необходимо членство в следующей группе:

- `Domain Admins`

Запуск команды `adprep /rodcprep` требует членства в следующей группе:

- `Enterprise Admins`

Команду придется запускать вручную, как описано далее.

1. Откройте окно командной строки с повышенными полномочиями на контроллере домена Windows Server 2008 R2, который необходимо модернизировать.
2. Запустите команду `adprep`, для чего введите (подставив при необходимости вместо `d:` букву своего устройства чтения DVD/CD) **`d:\support\adprep\adprep`** и нажмите <Enter>.

   Это отобразит все параметры синтаксиса наряду с краткими пояснениями.
3. Чтобы запустить процесс подготовки к модернизации на месте, введите **`adprep /forestprep`** и нажмите <Enter>.

   Вы увидите примерно такой вывод:

```
D:\support\adprep>adprep /forestprep

ADPREP WARNING:
Before running adprep, all Windows Active Directory Domain Controllers
in the forest should be upgraded to Windows 2003 or later.

[User Action]
If all domain controllers in the forest run Windows Server 2003 or
later and
you want to upgrade the schema, confirm by typing 'C' then press ENTER to
continue. Otherwise, type any other key and press ENTER to quit.

ПРЕДУПРЕЖДЕНИЕ ADPREP:
Перед запуском adprep все контроллеры домена Windows Active Directory
в лесе должны быть модернизированы до Windows Server 2003 или
последующей версии.
[Действие пользователя]
Если все контроллеры домена в лесе работают под управлением Windows
Server 2003 или последующей версии, и вы хотите модернизировать схему,
подтвердите это, введя C и нажав <Enter> для продолжения. В противном
случае введите любую другую букву и нажмите <Enter> для завершения.
```

   У вас может возникнуть соблазн проигнорировать этот текст и просто нажать <Enter>. Это привело бы к внезапному завершению команды. Мы рекомендуем внимательно прочитать этот текст.
4. Введите с клавиатуры **`c`** и нажмите <Enter>, чтобы увидеть команду `adprep` в действии.

   На экране появится текст и бесчисленное количество точек.

   Это будет продолжаться до тех пор, пока AD не импортирует и не внесет изменения в схему. Наконец, выводится следующее сообщение:

```
Adprep successfully updated the forest-wide information.
Adprep успешно обновила информацию в масштабах всего леса.
```

   Откат после изменения схемы требует восстановления данных состояния системы на контроллере домена с ролью Schema Master. Состояние системы будет содержать последнюю резервную копию базы данных Active Directory. Хозяином схемы является основной контроллер домена для репликации схемы, поэтому восстановление базы данных Active Directory будет включать схему. Затем данные реплицируются на другие контроллеры домена.

Теперь вы можете подготовить свой домен.

5. Перейдите на компьютер с ролью хозяина инфраструктуры и обеспечьте готовность как перед запуском `adprep`.
6. Введите **`adprep /domainprep /gpprep`**.

   Инструмент `DomainPrep` подготавливает домен к появлению контроллера домена Windows Server 2012. Инструмент `GPprep` модифицирует разрешения на объектах групповой политики для репликации на контроллеры домена Windows Server 2012. После выполнения этой команды отобразится следующая информация:

   ```
   D:\support\adprep>adprep/domainprep /gpprep
   Adprep successfully updated the domain-wide information.
   Adprep successfully updated the Group Policy Object (GPO) information.
   ```

   Adprep успешно обновила информацию в масштабах всего домена.
   Adprep успешно обновила информацию объектов групповой политики (GPO).

   Если вы еще не запускали `adprep` в отношении контроллеров домена только для чтения, у вас есть замечательная возможность заняться этим. Возможно, вы уже это делали, если располагаете функционирующей средой Active Directory версии Windows Server 2008; учитывая, что схема та же самая, никаких изменений не произойдет. Тем не менее, такое действие рекомендуется для возможного будущего RODC, а также просто для того, чтобы удостовериться в том, что все было сделано ранее.

7. Введите **`adprep /rodcprep`**.

Подведем итоги. Прежде чем вы сможете модернизировать домен AD, основанный на Windows Server 2008/2008 R2, до домена AD на базе Windows Server 2012, вы должны выполнить описанные ниже шаги.

1. Все контроллеры домена должны функционировать под управлением 64-разрядной версии операционной системы.
2. Модернизируйте лес, запустив команду `adprep /forestprep` на компьютере с ролью хозяина схемы для леса, даже если этот компьютер не находится в домене, который вы собираетесь модернизировать.
3. Модернизируйте структуру домена, запустив команду `adprep /domainprep /gpprep` на компьютере с ролью хозяина инфраструктуры для каждого домена, который вы планируете модернизировать.
4. Дополнительно запустите `adprep /rodcprep`, чтобы подготовить контроллеры домена только для чтения.

Выполнение программы установки

Теперь вы готовы к выполнению программы установки.

1. Вставьте DVD-диск (или диск с ISO-образом).
2. Если не произошел автозапуск, дважды щелкните на его значке в окне My Computer (Мой компьютер).
3. В открывшемся окне выберите пункт Upgrade (Модернизация).

Программа установки предупредит обо всем, что изменится в результате модернизации. Она также проверит, провели ли вы надлежащим образом подготовку леса и домена. После этого выполнение программы установки не требует вмешательства до тех пор, пока она не завершится, и вы не войдете в систему только что модернизированного до Windows Server 2012 контроллера домена в первый раз. Модернизация прошла успешно.

Модернизация на месте: доводы за и против

Ниже перечислены доводы в пользу проведения модернизации на месте.

- Как правило, такая модернизация не требует использования новых компьютеров.
- Ваши пользователи сохраняют свои старые идентификаторы SID, а домен сохраняет свои старые доверительные отношения, поэтому любые серверы в других доменах — например, в доменах ресурсов, которые содержат файловые серверы и серверы печати или почтовые серверы — будут по-прежнему без проблем опознавать этих пользователей.
- Пользователи сохраняют свои старые пароли.
- Это относительно простая и быстрая модернизация.
- Если вы переходите от AD на основе Windows Server 2008, к AD на базе Windows Server 2012, то процедура модернизации в принципе не вызывает сложностей.
- Модернизация на месте от Windows Server 2008 R2 является гладкой и простой.

А вот некоторые ограничения модернизации на месте.

- Путь модернизации в некоторой степени ограничен. Поддерживаются только 64-разрядные версии Windows Server. Когда стала доступной ОС Windows Server 2003, многие организации развернули 32-разрядные контроллеры доменов, поэтому у них нет возможности провести модернизацию на месте.
- Это модернизация по принципу "все или ничего". Вы модернизируете *все* учетные записи, причем такая модернизация является путем в одном направлении — какой-то мастер отката AD не предусмотрен. (Однако вы можете, как было указано ранее, восстановить данные состояния системы.) Мы предпочитаем более последовательные подходы.
- Любой накопившийся за время работы "мусор" останется в базе данных Active Directory. Об этом здесь упоминается потому, что многие думают, что модернизация очистит базу данных от устаревших и недействительных объектов. Избавиться от таких объектов могут помочь некоторые из новейших инструментов Windows Server 2012 из состава модулей PowerShell для AD.

Выполнение постепенной миграции

Одним из последовательных подходов является постепенная миграция, которую иногда называют *миграцией Active Directory*. Она предусматривает добавление контроллера домена Windows Server 2012 в домен Active Directory. Среда остается, по сути, той же, но существующие контроллеры домена могут быть модернизированы или заменены по усмотрению администраторов. Исторически сложилось так, что недостатком такого подхода является потребность в дополнительном оборудовании, но в условиях нынешней виртуализации, такой как Hyper-V, вы можете просто создать виртуальный контроллер домена на компьютере Windows Server 2012.

Вы избегаете модернизации сервера по принципу "все или ничего", поскольку новый контроллер домена не угрожает целостности базы данных Active Directory — эта реплика просто принимает копию базы данных Active Directory. Такой процесс по-прежнему требует соответствующей подготовки схемы леса и доменов, однако эти процедуры менее утомительны, чем модернизация.

Повторное развертывание контроллера домена вызывает сложности, которые требуют определенного планирования. Исходный контроллер домена является важной частью среды. Он может содержать роли FSMO и быть сервером глобального каталога. На нем могут функционировать другие службы, такие как DNS, DHCP, общие файлы и принтеры, к которым регулярно обращаются пользователи. Могут существовать сценарии и групповые политики, которые указывают на этот контроллер домена. Вы должны выяснить, что произойдет, когда этот сервер будет изъят из сети. Вам следует подумать над тем, чем вы заполните образовавшиеся бреши. Возможно, новый контроллер Windows Server 2012 сможет взять на себя таких роли и службы.

Постепенная миграция предусматривает выполнение следующих базовых шагов.

1. Подготовка схемы леса для обеспечения ее совместимости с Windows Server 2012.
2. Подготовка домена для Windows Server 2012.
3. Подготовка исходного контроллера домена к возможному выводу из эксплуатации либо изменению конфигурации.
4. Подготовка нового сервера-члена и его повышение до контроллера домена.
5. Выполнение постмиграционных процедур с учетом размещения ролей FSMO, изменения IP-адресов или других изменений.
6. Повторное развертывание исходного контроллера домена необходимым образом.

Подготовка схемы леса и домена

Как и в случае модернизации на месте, существующий лес и целевой домен нужно подготовить к изменениям Active Directory версии Windows Server 2012. Вы должны выполнить команды `ForestPrep`, `DomainPrep` и `Gpprep`, но в Windows Server 2012 при добавлении роли Active Directory Domain Services команда `adprep` запускается автоматически, аналогично тому, как обсуждалось в разделе "Миграция посредством модернизации на месте".

Процедуры отката на данном этапе такие же, как и при модернизации на месте. Вы должны восстановить данные состояния системы на контроллере домена с ролью хозяина схемы.

Построение сервера-члена Windows Server 2012

Новый контроллер домена начинается как сервер-член Windows Server 2012 в исходном домене. Во время подготовки понадобится установить роль Active Directory Domain Services и роль DNS до запуска процесса Active Directory Roles.

Верификация DNS

Поскольку новый контроллер домена будет поддерживать DNS, вы должны добавить его как сервер имен в подходящие зоны прямого и обратного просмотра. После повышения сервера-члена до контроллера домена будет выполняться репликация зон DNS.

Чтобы обеспечить надлежащее преобразование имен контроллеров домена, понадобится протестировать распознавание DNS. Выполните проверку записей ресурсов служб с помощью инструментов `NsLookup` и `DcDiag`, как было описано в главе 6.

Подготовка исходного контроллера домена

Вы должны спланировать, что будете делать с исходным контроллером домена, до самой операции. Если сервер предполагается оставить в домене как контроллер домена, потребуется не так уж много. Если же сервер будет повторно развернут, вы должны продумать, каким образом возместить отсутствие этого сервера в сети.

Вам понадобится собрать перечисленные ниже данные для исходного сервера, чтобы применить аналогичные настройки к целевому серверу-члену после повышения до контроллера домена.

- Имя сервера.
- IP-адреса (IPv4 и IPv6).
- Назначенный сайт Active Directory.
- Назначенная организационная единица.
- Применяемые объекты GPO и результирующий набор политики (RSOP). Для помещения результатов в текстовый файл можете выполнить команду `gpresult /scope computer > GPOResult.txt`.
- Назначенные роли FSMO. Они будут перемещены, если сервер будет выведен из эксплуатации.
- Роль глобального каталога.
- Дополнительные службы, такие как DHCP, File and Print Services, а также Internet Authentication Services для VPN-подключений.

Наконец, создайте резервные копии данных состояния системы для всех контроллеров домена и резервные копии файловой системы для важных служб, которые предполагается вынести за пределы AD DS.

Повышение сервера-члена

В Windows Server 2012 инструмент `DCPromo` объявлен устаревшим и все возможности, необходимые для Active Directory Domain Services, предоставляются посредством ссылки Add Roles and Features (Добавить роли и компоненты) в диспетчере серверов (рис. 25.1). В процессе установки будут добавлены все обязательные компоненты для Active Directory Domain Services, в том числе модули PowerShell, инструменты командной строки и центр администрирования.

Подобно инструменту `DCPromo`, вам будет оказана помощь в подключении к серверам DNS, пространствам имен и контроллерам домена.

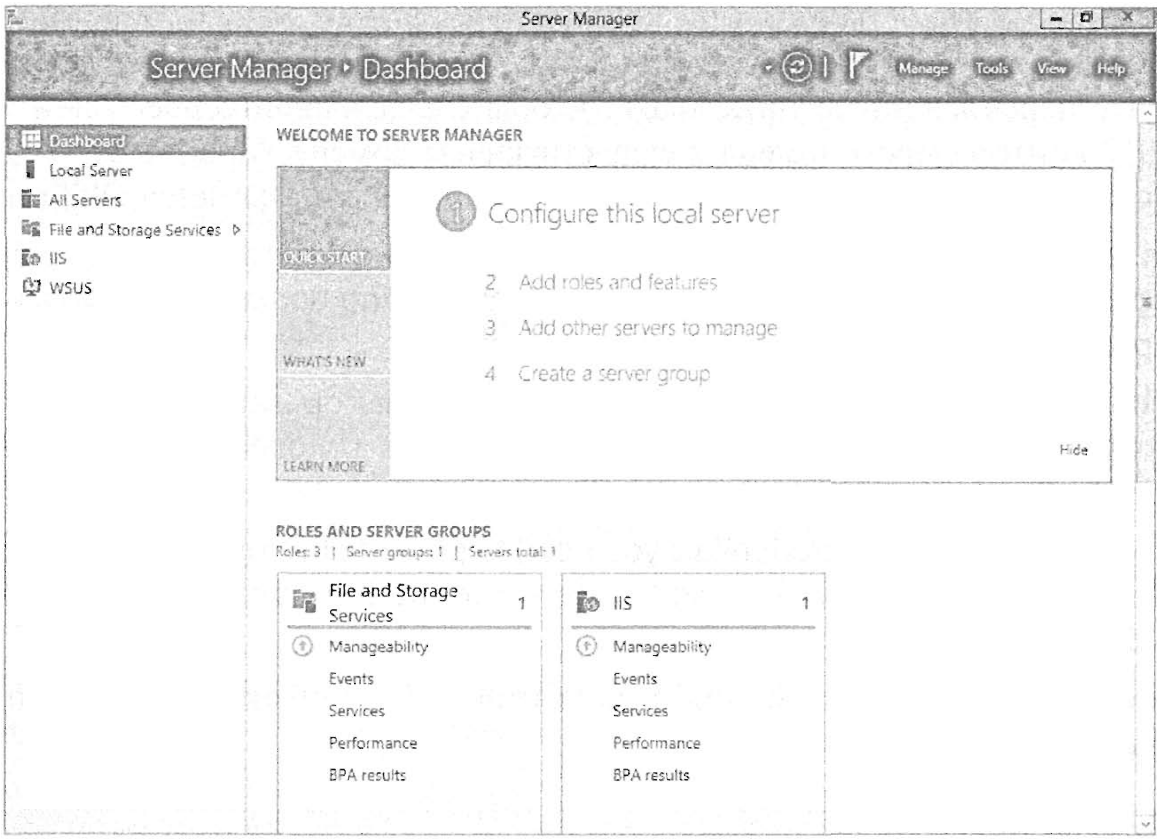


Рис. 25.1. Ссылка Adding Roles and Features в диспетчере серверов

Перед присоединением к домену вы должны завершить установку обязательных базовых компонентов; мастер добавления ролей и компонентов (Add Roles and Features Wizard) проведет вас через этот процесс. Установка всех компонентов займет несколько минут, после чего вам будет предложена ссылка Promote this server to a domain controller (Повысить этот сервер до контроллера домена), как показано на рис. 25.2.

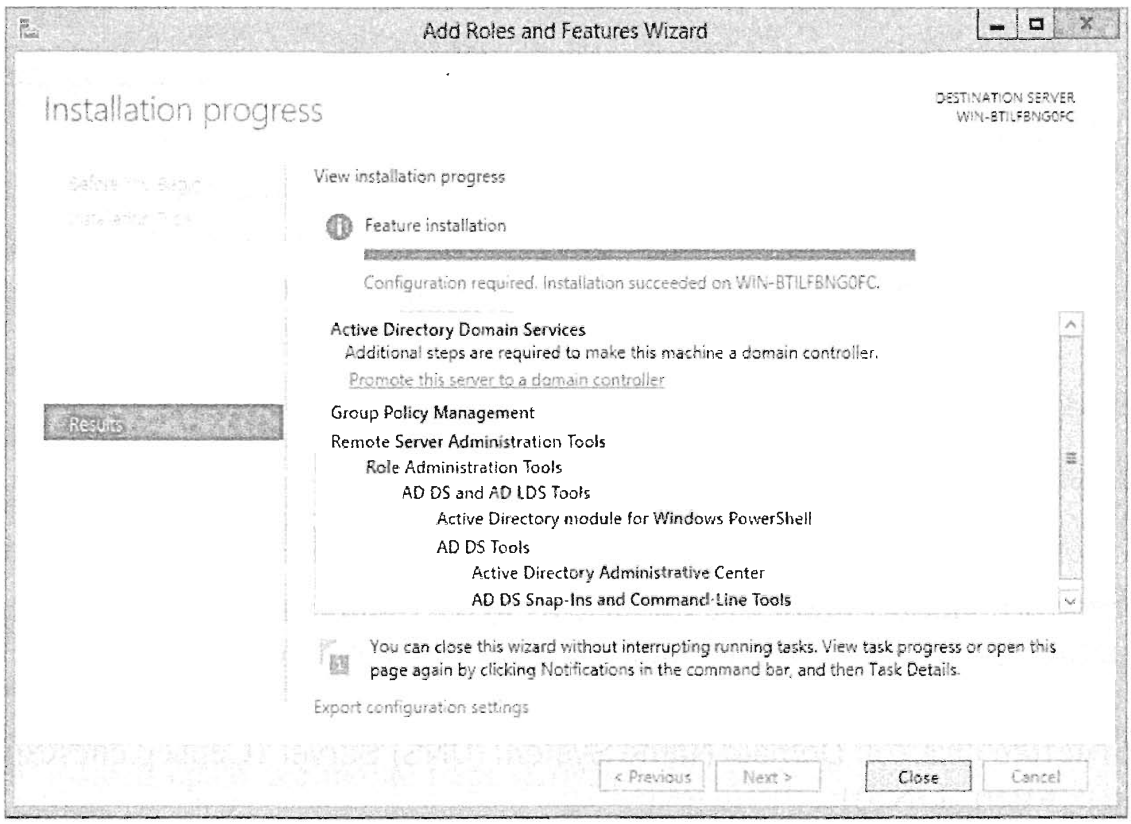


Рис. 25.2. Повышение сервера-члена до контроллера домена

В результате щелчка на этой ссылке запустится мастер конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard). Выполните перечисленные ниже шаги, чтобы сделать свой сервер-член Windows Server 2012 контроллером домена в существующем домене Windows Server 2008 R2. Домен, с которым проводится работа в данном примере, называется Oldfirm.com.

1. На первом экране мастера AD DS Configuration Wizard оставьте выбранным переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен).
2. В области Specify the domain information for this operation (Укажите информацию о домене для этой операции) укажите в поле Domain (домен) имя `Oldfirm.com`.
3. В области Supply the credentials you need to perform this operation (Предоставьте учетные данные, необходимые для выполнения этой операции) введите `Oldfirm\oldadmin`.
4. После того как информация задана (рис. 25.3), щелкните на кнопке Next (Далее).

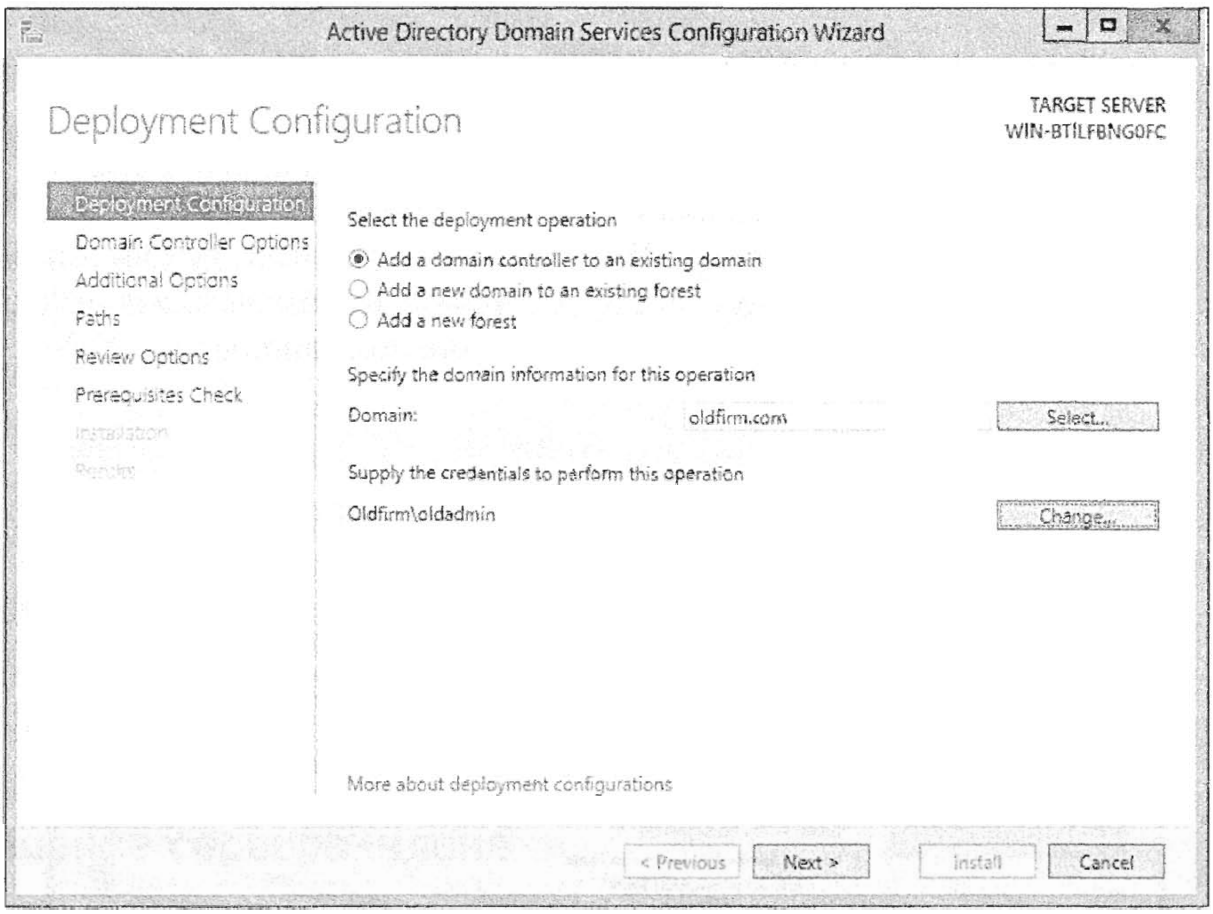


Рис. 25.3. Информация о членстве в домене

5. После того как вы пройдете процедуру аутентификации, и мастер конфигурирования продолжит свою работу, выберите подходящие параметры для своего контроллера домена:
   - отметьте флажок Domain Name System (DNS) Server (Сервер системы доменных имен (DNS));
   - отметьте флажок Global Catalog (GC) (Глобальный каталог (GC));

- отметьте флажок Read-only domain controller (RODC) (Контроллер домена только для чтения (RODC));
- в поле Site name (Имя сайта) укажите подходящий сайт;
- в полях Directory Services Restore Mode Password (DSRM) введите пароль администратора режима восстановления службы каталогов.

6. Щелкните на кнопке Next.
7. Укажите параметры делегирования DNS и щелкните на кнопке Next.
8. Выберите либо переключатель Install from Media (Установка с носителя), либо переключатель Replicate from a Domain Controller (Репликация из контроллера домена).

   Вы можете выполнить репликацию из любого контроллера домена или, если у вас распределенная сеть, выбрать быстродействующий канал для данного расположения.

9. Укажите местоположение базы данных AD DS, журнальных файлов и папки SYSVOL. Щелкните на кнопке Next.
10. Просмотрите выбранные параметры.

    На этом экране также присутствует кнопка View Script (Просмотреть сценарий). Как и в случае со многими компонентами Windows Server 2012, вы можете просмотреть и сохранить сценарий PowerShell, используемый для выполнения этой операции.

11. После просмотра выбранных параметров щелкните на кнопке Next.
12. Перед повышением этого сервера до контроллера домена вы должны убедиться в удовлетворении предварительных условий.

    При наличии каких-то проблем в любом разделе мастер конфигурирования предоставит базовую информацию о том, как устранить эти проблемы, а также веб-ссылку для получения более подробных сведений.

13. Убедившись в том, что все предварительные условия удовлетворены и конфигурирование проведено нормально, щелкните на кнопке Install (Установить).

    Обычно выполнение этой задачи `DCPromo` занимает несколько минут, и вы будете видеть информацию о ходе выполнения, если во время установки оставите окно мастера открытым.

14. Перезагрузите систему. Опция принудительной перезагрузки системы не предоставляется; вам придется выполнить ее самостоятельно.

После перезапуска сервер становится контроллером домена в домене Oldfirm.com и будет готов принять на себя любые роли FSMO и обязанности, которые вы предусмотрите для него. Одна из замечательных особенностей этого процесса постепенной миграции заключается в том, что в ходе задач повышения сервера до контроллера домена ОС Windows Server 2012 выполнит всю репликацию базы данных, папки SYSVOL и журналов, необходимую для получения полностью функционирующего контроллера домена сразу же после перезагрузки. Поскольку речь идет о постепенной миграции всех контроллеров домена на Windows Server 2012, можете приступать к определению и переносу на этот контроллер домена некоторые ролей FSMO.

Мониторинг производительности нового контроллера домена

Как правило, вы должны оставить этот контроллер домена Windows Server 2012 подключенным к сети и в течение нескольких дней не вносить в систему другие изменения, чтобы провести мониторинг его производительности и обнаружить возможные аномалии.

Постмиграционные процедуры

После миграции вы должны проверить доменные службы. Для выявления изначальных проблем выполните инструментальные тесты с использованием Event Viewer (Просмотр событий), `DcDiag` и `NetDiag`. Вы должны также провести тестирование приемлемости для пользователя, попробовав, например, войти в домен и обратиться к сетевым ресурсам посредством нового контроллера домена в качестве доступной службы аутентификации.

С учетом планов для процесса миграции, потребуется выполнить перечисленные ниже действия.

- Перенос ролей FSMO и назначение роли глобального каталога.
- Переназначение IP-адресов.
- Переназначение сетевых имен. Контроллер домена можно переименовать с помощью аплета System (`sysdm.cpl`) панели управления или команды `netdom renamecomputer`.
- Для DNS может потребоваться переназначение стандартных основных зон.

Откат несложен. Если во время процесса повышения произошел отказ, повторный запуск мастера Add Roles and Features Wizard на целевом контроллере домена должен привести к удалению любой записи об этом компьютере из базы данных Active Directory. В противном случае решить проблему поможет ручное удаление соответствующего объекта компьютера в оснастке Active Directory Sites and Services.

Переналадка оборудования

Постепенная миграция предоставляет возможность повторно развернуть существующий контроллер домена как контроллер домена Windows Server 2012. Помните, что ОС Windows Server 2012 доступна только в виде 64-разрядных редакций, поэтому модернизация любых 32-разрядных серверов Windows Server 2003 или Windows Server 2008 невозможна.

Эта процедура требует наличия виртуальной машины или оборудования, способного поддерживать Windows Server 2008 R2. Такая запасная машина служит промежуточной фазой между двумя состояниями Active Directory. Выполните указанные ниже общие действия.

1. Подготовьте схему леса и домен.
2. Постройте на запасной машине сервер-член Windows Server 2012.
3. Убедитесь в том, что система DNS адекватно поддерживает Active Directory.
4. Подготовьте исходный сервер.
5. Повысьте запасной сервер-член.

6. Подобно постмиграционным процедурам, вы должны удостовериться в стабильном функционировании сети, а также в возможности пользователей получать доступ к ресурсам. Запустите `DCPromo`, чтобы удалить Active Directory из исходного контроллера домена. После этого данный компьютер будет указан как сервер-член в домене.
7. Постройте сервер-член Windows Server 2012 на исходном оборудовании. Вы можете применять то же самое имя и IP-адрес, как у исходного сервера, при условии, что удалите учетную запись компьютера из Active Directory.
8. Повысьте сервер-член до контроллера домена.
9. Выполните постмиграционные процедуры, включая просмотр местонахождения ролей FSMO. Запасной контроллер домена может иметь роли FSMO, назначенные ему в результате вывода из эксплуатации исходного контроллера домена.
10. После проверки функционирования служб домена и контроллера домена запасной компьютер можно вывести из эксплуатации.

Постепенная миграция из Windows Server 2003

Многие организации до сих пор активно используют Windows Server 2003 в качестве основного домена Active Directory, рассматривая в будущем возможность перехода на Active Directory версии Windows Server 2012.

Чтобы провести миграцию старой системы на Active Directory версии Windows Server 2012, понадобится выполнить процесс, подобный описанному в предыдущем разделе, и построить сервер-член Windows Server 2012, добавив на него роль Active Directory Domain Services (AD DS). Как указывалось ранее, для создания сервера-члена настоятельно рекомендуется применять виртуальную инфраструктуру. После получения всех необходимых резервных копий контроллеров домена и схемы вы будете готовы приступить к миграции.

Перенос ролей FSMO

Запуск процесса несколько отличается, если функционирует Windows Server 2008 R2, т.к. Windows Server 2003 не поддерживается. Вам нужно перенести роли FSMO на новый контроллер домена Windows Server 2012.

Откройте консоль Active Directory Domain and Trusts и внесите изменения в роли FSMO следующим образом.

1. Перенесите роль RID Master на новый контроллер домена Windows Server 2012.
2. Перенесите роль PDC Emulator.
3. Перенесите роль Infrastructure Master.

Соответствующие вкладки расположены последовательно, поэтому никаких неожиданностей возникнуть не должно. После выполнения указанных действий понадобится вручную запустить репликацию домена. Рекомендуется отвести по паре минут на то, чтобы каждое изменение, касающееся домена в целом, вступило в действие и стабилизировалось, после чего вручную синхронизировать их. Время, которое займет весь этот процесс, зависит от количества имеющихся контроллеров домена и скорости каналов передачи данных.

После внесения изменений и синхронизации домена можете воспользоваться консолью Active Directory Domain and Trusts и заменить текущий контроллер домена контроллером домена Windows Server 2012. Это может сводиться к простой верификации, т.к. к данному моменту текущий контроллер домена *уже* может быть контроллером домена Windows Server 2012, но в этом нужно убедиться. Теперь необходимо перенести на контроллер домена Windows Server 2012 роль Domain Naming Master.

Изменение роли Schema Master

Роль Schema Master принадлежит одному из контроллеров домена; она будет выполнять все обновления и модификации схемы Active Directory. Схема является той частью Active Directory, которая определяет все объекты и ассоциированные атрибуты для всех элементов в домене, а также управляет обработкой каталога и всех его объектов. Поскольку для каждого каталога существует только один хозяин схемы, его перенос не производится в обычной манере.

Чтобы перенести роль Schema Master, откройте окно командной строки с повышенными полномочиями и выполните следующие шаги.

1. Введите команду `regsvr32 schmmgmt.dll`.

   Всплывающее окно сообщит, успешно ли выполнилась эта команда.
2. Если команда выполнилась успешно, щелкните на кнопке OK и закройте окно командной строки.
3. Откройте консоль MMC (это можно сделать из начального экрана Windows Server 2012).
4. Выберите в меню File (Файл) пункт Add/Remove Snap-in (Добавить или удалить оснастку).
5. Выберите оснастку Active Directory Schema (Схема Active Directory) и щелкните на кнопке Add (Добавить).
6. Щелкните на кнопке OK.

   Это должно привести к открытию новой консоли MMC с загруженной и готовой к использованию схемой Active Directory.

Предостережение

Вносить изменения в схему всегда необходимо с чрезвычайной осторожностью. Даже если в ходе этой процедуры вы не удаляете или не добавляете любые записи, вы должны действовать предельно аккуратно.

Теперь внутри оснастки Active Directory Schema вы должны проверить, что подключены к новому контроллеру домена Active Directory Windows Server 2012. Удостоверившись в этом, выполните перечисленные ниже действия.

1. Щелкните правой кнопкой мыши на Active Directory Schema и выберите в контекстном меню пункт Operations Manager (Диспетчер операций).
2. Выберите Change Schema Master (Изменить хозяина схемы).
3. Щелкните на кнопке Yes (Да) в окне с предложением подтвердить выбранную задачу.
4. Закройте раздел Change Schema Master.

Теперь вам нужно реплицировать контроллеры домена и дать им несколько минут на обновление базы данных Active Directory. После этого можно переходить к выполнению следующих двух задач, которыми являются удаление сервера Windows Server 2003 как сервера глобального каталога (GC) и затем удаление сервера Windows Server 2003 как контроллера домена.

Процесс удаления сервера как сервера GC довольно прост. Откройте консоль Active Directory Sites and Services на новом контроллере домена Windows Server 2012, перейдите на соответствующий сайт и выберите папку Servers (Серверы). В этой папке вы должны увидеть свой контроллер домена Windows Server 2003. Выберите его и выполните следующие шаги.

1. Щелкните правой кнопкой мыши на NTDS Settings (Параметры NTDS) и выберите в контекстном меню пункт Properties (Свойства).
2. На вкладке General (Общие) открывшегося диалогового окна NTDS settings Properties (Свойства параметров NTDS) снимите отметку с флажка Global Catalog (Глобальный каталог).
3. Щелкните на кнопке Apply (Применить), а затем на кнопке OK, чтобы изменение вступило в силу.

После репликации вы можете воспользоваться `DCPromo`, чтобы удалить свой контроллер домена Windows Server 2003. Но прежде чем сделать решающий шаг, не забудьте выполнить `Netdom` и запросить роли FSMO. Удостоверьтесь в отсутствии ошибок в журнале событий, в частности, связанных со службами каталогов (Directory Services).

Постепенная миграция: доводы за и против

Ниже перечислены доводы в пользу проведения постепенной миграции.

- Ее реализация носит последовательный характер. После внедрения первого контроллера домена Windows Server 2012 остальные контроллеры домена можно модернизировать или заменять по мере необходимости.
- Ваши пользователи сохраняют свои старые идентификаторы SID, а домен сохраняет свои старые доверительные отношения, поэтому любые серверы в других доменах — например, в доменах ресурсов, которые содержат файловые серверы и серверы печати или почтовые серверы — будут по-прежнему без проблем опознавать этих пользователей.
- Пользователи сохраняют свои старые пароли.
- Постепенная миграция предоставляет возможность повторного развертывания Windows Server 2012 на исходном сервере.

Этот метод не лишен недостатков. Ниже перечислены наиболее типичные из них.

- Чтобы обеспечить гладкий переход, требуется больший объем подготовительных работ и планирования.
- Любой накопившийся за время работы "мусор" останется в базе данных Active Directory.

Миграция домена Active Directory

Этот третий подход характеризуется как *чистый и изначальный*. При таком подходе вы оставляете в неприкосновенности существующие домены (домены AD, основанные на Windows Server 2003 или Windows Server 2008 R2) и создаете новый пустой домен AD. Затем вы используете программу, которая называется *инструментом миграции*, для копирования учетных записей пользователей и компьютеров из старого домена (или доменов) в новый домен AD.

Преимущество этого метода заключается в его последовательности. Процесс миграции может растянуться на достаточно продолжительный период, в течение которого вы можете заняться тестированием и решением возникающих проблем. Во время этого периода пользователям по-прежнему необходим доступ к своим данным. Обеспечить такой доступ можно путем переназначения разрешений или просто положиться на возможности хронологии SID.

Миграция домена является последовательной

В отдельных случаях мы отдаем предпочтение методу миграции домена. Прежде всего, он носит последовательный характер. При модернизации на месте вы отправляете свой домен в путешествие без возврата. Если впоследствии обнаружится, что AD на основе Windows Server 2012 — вовсе не то, что вам требуется, вы окажетесь в тупике. Но если у вас есть новый домен и вы копируете на этот домен подмножество пользователей, то вам останется только сообщить пользователям о необходимости входа в этот новый домен. Если после использования новым доменом в течение одной или двух недель окажется, что такая среда AD не подходит, вы всегда можете предложить пользователям возвратиться к своим учетным записям в старом домене.

Несмотря на то что метод постепенной миграции также является последовательным, его процесс все-таки оставляет после себя всевозможные артефакты, которые могут обусловливать низкую производительность и усугублять проблемы, которые предполагалось решить посредством миграции. Со временем неосведомленные администраторы могут сконфигурировать Active Directory таким способом, который может привести в замешательство тех, кто прочитал эту книгу и понимает что к чему. Эти проблемы по-прежнему придется решать после выполнения миграции домена на более новую версию.

Подход с миграцией домена также предоставляет промежуточную фазу, которая не доступна в двух других подходах. Во время этой промежуточной фазы у вас появляется возможность протестировать процесс, убедившись в том, что пользователи смогут обращаться к своим ресурсам, и выявить ряд типичных проблем, которые могут возникнуть в ходе последующих запусков миграции в производственной среде. Это избавляет от затруднений, связанных с отсутствием возврата.

Обработка разрешений с помощью нового домена

Предположим, что вы решили задействовать метод миграции домена. Так как здесь будет промежуточная фаза, вы можете рассчитывать на то, что пользователи организации будут членами старого домена или нового домена. Это потребует, чтобы пользователи в новом домене могли обращаться к файлам и другим ресурсам в старом домене.

Миграции в пределах одного леса

Имейте в виду, что те же самые процессы применимы и к миграциям в пределах одного леса. В главе 23 вы узнали, что лес представляет собой группу доменов, построенных как связанные друг с другом.

Иногда возникает необходимость переместить пользователей, компьютеры и группы в другой домен внутри леса. Миграция этих объектов из одного домена в другой в лесе производится с помощью таких процедур. Основное отличие заключается в том, что объекты вроде пользователей и групп должны быть перемещены, а не скопированы. После создания целевой учетной записи пользователя его исходная запись удаляется. При выполнении отката миграция учетных записей обратно в исходный домен осуществляется с помощью инструмента Active Directory Migration Tool (ADMT). В новом домене создаются новые учетные записи компьютеров, но старые учетные записи компьютеров блокируются для целей возможного отката. Есть две комбинации объектов, которые необходимо мигрировать вместе. Их называют *закрытыми наборами*.

- **Пользователи и глобальные группы.** Членами глобальных групп могут быть только пользователи и другие глобальные группы из того же домена. Когда пользователь изменяет домен, он уже не может быть членом своей исходной группы. При перемещении глобальной группы ее члены из исходного домена также удаляются. Их нужно мигрировать вместе, чтобы сохранить доступ в границах правил членства в глобальных группах.
- **Компьютеры ресурсов и локальные группы домена.** Ресурсы не могут назначать разрешения локальным группам домена из других доменов. Если миграция компьютера производится без назначенных локальных групп домена, то этот компьютер не сможет видеть идентификатор SID группы в маркере безопасности пользователя, предназначенном для доступа. В качестве альтернативы можете изменить область действия группы с локальной домена на универсальную, но это повлияет на размер глобального каталога.

Растягиваясь на два домена, организация будет сильно зависеть от доверительных отношений между контроллерами доменов до тех пор, пока все серверы, содержащие ресурсы, не окажутся на той же стороне, что и пользователи.

Каким образом пользователи в новом домене будут поддерживать такой же доступ к ресурсам, какой у них был в старом домене? Для руководства организации очень важно поддерживать непрерывность ее функционирования; руководство должно обеспечить своим сотрудникам постоянный доступ к их данным. Гладкая миграция минимизирует любые перерывы в доступе.

Существуют два подхода к обеспечению доступа к ресурсам.

- **Списки ACL.** Аббревиатура ACL означает *access control list* (список управления доступом) — технический термин для обозначения вкладки Security (Безопасность) диалогового окна свойств ресурса, подобного общей папке.
- **Хронологии SID.** Идентификатор безопасности (security identifier — SID) представляет собой уникальное число, назначаемое учетной записи для идентификации ее в рамках структуры разрешений.

Если вы будете неотрывно следить за экраном во время открытия вкладки Security диалогового окна свойств файла, то сможете заметить идентификатор SID в списке ACL до того, как компьютер преобразует этот SID в дружественное отображаемое имя.

Пример из практики

Миграция доменов применительно к случаю слияния компаний

Один из авторов книги имел дело с фирмой, представляющей собой объединение 11 небольших компаний, каждая из которых пользовалась своей инфраструктурой Active Directory. В определенных местах это имело наибольший смысл или предоставляло сотрудникам возможность решать задачи в собственных границах. Одной из главных проблем этой фирмы была высокая текучесть кадров среди IT-специалистов. Когда один из IT-администраторов увольнялся, это часто создавало крупную брешь в знаниях и поддержке. Было принято решение, что наряду с грядущей модернизацией до Active Directory версии Windows Server 2012 все эти домены будут консолидированы в один. Руководство вновь сформированного леса и домена хотело объединить леса Active Directory мелких компаний в один лес, чтобы обеспечить унифицированную систему сообщений на основе Exchange Server и сократить административные накладные расходы и риски.

Казалось, что сетевые среды многих этих небольших компаний удерживались в относительно целостном состоянии только за счет постоянного "склеивания". Неожиданные простои систем были общим явлением, а производительность снижалась по прошествии всего нескольких дней работы после очередной перезагрузки.

Чтобы решить проблемы в стареющей и собранной по частям среде, администраторы и IT-специалисты, занятые неполный рабочий день, обеспечивали временные решения, которые впоследствии становились постоянными. Похожие решения были и в Active Directory. Количество учетных записей пользователей втрое превышало фактическое число сотрудников. Количество учетных записей компьютеров также было больше реального числа компьютеров. Недокументированное решение VPN, которое опиралось на исходный контроллер домена, нельзя было переконфигурировать. Таким образом, модернизация на месте или постепенная миграция потенциально могли бы привести к уничтожению туннеля в сеть для удаленных пользователей. Было решено, что наилучшим подходом в данной ситуации будет полная миграция доменов. Это могло бы обеспечить инфраструктуру централизованного управления и поддержки, в которой отчаянно нуждалась фирма.

Повторное создание списков ACL для сервера

Один из подходов является вполне очевидным (и весьма трудоемким): просто обойдите все старые серверы и добавьте в списки разрешений на них новую учетную запись пользователя. Это называется повторным созданием списка ACL. Такая работа могла бы стать настоящей головной болью, однако некоторые инструменты миграции могут делать это автоматически.

Не принимая во внимание общие затраты, которые сулит этот процесс, особенно когда действия нужно проделать для более 100 открытых ресурсов и свыше 100 групп или пользователей, при его выполнении довольно высока вероятность допущения ошибок. Возможность непреднамеренной отмены доступа для одной группы, предоставления доступа не той группе или не добавления по забывчивости какой-то другой обязательной группы значительно снижает привлекательность данного подхода.

Использование хронологий SID

Вы уже знаете, что каждый пользователь располагает идентификатором SID. Так повелось со времен NT 3.1. Но на функциональных уровнях домена, начиная

с Windows 2000 Server в собственном режиме и заканчивая Windows Server 2008 R2, среда Active Directory позволяет каждому пользователю иметь несколько SID. Когда инструменты миграции создают новые учетные записи пользователей AD, эти учетные записи получают новые идентификаторы SID. Однако с помощью средства, называемого *хронологией SID*, инструменты миграции могут также прикреплять старые SID пользователя к новой учетной записи пользователя. После этого, когда пользователь попытается обратиться к какому-то ресурсу, к которому он имел доступ под своей старой учетной записью, рабочая станция попробует подключить его к этому ресурсу с применением новой учетной записи Active Directory.

Как и в случае всех входов в домен, AD создает для пользователя *маркер*, который содержит идентификатор SID пользователя, а также идентификаторы SID любых глобальных и универсальных групп, к которым принадлежит этот пользователь. Принцип использования хронологий SID заключается в следующем: среда AD сообщает, что Мэтью является членом группы с *этим* SID, и отправляет его старый SID из старого домена. Хотя это идентификатор SID учетной записи пользователя, контроллер домена AD передает данный SID, как если бы он относился к глобальной группе, и вполне очевидно, что такой вариант является приемлемым.

Ресурс, просматривающий маркер, говорит: "Хм... Знаю я кого-нибудь из этих парней? Хорошо, вот SID этого пользователя ... Нет, мне этот парень незнаком... Но стоп, он же является членом группы 'Мэтью из старого домена'. Я имею ACL для этой группы, так что я догадываюсь, кто он такой". Таким образом, несмотря на то, что пользователь Мэтью вошел как член новой группы с новым SID, он притащил с собой старый SID, поэтому получает доступ к своим старым ресурсам.

Подход с хронологиями SID предпочтительнее метода с ACL, т.к. разрешения для доступа к ресурсам остаются незатронутыми. Важно обеспечить запись хронологий SID во время миграции и удостовериться в том, что доверительные отношения между доменами не фильтруют их, когда пользователи "пересекают границы доверия" с целью доступа к ресурсу.

Что необходимо для созданий хронологий SID

Вам необходим инструмент миграции, которому известно, как создавать хронологии SID. Это умеет делать бесплатный инструмент миграции Active Directory (Active Directory Migration Tool — ADMT) от Microsoft, который будет описан далее в главе. Доступны и другие инструменты миграции, но за них придется платить. Например, Quest Software предлагает комплект инструментов миграции, утвержденных в отрасли.

Инструменты миграции создают хронологии SID, когда копируют учетные записи пользователей из старого домена в новый домен с функциональным уровнем Windows Server 2012. Прежде чем инструмент миграции сможет работать, вы должны создать доверительное отношение между старым и новым доменами. Но не имеет значения, каким инструментом миграции вы располагаете; он не сможет создавать хронологии SID до тех пор, пока вы не создадите такое доверительное отношение с помощью утилиты `netdom` или мастера создания доверительного отношения (New Trust Wizard) в ADDT. Хронологии SID можно создавать только на доменах с функциональным уровнем Windows 2000 Server в собственном режиме или более современным. Таким образом, когда вы создаете чистый изначальный домен AD, удостоверьтесь, что он уже переведен на функциональный уровень Windows Server 2012 (в конце концов, вы строите совершенно новый домен, и можете извлечь из него максимум), прежде чем создавать доверительное отношение и запускать инструмент миграции.

Обратите внимание, что если вы планируете использовать инструмент ADMT, то должны оставаться на функциональном уровне Windows Server 2008 R2, т.к. ADMT v3.2 в настоящее время не поддерживает Windows Server 2012.

ОС Windows Server 2012 также включает возможность управления и конфигурирования хронологии SID из PowerShell; соответствующий модуль в PowerShell позволяет вносить изменения в конфигурацию и устанавливать размеры маркеров. Это совершенно необходимо для поиска и устранения любых проблем, которые могут возникать. За дополнительными сведениями о PowerShell и хронологии SID обращайтесь к статье по адресу `http://tinyurl.com/c25PSSIDHistory`.

Миграция домена (чистая изначальная): доводы за и против

Ниже перечислены некоторые преимущества такой миграции.

- Миграция позволяет проводить последовательные усовершенствования.
- Миграция *копирует* учетные записи пользователей, а не *переносит* их. Старые учетные записи остаются в неприкосновенности на тот случай, если что-то пойдет не так.
- Миграция позволяет строить контроллеры доменов посредством чистой установки, избегая дополнительной сложности и потенциальных проблем модернизации на месте.
- Миграция хорошо подходит для объединения доменов, сворачивая огромное количество доменов в один или несколько доменов.
- Новую доменную структуру можно формировать в виртуальной среде.

Хотя, как уже было сказано, миграция этого вида обладает таким важным преимуществом, как обратимость, она не лишена недостатков.

- Вам понадобится иметь больше машин, чем при простой модернизации. В новом домене потребуются машины (или виртуальные машины) для функционирования в качестве контроллеров домена.
- Большинство инструментов миграции не могут копировать пароли. Инструмент ADMT предоставляет для этого отдельную службу, которая должна быть установлена в исходном домене. В противном случае пользователям придется создавать новые пароли при первом входе в новый домен AD. Это не является проблемой, но при большом количестве удаленной рабочей силы может вызвать изрядную головную боль.
- Вам придется приобрести какой-то инструмент миграции. Вам доступен ADMT, но в действительности он предназначен для миграций малых масштабов — в лучшем случае 1000 пользователей. Более развитые инструменты миграции недешевы; расходы начинаются примерно с $10 на пользователя. Да, именно так — на пользователя, а не на администратора.
- Невозможно создать домен Active Directory с таким же именем NetBIOS или FQDN, как у исходного домена, поскольку это потребует возможности создания двух доменов с одним и тем же именем (т.к. при выполнении чистой изначальной миграции вы не выводите из эксплуатации старые домены).
- Чистая изначальная миграция требует большего объема работы. Вам придется позаботиться о том, когда именно перемещать любое заданное множество пользователей и групп, может понадобиться корректировка ACL или преобразование локальных профилей и т.д.

Использование бесплатного инструмента миграции ADMT от Microsoft

Если вы подумываете о чистой изначальной миграции, то вам нужен инструмент миграции, а необходимость платить за такой инструмент может привести к отказу от этого подхода к миграции. Тем не менее, компания Microsoft предлагает бесплатный инструмент миграции, который называется Active Directory Migration Tool (ADMT). Первоначально написанный для Microsoft компанией NetIQ, инструмент ADMT v3.2 поддерживает простоту использования, присущую его первой версии, и также добавляет ряд удобных возможностей.

Несовместимость версий

На момент написания книги версия ADMT v3.2 прямо не поддерживалась на Windows Server 2012 для миграции. Если вы хотите воспользоваться инструментом ADMT, то понадобится сконфигурировать сервер Windows Server 2008 R2, который сможет действовать в качестве хоста миграции. Кроме того, в новом домене Windows Server 2012 необходимо иметь контроллер домена Windows Server 2008 R2. Это позволит надлежащим образом установить инструмент ADMT и службу PES (Password Encryption Service — служба шифрования паролей).

После проведения миграции и завершения всех задач, включая перемещение пользователей и других компонентов для обеспечения их полной поддержки в новом домене Active Directory, вы можете с помощью `DCPromo` удалить контроллер домена Windows Server 2008 R2 и продолжить работу.

Если вы уже подняли свой домен Active Directory версии Windows Server 2012 до функционального уровня домена Windows Server 2012, воспользуйтесь указанными ниже командами PowerShell для выполнения отката. Чтобы возвратить функциональный уровень леса к Windows Server 2008 R2, выполните команду:

```
Set-AdForestMode -identify oldfirm.com -forestmode Windows2008R2Forest
```

Чтобы возвратить функциональный уровень домена к Windows Server 2008 R2, выполните команду:

```
Set-AdDomainMode -identity oldfirm.com -domainmode Windows2008R2Domain
```

Учитывая, что на данном этапе версия ADMT v3.2 не поддерживается формально, мы не намерены описывать здесь процедуру, с помощью которой можно было бы достичь требуемого результата. В Active Directory версии Windows Server 2012 предусмотрено немало параметров, которые помогут провести очистку текущего домена, получить великолепный отчет и проверить наличие ошибок. Гораздо лучше применить к Active Directory подход модернизации на месте или постепенной миграции, чем выполнять миграцию домена Active Directory.

Если вы все же решитесь на миграцию домена, то должны всерьез рассмотреть возможность получения дополнительной поддержки от Microsoft или частной консультационной компании. В следующих двух разделах мы пройдемся по основам доверительных отношений и посмотрим, как включить ряд специфичных политик безопасности и конфигураций, чтобы обеспечить возможность работы инструментов вроде ADMT. Мы предложим вам своего рода руководство по подготовке нового и старого домена к использованию любого инструмента или обновленной версии ADMT, которая вскоре может стать доступной.

Установка доверительного отношения

Хотя мы не собираемся рассматривать процесс установки ADMT v3.2, при выполнении любого вида миграции Active Directory чрезвычайно важно создать доверительное отношение между двумя доменами. Самый быстрый способ установки такого доверительного отношения предусматривает применение консоли Active Directory Domains and Trusts (`domain.msc`). Воспользуйтесь мастером New Trust Wizard для выполнения описанных ниже действий.

- Укажите тип доверительного отношения. Простым и эффективным здесь будет внешнее доверительное отношение.
- Укажите двухстороннее доверительное отношение. Учетным записям из каждого домена нужен будет доступ к ресурсам в другом домене.
- Создайте доверительное отношение в другом домене. Это требует наличия учетных данных администратора домена данного домена.
- Проверьте доверительное отношение, убедившись в том, что все работает корректно.

После установки доверительного отношения вы должны проверить, работает ли оно и корректны ли разрешения в двух доменах. Поскольку пользователи и глобальные группы из любого домена могут быть членами локальных групп домена и членами локальных групп сервера-члена, можно попробовать добавить пользователя из противоположного домена во встроенную группу на контроллере домена. Это обязательный шаг при использовании любого инструмента миграции. Итак, вы можете найти и добавить администратора домена Bigfirm во встроенную группу `Administrators` домена Oldfirm в оснастке Active Directory Users and Computers.

Но добавление пользователей и групп — это не то, что *действительно* необходимо. Мы хотим, чтобы мигрированные учетные записи имели возможность доступа к ресурсам в противоположном домене. Именно здесь в игру вступает хронология SID. Как утверждалось ранее, хронология SID трактуется как другая группа в маркере безопасности, который будет передаваться домену ресурсов для доступа к ресурсам со стороны мигрированных учетных записей.

Фильтрация SID на доверительных отношениях по умолчанию отключена, и если она должна быть включена, то это придется сделать вручную. Хронологией SID может воспользоваться злоумышленник при атаке с повышением привилегий. Он мог бы сконструировать маркер безопасности с SID администратора домена внутри доверяемого домена ресурсов. Из-за того, что SID распознается как принадлежащий администратору домена, учетная запись злоумышленника получит такой же уровень доступа. Фильтрация SID усекает любые идентификаторы SID, которые не происходят из доверенного домена пользователя. По существу маркер безопасности ваших пользователей не сможет нормально работать в исходном домене с включенной фильтрацией SID, т.к. значение хронологии SID отбрасывается. Проследовав по гиперссылке Securing external trusts (Защита внешних доверительных отношений) в окне с предупреждением о фильтрации SID, вы узнаете, что с помощью команды `netdom` можно отключать и включать фильтрацию SID для миграции, такой как проводимая в настоящее время.

Команда `netdom` устанавливается в составе Windows Server 2012, но обязательно поищите на сайте Microsoft ее актуальную версию.

Для отключения фильтрации SID запустите показанную ниже команду. Само отключение делает параметр /quarantine:no. Вы должны быть способны самостоятельно догадаться, как включить фильтрацию.

```
Rem выполняется на bf1.Bigfirm.com
Netdom trust oldfirm /domain:bigfirm /quarantine:No
/usero:administrator /passwordo:P@ssw0rd

Rem выполняется на of1.oldfirm.com:
Netdom trust bigfirm /domain:oldfirm /quarantine:No
/usero:administrator /passwordo:P@ssw0rd
```

Обеспечение дружественности к ADMT на обеих сторонах

Из-за своих потребностей ADMT может считаться совершенно пугающей программой. Она извлекает информацию, которая является закрытой и внутренней для домена — учетные записи и пароли пользователей — и открывает ее в совершенно другом домене. Прежде чем ADMT сможет делать это, вам придется открыть несколько запертых дверей. Ниже описано, что понадобится предпринять.

Помещение учетной записи администратора домена в группы Administrators в каждом противоположном домене

Инструменты, подобные утилите ADMT, нуждаются в учетной записи, которая является членом группы Domain Admins в целевом домене Bigfirm.com и членом локальных групп Administrators на серверах и рабочих станциях в исходном домене Oldfirm.com. Это позволит утилитам миграции вносить изменения в разрешения, права доступа пользователей и другие настройки, на что имеют привилегии все опытные администраторы. В рассматриваемом примере мы создали учетную запись с незамысловатым именем ADMT в домене Bigfirm.com и поместили ее в группу Domain Admins. Из-за наличия доверительного отношения между двумя доменами она была также помещена во встроенную группу Administrators внутри домена Oldfirm.com и в локальную группу Administrators на рабочей станции OFIT1.

В исходном домене Oldfirm.com имеется похожее требование для службы шифрования паролей (PES). Эта дополнительная служба будет читать пароль перемещаемой учетной записи, шифровать его и затем сохранять в свойствах новой учетной записи. Ее учетная запись должна быть членом группы Domain Admins в исходном домене Oldfirm.com и членом встроенной группы Administrators в целевом домене Bigfirm.com. Мы создали учетную запись с таким же незамысловатым именем PES в домене Oldfirm.com. В домене Bigfirm.com мы открыли оснастку Active Directory Users and Computers и добрались до папки Built-in (Встроенные), чтобы найти там группу Administrators. Затем мы сделали учетную запись PES членом этой группы.

Включение аудита

Инструмент ADMT имеет некоторые специфичные потребности аудита, скорее всего для того, чтобы он мог проводить мониторинг своих действий. В исходном домене — домене, из которого копируются пользователи, т.е. Oldfirm.com — должен быть включен аудит успехов и отказов для управления пользователями и группами.

На целевой и исходной машинах (Bf1.Bigfirm.com и OF1.Oldfirm.com) аудит включается путем модификации групповой политики, которая называется стандартной политикой контроллеров домена (Default Domain Controllers Policy). В Windows Server 2012 консоль управления групповыми политиками (Group Policy Management Console) устанавливается автоматически. Открыв эту консоль, доберитесь до контейнера Group Policy Objects (Объекты групповой политики). Затем щелкните правой кнопкой мыши на элементе Default Domain Controllers Policy и выберите в контекстном меню пункт Edit (Редактировать).

Чтобы получить искомую политику, последовательно раскройте узлы Computer Configuration (Конфигурация компьютера), Windows Settings (Настройки Windows), Security Settings (Настройки безопасности) и Local Policies (Локальные политики); внутри Local Policies вы увидите папку Audit Policy (Политика аудита). В папке Audit Policy дважды щелкните на элементе Audit Account Management (Аудит управления учетными записями) и удостоверьтесь, что флажок Define These Policy Settings (Определить следующие параметры политики) отмечен и рядом указано Success and Failure (Успех и отказ). Затем щелкните на кнопке Close (Закрыть).

Теперь, когда в конфигурацию внесены необходимые изменения, можно приступать к выбору инструмента миграции домена.

Установка ADMT и PES

Утилита ADMT доступна в виде загружаемого файла на веб-сайте Microsoft. Установка этой утилиты в чистой изначальной среде совершенно прямолинейна, т.к. импорт баз данных из предыдущих версий не выполняется. Будет выдан запрос о том, в каком формате должна быть создана база данных — SQL Express или в стандартном экземпляре SQL Server. В большинстве случаев предпочтение следует отдавать SQL Express.

Резюме

Внедрите в сеть новые версии Active Directory. Модернизация до новой версии Windows Server означает также необходимость в модернизации существующих контроллеров домена. Добавить в организацию новую версию Active Directory можно с помощью двух базовых методов — модернизации контроллера домена и модернизации домена за счет добавления нового контроллера домена.

> *Контрольный вопрос.* Обе операции требуют модификации базы данных Active Directory с использованием утилиты `adprep.exe`. С какими тремя параметрами ее нужно запускать? С каким еще параметром ее можно запускать?

Проведите миграцию доменных учетных записей из одного домена в другой. Требование перемещения пользователей и групп из существующего домена в чистый изначальный домен часто возникает при слиянии или разделении компаний. Кроме того, это может потребоваться, когда оправдана реструктуризация леса. Для выполнения миграций доменов Microsoft предлагает утилиту ADMT.

> *Контрольный вопрос.* Что обеспечивает пользователю доступ к ресурсам, находящимся внутри исходного домена, после того как учетная запись пользователя перенесена в новый домен?

Глава 26

Расширенное управление пользовательскими учетными записями и поддержка пользователей

Вы уже ознакомились с основами управления пользователями и группами. В настоящей главе мы переходим на следующий, более высокий уровень управления пользователями. Здесь вам придется задействовать некоторые навыки и умения, полученные в ходе изучения предыдущих глав этой книги, такие как управление общими файлами, пространствами имен распределенной файловой системы (Distributed File System — DFS) и объектами групповой политики (Group Policy object — GPO). С применением этих технологий вы можете разработать гибкую, отказоустойчивую и мобильную рабочую среду — то, что в Microsoft принято называть *динамической IT-средой*.

Мы расскажем о том, как развертывать решения, при которых данные и настройки пользователя следуют за ним по сети, для чего используются домашние каталоги и перемещаемые профили. Вы узнаете, как заставить пользователя работать в среде с ограниченной функциональностью, применяя для этого обязательные профили. Затем вы научитесь вносить небольшие изменения с помощью объектов GPO. Вы сможете управлять личным профилем пользователя с помощью настроек групповой политики (Group Policy). Вы сможете разрешать пользователю иметь разные перемещаемые профили для разных местоположений или для служб удаленного рабочего стола (Remote Desktop Services). Вы также узнаете, в каких случаях (когда приходится действовать в мире BYOD (bring-your-own-device — принеси свое собственное устройство)) в среде со смешанными устройствами можно отказаться от сложностей перемещаемых профилей, задействовав вместо них перенаправляемые папки. Эта технология позволяет брать папки на каком-либо устройстве и перемещать их на сервер незаметно для пользователя.

Перенаправляемые папки существуют уже достаточно давно, а в версии Windows Server 2012 для них добавлены возможности детализированного управления. ОС Windows Server 2012 и Windows 8 позволяют перенаправлять более важные папки на файловые серверы, чтобы персональные рабочие среды становились доступными для пользователей сразу же после входа — причем все это безо всяких сложностей, присущих перемещаемым профилям.

Вы также увидите, как использовать предпочтения групповой политики для управления отображениями дисков и как благодаря сценариям входа и выхода выполнять набор команд каждый раз, когда пользователь входит или даже выходит из системы. Вы узнаете об оптимальных способах подключения пользователей к ресурсам, подготовке которых вы уделили немало времени. Мы приведем реальные ситуации, где эти решения применяются для многих сценариев, с которыми вам придется столкнуться в ходе расширенного управления пользователями.

В этой главе вы изучите следующие темы:

- развертывание домашних каталогов для множества пользователей;
- настройка обязательных перемещаемых профилей;
- создание сценариев входа для автоматизации администрирования.

Освоение гибкого рабочего стола

Идеальный сценарий для рабочей среды пользователя заключается в том, что настольный компьютер, переносной компьютер или даже сервер удаленных рабочих столов является обыкновенным прибором.

Рассмотрим случай, когда инженер отдела технической поддержки принимает звонок от пользователя, у которого возникли проблемы с одним из его специальных приложений. По какой-то причине приложение работает некорректно. Унаследованный подход в организации сети настольных компьютеров требует от инженера присутствия возле этого настольного компьютера до тех пор, пока проблема не будет решена. На компьютере установлено множество программ. Пользователь хранит свои бизнес-данные в “разделе данных”. Настройки пользователя, включая архив электронной почты, почтовые контакты и избранные страницы веб-браузера, являются локальными на этом ПК. Инженеру технической поддержки не остается ничего другого, как исправить проблему с приложением, сколько бы времени это не потребовало.

Как бы ни совершенствовалось оборудование с целью повышения его надежности и увеличения времени наработки на отказ, устройства по-прежнему выходят из строя. Когда это случается, пользователи обращаются в IT-отдел с просьбой восстановить данные, которые хранились на их устройствах. Конечно, в составе Windows 8 и Windows 7 имеется инструмент резервного копирования, но располагаете ли вы достаточным временем и прочими ресурсами, чтобы управлять резервными копиями для сотен или даже десятков тысяч настольных и переносных компьютеров? Что бы произошло в таких сценариях, если устройство пользователя было бы не более чем прибором? Вы могли бы воссоздать это устройство с помощью чего-то наподобие служб развертывания Windows (Windows Deployment Services), инструментального набора развертывания от Microsoft (Microsoft Deployment Toolkit) или другого платного инструмента клонирования вроде диспетчера конфигурации системного

центра (System Center Configuration Manager — SCCM/ConfigMgr) 2012. Они позволяют буквально за считанные минуты развернуть образ конфигурируемой операционной системы. Развертывание программного обеспечения можно автоматизировать с помощью таких решений, как групповая политика (Group Policy), диспетчер ConfigMgr 2012 или продукт для виртуализации приложений от Microsoft под названием App-V. Это позволяет сконфигурировать устройство до заранее известного и управляемого стандартного состояния в течение еще нескольких минут.

Исправления быстро разворачиваются с помощью службы обновлений программного обеспечения Windows (Windows Software Update Services — WSUS) или диспетчера ConfigMgr 2012. Групповая политика конфигурирует среду. Теперь устройство защищено. Это замечательно, поскольку устройство возвращено в работоспособное состояние, а специальное приложение функционирует корректно, выполняя необходимые пользователю функции. Весь процесс потребовал не более 30 минут. Скорее всего, это заняло гораздо меньше времени, чем пришлось бы потратить инженеру технической поддержки на решение возникшей проблемы.

А что можно сказать о данных, которые пользователь хранил на этом устройстве? Либо вы сформатировали диск в результате перестройки устройства, либо данные были утеряны во время аппаратного сбоя. Но не переживайте — все это время данные находились на сервере. Если у пользователя был переносной компьютер, вы обеспечили локальную доступность этих данных с помощью синхронизированного кеша. Пользователь по-прежнему будет иметь доступ ко всем данным, когда он войдет в систему своего воссозданного заново устройства.

С помощью действий, которые будут раскрыты в этой главе, вы научитесь выполнять следующие задачи:

- создание резервных копий пользовательских данных;
- обеспечение большей доступности данных;
- разрешение пользователю переходить с одного устройства на другое или на сервер Remote Desktop при сохранении постоянного доступа к данным;
- сокращение времени поиска и устранения неполадок;
- избавление пользователей от излишних проблем;
- создание защищенных рабочих сред, в которых имеется совместно используемое вычислительное решение;
- предварительное конфигурирование рабочей среды для применения политик безопасности или обеспечение еще большего удобства пользования этой средой.

Конфигурирование домашних каталогов

Домашний каталог — это общая папка или папка на общем сетевом ресурсе, выделенная для пользователя. Каждый пользователь имеет собственный домашний каталог на файловом сервере. Суть этой концепции в том, что вы хотите предложить пользователям хранить свои данные на серверах, чтобы их было легче подвергать резервному копированию, аудиту и архивированию. Некоторые организации будут применять политику компании и групповую политику, чтобы предотвращать использование дисков на устройствах пользователей и тем самым заставлять их сохранять персональные данные в домашних каталогах.

Пример из практики

Когда нужно перестраивать устройство

Рассмотрим простое правило, которое поможет определить, когда нужно применять этот подход. Если возникшая проблема является уникальной для данного устройства (т.е. речь не идет о проблемах с сетью или совместно используемыми службами) и вам кажется, что ее решение займет более 30 минут, тогда вы должны перестроить машину. Это сохранит время специалистов IT, пользователя и компании в целом. К тому же пользователь получит долгосрочное стабильное решение. Может даже оказаться, что при таком сценарии опытные пользователи смогут самостоятельно перестроить устройство, если вы разрешите им поступать так.

Конечно, при этом предполагается, что вы применяете описываемые в настоящей главе методы хранения пользовательских данных за пределами устройства, а именно — на серверах. Вам также понадобится инструмент, подобный диспетчеру System Center Configuration Manager, для автоматического развертывания приложений, которые не содержатся внутри стандартных образов.

Домашние каталоги в организациях применяются двумя основными способами. Наиболее распространенный способ предполагает такую настройку разрешений домашнего каталога, чтобы он был личным; другими словами, пользователь является единственным лицом, имеющим доступ к содержимому. Локальным администраторам и локальным системам на сервере, вероятно, также понадобится доступ для выполнения операций администрирования, резервного копирования/восстановления и архивирования. Альтернатива, с которой вы, возможно, встречались в некоторых реализациях, предусматривает отсутствие приватности домашних каталогов. Домашний каталог рассматривается как персональный общий ресурс для совместного использования данных с другими пользователями сети в случае, когда применение обычных общих ресурсов для рабочей группы, отдела или компании в целом по ряду причин оказывается невозможным.

В подобных ситуациях некоторые будут выдвигать аргументы о том, что на каждом ПК есть много дешевого дискового пространства, а дисковое пространство на сервере является относительно дорогим. Не будет ли более экономным хранение данных на устройстве с их распространением по электронной почте? Однако мы утверждаем, что сторонники такой точки зрения видят только краткосрочные издержки. Электронная почта — неудачный способ обмена файлами. Прежде всего, файл, которым вы пытаетесь поделиться с другими, может оказаться слишком большим для пересылки, в результате чего он возвратится обратно отправителю. Но важнее всего то, что каждый получатель будет располагать собственной отредактированной копией, а возможности хоть какого-то управления версиями отсутствуют. Если вы используете сервер почтовых ящиков, такой как Exchange Server, то файл хранится на этом почтовом сервере. Но самое главное — организация должна быть в состоянии гарантировать, что ее бизнес-данные помещены в резервную копию или даже архивированы в защищенное хранилище, где они могут удерживаться в течение нескольких лет. Это является юридическими требованиями во многих организациях по всему миру, как государственных, так и частных. Каким образом вы собираетесь создавать резервные копии данных на своих устройствах? Как вы обеспечите архи-

вирование файлов без вмешательства со стороны пользователя? Вы обнаружите, что гораздо дешевле, удобнее и надежнее централизовать хранилище данных, выполняя одно резервное копирование и управляя одним автоматизированным архивом.

Другой аргумент против домашних каталогов, который мы часто слышим, исходит из отдела кадров или бухгалтерии. Они не хотят, чтобы специалисты IT-отдела имели возможность видеть их данные, поэтому предпочли бы хранить информацию на своих устройствах. Жаль разочаровывать этих людей, но любой заинтересованный администратор может получить доступ к данным, где бы они ни находились. Однажды нам пришлось иметь дело с отделом кадров, в котором решили хранить конфиденциальные данные на жестком диске USB, который запирали в сейфе. Можете ли вы представить себе хранение важных данных о сотрудниках компании в устройстве с механически движущимися элементами, которое способно в любой момент выйти из строя? Гораздо лучшим решением является наличие независимо контролируемого аудита доступа к данным на файловом сервере с четко документированными и доведенными до всеобщего сведения политиками и действиями, которые последуют в ответ на любые нарушения этих политик.

Далее мы покажем, как сконфигурировать домашние каталоги для пользователей в компании.

Установка испытательной среды

В этом примере вы будете работать с двумя серверами. Сервер BF1 представляет собой контроллер домена Windows Server 2012 R2 для организации BigFirm. Сервер BF2 является файловым сервером Windows Server 2012 R2. В сети также имеется настольный компьютер по имени Win81, работающий под управлением ОС Windows 8.1. Мы настоятельно рекомендуем выполнять любые работы в испытательной среде и тщательно все документировать, прежде чем переходить к производственной системе.

В этой главе вы узнаете, как применять пространства имен DFS каждый раз, когда вы пользуетесь общими файловыми ресурсами. Вы будете делать это по двум причинам.

- Вы можете абстрагироваться от физического местоположения общих файловых ресурсов.

  Пользователи и приложения отображаются на логическое имя, а не на физический сервер. Это означает, что вы можете перемещать общие файловые ресурсы с одного сервера на другой без необходимости в изменении конфигурации пользователей, сценариев входа или конфигурации приложений. Это очень удобно, когда какой-то сервер устаревает или когда на время отказа сервера данные нужно восстановить в другом месте. Вы можете быстро подкорректировать пространство имен, не прибегая к многочисленным изменениям, которые пришлось бы вносить в противном случае.

- Вы можете получить преимущества от применения репликации DFS (DFS Replication — DFS-R), оставив неизменными отображения дисков в конфигурациях пользователей, сценариях входа и настройках приложений.

  Это означает, что вы можете реплицировать пользовательские данные на другой сервер внутри другого сайта. Если в результате аварии вышел из строя

производственный сервер или даже весь сайт, то пользовательские данные будут доступны в другом месте через те же отображения дисков. Вы можете также внедрить более развитые стратегии резервного копирования. Например, вы можете применять службу теневого копирования томов (Volume Shadow Copy Service — VSS) для создания краткосрочных операционных резервных копий на производственном сайте. Вдобавок вы можете использовать сайт восстановления в аварийных ситуациях (disaster recovery — DR) для создания долгосрочных резервных копий, что иначе могло бы повлиять на производительность сети на производственном сайте.

Вы должны уже знать о том, как настраивать пространство имен и конфигурировать DFS-R. Вам предстоит применять пространство имен под названием `\\bigfirm.com\BigFirmShares`. Позже вы увидите, каким образом добавлять в это пространство имен папки, которые перенаправляются на общие ресурсы, содержащие персональные данные пользователя.

Создание домашних каталогов

Для каждого пользователя вам понадобится создать каталог и обеспечить его надежную защиту. При этом необходимо ответить на следующие вопросы.

- **Кто должен иметь возможность доступа к домашнему каталогу каждого пользователя?**

  Обычно доступ к этой папке должен быть предоставлен только пользователю, администраторам и учетной записи `System` (Система). Некоторые организации предпочитают трактовать домашний каталог как персональную папку, которую пользователь может применять для совместного использования данных с другими. В этом разделе мы продемонстрируем более привычный приватный подход.

- **Как вы назовете такие папки?**

  Некоторые люди предпочитают иметь дело с чем-то предсказуемым. Они называют такую папку по имени пользователя, которому принадлежит домашний каталог. Например, пользователь Joe Bloggs имеет учетную запись с именем `JBloggs`. Его домашний каталог будет называться `JBloggs`. Это облегчает выполнение автоматизированных задач, таких как подключение пользователя к общему ресурсу.

- **Как вы откроете общий доступ к такой папке?**

  Кто-то решает открывать общий доступ к каждому домашнему каталогу. Это влечет за собой большой объем работы. Другие предпочитают создавать один общий ресурс, а внутри него предусматривать папки для каждого пользователя. Это удовлетворяет требованиям обсуждавшегося ранее подхода DFS, потому что есть только одна ссылка DFS, которую понадобится изменить, если необходимо восстановить или переместить общий ресурс с домашними каталогами в новое место. Общая папка будет сделана доступной через пространство имен DFS.

Давайте приступим к созданию ряда домашних каталогов, но для начала нужно иметь несколько пользователей. Вопросам создания пользователей и групп была

посвящена глава 8, так что вы уже должны знать, как это делается. В оставшемся материале настоящей главы мы будем иметь дело с перечисленными ниже пользователями и группами.

Пользователи:

- `Alexandra Garcia` (Александра Гарсия)
- `Joe Bloggs` (Джо Блоггс)
- `Joe Elway` (Джо Элвей)

Группы:

- `Accounts` (Бухгалтерия)
- `Home` (Домашняя)
- `HR` (Кадры)
- `IT` (IT-отдел)
- `Profiles` (Профили)
- `Senior Management` (Старшее руководство)

Пользователи будут помещены в организационную единицу `\bigfirm.com\BigFirm\Users`, как показано на рис. 26.1. На протяжении данной главы вы будете конфигурировать рабочую среду для этих пользователей.

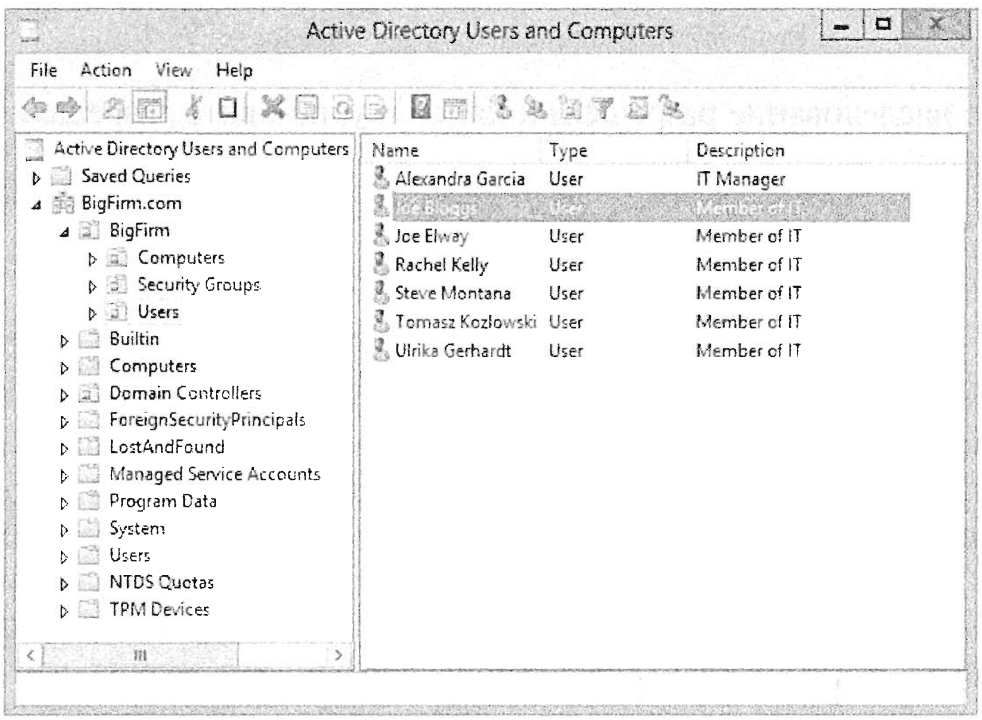


Рис. 26.1. Тестовый пользователь Joe Bloggs

На сервере BF2 будет создана общая папка по имени `Home`. Некоторым администраторам нравится создавать все общие ресурсы в единственной папке на файловом сервере. Такой подход преследует две цели.

- Поддерживается определенный порядок, и администраторы могут находить все общие ресурсы в одном местоположении.
- Намного облегчается автоматизация таких задач, как резервное копирование и репликация каталогов, поскольку для выбора имеется только одна папка.

Создайте папку по имени `Shares` на диске `D` (рис. 26.2).

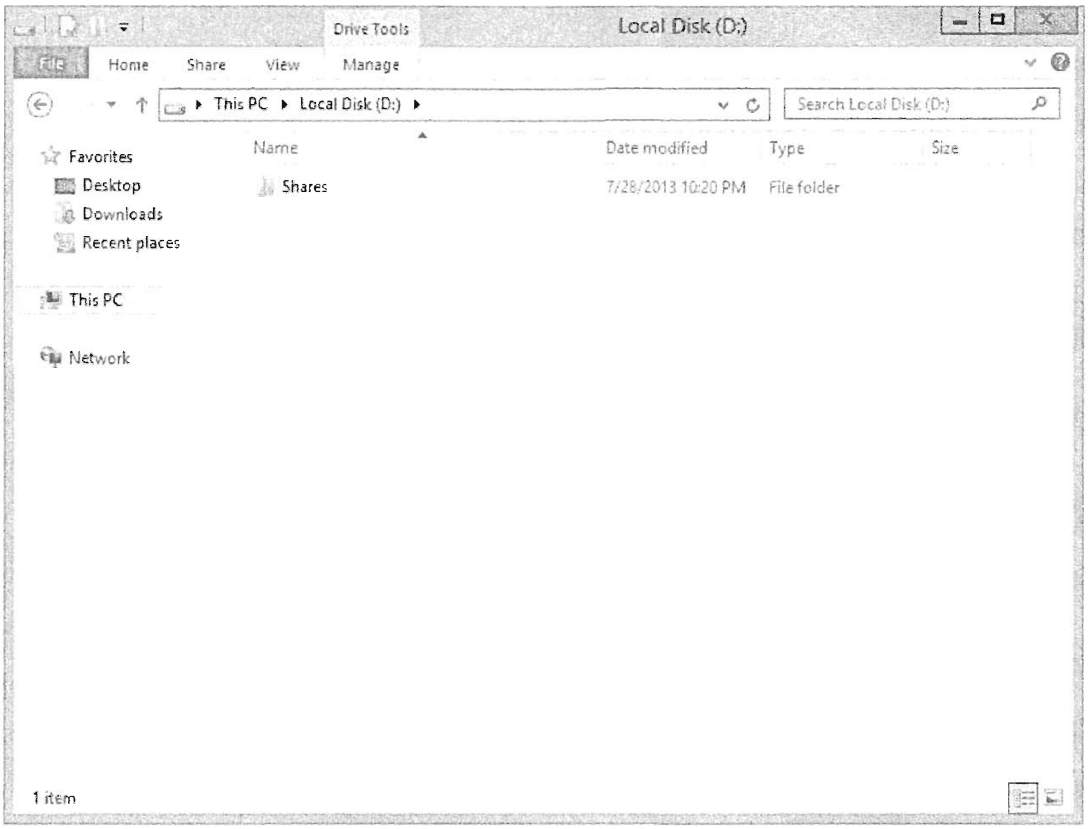


Рис. 26.2. Папка `Shares` на сервере BF2

Отключите наследование разрешений папок и установите разрешения папок следующим образом:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`System`	Full Control (Полный доступ)

Так делается потому, что любые папки, создаваемые в `D:\Shares`, по умолчанию будут наследовать эти разрешения. В результате обеспечивается защита новых общих папок. Именно вы (и другие администраторы) будете предоставлять доступ необходимым пользователям или группам доступа. Кроме того, это позволяет предотвратить создание здесь папок пользователями, которые не являются администраторами, без специального разрешения. Теперь создайте в `D:\Shares` папку по имени `Home`.

Далее к папке `Home` будет открыт общий доступ. Это значит, что для каждого пользователя можно будет создавать вложенные папки, но управлять только одним общим ресурсом. Целью такого подхода является упрощение развертывания и максимальное облегчение управления безопасностью.

Теперь вам предстоит воспользоваться инструментом File and Storage Services. Окно этого инструмента, показанное на рис. 26.3, откроется после щелчка на ссылке File and Storage Services (Службы файлов и хранилища) в управляющей панели диспетчера серверов и выбора вкладки Shares (Общие ресурсы).

В меню Tasks (Задачи) выберите пункт New Share (Создать общий ресурс), чтобы запустить мастер создания общего ресурса (New Share Wizard). Мастер предложит выбрать профиль для нового общего ресурса (рис. 26.4).

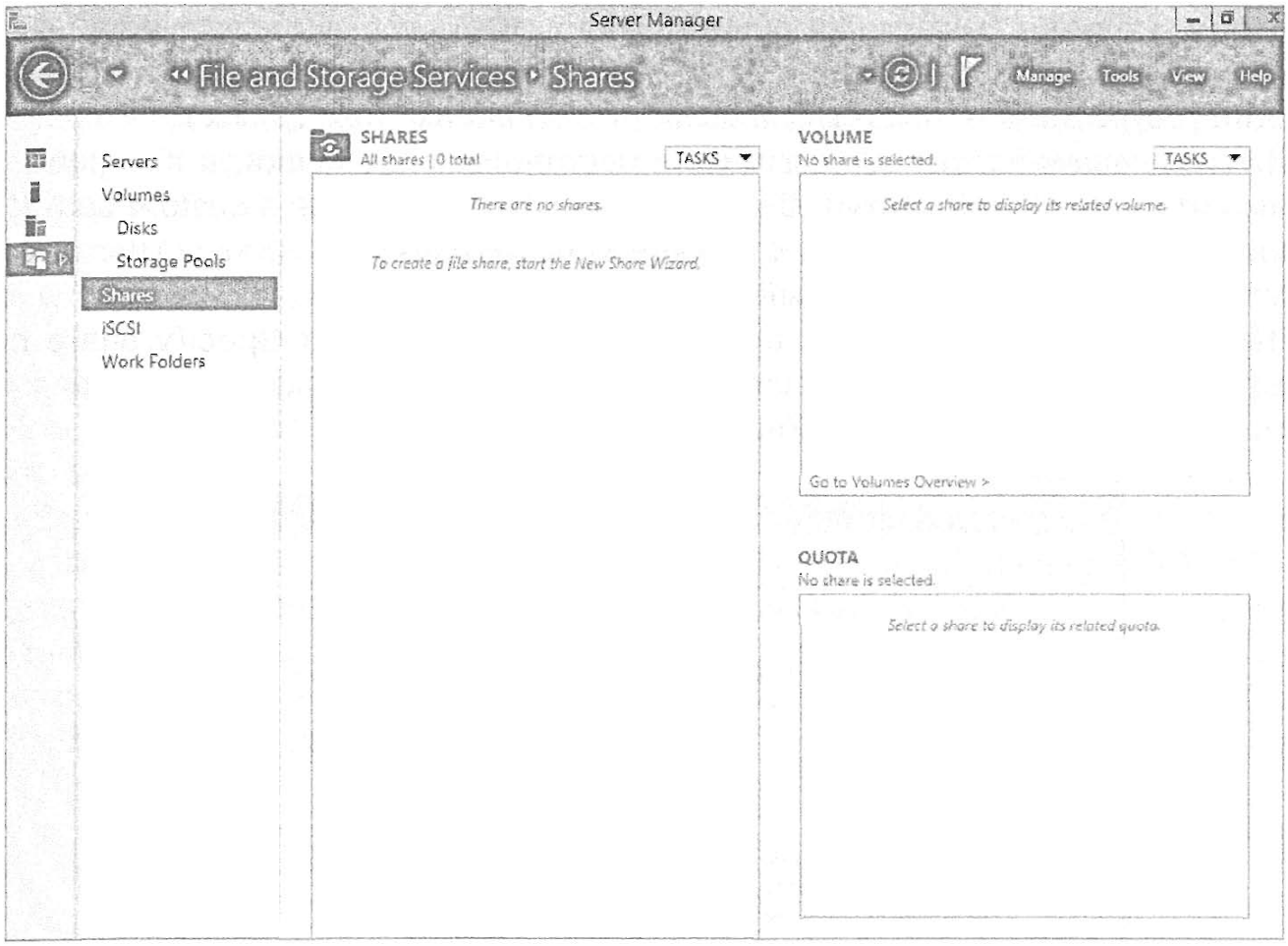


Рис. 26.3. Инструмент File and Storage Services

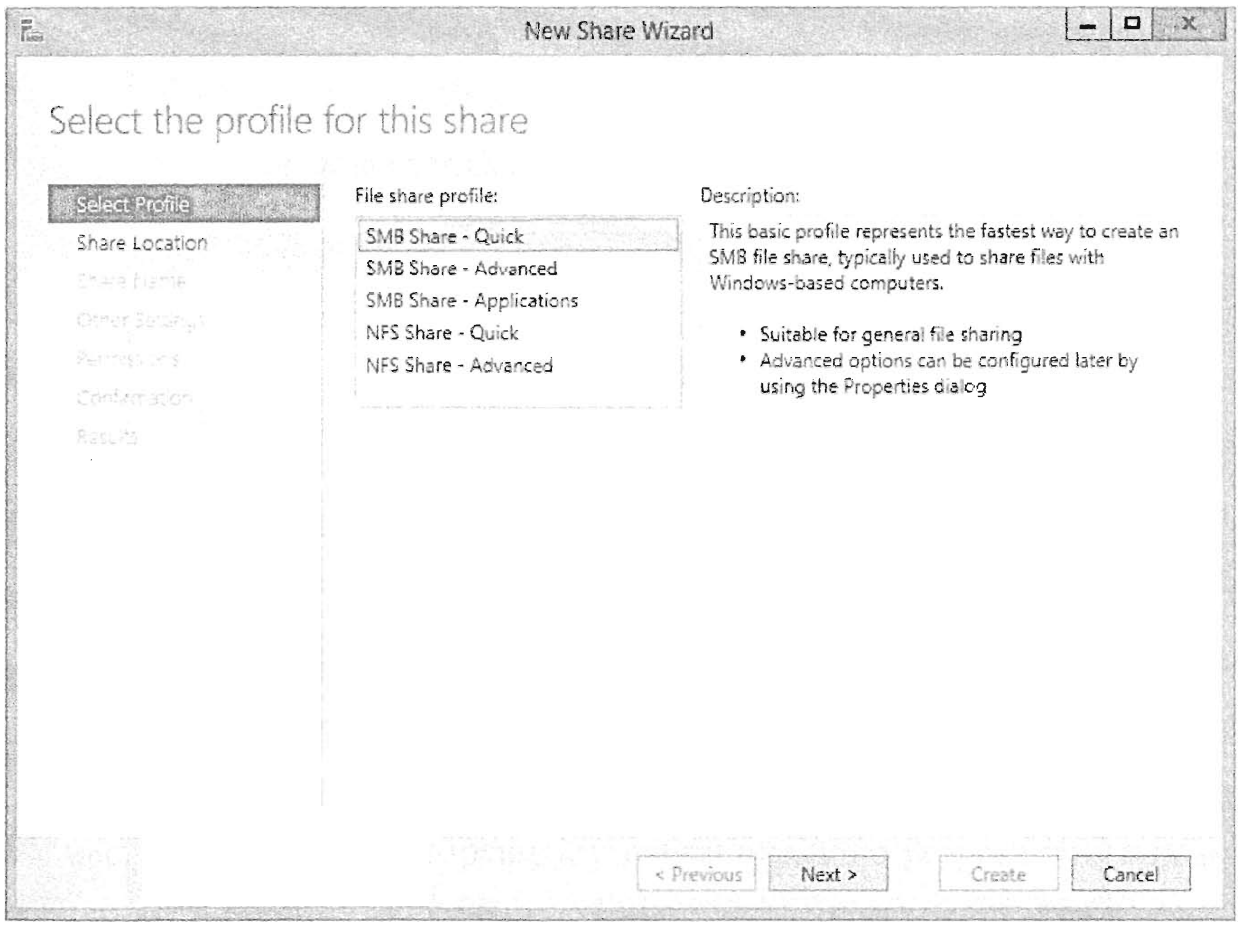


Рис. 26.4. Профиль общего ресурса

Чтобы создать стандартный общий файловый ресурс, выберите в списке File share profile (Профиль общего файлового ресурса) вариант SMB Share — Quick (Общий ресурс SMB — Быстрый) и щелкните на кнопке Next (Далее).

На следующем экране вы указываете местоположение папки, к которой необходимо открыть общий доступ. Выберите переключатель Type a custom path (Ввод специального пути) и перейдите к созданной ранее папке `D:\Shares\Home`. Экран должен быть похож на показанный на рис. 26.5.

Щелкните на кнопке Next, после чего появится экран Specify share name (Укажите имя общего ресурса) мастера New Share Wizard, приведенный на рис. 26.6. Именем общего ресурса должно быть `Home$`.

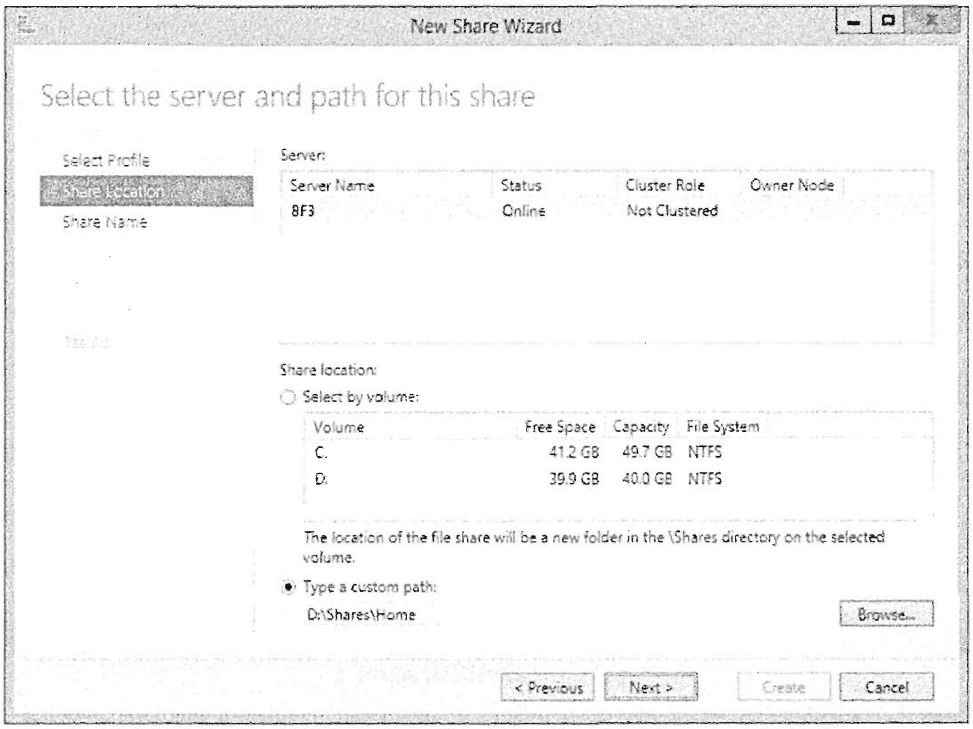


Рис. 26.5. Местоположение общего ресурса

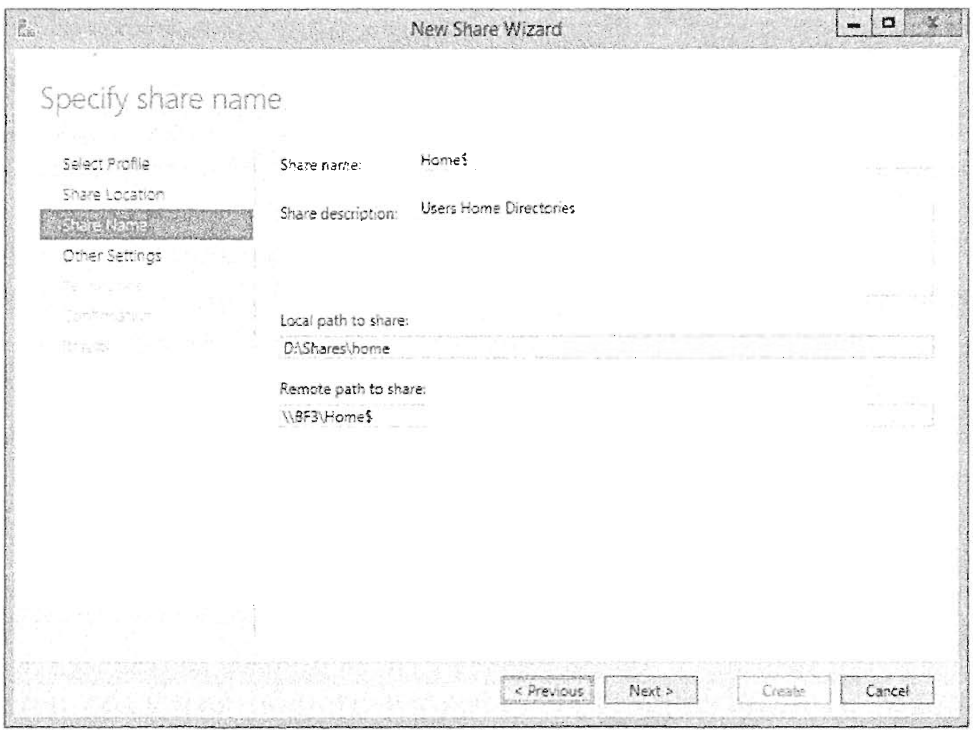


Рис. 26.6. Описание общего ресурса

На этом экране общий ресурс можно также документировать. Общую папку имеет смысл описать на тот случай, если кому-то другому понадобится диагностировать или устранять проблему, а вас поблизости не окажется. Введите описание общего ресурса в области Share description (Описание общего ресурса) и щелкните на кнопке Next.

Открывшийся далее экран Other Settings (Другие настройки) содержит ряд дополнительных параметров конфигурирования для вашего общего ресурса. Флажок Allow caching (Разрешить кеширование) по умолчанию будет отмечен. У вас также есть возможность зашифровать доступ к данным, отметив флажок Encrypt data access (Шифровать доступ к данным), и разрешить перечисление на основе доступа с помощью флажка Enable access-based enumeration (Включить перечисление на основе доступа).

Рекомендуется ограничить разрешения на общей папке двумя способами. Первый способ предусматривает блокирование разрешений на папке NTFS; это уже сделано. Второй способ заключается в блокировании разрешений для общей папки. Щелкните на кнопке Customize permissions (Настроить разрешения), в открывшемся окне перейдите на вкладку Share (Общий ресурс) и задайте разрешения для этого общего ресурса следующим образом:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`Everyone`	Read (Чтение)

По завершении в поле Share permissions (Разрешения общего ресурса) будет отображаться Custom (Специальные), как показано на рис. 26.7.

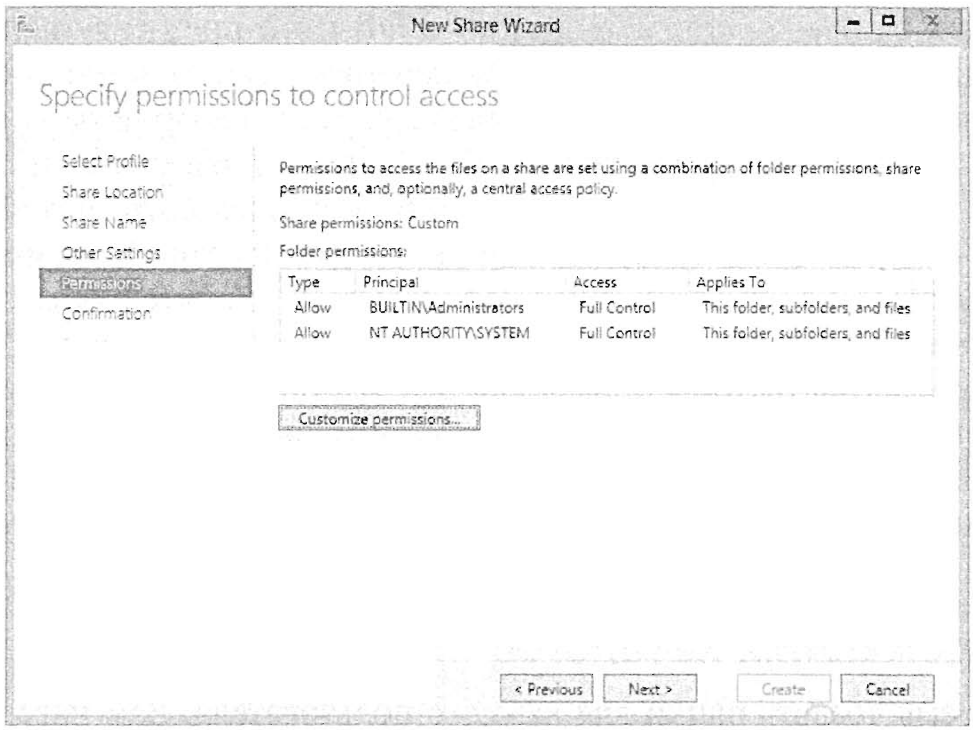


Рис. 26.7. Установка разрешений SMB

Совместные результаты разрешений папки и общего ресурса описаны ниже.

- Пользователи будут иметь возможность переходить через общий ресурс `Home$` в расположенные внутри него папки. Тем не менее, создавать что-либо в нем они не смогут. Это обусловлено разрешениями NTFS в папке.

- Пользователь будет способен изменять содержимое чего угодно внутри Home$ *при условии, что он имеет разрешение*. Это требуется для того, чтобы пользователь мог создавать и модифицировать файлы и папки в своем домашнем каталоге. Итак, пользователи практически ничего не могут делать на общем ресурсе Home$, но такое положение вещей изменится, когда вы создадите их персональные домашние каталоги.

После завершения работы мастера вам понадобится добавить новый общий ресурс в DFS. Это можно сделать с помощью инструмента администрирования DFS или в PowerShell. Внутри пространства имен BigFirmShares будет настроена папка с новым именем Home. В сети она будет доступна как \\bigfirm.com\BigFirmShares\Home. Ниже показано, как добавить общий ресурс в корень DFS посредством PowerShell. Для этого будет применяться командлет new-dfsnfolder:

```
new-dfsnfolder -path "\\BigFirm.com\BigFirmShares\Home"
  -TargetPath "\\BF2\Home$"
  -EnableTargetFailback $True
  -Description "Users home directory"
```

Теперь, когда общий ресурс создан, вы должны удостовериться в его доступности. Это можно сделать, перейдя по пути UNC общего ресурса внутри пространства имен DFS. Проверьте это с использованием учетных записей администратора и не администратора, чтобы убедиться в корректности разрешений.

Файловую систему DFS можно было бы применить для настройки репликации папок, если вы располагаете дублированным сервером на сайте восстановления в аварийных ситуациях (DR). Если вы сделали это и инициирован план восстановления в аварийных ситуациях, то пользователи смогут входить в системы ПК или серверов удаленных рабочих столов на сайте DR и по-прежнему использовать те же самые пути UNC для перехода или подключения к своим домашним каталогам. Модифицировать какие-то объекты пользователей или сценарии не понадобится.

Благодаря абстракции, предоставляемой пространством имен DFS, вы можете легко переместить папку Home на другой сервер. Для этого потребуется только быстро изменить отображение для данной папки внутри пространства имен. Никаких изменений, которые бы отражали такое перемещение, вносить в объекты пользователей или сценарии не придется.

В прошлом администраторы применяли оба эти подхода, сводя к минимуму перерывы в работе пользователей. Администраторы, использующие традиционные общие файловые ресурсы без DFS, обнаружат, что для внедрения DFS требуются некоторые усилия. Тем не менее, получаемые выгоды окупят эти дополнительные усилия, после того как миграции будут завершены.

Создание домашних каталогов

Пришло время создать папки для каждого пользователя. Вам наверняка понравится, насколько легко и быстро это можно сделать.

Войдите в систему своего контроллера домена и запустите предпочитаемый инструмент администрирования Active Directory — либо Active Directory Users and Computers (ADUC), либо Active Directory Administrative Center (ADAC). В рассматриваемом примере войдите в систему BF1, запустите ADUC и перейдите туда, где сосредоточены пользователи: \BigFirm\Users.

Выделите всех пользователей, щелкните правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства). Откроется диалоговое окно, показанное на рис. 26.8. Здесь можно сконфигурировать домашний каталог одновременно для всех этих пользователей. Как видите, домашний каталог сконфигурирован так, что при входе пользователей в систему он отображается как `Z:\`. Пользователи будут отображаться на `\\bigfirm.com\BigFirmShares\Home\%Username%`. Вся магия здесь скрыта в `%Username%`.

Конструкция `%Username%` автоматически завершает путь именем пользователя в соответствующей учетной записи. Например, когда вы проверите настройку Home Folder (Домашняя папка) в объекте пользователя `JBloggs`, то заметите, что она отображена на `\\bigfirm.com\BigFirmShares\Home\JBloggs`. В этом можно убедиться, взглянув на рис. 26.9, где представлено диалоговое окно свойств учетной записи пользователя `JBloggs`.

Здесь есть интересный момент: ОС Windows создает папку и устанавливает корректные разрешения на вашем файловом сервере. Это можно просмотреть на файловом сервере (рис. 26.10).

На рис. 26.11 видно, что домашний каталог для каждого пользователя унаследовал разрешения от папки `Home`. Каждому пользователю было выдано разрешение Full Control для собственной папки:

Группа	**Разрешение**
`BF2\Administrators`	Full Control (Полный доступ)
`System`	Full Control (Полный доступ)
`BigFirm\<`*`пользователь`*`>`	Full Control (Полный доступ)

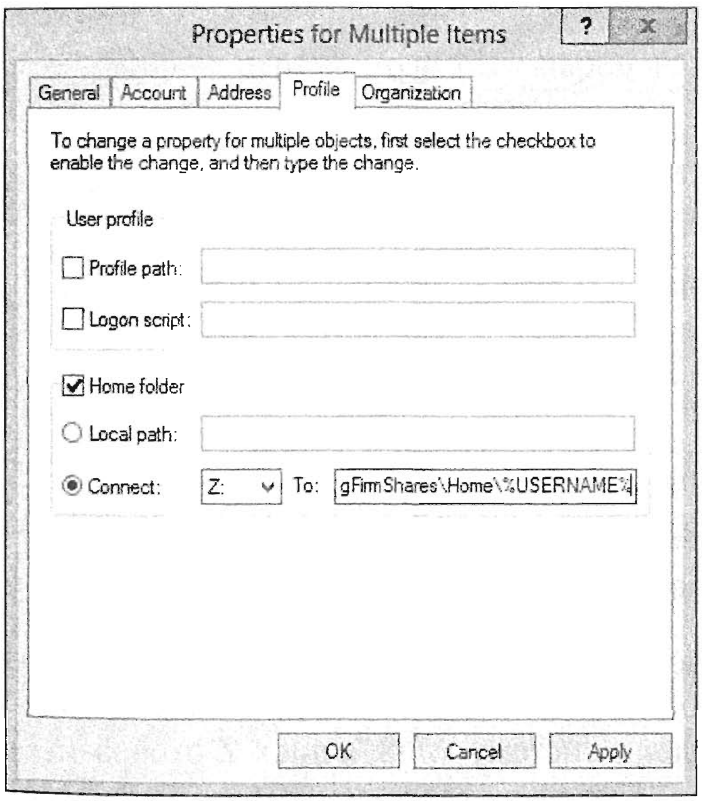


Рис. 26.8. Установка домашних каталогов для множества пользователей

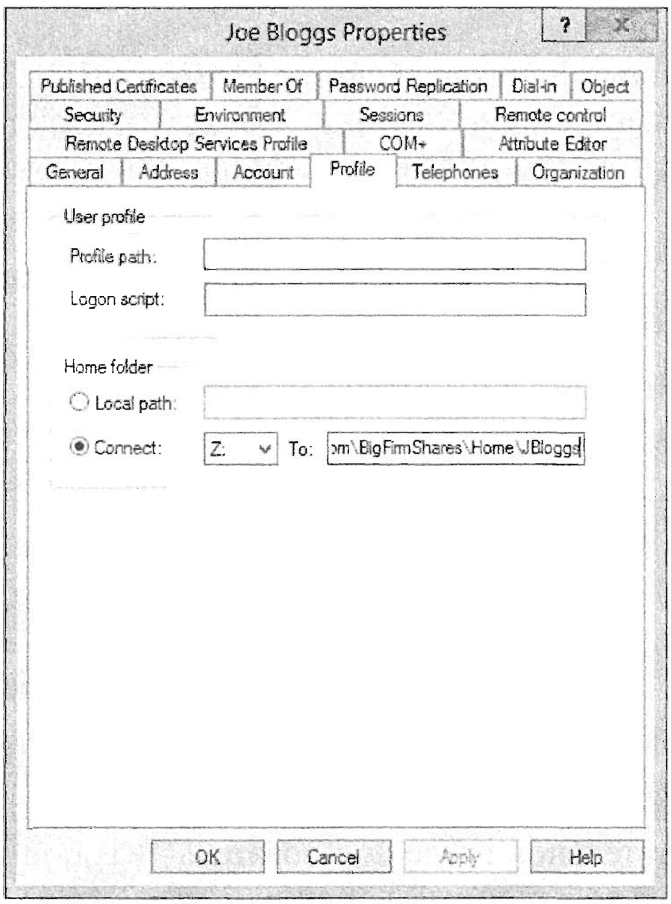


Рис. 26.9. Проверка настройки домашнего каталога для объекта пользователя

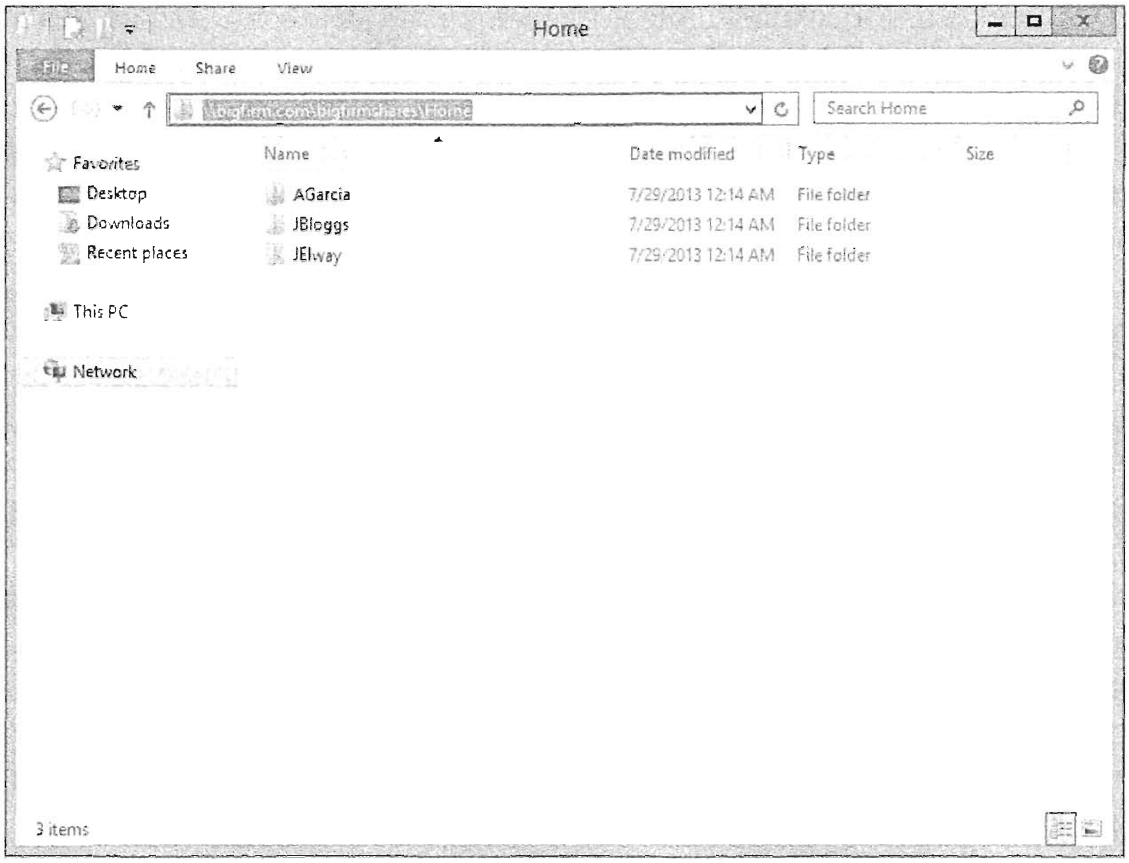


Рис. 26.10. Автоматически созданные домашние каталоги

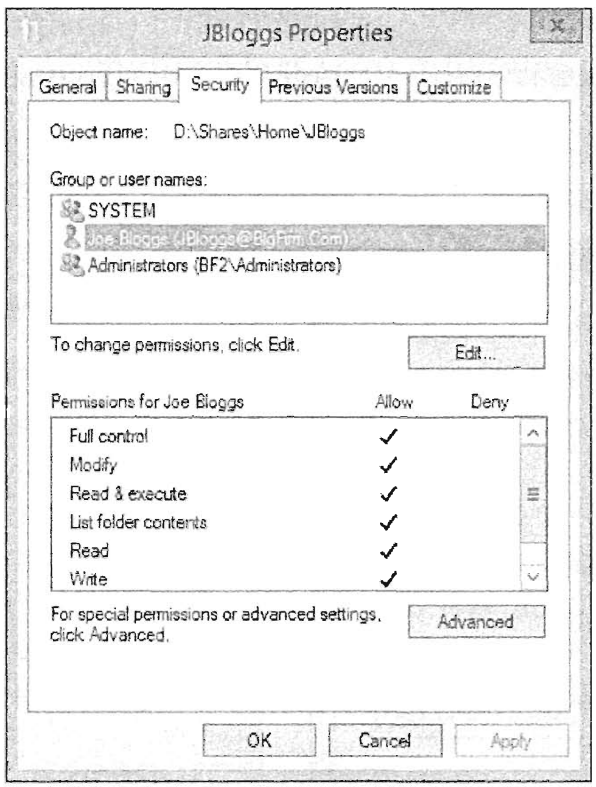


Рис. 26.11. Автоматически созданные разрешения домашнего каталога

Итак, вся работа выполнена! Это было довольно просто. Теперь вы можете войти в систему с применением учетной записи одного из пользователей. В нашей испытательной среде пользователь `JBloggs` войдет в систему Win8, а диск Z отобразится на собственный домашний каталог `JBloggs`. Благодаря разрешениям, которые имеются для каждой папки, данный пользователь не сможет получить доступ к домашнему каталогу, принадлежащему какому-то другому пользователю.

Совместное использование домашних каталогов

Ранее мы упоминали, что некоторые организации предоставляют доступ к домашним каталогам не только их владельцам, но также и другим пользователям. Вы можете достаточно легко обеспечить такой доступ, добавив возможность доступа к `D:\Shares\Home` группе `Authenticated Users` (Аутентифицированные пользователи). Это разрешение будет унаследовано каждым домашним каталогом. Пользователям группы `Authenticated Users` могут быть выданы права Read & Execute (Чтение и выполнение) для доступа только для чтения или же права Change (Изменение), чтобы они могли модифицировать содержимое домашних каталогов других пользователей.

Некоторые организации предпочитают не конфигурировать атрибут Home Folder объекта пользователя. По их мнению, диск легче отобразить с помощью сценария входа. Сценарий входа выполняется каждый раз, когда пользователь входит в систему, и выполняет набор команд. Мы рассмотрим такие сценарии позже. В качестве альтернативы для отображения дисков вы можете применять предпочтения групповой политики (Group Policy Preferences). Если диск перемещается на другой сервер, гораздо проще модифицировать одну команду сценария входа или групповую политику, вместо того чтобы вносить изменения в настройки сотен или даже тысяч пользователей.

Противоположное мнение по этому вопросу заключается в том, что за счет использования пространства имен DFS с целью абстрагирования от физического местоположения общего ресурса вы сделаете свое решение для домашних каталогов весьма динамичным. Вы можете переместить общий ресурс, и все пользователи сохранят свои отображения, после того как вы модифицируете единственное отображение папки в пространстве имен DFS. Вдобавок, когда установлен атрибут Home Folder объекта пользователя, для его домашнего каталога становятся доступными некоторые переменные. Эти переменные могут применяться сценариями или приложениями.

- **HOMEDRIVE.** Представляет букву, используемую для отображения домашнего каталога, например `Z:`.
- **HOMEPATH.** Представляет путь внутри `HOMEDRIVE`, где содержится домашний каталог, например, `\`. Полным путем является `%HOMEDRIVE%%HOMEPATH%`, например, `Z:\`.
- **HOMESHARE.** Это путь UNC к домашнему каталогу пользователя, например, `\\bigfirm.com\BigFirmShares\Home\JBloggs`.

Сравнение домашнего каталога и локального хранилища

Вы предоставили своим пользователям централизованный механизм хранения. Вам понадобится довести до сведения пользователей, что данные должны храниться на этом диске, а не на локальных дисках их устройств. Чтобы обеспечить это, можно использовать групповую политику (Group Policy).

Ниже перечислены ключевые действия.

- Сообщите своим пользователям, что домашние каталоги регулярно подвергаются резервному копированию, а устройства — нет. Для данных, хранящихся на устройствах, отсутствует соглашение об уровне обслуживания.
- Включите службу теневого копирования томов (VSS) на своих файловых серверах и научите пользователей работать с клиентом предыдущих версий (Previous Versions Client) для восстановления своих файлов.
- Данные на устройстве могут быть не защищены. Расскажите пользователям о необходимости обеспечения безопасности данных.
- Где требуется, используйте аудит, чтобы дополнительно подстраховать пользователей в плане уязвимых файлов. Можете даже рассмотреть вопрос применения службы управления правами Active Directory (Active Directory Rights Management Services), чтобы позволить пользователям управлять на уровне файлов тем, кому разрешено видеть или редактировать файл.

Чуть позже мы рассмотрим автоматизированные механизмы, которые еще больше стимулируют пользователей хранить свои данные на сервере, а не на устройстве.

В настоящем разделе мы обсудили, как позволить пользователю сделать свои персональные данные доступными независимо от того, в систему какого сервера или устройства он входит. Далее мы раскроем тему перемещаемых профилей и расскажем, как с их помощью делать то же самое в рабочей среде.

Создание перемещаемых профилей

Профиль — это папка, которая содержит все настройки, имеющие отношение к рабочей среде пользователя. По умолчанию профиль сохраняется в каталоге `C:\Users`. *Перемещаемый профиль* хранится в сети, а не на локальном диске компьютера, в систему которого пользователь вошел. Тем не менее, по умолчанию такой профиль кешируется локально. Преимущество перемещаемого профиля заключается в том, что пользователь может войти в систему любого компьютера в домене и получить в свое распоряжение согласованную рабочую среду. Однако вы должны отслеживать, не содержит ли профиль информацию, являющуюся специфичной для компьютера, приложения или операционной системы, которая неприменима ко всем компьютерам, куда пользователь может войти. Профиль имеет два типа содержимого:

- файлы и папки;
- файл `ntuser.dat`.

Настройки Windows и приложений пользователя обычно хранятся в разделе `HKEY_CURRENT_USER` реестра. Он должен быть доступен пользователю каждый раз, когда он входит в систему и находится в файле `ntuser.dat`.

Другие типы содержимого хранятся в виде файлов папках профиля со специальными именами, которые перечислены ниже.

- **`My Documents`.** Это стандартное местоположение, где хранят свои документы такие программы, как Microsoft Office.
- **`My Music`.** Это стандартное местоположение, куда музыкальные проигрыватели сохраняют и загружают музыкальные файлы.

- **Favorites.** Здесь Internet Explorer хранит файлы ссылок Favorites (Избранное).
- **AppData.** ОС Windows и другие программы будут сохранять сюда файлы и параметры, которые являются ориентированными на конфигурацию, но по умолчанию не должны быть видимыми, упрощая жизнь пользователю.
- **Desktop.** Здесь хранится содержимое рабочего стола пользователя.

Когда пользователь впервые входит в систему компьютера, для него должен быть создан новый профиль. Изначально Windows создает такой профиль путем копирования стандартного профиля. Новому профилю назначается имя пользователя. В каталоге `C:\Users` вы увидите новую папку с именем пользователя, например, `C:\Users\JBloggs`. Она будет защищена так, что доступ к ней будут иметь только учетные записи `System`, `Administrator` и самого пользователя. После входа пользователя в систему настройки из профиля загружаются в его рабочий сеанс. Когда пользователь выходит из системы, внесенные изменения сохраняются.

К этому моменту вы уже могли заметить, что по умолчанию профиль является локальным ресурсом. Это означает, что данные и конфигурация, имеющиеся на одном ПК, на другом ПК будут отличаться. Только представьте себе разочарование, постигшее пользователей, если после входа в систему другого компьютера у них исчезнут избранные ссылки в браузере или почтовые контакты. Такая проблема возникает в различных сценариях.

- Пользователи входят в системы фермы серверов Remote Desktop или виртуальных рабочих столов. Они никогда не знают, на какой из серверов попадут, поэтому их пользовательская конфигурация отличается на каждом сервере.
- Вы работаете в конторском офисе, где пользователи каждый день садятся за другой ПК. На каждом компьютере у них будут разные профили.
- ПК пользователя вышел из строя или заменен. В результате он полностью утратит свою персональную конфигурацию. Подумайте о бизнес-данных, которые будут безвозвратно утеряны из-за того, что ПК не подвергался нормальному резервному копированию.

Как видите, все это противоречит с желанием трактовать ПК как прибор и располагать динамической IT-средой. Пользователи начинают выражать протесты IT-отделу, как только они узнают о риске утраты своих данных или о несогласованности рабочей среды.

Решением проблемы является перемещаемый профиль. Его концепция заключается в том, что профиль пользователя хранится на общем файловом ресурсе, похожем по структуре на тот, который вы настраивали для домашних каталогов. Такой профиль загружается из файлового сервера каждый раз, когда пользователь входит в систему, и кешируется в каталоге `C:\Users` на этом компьютере. Содержимое профиля, которое было изменено, сохраняется обратно на файловый сервер при выходе пользователя из системы. У вас может сложиться впечатление, что по сети перемещается множество файлов. Потенциально это возможно. Тем не менее, Windows будет загружать или выгружать только те файлы, которые в этом нуждаются.

Например, когда пользователь входит в систему ПК с перемещаемым профилем, будут передаваться только файлы, которые пока еще не загружены. Когда пользователь выйдет из системы, будут выгружены только файлы, которые были изменены.

Давайте рассмотрим два способа создания перемещаемых профилей. Один из них является очень быстрым и легким в реализации. Второй способ позволяет повысить уровень безопасности, но требует несколько большего объема работы.

Создание общего ресурса перемещаемых профилей: простой способ

Сейчас мы пройдемся по процессу конфигурирования перемещаемых профилей для пользователей в BigFirm. Этот подход предполагает установку настроек профиля в объектах пользователей. В отличие от простого подхода к созданию домашних каталогов, если установлен атрибут перемещаемого профиля, папка для пользователя создаваться не будет. Вместо этого при входе пользователя в систему будет автоматически устанавливаться его перемещаемый профиль.

Начнем с часто рекомендуемого Microsoft подхода, который облегчает задачу развертывания профилей. Вам предстоит создать общий файловый ресурс на файловом сервере BF2.

1. Создайте в `D:\Shares` папку под названием `Profiles`, как показано на рис. 26.12.

   Полезно отметить еще раз, что в производственной среде вы никогда не будете помещать пользовательские данные на системный диск, а взамен размещать их в отдельном, специально выделенном для этого томе.

2. Отключите наследование разрешений для этой папки и сконфигурируйте разрешения, как показано ниже (и на рис. 26.13):

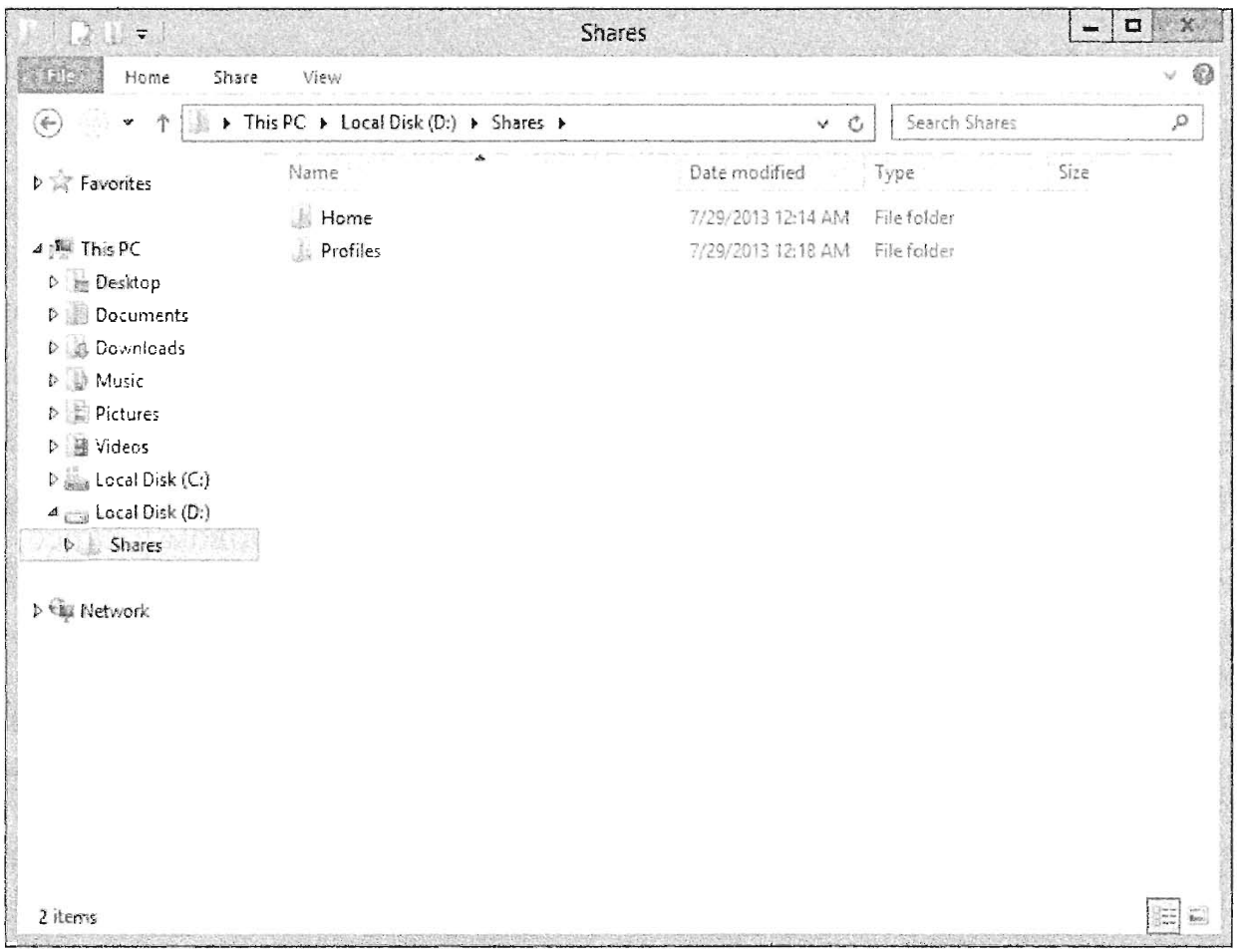


Рис. 26.12. Папка перемещаемых профилей на файловом сервере

Группа	Разрешение	К чему применяется
`Creator Owner`	Full Control (Полный доступ)	Вложенные папки и файлы
`BF2\Administrators`	Full Control (Полный доступ)	Эта папка, вложенные папки и файлы
`System`	Full Control (Полный доступ)	Эта папка, вложенные папки и файлы
`Authenticated Users`	List Folder/Read Data (Список папки / Чтение данных); Create Folders/Append Data (Создание папок / Добавление данных); Read Attributes (Чтение атрибутов)	Эта папка, вложенные папки и файлы

Для чего нужно разрешение Read Attributes?

Обратите внимание, что в самом конце было добавлено разрешение Read Attributes (Чтение атрибутов). Оно не отражено ни в одном из документов Microsoft, которые нам приходилось читать. Однако профиль пользователя не будет полностью сохранен на файловом сервере, если это разрешение не будет добавлено к папке профилей.

Установленные разрешения позволят пользователю создать внутри общего ресурса папку, где будет сохранен его перемещаемый профиль. Данному подходу присущ недостаток. Пользователь может создать на этом общем ресурсе папку и хранить в ней данные без предварительного утверждения. Без этого не обойтись, т.к. подход предусматривает применение прав пользователя для создания его перемещаемого профиля. Пользователь, не знакомый с ними, при входе в систему создаст на файловом сервере собственную папку перемещаемого профиля. Теперь нужно открыть общий доступ к папке `Profiles` и добавить ее в пространство имен DFS.

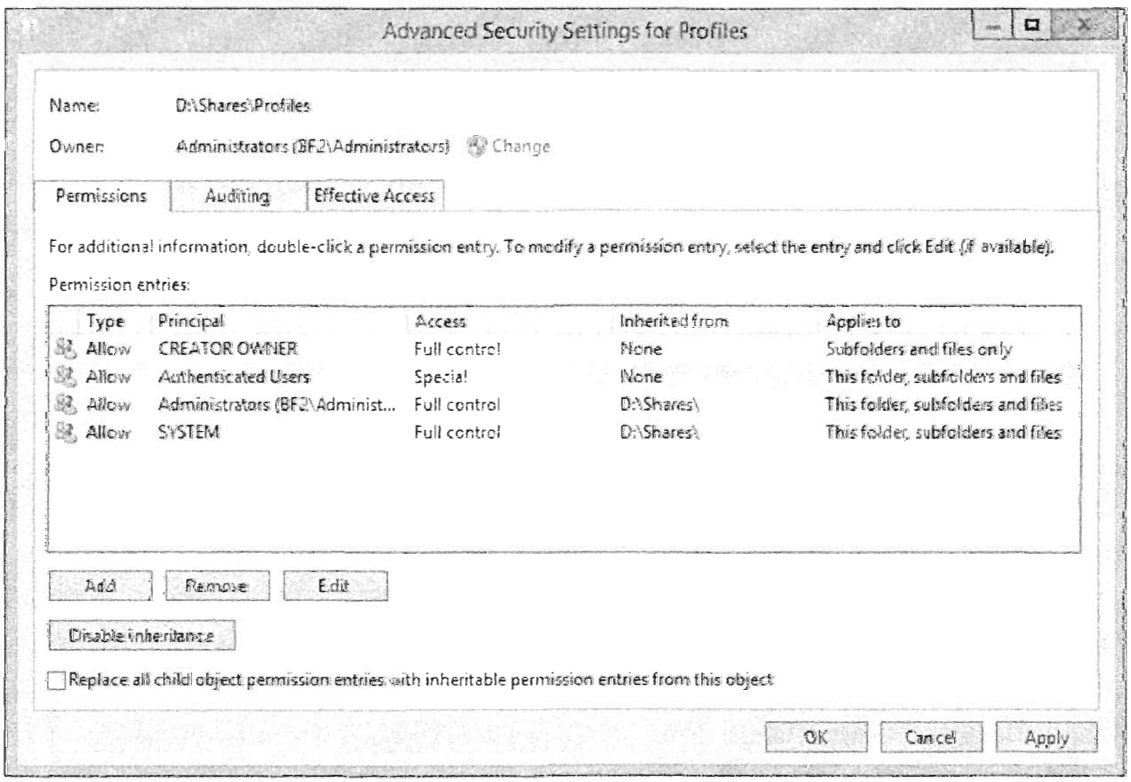


Рис. 26.13. Расширенные разрешения для папки `Profiles`

3. В окне инструмента File and Storage Services перейдите на вкладку Shares (Общие ресурсы) и выберите в раскрывающемся меню Tasks (Задачи) пункт New Share (Создать общий ресурс), чтобы запустить мастер создания общего ресурса (New Share Wizard), окно которого показано на рис. 26.14.
4. Укажите для местоположения `D:\Shares\Profiles`; это местоположение папки, которую вы собираетесь использовать для хранения перемещаемых профилей.
5. Откройте общий доступ к папке `Profiles` как к скрытому общему ресурсу по имени `Profiles$` (рис. 26.15).

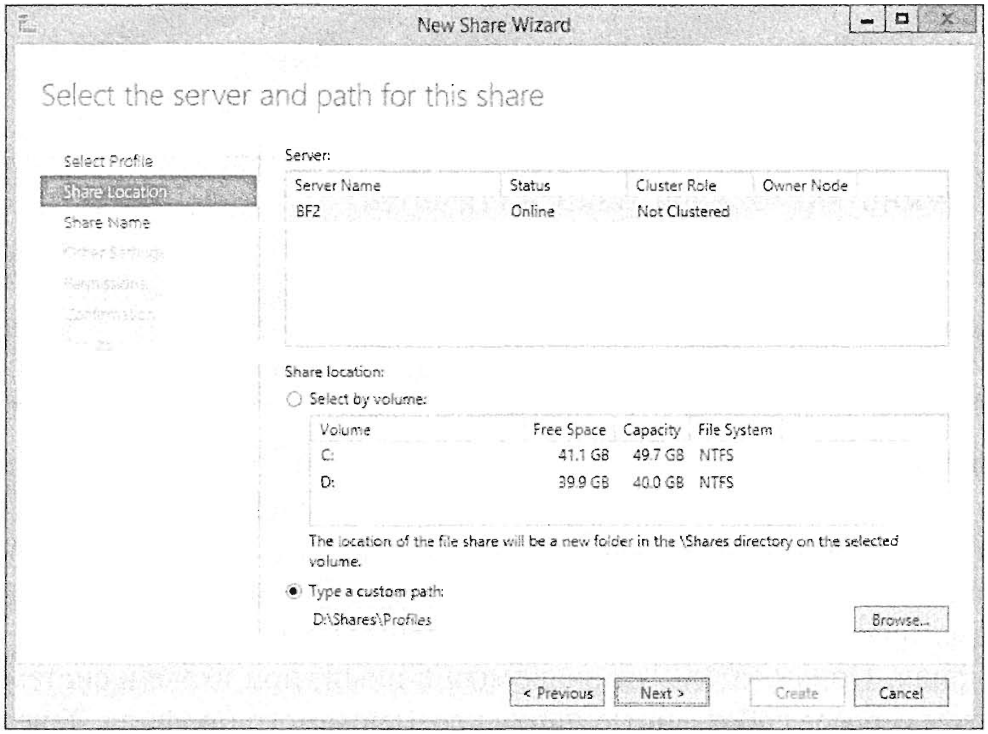


Рис. 26.14. Местоположение общей папки с профилями

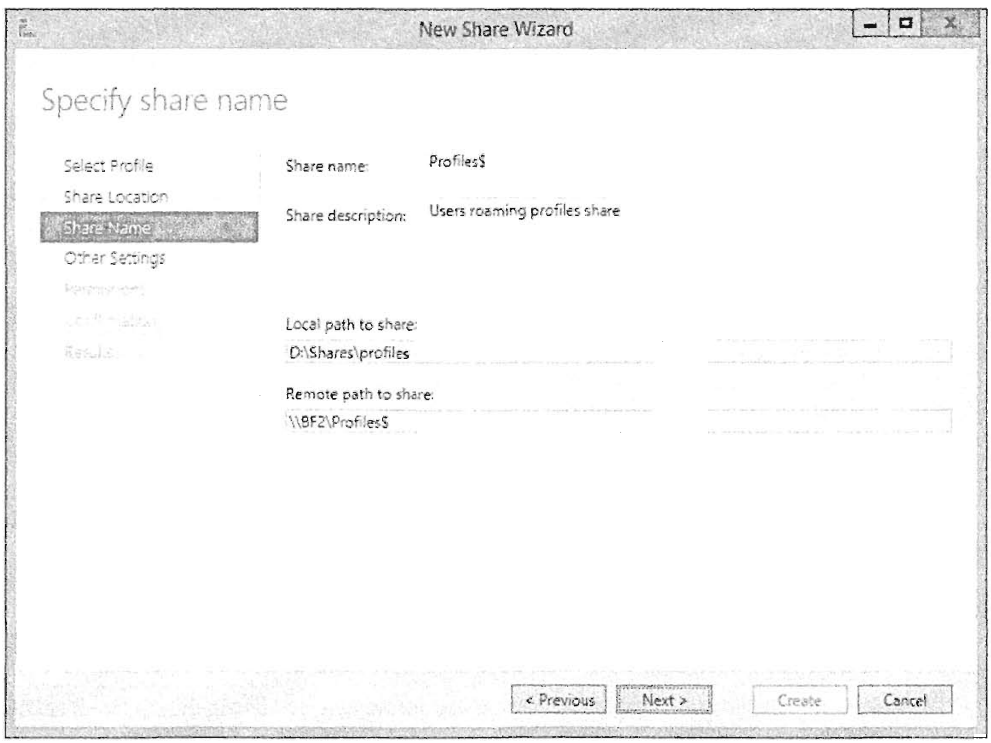


Рис. 26.15. Имя и описание общего ресурса профилей

6. Также предусмотрите описание. Для этого примера введите в области Share description (Описание общего ресурса) описание `Users roaming profiles share` (Общий ресурс перемещаемых профилей пользователя).
7. На экране Permissions (Разрешения) щелкните на кнопке Customize permissions (Настроить разрешения), в открывшемся окне перейдите на вкладку Share (Общий ресурс) и задайте разрешения общего ресурса следующим образом:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`Authenticated Users`	Change (Изменение)

По завершении в поле Share permissions (Разрешения общего ресурса) будет отображаться Custom (Специальные), как показано на рис. 26.16.

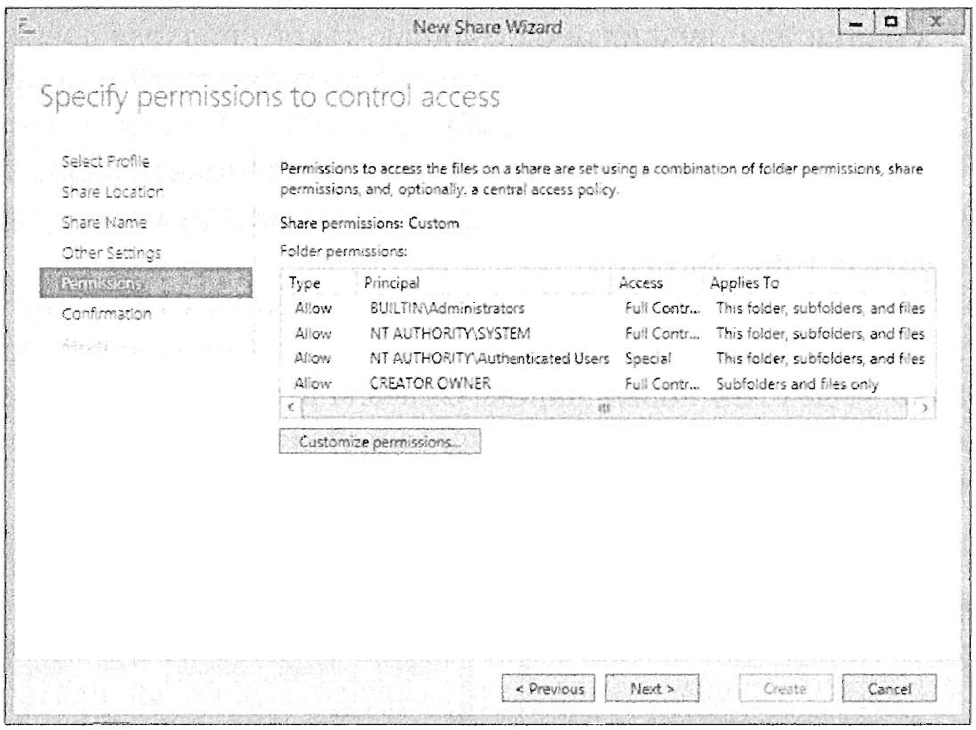


Рис. 26.16. Установка разрешений общего ресурса профилей

Чтобы сделать общий ресурс профилей доступным в пространстве имен DFS, вы будете применять PowerShell (рис. 26.17). Вам придется воспользоваться командлетом `new-dfsnfolder`:

```
new-dfsnfolder -path "\\BigFirm.com\BigFirmShares\Profiles"
  -TargetPath "\\BF2\Profiles$" -EnableTargetFailback $True
  -Description "Users profile directory"
```

За счет использования DFS вы получите возможность реплицировать папку или перемещать ее, когда это необходимо, не прибегая к многочисленным корректировкам, если система находится в производственной среде.

По завершении работы мастера New Share Wizard вы должны удостовериться в том, что действительно можете перейти на `\\bigfirm.com\BigFirmShares\Profiles`. Если это так, то вы готовы к следующему шагу. Если же нет, то, по-видимому, имеется проблема с разрешениями на общем ресурсе, или просто необходимо подождать, пока обновленные настройки пространства имен DFS будут реплицированы между контроллерами домена (либо же принудительно инициировать такую репликацию).

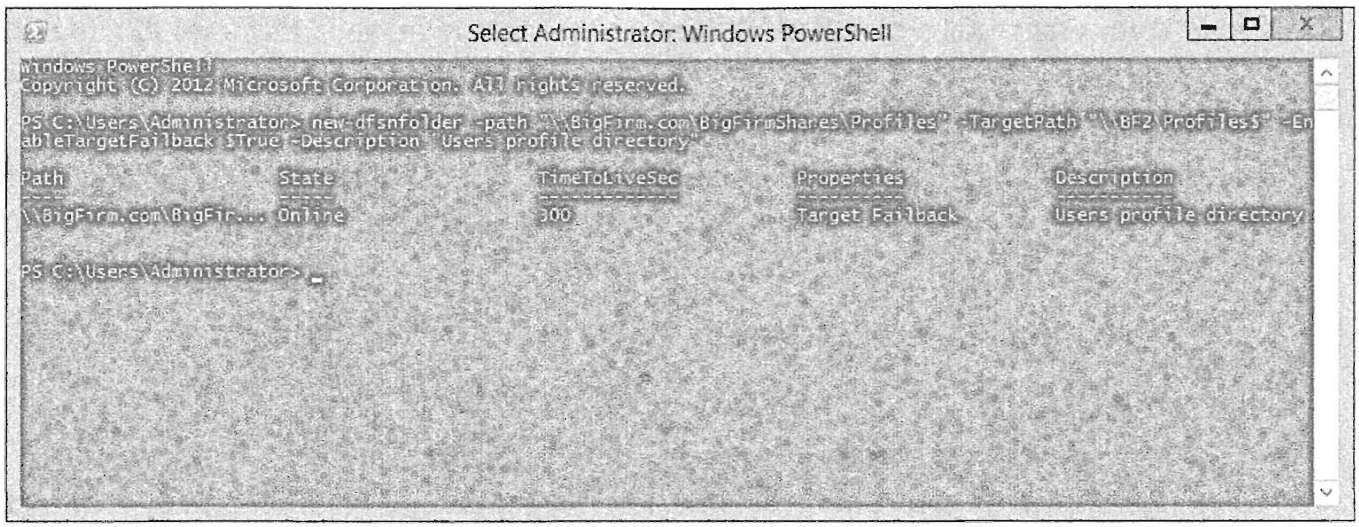


Рис. 26.17. Добавление общего ресурса `Profiles$` в пространство имен DFS

Развертывать папки для профилей с помощью такого подхода довольно легко. Вы просто конфигурируете объекты учетных записей пользователей и поручаете Windows сделать все остальное. На рис. 26.18 мы выбрали сразу все учетные записи пользователей и открыли диалоговое окно их свойств, чтобы установить свойство профиля.

В качестве альтернативы это можно сделать, редактируя свойства одиночного объекта пользователя (рис. 26.19).

При этом папка не создается. Вспомните, что папка будет создана от имени пользователя, когда он входит в систему. Таким образом, не удивляйтесь, если не обнаружите в папке `Profiles` новых папок. Сначала вы должны ее протестировать.

Чтобы сконфигурировать для объекта пользователя атрибут перемещаемого профиля, также можно применять PowerShell.

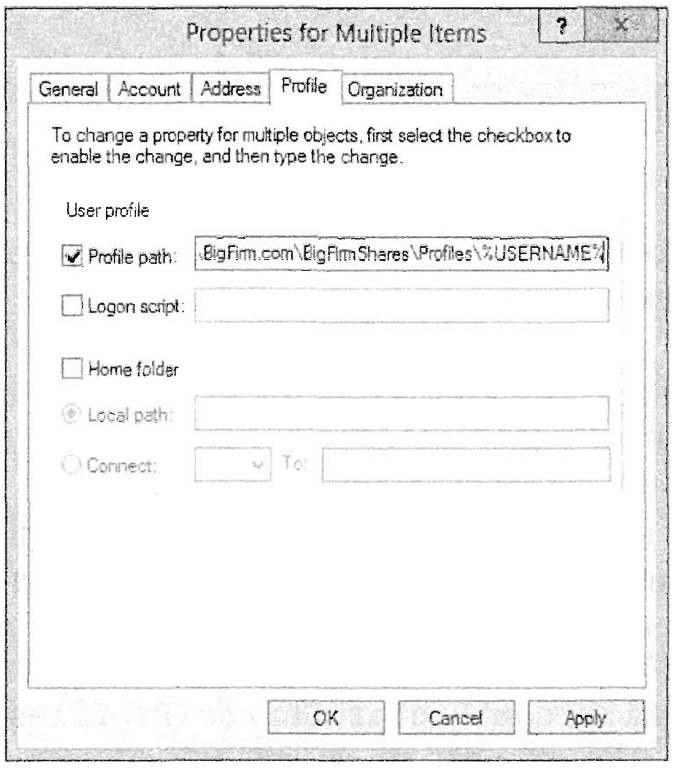


Рис. 26.18. Конфигурирование свойства перемещаемого профиля для множества пользователей

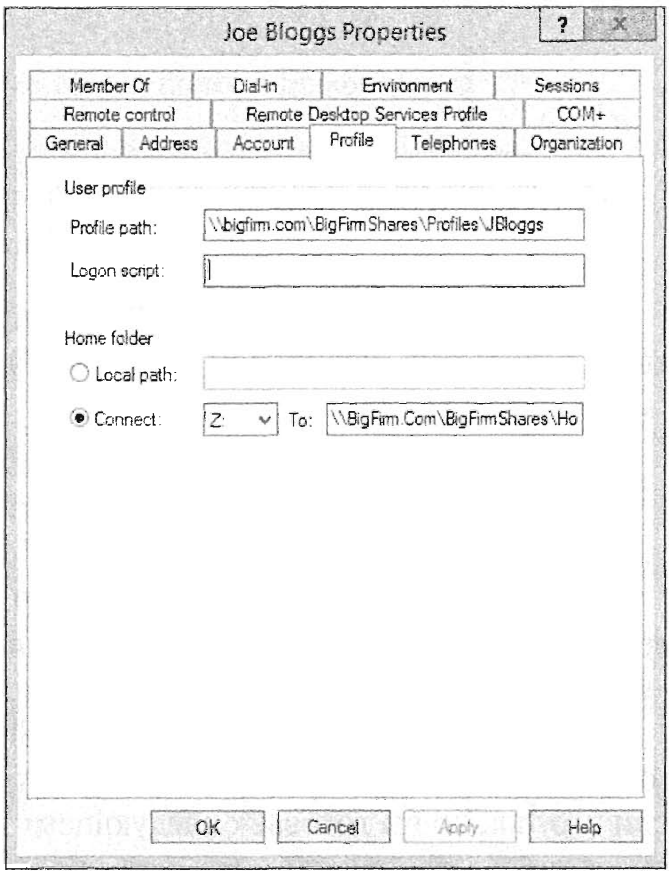


Рис. 26.19. Конфигурирование свойства перемещаемого профиля для отдельного пользователя

Для этого предназначен командлет `set-aduser`:

```
set-aduser jbloggs -profilepath "\\bigfirm.com\bigfirmshares\Profiles\JBloggs"
```

Теперь вы готовы провести тестирование, что является обязательным шагом перед тем, как разрешить пользователям входить в систему. Здесь следует обратить внимание на ряд моментов.

Профиль создается на рабочей станции (или сервере Remote Desktop) при первом входе пользователя в систему. Вы можете видеть это на рис. 26.20.

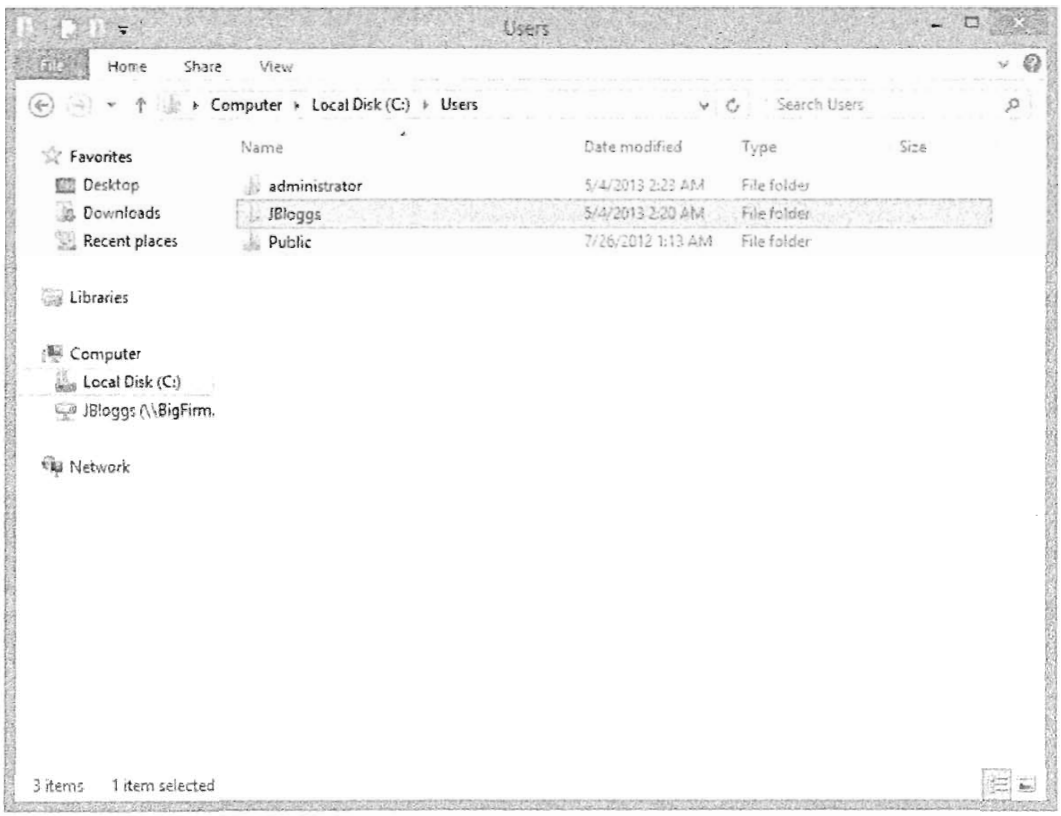


Рис. 26.20. Кешированный профиль на ПК

Для пользователя на общем ресурсе профиля создается новая пустая папка. Обратите внимание, что имя имеет расширение `.V2`. Это указывает на то, что такой профиль является профилем *версии 2*, и был создан Windows 7 или более новой версией ОС. *Ни в коем случае не указывайте* `.V2` *в пути такого профиля. В эту ловушку попасть очень легко*. Например, указание профиля как `\\bigfirm.com\BigFirmShares\Profiles\JBloggs.V2` приведет к тому, что он не загрузится. ОС Windows будет автоматически добавлять такое расширение к имени папки, когда это необходимо.

После выхода пользователя из системы его профиль передается из рабочей станции на общий файловый ресурс. Теперь этот пользователь может переходить с одной рабочей станции на другую, сохраняя одну и ту же рабочую среду.

Проверка на наличие ошибок

Обязательно войте и выйдите из системы несколько раз от имени пользователя. Проверьте, нет ли в области уведомлений и в журнале приложений (в программе Event Viewer) сообщений об ошибках. Ошибки обычно бывают связаны с опечатками или с разрешениями.

Давайте остановимся на минуту. Как узнать, есть ли что-нибудь в папке профиля? Возможно, вы только что воссоздали этот сценарий и заметили, что администраторы не имеют доступа к профилю. В действительности именно так было задумано. Пользователь создал собственную папку и, будучи владельцем создателя (Creator Owner), он имеет полный и *единоличный* доступ к ней. Это создает определенные проблемы, поскольку такие действия, как резервное копирование/восстановление и оказание пользователю помощи, становятся практически невозможными!

Выдача администраторам полный доступ к пользовательским профилям приведет к беспорядку. В идеальном случае должен был бы существовать способ предоставления администраторам доступа по мере надобности. Это можно сделать с помощью настройки групповой политики, которая применяется к компьютерам, создающим профили. Однако такое решение должно быть реализовано до создания профилей. Оно не имеет обратной силы.

1. Войдите в систему контроллера домена BF1 и запустите консоль управления групповой политикой (Group Policy Management) через меню Administrative Tools (Администрирование).
2. Создайте новый объект групповой политики и свяжите его с организационной единицей `Computers`, где находится рабочая станция Win8 (рис. 26.21).

Рис. 26.21. Новый объект групповой политики

Политика, которую вы включите, применяется к компьютеру, куда пользователь будет входить, а не к пользователю и не к файловому серверу, где создан профиль. Именно поэтому данная политика связывается с контейнером Computers, а не Servers, где находится файловый сервер.

Включаемая политика называется Add the Administrators security group to roaming user profiles (Добавить группу доступа `Administrators` в перемещаемые профили пользователя) и расположена в папке Computer Configuration \

Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей). Вы можете видеть ее на рис. 26.22.

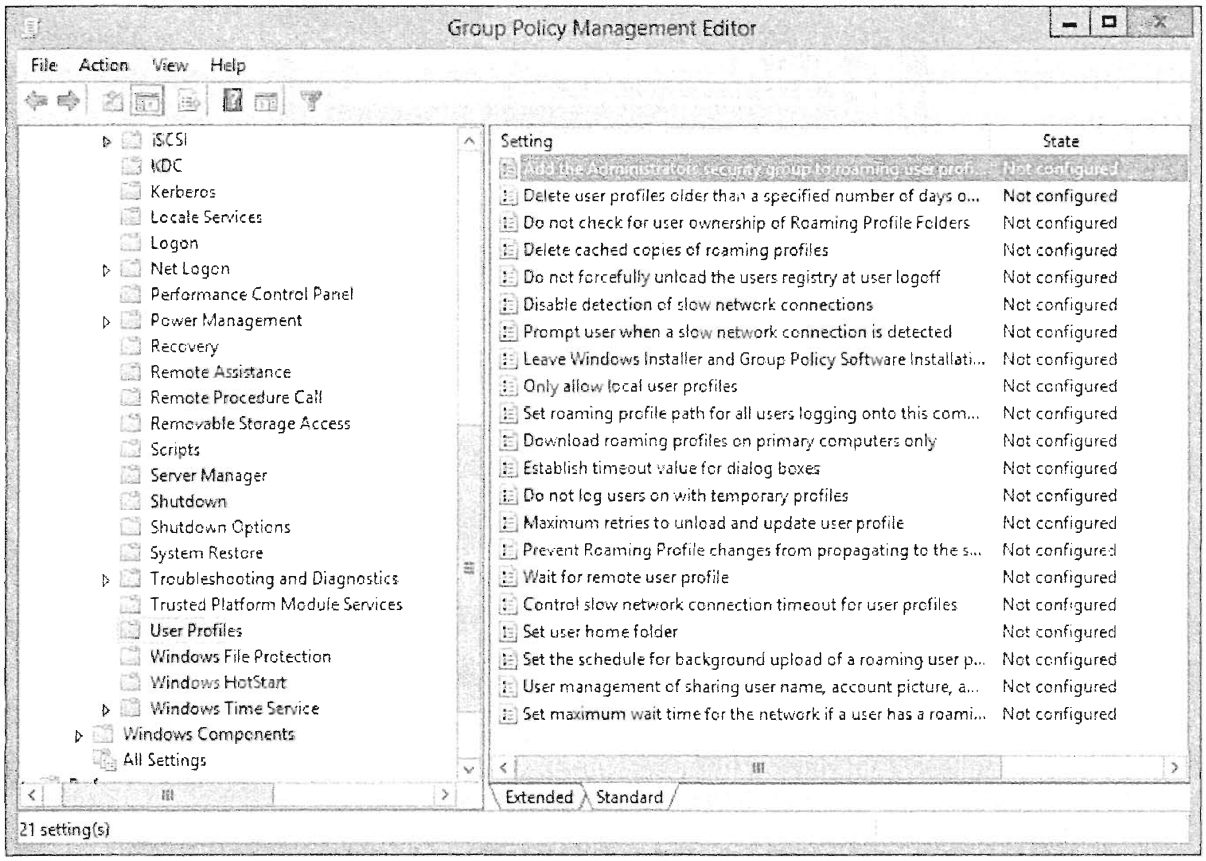


Рис. 26.22. Конфигурирование объекта групповой политики

3. Установите ее в Enabled (Включена), и эта политика предоставит группе `Administrators` полный доступ (Full Control) к любому вновь созданному профилю.

   Вспомните, что политики не применяются немедленно. В производственной среде вам, скорее всего, придется подождать, пока истечет период обновления.

4. В испытательной среде запустите приведенную ниже команду, чтобы принудительно применить конфигурацию компьютера из унаследованных объектов GPO:

```
gpupdate /target:computer /force
```

На рис. 26.23 показано, что при тестировании группа `Administrators` имеет полный доступ (Full Control) к профилю. Это существенно облегчит администраторам управление пользователями, а также поиск и устранение неполадок, и позволит службам, выполняющимся от имени администратора, получать доступ к содержимому.

Перемещаемые профили развертываются путем создания общей папки и конфигурирования учетных записей пользователя. Это было довольно просто. Однако мы уже упоминали о том, что защита папки `Profiles` не настолько высока, как вам, возможно, хотелось бы, из-за разрешений, которые требуются для этого метода. Какой-то хитрый пользователь мог бы начать создавать папки на общем ресурсе `Profile$` и хранить там данные. Скорее всего, вы предпочли бы альтернативный способ развертывания перемещаемых профилей.

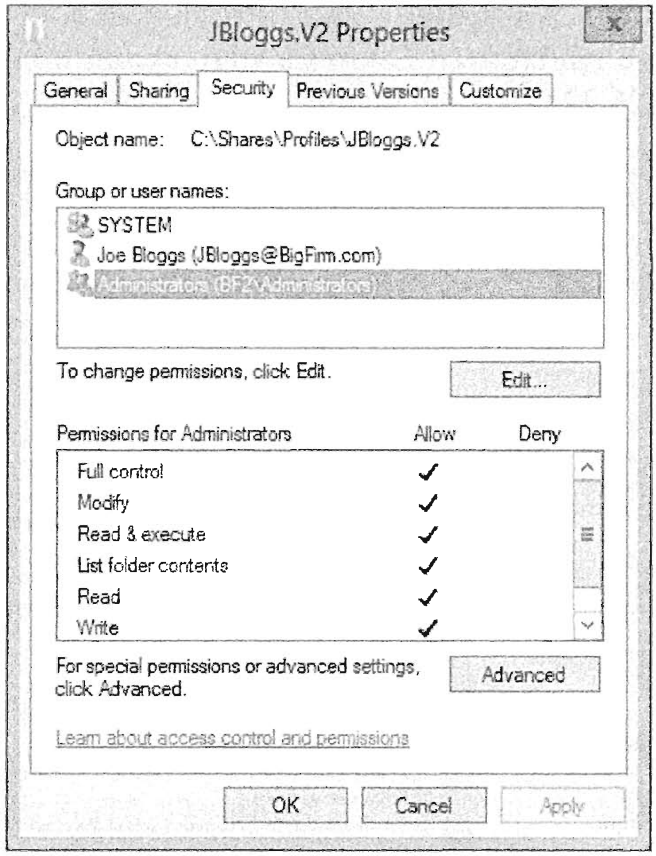


Рис. 26.23. Администраторы имеют доступ к папкам перемещаемых профилей

Создание общего ресурса перемещаемых профилей: сложный способ

Вы можете использовать это решение, когда требуется стопроцентный контроль над содержимым папки с перемещаемыми профилями. Вы вручную создаете каждую папку и устанавливаете для нее разрешения.

1. Создайте папку `Profiles` в том же месте, где она создавалась в предшествующих разделах.
2. Отключите наследование, но не копируйте унаследованные разрешения.
3. Теперь назначьте папке следующие разрешения:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`System`	Full Control (Полный доступ)
`Authenticated Users`	Read & Execute (Чтение и выполнение)

   Удостоверьтесь в том, что группа `Authenticated Users` не имеет какого-то специального разрешения, позволяющего этой группе создавать папки внутри `Profiles`.

4. Настройте общий ресурс `Profile$`, как показано ниже:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`BigFirm/Authenticated Users`	Full Control (Полный доступ)

Не беспокойтесь по поводу того, что у группы Authenticated Users есть разрешение Full Control на этом общем ресурсе; разрешения папки ограничат членов этой группы только чтением ее содержимого. Пользователю впоследствии будут выданы дополнительные разрешения, касающиеся его папки профиля. Теперь вы можете связать общий ресурс Profile$ с папкой из пространства имен DFS.

Этот дополнительный шаг требует гораздо большего объема работы. Вы должны вручную создать и установить разрешения папки, которая будет содержать профиль пользователя. Папка профиля не создается автоматически при входе пользователя в систему из-за ограничивающих разрешений, заданных для папки Profiles. Например, пользователю Joe Bloggs потребуется папка D:\Shares\Profiles\JBloggs.V2, которая должна иметь следующие разрешения:

Группа	Разрешение
BF2\Administrators	Full Control (Полный доступ)
System	Full Control (Полный доступ)
BigFirm/JBloggs	Modify (Изменение)

Вы заметите, что для получения предыдущего набора разрешений должны отключить наследование разрешений. Теперь можете сконфигурировать учетные записи пользователей, указав путь к их профилям. В целом решение выглядит так, как описано ниже.

- Пользователь может перемещаться по общему ресурсу Profile$ с помощью разрешений только для чтения.
- Пользователь имеет разрешение Change (Изменение) только на своем профиле, чего вполне достаточно для обеспечения нормальной функциональности.
- Пользователь не может создавать папки или файлы в Profile$ любыми средствами, не имея административных прав.

Во время тестирования вы обнаружите, что в папке перемещаемого профиля пользователя на файловом сервере ничего не появляется до тех пор, пока пользователь не выйдет из системы. В ходе тестирования вы должны обязательно выполнить следующие два действия.

1. Несколько раз войдите и выйдите из системы от имени отдельного пользователя, чтобы убедиться в том, что его профиль загружается и сохраняется корректно. При каждом входе вносите какие-то изменения.
2. Удостоверьтесь в том, что пользователь, не являющийся администратором, не может читать профили других пользователей, а также не может создавать папки в общем ресурсе Profile$ за пределами собственного профиля.

Проводя тестирование, обратите внимание на папки на файловом сервере и ПК, который вы тестируете. Это послужит хорошим учебным опытом. Вы увидите, что Windows кеширует профиль на ПК. Такой подход очень удобен для пользователей ПК, особенно переносных моделей, если файловый сервер оказывается недоступным при входе пользователя в систему. Представьте ситуацию, когда пользователь приходит к себе домой и не может загрузить свой профиль. При отсутствии кеша пользователь получает временный профиль, который не содержит ни его файлов, ни его настроек. Благодаря кешированию пользователь по-прежнему располагает своими файлами и настройками.

Пример из практики

Полезные советы по поиску и устранению неполадок

Вы можете удалить локально кешированные перемещаемые профили на своем компьютере Windows 8, щелкнув правой кнопкой мыши на значке начального экрана в нижнем левом углу рабочего стола и выбрав в контекстном меню пункт System (Система). Это приведет к запуску аплета System панели управления (очень удобное сокращение). Затем щелкните на ссылке Advanced System Settings (Расширенные параметры системы). На вкладке Advanced (Дополнительно) открывшегося диалогового окна свойств системы щелкните на кнопке Settings (Параметры) в разделе User Profiles (Профили пользователей). В появившемся диалоговом окне отобразятся профили, кешированные на данном ПК. При желании можете выбрать один из них и удалить его.

Вы не должны пытаться удалить профиль пользователя, вошедшего в систему. Даже если вы закроете сеанс этого пользователя и войдете как администратор, то все равно не сможете удалить данный кешированный профиль, поскольку остается открытый или заблокированный файл или папка. Вам придется перезагрузить систему этого ПК.

Если информация на ПК хранится в беспорядке, найти в `C:\Users` папку кешированного профиля, принадлежащую пользователю, может быть нелегко. В случае неполадки или проблемы с доступом возможно наличие нескольких версий профиля, с последней из которых возможно работал пользователь. Выяснить, какую папку использует пользователь, можно с помощью инструмента редактирования реестра `regedit.exe`. Перейдите к разделу `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`. Здесь вы увидите идентификаторы безопасности (SID) пользователей. Если это тестовый компьютер, выяснение данного вопроса не должно составить особого труда. Откройте ключ, имя которого соответствует идентификатору SID пользователя. Значение `ProfileImagePath` будет содержать путь к локально кешированному профилю этого пользователя.

Полезно провести в своей испытательной среде несколько интересных и полезных экспериментов по воссозданию сценариев реального мира. Измените разрешения для папки `Profiles` так, чтобы у пользователя не было никаких разрешений. Переименуйте профиль на файловом сервере, не изменяя объект пользователя. Вы обнаружите, что Windows загрузит локально кешированную копию или сгенерирует временный профиль из стандартного профиля пользователя. Теперь можете попрактиковаться в поиске и устранении неполадок.

Вы уже видели, как создавать перемещаемые профили двумя способами. Это позволяет пользователям переносить по сети рабочую среду, созданную ими в соответствии с индивидуальными потребностями, где бы они ни работали в текущий момент. Но что, если вашей организации требуется заблокировать рабочую среду определенного пользователя, чтобы максимизировать безопасность и упростить пользовательский интерфейс? Такая задача решается с помощью обязательных профилей, которые представляют собой разновидность перемещаемых профилей.

Конфигурирование обязательных профилей

Спросите у бывалого администратора, в чем причина возникновения многих проблем в настольной среде, и вы узнаете, что конфигурация пользователя находится совсем недалеко от верхушки списка. Вам может понадобиться решение, которое обеспечит пользователям ясную конфигурацию всякий раз, когда они входят в систему.

Решением, о котором идет речь, является обязательный профиль. Концепция обязательных профилей предполагает заблаговременное создание профиля для пользователей, его конфигурирование как обязательного профиля и обеспечение его доступности всем требуемым пользователям в качестве их перемещаемого профиля. Какие бы изменения ни вносил пользователь, они сохраняться не будут. При каждом входе пользователя в систему его профиль сбрасывается в то, что определил администратор. Ниже перечислены другие преимущества обязательных профилей.

- Вы можете предоставить пользователю заранее сконфигурированную и согласованную рабочую среду.
- Вы можете гарантировать, что пользователь всегда будет располагать требуемыми ярлыками для доступных приложений.
- Вы можете сократить административную рабочую нагрузку и минимизировать сложности, связанные с перемещаемыми профилями.

Вот типичные сценарии, в которых могут применяться обязательные профили.

- Фермы серверов Remote Desktop Services.
- Среды, где возможна значительная текучесть кадров, а время обучения минимально (например, центры телефонного обслуживания).

Далее вы узнаете, как создать обязательный профиль.

Обязательные профили в Windows 8

Создание обязательных профилей в Windows 8 по-прежнему является процессом, выполняемым вручную. Начните с открытия проводника Windows и перехода в папку `C:\Users` (рис. 26.24). Здесь вы можете увидеть профили, кешированные на этом ПК. Профиль, который вас интересует — `C:\Users\JElway`. Вам нужно скопировать эту папку на общий ресурс `Profiles` на файловом сервере, т.е. в `\\bigfirm.com\BigFirmShares\Profiles\`.

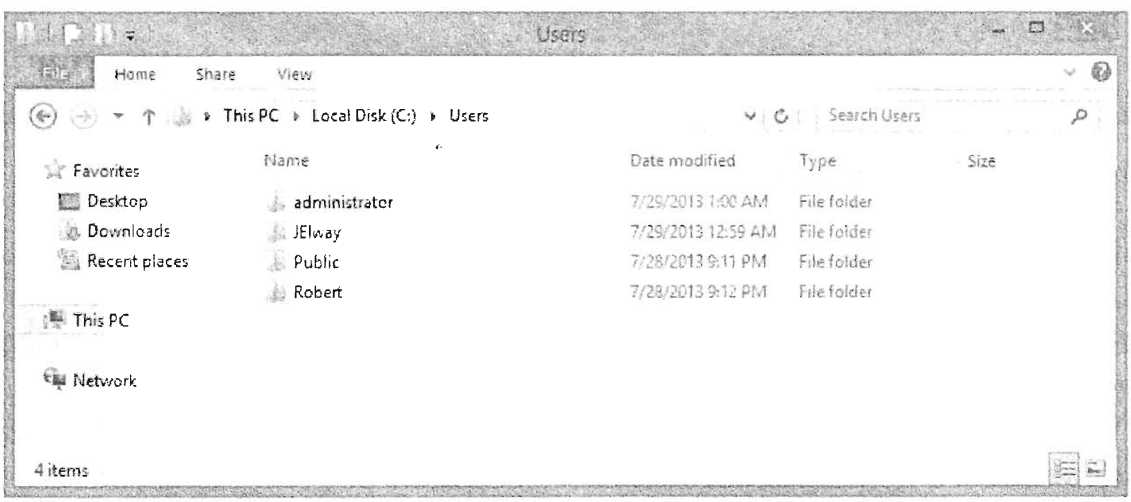


Рис. 26.24. Профили на ПК с Windows 8 в испытательной среде

После копирования вы должны переименовать папку. Имя должно содержать расширение .V2. Мы переименовали папку профиля в Mandatory.V2 (рис. 26.25).

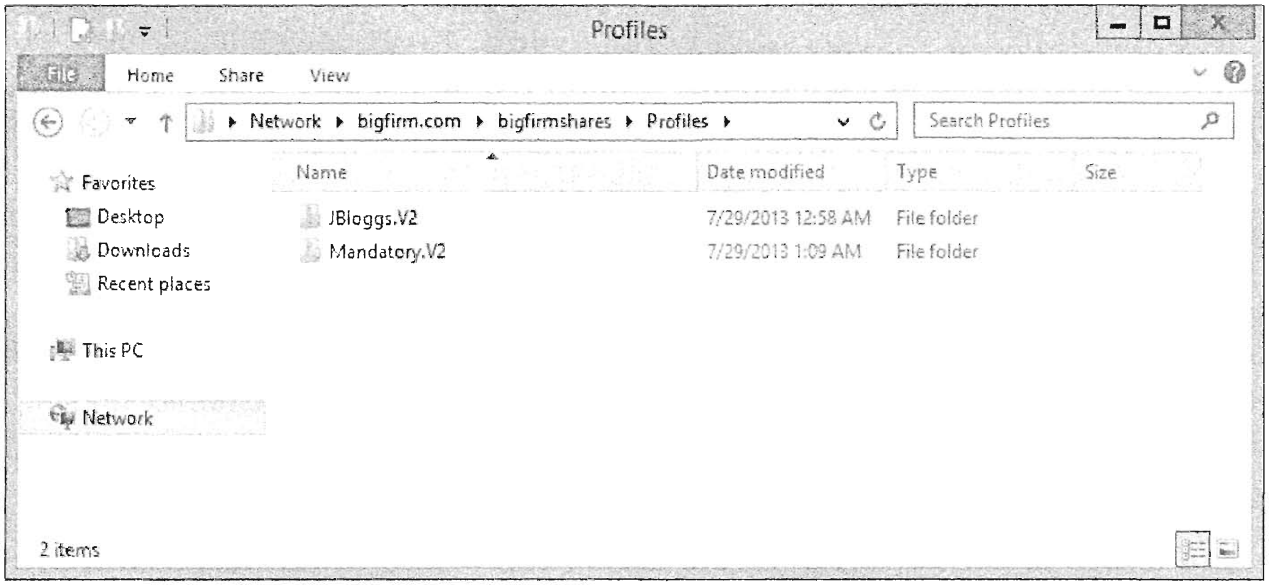


Рис. 26.25. Скопированный профиль на файловом сервере

На рис. 26.26 показаны две папки, которые понадобится удалить из перемещаемого профиля:

- AppData\Local
- AppData\LocalLow

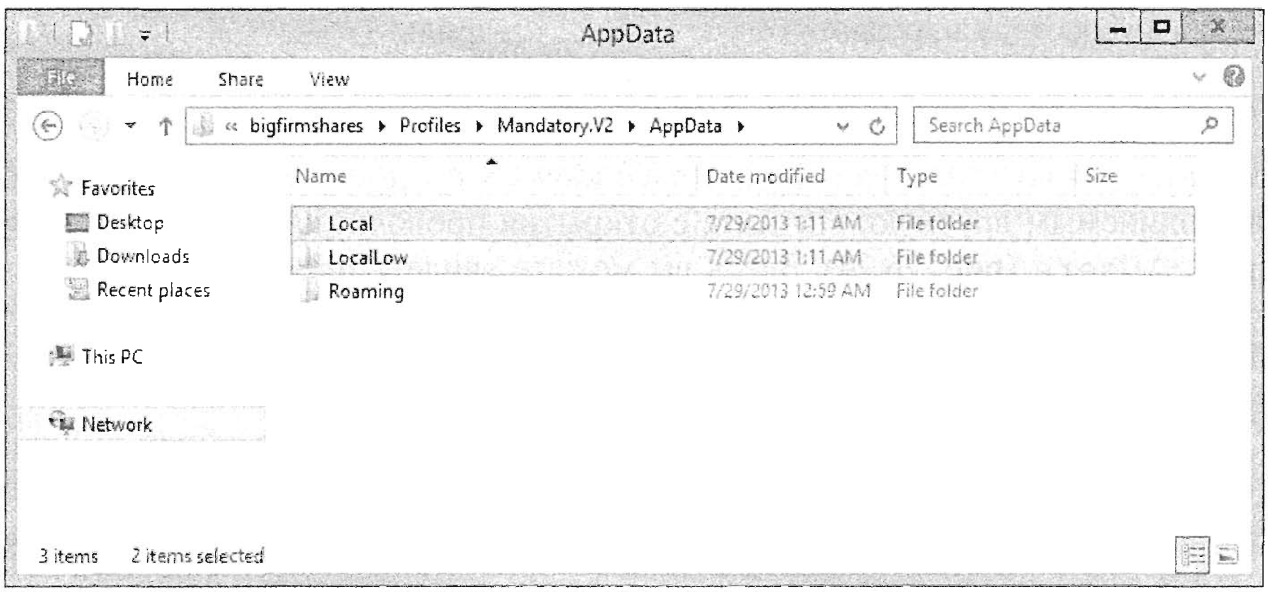


Рис. 26.26. Удаление папок из перемещаемого профиля

Частью профиля является файл по имени NTUSER.DAT. Он содержит куст HKEY_CURRENT_USER из реестра Windows. Он имеет внутренние (не NTFS и не файловой системы) разрешения, которые защищают содержимое файла реестра так, чтобы доступ к нему был только у назначенного пользователя (в этом случае Joe Elway) и у администраторов. Вам необходимо изменить это таким образом, чтобы пользователи нового обязательного перемещаемого профиля имели доступ к содержащемуся в NTUSER.DAT кусту реестра HKEY_CURRENT_USER.

Теперь вам нужно открыть файл NTUSER.DAT в редакторе реестра regedit.exe и изменить разрешения куста HKEY_CURRENT_USER в этом файле.

1. Запустите regedit.exe на файловом сервере и перейдите к разделу HKEY_USERS (рис. 26.27).

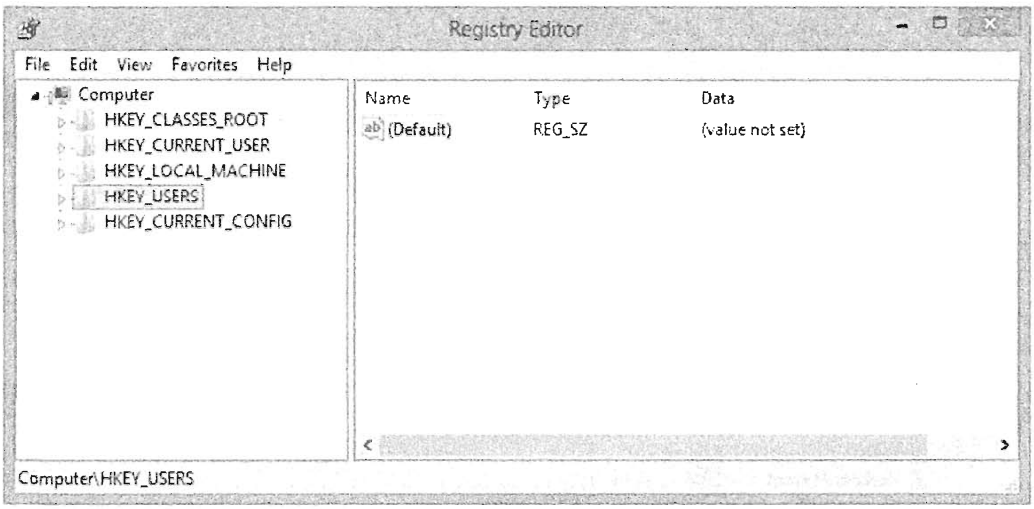


Рис. 26.27. Открытие редактора реестра

2. Выберите пункт меню File⇨Load Hive (Файл⇨Загрузить куст). Откроется диалоговое окно Load Hive (Загрузить куст), приведенное на рис. 26.28.
3. Перейдите в папку на файловом сервере, где содержится файл NTUSER.DAT.

   В данном случае следует перейти к D:\Shares\Profiles\Mandatory.V2\NTUSER.DAT. Откройте этот файл.

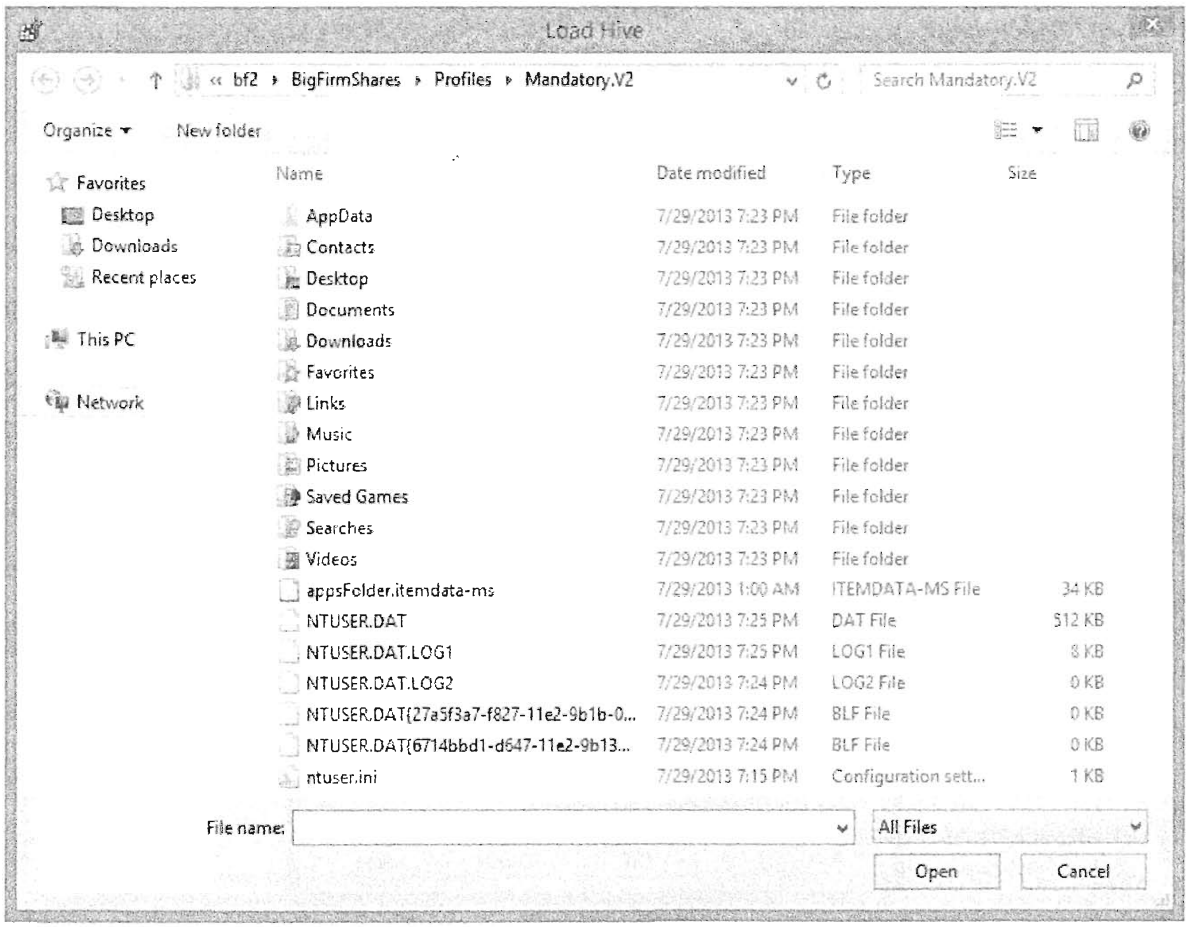


Рис. 26.28. Диалоговое окно Load Hive в редакторе реестра

4. Вам нужно назначить загруженному кусту новое имя. Иметь еще один куст HKEY_CURRENT_USER не допускается. Но не беспокойтесь: это лишь временная метка, которая будет использоваться в ходе редактирования открытого файла NTUSER.DAT. Для простоты мы назвали этот куст по имени профиля, т.е. Mandatory.V2.
5. Перейдите к загруженному кусту, например, Mandatory.V2 (рис. 26.29), и щелкните на нем правой кнопкой мыши.

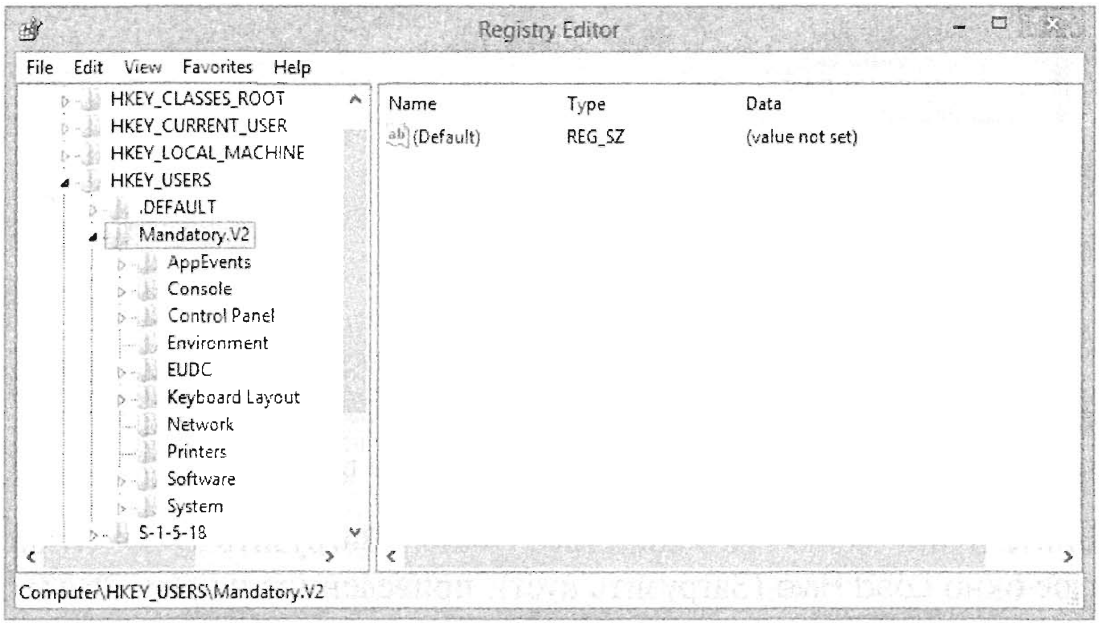


Рис. 26.29. Переход к загруженному кусту реестра

6. Выберите в контекстном меню пункт Permissions (Разрешения); откроется диалоговое окно Permissions (Разрешения).

   На рис. 26.30 показаны разрешения для куста HKEY_CURRENT_USER, содержащегося в файле NTUSER.DAT внутри нового перемещаемого профиля.

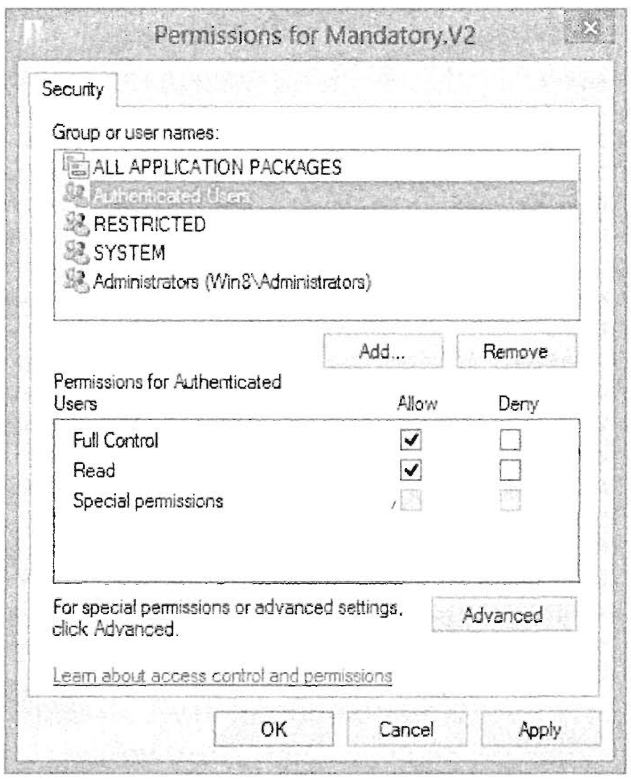


Рис. 26.30. Разрешения для загруженного куста реестра

7. Выполните по отношению к этим разрешениям два действия.
   - Удалите запись для пользователя, который был выбран для создания этого профиля, т.е. `JElway`.
   - Добавьте запись для группы доступа, которой будет требоваться доступ к обязательному перемещаемому профилю. В этом случае такой группой является `Authenticated Users` из домена. Выдайте этой группе разрешение Full Control (Полный доступ) для данного куста.
8. Закройте диалоговое окно Permissions, а затем выберите пункт меню File⇨Unload Hive (Файл⇨Выгрузить куст) в редакторе реестра. Будет задан вопрос, хотите ли вы выгрузить текущий раздел и все его подразделы.
9. Щелкните на кнопке Yes (Да), и модифицированный файл `NTUSER.DAT` сохранится.

Вы не можете использовать этот перемещаемый профиль до тех пор, пока не выгрузите данный куст.

Завершение создания обязательных профилей

К этому моменту вы только создали перемещаемый профиль, который может применять любой пользователь. Вы еще не сделали его *обязательным* перемещаемым профилем. Преобразование производится довольно просто. Перейдите к созданному перемещаемому профилю и переименуйте файл `NTUSER.DAT` в `NTUSER.MAN` (рис. 26.31). Расширение `.MAN` сообщает Windows о том, что никакие изменения в этом профиле сохраняться не должны, т.е. он является обязательным перемещаемым профилем.

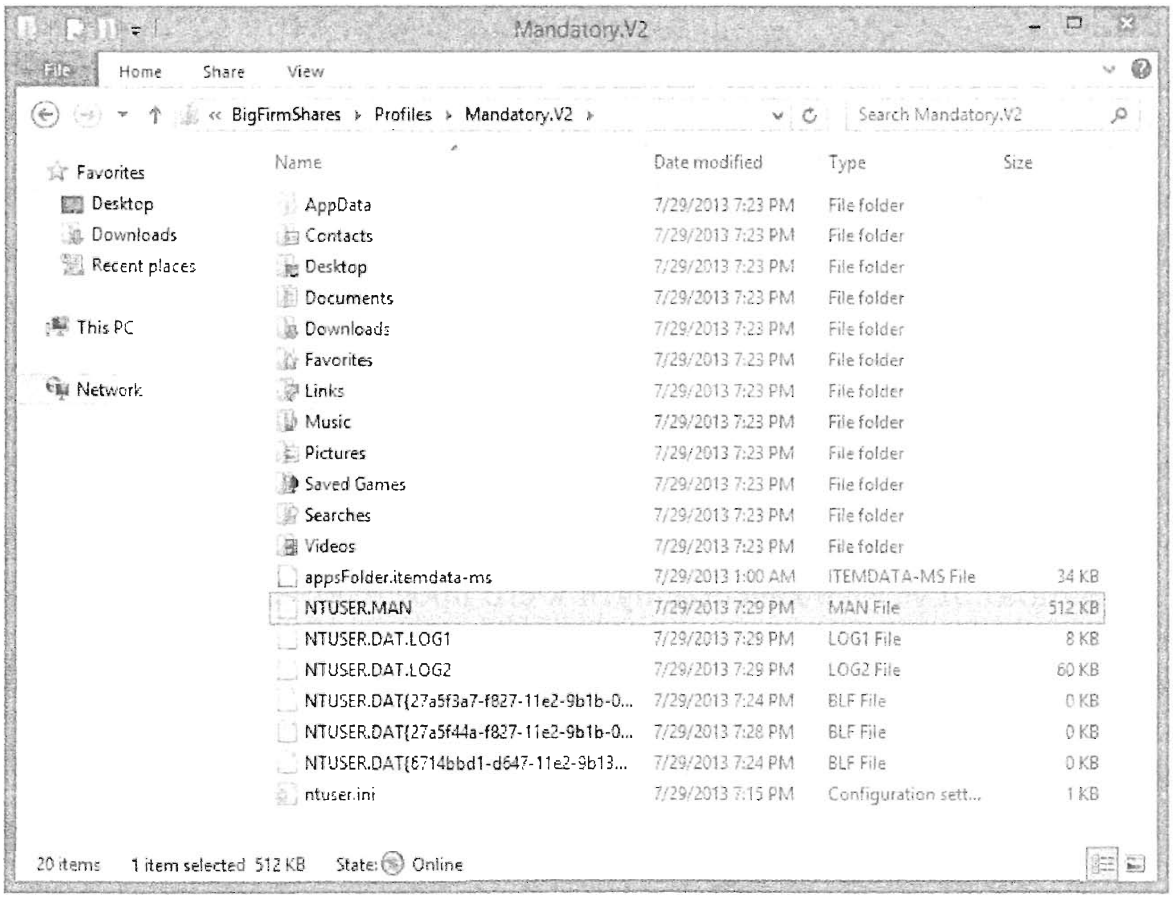


Рис. 26.31. Переименование файла `NTUSER.DAT` в `NTUSER.MAN`

Вам необходимо надлежащим образом защитить папку обязательного перемещаемого профиля на файловом сервере. Выполните следующие шаги.

1. Отключите наследование разрешений из родительской папки и установите разрешения обязательного профиля, как показано ниже:

Группа	Разрешение
`BF2\Administrators`	Full Control (Полный доступ)
`System`	Full Control (Полный доступ)
`BigFirm\Authenticated Users`	Read & Execute (Чтение и выполнение)

   Вы предоставили доступ группе `Authenticated Users`.

2. Выберите группу, соответствующую группе, которой вы предоставили доступ к кусту реестра в `NTUSER.DAT`.

   Установка разрешений папки преследует две цели. Она предоставляет группе `Authenticated Users` (или другой выбранной группе) доступ к обязательному перемещаемому профилю, но не позволяет членам этой группы изменять его.

   Теперь необходимо протестировать этот обязательный перемещаемый профиль.

3. Перейдите к тестовому пользователю и измените его запись профиля на `\\bigfirm.com\BigFirmShares\Profiles\Mandatory`.

Куда делось расширение `.V2`?

Обратите внимание, что расширение `.V2` не добавлялось. Как обсуждалось ранее, более новые версии Windows добавляют его по мере надобности.

---

4. Войдите в систему от имени тестового пользователя и убедитесь в том, что настройки обязательного перемещаемого профиля загружены.

5. Внесите какие-нибудь изменения, затем отмените их и внесите еще несколько произвольных изменений.

6. Выйдите из системы и войдите еще раз.

Вы должны обнаружить, что загруженный профиль сбрасывается к исходному обязательному перемещаемому профилю; никакие изменения не сохраняются. Если это действительно так, значит, обязательный перемещаемый профиль функционирует корректно.

Вы сконфигурировали пользователя `JBloggs` с `\\bigfirm.com\BigFirmShares\Profiles\Mandatory.V2` в качестве пути к его профилю.

Пользователь Joe Bloggs теперь попытается загружать обязательный перемещаемый профиль каждый раз, когда будет входить в систему. Если вы вошли как `JBloggs` в систему рабочей станции, то увидите, что весь профиль идентичен профилю пользователя `JElway`. Вы по-прежнему можете вносить изменения. Тем не менее, при выходе из системы эти изменения не сохраняются. Вы можете войти снова и получить тот же самый обязательный профиль, как и ранее, безо всяких внесенных до этого изменений, которые не были сохранены.

Конфигурирование принудительных профилей

Существуют сценарии, при которых вы применяете обязательные профили, но не можете разрешить пользователю вход в систему, если по какой-то причине не удается загрузить обязательный профиль (например, из-за проблем в сети или на файловом сервере). Когда это может оказаться реалистичным вариантом? Возможно, речь идет об информационном киоске или публично доступном компьютере, где лучше вообще не предоставлять обслуживание, чем делать это, не обеспечивая жесткий контроль. Таким образом, похоже, что вам необходимо найти решение для этого сценария. К счастью, решение имеется в форме *принудительных (super-mandatory) профилей*. Реализация этого решения особо не отличается от реализации обязательных профилей.

Настройка принудительного профиля является продолжением настройки обязательного профиля. Выполните ранее описанные шаги для конфигурирования обязательного профиля, а затем перечисленные ниже действия.

1. Переименуйте папку профиля на файловом сервере, добавив расширение `.MAN.V2`; например, переименуйте `Mandatory.V2` в `Mandatory.MAN.V2`.
2. Сконфигурируйте профиль пользователя так, чтобы он включал расширение `.MAN`.
3. Проигнорируйте компонент `.V2`; например, установите профиль в `\\bigfirm.com\BigFirmShares\Profiles\Mandatory.MAN`.

Вот и все, что требовалось сделать. Вы создали принудительный профиль для пользователя. Этот профиль будет действовать подобно нормальному обязательному профилю, не позволяя сохранять на файловом сервере какие-либо изменения. Однако в отличие от обычного обязательного профиля данный пользователь не сможет войти в систему, если принудительный не удается загрузить.

Существует одна распространенная ошибка, которую вы можете воссоздать с целью тестирования этой функциональности, не допускающей открытия сеанса. Переименуйте файл `NTUSER.MAN` внутри принудительного профиля в `NTUSER.DAT`. После этого попробуйте войти в систему как пользователь `JBloggs`. Вы будете проинформированы о том, что данный профиль загрузить не удалось и пользователь не может войти. Завершив тестирование, не забудьте переименовать файл обратно в `NTUSER.MAN`!

Конфигурирование стандартного сетевого профиля

Стандартный профиль применяется для создания пользователю профиля, если он еще им не располагает. Предположим, что пользователь, не имеющий конфигурации перемещаемого профиля, входит в систему Windows 8 или Windows Server 2012. Его новый профиль создается за счет копирования содержимого папки `C:\Users\Default` в новую папку профиля пользователя `C:\Users\<имя_пользователя>`.

Администраторам доступен способ предоставления пользователям адаптированного стандартного профиля по сети. Компьютеры, являющиеся членами домена, будут автоматически искать стандартный сетевой профиль. Если он существует, то используется вместо стандартного профиля, который хранится локально на компьютере. Стандартный сетевой профиль применяется в случае, когда нужно обеспечить для пользователей заранее сконфигурированную рабочую среду. Напоминает обя-

зательный профиль, не так ли? Разница заключается в том, что стандартный сетевой профиль просто копируется, чтобы стать собственным профилем пользователя. Пользователь имеет возможность сохранять изменения в собственном профиле.

Процесс создания стандартного сетевого профиля очень похож на процесс создания обязательного профиля.

1. Создайте шаблонного пользователя.
2. Войдите в систему тестового компьютера от имени этого пользователя.
3. Сконфигурируйте профиль шаблонного пользователя и выйдите из системы.
4. Войдите в систему компьютера как администратор и скопируйте профиль шаблонного пользователя в `\\<Имя домена Active Directory>\Netlogon\Default User.V2`.

   В примере, рассматриваемом в настоящей главе, это будет `\\bigfirm.com\Netlogon\Default User.V2`. Обратите внимание на расширение `.V2`. Оно обозначает профили версии 2 для Windows 8 и Windows Server 2012 или последующих версий.
5. Удостоверьтесь в том, что группе `Authenticated Users` разрешено использовать этот новый профиль, когда вы копируете его.
6. Выполните процесс, который применялся ранее в главе для копирования и назначения разрешений профилям.

Этот стандартный сетевой профиль теперь будет копироваться каждому новому пользователю в сети.

Недостаток такого решения связан с последним утверждением. Стандартный сетевой профиль определяет конфигурацию пользователя, в том числе региональные настройки. Рассмотрим организацию, имеющую офисы филиалов в других странах. Пользователям филиалов могут быть необходимы разные региональные настройки, которые соответствовали бы их клавиатурам и т.п. Изменять эти настройки для пользователя, когда он впервые входит в систему, было бы несколько надоедливо. Кроме того, следует проявлять аккуратность при сохранении в профиле настроек, специфичных для местоположения. Вряд ли имеет смысл сохранить отображения дисков для файлового сервера в Нью-Йорке лишь для того, чтобы пользователь, который вошел в систему офиса в Сан-Франциско, отдаленного более чем на 5000 км, обнаружил, что его файловый сервер работает чересчур медленно.

Нельзя предусмотреть стандартный сетевой профиль для каждого местоположения. Такой профиль можно хранить только в определенной папке, которая копируется на все контроллеры домена посредством репликации SYSVOL.

Стандартные сетевые профили хороши для простых сетей, где каждый пользуется одной и той же базовой конфигурацией. Вы должны все тщательно взвесить и обдумать вопрос развертывания стандартных сетевых профилей в более сложных сетях, в которых пользователям требуются отличающиеся базовые конфигурации, такие как региональные настройки. Действительно, пользователь имеет возможность изменить эти настройки, когда впервые входит в систему, но при этом могут возникать немало обращений в службу поддержки. Можно обратиться к автоматизированному конфигурированию. Для определения региональных настроек после входа пользователя в систему можно было бы воспользоваться объектом GPO, но это ограничит возможности пользователя. Практика показывает, что в такой среде

не все пользователи одного офиса применяют одну и ту же конфигурацию. Вместо стандартного сетевого профиля подумайте о решении со сценариями или групповой политикой, которая будет создавать такие локализованные конфигурации при первом входе пользователя. Это позволит тем немногим пользователям, которым требуется специализированная конфигурация, изменять свою конфигурацию и сохранять нужные настройки.

Управление перемещаемыми профилями

Перемещаемые профили требуют определенного обдумывания, если у вас применяются разные операционные системы, пользователи перемещаются между филиалами, которые соединены ограниченными сетевыми каналами, и используются службы удаленных рабочих столов. Некоторые действия по расширенному управлению профилями могут быть выполнены с помощью групповой политики, как было показано выше, когда вы выдавали администраторам права на автоматически генерируемые профили.

Давайте взглянем на несколько примеров, когда могут возникнуть проблемы. Если вы располагаете фермой серверов Remote Desktop, то пользователь может войти в систему любого из них. При наличии 1000 пользователей, входящих в системы 10 серверов, может быть создано 10 000 кешированных перемещаемых профилей. В результате значительное дисковое пространство расходуется впустую.

Вам может понадобиться учесть, сколько пространства на диске занимает перемещаемый профиль. Например, пользователи могут выгрузить в папку `My Music` полную коллекцию своих файлов MP3. Это может представляться пользователям вполне невинным действием, поскольку по их предположению они потребляют только локальное хранилище. Но речь идет о перемещаемых профилях: если 1000 пользователей начнут регулярно делать что-то подобное, то вскоре на файловых серверах организации терабайты дисковой памяти будут заняты данными, не связанными с бизнес-деятельностью. Должна ли организация платить за это? Решение предусматривает применение объектов GPO компьютера и пользователя для управления поведением перемещаемых профилей в этих и других обстоятельствах.

Настройки компьютера

Сейчас мы покажем, как с помощью групповой политики можно управлять перемещаемыми профилями на основе индивидуальных компьютеров. Каждый пользователь, входящий в систему компьютера, который наследует сконфигурированные вами настройки GPO, будет подчиняться этим настройкам.

Очистка профилей

Вы наверняка заметите, что локально кешируемая копия обязательного профиля создается и *сохраняется* на рабочей станции, относящейся к серверу Remote Desktop. Если хорошо подумать, то нет особого смысла хранить такую копию в средах, где используется обязательные профили.

Даже если обязательные профили не применяются, может понадобиться какой-нибудь способ очистки устаревших профилей при перезагрузке компьютера. Групповая политика предоставляет ряд инструментов для решения этой задачи (табл. 26.1).

Таблица 26.1. Объект GPO кешированных пользовательских профилей

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей)	Delete cached copies of roaming profiles (Удалять кешируемые копии перемещаемых профилей)	Локально кешируемые копии перемещаемых профилей будут удалены, когда пользователь выходит из системы
Computer Configuration \ Administrative Templates \ System \ User Profiles	Delete user profiles older than a specified number of days on system restart (Удалять профили пользователей, которые старее указанного количества дней, при перезапуске системы)	Профили, которые старее указанного количества дней, будут автоматически удалены при перезапуске компьютера

Множество сайтов и перемещаемые профили

Как вы поступите с пользователем, который имеет перемещаемый профиль и объезжает филиалы компании, разбросанные по всему миру? По умолчанию компьютер, в систему которого входит этот пользователь, будет измерять скорость сети между собой и местом, где хранится профиль. Если канал считается слишком медленным, профиль загружаться не будет. Вместо этого пользователю будет предложен временный локальный профиль. Однако следует помнить о том, что такой вариант не подходит для принудительных профилей. Вы можете управлять этим процессом измерения с использованием объекта GPO (табл. 26.2).

Таблица 26.2. Медленные сети и объект GPO профилей пользователей

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей)	Do not detect slow network connections (Не обнаруживать медленные сетевые подключения)	Вы можете предотвратить обнаружение компьютером ситуации, когда загрузка профиля окажется слишком долгой. Будьте осторожны с этой политикой, потому что вход пользователя в систему может занимать *очень* много времени и вызывать перегрузку канала WAN в офисе филиала
Computer Configuration \ Administrative Templates \ System \ User Profiles	Prompt user when a slow network connection is detected (Запросить пользователя при обнаружении медленного сетевого подключения)	Если обнаружено медленное сетевое подключение, пользователю можно выдать запрос, что позволит ему принять решение загружать свой перемещаемый профиль, невзирая на проблемы с сетью. Пользоваться этой политикой также следует очень осторожно
Computer Configuration \ Administrative Templates \ System \ User Profiles	Control slow network connection time-out for user profiles (Управлять тайм-аутом медленного сетевого подключения для профилей пользователей)	Это позволяет определить, что означает "медленный" при измерении скорости канала к файловому серверу, хранящему профиль пользователя. Скорость указывается в Кбит/с, а время ожидания — в миллисекундах
Computer Configuration \ Administrative Templates \ System \ User Profiles	Wait for remote user profile (Ожидать профиль удаленного пользователя)	Это предписывает системе ожидать столько времени, сколько требуется для загрузки перемещаемого профиля. Игнорируется, если включена политика Do not detect slow network connections

Это дает довольно грубый механизм предоставления пользователям перемещаемых профилей, когда они отправляются в другие местоположения. В вашем распоряжении есть и ряд других способов приспособления среды к бизнес-нуждам.

Если пользователи располагают предсказуемыми маршрутами поездок, появляется возможность задействовать репликацию DFS (DFS Replication — DFS-R). Теперь вы понимаете, почему мы предпочитаем применять файловую систему DFS для размещения домашних каталогов и профилей пользователей. Избранные папки можно реплицировать на серверы в других офисах филиалов. Вы обнаружите, что управлять всем этим может быть нелегко, поэтому планируйте такую репликацию предельно внимательно.

Альтернативным вариантом является предоставление пользователям возможности иметь для каждого сайта разные перемещаемые профили. Это означало бы, что перемещаемый профиль пользователя в действительности не переносился бы между сайтами, а только между компьютерами внутри сайта. Это можно сконфигурировать с помощью перечисленных ниже настроек объекта GPO.

- **Путь.** Путь выглядит как Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей).
- **Политика.** Политикой является Set roaming profile path for all users logging onto this computer (Устанавливать путь перемещаемого профиля для всех пользователей, входящих в систему этого компьютера).
- **Описание.** Вы можете указывать путь к перемещаемым профилям для любых пользователей, входящих в систему данного компьютера. Применяйте переменную `%username%`, чтобы предоставить пользователям разные профили. Это имеет более высокий приоритет, чем профиль, указанный в объекте пользователя.

Службы Remote Desktop Services

Существует ряд сложностей, которые должны быть приняты во внимание при работе со службами Remote Desktop Services и перемещаемыми профилями.

- Не рекомендуется сочетать перемещаемый профиль рабочего стола пользователя с профилем, который будет использоваться на сервере Remote Desktop или виртуальном рабочем столе, т.к. произойдет смешивание настроек реестра и ярлыков из разных систем.
- На ферме серверов Remote Desktop можно задействовать концепцию "хранилищ приложений"; другими словами, на серверах Server1 и Server2 может быть установлено приложение BizzApp, а на Server3 — нет. При этом нежелательно, чтобы ярлыки для BizzApp появлялись, когда пользователь входит в систему сервера Server3 с перемещаемым профилем.
- Распространенным применением серверов Remote Desktop является обеспечение доступа пользователей, работающих в офисах филиалов, к приложениям из центрального сайта. Нежелательно, чтобы перемещаемые профили филиалов загружались через WAN, но нужно какое-то решение для перемещаемых профилей.

Отключить перемещаемые профили на компьютере можно с помощью следующего объекта GPO.

- **Путь.** Путь выглядит как Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей).
- **Политика.** Политикой является Only allow local user profiles (Разрешить только локальные профили пользователей).
- **Описание.** Запрещает использование перемещаемых профилей на этом компьютере.

Это довольно примитивное решение. Оно отключает возможность загрузки перемещаемого профиля и возвращает вас к сценарию, при котором пользователь не располагает согласованной рабочей средой.

В качестве альтернативы можно сконфигурировать пользователей со специальными перемещаемыми профилями для ферм компьютеров. Например, когда пользователь входит в систему на ферме серверов Remote Desktop, он получит отдельный профиль из общего ресурса перемещаемых профилей для серверов Remote Desktop. Когда пользователь входит в систему своего ПК, он будет использовать выделенный профиль из общего ресурса перемещаемых профилей для ПК. Наконец, когда пользователь входит в систему виртуального рабочего стола, он будет применять специальный профиль из общего ресурса перемещаемых профилей для виртуальных рабочих столов. Требуемые для этого настройки перечислены в табл. 26.3.

Таблица 26.3. Объект GPO для профилей Remote Desktop Services

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ Windows Components \ Remote Desktop Services \ Remote Desktop Session Host \ Profiles (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Службы удаленных рабочих столов \ Хост сеансов Remote Desktop \ Профили)	Set path for Remote Desktop Services roaming user profile (Установить путь для перемещаемого профиля пользователя Remote Desktop Services)	Вы можете указать путь к профилю для учетной записи пользователя, когда он входит посредством Remote Desktop Services. Это имеет более высокий приоритет, чем все остальные настройки профилей. С помощью переменной `%username%` можно разрешить множество профилей или просто применять одну папку для всех пользователей
Computer Configuration \ Administrative Templates \ Windows Components \ Remote Desktop Services \ Remote Desktop Session Host \ Profiles	Use mandatory profiles on the Remote Desktop session host server (Использовать обязательные профили на сервере хоста сеансов Remote Desktop)	Если эта политика включена, она превращает профиль, указанный в предыдущей настройке объекта GPO, в обязательный профиль

Второй набор настроек в табл. 26.3 позволяет сообщить компьютеру о необходимости трактовать любой перемещаемый профиль как обязательный профиль, т.е. никогда не сохранять любые изменения, внесенные пользователем. Это является альтернативой ранее описанному методу создания обязательного перемещаемого профиля.

В среде Windows Server 2012 вы найдете эти настройки GPO в Computer Configuration \ Administrative Templates \ Windows Components \ Remote Desktop Services \ Remote Desktop Session Host \ Profiles (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Службы удаленных рабочих столов \ Хост сеансов Remote Desktop \ Профили).

Указание профиля Remote Desktop Services

В учетной записи пользователя есть параметр для указания профиля Remote Desktop Services. Это довольно простое решение, которое предполагает существование для пользователя только одного возможного профиля, подходящего всем серверам Remote Desktop. Такой вариант может быть приемлемым в небольших организациях с одним или двумя серверами Remote Desktop. Мы рекомендуем обдумать применение для управления перемещаемыми профилями Remote Desktop Services подхода с GPO.

Если вы используете перемещаемые профили на своих серверах Remote Desktop, то вам понадобится очищать кешированные профили (обсуждаемые ранее в этой главе). Если не обращать на них внимания, они могут быстро поглотить значительное пространство на системном диске.

Дополнительные настройки GPO для перемещаемых профилей

Вы ознакомились примерно лишь с половиной настроек GPO, которые можно применять для конфигурирования перемещаемых профилей. Остальные настройки перечислены в табл. 26.4.

Таблица 26.4. Прочие настройки GPO для перемещаемых профилей

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей)	User management of sharing user name, account pictures and domain information with apps (Пользовательское управление совместным доступом приложений к именам пользователей, изображениям учетных записей и информации о домене)	Позволяет приложениям иметь доступ к имени пользователя, изображению учетной записи и информации о домене
Computer Configuration \ Administrative Templates \ System \ User Profiles	Set user home folder (Установить домашнюю папку пользователя)	Вы можете сконфигурировать домашнюю папку пользователя здесь, а не в учетной записи пользователя
Computer Configuration \ Administrative Templates \ System \ User Profiles	Set the schedule for background upload of a roaming user profile's registry file while user is logged on (Установить расписание для фоновой выгрузки файла реестра перемещаемого профиля пользователя, когда пользователь вошел в систему)	Вы можете сконфигурировать расписание для регулярной выгрузки файла `NTUSER.DAT` на файловый сервер в фоновом режиме, когда пользователь вошел в систему

Продолжение табл. 26.4

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ User Profiles	Do not check for user ownership of Roaming Profile Folders (Не проверять право владения пользователем папками перемещаемых профилей)	По умолчанию Windows проверяет право владения пользователем для профиля, прежде чем загружать его. Эта политика может отменить такую проверку
Computer Configuration \ Administrative Templates \ System \ User Profiles	Do not forcefully unload the user's registry at user logoff (Не выполнять принудительную выгрузку реестра пользователя при выходе из системы)	Когда пользователь выходит из системы, его приложения должны закрыться и освободить дескрипторы открытых файлов в реестре. Приложения, которые завершились некорректно, могут это не сделать. В таком случае Windows закроет дескрипторы принудительно. Возможны сценарии, когда это нежелательно
Computer Configuration \ Administrative Templates \ System \ User Profiles	Do not log on users with temporary profiles (Не разрешать вход пользователей с временными профилями)	Оказывает такое же воздействие, как и принудительный профиль. Когда профиль, назначенный пользователю, не может быть загружен, пользователь немедленно автоматически выводится из системы после успешной попытки входа
Computer Configuration \ Administrative Templates \ System \ User Profiles	Leave Windows Installer and Group Policy Software Installation Data (Оставлять данные программы установки Windows и групповой политики установки программного обеспечения)	Приложения для пользователя допускается устанавливать посредством групповой политики. При этом данные сохраняются в профиле пользователя. Удаление этого профиля приводит к удалению сохраненных в нем данных и, как следствие, к необходимости повторной установки приложений. Эта политика предотвращает такие нежелательные повторные установки
Computer Configuration \ Administrative Templates \ System \ User Profiles	Maximum retries to unload and update user profile (Максимальное количество повторных попыток выгрузки и обновления профиля пользователя)	Позволяет администратору указать, сколько раз Windows будет пытаться сохранить файл `NTUSER.DAT` на общем файловом ресурсе. Может возникнуть потребность увеличить это число, если неустойчиво работающее приложение не успевает обновить упомянутый файл при выходе из системы. По умолчанию Windows совершает максимум 60 попыток в течение 60 секунд
Computer Configuration \ Administrative Templates \ System \ User Profiles	Prevent Roaming Profile changes from propagating to the server (Предотвращать распространение изменений перемещаемого профиля на сервер)	Любые изменения, внесенные в профиль пользователя на данном компьютере, не сохраняются в его перемещаемом профиле

Окончание табл. 26.4

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ User Profiles	Set maximum wait time for the network if a user has a roaming user profile or remote home directory (Установить максимальное время ожидания для сети, если пользователь имеет перемещаемый профиль или удаленный домашний каталог)	В случае недоступности файлового сервера с такими общими ресурсами Windows ожидает вплоть до 30 секунд. Вы можете переопределить эту настройку. Это может применяться в беспроводных сетях, когда вы замечаете, что загрузка перемещаемых профилей и подключение к домашним каталогам не происходят по причине нехватки времени
Computer Configuration \ Administrative Templates \ System \ User Profiles	Establish time-out for dialog boxes (Установить тайм-аут для диалоговых окон)	Когда для принятия решения требуется взаимодействие с человеком, Windows отображает диалоговое окно. По умолчанию тайм-аут для диалоговых окон составляет 30 секунд. Этот параметр можно изменять в пределах от 0 до 600 секунд

Все эти настройки относятся к компьютеру, т.е. оказывают влияние на всех пользователей, входящих в систему компьютера, к которому применена данная политика. Для управления перемещаемыми профилями политики можно также применять к объектам пользователей.

Настройки пользователя

Некоторые настройки можно применять для управления перемещаемыми профилями каждого индивидуального пользователя. С помощью настроек, приведенных в табл. 26.5, можно управлять содержимым перемещаемого профиля или даже размером самого профиля.

Таблица 26.5. Настройки GPO для содержимого перемещаемых профилей

Путь	Политика	Описание
User Configuration \ Administrative Templates \ System\User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей)	Exclude directories in roaming profile (Исключить каталоги в перемещаемом профиле)	Иногда необходимо, чтобы некоторые папки были доступными не на всех компьютерах. Такие папки можно указать в этой политике. Папки `Appdata\Local` и `Appdata\LocalLow`, а также их содержимое по умолчанию на файловый сервер не реплицируются
User Configuration \ Administrative Templates \ System \ User Profiles	Limit profile size (Ограничить размер профиля)	Для перемещаемых профилей можно определить квоту. Операционные системы версий, предшествующих Windows Vista, просто отказывали пользователю во входе, если квота была превышена. ОС Windows Vista позволяет пользователю выходить без сохранения профиля на файловом сервере. Пользователи могут получать уведомление о проблеме, а также напоминания о ней с применением установленного сообщения, которое выдается в заданные моменты времени

Будьте внимательны, применяя политику Limit profile size. Помните, что внутри нее содержатся такие папки, как `My Documents` и `Desktop`. Вам понадобится найти способ перенести их в другое место (вскоре мы обсудим этот вопрос).

Перенаправление папок

Использование перемещаемых профилей стало распространенной практикой в мире Windows. Они справляются со своими задачами, но далеки от совершенства.

Перемещаемым профилям присущи сложности, связанные с загрузкой, выгрузкой и порчей файлов. Сложности могут оказаться весьма существенными. Решением является *перенаправление папок*.

Перенаправление папок позволяет перемещать специальные папки внутри профиля пользователя в другое, более подходящее место. Например, вместо того чтобы хранить эти папки в перемещаемом профиле, вы можете поместить их в домашний каталог пользователя. Перенаправление папок позволяет перемещать следующие папки:

- `AppData(Roaming)`
- `Desktop`
- `Start Menu`
- `Documents`
- `Pictures`
- `Music`
- `Videos`
- `Favorites`
- `Contacts`
- `Downloads`
- `Links`
- `Searches`
- `Saved Games`

Происхождение перенаправления папок

Перенаправление папок впервые появилось в Windows 2000 Server как часть технологии IntelliMirror. Концепция IntelliMirror заключалась в том, чтобы предоставить пользователю мобильную рабочую среду, которая сопровождала бы его везде, куда бы он ни перемещался. К сожалению, по прошествии лет это фирменное название, похоже, вышло из употребления.

После просмотра этого списка может показаться, что он представляет все самое важное в профиле. Если вы можете хранить эти папки внутри какой-то специальной папки, то зачем вообще нужны перемещаемые профили?

Это очень хороший вопрос. На самом деле многие организации больше не беспокоятся о развертывании перемещаемых профилей. Вы уже видели, что разверты-

вание перемещаемого профиля в дополнение к домашнему каталогу удваивает объем работы по администрированию, которую придется выполнять. Сохраняя папки в домашнем каталоге пользователя, вы можете в два раза уменьшить объем администрирования общего файлового ресурса в сети. Это упрощает развертывание, резервное копирование/восстановление, обеспечение безопасности, аудит, архивирование, а также планирование и реализацию восстановления в аварийных ситуациях. С перемещаемыми профилями связано много сложностей, таких как их мобильность между компьютерами с разными конфигурациями программного обеспечения и между компьютерами с разными операционными системами.

Так что же в точности делает перенаправление папок? Все довольно просто: вы конфигурируете каждую из перечисленных выше специальных папок так, чтобы она указывала на другое местоположение за пределами профиля. Этим местоположением может быть общий файловый ресурс, уникальный для пользователя. Возможно, такая папка уже существует — если вы создали домашние каталоги для каждого из своих пользователей, то можете сконфигурировать перенаправление папок для отображения на домашние каталоги, а не на профиль. Например, папка `My Documents` обычно существует в профиле как `Documents`. При использовании перенаправления папок она могла бы существовать как `Documents` в домашнем каталоге. Подобным образом можно достичь следующих целей.

- Вы можете перенаправить все требуемые папки в домашний каталог, чтобы обеспечить пользователю согласованную рабочую среду в текущей и унаследованной операционных системах; т.е. данные существуют за рамками ограничений, налагаемых версиями профиля.
- За счет перенаправления папок, которые содержат пользовательские данные, вы можете надежно применять квоты размеров профилей, не оказывая влияния на бизнес-данные в таких папках, как `My Documents`.
- Возможно, вам удалось бы полностью устранить потребность в профилях посредством перенаправления всех папок, которые важны для организации. Перемещаемые профили могут быть источником неприятностей, а некоторые администраторы считают их устаревшей технологией.

Прежде чем двигаться дальше, мы должны быстро обдумать вопрос, который может возникнуть в этот момент. Как воспользоваться папкой вроде `My Documents`, если она перенаправлена на файловый сервер, а вы являетесь пользователем, который путешествует с переносным компьютером? По умолчанию перенаправленные папки реплицируются на локальный компьютер с применением средства Offline Files (Автономные файлы), которое создает на этом компьютере защищенный кеш файлов. Когда компьютер подключен к сети, он синхронизирует кеш Offline Files с общими ресурсами на файловом сервере (или серверах).

Базовое перенаправление папок

Возможно, вам уже не терпится узнать, как выполняется перенаправление папок. Что же, мы не будем тянуть с этим. Перенаправление папок управляется с помощью настроек групповой политики, которые применяются к пользователям. Предположим, что все ваши пользователи находятся в `\bigfirm.com\BigFirm\Users`.

Вы уже создали и привязали к этой организационной единице политику под названием User Folder Redirections.

1. Отредактируйте объект политики, предназначенный для применения к учетным записям пользователей, для которых вы хотите перенаправить папки.
2. Создайте политику и привяжите ее к организационной единице `Users`, как показано на рис. 26.32.

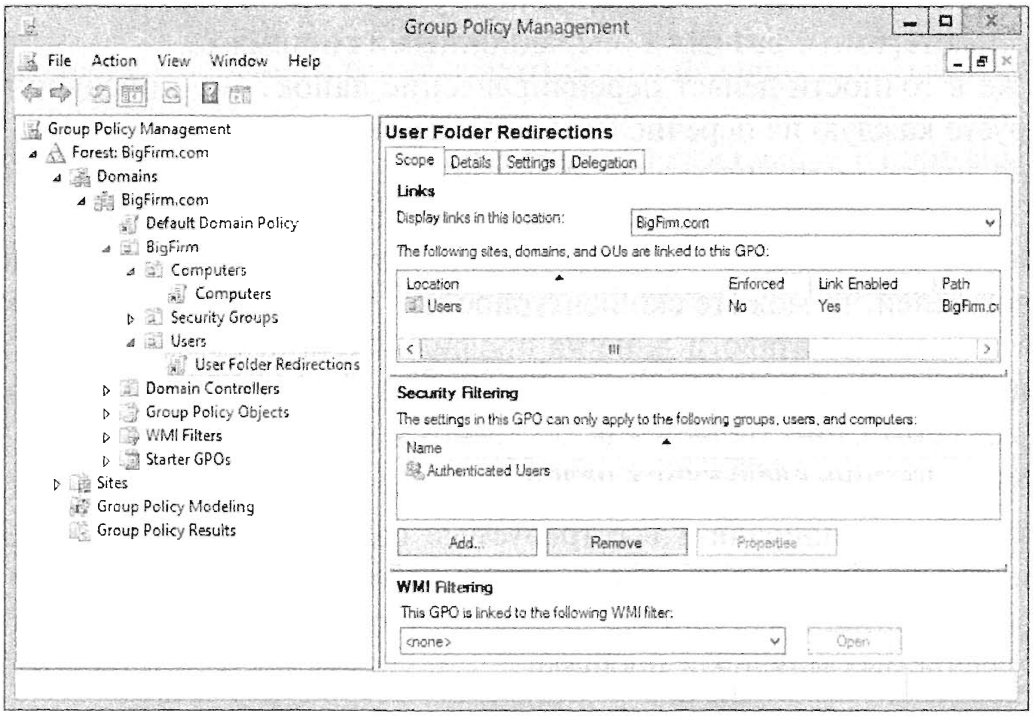


Рис. 26.32. Новый объект GPO для перенаправления папок пользователя

3. Перейдите к контейнеру User Configuration \ Windows Settings \ Folder Redirection (Конфигурация пользователя \ Настройки Windows \ Перенаправление папок).

   Здесь видны все папки, которые можно перенаправить на текущем компьютере Windows (рис. 26.33).

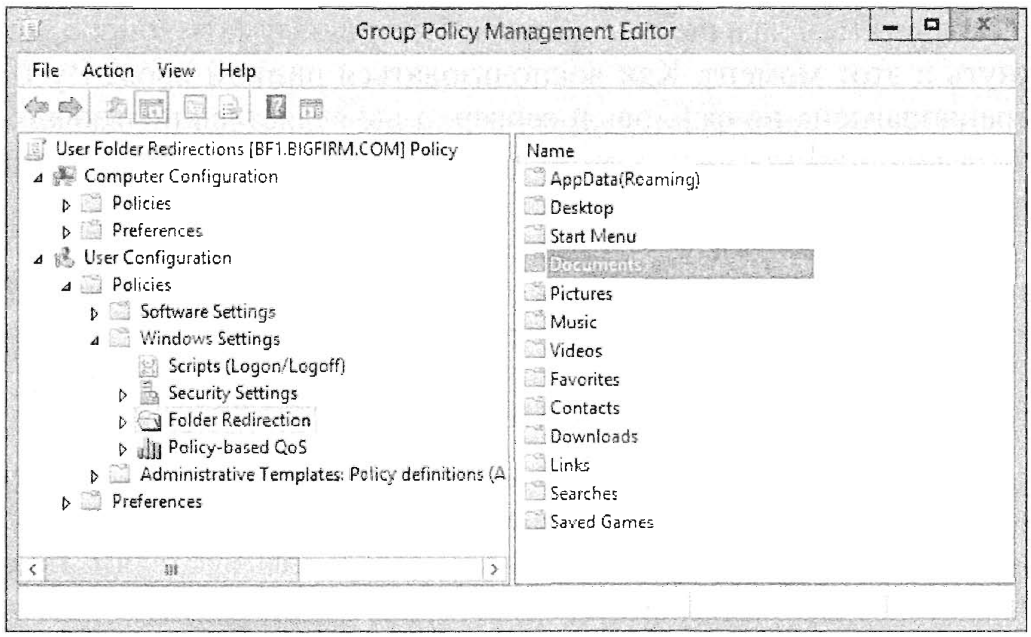


Рис. 26.33. Политики перенаправления папок

Для начала вам предстоит перенаправить папку Documents в домашний каталог пользователя.

4. Щелкните правой кнопкой мыши на папке Documents и выберите в контекстном меню пункт Properties (Свойства).

   Откроется диалоговое окно свойств, в котором можно сконфигурировать перенаправление этой папки. В раскрывающемся списке Setting (Настройка) доступно три варианта перенаправления.

   - **Not Configured (Не сконфигурировано).** Отключает перенаправление папки.
   - **Basic — Redirect Everyone's Folder To The Same Location (Базовое — перенаправить папку любого пользователя в одно и то же место).** Позволяет сконфигурировать всех пользователей на перенаправление в общее местоположение. Например, домашние каталоги всех пользователей находятся на общем файловом ресурсе, поэтому все папки следует перенаправить в \\bigfirm.com\BigFirmShares\Home. Это политика "на все случаи жизни", которая обычно оказывается самым подходящим вариантом.
   - **Advanced — Specify Locations For Various User Groups (Расширенное — указать места для разных групп пользователей).** Позволяет указывать уникальные пути для разных групп. Этот вариант будет выбираться, когда структура организационной единицы не соответствует желаемой схеме перенаправления папок.

   Мы рассмотрим простой подход, который, скорее всего, будет применяться — базовое перенаправление.

5. Выберите Basic — Redirect Everyone's Folder To The Same Location, как показано на рис. 26.34.

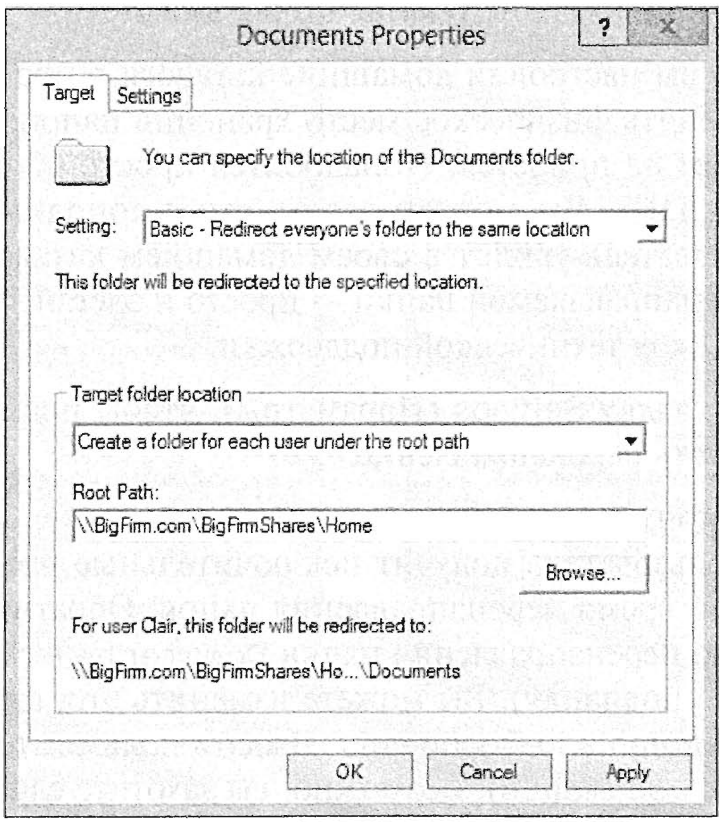


Рис. 26.34. Перенаправление папок в домашний каталог пользователя

В раскрывающемся списке внутри раздела Target Folder Location (Местоположение целевой папки) на выбор предлагаются варианты, зависящие от того, какая папка перенаправляется.

- **Redirect To The User's Home Directory (Перенаправить в домашний каталог пользователя).** Это очень простое решение перенаправляет папку в домашний каталог пользователя. Оно не создает подпапку для перенаправляемой папки. Вместо этого содержимое перенаправляемой папки просто копируется в корень домашнего каталога пользователя. При перенаправлении множества папок для пользователей возникнет путаница.
- **Create A Folder For Each User Under The Root Path (Создать папку для каждого пользователя под корневым путем).** При выборе этого варианта будет создаваться папка с именем перенаправляемой папки внутри указанного пути; например, папка `Documents` будет создана в `\\bigfirm.com\BigFirmShares\Home\JBloggs`, если вы указали путь `\\bigfirm.com\BigFirmShares\Home`. Заметили, насколько интеллектуально добавляется имя пользователя? Такой подход позволяет не допустить упомянутой выше путаницы.
- **Redirect To The Following Location (Перенаправить в следующее место).** Это простое перенаправление, где все пользователи будут совместно пользоваться общей папкой. Такой вариант может оказаться подходящим в случае перенаправления папки `Start Menu` для фермы серверов Remote Desktop.
- **Redirect To The Local User Profile Location (Перенаправить в место, где хранится профиль локального пользователя).** Это приводит к возвращению папки обратно в локальный профиль.

6. Как показано на рис. 26.34, выберите папку `Documents` для перенаправления на подпапку внутри домашнего каталога пользователя.

   Вспомните, что вы настроили домашние каталоги в пространстве имен DFS. Вы можете изменять физическое место хранения папок, но модифицировать эту политику вам не придется. Понадобится просто обновить ссылку в пространстве имен DFS. Вы можете делать это с дополнительными папками, зная, что пользователь увидит в своем домашнем каталоге отдельную папку для каждой перенаправляемой папки — просто и элегантно, к тому же меньше обращений в службу технической поддержки.

7. Перейдите на вкладку Settings (Параметры), чтобы посмотреть, как Windows будет обрабатывать перенаправление.

Вскоре мы рассмотрим настройки, представленные на рис. 26.35.

По умолчанию пользователь получит исключительные права доступа к любым папкам, созданным во время перенаправления папок. Обратите внимание, что это не относится к случаю перенаправления папки `Documents` в сам домашний каталог (т.е. не в какую-то его подпапку). Вы можете изменить это, сняв отметку с флажка Grant the user exclusive rights to Documents (Выдать пользователю исключительные права доступа к папке `Documents`). Возможно, вы захотите сделать это, если планируете выполнять административные задачи с папкой `Documents`, оказывая помощь

пользователю, либо использовать учетные записи администраторов для проведения таких действий по обслуживанию, как архивирование или резервное копирование/восстановление. Мы сделали это, как показано на рис. 26.36.

Во время применения политики перенаправления можно перемещать все содержимое папки `Documents` в профиле. По умолчанию флажок Move the contents of Documents to the new location (Переместить содержимое папки `Documents` в новое место) отмечен, поскольку обычно именно это и требуется. Тем не менее, такое поведение можно отключить, сняв отметку с упомянутого флажка.

Вы можете изменить то, что произойдет, когда конфигурируемая в данный момент политика больше не применяется к пользователю. По умолчанию выбран переключатель Leave the folder in the new location when policy is removed (Оставить папку в новом месте, когда политика удаляется), т.е. при отключении перенаправления папка и ее содержимое остаются там же, где они находятся в настоящий момент. В такой ситуации можно выбрать переключатель Redirect the folder back to the local userprofile location when policy is removed (Перенаправить папку обратно в локальный профиль пользователя, когда политика удаляется).

В диалоговом окне свойств папки `Documents` на рис. 26.36 запрещено предоставление исключительных прав доступа, а также включено перемещение ее содержимого и поддержка унаследованных операционных систем. Кроме того, папка `Documents` будет перенаправляться обратно в профиль пользователя, когда политика больше не применяется.

Теперь необходимо провести тестирование, как описано ниже.

1. Войдите в систему тестовой рабочей станции с применением учетной записи пользователя, наследующей новую политику.

   Для входа в систему Win8 используйте учетную запись `JBloggs`, которая сконфигурирована так, чтобы не применять перемещаемый или обязательный профиль.

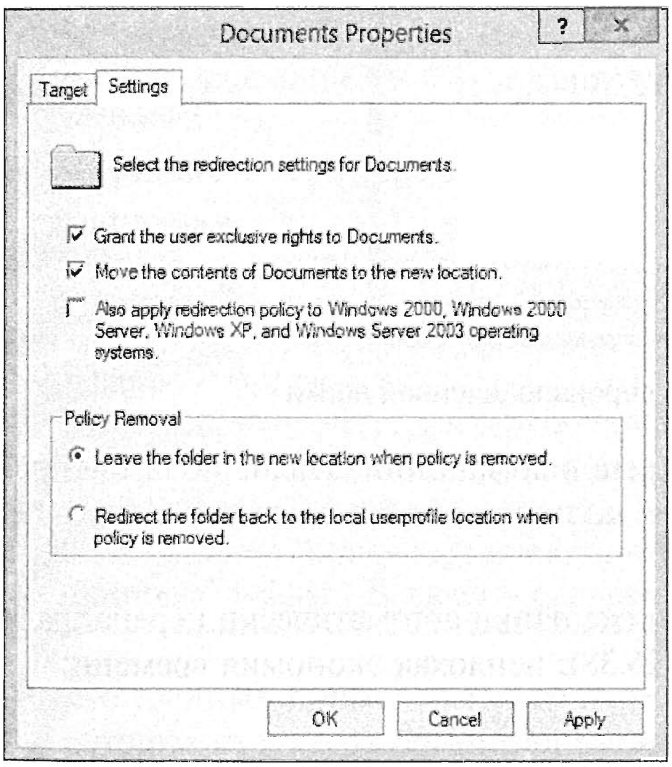


Рис. 26.35. Стандартные настройки перенаправления папки `Documents`

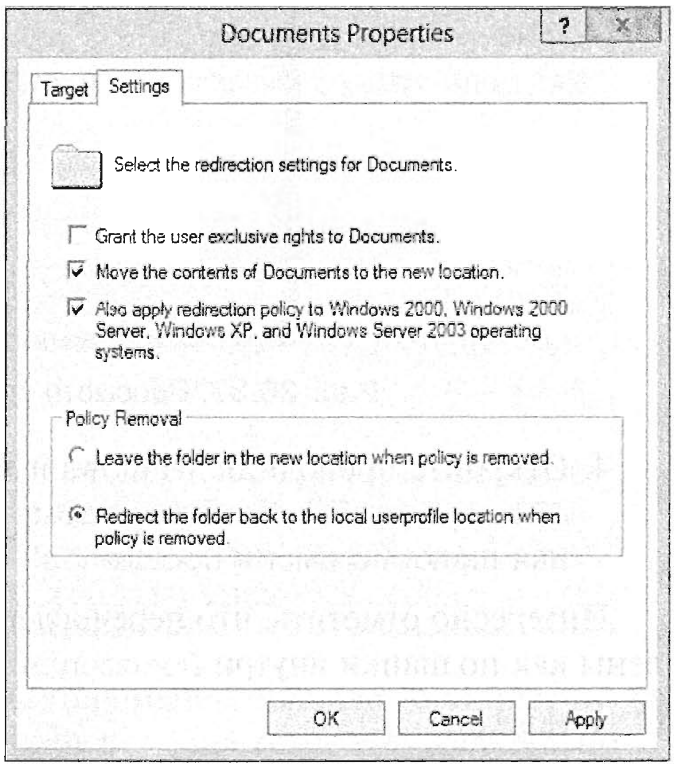


Рис. 26.36. Сконфигурированные настройки перенаправления папки `Documents`

2. В испытательной среде ждать обновления политик не обязательно, поэтому запустите на тестовой рабочей станции следующую команду:

   ```
   gpupdate /target:user /force
   ```

   В команде указан флаг `/force`, т.к. некоторые настройки GPO для применения могут требовать двух обновлений.

   Вы получите уведомление о том, что для вступления в силу новых настроек политики потребуется выйти из системы. Это является признаком того, что перенаправление папок работает — оно применяется только во время входа. Войдите в систему еще раз и проверьте, где теперь находится папка `Documents`.

3. Войдите от имени пользователя `JBloggs` и откройте диалоговое окно свойств папки `Documents`.

   Местоположение папки `Documents` указывает на то, что она была перенаправлена в домашний каталог пользователя. На рис. 26.37 видно, что в этом примере `Documents` перемещена в папку по имени `Documents` внутри домашнего каталога пользователя `JBloggs` на файловом сервере.

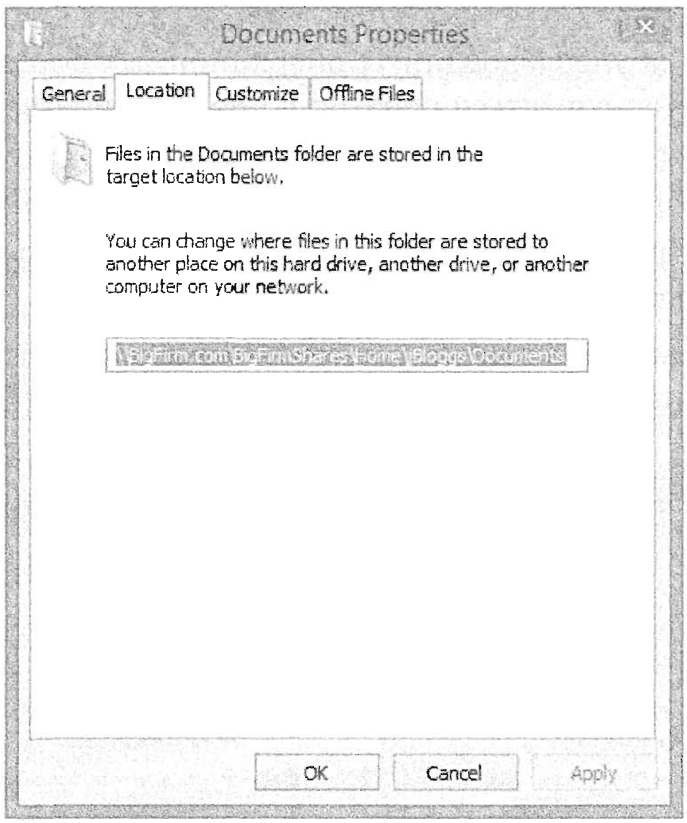


Рис. 26.37. Просмотр свойств перенаправленной папки

4. Откройте проводник Windows и перейдите в домашний каталог пользователя `JBloggs`, чтобы убедиться в том, что для пользователя была создана специальная папка по имени `Documents`.

Интересно отметить, что перечисленные ниже папки автоматически перенаправлены как подпапки внутри `Documents` (рис. 26.38); неплохая экономия времени:

- `Music`
- `Pictures`
- `Videos`

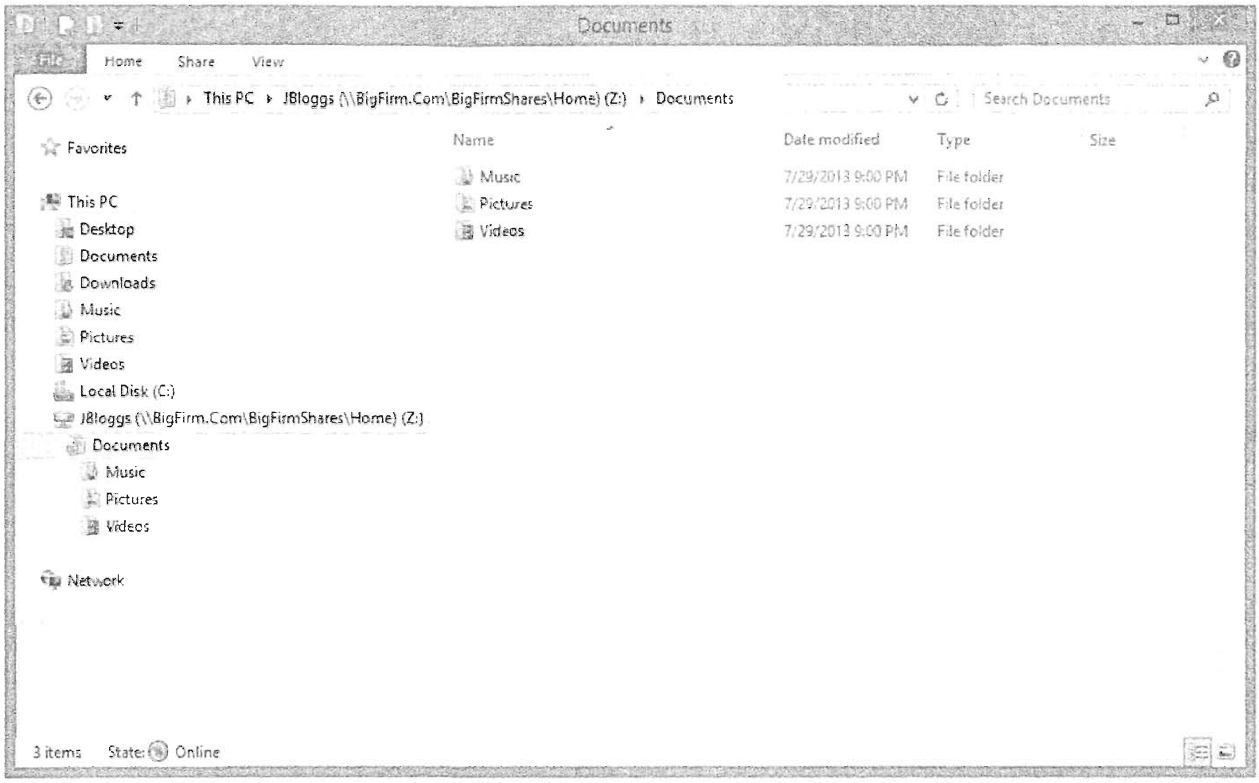


Рис. 26.38. Содержимое перенаправленной папки `Documents`

Причина в том, что стандартная настройка групповой политики для этих папок предусматривает их следование за папкой `Documents`, куда бы она ни была перенаправлена. В действительности пользовательских данных в указанных папках вполне достаточно, чтобы можно было полностью отказаться от концепции профилей!

Синхронизация с учетом стоимости

В Windows Server 2012 и Windows 8 теперь имеется возможность отключить фоновую синхронизацию данных при соблюдении следующих условий:

- пользователь подключен к сети с помощью измеряемого сетевого соединения (типа мобильной сети 4G) и вплотную приблизился к своему лимиту или даже превысил его;
- пользователь находится в сети другого поставщика.

Операционные системы Windows Server 2012 и Windows 8 автоматически отслеживают коэффициент использования полосы пропускания и роуминг на измеряемых соединениях. Это позволяет им узнать, когда переключаться в автономный режим, и предотвращает синхронизацию данных. Пользователю по-прежнему доступна синхронизация вручную, и эту возможность можно переопределить для определенных пользователей, например, для руководителей.

Данная функция управляется политикой Computer Configuration \ Administrative Templates \ Network \ Offline Files \ Enable file synchronization \ Enable file synchronization on costed networks (Конфигурация компьютера \ Административные шаблоны \ Сеть \ Автономные файлы \ Включить синхронизацию файлов в затратных сетях).

Рассмотренный пример базового перенаправления папок подойдет организациям, в которых структура организационных единиц подобна тому, как желательно применять перенаправление папок. Далее мы перейдем к исследованию расширенного перенаправления папок.

Расширенное перенаправление папок

Базовое перенаправление папок конфигурирует каждого пользователя, получившего эту политику, для перенаправления своих папок в похожей манере. В большинстве ситуаций такого способа, вероятно, будет вполне достаточно, но временами может понадобиться применить единственную политику, обеспечивающую перенаправление пользователей в разные места в зависимости от членства в группах, а не только от местоположения организационной единицы. Ниже приведено несколько примеров.

- Для разных групп внутри организации вы применяете разные политики безопасности к общим ресурсам с домашними каталогами. Это означает, что профиль пользователя A может храниться не в том же общем ресурсе, где находится профиль пользователя B.
- Вы управляете репликацией DFS домашних каталогов на основе индивидуальных общих ресурсов.
- Вам пришлось развернуть несколько серверов для общих файловых ресурсов с домашними каталогами.

Для применения политики к группам доступа можно использовать расширенное перенаправление папок. Каждая группа доступа будет получать отличающуюся конфигурацию для политики перенаправления папок. Все станет немного яснее, когда вы посмотрите на него в действии.

Откройте диалоговое окно свойств папки, которую необходимо перенаправить. В предыдущем примере было выбрано базовое перенаправление папок. На этот раз выберите в раскрывающемся списке Setting (Настройка) вариант Advanced — Specify Locations For Various User Groups (Расширенное — указать места для разных групп пользователей). Чтобы указать конкретную группу пользователей и место для перенаправления папки, щелкните на кнопке Add (Добавить). Диалоговое окно, показанное на рис. 26.39, позволяет выполнить следующие действия.

- Выбрать группу доступа, к которой будет применяться данная политика.
- Определить, куда будет перенаправляться папка. Набор настроек идентичен тем, что находятся в разделе Target Folder Location (Местоположение целевой папки) окна при базовом перенаправлении папок.
- Указать путь, где будет располагаться перенаправленная папка.

На рис. 26.40 видно, что с помощью единственного объекта GPO перенаправление одиночной папки можно конфигурировать для разных групп доступа по-разному.

На рис. 26.41 мы сконфигурировали три группы доступа для перенаправления папки `Documents`, используя разнообразные методы внутри единственного объекта GPO. Это демонстрирует, насколько гибким может быть перенаправление папок и как его можно подгонять под нужды организации.

Управление перенаправлением папок

Для конфигурирования перенаправления папок применяются настройки GPO, описанные в табл. 26.6. Управление обработкой перенаправления папок осуществляется с помощью других настроек групповой политики.

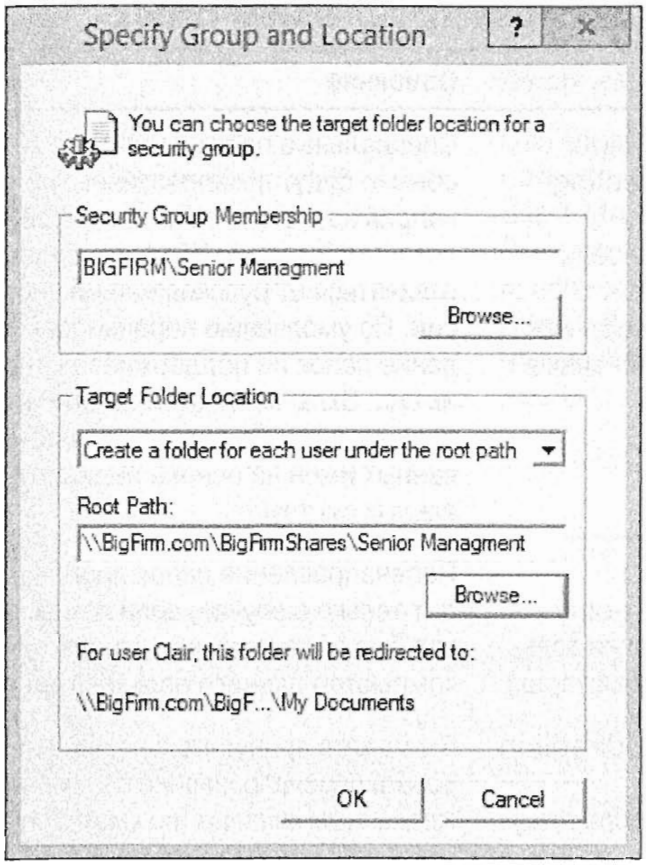


Рис. 26.39. Настройка расширенного перенаправления папок под корневым путем

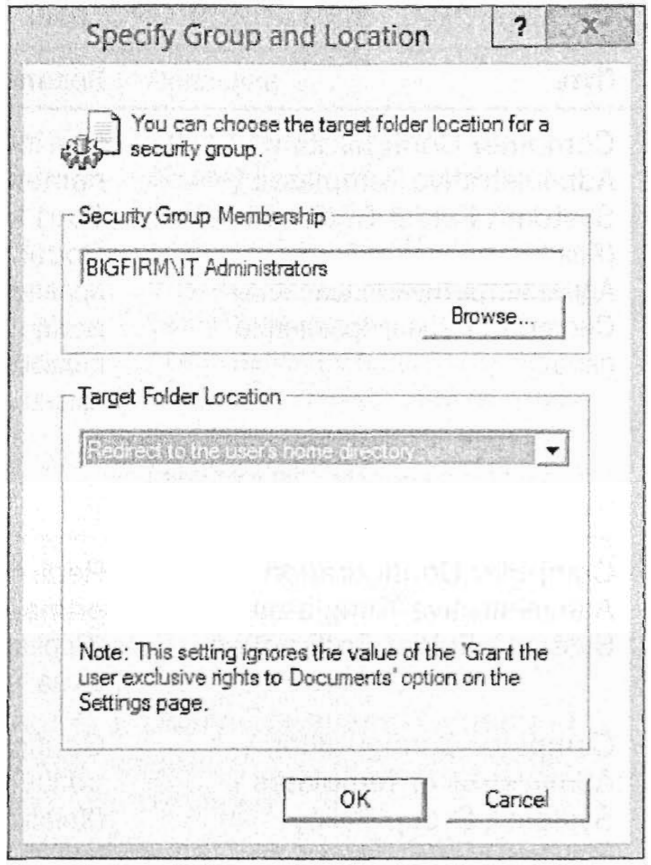


Рис. 26.40. Расширенное перенаправление папок в домашний каталог пользователя

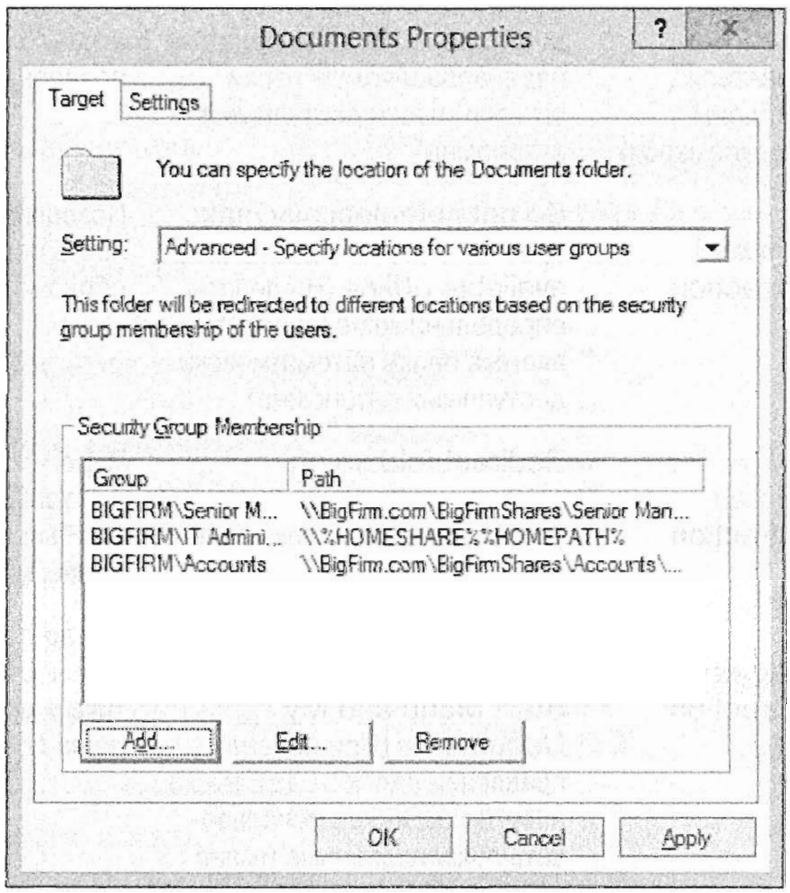


Рис. 26.41. Настройки расширенного перенаправления папок

Таблица 26.6. Настройки GPO для управления перенаправлением папок

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ Folder Redirection (Конфигурация компьютера \ Административные шаблоны \ Система \ Перенаправление папок)	Use localized subfolder names when redirecting Start Menu and My Documents (При перенаправлении папок `Start Menu` и `My Documents` использовать локализованные имена подпапок)	Специальные папки в профиле обычно будут локализованными; например, то, что вы видите в англоязычной версии Windows, будет отличаться от русскоязычной версии. По умолчанию перенаправление папок не поддерживает эти имена. Включение этой политики разрешит применение локализованных имен на основе индивидуальных систем
Computer Configuration \ Administrative Templates \ System \ Folder Redirection	Redirect folders on primary computers only (Перенаправлять папки только на основных компьютерах)	Перенаправление папок происходит только в случае, если компьютер был обозначен как основной компьютер данного пользователя
Computer Configuration \ Administrative Templates \ System \ Group Policy (Конфигурация компьютера \ Административные шаблоны \ Система \ Групповая политика)	Configure folder redirection policy processing (Конфигурировать обработку политики перенаправления папок)	Вы можете принудительно инициировать перенаправление папок по медленным каналам (по умолчанию отключено). Вы можете также сконфигурировать обработку политики перенаправления папок так, чтобы она выполнялась, даже если эта политика не была изменена
User Configuration \ Administrative Templates \ System\Folder Redirection (Конфигурация пользователя \ Административные шаблоны \ Система \ Перенаправление папок)	Do not automatically make redirected folders available offline (Не делать перенаправляемые папки автоматически доступными автономно)	Перенаправляемые папки автоматически синхронизируются с помощью средства Offline Files. Это поведение можно отключить
User Configuration \ Administrative Templates \ System \ Folder Redirection	Do not automatically make specific redirected folders available offline (Не делать определенные перенаправляемые папки автоматически доступными автономно)	Позволяет предотвратить доступность перенаправляемых папок оболочки автономно
User Configuration \ Administrative Templates \ System \ Folder Redirection	Redirect folders on primary computers only (Перенаправлять папки только на основных компьютерах)	Перенаправление папок происходит только в случае, если компьютер был обозначен как основной компьютер данного пользователя
User Configuration \ Administrative Templates \ System \ Folder Redirection	Use localized subfolder names when redirecting Start Menu and My Documents (При перенаправлении папок `Start Menu` и `My Documents` использовать локализованные имена подпапок)	Предоставляет такую же функциональность, как аналогичная политика в конфигурации компьютера, но на основе пользователей

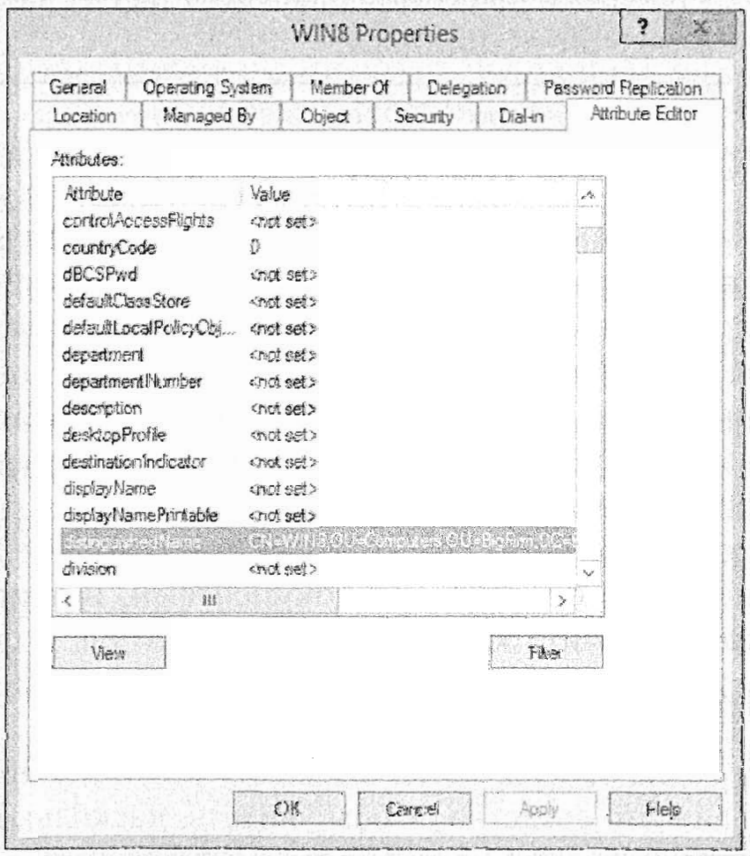
Окончание табл. 26.6

Путь	Политика	Описание
User Configuration \ Administrative Templates \ System \ Folder Redirection	Use localized subfolder names when redirecting Start Menu and My Documents (При перенаправлении папок `Start Menu` и `My Documents` использовать локализованные имена подпапок)	Специальные папки в профиле обычно будут локализованными; например, то, что вы видите в англоязычной версии Windows, будет отличаться от русскоязычной версии. По умолчанию перенаправление папок не поддерживает эти имена. Включение этой политики разрешит применение локализованных имен на основе индивидуальных пользователей

Поддержка основного компьютера

В Windows Server 2012 и Windows 8 появилось функция Primary Computer (Основной компьютер), или поддержка родства пользовательских устройств в отношении перемещаемых профилей и перенаправлению папок. Что это означает? Теперь у вас есть возможность отслеживать, какие компьютеры могут обращаться к перенаправляемым папкам и/или перемещаемым профилям пользователя. Применение этой возможности обеспечивает много преимуществ:

- сокращает время входа в систему, когда это делается не на основном компьютере пользователя;
- снижает риск оставления пользователем важных данных на компьютере, не отмеченном в качестве основного, в систему которого входил пользователь (например, на компьютере в конференц-зале или в киоске);
- предотвращает порчу профилей пользователей, когда используются компьютеры с разными аппаратными конфигурациями, такие как системы x86 и x64.

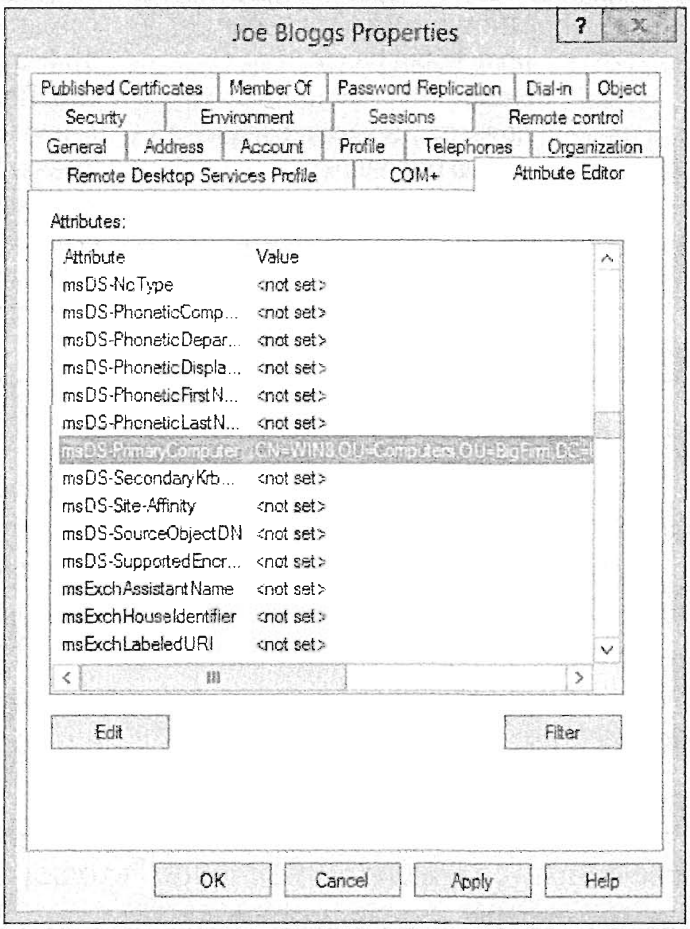


Чтобы задействовать поддержку Primary Computer, каждому пользователю понадобится назначить, по меньшей мере, один основной компьютер, выполнив следующие шаги.

1. Получите отличительное имя компьютера пользователя.

   Это можно сделать в расширенном представлении оснастки Active Directory Users and Computers. Откройте диалоговое окно свойств объекта компьютера, выполните прокрутку до атрибута `distinguishedName` и скопируйте его значение.

2. Откройте диалоговое окно свойств объекта пользователя, которому необходимо назначить основной компьютер. Выполните прокрутку до атрибута `msDS-PrimaryComputer` и вставьте в качестве его значения скопированное ранее отличительное имя.



3. Создайте и привяжите политику GPO из табл. 26.6, которая управляет поддержкой основного компьютера.

Рабочие папки

Еще одной новой возможностью в Windows Server 2012 R2 является Work Folders (Рабочие папки). Это средство позволяет конечным пользователям синхронизировать рабочие данные на всех своих устройствах. Когда пользователь сохраняет файлы в своих рабочих папках на рабочей станции в офисе, эта рабочая станция будет синхронизироваться с устройствами пользователя. Звучит знакомо? Именно это делают SkyDrive, SkyDrive Pro и множество других потребительских продуктов. Зачем тогда применять Work Folders? В решении для предприятия можно использовать продукт SkyDrive Pro, который интегрирован с SharePoint, позволяет пользователям совместно работать над документами, и доступен на мобильных устройствах. Но если вы хотите задействовать существующие файловые серверы и только расширить возможность синхронизации пользовательских файлов, то Work Folders будет оптимальным выбором.

Итак, теперь, когда вы знаете причины применения Work Folders, давайте установим это средство, чтобы увидеть, насколько легко добавить такую возможность в среду.

Установка Work Folders

Войдите в систему файлового сервера BF2. Откройте окно диспетчера серверов и добавьте роль Work Folders, которая находится в разделе File and Storage Services (Службы файлов и хранилища). Данную роль можно также установить с помощью следующей команды PowerShell:

```
Install-WindowsFeature FS-SyncShareService
```

Это приведет к установке роли Work Folders и ее зависимостей — роли IIS Web Server (Веб-сервер IIS) с компонентом IIS Hostable Web Core (Размещаемое веб-ядро IIS). Следует также отметить, что клиенты Work Folders взаимодействуют с серверами Work Folders только через протокол SSL, поэтому вам потребуется сконфигурировать открытый или самозаверяющий сертификат и обеспечить его установку на всех клиентах. Кроме того, понадобится сделать этот сервер доступным в Интернете — возможно, посредством обратного прокси или сетевого шлюза.

Конфигурирование общего ресурса синхронизации

Интерфейс средства Work Folders очень прост и удобен в использовании; вы найдете его в виде узла управляющей панели File and Storage Services. Чтобы создать новый общий ресурс синхронизации, щелкните правой кнопкой мыши в окне Work Folders и выберите в контекстном меню пункт New Sync Share (Создать общий ресурс синхронизации) или выберите пункт New Sync Share в раскрывающемся меню Tasks (Задачи). Откроется мастер создания общего ресурса синхронизации (New Sync Share Wizard), который проведет вас через соответствующий процесс.

1. На экране Server and Path (Сервер и путь) отобразятся все серверы, которые были добавлены в управляющую панель диспетчера серверов с включенной функцией Work Folders. Вы можете выбрать общий ресурс, существующий на одном из серверов, или указать локальный путь. Введите локальный путь **`D:\ITSyncShare`**, как показано на рис. 26.42, и щелкните на кнопке Next (Далее).

   На открывшемся экране User Folder Structure (Структура папок пользователя) предусмотрено два переключателя — User alias (Псевдоним пользователя), выбранный по умолчанию, и User alias@domain (Псевдоним пользователя@домен), как показано на рис. 26.43. Выбор переключателя User alias приведет к созданию пользовательских папок, как вы делали это с перенаправлением папок и домашними папками. Выбор переключателя User alias@domain обеспечит присоединение к имени папки конструкции `@домен` каждой учетной записи, что полезно при наличии множества доменов с потенциально конфликтующими между собой именами. У вас также есть возможность выбрать определенную папку для синхронизации, пропуская все остальные, которые находятся в общем ресурсе. Это может быть удобно при перенаправлении папок, поскольку появляется возможность синхронизировать папку `Documents`, не затрагивая остальные перенаправляемые папки.
2. На данном этапе просто примите стандартные настройки.
3. На экране Sync Share Name (Имя общего ресурса синхронизации) вы можете переименовать данный общий ресурс и предоставить его описание. Описание является необязательным, однако через полгода или год, когда вы попытаетесь вспомнить, для чего использовалась та или иная папка синхронизации, оно может оказаться весьма кстати.

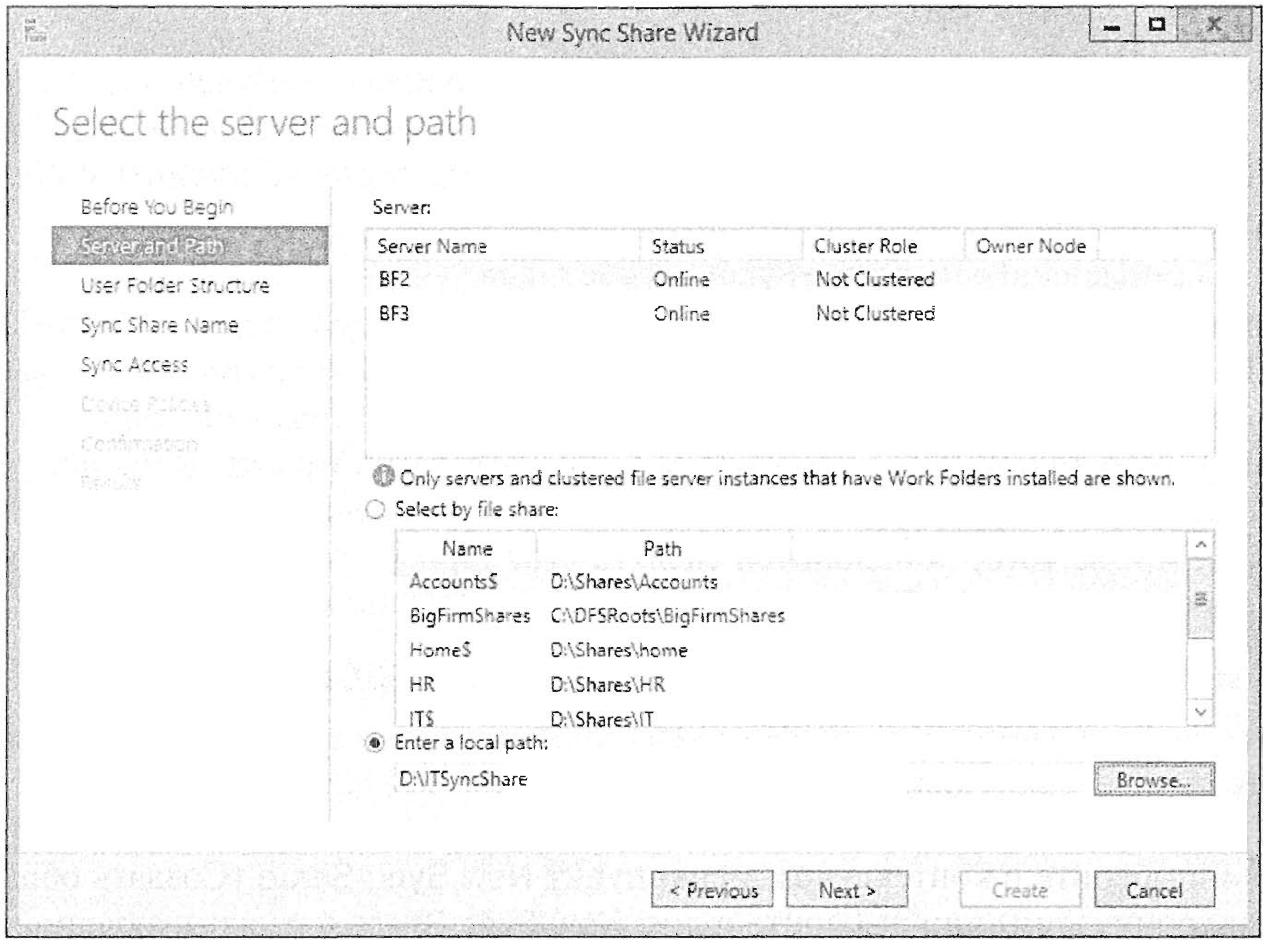


Рис. 26.42. Окно мастера New Sync Share Wizard — экран Server and Path

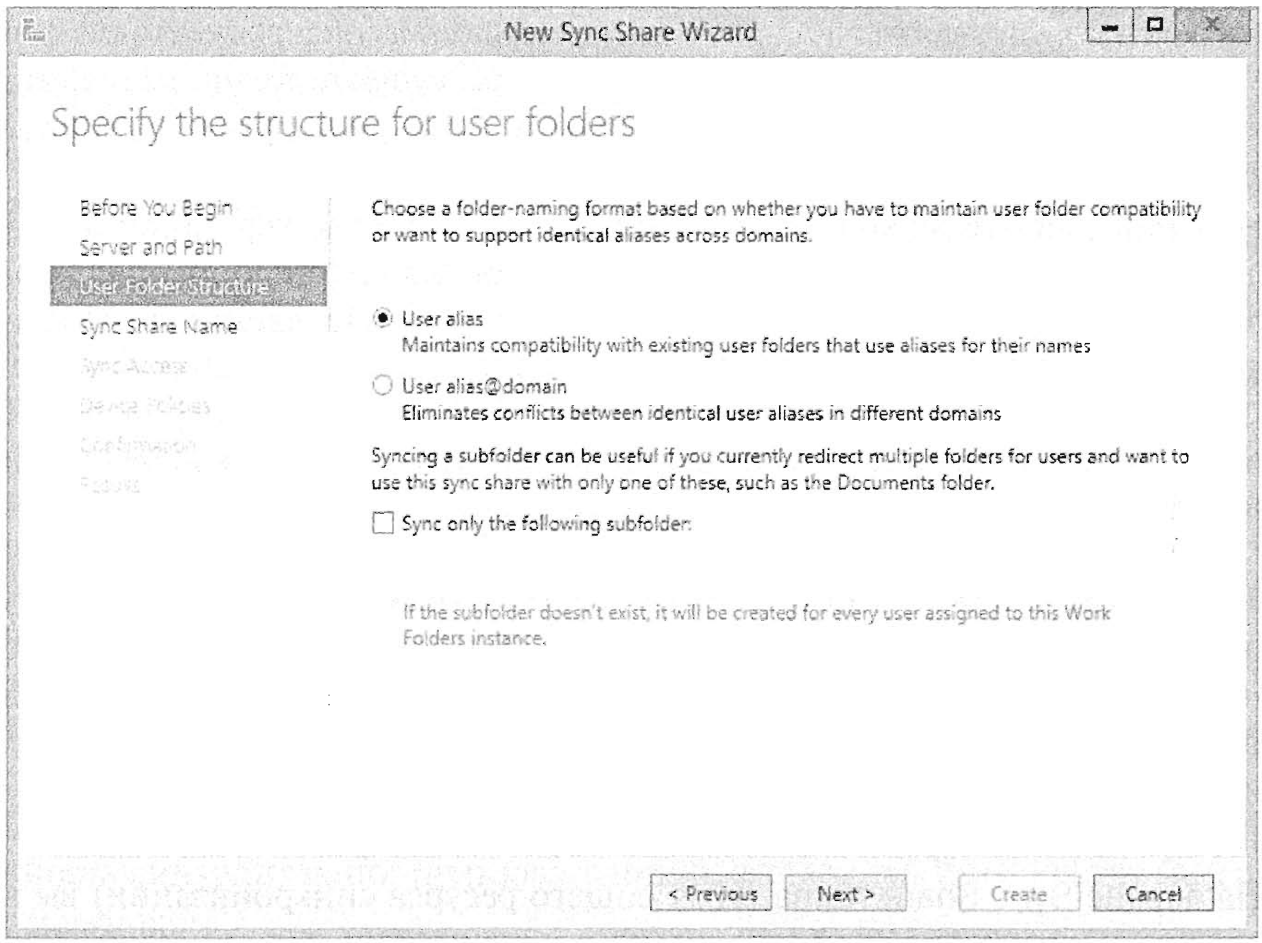


Рис. 26.43. Окно мастера New Sync Share Wizard — экран User Folder Structure

4. Следующий экран, Sync Access (Доступ к общему ресурсу синхронизации), позволяет предоставлять доступ к данному общему ресурсу. Это можно делать на основе пользователей или групп доступа. Щелкните на кнопке Add (Добавить) и выберите группу IT Administrators (Администраторы IT). По умолчанию администраторы не будут иметь доступ к пользовательским данным на сервере; если же вы хотите выдать администраторам доступ к этим данным, снимите отметку с флажка Disable inherited permissions (Отключить унаследованные разрешения).

   На экране Device Policy (Политика устройства) можно ввести в действие политики на устройстве, с которым будут синхронизироваться данные.

5. Отметьте оба флажка и перейдите к следующему шагу.
6. Пересмотрите выбранные настройки и затем создайте общий ресурс.

Теперь на экране Work Folders будет отображаться только что созданный общий ресурс, пользователи, имеющие к нему доступ, информация о томе, а также любые квоты, которые были определены для пользователей (рис. 26.44).

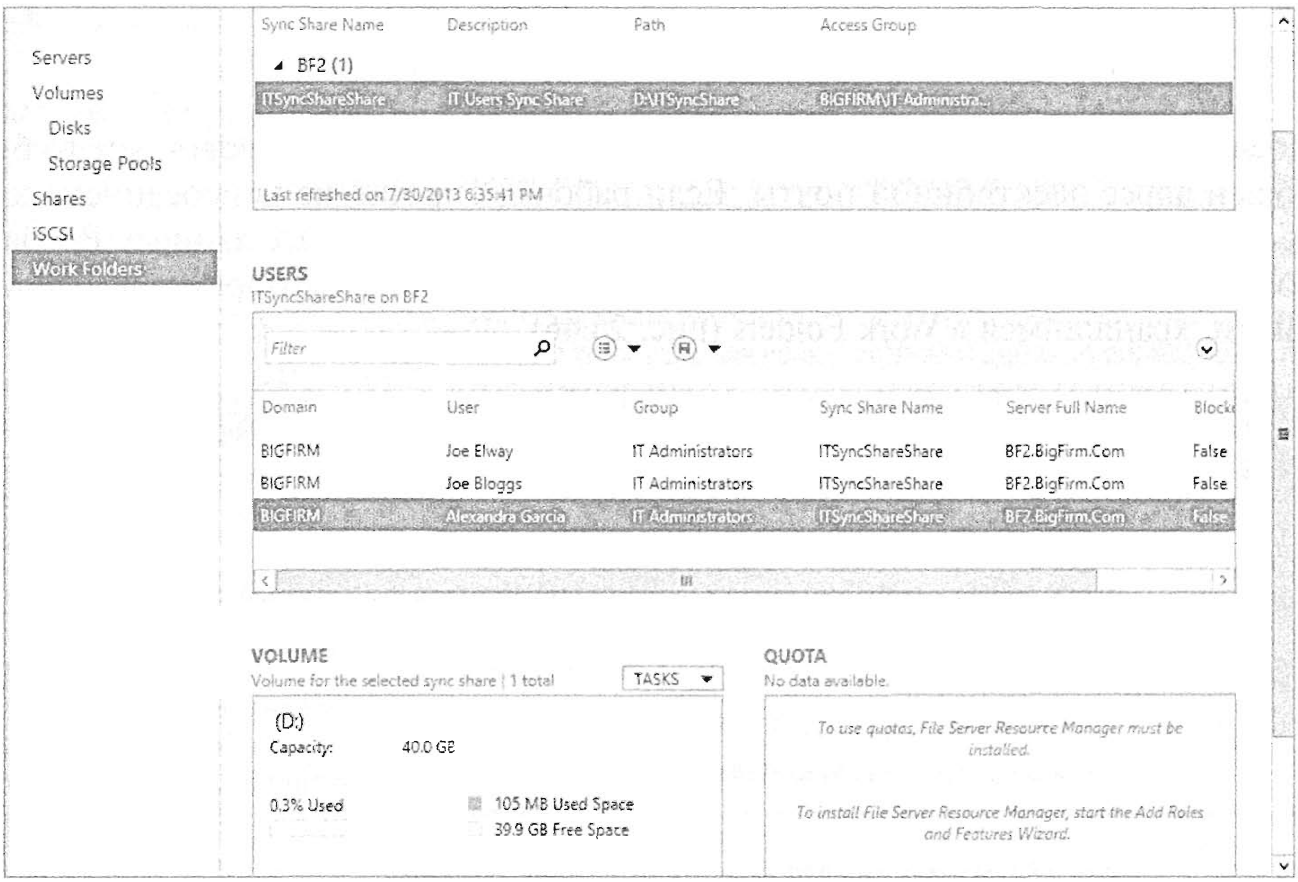


Рис. 26.44. Конфигурация Work Folders завершена

Вот и все! Серверная сторона сконфигурирована и готова к тому, чтобы пользователи начали синхронизировать свои файлы. В качестве альтернативы средство Work Folders можно было бы сконфигурировать с применением следующей команды PowerShell:

```
PS C:\> New-SyncShare ITSyncShare -path D:\ITSyncShare
          -User "BigFirm\IT Administrators"
          -RequireEncryption $true
          -RequirePasswordAutoLock $true
```

Конфигурирование клиентов

Теперь, когда сервер сконфигурирован, клиентам понадобится знать, к чему подключаться, и согласиться с настройками устройств, которые будут применяться для запуска синхронизации файлов.

Пользователи могут сконфигурировать свои настройки Work Folders, выбрав в панели управления элемент System and Security⇨Work Folders (Система и безопасность⇨Рабочие папки). Здесь находится ссылка Set up Work Folders (Настроить рабочие папки), как показано на рис. 26.45.

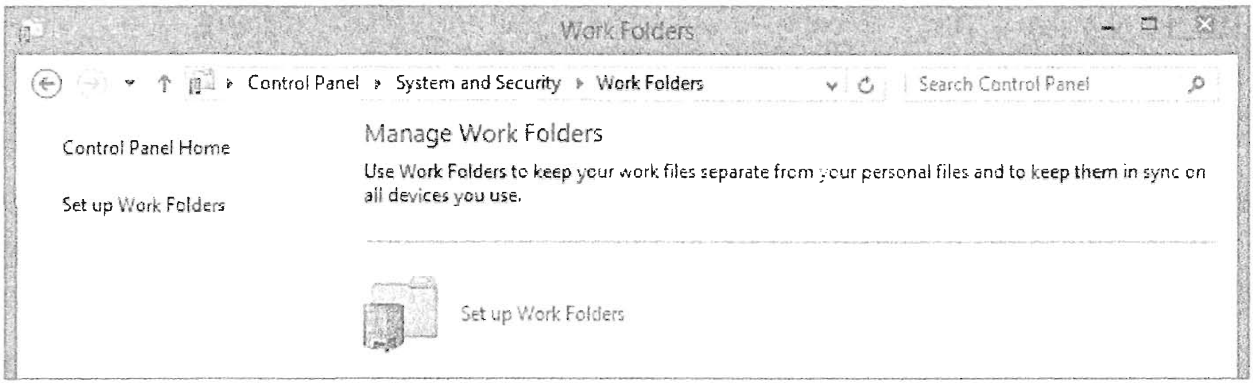


Рис. 26.45. Управление рабочими папками

После того как пользователь щелкнет на ссылке Set up Work Folders, у него будет запрошен адрес электронной почты. Если рабочая станция не присоединена к домену, пользователю будет предложено ввести доменные учетные данные. Вдобавок пользователю необходимо согласиться с политиками данных, которые применяются к файлам, хранящимся в Work Folders (рис. 26.46).

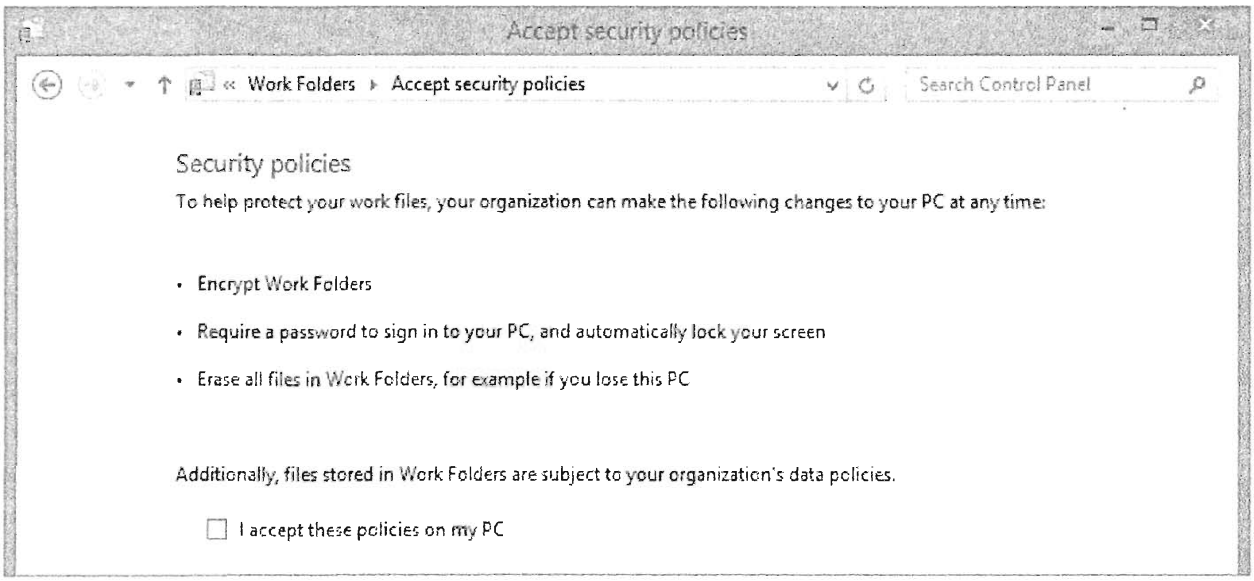


Рис. 26.46. Политики безопасности

После согласия с политиками производится установка Work Folders. Пользователь сможет просматривать свои настройки синхронизации в панели управления Work Folders, а значок Work Folders отображается в узле My Computer/This PC (Мой компьютер/Этот ПК), как показано на рис. 26.47. Заставлять всех пользователей конфигурировать собственные настройки Work Folders нецелесообразно, поэтому такие настройки можно также сконфигурировать посредством групповой политики.

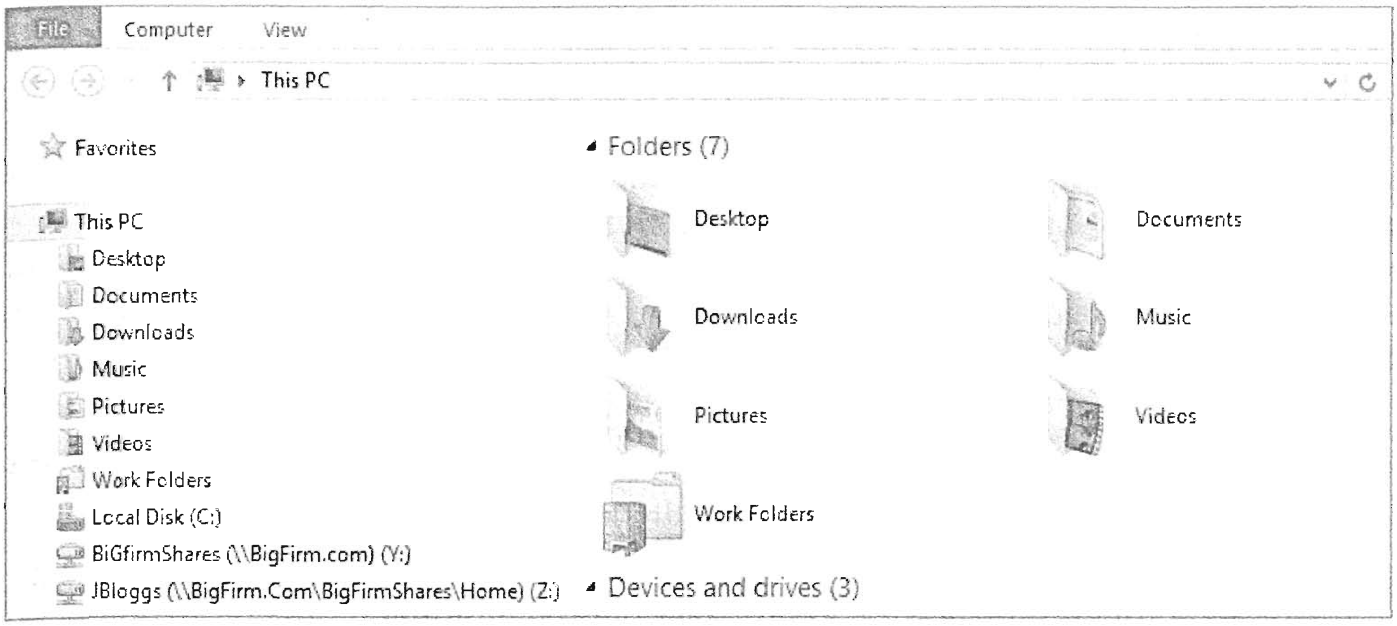


Рис. 26.47. Панель управления Work Folders

В табл. 26.7 представлены две политики, которые управляют настройками Work Folders.

Таблица 26.7. Управление Work Folders с помощью групповой политики

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ Windows Components \ Work Folders (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Рабочие папки)	Force automatic setup for all users (Инициировать автоматическую установку для всех пользователей)	Эта политика принудительно задает конфигурацию Work Folders для всех пользователей. Никакие настройки здесь не определены, поэтому данная политика должна использоваться наряду с политикой Specify Work Folders settings, специфичной для пользователей
User Configuration \ Administrative Templates \ Windows Components \ Work Folders (Конфигурация пользователя \ Административные шаблоны \ Компоненты Windows \ Рабочие папки)	Specify Work Folders settings (Указать настройки Work Folders)	Эта политика определяет, к какому серверу Work Folders должны подключаться пользователи

Средство Work Folders легко настраивать и можно комбинировать с другими технологиями, такими как Workplace Join и RMS Protection. Совместное применение этих возможностей поможет вам защитить свои данные, одновременно обеспечивая для пользователей гибкость использования устройств, с которыми им нравится работать.

На момент написания этой книги средство Work Folders было ограничено синхронизацией устройств Windows 8.1, но ожидается, что вскоре Work Folders расширит свою функциональность на Windows 7 и Windows 8. Не удивляйтесь, если после выхода пары версий Work Folders станет стандартом для синхронизации пользовательских данных.

Управление рабочим столом с помощью групповой политики

Обязательные профили позволяют администраторам предоставлять пользователям согласованную рабочую среду, когда они входят в систему. Никакие изменения не могут быть сохранены. Однако что, если вы вообще не хотите разрешать пользователям вносить любые изменения? Обязательные профили нельзя рассматривать как решение по защите, т.к. они не препятствуют пользователям делать все, что им вздумается. Рассмотрим следующие сценарии:

- сервер Remote Desktop, на котором вы хотите ограничить пользователей возможностью запуска только определенных программ;
- информационный киоск, на котором может выполняться только одна программа и отсутствует другое взаимодействие с системой;
- ПК в организации с высокими требованиями к безопасности и управлению, где администраторы обязаны следить за тем, что может делать пользователь.

Все проблемы подобного рода требуют решения, которое препятствовало бы внесению пользователем каких-либо изменений. Очевидно, что обязательные профили не позволяют обеспечить полноценное решение.

ОС Windows предоставляет возможность заблокировать рабочий стол путем редактирования реестра. Администраторам предоставляется широкий спектр возможностей, в частности:

- ограничение того, что находится в меню Start (Пуск);
- запрет просмотра содержимого диска C;
- ограничение доступа к панели управления.

Возможно, вы не желаете развертывать решение по защите, используя редактирование реестра, т.к. это влечет за собой непомерный объем работ. К счастью, в административные шаблоны Windows Server 2012 включен набор встроенных настроек групповой политики. С их помощью можно сконфигурировать групповую политику для пользователей и/или компьютеров, которые необходимо защитить. Мы кратко рассмотрим *несколько* таких настроек, с помощью которых можно ограничить ваши компьютеры или серверы Remote Desktop. Доступно *намного* больше настроек, но здесь будут описаны лишь те из них, которые на начальном этапе могут оказаться важнее других.

Настройки в Computer Configuration \ Administrative Templates \ Network \ Offline Files (Конфигурация компьютера \ Административные шаблоны \ Сеть \ Автономные файлы) позволяют управлять автономными файлами на основе индивидуальных систем; т.е. применяемые здесь параметры будут оказывать влияние на всех пользователей, которые входят в системы целевых компьютеров (табл. 26.8).

В Computer Configuration\Administrative Templates\Windows Components\Internet Explorer (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Internet Explorer) содержится вложенный набор настроек GPO, позволяющих управлять тем, как пользователь может работать с Internet Explorer на компьютере (табл. 26.9).

Таблица 26.8. Конфигурация компьютера: автономные файлы

Настройка	Описание
At logoff, delete the local copy of user's offline files (При выходе из системы удалять локальную копию автономных файлов пользователя)	Используйте эту настройку, если вы решили, что при выходе пользователя из системы все автономные файлы должны быть удалены из компьютера
Encrypt the offline files cache (Шифровать кеш автономных файлов)	Если данные на компьютере не зашифрованы, то они уязвимы при атаках. Включение этой настройки обеспечивает защиту кеша автономных файлов путем его принудительного шифрования. Пользователь не может отключить шифрование
Prohibit 'Make Available Offline' for these files and folders (Запретить пункт Make Available Offline (Сделать доступным автономно) меню File (Файл) для этих файлов и папок)	Вы можете указать папки, которые не должны делаться доступными автономно. Размещение определенной информации на переносных компьютерах связано с высоким риском: такая информация может быть похищена, если разрешить доступ к ней
Synchronize all offline files before logging on (Синхронизировать все автономные файлы перед входом в систему)	Все помеченные файлы и папки синхронизируются перед входом пользователя в систему. Это гарантирует, что изменения, внесенные пользователем во время его поездок с переносным компьютером, будут скопированы на файловый сервер
Synchronize all offline files before logging off (Синхронизировать все автономные файлы перед выходом из системы)	Это гарантирует, что у пользователя будет самая последняя копия всех файлов, когда он забирает свой переносной компьютер из офиса
Prohibit user configuration of offline files (Запретить конфигурацию пользователя для автономных файлов)	Пользователи часто являются причиной возникновения проблем на компьютерах. Вы можете сконфигурировать автономные файлы с помощью объекта GPO и запретить пользователям вмешательство в эту конфигурацию

Таблица 26.9. Конфигурация компьютера: Internet Explorer

Настройка	Описание
Disable automatic install of Internet Explorer components (Отключить автоматическую установку компонентов Internet Explorer)	По умолчанию пользователям предлагается загрузить компоненты Internet Explorer, когда веб-страница требует их. Воспользовавшись этой политикой, вы можете запретить такое поведение
Make proxy settings per machine (rather than per user) (Создать настройки прокси для каждого компьютера (а не для каждого пользователя))	Вы можете сконфигурировать настройки прокси для компьютера и принудительно применять эти параметры ко всем пользователям, вошедшим в систему
Security Zones: Do not allow users to add/delete sites (Зоны безопасности: не разрешать пользователям добавлять/удалять сайты)	Зона в Internet Explorer изменяет разрешения для сайтов в этой зоне, а также поведение Internet Explorer. Добавление или удаление сайтов в зону изменяет то, как Internet Explorer будет обрабатывать эти сайты. Включение этой настройки приводит к принудительному применению конфигурации каждой системы ко всем пользователям, чтобы предотвратить редактирование ими своего членства в зонах
Internet Control Panel\Disable the connections page (Панель управления Интернетом \ Отключить страницу подключений)	Это не позволяет пользователям изменять способ подключения Internet Explorer к Интернету, например, через настройки прокси

Несколько настроек для управления приложениями являются встроенными в Windows. Вам может потребоваться выполнить следующие действия:

- предварительно сконфигурировать приложения;
- заблокировать конфигурирование приложений;
- запретить доступ к приложениям.

Некоторые приложения, скажем, Microsoft Office, позволяют добавлять шаблоны для решения этих задач. Примером встроенного шаблона может служить программа мгновенного обмена сообщениями Windows Messenger (табл. 26.10), которой можно управлять на основе индивидуальных систем с помощью настроек в Computer Configuration\Administrative Templates\Windows Components\Windows Messenger (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Windows Messenger).

Таблица 26.10. Конфигурация компьютера: Windows Messenger

Настройка	Описание
Do not allow Windows Messenger to be run (Не разрешать запуск Windows Messenger)	Предотвращает запуск Windows Messenger системой Windows или пользователям
Do not automatically start Windows Messenger initially (Не запускать автоматически Windows Messenger)	Отключает стандартную настройку запуска Windows Messenger при входе пользователя в систему. Однако эта настройка может быть переопределена, если пользователь решил, что запуск Windows Messenger необходим

Мы представили лишь небольшую выборку инструментария, который доступен администратору для ограничения функциональности рабочего стола пользователя на основе отдельных систем. А теперь давайте посмотрим, что можно делать применительно к отдельным пользователям.

Одним из действий, которые вам, скорее всего, понадобится выполнить, является предварительное конфигурирование Internet Explorer. Вы можете делать это на базе пользователей, используя настройки в User Configuration \ Preferences \ Windows Settings \ Internet Explorer (Конфигурация пользователя \ Предпочтения \ Настройки Windows \ Internet Explorer), которые были описаны в табл. 26.9. Настройки Preferences заменили собой настройки Internet Explorer Maintenance (Поддержка Internet Explorer) и позволяют определять настройки, начиная с IE 5 и заканчивая самой последней версией этого браузера. Если же настройки Preferences не обеспечивают всей функциональности, которая требуется вашей среде, можете настроить Internet Explorer с помощью пакета администрирования Internet Explorer (Internet Explorer Administration Kit — IEAK). Дополнительные сведения о пакете IEAK доступны по ссылке `https://technet.microsoft.com/ru-ru/ie/bb219517.aspx`.

Панель управления является одним из тех мест, где пользователь реально способен создать себе проблемы. Вы можете лишить пользователя возможности доступа к компонентам панели управления или даже не позволить ему открывать саму панель управления (табл. 26.11). Все это управляется настройками в User Configuration \ Administrative Templates \ Control Panel (Конфигурация пользователя \ Административные шаблоны \ Панель управления).

Таблица 26.11. Конфигурация пользователя: панель управления

Настройка	Описание
Hide specified Control Panel items (Скрывать указанные элементы панели управления)	Вы можете перечислить конкретные модули в панели управления, которые должны быть сделаны недоступными для пользователя
Show only specified Control Panel items (Отображать только указанные элементы панели управления)	Иногда легче предоставить список элементов, которые должны отображаться в панели управления, чем перечислять множество элементов, подлежащих сокрытию. Эта настройка разрешает пользователю обращаться лишь к элементам, перечисленным в списке
Prohibit access to Control Panel (Запретить доступ к панели управления)	Вы можете лишить пользователя возможности видеть либо использовать панель управления
Personalization \ Force specific screen saver (Персонализация \ Вызывать определенный хранитель экрана)	Эта настойка заставляет пользователя выбирать определенный хранитель экрана
Personalization \ Screen saver time-out (Персонализация \ Тайм-аут хранителя экрана)	Эта настойка конфигурирует время, через которое появляется хранитель экрана; другими словами, он будет активизирован через *x* секунд бездействия
Personalization \ Enable screen saver (Персонализация \ Включить хранитель экрана)	Эта настойка включает хранитель экрана. Она требует конфигурирования двух предшествующих настроек
Personalization \ Password protect the screen saver (Персонализация \ Защитить паролем хранитель экрана)	Эта настойка заставляет пользователя вводить свой пароль, чтобы разблокировать хранитель экрана

Пример из практики

Будьте внимательны при защите хранителя экрана

Соблюдайте осторожность во время применения таких политик, как конфигурация хранителя экрана. С точки зрения безопасности рекомендуется включать хранитель экрана для всех пользователей и требовать ввода пароля для его разблокирования. По опыту те, кто в наибольшей степени нуждаются в защите подобного рода, больше всего ее и недолюбливают. Начальники отделов и персонал, занимающийся продажами, терпеть не могут такие вещи, как хранители экрана с разблокировкой посредством пароля. Вы должны найти разумный компромисс между IT-безопасностью и гарантией своей занятости; неплохо получить рекомендации по этим вопросам от вашего работодателя, предварительно ознакомив его с передовым опытом в области безопасности. Лишь после этого можно приступать к внедрению выбранных вами политик.

В большинстве развертываний объектов GPO функциональность проводника файлов в определенной степени ограничена. Проводник файлов можно сконфигурировать с помощью настроек в User Configuration \ Administrative Templates \ Windows Components \ File Explorer (Конфигурация пользователя \ Административные шаблоны \ Компоненты Windows \ Проводник файлов), кратко описанных в табл. 26.12.

Таблица 26.12. Конфигурация пользователя: проводник файлов

Настройка	Описание
Do not track shell shortcuts during roaming (Не отслеживать ярлыки оболочки во время роуминга)	Эта настройка блокирует компьютер от попыток обратного отслеживания исходной удаленной цели ярлыка, если найти локальную цель не удается
Remove CD burning features (Удалить средства прожига компакт-дисков)	Проводник файлов включает способность создавать компакт-диски. С помощью этой настройки эту возможность можно отключить
Hide these specified drives in My Computer (Скрыть указанные диски в "Мой компьютер")	Вы можете скрыть в проводнике файлов определенную комбинацию локальных дисков или все диски компьютера. Это не ограничивает доступ к ресурсам на дисках (например, к программам). Обойти такое ограничение можно за счет использования других инструментов вместо проводника
Prevent access to drives from My Computer (Запретить доступ к дискам из "Мой компьютер")	Вы можете предотвратить доступ к определенной комбинации локальных дисков или ко всем дискам компьютера посредством проводника файлов. Это не ограничивает доступ к ресурсам на этих дисках; установленные на них программы по-прежнему можно запускать посредством обычных ярлыков. Обойти такое ограничение можно за счет использования других инструментов вместо проводника

Как видите, для конфигурирования на основе отдельных пользователей доступны многие настройки. Скорее всего, вы будете использовать смесь конфигураций на базе пользователей и на базе систем. Например, с помощью политик конфигурации компьютера можно эффективно ограничить функциональность организационной единицы, содержащей информационные киоски Windows. План открытого офиса, включающий систему работы за одним компьютером нескольких сотрудников в разное время, вероятно, будет в большей степени полагаться на применение политик конфигурации пользователя. Причина в том, что политика на основе системы не подойдет широкому разнообразию пользователей, которые могут работать на одном и тем же компьютере. В таком случае лучше конфигурировать пользователей, а не компьютеры.

От того, какой метод вы используете для тестирования и выработки политики ограничения функциональности, зависит успех развертывания и легкость управления. Вы ознакомились только с совсем небольшим подмножеством доступных настроек. В Windows Server 2012 их предусмотрено очень много. Кроме того, дополнительные параметры можно добавлять через шаблоны для приложений, например, Microsoft Office. Вы можете также реализовать специальные шаблоны, внося желаемые изменения в существующие шаблоны самостоятельно или применяя утилиты сторонних разработчиков.

Мы рекомендуем построить испытательную среду, идентичную производственной сети, если вы можете себе позволить подобное. Это может быть виртуальной сетью, которая предоставит вам возможность развернуть Hyper-V. Формирование ваших политик должно представлять собой постепенный и целенаправленный процесс. Добавляйте по одному параметру политики за раз. Лишь в таком случае вы сможете увидеть, в чем заключается подлинный эффект от политики. Если же вы за раз реализуете несколько политик, то каким образом сможете понять, какая из них

вызвала проблему? Вы должны проводить тестирование, чтобы оценить применение политики, например, при каждом входе в систему, после второго входа или во время обычного обновления политик. Мы рекомендуем входить в систему несколько раз, поскольку нам встречались довольно сложные сценарии, при которых реализация политики была несогласованной. Чтобы документировать политики, завершив их создание, и экспортировать их для внедрения в производственной сети, можете использовать консоль управления групповыми политиками (Group Policy Management Console).

Управление пользователями с помощью предпочтений групповой политики и сценариев входа

До сих пор в этой главе вы видели, как устанавливать для пользователя такие сетевые ресурсы, как профиль, домашний каталог и перенаправляемые папки. В сети имеются и другие ресурсы наподобие общих файловых ресурсов, пространств имен DFS и принтеров. Как подключить к ним пользователя? Более традиционное решение предусматривает применение сценариев входа, которые выполняются каждый раз, когда пользователь входит в систему, чтобы отображать диски, использовать принтеры и вносить изменения в реестр. Однако существует более эффективный метод — предпочтения групповой политики (Group Policy Preferences), которые позволяют делать все то, для чего обычно применяются сценарии, но с более высокой степенью контроля и быстрой обработкой. Они являются предпочтительным методом для управления настройками пользователей в Windows Server 2012.

Управление отображениями дисков

Одна из самых типичных задач, которые приходится решать сетевому администратору, связана с управлением отображениями дисков для разных пользователей и отделов. Традиционно для этого использовались сценарии входа, однако они могут стать довольно сложными и требовать большего времени на тестирование и отладку. Предпочтения групповой политики устраняют многие из этих проблем и облегчают привязку отображений дисков к группам доступа посредством целевого уровня элемента.

Ранее в этой главе мы развернули пространство имен DFS под названием `\\bigfirm.com\BigFirmShares`, представленное на рис. 26.48. После этого мы добавили несколько общих файловых ресурсов, чтобы позволить пользователям работать друг с другом на основе команды или отдела. Предположим, что вы хотите автоматически отображать указанное пространство имен для всех пользователей группы `Senior Management` (Старшее руководство) как диск Y на их компьютерах. Это означает, что все члены данной группы будут просматривать все общие файловые ресурсы с применением единственной буквы диска.

В главе 9 уже раскрывались основы создания и привязки объектов GPO, поэтому сейчас мы перейдем непосредственно к сути предпочтений отображений дисков. В только что созданной групповой политике `Drive Mappings` выберите элемент предпочтения Drive Maps (Отображения дисков) и создайте новое отображение.

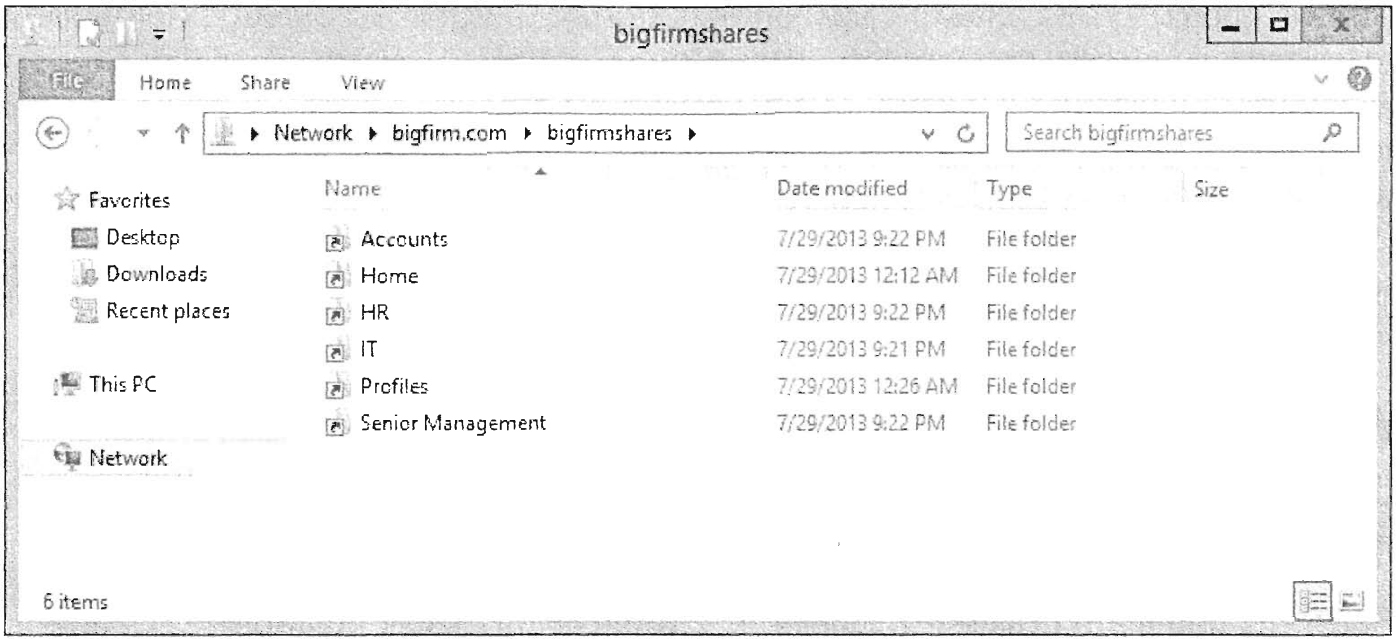


Рис. 26.48. Пространство имен DFS для BigFirm

Прежде всего, вам предлагается выбрать действие, которое должно выполнять отображение диска. Как показано в табл. 26.13, в вашем распоряжении имеются четыре варианта. Полезно также отметить, что эти же четыре действия будут появляться в большинстве предпочтений групповой политики.

Таблица 26.13. Действия отображения дисков

Действие	Описание
Create (Создать)	Это действие создаст новое отображение диска, если оно еще не существует. При наличии отображения с такой буквой диска ничего не предпринимается
Replace (Заменить)	Удаляет существующий отображенный диск и создает новый
Update (Обновить)	Изменяет параметры существующего отображенного диска. Если отображенного диска нет, будет создан новый такой диск
Delete (Удалить)	Удаляет отображенный диск

В открывшемся диалоговом окне New Drive Properties (Свойства нового диска) мы собираемся выбрать действие Replace, поскольку хотим обеспечить, чтобы диск был отображен на наш общий файловый ресурс DFS как Y. Затем понадобится ввести местоположение общих файловых ресурсов DFS и установить букву диска в Y, как показано на рис. 26.49.

Далее необходимо позаботиться о том, чтобы это отображение диска получили только члены группы `Senior Management`. Для этого вы будете применять нацеливание на уровне элементов. Во все еще открытом диалоговом окне New Drive Properties перейдите на вкладку Common (Общие), выберите переключатель Item-level targeting (Целевой уровень элемента) и щелкните на кнопке Targeting (Целевой объект). Как показано на рис. 26.50, вы можете выбрать множество вариантов для применения этого предпочтения, начиная с доступного типа подключения к сети и заканчивая временем суток. В нашем сценарии мы выберем вариант Security Group (Группа доступа), укажем группу `BigFirm\Senior Management` и привяжем данную групповую политику к корню BigFirm.

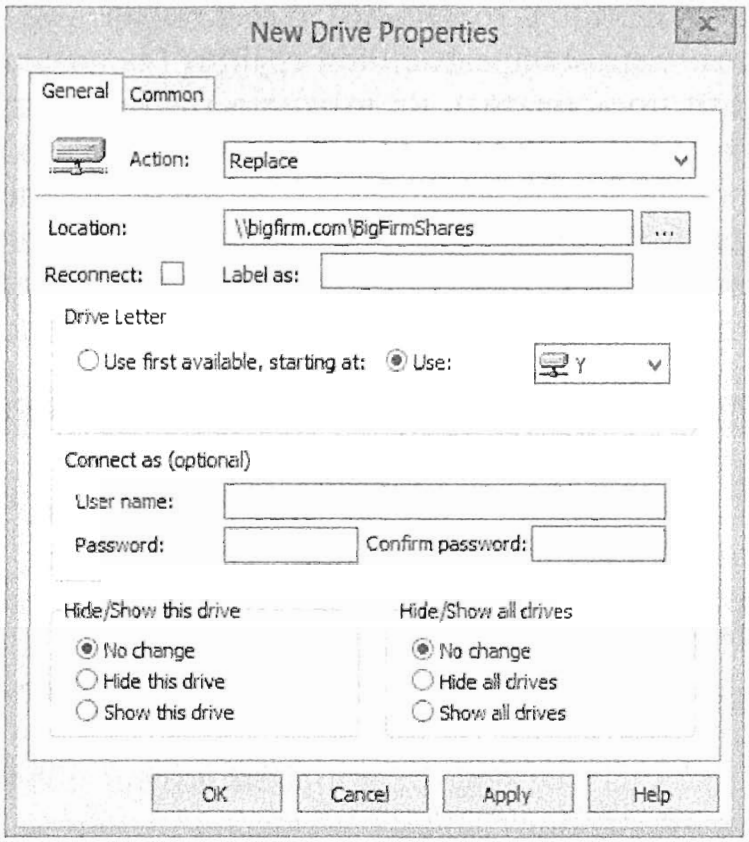


Рис. 26.49. Свойства нового диска

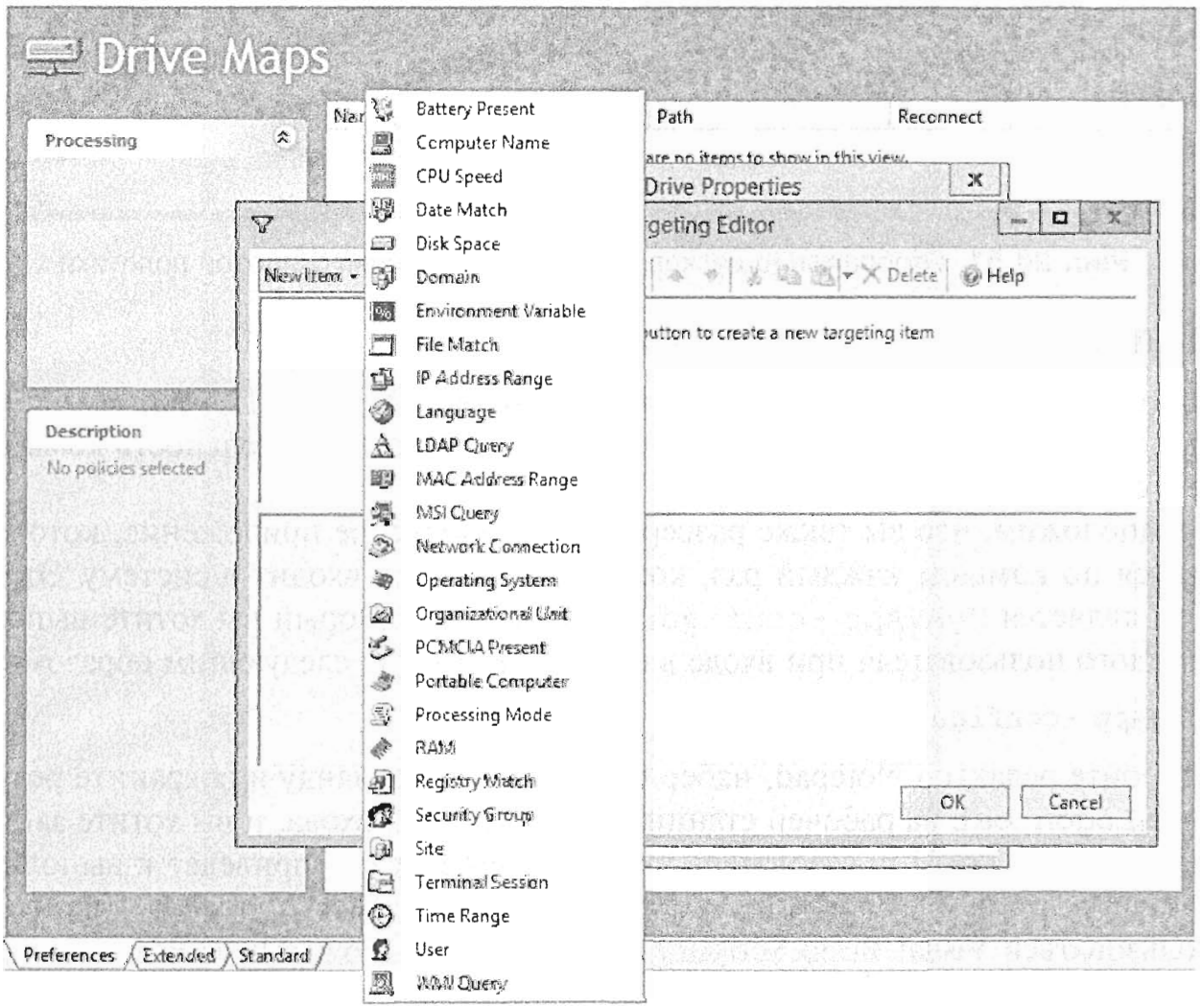


Рис. 26.50. Варианты целевых объектов

Целевой уровень элемента не только позволяет выбрать условие вроде того, что пользователь является членом определенной группы (включающее), но также применять политику, если пользователь не входит в группу доступа (исключающее). У вас есть возможность комбинировать условия, например, что пользователь является членом группы доступа и вдобавок у него установлено определенное приложение.

Как видно на рис. 26.51, когда вы входите в систему как один из тестовых пользователей в группе `Senior Managers`, этот пользователь наследует объект групповой политики, а предпочтение отображения диска Y применено.

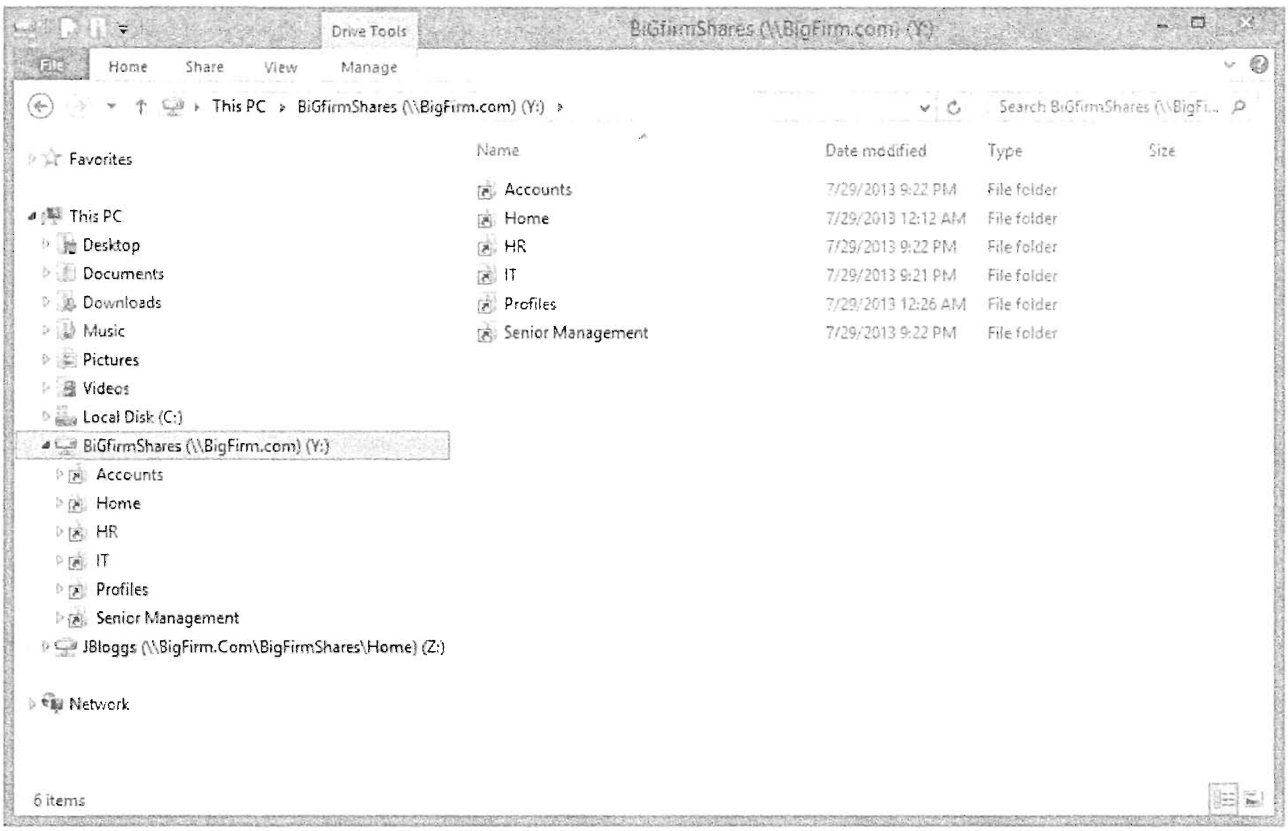


Рис. 26.51. Отображение дисков через предпочтения групповой политики

Выполнение команд при входе

Сценариям входа нашлось место и в мире Windows Server 2012. Они по-прежнему очень полезны, например, когда нужно выполнить последовательность команд при входе в систему.

Предположим, что вы также развернули антивирусное приложение, которое запускается по команде каждый раз, когда пользователь входит в систему. Этой командой является `MyAVApp -configure`. Сценарий, который вы хотите выполнять для каждого пользователя при входе в систему, выглядит следующим образом:

```
MyAVApp -configure
```

Откройте редактор Notepad, наберите указанную команду и сохраните результат в файле **`Logon.bat`** на рабочей станции. Это сценарий входа, и вы хотите запускать его каждый раз, когда пользователь входит в систему, что приведет к выполнению содержащихся в нем команд при входе пользователя. Вместо этого можно было бы воспользоваться Visual Basic Scripting (VBScript) или PowerShell. Вам необходимо сделать этот сценарий входа доступным всем пользователям в домене во всех местах, где они могут входить. К счастью, на каждом контроллере домена есть общий

ресурс, который является частью Active Directory и, следовательно, реплицируется. Этот общий ресурс называется NETLOGON; его можно найти в `\\bigfirm.com\SYSVOL\bigfirm.com\scripts`, а также в `\\bigfirm.com\Netlogon`. Его также можно обнаружить на каждом контроллере домена в `\\<имя_сервера>\NETLOGON`, например, `\\bf1\NETLOGON`. Скопируйте туда все свои сценарии входа.

При наличии крупного домен и множества сценариев входа вам следует подумать об именах для сценариев. Стандарт именования, который описывает роль сценария и указывает, кто с ним ассоциирован, упростит отслеживание этого сценария.

Вы должны решить, как этот сценарий входа будет привязан к пользователям. Это можно сделать несколькими способами.

Простейший способ предусматривает определение сценария входа на основе индивидуальных пользователей, как показано на рис. 26.52. Поле Logon script (Сценарий входа) в диалоговом окне свойств объекта пользователя позволяет указать сценарий, который находится внутри общего ресурса NETLOGON на контроллерах домена. Сценарий входа *должен* содержаться в NETLOGON.

Этот метод хорош при небольшом количестве пользователей или при наличии у них уникальных сценариев. Однако если нужно конфигурировать большое число пользователей, потребуется другой механизм.

Гораздо более эффективным способом конфигурирования сценария входа для пользователей является применение объектов GPO.

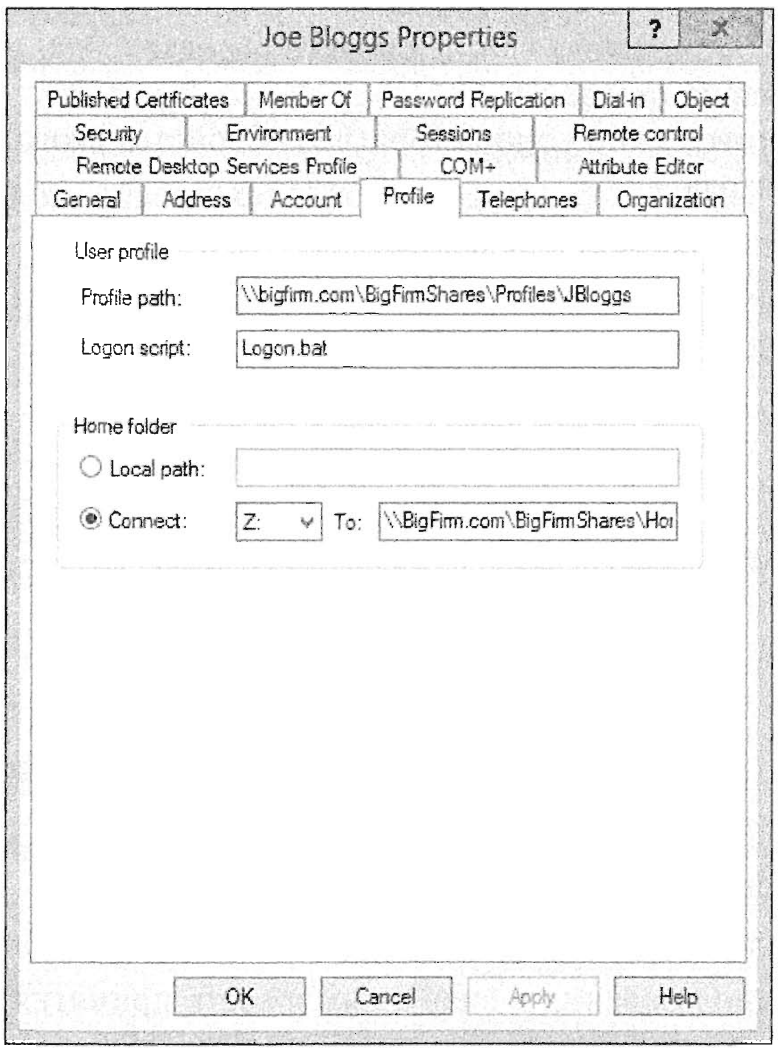


Рис. 26.52. Конфигурирование атрибута Logon script для объекта пользователя

Ниже перечислены преимущества этого подхода.

- Один объект GPO можно применять ко многим пользователям.
- Объект GPO можно привязать к организационной единице; т.е. сценарий входа можно связать с единицей логической структуры организации.
- Объект GPO можно привязать к сайту Active Directory; т.е. сценарий входа можно связать с единицей физической структуры организации. Например, возможно, что определенные действия должны выполняться, когда пользователь входит в специфичные локальные сети внутри сайта.
- Вы можете использовать обработку политики с обратной связью, чтобы ассоциировать с пользователем отличающийся сценарий входа, когда он входит в систему определенных компьютеров.

Создайте и привяжите объект GPO, после чего откройте его для редактирования. Перейдите к узлу \User Configuration \ Windows Settings \ Scripts (Logon/Logoff) (\ Конфигурация пользователя \ Настройки Windows \ Сценарии (входа/выхода)).

Этот метод трудно назвать более эффективным. В некоторых организациях выбирали вариант с конфигурацией на базе отдельных пользователей. Они обосновывали это тем, что каждый пользователь должен иметь уникальный сценарий входа. Тем не менее, такое обоснование легко свести на нет благодаря возможности использования в сценариях входа организационных единиц, групп доступа и средств принятия решений. Теперь развернем сценарий с применением GPO. Дважды щелкните на элементе Logon (Вход) в окне свойств объекта GPO, чтобы отредактировать настройки сценария входа.

Откроется диалоговое окно Logon Properties (Свойства входа), в котором можно добавить сценарий входа.

1. Щелкните на кнопке Add (Добавить).

   Это приведет к открытию диалогового окна Add a Script (Добавление сценария), показанного на рис. 26.53.

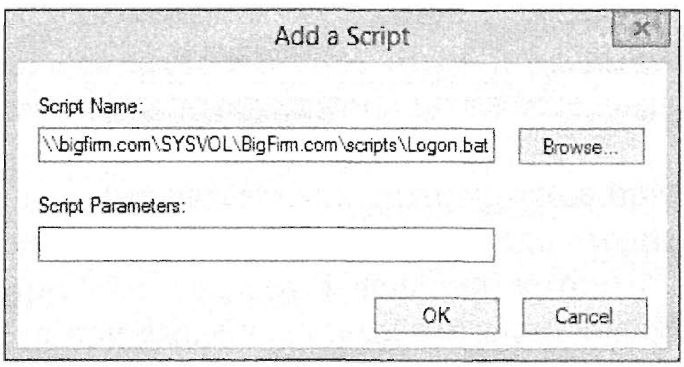


Рис. 26.53. Указание сценария входа

2. Выберите определенный сценарий входа.
3. Введите в сценарий входа параметры, которые будут изменять его поведение.

   Это пример использования в сценариях средств принятия решений, что позволяет сократить количество сценариев, которые необходимо реализовать.

4. Щелкните на кнопке Browse (Обзор), чтобы открыть мастер, который позволит выбрать существующий сценарий входа.

Стандартным местоположением, выбранным мастером, является папка (\User\Scripts\Logon), где содержится редактируемый объект GPO. Если не редактировать объект GPO, то найти эту папку нелегко. Именно по этой причине мы не рекомендуем помещать в нее сценарий входа. Тем не менее, данная папка доступна каждому пользователю как общий ресурс, поэтому вы могли бы воспользоваться этим стандартным местоположением для хранения своих сценариев входа в очень сложных развертываниях AD.

5. Перейдите в папку пространства имен DFS, которая представляет общий ресурс NETLOGON в вашем домене.

   Нашим доменом является bigfirm.com, так что папкой будет \\bigfirm.com\SYSVOL. Общий ресурс NETLOGON находится в папке \\bigfirm.com\SYSVOL\bigfirm.com\scripts. Здесь можно обнаружить сценарий входа, который был ранее скопирован в NETLOGON.

   Сценарий входа отобразится в диалоговом окне Add a Script.

6. Щелкните на кнопке OK в диалоговом окне Logon Properties, показанном на рис. 26.54. На этом процесс развертывания сценария входа посредством GPO завершен. Перед конфигурированием пользователей необходимо протестировать сценарий входа, войдя в систему и удостоверившись в выполнении команды.

Множество сценариев входа

Когда используется назначение групповой политики, с пользователем можно связать несколько сценариев входа. Каждый из этих сценариев будет выполняться при входе пользователя в систему.

На рис. 26.55 показано, где добавляются дополнительные сценарии входа в случае применения одного объекта GPO.

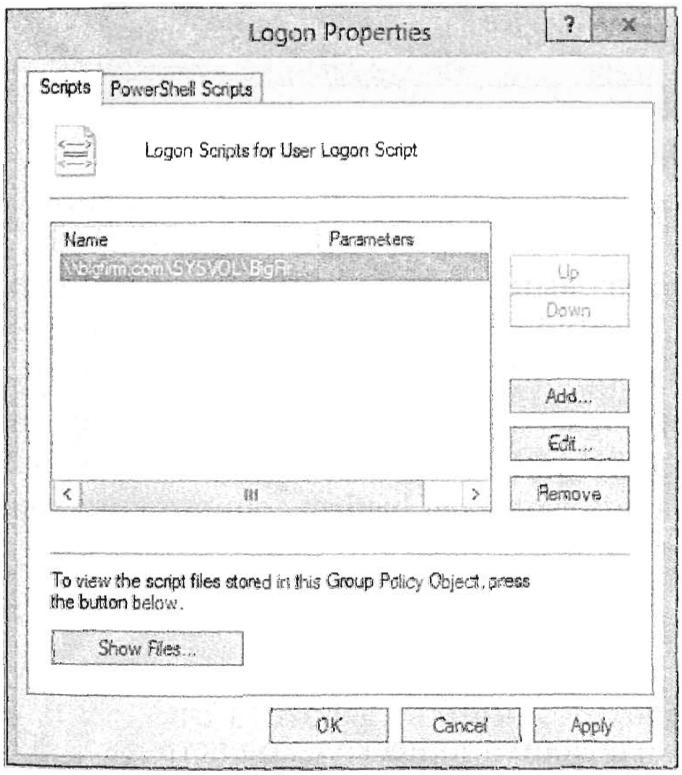


Рис. 26.54. Сценарий входа, сконфигурированный с применением групповой политики

Рис. 26.55. Конфигурирование нескольких сценариев входа с использованием групповой политики

С помощью кнопок Up (Вверх) и Down (Вниз) можно изменять порядок следования сценариев входа. Сценарий, находящийся в начале списка, будет выполнен первым.

Вы можете иметь дело со случаем, когда множество сценариев входа назначаются несколькими объектами GPO. На рис. 26.56 показан пример в окне Group Policy Results (Результаты групповой политики).

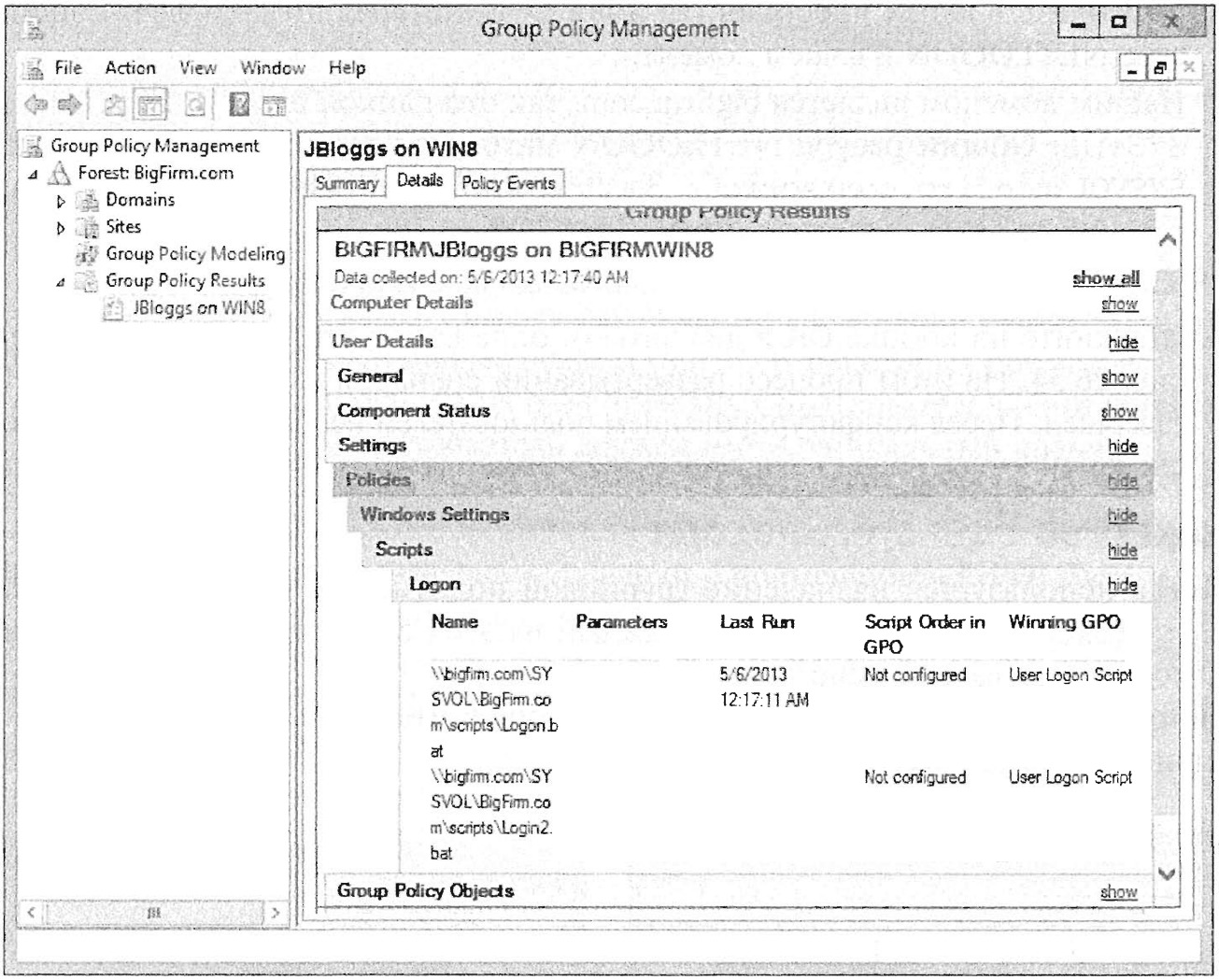


Рис. 26.56. Окно Group Policy Results, отображающее множество сценариев входа

Это пример, в котором один сценарий входа выполняет задачи, общие для всех пользователей домена bigfirm.com. Другой сценарий входа выполняет задачи для организационной единицы `Users`. Для членов организационной единицы `Users` будут запускаться оба сценария входа. Поддерживается обычная последовательность выполнения политики (сайт, домен, организационная единица, дочерняя организационная единица). В данном примере сценарий входа для bigfirm.com выполняется перед сценарием входа для `Users`.

Управление сценариями входа с помощью групповой политики

Для управления обработкой сценариев входа доступно несколько настроек GPO, которые перечислены в табл. 26.14. Это можно делать на основе отдельных систем или пользователей.

Таблица 26.14. Настройки GPO для сценариев входа

Путь	Политика	Описание
Computer Configuration \ Administrative Templates \ System \ Scripts (Конфигурация компьютера \ Административные шаблоны \ Система \ Сценарии)	Maximum wait time for Group Policy scripts (Максимальное время ожидания для сценариев групповой политики)	Этот параметр определяет количество секунд, которое механизм обработки групповой политики отводит на выполнение сценария, прежде чем процесс будет завершен. По умолчанию предусмотрено 600 секунд
Computer Configuration \ Administrative Templates \ System \ Scripts	Run logon scripts synchronously (Запускать сценарии входа синхронно)	Включение этой настройки заставляет проводник Windows ожидать до тех пор, пока не будут выполнены все сценарии входа, и только после этого пользователю будет разрешено выполнять какие-то действия
User Configuration \ Administrative Templates \ System \ Scripts	Run logon scripts visible (Запускать сценарии входа видимым образом)	По умолчанию пользователи не могут наблюдать за выполнением сценариев входа. Включение этой настройки позволяет пользователям следить за выполнением команд в окне
User Configuration \ Administrative Templates \ System \ Scripts (Конфигурация пользователя \ Административные шаблоны \ Система \ Сценарии)	Run Windows PowerShell scripts first at user logon, logoff (Запускать сценарии Windows PowerShell первыми при входе и выходе пользователя)	Сценарии PowerShell запускаются перед сценариями, не относящимися к PowerShell. Эту политику можно обратить. Для ее применения необходимо иметь, по меньшей мере, ОС Windows 7 или Windows Server 2008 R2
User Configuration \ Administrative Templates \ System \ Scripts	Run Windows PowerShell scripts first at computer startup, shutdown (Запускать сценарии Windows PowerShell первыми при запуске и выключении компьютера)	При запуске и выключении компьютера сценарии Windows PowerShell выполняются перед сценариями, не относящимися к PowerShell. Для ее применения необходимо иметь, по меньшей мере, ОС Windows 7 или Windows Server 2008 R2

Управление задачами отключения с помощью сценариев выхода

Поскольку с использованием групповой политики можно настраивать сценарии входа, вполне логично предположить наличие аналогичной возможности для сценариев выхода.

Сценарий выхода запускается каждый раз, когда пользователь выходит из системы. Это позволяет администраторам определять ряд задач, которые могут выполняться при каждом выходе пользователя из системы. Такие сценарии создаются идентично сценариям входа. Пример сконфигурированного сценария выхода показан на рис. 26.57.

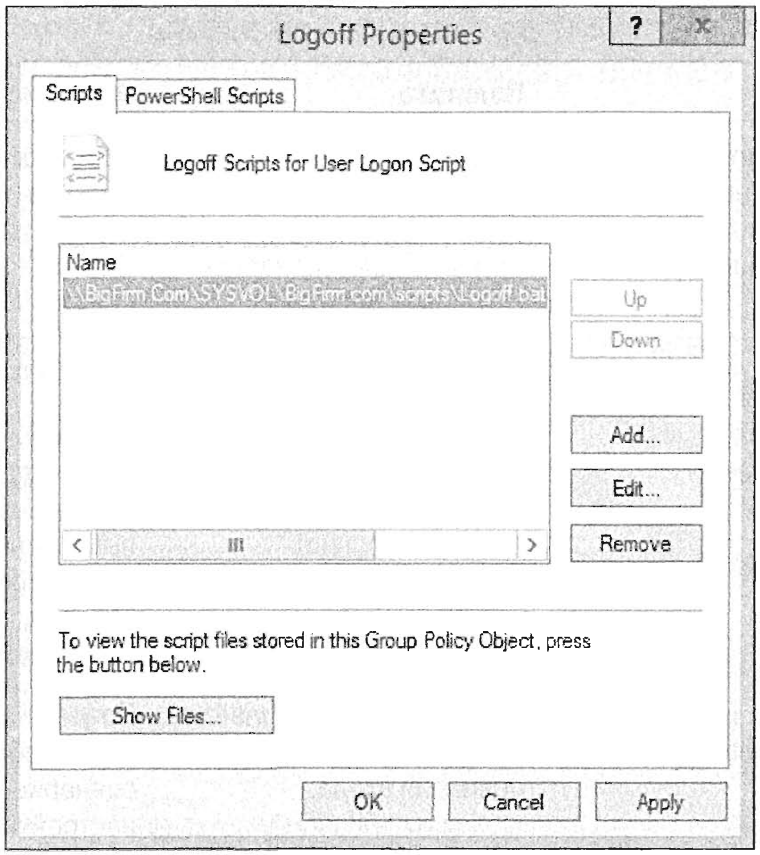


Рис. 26.57. Сценарий выхода, сконфигурированный с помощью групповой политики

Обратите внимание, что сценарий выхода не будет запускаться, если пользователь просто выключает свой ПК, не пройдя процедуру корректного завершения работы. Сценарий выхода также не выполняется, если пользователь переводит свой компьютер в режим сна или отключается от сеанса Remote Desktop Services.

Резюме

Разверните домашние каталоги для множества пользователей. Домашние каталоги позволяют пользователю иметь персональное хранилище информации на файловом сервере. Это делает данные доступными пользователю независимо от того, где он входит в сеть.

> *Контрольный вопрос.* Перед вами поставлена задача создать домашние каталоги для многих пользователей в организационной единице, которой вы управляете. Вы хотите решить эту задачу как можно быстрее. Ваше приложение резервного копирования использует учетную запись администратора, поэтому вам нужно позаботиться о том, чтобы у приложения был доступ к домашним каталогам пользователей на файловом сервере. Как вы поступите?

Настройте обязательные перемещаемые профили. Обязательные перемещаемые профили можно применять для предоставления пользователям предварительно сконфигурированной рабочей среды и предотвращения сохранения в ней изменений.

> *Контрольный вопрос.* Ваш руководитель попросил вас настроить обязательный перемещаемый профиль для пользователей Windows 8. Вас также попросили выяснить, нельзя ли каким-то образом предотвратить вход пользователей в систему, если обязательный перемещаемый профиль не удалось загрузить.

Создайте сценарии входа для автоматизации администрирования. Администраторы могут использовать сценарии входа, чтобы запускать последовательность команд для предварительного конфигурирования рабочей среды пользователям при их входе в систему. Для этих целей администраторы могут применять команды командной строки, VBScript или PowerShell.

Контрольный вопрос. Вы проектируете среду Active Directory для крупной организации, включающей множество сайтов. Вам требуется возможность настройки сценариев входа для разных ситуаций:

- имеются глобальные команды, которые должны выполняться для каждого пользователя;
- любой пользователь в организационной единице `Accounts` должен иметь доступ к определенным ресурсам;
- любой пользователь, в том числе посетители, который входит на сайт Dublin Active Directory, должен подключаться к локальному общему диску.

У вас спрашивают, какой окажется последовательность запуска для любого пользователя, который будет выполнять все эти сценарии входа.

Глава 27

Виртуализация серверов с помощью Hyper-V

В Windows Server 2012 R2 компания Microsoft значительно расширила возможности Hyper-V — готового решения для виртуализации. Когда Microsoft впервые явила миру Hyper-V в составе Windows Server 2008, было ясно, что разработчикам Hyper-V предстояло еще немало сделать, чтобы предложить своим клиентам то, что уже предлагали конкуренты, которые достаточно долго занимались проблемой виртуализации. Ситуация изменилась на конференции TechEd North America 2013 в Новом Орлеане, где представители Microsoft объявили об огромном количестве усовершенствований уже имеющихся функциональных средств и новых дополнений к Hyper-V в Windows Server 2012 R2. Все эти усовершенствования и дополнения к Hyper-V значительно расширяют возможности и повышают производительность данной системы.

Виртуализация охватывает очень широкий круг вопросов. Говоря о виртуализации сервера, обычно имеют в виду крупные компьютерные системы, которые идеально подходят для облачных вычислений: множество больших многопроцессорных серверов, огромный объем оперативной памяти, технологии кластеризации и SAN, виртуальные жесткие диски, программная организация сетей, ПО для управления и т.д. В одной главе универсальной книги по Windows Server 2012 R2 вроде этой невозможно охватить весь круг вопросов. Если вас интересует более глубокое изложение технологии Windows Server 2012 Hyper-V, обратитесь к книге *Windows Server 2012 Hyper-V Installation and Configuration Guide* (Sybex, 2013 г.), которая написана рядом лучших специалистов в мире виртуализации.

В этой главе вы найдете введение в Hyper-V, включая обзор новых возможностей Windows Server 2012 R2. Приведенной здесь информации будет достаточно для того, чтобы вы смогли приступить к построению собственной небольшой среды с помощью только ПО на основе Windows. Мы рассмотрим такие темы, как понятие и виртуализации сервера и ее использование, установка и применение Hyper-V, а также компоненты Hyper-V и их взаимодействие друг с другом во вновь созданной виртуальной машине.

В этой главе вы изучите следующие темы:

- понятие виртуализации сервера;
- исследование нововведений Hyper-V в Windows Server 2012 R2;
- архитектура Hyper-V;
- установка и конфигурирование хоста Hyper-V;
- конфигурирование виртуальной машины и установка на ней операционной системы.

Понятие виртуализации сервера

В наши дни термин *виртуализация* используется для обозначения множества разных вещей. Он применяется в сочетании с приложениями, хранилищем, сетью, серверами, экранным представлением и т.д. В данной главе *виртуализация* означает способность запуска полномасштабной операционной системы на какой-то программной платформе таким образом, чтобы ОС казалось, будто она функционирует на "реальном" компьютере. Этот тип виртуализации называется *аппаратной виртуализацией* или *виртуализацией сервера*. Итак, для чего это может понадобиться?

Не исключено, что вы — системный администратор, отвечающий за функционирование ряда серверов в вашей организации. Если вы уже достаточно долго занимаетесь деятельностью такого рода, то вы обратите внимание, что мощность сервера растет быстрее, чем потребности приложений в ресурсах.

В прошлом, если компании необходимо было разместить новую линейку бизнес-приложения, скорее всего, она приобретала для этой цели новый сервер. Как правило, это был низкопроизводительный сервер с объемом ОЗУ не менее 4 Гбайт, а чаще 8 Гбайт или больше. Кроме того, поскольку ОС Windows Server требует 64-разрядного оборудования, компании приходилось покупать машину, поддерживающую это. Впоследствии этот процесс повторялся каждый раз, когда становились доступными новые приложения; в итоге многие такие серверы просто простаивали с коэффициентом использования ЦП, составляющим 5%, имели большой объем свободной памяти и запасную полосу пропускания ввода-вывода. Вполне очевидно, что это являлось пустой тратой ресурсов, и именно здесь виртуализация начинает обретать большой смысл.

С помощью виртуализации вы можете консолидировать множество серверов на том же самом оборудовании. Эти серверы не только повысят эффективность использования оборудования, но из-за меньшего количества физических серверов снизится потребление электроэнергии и уменьшится пространство, занимаемое стойками. Более того, посредством надлежащего программного обеспечения вы легко сможете перемещать виртуальные серверы между физическими серверами, что обеспечит гибкую конфигурацию.

Для иллюстрации этого принципа на рис. 27.1 показан один физический сервер, на котором функционирует ОС Windows Server 2012 R2 с ПО виртуализации Hyper-V и несколько виртуальных машин с разными гостевыми операционными системами, такими как Linux, Windows 8.1, Windows Server 2008 R2 и Windows Server 2012. Машина, на которой выполняется Hyper-V, называется *хостом*.

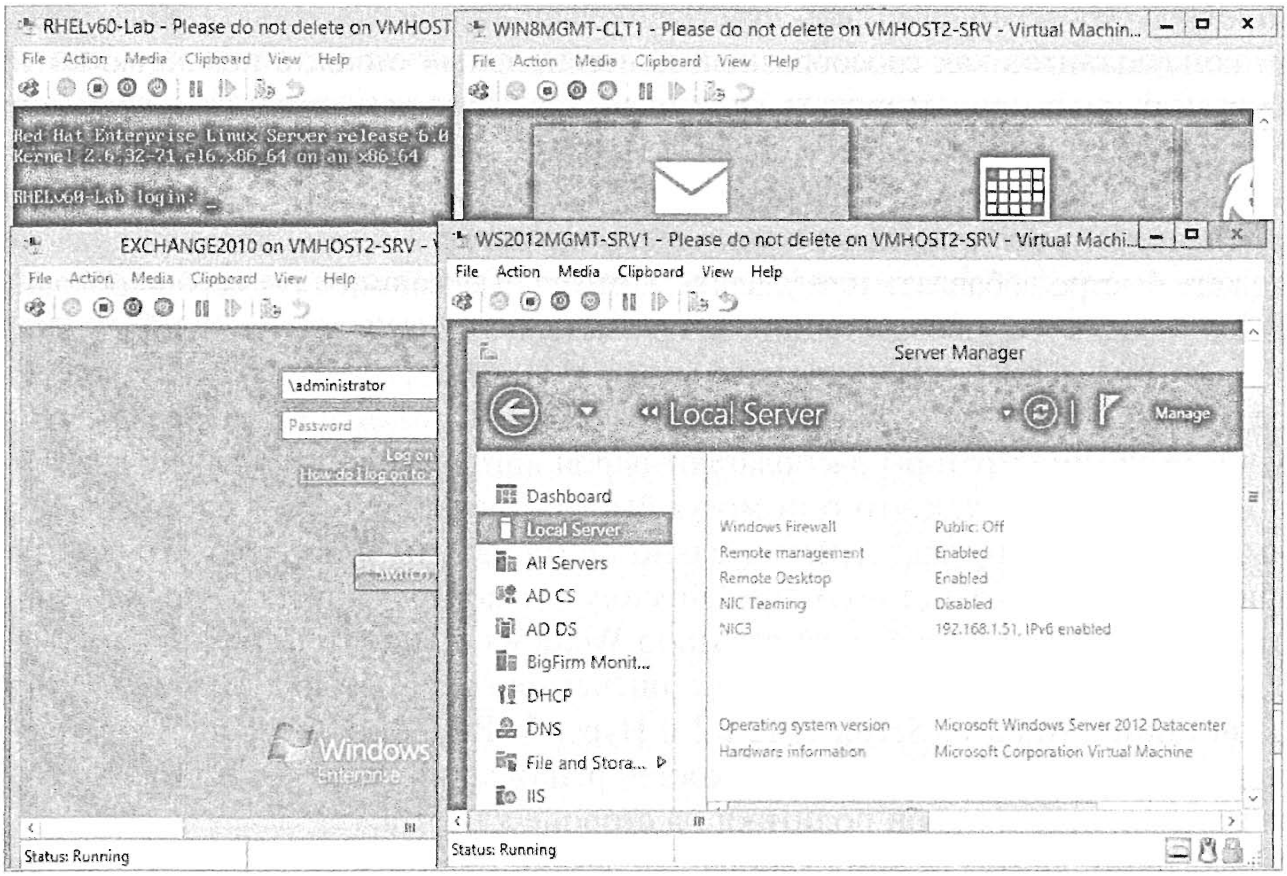


Рис. 27.1. ПО Hyper-V на сервере Windows Server 2012 R2, выполняющем несколько виртуальных машин

Как это в целом работает? Ясно, что у вас не может быть двух операционных систем, одновременно обращающихся к одному и тому же оборудованию. Одна ОС должна управлять (быть хостом), а другой ОС (виртуальной машине) придется обращаться к этому оборудованию с помощью эмуляции, синтетических драйверов или каких-то других средств. В принципе, то же самое касается выполнения инструкций ЦП и даже доступа в память.

Современные специализированные системы виртуализации, подобные Hyper-V, делают все возможное для максимально эффективного использования системных ресурсов. Они работают с реальной памятью, а ЦП непосредственно выполняет код виртуальной машины — за некоторыми исключениями, которые мы обсудим позже. Это же относится к таким высокопроизводительным устройствам, как сетевые, дисковые или видео-интерфейсы. Эмуляция, при которой приходится моделировать поведение существующего оборудования, обернется снижением производительности. Иногда это неизбежно, но в Hyper-V избран другой путь. Чтобы как можно больше сократить подобные накладные расходы, в Hyper-V применяется собственная архитектура драйверов для каждого типа устройств. Такое проектное решение тесное интегрируется с архитектурой компьютера.

Для чего используется виртуализация сервера?

Теперь, когда у вас сложилось некоторое представление о том, что собой представляет виртуализация, давайте обсудим, для чего ее использовать. Важными применениями виртуализации являются тестирование и разработка, консолидация серверов и восстановление в аварийных ситуациях. Все перечисленные задачи получают преимущество от высокой степени гибкости, предлагаемой виртуализацией.

Поначалу эта технология пользовалась большой популярностью у администраторов и консультантов как своеобразный испытательный стенд, с помощью которого они могли быстро протестировать свои идеи. Их более чем устраивала возможность использовать существующий компьютер с ПО виртуализации для запуска пары виртуальных машин. В распоряжении более крупных организаций обычно имеется несколько сред тестирования, предназначенных для разных целей. С помощью виртуализации вы можете быстро добавлять или удалять виртуальные машины по мере необходимости. Всякий раз, когда появляется новое приложение или нужно интегрировать новый компонент инфраструктуры, для развертывания проекта, в котором применяется это новое приложение или компонент, понадобится лишь новая виртуальная среда.

Многие администраторы располагают парой виртуальных машин для своего личного использования, так что они могут быстро тестировать и исследовать планируемые изменения, прежде действительно применять их в производственной сети. Например, как специалист по Active Directory, вы можете запустить четыре или пять контроллеров домена и рабочую станцию Windows 8.1 внутри виртуальных машин на обычном настольном компьютере с оперативной памятью 8 Гбайт, на котором функционирует Windows Server 2012 R2 и Hyper-V. Вы могли бы использовать такую конфигурацию для исследования тонкостей репликации Active Directory или результатов изменения групповой политики на стороне клиента.

Аналогично, виртуализация удобна для демонстрации технологий. Из-за низких требований к производительности во время проведения демонстраций вы можете запустить несколько виртуальных машин на мощном переносном компьютере и показывать людям, как в действительности функционирует та или иная технология.

Помимо применения виртуализации в целях тестирования и демонстрации, крупнейшие развертывания виртуализации серверов встречаются в центрах хранения и обработки данных, где многочисленные серверы консолидируются для основного и частного использования облачных служб. Кроме того, большое число организаций (крупных и мелких) переносят свои физические IT-мощности на виртуальные платформы, чтобы получить выгоду от экономии расходов и повышения гибкости. Виртуализированная среда обеспечивает следующие преимущества.

- **Сберегает ресурсы и экономит расходы.** Установка одного хоста, выполняющего несколько виртуальных машин, позволяет сэкономить пространство под стойки, электроэнергию, а также нагрузку на систему охлаждения. Вполне обоснованно объединять 20 или 30 слабо используемых физических машин в одну высокоспециализированную хост-машину.
- **Совместное использование оборудования.** Хост предоставляет каждой виртуальной машине одно и то же "виртуальное" оборудование. Другими словами, все виртуальные машины совместно используют общее оборудование. Это делает их предсказуемыми и облегчает обслуживание драйверов. Развертывать виртуальные машины гораздо проще, чем физические, главным образом потому, что драйверы больше не являются проблемой.
- **Увеличивает гибкость системы.** Одинаковые возможности виртуального оборудования значительно увеличивают гибкость. Вы можете перемещать виртуальные машины между хостами с целью распределения нагрузки или проведения обслуживания. Если ваша компания подумывает о переходе на облако (открытое или закрытое), то виртуализация играет главную роль в обеспечении гибкости облака.

- **Присоединяет унаследованные операционные системы.** Во многих организациях применяется смесь операционных систем, в число которых входят не только Windows Server 2012 R2, но и более старые системы, такие как Windows Server 2008 или даже Windows Server 2003. Не исключено, что на современном оборудовании унаследованные системы будут требовать меньшего расхода вычислительной мощности. Это делает их идеальными кандидатами для консолидации. Один хост будет обладать вычислительной мощностью, достаточной для множества старых систем, что также позволит извлечь преимущество из унифицированного виртуального оборудования.

В крупных средах с развертываниями больших сетей хранения данных (storage area network — SAN), центрами хранения и обработки данных с зеркальным отображением и аналогичной инфраструктурой виртуализация серверов является важным активом для восстановления в аварийных ситуациях. Здесь преимущество заключается не только в консолидации серверов, но и в том, что все виртуальные машины располагают одним типом виртуального оборудования. При перезапуске виртуальной машины на новом хосте Hyper-V *никаких* проблем с драйверами или уровнем абстракции оборудования (HAL) возникать не будет. У каждой технологии имеются свои недостатки, и виртуализация тому не исключение. Некоторые из этих недостатков могут оказывать большее влияние, другие — меньшее.

- **Повышает сложность.** Виртуализация добавляет в существующую среду еще один уровень сложности. Теперь вам нужно знать, чем является конкретный сервер — виртуальной машиной, физическим сервером или, возможно, хостом для виртуальных машин. Например, ранее администраторы SQL Server несли ответственность за все аспекты SQL Server: программное обеспечение, оборудование и конфигурацию. Если же SQL Server виртуализирован, то поддержание работоспособности его виртуальных машин должно зависеть от администраторов сервера хоста. Любое воздействие на этот хост скажется также на виртуальных машинах SQL Server.
- **Предъявляет дополнительные требования к инфраструктуре.** Полнофункциональной среде виртуальных машин понадобится дополнительная инфраструктура: в крупных средах решение SAN, а также отдельное ПО управления и выделенная высокоскоростная IP-сеть являются обязательными компонентами.
- **Может приводить к крупномасштабным отказам.** Если вы специально не предпримете меры по обеспечению готовности служб, то хост будет единой точкой отказа. При неожиданной утрате работоспособности хоста, например, из-за перегрева и остановки центрального процессора, остановятся все виртуальные машины, функционирующие на нем. (Вот яркая иллюстрация того, как опасно "класть все яйца в одну корзину"!)
- **Требует специального обслуживания.** При наличии набора автономных виртуальных машин вам придется обслуживать также и их, скажем, применяя исправления.
- **Порождает уникальные проблемы, касающиеся безопасности.** С виртуализацией связаны некоторые неочевидные соображения безопасности. Например, в среде, основанной на SAN, вы будете иметь две дополнительные группы администраторов, которые могут обращаться к данным в виртуальной машине: администраторы, отвечающие за машины хостов, и администраторы SAN.

Администратор SQL Server, ответственный за виртуальную машину, может быть даже не осведомлен о том, что другим администраторам в принципе доступны его данные (предполагая, что у них есть желание и знания, которые необходимы для этого).

Еще одним примером может служить сценарий, при котором несколько доменов безопасности размещены в одной и той же инфраструктуре виртуализации: демилитаризованная зона и локальная сеть организации, находящиеся на том же самом хосте. Другой сценарий касается облака с множеством владельцев, в котором функционируют совершенно разные клиентские среды.

- **Требует обучения.** Когда вы развертываете новую технологию, вам нужно освоить ее. Во время обучения вы будете совершать ошибки. Некоторые из них могут повлиять на производственную среду. В этом нет ничего нового, но данный фактор должен быть принят во внимание.

Очевидно, что требуется достичь какого-то баланса. Для большинства (но не всех) организаций перечисленные выше достоинства значительно перевешивают недостатки. Главный аспект в том, что виртуализация серверов всегда находится в вашем распоряжении. Даже если организация еще не развернула ее, высока вероятность, что вскоре это произойдет. Еще один убедительный довод заключается в том, что поскольку Hyper-V покрывается лицензией на операционную систему Windows Server 2012 R2, после ее приобретения вы получаете решение виртуализации и не обязаны покупать какое-то дополнительное программное обеспечение.

Начало работы с Hyper-V

Неудивительно, что для запуска Hyper-V должны быть удовлетворены определенные требования к оборудованию и программному обеспечению. Вдобавок здесь замешаны запутанные проблемы лицензирования, которые мы обсудим позже в этой главе.

Требования к оборудованию

Базовые требования для функционирования Hyper-V довольно просты и перечислены ниже.

- **Центральный процессор и BIOS.** Вам нужен центральный процессор x64 и система BIOS, которая поддерживает виртуализацию, выполняемую с помощью ЦП, и функцию предотвращения выполнения данных (Data Execution Prevention — DEP). Распространенная проблема состоит в том, что хотя эти возможности предлагаются системой, обычно в системе BIOS на более старом серверном оборудовании они не включены. Позаботьтесь о включении данных функций. Если нужно изменить настройки DEP или виртуализации, помните о том, что для этого потребуется холодная начальная загрузка: компьютер должен быть полностью выключен. Сброса или программной перезагрузки будет недостаточно. Обратите внимание, что для любого подходящего серверного оборудования, приобретенного до 2008 года, может также понадобиться модернизация BIOS, чтобы получить доступ к указанным настройкам. Практически у всех современных серверов такие функции в BIOS по умолчанию включены, но это то, что следует проверить дважды, прежде чем приступать к работе с Hyper-V.
- **Сертификация для Windows Server 2012.** Если вы хотите иметь полную уверенность в том, что Hyper-V сможет нормально функционировать на приобрета-

емых серверах, то должны напрямую поинтересоваться этим вопросом у поставщика. Именно поставщик отвечает за проверку, действительно ли Hyper-V может работать на поставляемом им оборудовании. Большинство крупных поставщиков также принимают участие в программе "Certified for Windows Server 2012" ("Сертифицировано для Windows Server 2012"), которая требует от них тестирования своего оборудования с помощью процедур соответствия стандартам Microsoft. После того как сервер пройдет такую проверку, поставщик может отправить конфигурацию в Microsoft для ее включения в открытый каталог. Тем не менее, далеко не все поставщики отправляют сведения обо всем своем оборудовании. Именно поэтому вы должны спрашивать их напрямую. Каталог Microsoft доступен по адресу `http://windowsservercatalog.com`. В поле Search (Поиск) можно ввести *Hyper-V compatible systems*.

Теперь, когда вы в целом знаете, на какие возможности обращать внимание, давайте обсудим детали. При выборе оборудования для виртуализации важно иметь в виду несколько моментов. Чтобы виртуальные машины функционировали оптимально, им требуется много памяти (ОЗУ) и значительная полоса пропускания дискового ввода-вывода; кроме того, чем больше сетевых интерфейсных плат, тем лучше.

- **ОЗУ.** При развертывании Hyper-V вы должны в первую очередь удостовериться в том, что сервер удовлетворяет минимальным требованиям для запуска Windows Server 2012 R2, как было показано в главе 2. Если объем ОЗУ является достаточным для нормального функционирования операционной системы хоста, вам необходимо выяснить, сколько дополнительной памяти понадобится для каждой виртуальной машины. Для низкопроизводительной персональной тестовой системы, выделенной под виртуализацию, скорее всего, потребуется не менее 8 Гбайт памяти и материнская плата с одним или двумя сокетами и четырехядерными ЦП.
- **Диски.** Приобретите столько дисководов, сколько позволяют финансы. При использовании нескольких виртуальных машин четыре независимых диска средней емкости будут быстрее, чем два диска большой емкости. Диски SATA подойдут для тестирования не слишком требовательных приложений. Более высокую производительность обеспечат диски SCSI или SAS, но если денег достаточно, то инвестируйте их в высокоскоростные твердотельные диски для обеспечения оптимальной производительности. Избегайте конфигурации RAID-5, т.к. она характеризуется медленными операциями записи. Сочетания RAID 0 и RAID 1 хороши для низкопроизводительных систем — к тому же помните, что RAID 0 не является отказоустойчивой конфигурацией. Для высокопроизводительных приложений подумайте о выборе RAID 10.
- **Сетевые интерфейсные платы.** Для сетей с Hyper-V согласно общей рекомендации необходимо иметь, по меньшей мере, две сетевых интерфейсных платы: одну для управления хостом и еще одну для обеспечения доступа виртуальных машин в сеть. Предпочтительнее располагать четырьмя и более сетевыми интерфейсными платами, чтобы задействовать такие встроенные возможности Windows Server 2012 R2, как NIC Teaming, Converged Networking и Failover Cluster. Если вы ожидаете высокой пропускной способности сети либо имеете дело с подключениями iSCSI, которые требуют выделенных сетевых интерфейсных плат, то таких плат потребуется еще больше.

Требования к программному обеспечению

Теперь, когда вы ознакомились с требованиями к оборудованию, настало время обсудить требования к программному обеспечению. В табл. 27.1 перечислены разные варианты Hyper-V и связанные с ними права виртуализации, основанные на количестве экземпляров VOSE (Virtual Operating System Environment — среда виртуальной операционной системы), которые можно запускать на них. VOSE — это лицензионный термин для обозначения гостевой операционной системы, функционирующей на хосте.

Таблица 27.1. Редакции Windows Server 2012 и Hyper-V

Редакция Windows Server 2012	Сокеты ЦП	Права виртуализации
Windows Server 2012 R2 Datacenter	Два	Неограниченное количество бесплатных экземпляров VOSE
Windows Server 2012 R2 Standard	Два	Два бесплатных экземпляра VOSE
Hyper-V Server 2012	–	Нет бесплатных экземпляров VOSE
Windows Server 2012 Essentials	–	Средство Hyper-V не доступно
Windows Server 2012 Foundation	–	Средство Hyper-V не доступно

Обратите внимание на специфичную редакцию под названием Hyper-V Server 2012. По существу это сокращенная версия Server Core, у которой по умолчанию включена роль Hyper-V. Ее главное преимущество заключается в том, что она доступна для бесплатной загрузки и может применяться для базовой виртуализации. Остальные редакции отличаются своими возможностями виртуализации и моделями лицензирования. Коротко говоря, лицензии редакций Datacenter и Standard распространяются на два сокета ЦП. Таким образом, если у сервера есть четыре сокета, вам понадобятся две лицензии. Неограниченное количество VOSE обеспечивается при корректном лицензировании сокетов. Использовать Hyper-V Server 2012 разрешено, когда клиенты уже имеют лицензии, действие которых может распространяться на виртуальные машины. В двух других редакциях Windows Server 2012 (Essentials и Foundation) роль Hyper-V отсутствует.

Hyper-V в клиентских операционных системах

Хотя в табл. 27.1 перечислены только серверные редакции Windows, под управлением которых можно запускать Hyper-V, здесь полезно упомянуть о том, что роль Hyper-V можно также развернуть как часть клиентских операционных систем Windows 8 или Windows 8.1. Эта возможность, известная как *Client Hyper-V*, является той же самой технологией, которую вы получаете в Windows Server, но без функциональности кластеризации уровня предприятия, восстановления в аварийный ситуациях и масштабируемости. Основное применение Client Hyper-V связано с предоставлением IT-специалистам и разработчикам среды базовой виртуализации на их переносных компьютерах или ПК, которую они могут использовать в тестовых и демонстрационных целях. Средство Client Hyper-V не предназначено для запуска каких-то гостевых экземпляров или обработки рабочей нагрузки, характерной для производственного сервера. Если хотите узнать больше о Client Hyper-V, это средство доступно для загрузки по ссылке `http://tinyurl.com/win8clienthyperv`.

Что нового в Hyper-V версии Windows Server 2012 R2?

Можно с полным основанием утверждать, что в ходе разработки Windows Server 2012 R2 компания Microsoft вложила огромные ресурсы и бюджет, чтобы средство Hyper-V стало еще лучше, чем его предшественник Windows Server 2012 (RTM). Также можно отметить, что при создании версии Windows Server 2012 R2 в Microsoft использовали в качестве отправной точки перечень возможностей, предлагаемых конкурирующей разработкой (VMware), после чего предоставили множество усовершенствований и функций, оставив своих конкурентов далеко позади. Это оказалось огромным благом для IT-специалистов, консультантов и администраторов, поскольку им теперь гораздо легче убедить своих клиентов или руководителей в выгодности применения Hyper-V в своей бизнес-среде.

В данном разделе мы сначала предложим обзор того, что является новым и исключительным для Hyper-V в Windows Server 2012 R2. Затем мы обсудим, на что можно рассчитывать при обеспечении масштаба уровня предприятия и производительности для центра обработки и хранения данных.

- **Новый формат VHDX.** В Windows Server 2012 (RTM) был представлен новый формат виртуального жесткого диска (`.vhdx`) от Microsoft, призванный заменить давно существовавший первоначальный формат виртуального диска (`.vhd`), который использовался со времен старого продукта Virtual PC. С помощью VHDX компании Microsoft удалось преодолеть ограничение формата VHD, касающееся максимального объема дисковой памяти в 2 Тбайт, и довести максимальный объем памяти виртуальных дисков до 64 Тбайт. Размер физического сектора дисков VHD был ограничен 512 байтами, но в VHDX размер физического сектора неизмеримо больше и составляет 4 Кбайт. Кроме того, в Windows Server 2012 R2 формат VHDX позволяет изменять размеры виртуальных жестких дисков, когда виртуальная машина находится в онлайновом режиме (рис. 27.2).

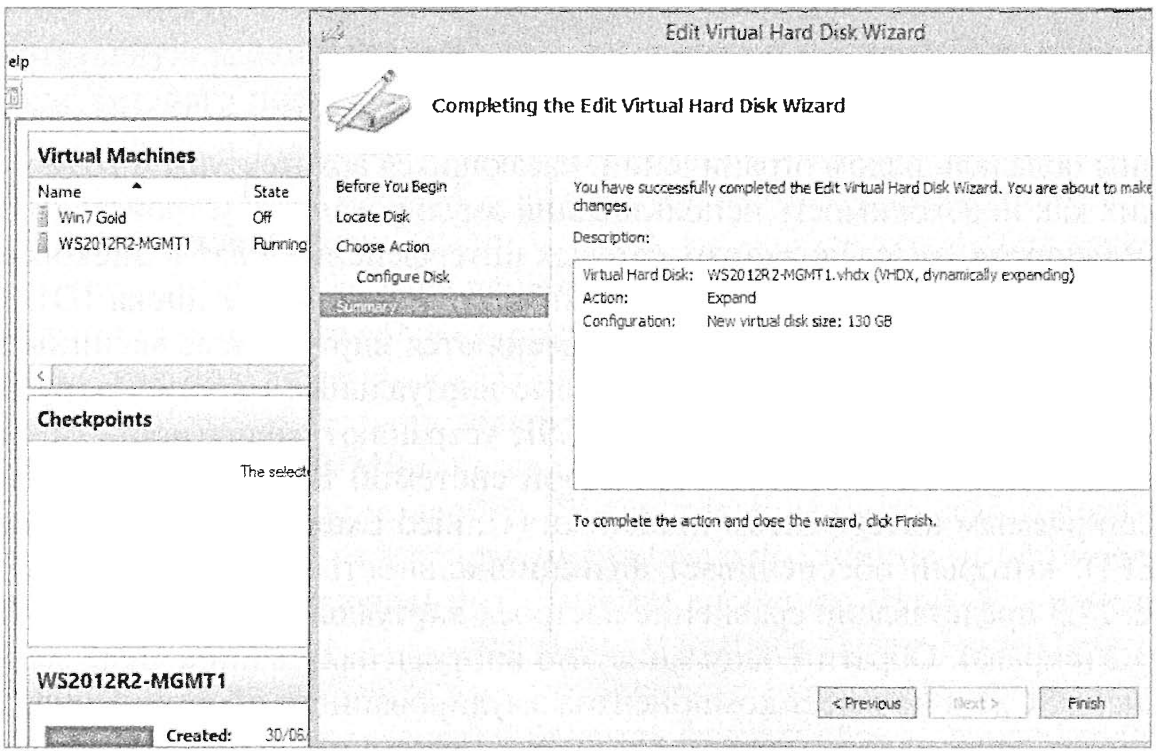


Рис. 27.2. Изменение размеров дисков VHDX в онлайновом режиме

Изменение размеров в Windows Server 2008 R2 или даже Windows Server 2012 RTM было невозможным без предварительного прекращения работы виртуальной машины, что приводило к периодам бездействия. Для того чтобы воспользоваться этой поистине замечательной возможностью, необходимо всего лишь присоединить диск VHDX к виртуальному контроллеру SCSI на виртуальной машине.

- **Общие диски VHDX.** Благодаря новому формату VHDX в Windows Server 2012 R2, теперь можно открывать совместный доступ к виртуальным дискам, предоставляя общее хранилище для гостевых кластеров Hyper-V. В сущности, это означает, что вам больше не придется усложнять свои решения общими файловыми ресурсами iSCSI, Fibre Channel или SMB 3.0, когда нужно создать кластеры с обходом отказа на основе виртуальных машин. Вы можете сконфигурировать совместное использование дисков VHDX либо посредством графического пользовательского интерфейса, либо с помощью нескольких простых строк кода PowerShell. За дополнительными сведениями обращайтесь в статью по ссылке `http://workinghardinit.wordpress.com/2013/06/06/shared-virtual-disks-in-windows-server-2012-r2-hyper-v-maximizes-tcoroi/`.

Преобразование дисков VHD в VHDX

Ознакомившись с возможностями, которые обеспечивает новый формат VHDX в Windows Server 2012 R2, вам наверняка будет интересно узнать, что вы можете легко преобразовать в VHDX старые файлы VHD, которые сейчас применяются на виртуальных машинах в средах Windows Server 2008. Это можно сделать либо через консоль диспетчера Hyper-V, щелкнув на ссылке Edit Disk (Редактировать диск) в панели Actions (Действия) и выбрав в мастере действие Convert (Преобразовать), либо посредством следующей команды PowerShell (подставив имя диска и путь из своей конфигурации):

```
Convert-VHD -Path E:\VirtualMachine1\DataDisk.vhd
  -DestinationPath E:\VirtualMachine1\DataDisk.vhdx
```

- **Виртуальные машины Gen2.** В более ранних версиях Hyper-V виртуальные машины обладали рядом ограничений, касающихся архитектуры и возможностей, таких как необходимость использования эмулированных устройств (например, COM-портов, унаследованных сетевых интерфейсных плат и дисководов гибких дисков) и возможность начальной загрузки только с диска IDE. Однако в Windows Server 2012 R2 теперь применяются виртуальные машины поколения 2 (Generation 2 –Gen2). Эти новые виртуальные машины допускают загрузку из виртуальных адаптеров SCSI, устраняют зависимость от эмулированных устройств и снабжаются новой системой BIOS с унифицированным расширяемым интерфейсом прошивки (Unified Extensible Firmware Interface — UEFI), который обеспечивает функциональность безопасной загрузки. На рис. 27.3 представлено сравнение настроек виртуальных машин Gen1 (слева) и Gen2 (справа). Обратите внимание, что виртуальная машина Gen2 загружается с диска SCSI и не имеет компонентов эмулированного оборудования, которые содержит виртуальная машина Gen1.

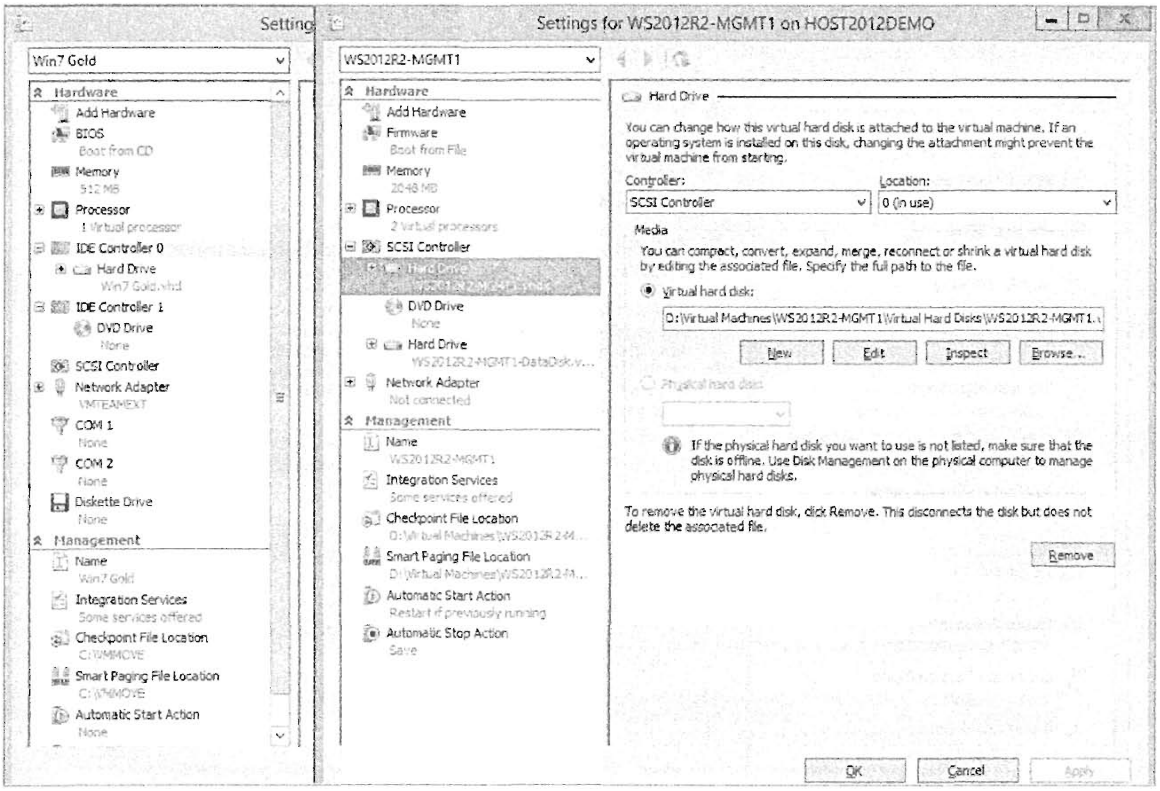


Рис. 27.3. Настройки виртуальных машин Gen1 и Gen2

- **Режим расширенного сеанса (прямое подключение к виртуальной машине (VM Direct Connect)).** На первый взгляд, это довольно простое усовершенствование, но как консультанты, много лет работающие с Hyper-V, мы считаем эту возможность одной из наиболее примечательных характеристик Hyper-V в Windows Server 2012 R2. В более ранних версиях Hyper-V операция сложного копирования и вставки между сервером хоста и виртуальной машиной была невозможной. Вы могли выполнять копирование и вставку в виртуальную машину при наличии сконфигурированного сетевого подключения, однако отсутствие сетевого подключения означало невозможность копирования и вставки. Это усложняло решение даже таких простых задач, как ввод в новую виртуальную машину ключа продукта. Это также означало, что если вы не имели сетевого подключения с виртуальной машиной, то для управления ею должны были использовать консоль Hyper-V, и когда это приходилось делать в течение длительного времени, неизбежно страдала производительность.

  Однако в режиме расширенного сеанса вы можете теперь без труда выполнять копирование и вставку напрямую в и из виртуальной машины, даже без сконфигурированного сетевого подключения. На практике это выглядит точно так же, как подключение к удаленному рабочему столу, но без необходимости беспокоиться о сетевом подключении. Для этого в режиме расширенного сеанса применяется VMBus через компоненты интеграции Hyper-V; позже мы обсудим VMBus более подробно. Режим расширенного сеанса должен включаться и отключаться на основе индивидуальных хостов, и по умолчанию он отключен. Чтобы включить его, откройте диспетчер Hyper-V, в панели Actions (Действия) щелкните на ссылке Hyper-V Settings (Настройки Hyper-V), в открывшемся окне выберите элемент Enhanced Session Mode Policy (Политика режима расширенного сеанса) и отметьте флажок Allow enhanced session mode (Разрешить режим расширенного сеанса), как показано на рис. 27.4.

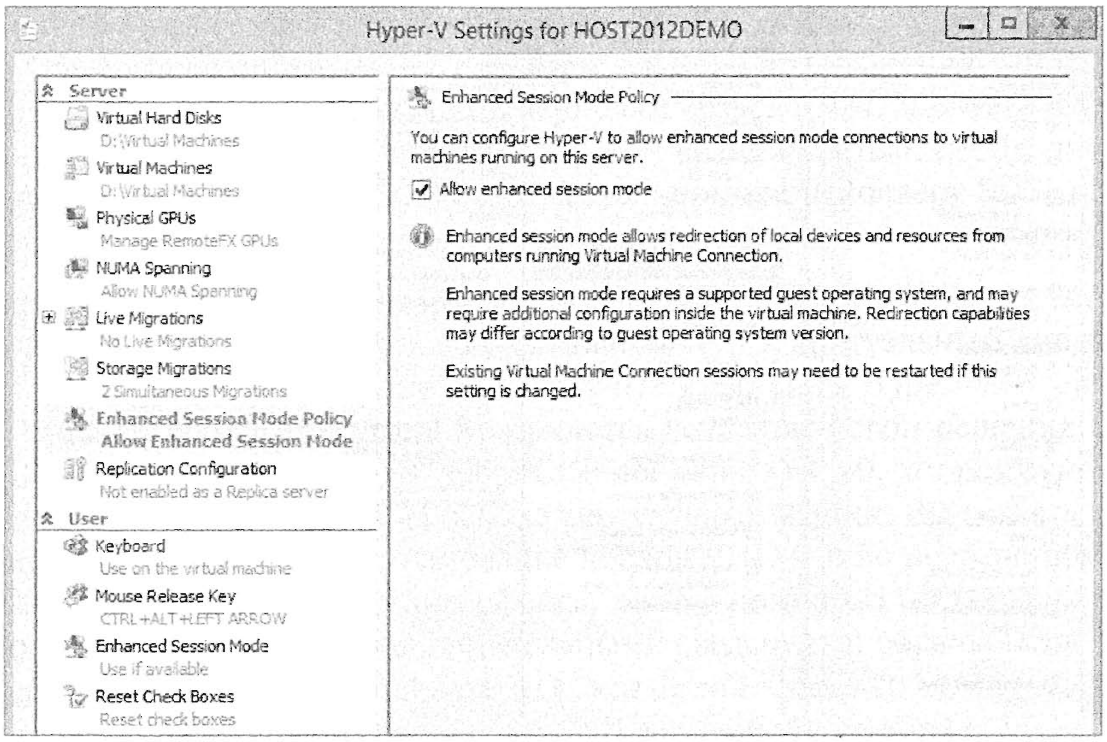


Рис. 27.4. Включение режима расширенного сеанса

- **Ускоренная живая миграция.** Живая миграция существовала еще в Hyper-V версии Windows Server 2008 R2 и позволяет выполнять переносы виртуальных машин между хостами, оставляя их в онлайновом режиме. Серьезная проблема заключалась в том, что такие переносы могли быть весьма затратными по времени, что зависело от таких факторов, как объем памяти, выделенной для виртуальной машины, и способ конфигурирования сетей кластеров. Если вам нужно было отключить хост в кластере Hyper-V версии Windows Server 2008 R2, а количество виртуальных машин, ожидающих миграции на другой хост, было большим, то приходилось ожидать, пока все они не будут перенесены по одной. Наблюдать за этим было довольно тягостно, особенно если вы располагали только небольшим окном обслуживания, чтобы выполнить перезагрузку хоста.

  В Hyper-V для Windows Server 2012 R2 предусмотрено несколько усовершенствований для живой миграции. Прежде всего, вам больше не придется ждать переноса виртуальных машин по отдельности, поскольку можно одновременно выполнять неограниченное количество живых миграций. Очевидно, что это может оказывать влияние на производительность хоста в зависимости от конфигурации сети и ЦП, поэтому разумно не пытаться одновременно переносить 100 виртуальных машин значительных размеров. Чтобы подкорректировать количество миграций, которые можно проводить одновременно, откройте диспетчер Hyper-V и в панели Actions (Действия) щелкните на ссылке Hyper-V Settings (Настройки Hyper-V). Выберите элемент Live Migrations (Живые миграции), отметьте флажок Enable incoming and outgoing live migrations (Включить входящие и исходящие живые миграции) и укажите требуемое количество в поле Simultaneous live migrations (Количество одновременных живых миграций). На рис. 27.5 приведен пример.

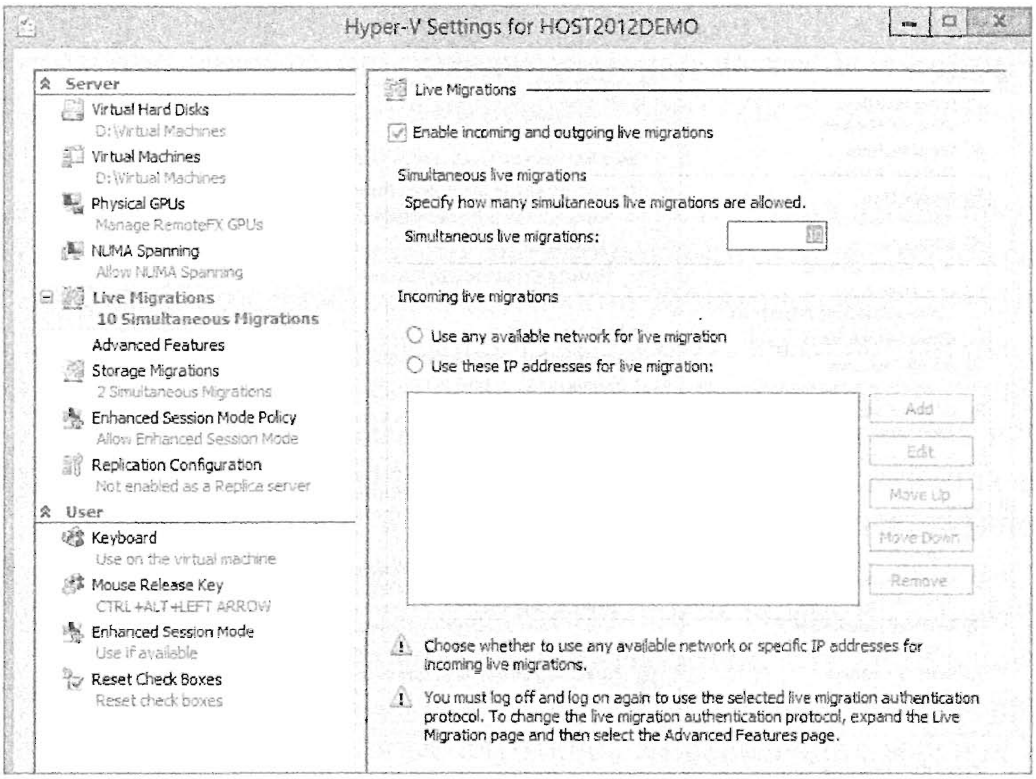


Рис. 27.5. Указание количества живых миграций, выполняемых одновременно

Однако в Microsoft на этом не остановились и в Hyper-V версии Windows Server 2012 R2 ввели (и по умолчанию включили) *сжатие во время живой миграции*. Во время переноса виртуальных машин со сжатием вы, по меньшей мере, удваиваете скорость миграции по сравнению с той, что достигалась в более ранних версиях Hyper-V. Из сжатия во время живой миграции можно извлечь еще большую пользу при наличии бюджета на приобретение некоторого высокопроизводительного сетевого оборудования и применение новой живой миграции через функциональность SMB. В таком случае вы можете использовать либо средство *SMB Multichannel* (когда для получения более широкой общей полосы пропускания автоматически задействуется множество сетевых интерфейсных плат), либо средство *SMB Direct* (если вы закупили для своих сетей с живой миграцией специализированные сетевые интерфейсные платы RDMA со скоростью 10 Гбит/с и коммутаторы с возможностью DCB). С помощью SMB Direct время переноса виртуальной машины можно сократить с нескольких минут буквально до нескольких секунд! Чтобы сконфигурировать живую миграцию поверх SMB, откройте диспетчер Hyper-V, в панели Actions щелкните на ссылке Hyper-V Settings, раскройте узел Live Migrations (Живые миграции) и выберите элемент Advanced Features (Дополнительные возможности). На рис. 27.6 показан экран Advanced Features, где можно выбрать переключатель Compression (Сжатие) или SMB.

- **Онлайновое слияние контрольных точек.** То, что в Hyper-V версии Windows Server 2008 R2 называлось снимками, в Windows Server 2012 (RTM) именуется контрольными точками. Они позволяют получать образ виртуальной машины в определенный момент времени, пока эта виртуальная машина продолжает функционировать. В Hyper-V версии Windows Server 2008 R2 создавался новый разностный диск (`.avhd`), который связывался с исходным диском VHD, но представлял собой полностью отдельный файл.

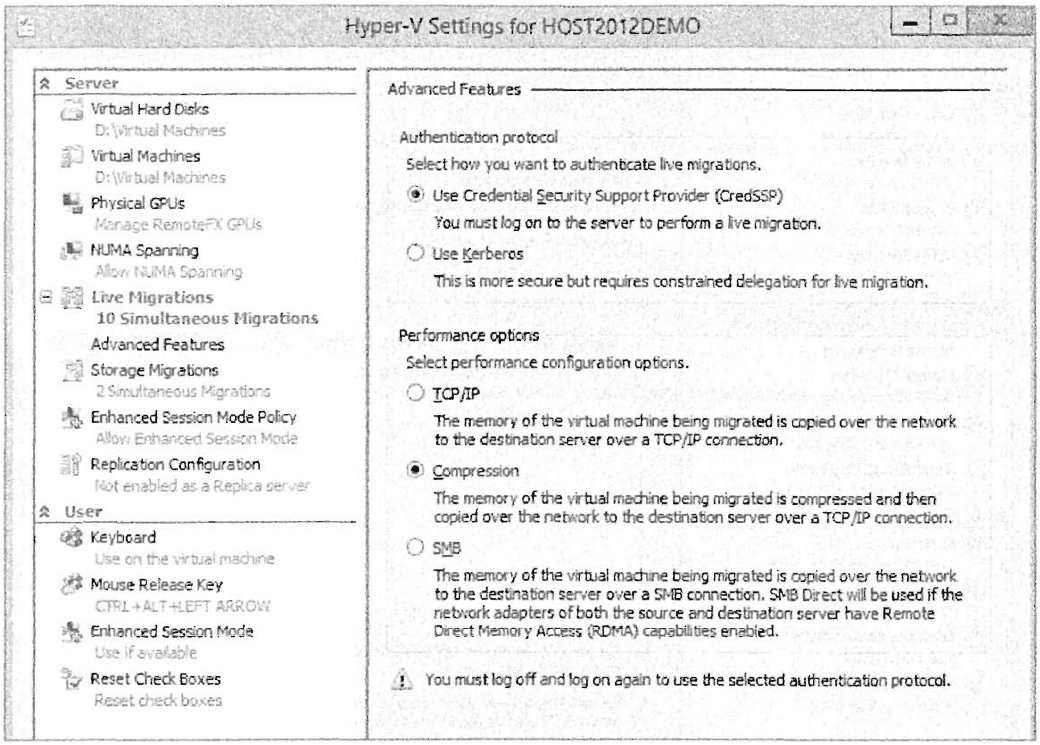


Рис. 27.6. Конфигурирование сжатия во время живой миграции и SMB

Это была удобная возможность, например, в ситуации, когда требовалось применить к серверу новый пакет обновлений или текущее исправление, и нужна была гарантия быстрого отката к первоначальному состоянию, если что-то пошло не так.

Однако недостатки существенно перевешивали достоинства, и до выхода Windows Server 2012 для удаления контрольной точки, представляющей определенный момент времени, необходимо было завершить работу виртуальной машины и подождать, пока выполнится слияние файла AVHD с родительским файлом VHD. Если файл AVHD был достаточно большим, то такая процедура занимала немало времени, в течение которого виртуальная машина простаивала. К счастью, в Windows Server 2012 R2 теперь можно выполнять онлайновое слияние контрольных точек, так что если для виртуальных машин требуется создать контрольные точки, вы можете безопасно объединять их безо всяких простоев. Онлайновое слияние контрольных точек будет приводить к появлению небольшим накладным расходам в плане производительности виртуальной машины, поэтому вы должны понимать, что оно оказывает некоторое влияние на производственные системы, и проводить его в нерабочие часы.

- **Шлюз Windows Server.** Шлюз Windows Server (Windows Server Gateway — WSG) является новым дополнением к и без того развитому сетевому стеку Hyper-V для Windows Server 2012, которое появилось в Windows Server 2012 R2. Он действует как программный маршрутизатор виртуальной машины, который позволяет поставщикам облачных служб и центров обработки данных маршрутизировать трафик между их физическими и виртуальными сетевыми средами, а также Интернетом. Шлюз WSG интегрирован в сетевые средства Hyper-V и применяет стандарт NVGRE (Network Virtualization using Generic Routing Encapsulation — виртуализация сетей с использованием общей инкапсуляции маршрутов), который обеспечивает изоляцию истинного адресного пространс-

тва центра обработки данных для сред с множеством владельцев. Подробное рассмотрение этой технологии выходит за рамки настоящей книги, но дополнительная информация доступна по ссылке `http://technet.microsoft.com/ru-ru/library/dn313101.aspx`.

- **Расширенная поддержка виртуальных машин Linux.** Если в вашей среде Hyper-V версии Windows Server 2012 R2 функционируют виртуальные машины Linux, то теперь вы можете пользоваться поддержкой динамической памяти, которая позволяет конфигурировать начальный объем ОЗУ, выделяемый для виртуальной машины, и возможность его динамического расширения в периоды пиковой нагрузки. Кроме того, если вы когда-либо пытались управлять виртуальной машиной Linux из консоли управления Hyper-V предшествующих версий, то помните, что быстродействие и поддержка мыши не были на должной высоте. В Hyper-V версии Windows Server 2012 R2 предлагаются усовершенствованные драйверы, улучшающие быстродействие мыши и видео и, в конечном итоге, удобство всего интерфейса управления. Наконец, для виртуальных машин Linux в Windows Server 2012 R2 стало возможным онлайновое резервное копирование безо всяких пауз, которые случались в предыдущих версиях Hyper-V.
- **Расширенная функция Hyper-V Replica.** Функция Hyper-V Replica (Реплика Hyper-V) впервые появилась в Windows Server 2012 (RTM). По существу она используется как способ восстановления в аварийных ситуациях, при котором существующие виртуальные машины из хоста на одном сайте реплицируются на хост другого сайта. В версии Windows Server 2012 R2 функция Hyper-V Replica расширена, чтобы позволить выполнять репликацию виртуальных машин на третий сайт. Эта функциональность привносит дополнительную гибкость в управление автономными репликами для восстановления в аварийных ситуациях или даже базового резервного копирования. Например, вы можете хранить один экземпляр реплики на собственном локальном сайте, а другой экземпляр — в облаке либо у стороннего поставщика услуг. Кроме того, в предыдущем выпуске Hyper-V Replica существовало ограничение на интервал обновления, который должен был составлять не менее 5 минут, и хотя этого было более чем достаточно для большинства организаций, в Windows Server 2012 R2 можно сконфигурировать интервал обновления, равный 30 секундам (рис. 27.7). Мы обсудим функцию Hyper-V Replica более подробно в следующей главе.
- **Автоматическая активация виртуальных машин.** В редакции Windows Server 2012 R2 Datacenter вы имеете неограниченные права виртуализации для своих хостов Hyper-V. Это означает, что при наличии лицензии вы можете запускать на каждом хосте столько виртуальных машин, сколько хотите, но на каждой виртуальной машине придется активировать ключ продукта. Хотя это не чрезмерно трудная задача, активация большого количества виртуальных машин может стать часто повторяющейся, и если виртуальные машины функционируют без подключения к Интернету, то данная задача превратится в серьезную проблему.

  Теперь у вас есть возможность с помощью автоматической активации виртуальных машин (Automatic Virtual Machine Activation — AVMA) сконфигурировать хост Hyper-V редакции Windows Server 2012 R2 Datacenter для автоматической активации любых гостевых виртуальных машин, которые функционируют на этом хосте. Чтобы воспользоваться этой новой возможностью,

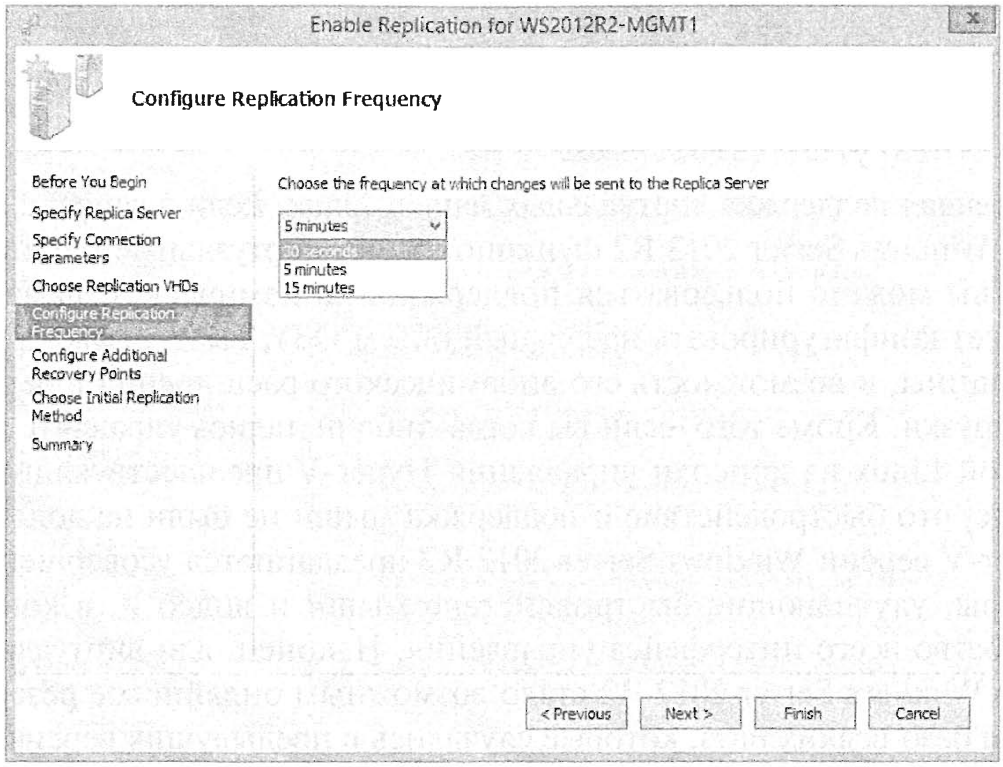


Рис. 27.7. Конфигурирование интервала обновления

потребуется развернуть гостевую виртуальную машину с редакцией Windows Server 2012 R2 Datacenter, Standard или Essentials (любая ОС, предшествующая Windows Server 2012 R2, работать с AVMA не будет) и установить ключ AVMA внутри этой гостевой виртуальной машины с помощью следующей команды:

```
slmgr /ipk <ключ_AVMA>
```

После запуска этой команды (с подстановкой вместо параметра `<ключ_AVMA>` действительного ключа, который вы получаете при покупке Windows Server 2012 R2 Datacenter) гостевая виртуальная машина автоматически активирует себя на своем хосте. Если вы развертываете виртуальные машины с использованием файла ответов для автономной установки, то добавление в него ключа AVMA позволит проводить активацию безо всякого вмешательства с вашей стороны.

- **Масштабируемость Hyper-V.** В Windows Server 2012 R2 единственное отличие между редакциями Standard и Datacenter основано на правах виртуализации. В прошлом у вас был доступ только к определенным ролям и компонентам в зависимости от приобретенной редакции Windows Server. Сейчас независимо от разворачиваемой редакции вы всегда будете иметь полный доступ ко всем ролям и компонентам, с самого начала намного облегчая понимание того, на что распространяются ваши права.

  Поскольку технология Hyper-V впервые была реализована еще в Windows Server 2008 SP1, в определенные ограничения вносились изменения, не привлекавшие к себе большого внимания, например, в количество поддерживаемых процессорных ядер или число функционирующих виртуальных машин. Хотя на момент написания этой книги приведенная в ней информация корректна, не исключено, что упомянутые здесь ограничения снова изменились, поэтому за актуальной информацией о текущем наборе возможностей обращайтесь на сайт Microsoft. В табл. 27.2 приведены сведения, действительные на время написания книги.

Таблица 27.2. Список масштабируемости Hyper-V версии Windows Server 2012 R2

Характеристика	Редакции Windows Server 2012 R2 Standard и Windows Server 2012 R2 Datacenter
Максимальный объем физической памяти хоста	4 Тбайт
Максимальное количество логических процессоров хоста	320
Максимальное количество выполняющихся виртуальных машин на хосте	1024
Максимальное количество виртуальных процессоров, функционирующих на хосте	2048
Максимальный объем памяти виртуальной машины	1 Тбайт на одну виртуальную машину
Максимальное количество виртуальных процессоров виртуальной машины	64 на одну виртуальную машину
Максимальное количество хостов в одном кластере	64
Максимальное количество виртуальных машин в одном кластере	8000
Максимальное количество живых миграций	Не ограничивается

Архитектура Hyper-V

К этому времени вы должны иметь общее представление о базовой функциональности Hyper-V. Вам уже известно, для чего используется виртуализация серверов, и какие требования к оборудованию и программному обеспечению должны быть удовлетворены для ее реализации. Тем не менее, чтобы понять механизм действия Hyper-V, а также уметь находить и устранять возможные проблемы, необходимы более глубокие знания того, как спроектировано средство Hyper-V. В этом разделе мы займемся исследованием программной архитектуры Hyper-V.

Возможности ЦП играют критически важную роль при внедрении виртуализации серверов. Модель процессоров Intel/AMD имеет несколько уровней привилегий; эти уровни называются *кольцами*. В этой традиционной модели наивысшей привилегией обладает кольцо 0. Данный уровень используют ядро Windows и драйверы устройств. Процессы в кольце 0 способны обращаться к любому оборудованию системы. В текущих версиях Windows кольца 1 и 2 обычно не применяются. Кольцо 3 имеет самый низкий уровень привилегий. В нем выполняются обычные "пользовательские" программы. На практике это должно означать любой код, который не требует привилегий ядра. Хитрость здесь в том, что ЦП запрещает выполнение в кольце более высокого уровня любого кода, связанного с записью данных, или кода, принадлежащего к кольцу более низкого уровня. Другими словами, это средство аппаратной безопасности.

При развертывании на своем компьютере роли Hyper-V вы создаете архитектуру гипервизора. *Гипервизор* представляет собой программный уровень, который находится между оборудованием и операционными системами, функционирующими на хосте. Это известно как подход с "голым железом": виртуализация на самом низком из возможных уровней. Главная цель гипервизора заключается в том, чтобы создать изолированные среды выполнения (разделы) для всех операционных систем.

Согласно этой функции, он отвечает за арбитраж доступа к оборудованию. В ходе развертывания роли Hyper-V хост пару раз перезапускается, чтобы обеспечить размещение Hyper-V поверх оборудования, находящегося в *кольце -1*, как показано на рис. 27.8.

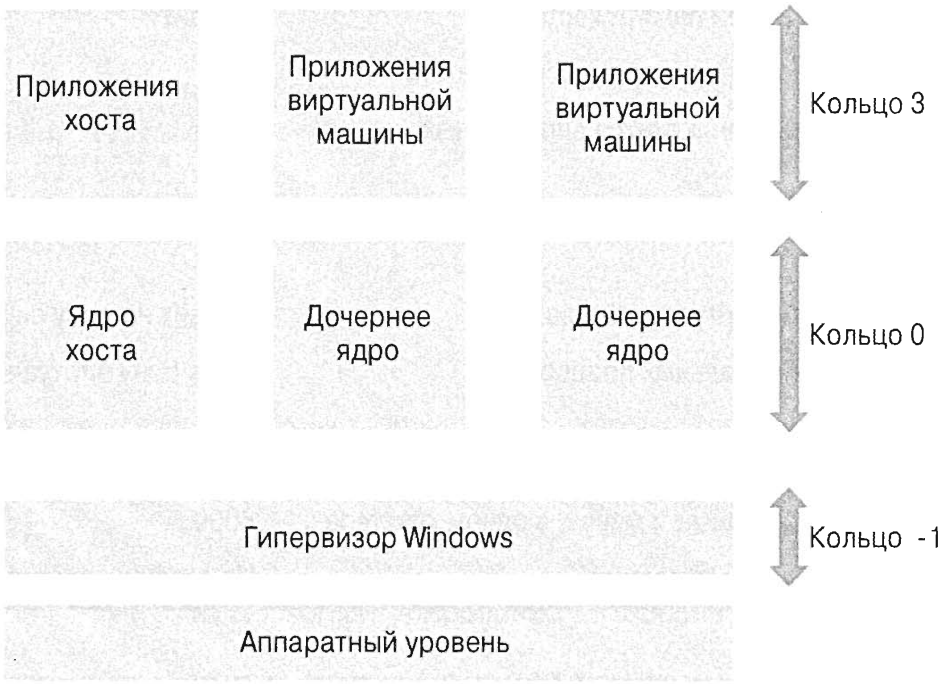


Рис. 27.8. Благодаря гипервизору хост функционирует на том же уровне, что и виртуальные машины: поверх уровня гипервизора

Давайте взглянем на структуру кольца. Кольцо 1 не является обязательным свойством гипервизора, но самые современные гипервизоры его используют. Данное кольцо является главной особенностью дополнений виртуализации центральных процессоров Intel VT и AMD-V. Оно представляет собой относительно новый уровень доступа, который даже выше, чем у кольца 0. Это позволяет всем ядрам действительно функционировать на кольце 0 без подстройки, которая требуется в более старых гибридных моделях, не включающих гипервизор. В результате получается более чистая архитектура, подразумевающая меньшее количество ошибок в коде и в идеальном случае более высокую производительность.

Диаграмма на рис. 27.8 иллюстрирует, что все виртуальные машины созданы равными, однако одна из них "более равна, чем другие": *операционная система хоста* или *управляющая ОС*, которая отвечает за управление и высокоуровневый арбитраж всех виртуальных машин. Она является стандартным владельцем всех аппаратных ресурсов и управляет запуском и остановом *дочерних* разделов.

Гипервизор Hyper-V построен по принципу *микроядра*. Как следует из самого термина, он создавался по возможности как не содержащий ничего лишнего. Гипервизор Hyper-V не имеет кода графического пользовательского интерфейса и достаточно интеллектуален, чтобы делать свою основную работу: управлять памятью и регулировать доступ к оборудованию. В других гипервизорах (не Microsoft) может применяться другой подход. При подходе с монолитным ядром гипервизор содержит драйверы и принимает на себя дополнительную ответственность за взаимодействие между виртуальными машинами. Одно из преимуществ монолитного гипервизора заключается в том, что теоретически он может обеспечивать более высокую максимальную производительность из-за более тесной интеграции с драйве-

рами, посредством которых производится доступ к оборудованию. С другой стороны, если гипервизор не располагает драйверами для имеющегося у вас специального оборудования, то считайте, что вам не повезло. Для зрелых продуктов это не должно быть реальной проблемой. В гипервизоре с микроядром драйверы фактически находятся в родительском разделе, которым в случае Hyper-V должен быть сервер Windows Server 2012. Этот родительский раздел содержит драйверы, поэтому, если для вашего оборудования предусмотрены драйверы для Windows Server 2012, то оно может работать с Hyper-V.

Давайте перейдем от общих рассуждений к рассмотрению конкретных подробностей Hyper-V в Windows Server 2012. Гипервизор Hyper-V разрабатывался Microsoft с учетом перечисленных ниже целей.

- Гипервизор должен по возможности не содержать ничего лишнего.
- Он должен быть управляемым с применением открытых API-интерфейсов.
- Надежность и производительность должны быть близки к максимальным.
- Гипервизор должен быть встроенным компонентом сервера Windows.

В результате разработки получилось то, что схематично представлено на рис. 27.9.

В нижней части диаграммы показаны уже знакомые уровни оборудования и гипервизора. В режиме ядра функционирует ядро управляющей ОС наряду с тремя разными разделами виртуальных машин (*гостевых ОС*). Начнем с раздела управляющей ОС.

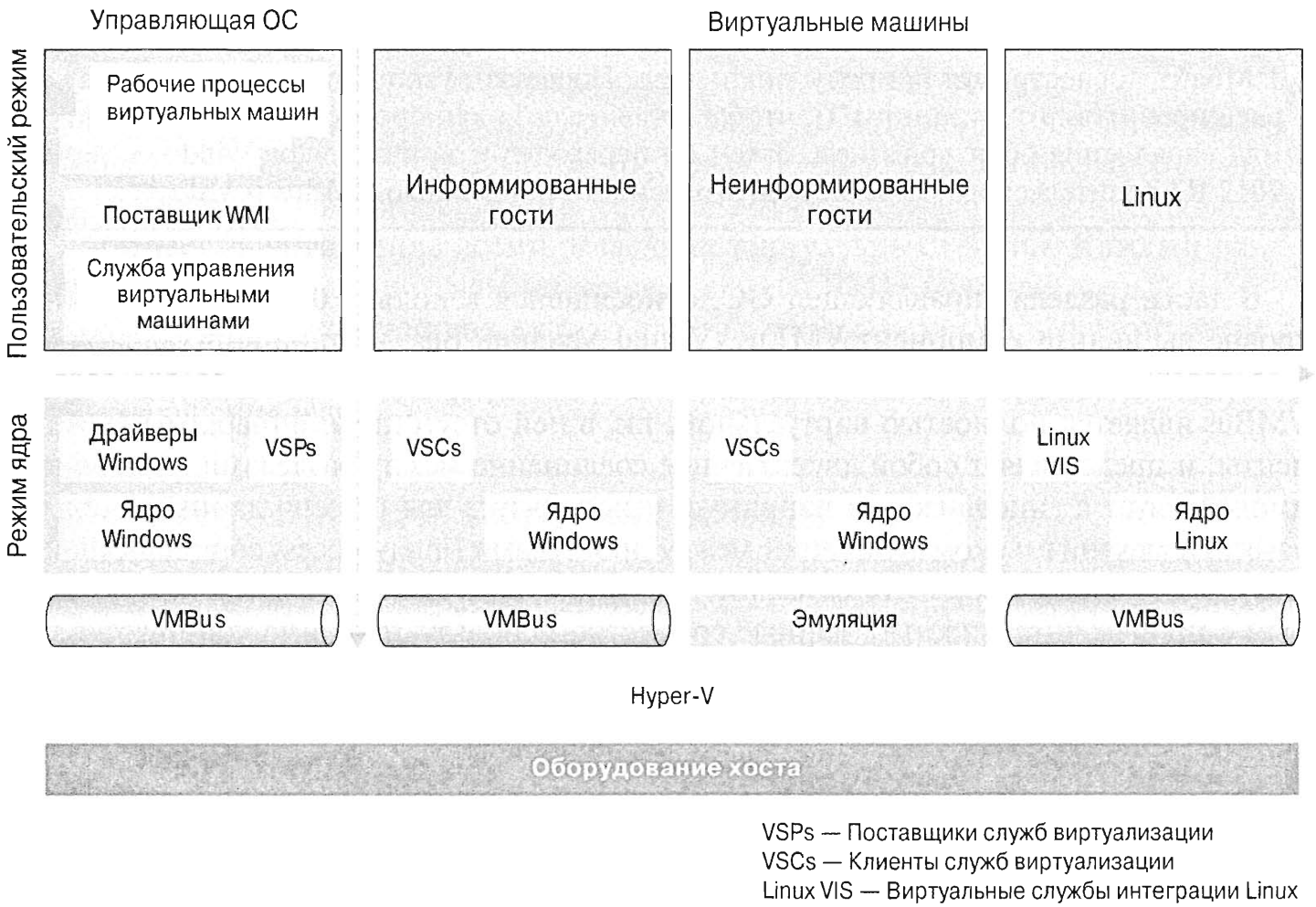


Рис. 27.9. Архитектура Hyper-V: гипервизор, виртуальные машины и отношения между ними

Раздел управляющей ОС

Этот раздел в действительности состоит из двух частей. Нижний блок выполняется в кольце 0, или в режиме ядра. Он содержит четыре блока, три из которых являются новыми в нашем обсуждении: VMBus, драйверы Windows и поставщики служб виртуализации (virtualization service provider — VSP). Верхний блок соответствует коду кольца 3, или пользовательскому режиму. Здесь показаны только компоненты, имеющие отношение к Hyper-V. Чтобы поддерживать гипервизор, раздел управляющей ОС должен функционировать с версией Windows Server, которая способна выполнять Hyper-V (это означает Windows Server 2008 или последующие версии). В зависимости от ваших потребностей это может быть полная версия с графическим пользовательским интерфейсом или редакция Server Core.

Процесс установки и загрузки гипервизора

Вас может заинтересовать данная проблема "первичности курицы и яйца": для управления гипервизором требуется родительский раздел Windows Server с Hyper-V, но родительскому разделу для того, чтобы он мог что-нибудь делать, необходим гипервизор. Вот что происходит: вы сначала устанавливаете редакцию Windows Server 2012 R2 с Hyper-V вроде Standard или Datacenter. В этот момент гипервизора пока нет. При включении роли Hyper-V ОС Windows установит все требуемые программные компоненты, такие как VMBus и VSP, но не гипервизор. Вместо этого Windows устанавливает драйвер устройства `Hvboot.sys`, который загрузит фактический гипервизор при следующей загрузке системы. Это может быть либо гипервизор `%Systemroot%\System32\Hvax64.exe` для процессоров AMD, либо гипервизор `%Systemroot%\System32\Hvix64.exe` для Intel. Размеры каждого из этих файлов не превышают 1 Мбайт, иллюстрируя природу микроядра. После загрузки гипервизор использует расширения виртуализации ЦП, чтобы вставить себя как процесс кольца -1, принимая управление оборудованием. Затем он переходит к загрузке ядра Windows Server 2012 R2 родительского раздела, подготовленного с помощью VMBus и VSP.

В части раздела управляющей ОС, относящейся к кольцу 0, на самом нижнем уровне вы видите компонент VMBus (Virtual Machine Bus — шина виртуальной машины). Как следует из названия, VMBus применяется для обмена данными. Шина VMBus является полностью виртуальной, т.к. в ней отсутствуют аппаратные компоненты, и представляет собой двухточечное соединение между разделами. Она не взаимодействует с гипервизором напрямую и использует для обмена данными общую память и механизмы коммуникаций между процессами (inter-process communication — IPC). Здесь следует обратить внимание на то, что по очевидным причинам, связанным с производительностью, данные совместно используются, а не копируются. По сравнению со старой гибридной моделью VMBus является важным отличием.

Драйверы Windows расположены поверх VMBus, но только в разделе управляющей ОС. Это указывает на то, что в дочерних разделах внешние драйверы не устанавливаются. Драйверы Windows в этом контексте являются обычными драйверами, которые поставляются с каждой версией Windows — для дисковых устройств, шины SCSI, RAID, сети, видео и т.д.

Ключевым фактором производительности Hyper-V является сочетание поставщика службы виртуализации (VSP) в разделе управляющей ОС и клиента службы

виртуализации (virtualization service client — VSC) в разделе виртуальных машин. Родительский компонент VSP отвечает за трансляцию данных между шиной VMBus и драйверами Windows. В действительности VSP представляет собой комбинацию множества модулей для каждого типа оборудования: внешней памяти, сетевого оборудования, видео, устройств ввода и т.п. Это имеет смысл, поскольку каждый из этих типов оборудования предъявляет очень разные требования, касающиеся скорости передачи и объема обрабатываемых данных. В табл. 27.3 приведен обзор наиболее важных файлов гипервизора.

Таблица 27.3. Файлы, относящиеся к гипервизору

Функция	Путь к файлу
Драйвер начальной загрузки гипервизора	`%systemroot%\system32\drivers\hvboot.sys`
Гипервизор (для AMD)	`%systemroot%\system32\hvax64.exe`
Гипервизор (для Intel)	`%systemroot%\system32\hvix64.exe`
Служба Virtual Machine Management (Управление виртуальными машинами)	`%systemroot%\system32\vmms.exe`
Рабочий процесс виртуальной машины	`%systemroot%\system32\vmwp.exe`

Эти модули VSP объединяются в пары с соответствующими модулями VSC. Например, модуль внешней памяти VSC будет взаимодействовать с модулем внешней памяти VSP. В то время как VSC взаимодействует только с VSP в родительском разделе, VSP взаимодействует со всеми компонентами VSC. Разработчики из компаний, отличных от Microsoft, могут проектировать и строить собственные модули, т.к. соответствующие API-интерфейсы открыты всем желающим.

После обсуждения части раздела управляющей ОС, которая относится к режиму ядра, можно переходить к рассмотрению компонентов пользовательского режима. Служба управления виртуальными машинами (Virtual Machine Management — VMM) отвечает за управление всеми разделами виртуальных машин. Каждый раз, когда запускается раздел виртуальных машин, служба VMM начинает новый рабочий процесс виртуальной машины (virtual machine worker — VMW) для этого гостя. На самом деле этот процесс не выполняет какую-либо работу кроме мониторинга, запуска, завершения и т.п.

Какой процесс "запускает" виртуальную машину?

В отличие от похожих рабочих процессов в гибридной модели, процесс VMW в действительности не "запускает" раздел виртуальных машин. Он просто управляет им. На основании коэффициента использования ЦП процессом VMW нельзя сказать, выполняет ли гость какую-то работу, за исключением передачи данных унаследованными (неинформированными) устройствами.

Фактически все разделы виртуальных машин могут отнимать до 100% загрузки ЦП, не демонстрируя при этом каких-либо признаков деятельности непосредственно в разделе управляющей ОС. Чтобы выяснить, чем занимается интересующий вас гость, вы должны либо подключиться к нему напрямую с применением обычных инструментов управления сервером, т.е. счетчиков монитора производительности, либо получить доступ к поставщику WMI в разделе управляющей ОС.

Последним компонентом раздела управляющей ОС является поставщик WMI. Несколько лет тому назад в Microsoft решили, что инструменты WMI (Windows Management Instrumentation — инструментальные средства управления средой Windows) должны стать предпочтительным способом управления и мониторинга системными ресурсами, и Hyper-V не является исключением. Поставщик WMI открыто документирован в MSDN и предоставляет следующую функциональность:

- отчеты о состоянии мыши и клавиатуры;
- доступ к системе BIOS виртуальной машины;
- управление и чтение конфигурации сети, последовательных устройств, внешней памяти, гостевых разделов и т.д.;
- чтение текущих свойств ЦП;
- управление состоянием питания.

Этот набор возможностей позволяет понять, что поставщик WMI обладает всей функциональностью, требуемой для управления средой Hyper-V. На самом деле ожидается, что большинство систем управления для Hyper-V будут использовать WMI. К сожалению, интерфейс WMI слишком мало задействован напрямую при выполнении большинства действий, связанных с повседневным управлением. Эффективно применять его смогут только те, кто имеет богатый опыт программирования для WMI, но с учетом того, что в PowerShell реализуется все больше и больше функциональности, способствующей легкости управления и администрирования, это определенно путь, ведущий нас вперед.

Два API-интерфейса Hyper-V

В действительности Hyper-V располагает двумя встроенными API-интерфейсами. Кроме WMI в Hyper-V имеется API-интерфейс Hypervisor — низкоуровневый интерфейс, который позволяет конфигурировать гипервизор, управлять состояниями разделов, обрабатывать коммуникации между разделами (VMBus), поддерживать планировщик и т.д. Вообще говоря, интерфейс Hypervisor предназначен для тех, кто разрабатывает собственные модули VSP/VSC и пишет другой код системного уровня. Как администратору вам вряд ли придется иметь дело с API-интерфейсом Hypervisor напрямую.

Чтобы завершить обзор раздела управляющей ОС, вы должны получить представление о службах, выполняющихся в родительском разделе Hyper-V (табл. 27.4).

Разделы виртуальных машин (гостей)

Прояснив большую часть архитектуры Hyper-V, нам осталось только обсудить раздел виртуальных машин, причем некоторые элементы этого раздела уже были раскрыты. В первом дочернем разделе на рис. 27.9 функционирует операционная система, которая осведомлена о гипервизоре. В Microsoft такую ОС называют *информированным гостем*, тогда как другие могут называть ее *паравиртуализированной*. По существу она имеет интерфейс VMBus и клиент службы виртуализации (Virtualization Service Client).

Таблица 27.4. Службы Hyper-V

Служба	Тип запуска	Описание
Hyper-V Data Exchange Service (Служба обмена данными Hyper-V)	Вручную	Предоставляет механизм обмена данными между виртуальной машиной и ОС, функционирующей на физическом компьютере
Hyper-V Guest Service Interface (Интерфейс гостевых служб Hyper-V)	Вручную	Предоставляет интерфейс для взаимодействия хоста Hyper-V с конкретными службами, функционирующими внутри виртуальной машины
Hyper-V Guest Shutdown Service (Служба завершения работы гостей Hyper-V)	Вручную	Предоставляет механизм для завершения работы ОС виртуальной машины из интерфейсов управления на физическом компьютере
Hyper-V Heartbeat Service (Служба работоспособности Hyper-V)	Вручную	Отслеживает состояние виртуальной машины, генерируя сигналы о работоспособности через регулярные интервалы. Эта служба помогает идентифицировать запущенные виртуальные машины, которые перестали реагировать
Hyper-V Remote Desktop Virtualization Service (Служба виртуализации удаленных рабочих столов Hyper-V)	Вручную	Предоставляет платформу для коммуникаций между виртуальной машиной и операционной системой, функционирующей на физическом компьютере
Hyper-V Time Synchronization Service (Служба синхронизации времени Hyper-V)	Вручную	Синхронизирует системное время данной виртуальной машины с системным временем физического компьютера
Hyper-V Virtual Machine Management (Управление виртуальными машинами Hyper-V)	Автоматически	Служба управления для Hyper-V, которая обеспечивает выполнение множества виртуальных машин

Прежде всего, возникает вопрос: как этот раздел виртуальных машин стал информированным? В разделе управляющей ОС вы установили роль Hyper-V, но вполне очевидно, что на стороне гостя необходимо сделать что-то еще, чтобы предоставить требуемые программные компоненты. Программное обеспечение Hyper-V для виртуальных машин принято называть компонентами интеграции (Integration Components), а в документации Microsoft на него ссылаются как на клиентов службы виртуализации (Virtualization Service Client — VSC). Версия VSC виртуальной машины должна соответствовать версии сервера Hyper-V хоста.

Встроенной версией клиентов VSC располагают только гости, функционирующие под управлением ОС Windows Server 2008 и выше, хотя эту версию потребуется модернизировать для соответствия текущей версии Hyper-V хоста; примером может служить выполнение гостевой виртуальной машины Windows Server 2008 на хосте Windows Server 2012 R2. Для других операционных систем понадобится явно установить клиенты VSC. Один из способов сделать это предусматривает вставку файла ISO с клиентами VSC в виртуальную машину. Этот файл ISO входит в комплект поставки Hyper-V.

Клиенты VSC в действительности представляют собой набор модулей, установленных в папку `%systemroot%\Virtualization\<версия>` внутри раздела виртуальных машин. Для каждого обновления клиентов VSC предназначена отдельная папка *<версия>*.

Информированность бывает двух видов

Информированность существует в двух вариантах — универсальном и специализированном. Вообще говоря, операционная система, которая работает с интерфейсом VMBus, считается информированным гостем. Более старые системы, такие как Windows XP и Windows Server 2003, которые требуют предварительной установки клиентов VSC, считаются неинформированными гостями. К ядру применяется специфичный вариант: если ядру изначально известно о гипервизоре, то говорят, что операционная система имеет *информированное ядро*. Это относится к любому гостю, работающему под управлением Windows Server 2008 или выше для серверных гостевых ОС и Vista SP1 и выше для клиентских гостевых ОС. Преимущество информированного ядра заключается в том, что оно может еще больше оптимизировать доступ к VMBus. Например, ОС Windows Server 2012 может обходить некоторые внутренние программные уровни для доступа к сети и дискам, когда она выясняет, что данные предназначены виртуальному устройству.

Внимательно присмотревшись к функциональности VSC, вы заметите, что в действительности она разделена на две части. С одной стороны, имеются драйверы для внешней памяти, видео и сети. Еще один драйвер напрямую интегрирован с ядром, чтобы оптимизировать его производительность при выполнении в качестве виртуальной машины. С другой стороны, есть многоцелевой исполняемый файл службы (`vmicsvc.exe`), который запускается четыре раза с разными аргументами для предоставления следующей функциональности.

- **Operating System Shutdown Service** (Служба завершения работы операционной системы). По запросу родительского раздела эта служба завершит работу виртуальной машины в установленном порядке.
- **Heartbeat Service** (Служба работоспособности). Родительскому разделу необходим способ сообщения о том, что дочерний раздел по-прежнему функционирует. Если родительский раздел больше не получает сигналы работоспособности, у него есть основания предположить, что у дочернего раздела возникла серьезная проблема.
- **Time Synchronization Service** (Служба синхронизации времени). Дочерний раздел не имеет прямого доступа к аппаратным часам. Эта служба предлагает альтернативу. Не применяйте эту возможность в среде домена Active Directory, т.к. она обладает собственной инфраструктурой синхронизации времени.
- **Data Exchange Service** (Служба обмена данными). Эта служба представляет собой единственный способ, с помощью которого пользовательские процессы (кольцо 3) в родительских и дочерних службах могут взаимодействовать за рамками обычных устройств. Она работает через определенные ключи реестра.
- **Backup (Volume Snapshot) Service** (Служба резервного копирования (создания снимков тома)). Эта служба функционирует вместе со службой резервного копирования в родительском разделе для предоставления согласованных резервных копий родительского и дочернего разделов с применением технологии VSS.
- **Guest Services** (Гостевые службы). Это новый клиент VSC, который доступен только на виртуальных машинах Windows Server 2012 R2 поколения 2. По умолчанию она отключена. После ее включения появляется возможность копировать файлы на работающую виртуальную машину, не используя сетевое подключение.

Полезно отметить, что клиенты VSC не могут быть сконфигурированы из раздела виртуальных машин. Это можно сделать только через раздел управляющей ОС — с помощью консоли управления Hyper-V, посредством PowerShell либо с помощью интерфейса WMI.

Продолжая обсуждение разделов виртуальных машин, рассмотрим второй дочерний раздел, показанный на рис. 27.9, который обозначен как "Неинформированные гости". На самом деле это означает, что операционная система является неинформированной. Причина может быть связана с тем, что клиенты VSC не установлены или недоступны.

Например, у вас может быть установлена ОС Windows Server 2003 в качестве унаследованной, но информированной системы. Для более старых неподдерживаемых систем, таких как Windows 2000 Server или Windows NT 4, в Microsoft не создавали клиенты VSC, хотя в принципе сторонние разработчики могли бы при необходимости сделать это. Отсутствие клиентов VSC не означает, что виртуальная машина не может быть установлена или запущена, однако из этого вытекает то, что она никогда не достигнет высокого уровня производительности, и не будет поддерживаться, если возникнут какие-то проблемы. С другой стороны, многие унаследованные ОС должны функционировать нормально на современном оборудовании, даже если они виртуализированы. Из диаграммы на рис. 27.9 следует, что неинформированная система не содержит VMBus или поставщика VSC и взамен использует эмуляцию.

Третий, и последний, тип разделов виртуальных машин работает под управлением операционной системы производства не Microsoft, такой как Linux, использующей виртуальные службы интеграции Linux (Virtual Integration Services — VIS). Это драйверы уровня ядра, которые предоставляют доступ к компоненту VMBus и предлагают практически всю функциональность клиентов VSC для виртуальных машин Microsoft. Эти компоненты Linux VIS созданы разработчиками из Microsoft специально для данной операционной системы, так что они полностью поддерживаются в случае возникновения каких-то затруднений при запуске виртуальных машин подобного типа в Hyper-V. От информированной системы такого рода можно ожидать производительности, близкой к оптимальной.

Установка и конфигурирование Hyper-V

В этом разделе вы узнаете, как установить Hyper-V на сервере Windows Server 2012 R2. Мы также обсудим разные настройки, доступные в консоли управления. По ходу дела вы ознакомитесь с рядом практических рекомендаций, которые помогут при работе Hyper-V.

К данному времени вы уже должны знать, как установить сервер, присоединить его к домену и т.п. Именно поэтому мы опускаем подробности, относящиеся к базовой установке, и переходим непосредственно к той части, которая касается Hyper-V. В табл. 27.5 приведена предполагаемая конфигурация для тестовой среды. Если для вашего случая подходят другие настройки, можете свободно изменять их по своему усмотрению. В этой пошаговой процедуре применяется ОС Windows Server 2012 R2, но если вы используете Windows Server 2012, то вряд ли обнаружите сколько-нибудь существенные изменения в процессе установки.

Таблица 27.5. Система хоста Hyper-V

Параметр	Конфигурация
Внутренняя память	8 Гбайт; практическим минимумом является объем 4 Гбайт
Жесткие диски	Два диска по 200 Гбайт или больше. Для тестовой системы достаточно одного диска, но это приведет к снижению производительности
Разделы	Диск 1: система на `C:\` Диск 2: зарезервирован для Hyper-V на `D:\`
Сеть	Для производственной среды — как минимум две сетевые интерфейсные платы 1 Гбит/с. Для тестовой (но не производственной) среды достаточно одной платы
Операционная система	Редакции Windows Server 2012 R2 или Windows Server 2012 с доступным средством Hyper-V
Тип установки	Чтобы воспроизвести приведенные здесь примеры, требуется полный графический пользовательский интерфейс
Имя хоста	`HOST2012DEMO`, если вы хотите следовать примерам; вообще говоря, подойдет любое другое имя
Конфигурация IP	Адрес: 192.168.1.54/24; шлюз: 192.168.1.1; DNS: 192.168.1.51
Active Directory	Для производственной среды рекомендуется инфраструктура Active Directory, присоединенная к домену. Рабочая группа пригодна для целей тестирования, хотя конфигурирование дистанционного управления затруднительно и намного проще, если вы просто используете Active Directory

Едва ли не единственное решение, которое вам нужно принять перед установкой роли Hyper-V — какую сетевую интерфейсную плату использовать для управления хостом Hyper-V. Идея заключается в том, чтобы иметь на хосте, по меньшей мере, две сетевых интерфейсных платы, но при реальной необходимости можно обойтись и одной платой. Правда, не рассчитывайте в этом случае на выдающуюся производительность. Когда доступны две сетевых платы, выделите одну из них для управления хостом, а другую — для сетевого трафика виртуальной машины. Чтобы сделать такое разделение очевидным, достаточно переименовать сетевые подключения, как показано на рис. 27.10.

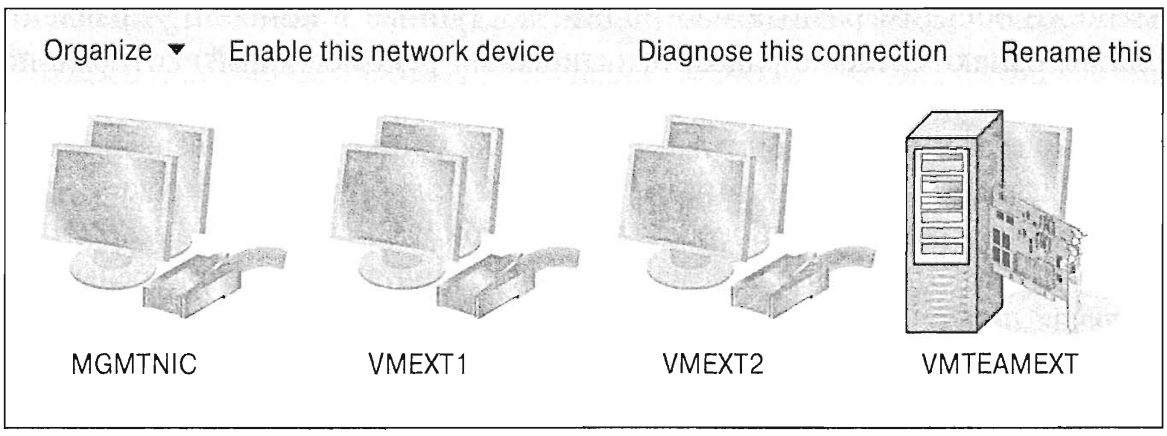


Рис. 27.10. Переименование сетевых подключений для отражения их роли на хосте Hyper-V

Давайте начнем с установки роли Hyper-V.

1. Установите сервер с использованием параметров, указанных в табл. 27.5, в качестве руководства по версии, имени сервера, конфигурации IP и т.д.

   Обеспечьте наличие выделенных дисков или разделов для данных Hyper-V.

2. Присоедините компьютер к домену, если хотите воспроизвести некоторые из рассматриваемых позже примеров.

   Повсеместно в этой книге применяется домен bigfirm.com.

   После установки серверной ОС на хосте Hyper-V все готово к установке роли Hyper-V. Во время установки подключение к сети будет разорвано один или два раза из-за обновления сетевых компонентов.

3. Войдите в систему Windows Server 2012 R2 с применением учетной записи, которая имеет разрешения администратора домена, и в окне диспетчера серверов при выбранном пункте меню Local Server (Локальный сервер) щелкните на ссылке Add roles and features (Добавить роли и компоненты).

4. На экране Before You Begin (Прежде чем начать) щелкните на кнопке Next (Далее).

5. На экране Select Installation Type (Выбор типа установки) проверьте, что выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов), и щелкните на кнопке Next.

6. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов), убедитесь, что ваш сервер выделен в разделе Server Pool (Пул серверов), и щелкните на кнопке Next.

7. На экране Select Server Roles (Выбор серверных ролей) выполните прокрутку экрана вниз до тех пор, пока не найдете в списке Roles (Роли) элемент Hyper-V, и отметьте флажок рядом с ним.

   Вам будет предложено добавить некоторые требуемые здесь компоненты, такие как Hyper-V Management Tools (Инструменты управления Hyper-V).

8. В открывшемся окне щелкните на кнопке Add Features (Добавить компоненты).

9. Для продолжения щелкните на кнопке Next.

10. На экране Select Features (Выбор компонентов) оставьте выбор компонентов в том виде, как есть, и два раза щелкните на кнопке Next.

11. На экране Create Virtual Switches (Создание виртуальных коммутаторов), показанном на рис. 27.11, выберите сетевую интерфейсную плату для виртуального коммутатора, который вы собираетесь использовать для своих виртуальных машин.

    Более подробные сведения о виртуальных коммутаторах вы найдете далее в этой главе, но если кратко, то для каждой сетевой интерфейсной платы, которую вы выбрали здесь, будет создан один виртуальный коммутатор. При наличии двух и более сетевых плат вы должны оставить одну из них неотмеченной (в рассматриваемом примере это MGMTNIC). Неотмеченная сетевая плата не будет иметь связанного с ней коммутатора и может применяться для управления хостом. Если есть только одна сетевая плата, выберите ее. Если вы не

выберете ни одной сетевой платы, то у ваших виртуальных машин не окажется простого способа взаимодействия с внешним миром, хотя это можно исправить позже. Поскольку мы уже упоминали о необходимости назначать сетевым подключениям осмысленные имена, теперь легко выбрать одно из них, которое будет использоваться для сетевого трафика виртуальных машин.

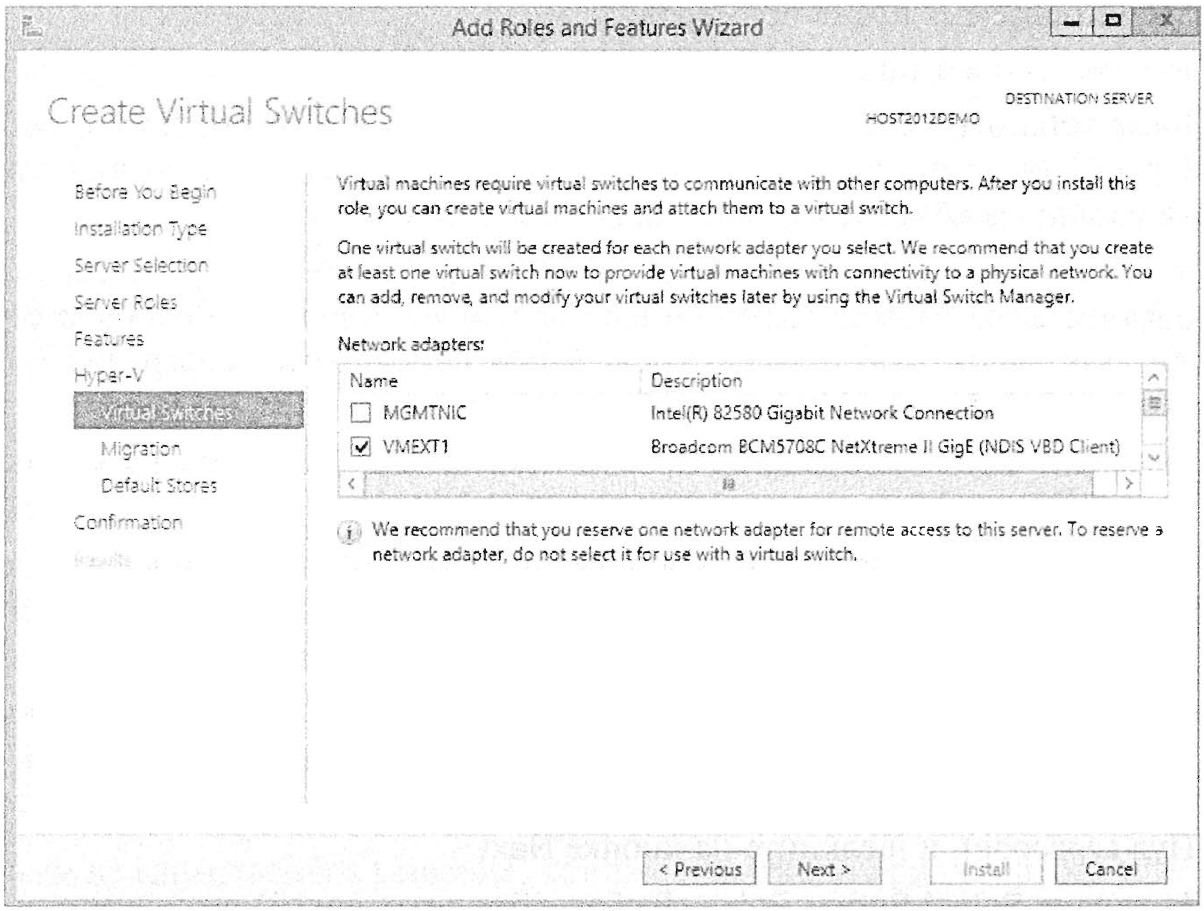


Рис. 27.11. Выберите одну сетевую интерфейсную плату, чтобы применять ее для трафика виртуальных машин. Неотмеченная сетевая плата используется для управления хостом Hyper-V

12. Щелкните на кнопке Next, и вы увидите экран Virtual Machine Migration (Миграция виртуальной машины).
13. Оставьте находящийся здесь флажок Allow this server to send and receive live migrations of virtual machines (Разрешить этому серверу отправлять и принимать живые миграции виртуальных машин) неотмеченным и щелкните на кнопке Next.
14. Действуйте с осторожностью на экране Default Stores (Стандартные хранилища), приведенном на рис. 27.12. Именно здесь необходимо указать, где на хосте будут храниться файлы виртуальных жестких дисков и файлы конфигурации виртуальных машин.

    Если доступно более одного диска или тома, то рекомендуется изменить на этом экране стандартные места, чтобы сохранить эти файлы на томе, который имеет достаточный объем дискового пространства для размещения виртуальных машин. Даже в тестовой или испытательной среде нежелательно, чтобы по мере разрастания виртуальных машин исчерпалось бы место в системном разделе `C:\`.

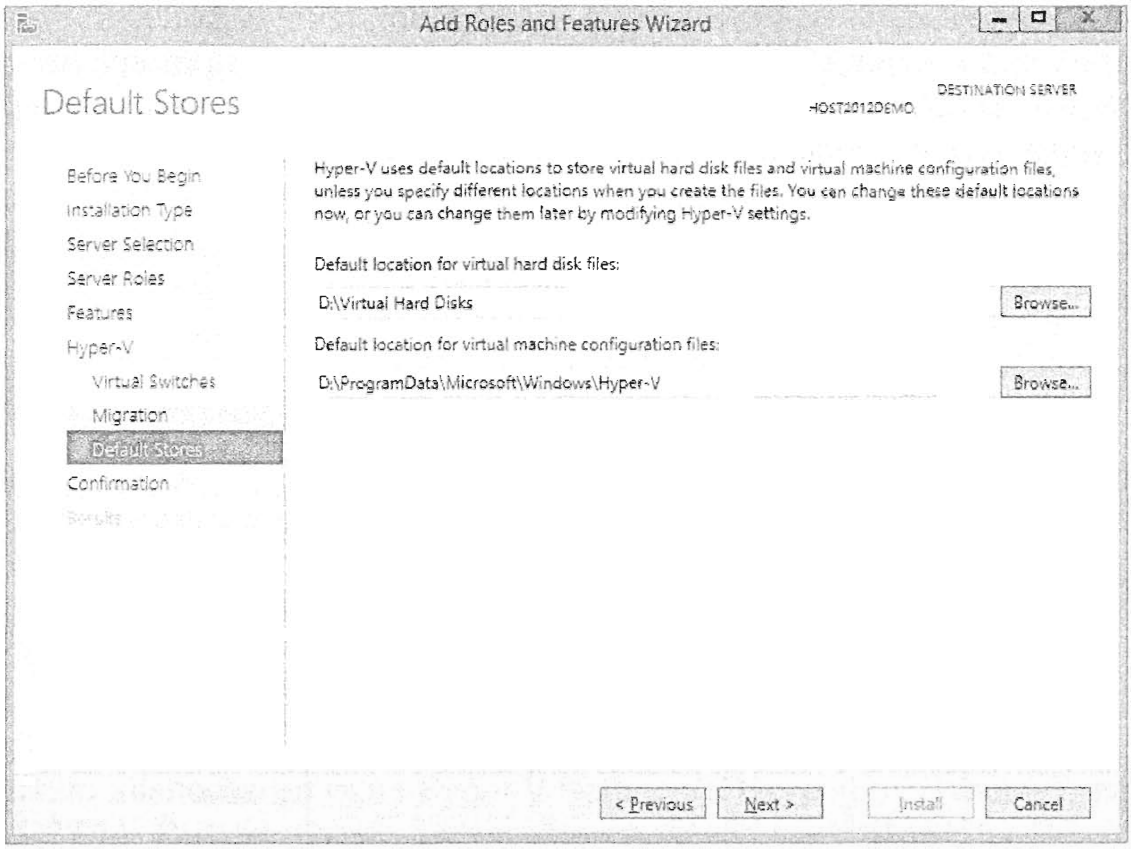


Рис. 27.12. Выбор стандартного хранилища для файлов виртуальных машин

15. Щелкните на кнопке Next, подтвердите настройки, выбранные в мастере, и щелкните на кнопке Install (Установить).
16. После завершения установки перезагрузите сервер; это не должно занять больше нескольких минут.
17. Войдите в систему с применением учетной записи администратора.

После инициализации диспетчера серверов процесс конфигурирования возобновится и завершит оставшиеся действия. Спустя минуту-другую вы должны увидеть в управляющей панели диспетчера серверов роль Hyper-V, подсвеченную зеленым цветом, что указывает на успешное завершение установки.

Перечень контрольных вопросов на предмет соответствия передовому опыту при построении сред Hyper-V

Если вы хотите удостовериться в том, что строите среды Hyper-V в соответствие с рекомендациями передового опыта, ознакомьтесь со статьей "Windows Server 2012 Hyper-V Best Practices (In Easy Checklist Form)" ("Рекомендации передового опыта для Windows Server 2012 Hyper-V (в форме простого перечня контрольных вопросов)") по ссылке `http://blogs.technet.com/b/askpfeplat/archive/2013/03/10/windows-server-2012-hyper-v-best-practices-in-easy-checklist-form.aspx`.

Работа с консолью

Давайте посмотрим, чем мы располагаем на данный момент. Запустите консоль, выбрав в окне диспетчера серверов пункт меню Tools⇨Hyper-V Manager (Сервис⇨Диспетчер Hyper-V). Откроется консоль, которая позволяет управлять на-

стройками среды виртуализации (рис. 27.13). В левой панели консоли представлен хост Hyper-V, подлежащий управлению. В рассматриваемом примере это текущий сервер HOST2012DEMO, но у вас может быть перечислено несколько серверов, если вы хотите управлять несколькими хостами из одной консоли.

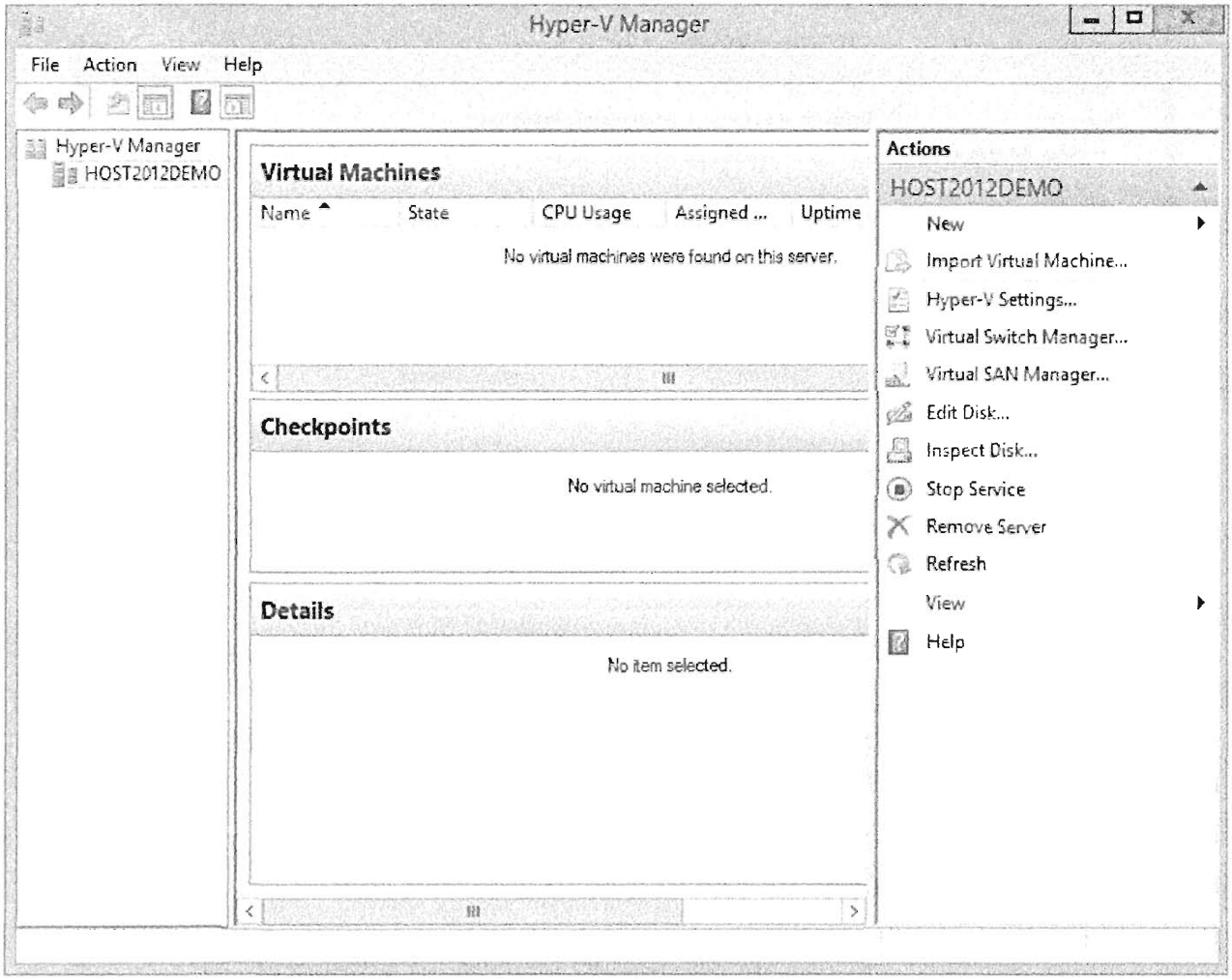


Рис. 27.13. Консоль управления Hyper-V

Средняя панель состоит из трех областей.

- **Virtual Machines (Виртуальные машины).** Здесь отображается список виртуальных машин на этом хосте с указанием некоторых важных параметров, таких как их текущее состояние (работает, выключена, сохранена и т.д.).
- **Checkpoints (Контрольные точки).** Как упоминалось ранее, контрольные точки — это образы дисков на определенные моменты времени, включая состояния памяти и ЦП. Контрольная точка сервера создается, например, в ситуации, когда необходимо иметь возможность отката к такому образу после развертывания пакета обновлений или текущего исправления, которое способно принести больше вреда, чем пользы. Кроме того, контрольную точку можно создать, если конкретная виртуальная машина используется для демонстрационных целей и нужно периодически сбрасывать ее в ее исходное состояние.
- **Details (Подробности).** Здесь содержится дополнительная информация о выбранной в текущий момент виртуальной машине (если есть), такая как общая сводка, память, работа в сети и репликация.

На данный момент наибольший интерес представляет панель Actions (Действия), расположенная справа. Она позволяет управлять разнообразными аспектами среды Hyper-V. Некоторые действия вполне очевидны, например, останов или запуск службы Hyper-V Virtual Machine Management либо удаление из консоли текущего сервера. Другие действия, такие как Virtual Switch Manager (Диспетчер виртуальных коммутаторов), Virtual SAN Manager (Диспетчер виртуальных сетей SAN), Edit Disk (Редактировать диск) и Inspect Disk (Инспектировать диск), не столь очевидны, если ранее вы не имели дела с виртуализацией.

Исследование панели Actions

Если вы хотите грамотно управлять Hyper-V посредством графического пользовательского интерфейса с собственными инструментами, то вам придется работать с панелью Actions консоли управления Hyper-V. Мастер создания виртуального диска (New Virtual Hard Disk Wizard) и мастер импорта виртуальной машины (Import Virtual Machine Wizard) имеют отношение к созданию виртуальных машин и виртуальных дисков, поэтому мы рассмотрим их в последующих разделах.

Щелчок на пункте Hyper-V Settings (Настройки Hyper-V) в панели Actions приводит к открытию диалогового окна Hyper-V Settings (Настройки Hyper-V), показанного на рис. 27.14. Оно позволяет устанавливать такие настройки для Hyper-V, как места хранения виртуальных дисков и конфигурации виртуальных машин, живые миграции и миграции хранилищ, режим расширенного сеанса и репликация.

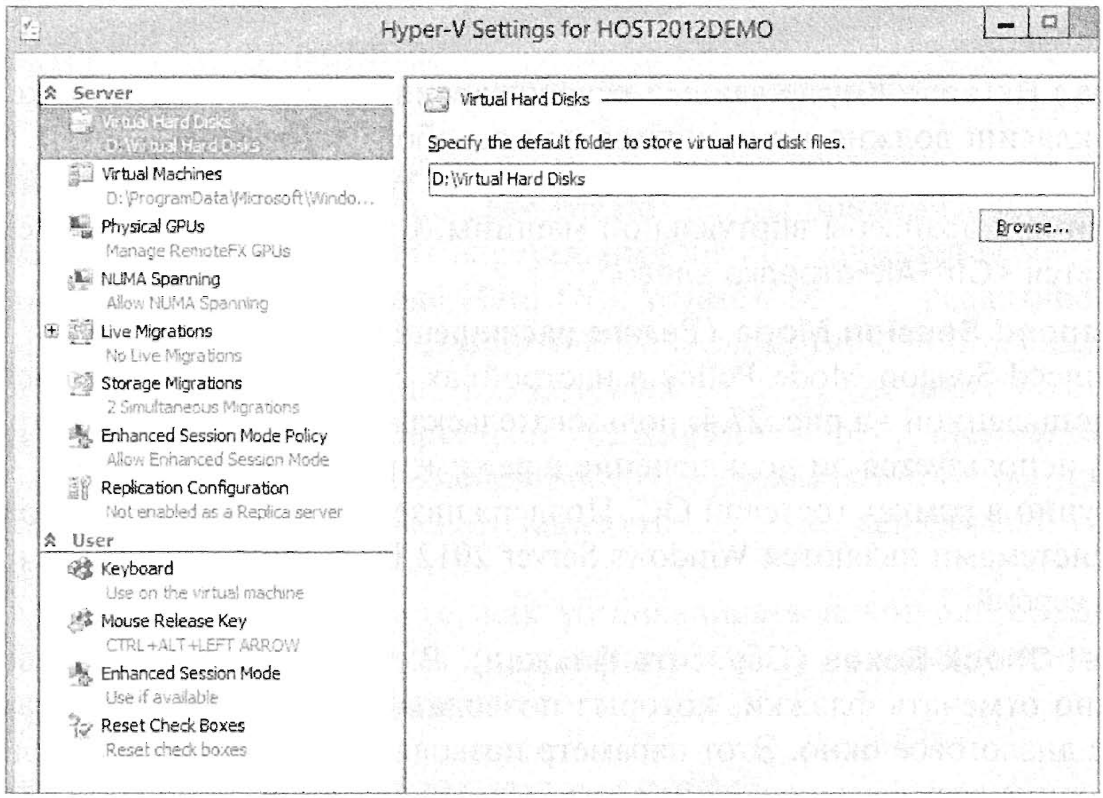


Рис. 27.14. Диалоговое окно Hyper-V Settings

Для каждого параметра отображается его текущая настройка. Как было указано ранее в разделе, посвященном установке Hyper-V, двумя наиболее важными параметрами являются стандартные пути для виртуальных жестких дисков и конфигураций виртуальных машин. Согласно философии Hyper-V, файлы для виртуальных дисков отделены от файлов, содержащих настройки виртуальных машин. Удостоверьтесь,

что устанавливаете их в практичные и отличающиеся друг от друга значения. Мы уже обсуждали параметр Enhanced Session Mode Policy (Политика режима расширенного сеанса), а в следующей главе более подробно рассмотрим параметры, связанные с живыми миграциями, миграциями хранилищ и репликацией.

- **Physical GPUs (Физические графические процессоры).** Этот параметр доступен, только если установлена роль Remote Desktop Virtualization Host (Хост виртуализации удаленных рабочих столов). Он позволяет выбирать физические устройства графических процессоров (graphics processing unit — GPU) вроде NVIDIA и применять их совместно с решением расширенного удаленного рабочего стола (advanced remote desktop — RDP), которое называется RemoteFX.
- **NUMA Spanning (Соединение узлов NUMA).** Этот параметр по умолчанию включен и позволяет виртуальным машинам соединять узлы NUMA (Non-Uniform Memory Architecture — архитектура доступа к неоднородной памяти). Если у хоста есть доступные для использования узлы NUMA, то включение этого параметра обеспечивает для виртуальных машин дополнительную производительность и позволяет одновременно запускать намного больше виртуальных машин, чем на хосте без NUMA.

Все остальные настройки касаются способа работы с Hyper-V и доступа к виртуальным машинам.

- **Keyboard (Клавиатура).** Укажите, как должны вести себя специальные клавиатурные комбинации Windows (например, <Alt+Tab>) в консоли виртуальной машины.
- **Mouse Release Key (Клавиша освобождения мыши).** Укажите, какое сочетание клавиш должно применяться для освобождения фокуса ввода консолью виртуальной машины в ситуации, когда не установлены компоненты интеграции или драйверы виртуальной машины. Стандартным сочетанием клавиш является <Ctrl+Alt+стрелка влево>.
- **Enhanced Session Mode (Режим расширенного сеанса).** Подобно политике Enhanced Session Mode Policy в настройках сервера, обсуждавшейся ранее и представленной на рис. 27.4, пользовательская версия этого параметра определяет, используется ли подключение в режиме расширенного сеанса, когда оно доступно в рамках гостевой ОС. Поддерживаемыми гостевыми операционными системами являются Windows Server 2012 R2 и Windows 8.1 или последующих версий.
- **Reset Check Boxes (Сбросить флажки).** В разных местах консоли Hyper-V можно отмечать флажки, которые позволяют больше не отображать то или иное диалоговое окно. Этот параметр позволяет восстановить первоначальное состояние всех флажков, каким оно было до внесения изменений.

Продолжим обзор панели Actions. Нам предстоит кратко обсудить еще три мастера. Диспетчер виртуальных коммутаторов (Virtual Switch Manager) является центральной точкой управления для виртуальных коммутаторов (или *сетей*). С его помощью можно просматривать, создавать и редактировать сети. Внешние коммутаторы могут быть назначены физическим сетевым интерфейсным платам. Мы обсудим диспетчер виртуальных коммутаторов более подробно позже в главе.

Диспетчер виртуальных сетей SAN (Virtual SAN Manager) позволяет конфигурировать виртуальные сети SAN на основе волоконно-оптических каналов (Fibre Channel), которые по существу группируют вместе физические порты HBA (host bus adapter — хост-адаптер шины) и представляют их виртуальным машинам. Создать виртуальную сеть Fibre Channel SAN удастся только в случае, если мастер обнаружит физические порты Fibre Channel на хосте Hyper-V, поэтому перед попыткой их подключения к виртуальным машинам удостоверьтесь в наличии таких портов и их доступности хосту. На рис. 27.15 видно, что в диспетчере виртуальных сетей SAN можно также определять адреса WWPN (World Wide Port Name — мировое имя порта) и WWNN (World Wide Node Name — мировое имя узла).

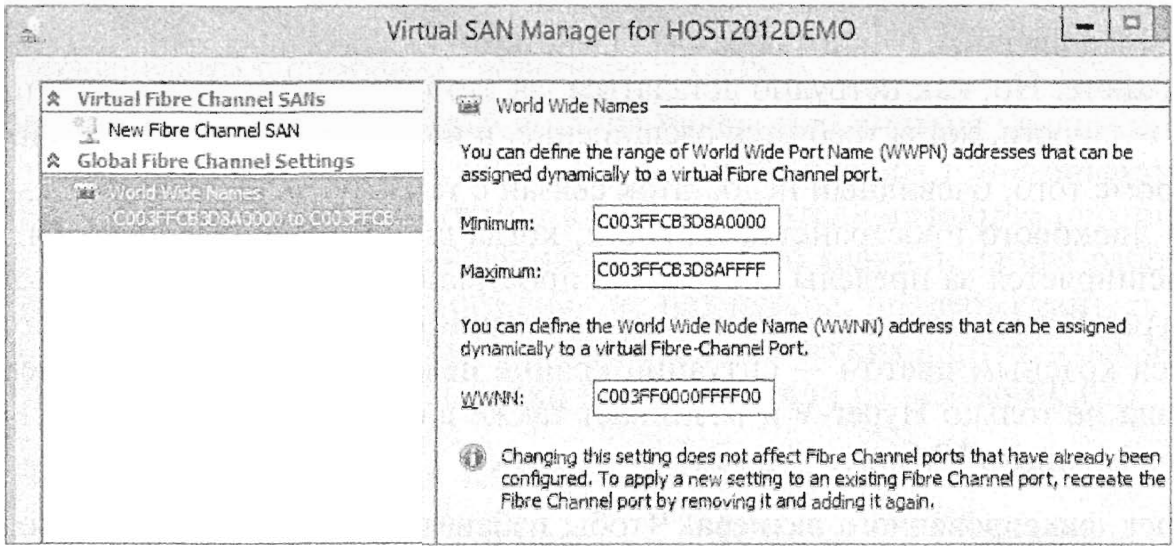


Рис. 27.15. Диспетчер виртуальных сетей SAN

Возможно, это покажется странным, но мастер редактирования виртуального жесткого диска (Edit Virtual Hard Disk Wizard) нельзя применять для создания виртуальных дисков. Построением виртуальных дисков занимается мастер создания виртуального диска (New Virtual Hard Disk Wizard). Мастер редактирования диска позволяет изменить формат с VHD на VHDX, а также тип с динамического на фиксированный, как будет показано в следующем разделе. Он также позволяет увеличить размер и удалить пустое пространство из файла виртуального диска. Наконец, диалоговое окно Inspect Disk (Инспектирование диска) осуществляет проверку диска на согласованность и отображает такие его свойства, как формат, тип, местоположение, имя и размер.

Теперь, когда вы понимаете, как устанавливать и конфигурировать службу Hyper-V, мы обсудим параметры виртуального диска, которые можно настраивать для его работы с виртуальными машинами.

Понятие виртуальных дисков

При создании виртуальной машины вы назначаете виртуальные устройства для сети, видео и т.д. Разумеется, вашей виртуальной машине понадобится и виртуальный диск. Вопрос в том, какой тип диска нужен? Физические диски используются хостом! Решение является простым и очевидным: поскольку вы уже выполняете виртуализацию и эмуляцию, воспользуйтесь вместо физического диска файлом и представьте его виртуальной машине как диск. Виртуальный диск — это не что

иное, как очень большой файл; не забывайте, что при необходимости его размер может достигать 64 Тбайт!

Средство Hyper-V может предложить виртуальной машине много разновидностей виртуальных дисковых систем, и существуют разные сценарии, в которых может требоваться каждая из таких систем.

- **Динамически расширяющийся диск.** Виртуальный диск в этом формате будет выделять пространство на физическом диске строго по мере необходимости, и не более того. Например, вы могли бы выделить 127 Гбайт для виртуальной машины Windows Server 2012, которая после базовой установки будет использовать менее 10 Гбайт. Каждый раз, когда эта виртуальная машина нуждается в дополнительном дисковом пространстве, файл расширяется. Расширяющийся виртуальный диск наилучшим образом задействует дисковое пространство, доступное на хосте. Но, как нетрудно догадаться, за это приходится снижением производительности, когда требуется расширение, и возможной фрагментацией.

  Кроме того, очевидный недостаток связан с тем, что может возникнуть нехватка дискового пространства на хосте, когда динамический виртуальный диск расширяется за пределы доступного пространства. Когда случается подобное, Hyper-V замораживает все виртуальные машины, и журнал событий отображается красным цветом — ситуация крайне нежелательная! Эта проблема присуща не только Hyper-V и возникает также в случае применения дисков Thin Provisioning в VMware.

- **Диск фиксированного размера.** Чтобы избавиться от накладных расходов, характерных для динамически расширяющихся дисков, вы можете использовать диск фиксированного размера. Полный размер виртуального диска будет выделен при его создании, поэтому вы можете без труда выяснить, сколько физического пространства задействовано под виртуальные машины. Как правило, этот формат является рекомендуемым для большинства производственных нагрузок.

  При создании такого диска создается файл указанного вами полного размера. Во время создания он заполняется двоичными нулями. В зависимости от размера это может занять некоторое время. Диск фиксированного размера широко рекомендуется для стандартного применения в любых производственных системах.

- **Разностный диск.** Это интересная возможность в случае, когда между двумя виртуальными дисками имеется отношение “родительский–дочерний”. Родительский диск является статическим эталоном только для чтения. На разностном (дочернем) диске хранятся все изменения, касающиеся родительского диска. Преимущество такого подхода заключается в экономии дискового пространства на хосте и возможности оперативного создания новой виртуальной машины. Однако если виртуальная машина, использующая разностный диск, записывает много новых данных, то преимущество, связанное с экономией дискового пространства, быстро исчезнет. Очевидно, что такой подход подходит только для целей тестирования.

- **Диск прямого доступа.** Последняя разновидность — диск прямого доступа, который получается при назначении физического диска специально для применения виртуальной машиной. Это возможно, когда диск не используется хостом. Диски прямого доступа позволяют подключить виртуальную машину непосредственно к сети SAN или к целевому диску iSCSI. Чтобы выделить физический диск виртуальной машине, он должен восприниматься как физический диск на машине хоста Windows. Это может быть локальный диск, диск в сети SAN, диск iSCSI и т.д. Он не может быть разделом. В действительности он должен быть полноценным диском, видимым в диспетчере дисков. Кроме того, чтобы была возможность применять такой диск в виртуальной машине, он должен находиться в автономном режиме на хосте, чтобы предотвратить его использование этим хостом. Режим диска — автономный или онлайновый — устанавливается с помощью диспетчера дисков.

  Вообще говоря, диск прямого доступа будет применяться только в определенных сценариях кластеризации, когда вам необходим том с объемом более 64 Тбайт либо IT-администратор или руководитель являются параноиками, настаивающими на использовании физического хранилища для рабочей нагрузки. Если в дисках прямого доступа нет нужды, придерживайтесь применения нормальных фиксированных или динамических виртуальных дисков и позвольте хосту монтировать диски в сети SAN или на целевом iSCSI.

Виртуальные диски и их контроллеры

Как было сказано в разделе "Что нового в Hyper-V версии Windows Server 2012 R2?", в вашем распоряжении появился новый формат файла *виртуального диска*. В Windows Server 2012 его обычным расширением является `.vhdx`, а в более ранних версиях продуктов виртуализации Microsoft для виртуальных дисков использовался формат `.vhd`. Еще важнее то, что эта структура опубликована и может свободно применяться всеми желающими. С точки зрения диска данная спецификация является низкоуровневой; это значит, что она не предполагает наличия в виртуальной машине файловой системы любого типа. Виртуальная машина может работать под управлением Windows с файловыми системами NTFS и FAT32 или Linux с EX2, ReiserFS или какой-то другой файловой системой, которая будет разработана в будущем. Открытая спецификация файлов VHDX и VHD означает, что их можно использовать для продуктов виртуализации от других компаний, и каждый может разрабатывать инструменты для их поддержки.

ОС Windows обращается к дискам посредством контроллеров, и виртуальная машина, функционирующая на Hyper-V, ничем в этом смысле не отличается. Двумя распространенными типами являются ныне действующие контроллеры IDE и SCSI. На физической машине системы SCSI в целом лучше работают на сервере. Диски SCSI не только быстрее дисков IDE (если выражаться очень обобщенно!), но интерфейс SCSI был спроектирован для обработки многих запросов ввода-вывода одновременно. В информированной виртуальной машине передача данных и IDE, и SCSI быстро транслируется в запросы VMBus, которые, в свою очередь, зависят от системы хранения хоста. По существу файлу `.vhdx` ничего не известно о контроллере. Это значит, что тот же самый файл `.vhdx` может применяться и с контроллером IDE и SCSI.

Фиксированный или динамический VHDX: какой тип виртуального диска лучше?

Если вы знакомы с Hyper-V и самостоятельно проводили исследования типов виртуальных дисков в Windows Server 2012 R2, но не смогли уловить, когда должны использоваться фиксированные, когда динамические, а когда диски прямого доступа, то знайте, что вы не одиноки. Для более ранних версий Hyper-V и унаследованного формата VHD общее соглашение заключалось в том, что если была нужна хорошая производительность, то, безусловно, должны были применяться фиксированные диски. Динамические диски VHD становились причиной бесчисленного количества проблем с производительностью, однако с появлением Windows Server 2012 в Microsoft призывают использовать динамические диски с их новым форматом VHDX, т.к. проблемы с производительностью решены.

Тем не менее, внутри сообщества Hyper-V существуют некоторые расхождения во мнениях относительно возможного выигрыша или проигрыша в производительности в случае применения фиксированных и динамических дисков VHDX, а также по поводу практичности каждого типа. Рекомендуем ознакомиться со статьей авторитетного ирландского специалиста по Hyper-V Айдана Финна, доступной по ссылке `http://www.aidanfinn.com/?p=13230`, чтобы увидеть, что его предпочитаемым типом являются фиксированные диски VHDX. Есть и другая точка зрения, с которой можно ознакомиться в статье еще одного авторитетного специалиста по Hyper-V Томаса Маурера: `http://www.thomasmaurer.ch/2012/11/windows-server-2012-hyper-v-virtual-disk-vhd-vhdx-recommendations/`; он предпочитает в большинстве сред использовать динамические диски VHDX.

Что касается версии Windows Server 2012 R2, то мы предпочитаем применять динамические диски VHDX для всех виртуальных машин с низким коэффициентом использования (таких как контроллеры домена, серверы печати и т.д.) и фиксированные диски VHDX для любых виртуальных машин, требующих более высокого уровня ввода-вывода (вроде SQL Server и Exchange Server). Это позволяет получить лучшее из двух миров в плане производительности и обслуживания внешней памяти.

Создание нового виртуального диска

Создать новый виртуальный диск можно во время развертывания новой виртуальной машины, при редактировании конфигурации существующей виртуальной машины или в любое время как автономный диск. В этом разделе мы рассмотрим процесс создания нового автономного виртуального диска VHDX фиксированного размера с применением мастера создания виртуального жесткого диска (New Virtual Hard Disk Wizard), доступного из консоли Hyper-V.

1. Откройте диспетчер Hyper-V, в панели Actions (Действия) щелкните на пункте New (Создать) и в открывшемся меню выберите пункт Hard Disk (Жесткий диск), чтобы запустить мастер создания виртуального жесткого диска (New Virtual Hard Disk Wizard).
2. Щелкните на кнопке Next (Далее).
3. На экране Choose Disk Format (Выбор формата диска), показанном на рис. 27.16, выберите переключатель VHDX. Щелкните на кнопке Next.

   Появится экран Choose Disk Type (Выбор типа диска), позволяющий выбрать один из переключателей Fixed size (Фиксированный размер), Dynamically expanding (Динамически расширяющийся) или Differencing (Разностный).

4. Выберите переключатель Fixed size (рис. 27.17). Щелкните на кнопке Next.
5. На экране Specify Name and Location (Указание имени и местоположения) назначьте новому диску имя и укажите, где он должен находиться.

   Щелкните на кнопке Next.

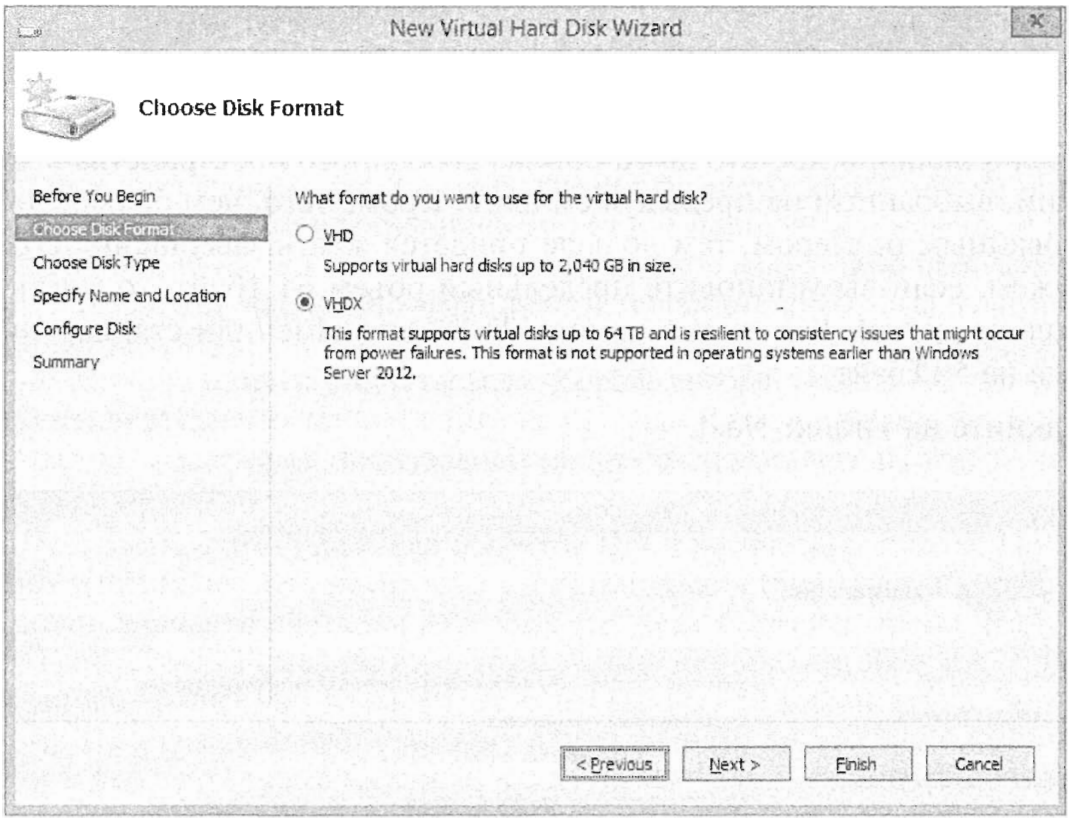


Рис. 27.16. Выбор формата для нового виртуального диска

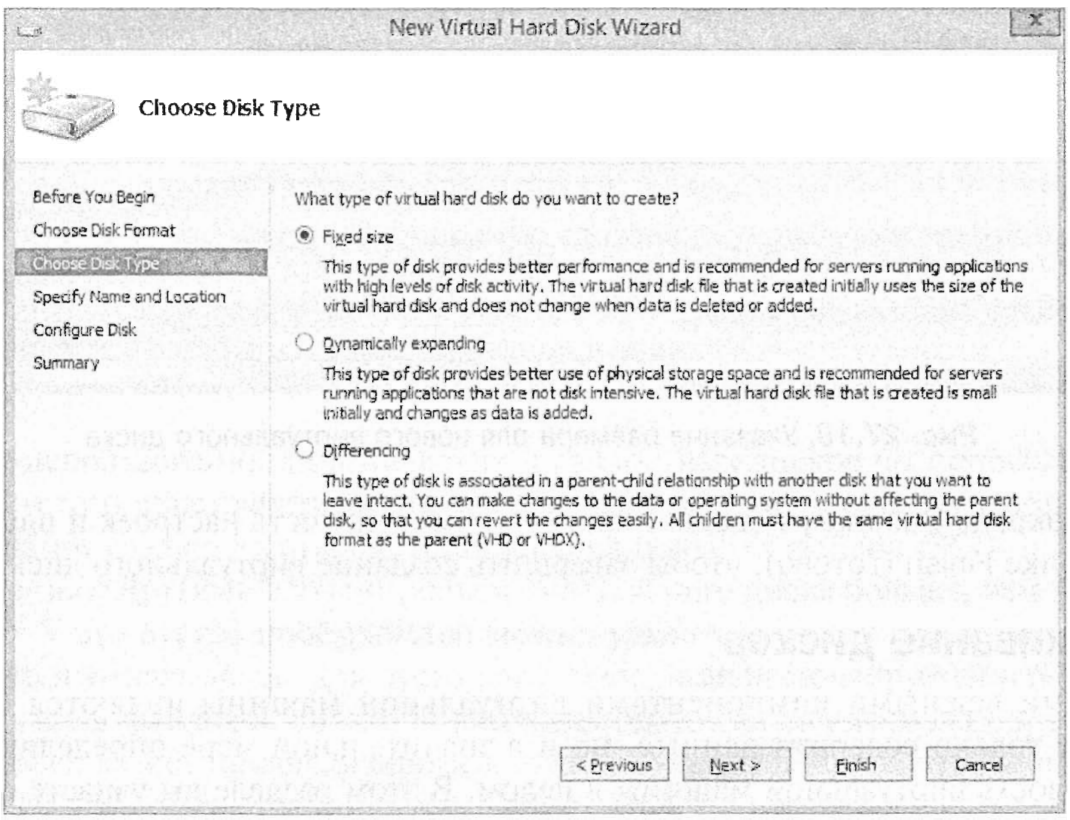


Рис. 27.17. Выбор типа диска

6. На экране Configure Disk (Конфигурирование диска) укажите размер нового виртуального диска; можно также скопировать содержимое определенного физического или другого виртуального диска.

   В качестве стандартного размера для новых пустых виртуальных дисков выбирается 127 Гбайт, но при необходимости можете увеличить его до максимального значения 64 Тбайт.

   При создании нового диска с фиксированным размером помните, что независимо от размера, указываемого для нового диска, вы должны заранее удостовериться в наличии достаточного объема свободного пространства в местоположении, выбранном на предыдущем шаге. Кроме того, чем больше диск с фиксированным размером, тем дольше придется ждать завершения его создания (скажем, если вы установите предельный объем 64 Тбайт, то ждать придется довольно долго). Как видно на рис. 27.18, мы изменили стандартный размер диска на 50 Гбайт.

   Щелкните на кнопке Next.

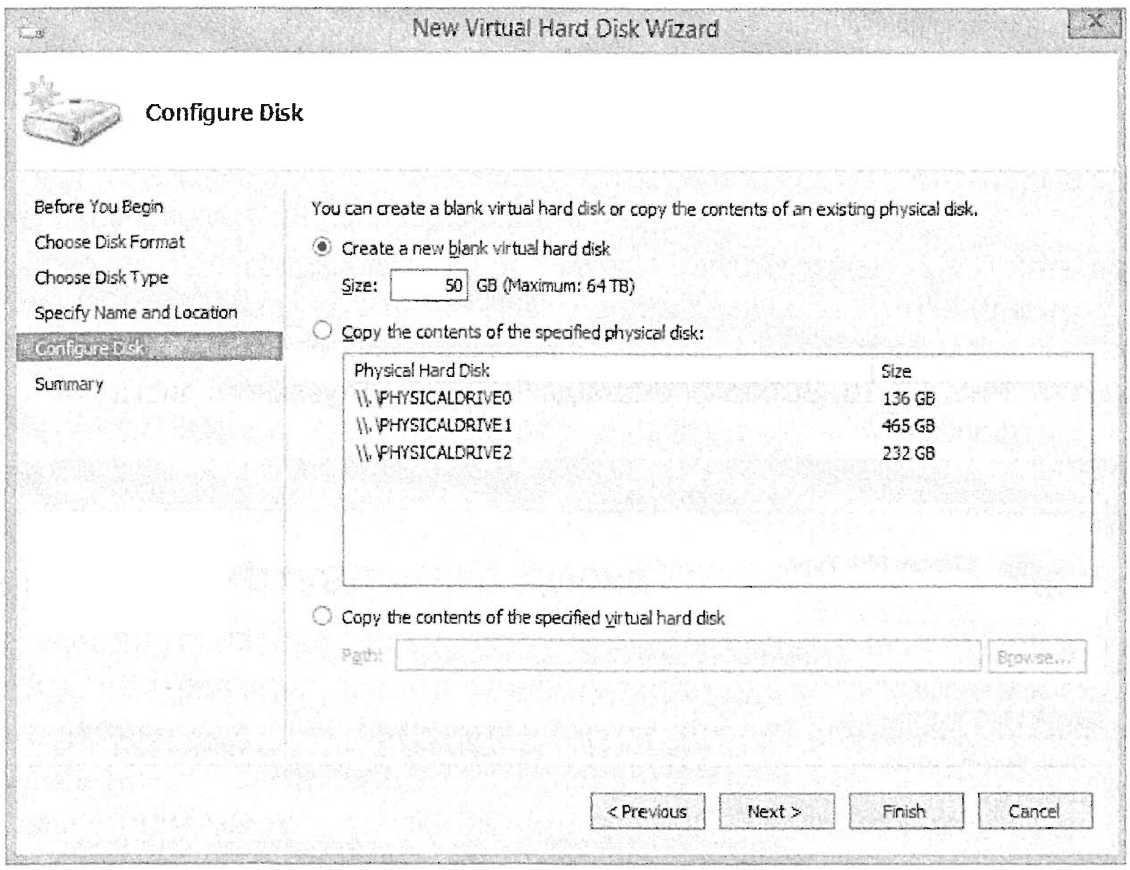


Рис. 27.18. Указание размера для нового виртуального диска

7. На экране Summary (Сводка) проверьте корректность настроек и щелкните на кнопке Finish (Готово), чтобы завершить создание виртуального диска.

Обслуживание дисков

Самыми важными компонентами виртуальной машины являются ее диски. Диски не только содержат данные, но и в значительной мере определяют производительность виртуальной машины в целом. В этом разделе вы узнаете о том, как обслуживать виртуальные диски.

Пример из практики

Загадочная медленная работа виртуальных машин

В качестве тестовой среды в Bigfirm было развернуто несколько серверов хостов Hyper-V. Каждый сервер имеет 128 Гбайт внутренней памяти и 12 Тбайт используемого дискового пространства. Эксплуатация хостов Hyper-V поручена отделу информационных систем.

В один прекрасный день начали поступать жалобы на медленное реагирование определенных виртуальных машин, хотя очевидная нагрузка на них не наблюдалась. Специалисты из отдела информационных систем приняли эти жалобы и приступили к выяснению причин, но не обнаружили признаков каких-либо проблем ни в одной из этих виртуальных машин. Коэффициент использования ЦП был в пределах нормы, все приложения функционировали, ОС не выполняла подкачку и чрезмерно активная эксплуатация памяти отсутствовала. Короче говоря, очевидных причин замедления работы виртуальных машин найти не удалось. Правда, имелась одна общая черта: большинство "медленных" виртуальных машин располагались на том же самом хосте.

Сотрудники отдела информационных систем запустили на этом хосте счетчики производительности, в том числе для объектов ЦП и логических дисков. После часа измерений выяснилось, что некоторые счетчики демонстрировали постоянно высокие показатели: значение счетчика Avg. Disk sec/Read (Среднее время чтения диска) в среднем составляло 30 миллисекунд, а значение счетчика Avg. Disk sec/Write (Среднее время записи на диск) по большей части превышало 50 миллисекунд. Значение счетчика Avg. Disk Queue Length (Средняя длина очереди диска) для диска, на котором размещались виртуальные машины, часто превышало 20. По сравнению с другими хостами эти значения были действительно высокими. Стало ясно, что у хоста была проблема с обеспечением требуемого дискового ввода-вывода.

Инспектирование хоста показало, что диск, на котором находились виртуальные машины, имеет конфигурацию RAID 5, которая хороша при чтении, но медленна при записи. Совокупный дисковый ввод-вывод всех виртуальных машин превышал предел возможностей хоста. Проблема была решена за счет реорганизации дисков в конфигурацию RAID 10 и добавления дополнительных дисков для увеличения максимальной пропускной способности ввода-вывода.

Этот случай иллюстрирует повышенную сложность управления средой виртуализированных серверов. Комбинация множества виртуальных машин может вызывать проблемы у хоста, если лежащее в основе оборудование физических дисков не было сконфигурировано на обеспечение оптимальной производительности.

При использовании динамических и разностных дисков вы оставляете на диске много пустого пространства, если сначала записываете на него большой объем данных, а затем удаляете их (вроде копирования больших файлов ISO и последующего их удаления). Другими словами, объем виртуального диска больше, чем необходимо. В Hyper-V это пустое пространство можно удалить с помощью операции, которая называется *уплотнением*. Для этого виртуальный диск монтируется в родительском разделе. Если файловой системой виртуального диска является NTFS, то родительский раздел может проанализировать свои структуры данных, чтобы выяснить, где находится пустое пространство. Эта информация применяется для сокращения размера файла, представляющего виртуальный диск. Во время уплотнения виртуаль-

ного диска соответствующая виртуальная машина не может функционировать. Ее работу потребуется завершить или сохранить ее состояние. После этого необходимо выполнить следующие действия.

1. В панели Actions (Действия) консоли управления Hyper-V щелкните на пункте Edit Disk (Редактировать диск), чтобы запустить мастер редактирования виртуального жесткого диска (Edit Virtual Hard Disk Wizard).
2. Найдите виртуальный диск, подлежащий уплотнению (например, созданный ранее виртуальный диск), и щелкните на кнопке Next (Далее).

   Как показано на рис. 27.19, экран Choose Action (Выбор действия) этого мастера позволяет выбрать одно из трех действий, которые могут быть применены к виртуальным дискам.

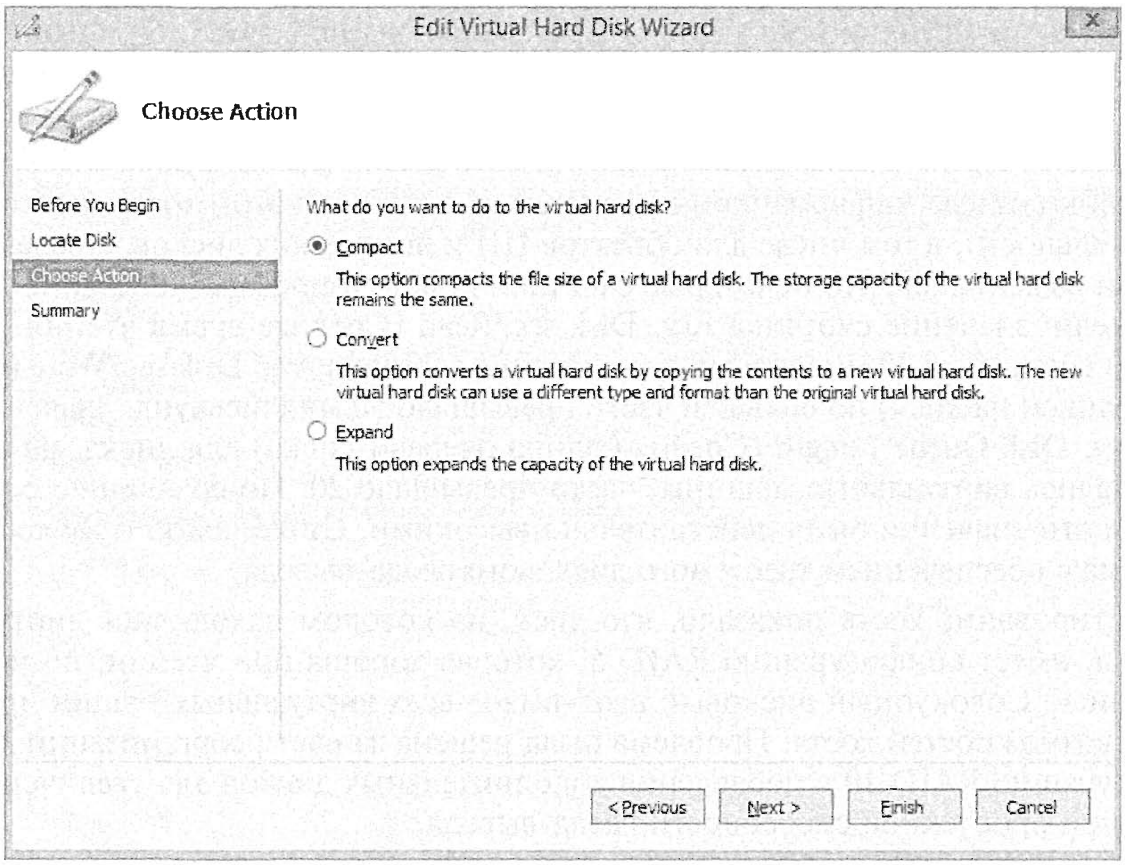


Рис. 27.19. Уплотнение виртуального диска с помощью мастера редактирования виртуального жесткого диска

3. Оставьте выбранным предлагаемый по умолчанию переключатель Compact (Уплотнить) и щелкните на кнопке Next.
4. Щелкните на кнопке Finish (Готово).

   Действительный процесс может занять некоторое время.

Может возникнуть ситуация, когда необходимо изменить тип диска, с которым вы работаете. Например, вы можете решить, что динамический диск не является лучшим вариантом, и было бы неплохо взамен иметь диск с фиксированным размером. Или, возможно, есть разностный диск, который вам хотелось бы разъединить с его родительским диском. В Hyper-V предлагается несколько операций преобразования дисков, которые доступны после выбора переключателя Convert (Преобразовать) в мастере Edit Virtual Hard Disk Wizard и кратко описаны в табл. 27.6.

Таблица 27.6. Операции преобразования дисков

Тип диска	Возможные операции
Динамически расширяющийся диск	Создание нового диска фиксированного размера, уплотнение или расширение
Диск фиксированного размера	Создание нового динамического диска или расширение
Разностный диск	Объединение с родительским диском, уплотнение или повторное соединение с родительским диском, который был перемещен по другому пути

Все эти операции доступны в мастере Edit Virtual Hard Disk Wizard. Если вам приходится выполнять большой объем тестирования с применением разностных дисков, то в какой-то момент вы решите создать автономные диски, поскольку интенсивно используемый разностный диск окажется больше своего родительского диска — а именно такой ситуации хотелось бы избежать. Давайте рассмотрим пример. Предположим, что имеется разностный диск `differencing.vhd` и вы хотите создать новый независимый виртуальный диск. Опять-таки, для такой процедуры виртуальная машина должна быть отключена.

1. В панели Actions (Действия) консоли управления Hyper-V щелкните на пункте Edit Disk (Редактировать диск), чтобы запустить мастер редактирования виртуального жесткого диска (Edit Virtual Hard Disk Wizard).
2. Найдите виртуальный диск, подлежащий объединению (`differencing.vhd` в этом примере).

   Мастер определит, что это разностный диск, и предложит только варианты, имеющие отношение к такому типу дисков.
3. На экране Choose Action (Выбор действия) выберите переключатель Merge (Объединить). Появится экран Merge Changes from Differencing Disk (Объединение изменений с разностным диском), предоставляющий в области How do you want to merge the changes? (Как вы хотите объединить изменения) два базовых переключателя: To the parent virtual hard disk (С родительским виртуальным жестким диском) и To a new virtual hard disk (С новым виртуальным жестким диском). При объединении диска с его родительским диском действуйте предельно осторожно, т.к. после этого любые другие дочерние диски станут недействительными.
4. В целях тестирования мы планируем создать новый динамический диск, поэтому выберите переключатель To a new virtual hard disk, затем в области New virtual hard disk type (Тип нового виртуального жесткого диска) выберите переключатель Dynamic virtual hard disk (Динамический виртуальный жесткий диск) и в поле Location (Местоположение) укажите подходящее имя, например, *имя_сервера*`-dynamic.vhd` (рис. 27.20).
5. Щелкните на кнопке Next (Далее), после чего на кнопке Finish (Готово), чтобы запустить процедуру на выполнение.
6. Чтобы использовать новый диск, внесите требуемые изменения в свойства виртуальной машины и замените текущий разностный диск.

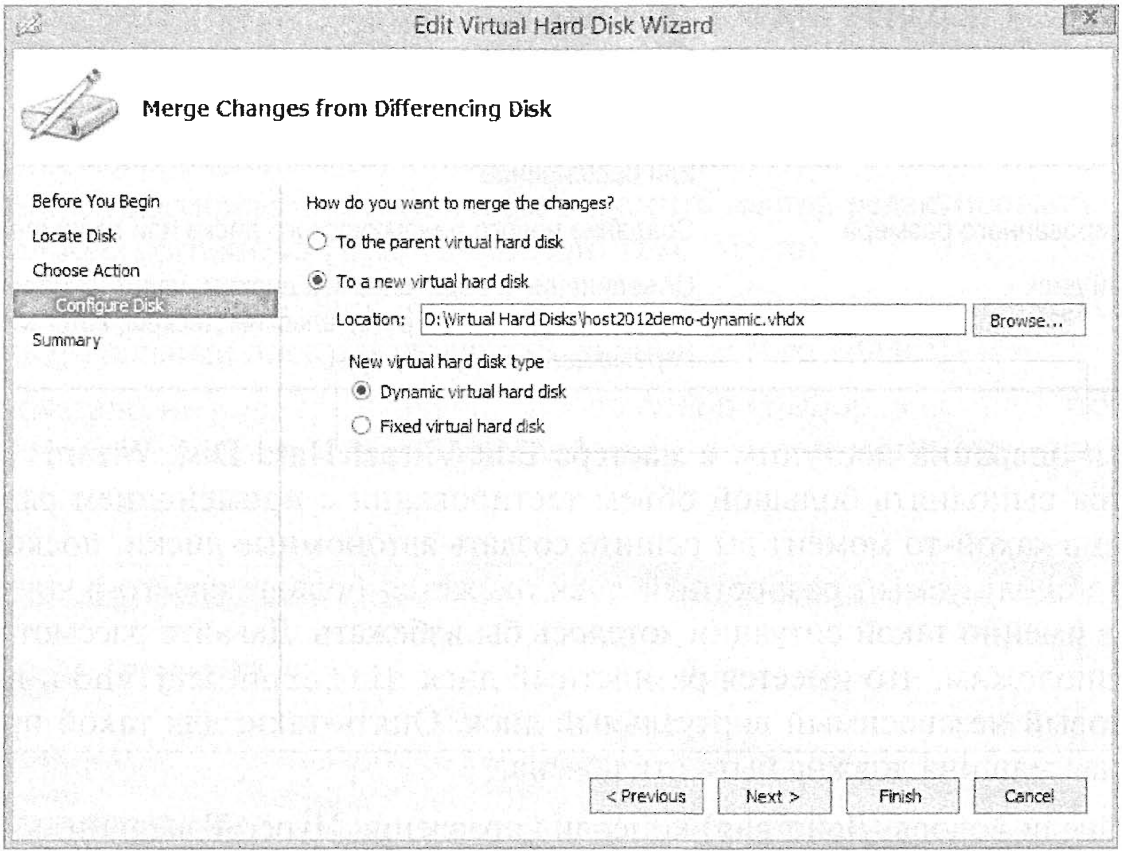


Рис. 27.20. Объединение разностного диска с его родительским диском в новый (динамический) виртуальный жесткий диск

В панели Actions консоли управления Hyper-V вы заметите один дополнительный пункт меню, связанный с дисками: Inspect Disk (Инспектировать диск). Как упоминалось ранее, это простой пункт меню, который позволяет всего лишь открыть виртуальный диск и выяснить его тип, а также получить кое-какую дополнительную информацию. Однако для разностных дисков предусмотрена одна полезная возможность: если родительский диск отсутствует, то здесь об этом сообщается. Разностный диск здесь можно повторно присоединить к родительскому диску, для чего просто перейти на него.

На основе этого обсуждения вы должны были понять, что виртуальные диски встречаются разных типов, и расширение `.vhdx` не несет в себе исчерпывающей информации.

Понятие виртуальных коммутаторов

В главе 4 вы узнали, что в Windows Server 2012 были достигнуты наиболее значительные по сравнению с предыдущими версиями Windows Server усовершенствования в деле организации сетей, потребовавшие самых крупных инвестиций за всю историю развития Windows Server. В текущей версии Hyper-V введены концепции сходящейся структуры, качества обслуживания внешней памяти и расширяемых коммутаторов. В этом разделе мы поможем вам понять некоторые из этих концепций, и объясним, как их можно использовать в продвижении развертываний Hyper-V.

В предшествующих версиях Hyper-V вы располагали довольно простым методом подключения виртуальных машин к трем разным типам базовых виртуальных сетей, которые можно было конфигурировать посредством диспетчера виртуальных сетей

(Virtual Network Manager). В Windows Server 2012 на смену концепции виртуальной сети пришла концепция *виртуального коммутатора*. На первый взгляд их поведение принципиально ничем не отличается. Тем не менее, если присмотреться к возможностям виртуального коммутатора внимательнее, скоро станет очевидным тот факт, что возможности, связанные с виртуальными сетями, значительно расширились.

Виртуальные коммутаторы — это полностью программное решение, которое обеспечивает высокоскоростные подключения между виртуальными машинами, которые сконфигурированы с одной или несколькими виртуальными сетевыми интерфейсными платами. Как и в реальном мире, на виртуальном коммутаторе вы "подключаете" виртуализированные сетевые интерфейсные платы виртуальных машин.

Выбор виртуального коммутатора

В Hyper-V на выбор доступны следующие типы виртуальных коммутаторов.

- **Внешний виртуальный коммутатор.** Предоставляет полный доступ в сеть. Виртуальная машина, подключенная к *внешнему* соединению, может обмениваться данными с внешним миром через физическую сетевую интерфейсную плату хоста. Любое другое сетевое устройство будет видеть эту виртуальную машину, как если бы она была нормальным компьютером. Единственным исключением является (физический) сетевой коммутатор, подключенный к хосту. Такой коммутатор видит один хост с двумя MAC-адресами и двумя IP-адресами. Имейте в виду, что некоторые более старые сетевые среды могут не разрешать это. Симптомом может служить то, что виртуальная машина способная взаимодействовать с хостом, но не с любой другой машиной в сети, несмотря на то, что был указан внешний доступ.
- **Внутренний виртуальный коммутатор.** Внутренний коммутатор довольно интересен. Он позволяет выполнять обмен данными между всеми виртуальными машинами и хостом, но не напрямую с внешним миром. Такой вариант подходит для большинства тестовых установок, когда вы хотите, чтобы виртуальные машины взаимодействовали друг с другом и могли передавать файлы и папки из хоста, но не могли передавать их на любой внешний компьютер. Для каждого создаваемого вами внутреннего виртуального коммутатора Hyper-V предусматривает дополнительное подключение по локальной сети (Local Area Connection), непосредственно соединенное с этим новым коммутатором. На конкретной сетевой интерфейсной плате протокол DHCP отсутствует (если только вы не установили его явно), поэтому все на этом коммутаторе получит адрес APIPA. Таким образом, подключение к сети имеется, но для его использования понадобится самостоятельно сконфигурировать настройки IP.
- **Частный виртуальный коммутатор.** В случае *частных* виртуальных коммутаторов виртуальные машины подключаются друг к другу, но не могут видеть хост. По существу они полностью изолированы от физической сети. Опять-таки, это идеально подходит для тестирования. Например, когда вы тестируете возможности DHCP, предлагаемые Windows Server 2012 R2, такое тестирование нежелательно проводить в физической сети. В некоторых компаниях за это вполне могли бы уволить! Если испытываете какие-либо сомнения, то частный виртуальный коммутатор является самым безопасным вариантом для тестирования.

Полезным свойством виртуальных коммутаторов является возможность изменения их области действия и функциональности. Вы могли бы начать в внутреннего коммутатора, а впоследствии подключить его к физической внешней сетевой интерфейсной плате. Применение виртуальных коммутаторов обеспечивает для виртуальных машин значительную гибкость, и внутри хоста вы можете создавать довольно сложные сети. Например, с помощью трех виртуальных коммутаторов вы могли бы сформировать классическую структуру DMZ: один из этих виртуальных коммутаторов использовать для внешнего интерфейса, подключенного к физической сетевой интерфейсной плате, другой коммутатор — для хостов DMZ, а третий — для внутренней локальной сети.

Создание виртуального коммутатора

В конфигурирование виртуальных сетей вовлечены две части: виртуальные сетевые интерфейсные платы и виртуальные коммутаторы. Виртуальными сетевыми интерфейсными платами можно управлять в диалоговом окне настроек виртуальной машины, как будет показано позже, а виртуальный коммутатор конфигурируется посредством диспетчера виртуальных коммутаторов (Virtual Switch Manager).

Чтобы создать новый виртуальный коммутатор, выполните следующие шаги.

1. Откройте диспетчер Hyper-V и в панели Actions (Действия) щелкните на пункте Virtual Switch Manager (Диспетчер виртуальных коммутаторов).
2. В открывшемся диалоговом окне Virtual Switch Manager (Диспетчер виртуальных коммутаторов) щелкните на элементе New virtual network switch (Новый виртуальный сетевой коммутатор), как показано на рис. 27.21.

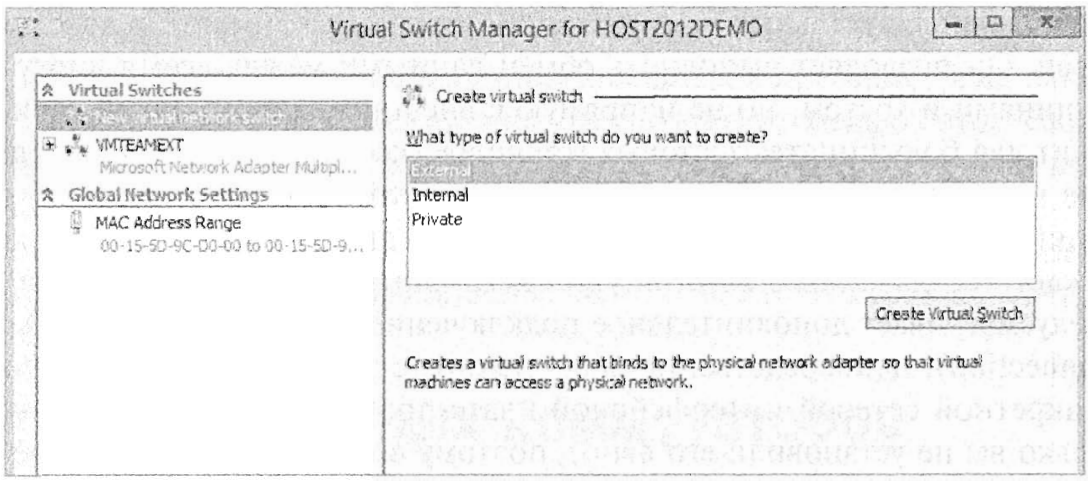


Рис. 27.21. Диалоговое окно Virtual Switch Manager, открываемое из панели Actions консоли управления Hyper-V

3. В разделе Create virtual switch (Создание виртуального коммутатора) выберите тип виртуального коммутатора, который хотите создать (External (Внешний), Internal (Внутренний) или Private (Частный)), и щелкните на кнопке Create Virtual Switch (Создать виртуальный коммутатор).

   На рис. 27.22 выбран виртуальный коммутатор VMEXT1. Этот коммутатор был создан, когда мы устанавливали роль Hyper-V и указывали мастеру, какие сетевые интерфейсные платы использовать для трафика виртуальной машины. Чтобы убедиться в этом, взгляните еще раз на рис. 27.11.

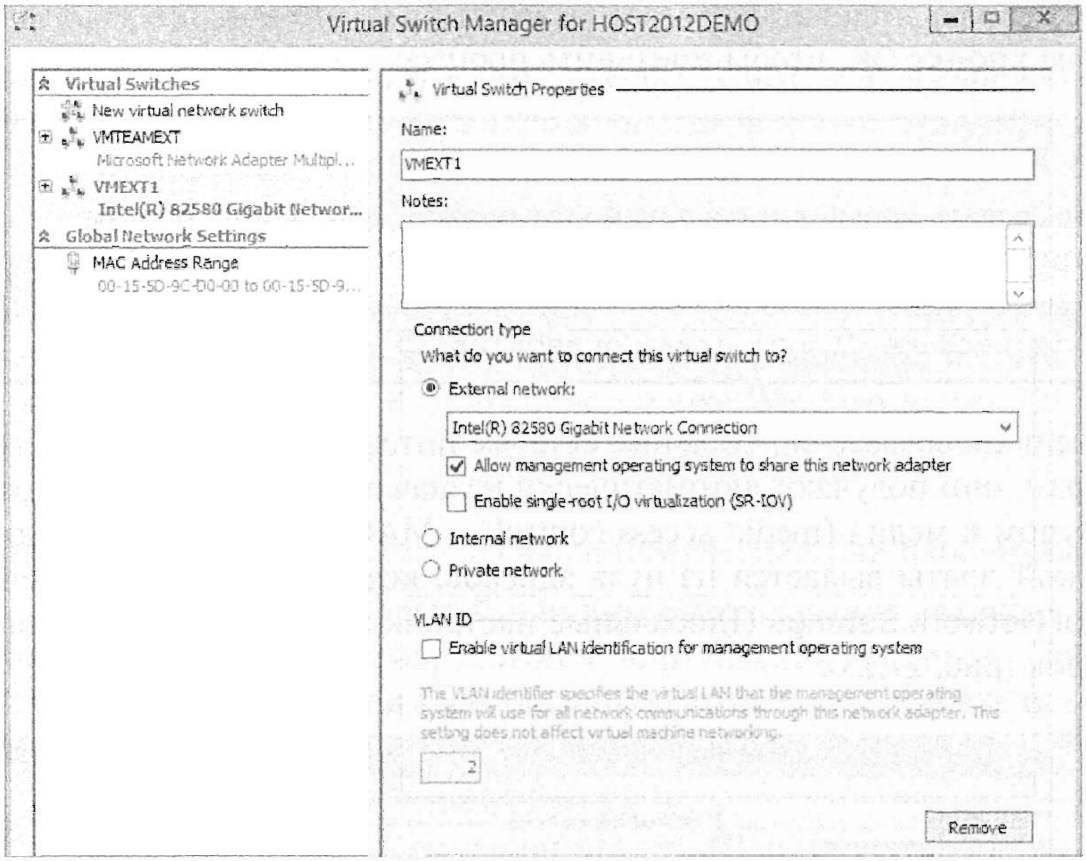


Рис. 27.22. Диалоговое окно Virtual Switch Manager после выбора виртуального коммутатора

Кроме того, по умолчанию здесь отмечен флажок Allow management operating system to share this network adapter (Разрешить управляющей операционной системе совместное использование этого сетевого адаптера). Оставляя этот флажок отмеченным, вы обеспечиваете хосту доступ к данному коммутатору, а это означает возможность разделения трафика между виртуальными машинами и операционной системой их хоста. В испытательной или непроизводственной среде, где в вашем распоряжении может оказаться только одна сетевая интерфейсная плата, отметки этого флажка должно быть вполне достаточно. Но при наличии нескольких сетевых интерфейсных плат или в случае работы в производственной среде Hyper-V рекомендуется снять отметку с этого флажка и щелкнуть на кнопке Apply (Применить).

4. Если вы хотите создать новый внешний виртуальный коммутатор вместо применения коммутатора, созданного во время установки Hyper-V, то в области Virtual Switch Properties (Свойства виртуального коммутатора) назначьте этому коммутатору имя и выберите в раскрывающемся списке физическую сетевую интерфейсную плату, с которой вы будете соединяться. При наличии нескольких физических сетевых интерфейсных плат вы столкнетесь с определенным неудобством: вместо дружественных описаний, которыми вы могли снабдить свои сетевые интерфейсные платы, отображается только перечень имен устройств. Это затрудняет идентификацию сетевой интерфейсной платы, которая должна быть назначена новому виртуальному коммутатору, но если вы воспользуетесь командлетами `Get-NetAdapter | Format-Table -Autosize` в PowerShell, то сможете увидеть список имен устройств сетевых интерфейсных плат, отображенных на более описательные и дружественные имена.

5. После выбора типа виртуального коммутатора и его конфигурирования щелкните на кнопке OK, чтобы завершить процесс.

Совет по PowerShell

Вы можете создать новый виртуальный коммутатор, который не пользуется соединениями совместно с управляющей ОС, посредством следующей команды PowerShell:

```
New-VMSwitch -Name "VMEXT1" -AllowManagementOS $false
    -NetAdapterName "Local Area Connection 2"
```

Когда вы подключаете виртуальные сетевые интерфейсные платы к виртуальным коммутаторам, они получают автоматически назначаемые уникальные адреса управления доступом к медиа (media access control — MAC). MAC-адрес каждой сетевой интерфейсной платы выдается из пула адресов, которые можно определить в области Global Network Settings (Глобальные настройки сети) диспетчера виртуальных коммутаторов (рис. 27.23).

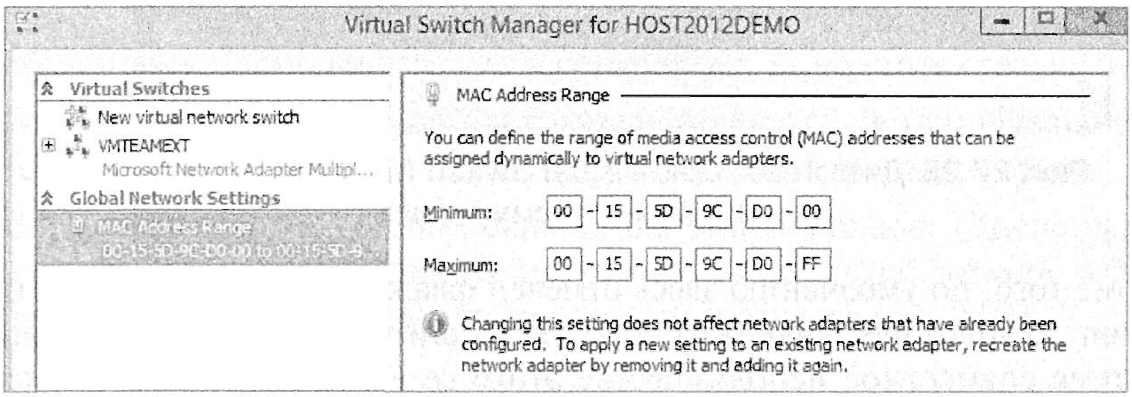


Рис. 27.23. Определение диапазона MAC-адресов

Виртуальные коммутаторы представляют собой мощную концепцию. С их помощью можно создавать внутреннюю сеть любой желаемой сложности. Это открывает широкие возможности для тестирования и изучения новых технологий. В настоящем разделе мы только начинаем обсуждение, и в последующих разделах вам предстоит узнать много нового об этих возможностях.

Начало работы с виртуальными машинами

К этому моменту у вас уже развернута служба Hyper-V, и вы понимаете, что собой представляют виртуальные диски и виртуальные коммутаторы. Вы готовы приступить к конфигурированию виртуальной машины. Прежде чем начать, удостоверьтесь в том, что располагаете всем необходимым.

- Образ ISO, содержащий операционную систему, которую необходимо установить. Образ ISO здесь необходим из-за того, что версия Windows Server 2012 R2 Hyper-V больше не предлагает физического диска CD/DVD в качестве средства для установки операционной системы на виртуальной машине. (Вариант DVD можно было бы позже добавить вручную, но в мастере создания виртуальной машины (New Virtual Machine Wizard) это не предусмотрено.) Мы сконфигурировали сервер `HOST2012DEMO` с общим ресурсом, на котором размещены наши файлы ISO: `\\host2012demo\ISO`.

- Имя для нового сервера.
- Соображения относительно типа виртуального коммутатора (внешний, внутренний или частный), который вы хотели бы применять с виртуальной машиной, и соответствующий IP-адрес.
- Сколько памяти использовать. Излишняя умеренность в данном случае неуместна. Если виртуальной машине придется начать подкачку памяти, это приведет к большой нагрузке на систему дискового ввода-вывода хоста, возможности которой разумнее задействовать для размещения большего количества виртуальных машин. В базовой установке Windows Server 2012 R2 выбирайте минимум 512 Мбайт, но желательно больше, что зависит от рабочей нагрузки.
- Тип используемого виртуального диска: динамический или фиксированный.

Концептуально создание виртуальной машины с нуля требует два шага. Сначала вы конфигурируете виртуальное оборудование виртуальной машины, а затем выполняете загрузку этой виртуальной машины и приступаете к установке операционной системы. О конфигурировании виртуальной машины позаботится мастер New Virtual Machine Wizard.

1. Откройте диспетчер Hyper-V, в панели Actions (Действия) щелкните на пункте New (Создать) и в открывшемся меню выберите пункт Virtual Machine (Виртуальная машина).

   На рис. 27.24 показан экран Before You Begin (Прежде чем начать) мастера New Virtual Machine Wizard, который кратко информирует о том, для чего предназначена виртуальная машина.

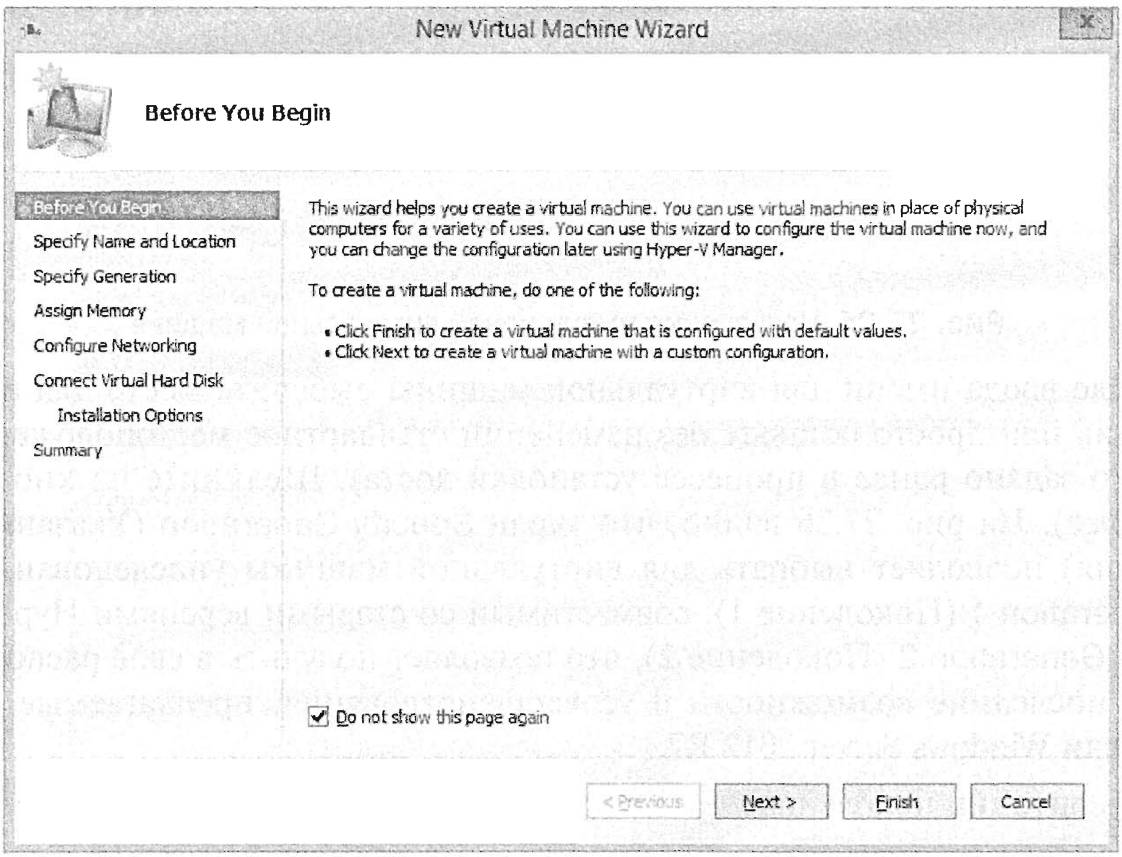


Рис. 27.24. Запуск мастера New Virtual Machine Wizard. Отметьте флажок Do not show this page again, чтобы никогда больше не видеть этот экран

2. Отметьте флажок Do not show this page again (Не показывать эту страницу снова), чтобы в будущем пропускать этот экран.

   В этот момент вы могли бы даже щелкнуть на кнопке Finish (Готово), чтобы создать виртуальную машину со стандартными настройками, но это не очень хорошая идея. Вообще говоря, не бывает двух виртуальных машин, которые бы в точности совпадали.

3. Введите имя для виртуальной машины, как показано на рис. 27.25.

   Обратите внимание, что это дружественное имя, применяемое в консоли управления, а не фактическое имя хоста. Конечно, имеет смысл делать эти имена хотя бы очень похожими, чтобы позже можно было легко идентифицировать их в консоли Hyper-V.

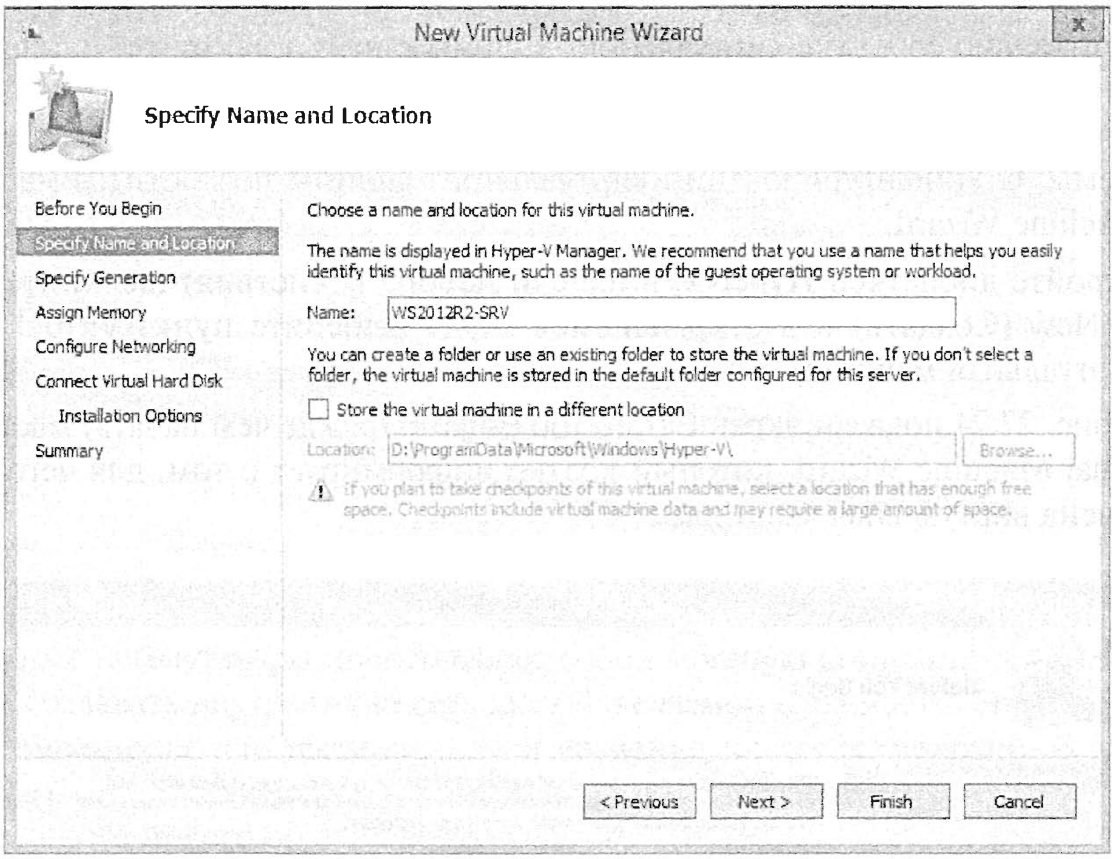


Рис. 27.25. Назначение имени новой виртуальной машине

4. После ввода имени для виртуальной машины выберите место для ее сохранения или просто оставьте без изменений стандартное местоположение (оно было задано ранее в процессе установки хоста). Щелкните на кнопке Next (Далее). На рис. 27.26 видно, что экран Specify Generation (Указание поколения) позволяет выбрать для виртуальной машины унаследованный тип Generation 1 (Поколение 1), совместимый со старыми версиями Hyper-V, или тип Generation 2 (Поколение 2), что позволяет получить в свое распоряжение все последние возможности и усовершенствования, предлагаемые Hyper-V версии Windows Server 2012 R2.

5. Выберите тип поколения.

   Обратите внимание на предупреждение, отображенное в нижней части экрана Specify Generation, которое сообщает о том, что в будущем тип поколения изменить невозможно. Для продолжения щелкните на кнопке Next.

На экране Assign Memory (Назначение памяти) предлагается указать объем памяти для создаваемой виртуальной машины.

6. В качестве объема начальной памяти укажите 512 Мбайт и отметьте флажок Use Dynamic Memory for this virtual machine (Использовать динамическую память для этой виртуальной машины), как показано на рис. 27.27.

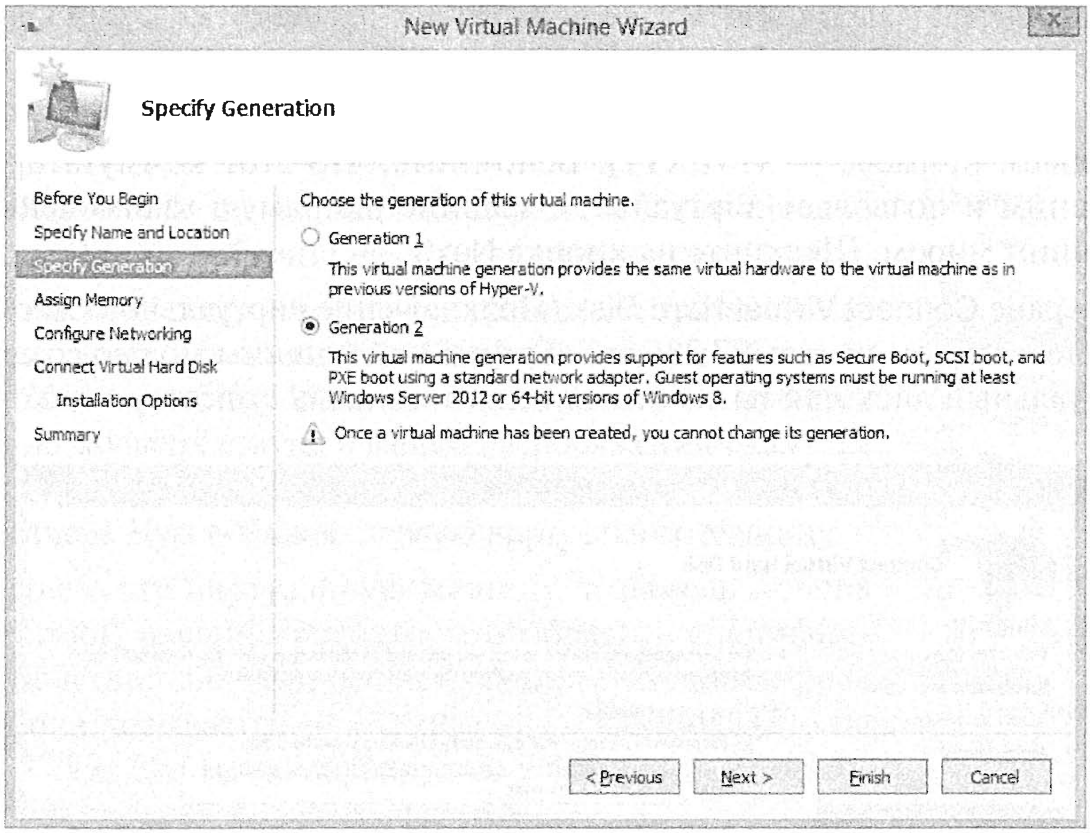


Рис. 27.26. Выбор типа поколения для новой виртуальной машины

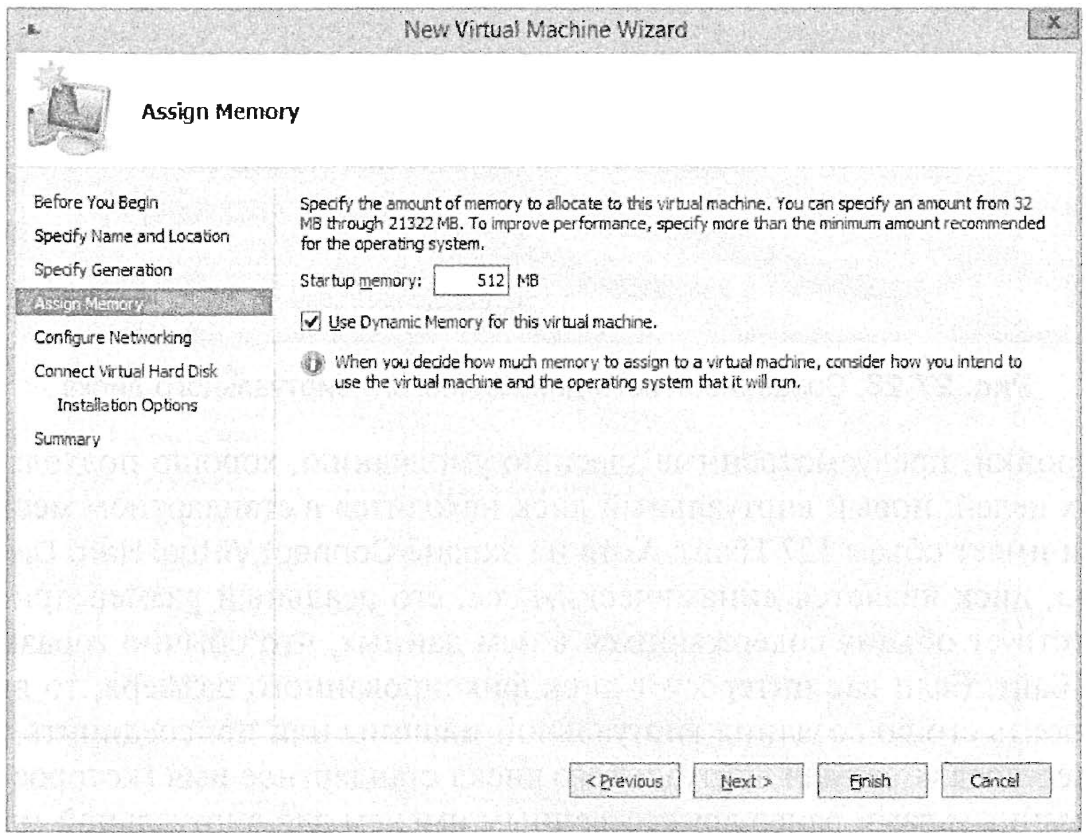


Рис. 27.27. Установка объема начальной памяти и включения средства Dynamic Memory

Средство Dynamic Memory (Динамическая память) оптимизирует выделение физической памяти для виртуальных машин из хоста Hyper-V управляющей ОС. Ниже мы разъясним эту возможность более подробно. Для продолжения щелкните на кнопке Next.

На экране Configure Networking (Конфигурирование сети) необходимо указать, какой виртуальный коммутатор должен использоваться. По умолчанию выбран переключатель Not Connected (Не подключено), который вполне безопасен, но практически бесполезен.

7. Выберите для подключения виртуальный коммутатор, созданный вами ранее (в нашем примере — VMEXT1). Вспомните, что этот коммутатор является внешним и позволяет виртуальной машине напрямую взаимодействовать с внешним миром. Щелкните на кнопке Next.
8. На экране Connect Virtual Hard Disk (Подключение виртуального жесткого диска), показанном на рис. 27.28, для виртуальной машины можно создать новый виртуальный диск или назначить какой-то из числа существующих.

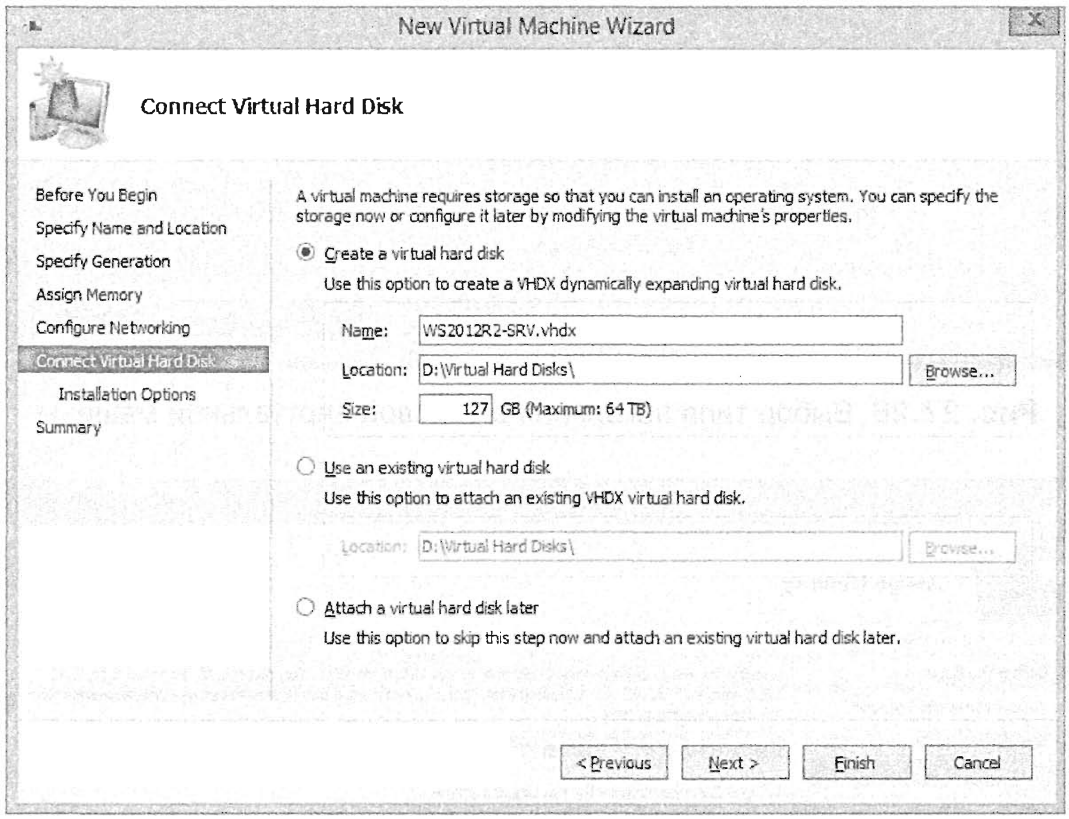


Рис. 27.28. Создание нового динамического виртуального диска

Настройки, предусмотренные здесь по умолчанию, хорошо подходят для тестовых целей: новый виртуальный диск находится в стандартном местоположении и имеет объем 127 Гбайт. Хотя на экране Connect Virtual Hard Disk этого не видно, диск является динамическим, т.е. его реальный размер примерно соответствует объему содержащихся в нем данных, что обычно гораздо меньше 127 Гбайт. Если вас интересует диск фиксированного размера, то вы должны построить его до создания виртуальной машины или присоединить его позже. Мастер предлагает для виртуального диска стандартное имя (которое совпадает с указанным вами ранее дружественным именем для виртуальной машины).

Когда будете готовы продолжить, щелкните на кнопке Next.

9. По существу экран Installation Options (Параметры установки) позволяет установить операционную систему позже или прямо сейчас. Здесь вы можете указать носитель для начальной установки: файл ISO или какой-то ресурс из сети. В данном примере установка выполняется с применением файла ISO.
10. Чтобы начать установку операционной системы, выберите переключатель Install an operating system from a bootable image file (Установить операционную систему из загружаемого файла образа).
11. Перейдите туда, где вы сохранили файл ISO для Windows Server 2012 R2, выберите его и щелкните на кнопке Next.
12. Просмотрите сводку по конфигурации виртуальной машины; щелкните на кнопке Finish (Готово), чтобы дать возможность мастеру выполнить свою работу. По прошествии нескольких секунд в вашем распоряжении окажется новая виртуальная машина. Теперь вы должны видеть в диспетчере Hyper-V свою первую виртуальную машину.
13. Выберите эту виртуальную машину, и панель Actions (Действия) расширится, чтобы отобразить специфичные действия для виртуальной машины (в нашем примере она называется `WS2012R2-SRV`), как показано на рис. 27.29. Это меню варьируется в зависимости от состояния питания и других аспектов.
14. Щелкните на пункте Settings (Параметры), чтобы открыть диалоговое окно Settings (Настойки) с конфигурацией этой виртуальной машины (рис. 27.30).

Рис. 27.29. Выберите виртуальную машину, чтобы просмотреть применимые к ней действия

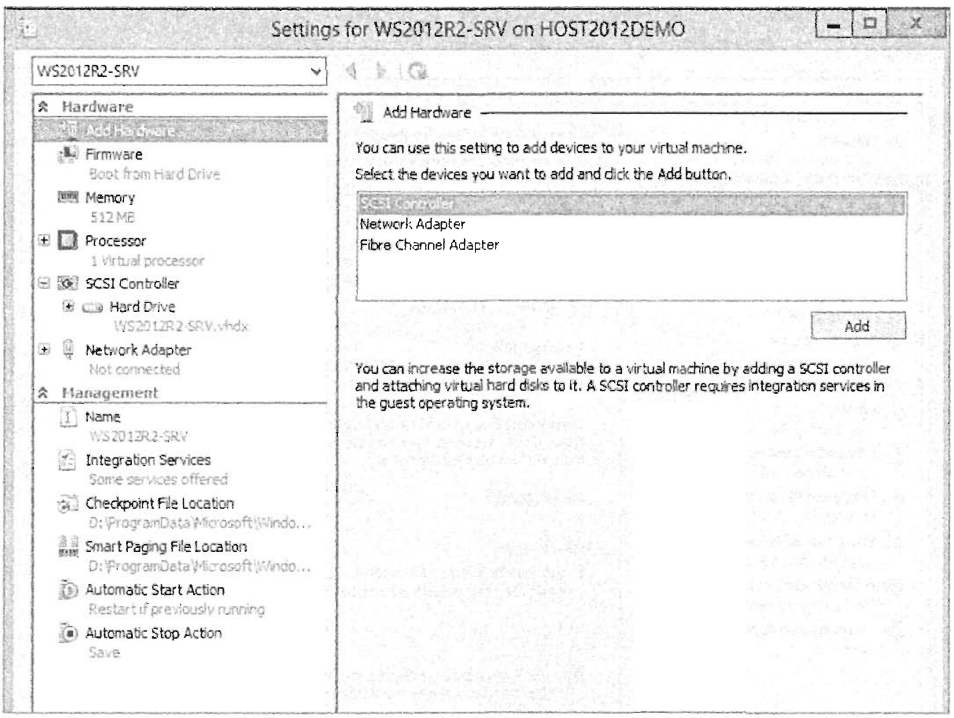


Рис. 27.30. Управление всеми параметрами виртуальной машины в диалоговом окне Settings

Диалоговое окно Settings — это окно, с которым вам придется многократно сталкиваться в будущем. Левая панель состоит из двух разделов: Hardware (Оборудование) и Management (Управление).

Из раздела Hardware можно управлять всем виртуальным оборудованием. Ниже приведено объяснение элементов этого раздела, которые доступны для виртуальной машины поколения 2.

- **Add Hardware (Добавить оборудование).** Здесь можно добавить контроллер SCSI, который будет использоваться для добавления виртуальных устройств SCSI. Как обсуждалось ранее, в этом выпуске Hyper-V виртуальные машины теперь можно загружать прямо из контроллера SCSI, и это единственный доступный вариант контроллера при конфигурировании виртуальных машин Gen2.
- **Firmware (Прошивка).** Именно здесь новая функция BIOS с унифицированным расширяемым интерфейсом прошивки (Unified Extensible Firmware Interface — UEFI) предоставляет возможность включения или отключения функциональности безопасной загрузки. Кроме того, можно выбирать порядок просмотра устройств загрузки: привод DVD, сетевой адаптер или жесткий диск.
- **Memory (Память).** На рис. 27.31 показан раздел Memory в окне Settings. Здесь видно, что в поле Startup RAM (Начальный объем ОЗУ) указано значение 512 Мбайт и флажок Enable Dynamic Memory (Включить динамическую память) отмечен, чтобы управлять объемом ОЗУ, который выделяется для виртуальной машины хостом в зависимости от степени ее использования.

  Настройка Minimum RAM (Минимальный объем ОЗУ) позволяет указать более низкий объем памяти, чем фактический начальный объем ОЗУ (который, конечно же, является минимумом, требуемым в первую очередь для запуска виртуальной машины). Это может быть полезно в виртуальных машинах, которые в течение длительных периодов времени работают с очень низким коэффициентом использования.

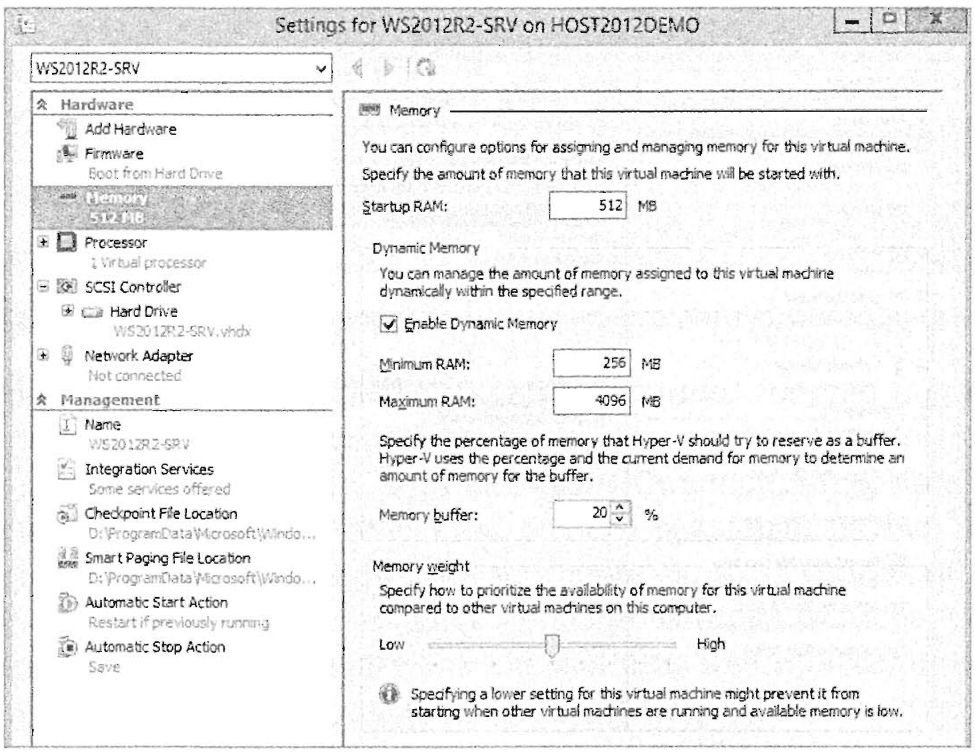


Рис. 27.31. Конфигурирование настроек динамической памяти

С помощью настройки Maximum RAM (Максимальный объем ОЗУ) можно определить объем памяти, выделяемый виртуальной машине из хоста, с верхним пределом 1 Тбайт. Полезно знать, что это значение может быть модифицировано во время работы виртуальной машины, оставляя ее доступной, но нельзя выделять объем ОЗУ, который больше доступного на физическом хосте.

Дополнительные сведения о динамической памяти можно почерпнуть из официального документа от Айдана Финна, опубликованного по ссылке `http://www.aidanfinn.com/?p=11289`.

- **Processor (Процессор).** Здесь можно указать количество виртуальных процессоров, сконфигурированных для этой конкретной виртуальной машины, с максимальным пределом 64. При загрузке виртуальная машина будет видеть такое количество процессоров. Разумеется, они не резервируются по умолчанию для этой виртуальной машины. Единственным владельцем процессоров является гипервизор, который решает, какая виртуальная машина и на какое время получает эти процессоры. В этом отношении сам хост находится под управлением гипервизора. Выражаясь по-другому, число виртуальных процессоров в сумме может быть гораздо больше, чем количество реальных ядер ЦП.

  На рис. 27.32 показаны настройки в области Resource control (Управление ресурсами). Здесь можно указать, какой процент выбранных процессоров должен быть зарезервирован для этой виртуальной машины. Поля, отображаемые серым цветом, сообщают о том, сколько это составляет в терминах суммарного потенциала данного хоста. Это нижний предел, который всегда доступен. Верхний предел задается лимитом виртуальной машины. Виртуальная машина никогда не сможет задействовать больше, чем это процентное значение. Такая возможность очень полезна, поскольку ограничивает те приложения, которые без веских причин расходуют ресурсы ЦП.

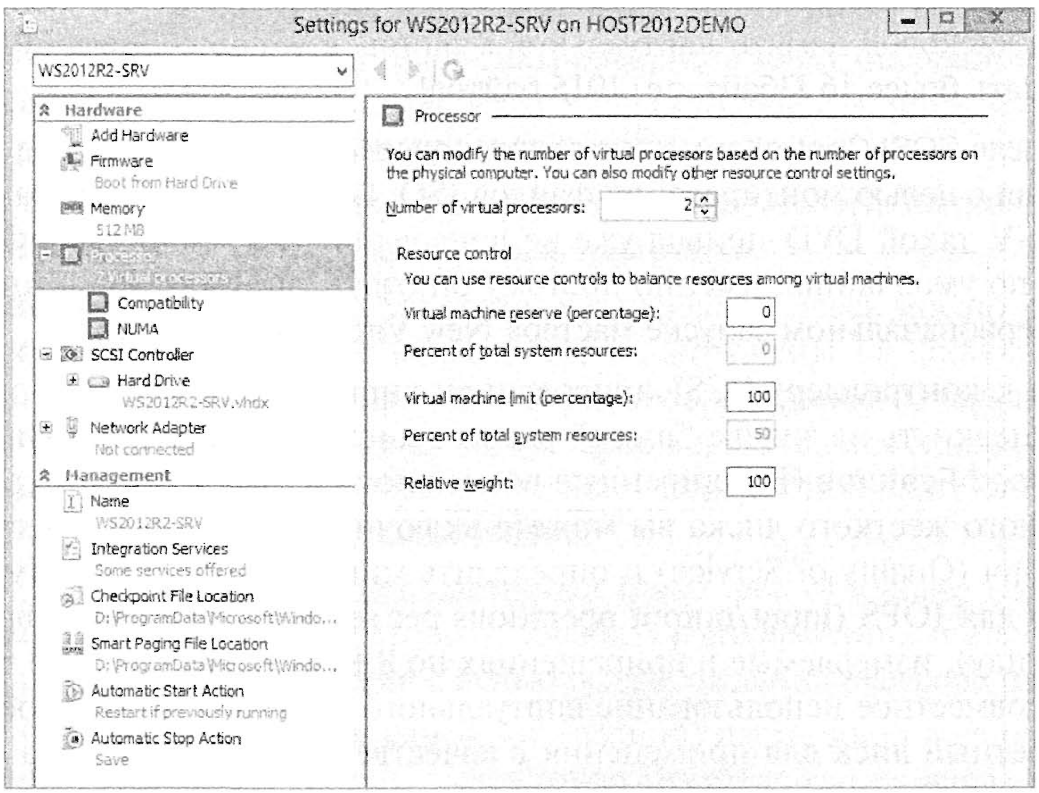


Рис. 27.32. Конфигурирование настроек процессора внутри виртуальных машин

На этом рисунке вы видите две дополнительных настройки процессора, которые необходимо принимать во внимание при конфигурировании функциональности процессора.

- **Compatibility (Совместимость).** Предоставляет в ваше распоряжение флажок Migrate to a physical computer with a different processor version (Перейти на физический компьютер с другой версией процессора) и используется в ситуации, когда имеются хосты Hyper-V со слегка отличающимися физическими ЦП от того же самого производителя. Принцип действия заключается в блокировании определенных инструкций процессора, функциональность которых варьируется между процессорами. За использование этой возможности придется заплатить потенциально более низкой производительностью в зависимости от рабочей нагрузки, и по данной причине флажок Migrate to a physical computer with a different processor version не отмечен.
- **NUMA**. Архитектура доступа к неоднородной памяти (Non-Uniform Memory Architecture — NUMA) обеспечивает масштабируемость для многопроцессорных виртуальных машин способом, посредством которого совместимые процессоры обращаются к разным банкам памяти на материнской плате. Эта настройка действует в сочетании с настройкой NUMA Spanning (Соединение узлов NUMA) из числа настроек Hyper-V, управляя тем, как средство Dynamic Memory охватывает множество узлов NUMA.

♦ **SCSI Controller (Контроллер SCSI).** Следующим элементом в разделе Hardware является SCSI Controller. Первый контроллер SCSI автоматически применяется для загрузки виртуального жесткого диска, который был сконфигурирован с помощью мастера New Virtual Machine Wizard. К виртуальной машине можно добавлять до четырех контроллеров SCSI, и каждый из них может иметь до 64 присоединенных виртуальных жестких дисков, а объем каждого виртуального жесткого диска может составлять до 64 Тбайт. Несложно подсчитать, что объем дисковой памяти виртуальной машины в Windows Server 2012 R2 может достигать более 16 Пбайт, т.е. 1015 байтов!

В разделе SCSI Controller можно также присоединить DVD-привод для использования с целью монтирования файлов ISO. В отличие от более ранних версий Hyper-V, такой DVD-привод уже не присоединяется к виртуальным машинам Gen2 по умолчанию; именно поэтому он отсутствует как возможный вариант при первоначальном запуске мастера New Virtual Machine Wizard.

Когда к контроллеру SCSI присоединен виртуальный жесткий диск, вы можете щелкнуть на значке "плюс" рядом с диском и получить доступ в область Advanced Features (Расширенные возможности). Здесь для конкретного виртуального жесткого диска вы можете включить управление качеством обслуживания (Quality of Service) и определить минимальное и максимальное значения для IOPS (input/output operations per second — операций ввода-вывода в секунду), измеряемые в приращениях по 8 Кбайт. Здесь можно также включить совместное использование виртуального жесткого диска, чтобы выделить конкретный диск для применения в качестве общего хранилища с целью упрощения сценариев кластеризации с вашими виртуальными машинами. Расширенные возможности представлены на рис. 27.33.

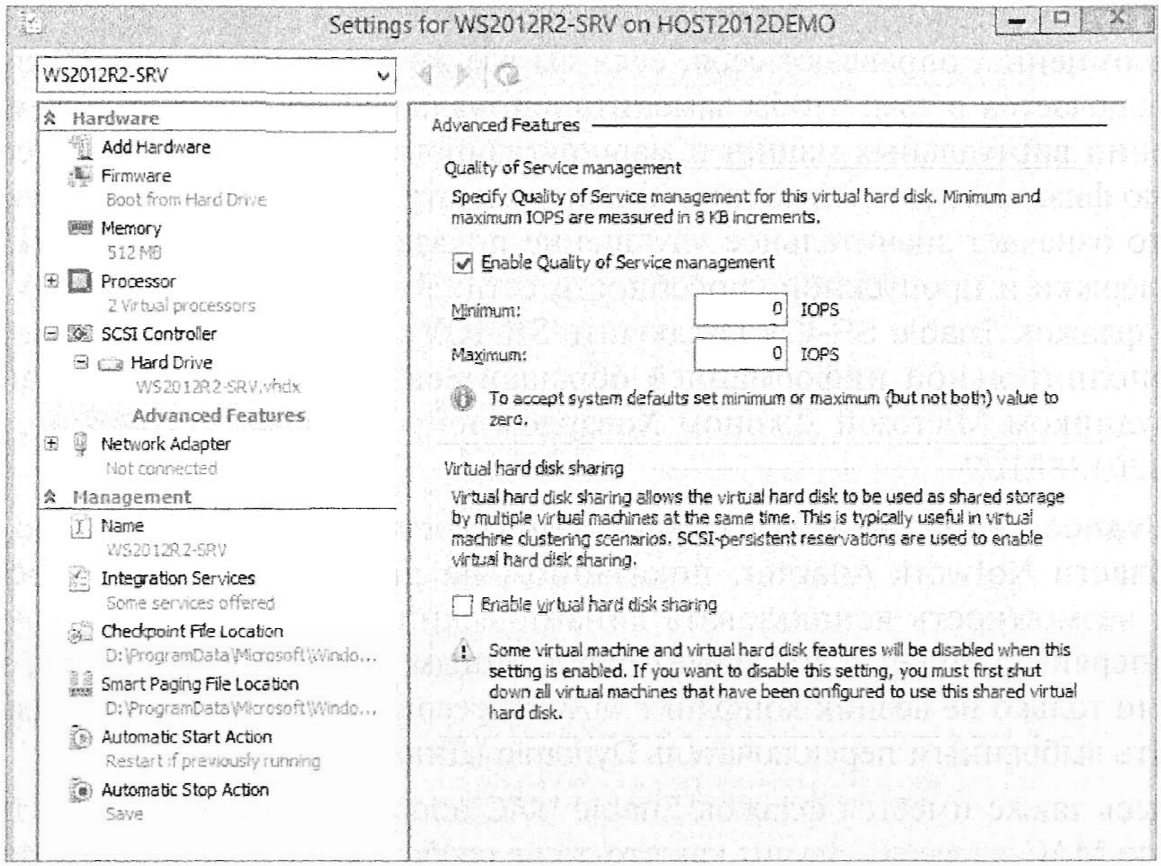


Рис. 27.33. Расширенные возможности, связанные с виртуальными жесткими дисками

- **Network Adapter (Сетевой адаптер).** Виртуальными подключениями к сети можно управлять из диалогового окна Network Adapter (Сетевой адаптер). Для каждой сетевой интерфейсной платы в раскрывающемся списке можно выбрать любой желаемый виртуальный коммутатор. Эту привязку можно изменять во время функционирования виртуальной машины, что также бывает весьма удобно. С точки зрения виртуальной машины это эквивалентно переключению кабеля из одного разъема в другой. Один из вариантов использования этой возможности предусматривает установку операционной системы, внесение исправлений с помощью Windows Update и затем соединение ее с внутренним коммутатором для тестирования.

  Как показано на рис. 27.34, раскрытие раздела Network Adapter предоставляет в ваше распоряжение следующие две настройки.

- **Hardware Acceleration (Аппаратное ускорение).** Здесь можно указывать различные задачи, которые должны быть выгружены на физический сетевой адаптер. Первая настройка — это Virtual machine queue (Очередь виртуальных машин), которая привязывает MAC-адрес виртуальной сетевой интерфейсной платы к очереди на физической сетевой интерфейсной плате, оптимизируя сетевой трафик для виртуальных машин.

  Следующим в списке идет настройка IPsec task offloading (Выгрузка задач IPsec). Она позволяет выгрузить обработку шифрования и дешифрации трафика IPsec на оборудование с целью высвобождения ресурсов на хосте.

  Последней (и, возможно, самой интересной) настройкой аппаратного ускорения является Single-root I/O virtualization (Виртуализация ввода-вывода с единым корнем), или SR-IOV. Чтобы воспользоваться этой возможностью, вам

понадобится выделенное оборудование, но такие вложения денег и времени, несомненно, оправдают себя, если вы все же решитесь на это. Идея SR-IOV заключается в том, чтобы заменить виртуальный коммутатор в схеме соединений виртуальных машин и маршрутизировать трафик прямо на специальную физическую сетевую интерфейсную плату SR-IOV, подключенную к хосту. Это означает значительное улучшение показателей утилизации ЦП, сетевой задержки и пропускной способности сети. Чтобы включить SR-IOV, отметьте флажок Enable SR-IOV (Включить SR-IOV), как показано на рис. 27.34. За дополнительной информацией обращайтесь к статье, опубликованной сотрудником Microsoft Джоном Ховардом по ссылке: `http://tinyurl.com/WS2012SRIOV`.

- **Advanced Features (Расширенные возможности).** В разделе Advanced Features области Network Adapter, показанном на рис. 27.35, вам предоставляется возможность использовать динамический или статический MAC-адрес. Гипервизор Hyper-V управляет собственным пулом MAC-адресов, поэтому, если только не возник конфликт MAC-адресов, скорее всего, вы должны оставить выбранным переключатель Dynamic (Динамический).

  Здесь также имеется флажок Enable MAC address spoofing (Включить имитацию MAC-адресов). Звучит как что-то не особо хорошее, не так ли? Между тем, это было единственное поведение, доступное в первом выпуске Hyper-V. Одна скомпрометированная виртуальная машина могла начать наводнять коммутатор или выдавать себя за какую-то другую виртуальную машину. В наши дни гипервизор Hyper-V защищен в гораздо большей степени. Виртуальный коммутатор выясняет, какой виртуальной машине соответствует тот или иной MAC-адрес, и не разрешает виртуальной машине впредь изменять свой MAC-адрес.

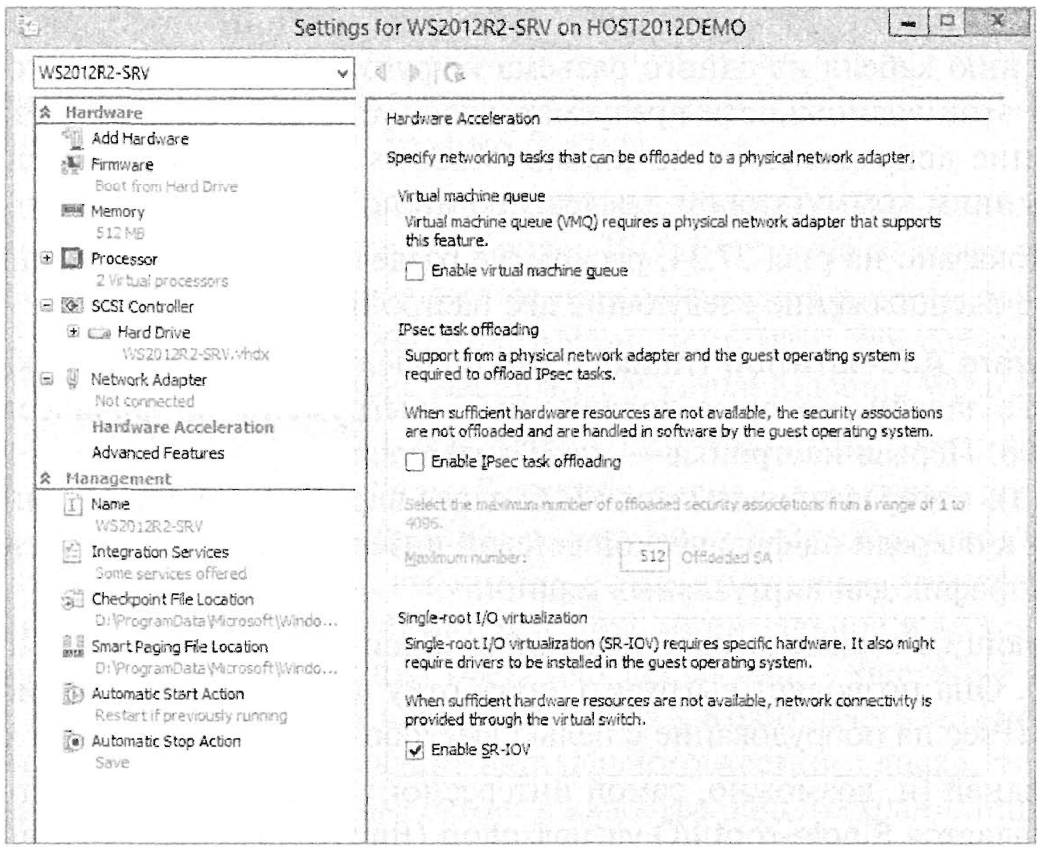


Рис. 27.34. Включение SR-IOV в виртуальной машине

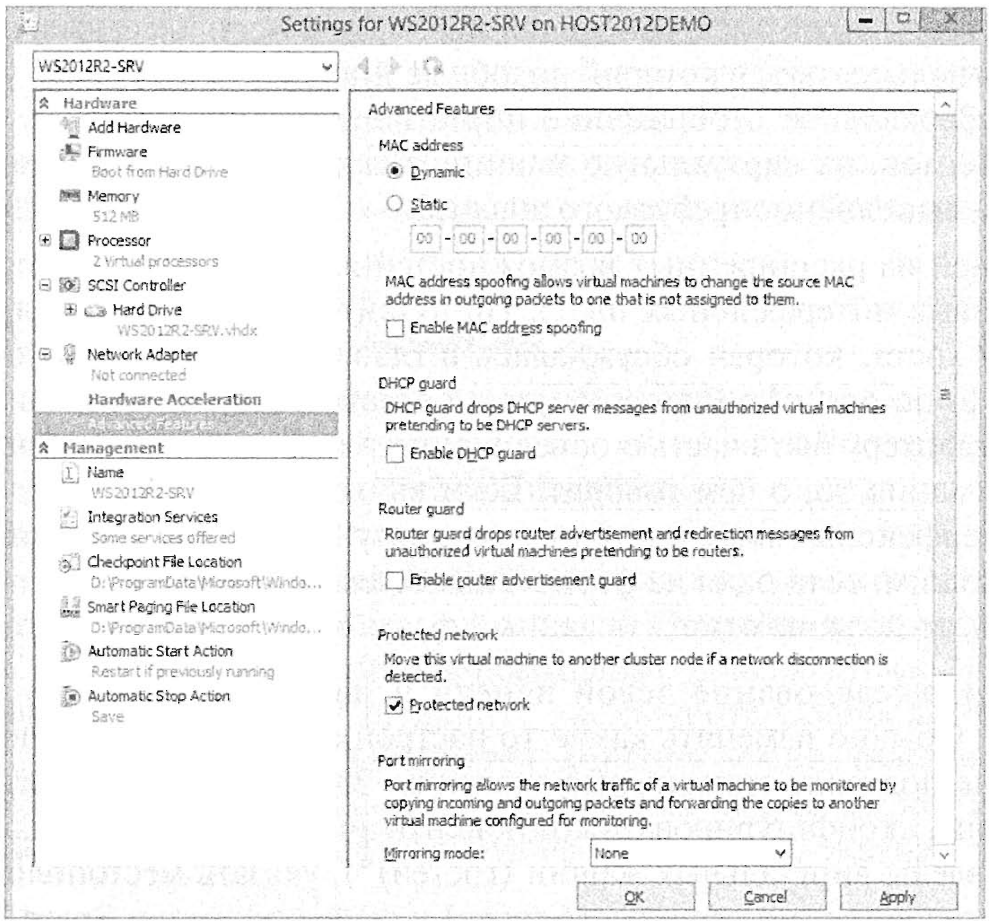


Рис. 27.35. Расширенные возможности сетевого адаптера

Обычно это не является проблемой за исключением ситуаций, когда действительно требуется много MAC-адресов. Не можете представить себе такую ситуацию? Вспомните о балансировке нагрузки или кластеризации с обходом отказа.

Если в вашей производственной среде возникли проблемы, вызванные развертыванием администраторами неавторизованных DHCP-серверов, то вряд ли стоит убеждать вас в том, что это может привести к появлению недопустимых IP-адресов и созданию серьезных проблем с администрированием. В таком случае полезной становится настройка в области DHCP guard (Защита DHCP). Если вы отметите здесь флажок Enable DHCP guard (Включить защиту DHCP), виртуальная машина перестанет отвечать DHCP-клиентам через этот конкретный сетевой адаптер.

Настройка в области Router guard (Защита маршрутизатора) очень похожа на DHCP guard: она предотвращает отправку виртуальными машинами перенаправление маршрутизатора в сеть из конкретного виртуального сетевого адаптера.

При наличии функционирующего кластера Hyper-V с обходом отказа, если вы отметите флажок Protected network (Защищенная сеть), то виртуальные машины будут перемещены в другой узел кластера в случае обнаружения утери подключения к сети, что обеспечит доступность ваших служб через сеть.

Настройку в области Port mirroring (Зеркальное отображение порта) можно применять для анализа сетевого трафика между двумя виртуальными машинами, подключенными к одному и тому же виртуальному коммутатору. Одна из этих виртуальных машин может иметь инструменты диагностики, позволяю-

щие провести такой анализ, а другая может быть частью среды с ограниченной функциональностью, в которой подобные инструменты анализа устанавливать нельзя. Зеркальное отображение порта виртуальной машины, не имеющей инструментов, на виртуальную машину с такими инструментами делает возможным выполнение требуемого анализа.

Последней из расширенных возможностей является NIC teaming (Объединение сетевых интерфейсных плат). Не путайте ее с функциональностью NIC Teaming хоста, которая обсуждалась в главе 4. Флажок Enable this network adapter to be part of a team in a guest operating system (Разрешить этому сетевому адаптеру быть частью объединения в гостевой операционной системе) делает именно то, о чем говорит. Если вы хотите создать объединение сетевых интерфейсных плат внутри своих виртуальных машин, которое остается действующим, если одна из физических сетевых интерфейсных плат перестает работать, то должны отметить данный флажок.

Продолжим исследование левой панели и перейдем к разделу Management (Управление). Обычно изменять какие-то настройки в этом разделе не приходится, т.к. вам вполне подходят стандартные значения. Здесь можно изменить имя виртуальной машины, сконфигурировать компоненты интеграции (обсуждавшиеся ранее в разделе "Разделы виртуальных машин (гостей)"), указать местоположения файла контрольных точек (рассматриваемого ниже) и файла подкачки Smart Paging, а также решить, что должно происходить при запуске или остановке хоста.

Мы еще не завершили обсуждение панели Actions, показанной на рис. 27.29. При выбранной виртуальной машине становятся доступными дополнительные действия, которые перечислены ниже.

- **Connect (Подключиться).** Используется для запуска виртуальной консоли.
- **Settings (Настройки).** Применяется для конфигурирования виртуальной машины, как объяснялось в предшествующих разделах.
- **Start (Запуск).** Используется для загрузки виртуальной машины. В зависимости от ее состояния будут предоставлены и другие возможности, такие как Shutdown (Завершение).
- **Checkpoint (Контрольная точка).** Применяется для создания образа виртуальной машины в определенный момент времени.
- **Move (Переместить).** Используется для перемещения виртуальной машины или ее хранилища.
- **Export (Экспортировать).** Применяется для сохранения всей виртуальной машины, включая конфигурацию и виртуальное оборудование.
- **Rename (Переименовать).** Используется для назначения виртуальной машине другого имени.
- **Delete (Удалить).** Применяется для удаления конфигурации виртуальной машины, но не ее виртуальных жестких дисков.
- **Enable Replication (Активизировать репликацию).** Используется для репликации всей виртуальной машины на другой хост Hyper-V.

Следует также отметить, что точный состав элементов в панели Actions зависит от состояния питания виртуальной машины. Выше перечислены действия, исходя из предположения, что питание виртуальной машины еще не включено. Когда виртуальная машина запущена, появляются дополнительные элементы, которые позволяют выключить питание виртуальной машины, выполнить сброс, завершить работу и т.п.

Установка виртуальной машины

Конфигурирование виртуальной машины — самая сложная часть работы. Следующим шагом является установка операционной системы на виртуальную машину. Хотя вы уже привыкли иметь дело с физическими серверами, но процесс установки ОС на виртуальной машине несколько отличается.

Первый вопрос касается подключения к консоли виртуальной машины. В конце концов, вы хотите видеть, что именно происходит. Откройте диспетчер Hyper-V, выберите виртуальную машину, к которой необходимо подключиться (`WS2012R2-SRV` в рассматриваемом примере), и щелкните на элементе Connect (Подключиться) в панели Actions (Действия). Откроется консоль Virtual Machine Connection (Подключение к виртуальной машине), приведенная на рис. 27.36. По-другому открыть эту консоль можно, дважды щелкнув на значке внизу экрана.

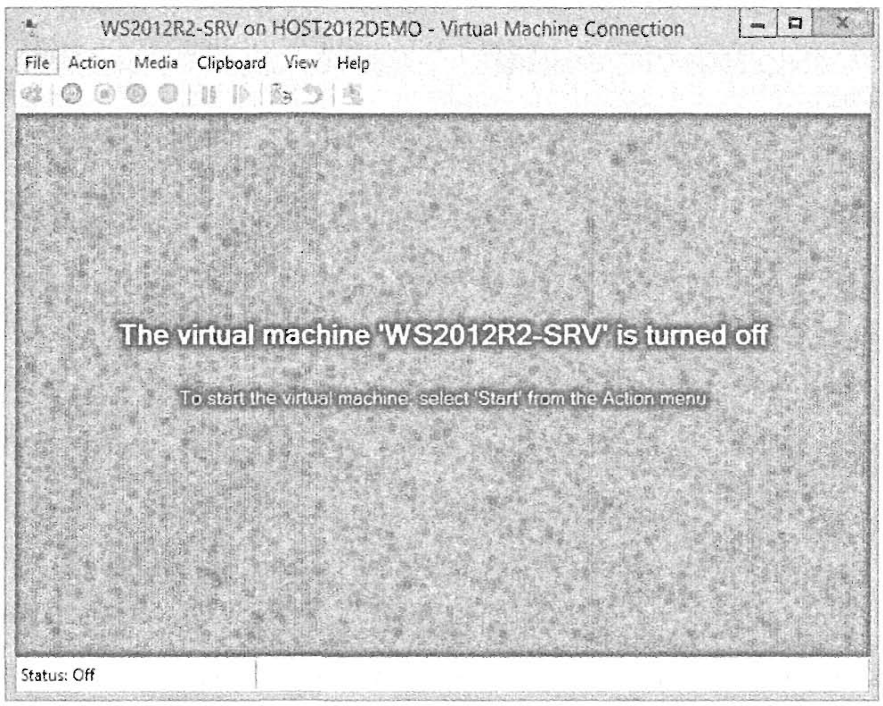


Рис. 27.36. Подключение к виртуальной машине приводит к отображению ее консоли

Виртуальная консоль содержит строку меню и панель кнопок. Большинство функций имеют дубликаты в консоли управления Hyper-V, с которыми вы уже знакомы. Черный экран, сообщающий о том, что питание виртуальной машины по имени `WS2012R2-SRV` отключено, является виртуальным экраном. Во время загрузки виртуальной машины на этом экране будут отображаться обычные сообщения, появляющиеся в процессе перехода Windows от начальной загрузки к полному графическому пользовательскому интерфейсу. Прежде чем приступить к загрузке виртуальной машины, вы должны кое о чем знать. Работа этого экрана вполне понятна, но что можно сказать о клавиатуре и мыши?

Консоль может "захватывать" клавиатуру и мышь. Вы разрешаете ей это делать, щелкая на виртуальном экране. Когда клавиатура и мышь захвачены, весь их ввод отправляется виртуальной машине. В исходном положении вы не можете перехватить управление у виртуальной машины простым перемещением курсора мыши. Чтобы освободить управление, понадобится нажать сочетание клавиш <Ctrl+Alt+стрелка влево>. В полноценно функционирующей виртуальной машине с установленными компонентами интеграции (Integration Components) все намного проще: перемещение курсора мыши с виртуального экрана на рабочий стол приводит к тому, что хост возобновляет управление клавиатурой и мышью. Существует один особый случай: последовательность <Ctrl+Alt+Del>. Даже когда управление принадлежит виртуальной машине, эту последовательность обрабатывает хост. Чтобы отправить последовательность <Ctrl+Alt+Del> виртуальной машине, можно либо нажать <Ctrl+Alt+End>, либо воспользоваться соответствующим действием в меню консоли.

Внутри виртуальной консоли

Для взаимодействия с виртуальной машиной виртуальная консоль Hyper-V использует протокол удаленного рабочего стола (Remote Desktop Protocol — RDP); это тот же самый протокол, который применяется для Remote Desktop Services. Отличие в том, что он не использует стандартный порт RDP, а взамен работает с TCP-портом 2179. Когда вы запускаете виртуальную консоль из диспетчера Hyper-V, она стартует клиентское приложение `vmconnect.exe`, находящееся в `%programfiles%\hyper-v`. Это приложение похоже на клиента Remote Desktop Client, но вдобавок позволяет выбирать виртуальную машину, к которой необходимо подключиться. Служба управления виртуальными машинами (Virtual Machine Management Service) является прослушивающей службой. Когда вы подключаетесь к ней с помощью `vmconnect.exe`, она сообщает клиенту, какие виртуальные машины доступны, и обеспечивает поступление RDP-трафика на подходящую виртуальную машину. Другими словами, эта служба действует как мультиплексор RDP.

Применение RDP и клиентского кода означает, что VMConnect использует ряд клавиатурных сокращений совместно с RDP, хотя имеет несколько собственных сокращений. Наиболее полезные из них перечислены в табл. 27.7.

Таблица 27.7. Клавиатурные сокращения виртуальной консоли Hyper-V

Комбинация клавиш Hyper-V	Комбинация клавиш Windows	Описание
<Ctrl+Alt+End>	<Ctrl+Alt+Del>	Хорошо известное "трехпальцевое приветствие", с помощью которого можно отобразить экран входа в систему или диалоговое окно безопасности
<Alt+Page Up>	<Alt+Tab>	Переключает на следующую программу
<Alt+Page Down>	<Shift+Alt+Tab>	Переключает на предыдущую программу
<Ctrl+Alt+стрелка влево>		Освобождает фокус клавиатуры и мыши, принадлежащий виртуальной машине
<Ctrl+Alt+Pause>		Выполняет переключение в полноэкранный режим и обратно

Если вы присоединили DVD-привод к контроллеру SCSI и указали с его помощью ISO-файл, как обсуждалось ранее, то можете затем открыть в виртуальной консоли меню Media (Носитель) и получить доступ к меню DVD Drive (Привод DVD). Здесь вы увидите, что файл ISO для Windows Server 2012 R2 смонтирован. Подготовив DVD-привод к загрузке, вы сможете продолжить работу. В меню Action находится пункт Start (Пуск), но быстрее щелкнуть на зеленой кнопке включения питания. На консоли отобразится несколько сообщений, после чего на короткое время появится хорошо знакомый экран загрузки Windows Server 2012 R2. Щелкните на виртуальной консоли, чтобы она захватила клавиатуру и мышь. Не забывайте, что для освобождения мыши достаточно просто нажать комбинацию клавиш <Ctrl+Alt+стрелка влево>.

Теперь следуйте приглашениям на экране и конфигурируйте операционную систему обычным образом. После установки и финальной перезагрузки вы получаете в свое распоряжение полноценно функционирующую виртуальную машину Windows Server 2012 R2. При наличии сервера DHCP в локальной сети, подключенной к виртуальному коммутатору, он также будет полностью готов к работе в сети.

Использование PowerShell для создания новой виртуальной машины

Новую виртуальную машину можно создать с применением графического пользовательского интерфейса буквально за пару минут, однако с помощью командлета `New-VM` в PowerShell это делается буквально за считанные секунды! Можете сами в этом убедиться, для чего откройте окно PowerShell с повышенными полномочиями, введите **`New-VM`** и нажмите <Enter>. Это незамедлительно создаст пустую виртуальную машину Gen1 по имени `New Virtual Machine` с ОЗУ объемом 512 Мбайт и одним ЦП.

Путем добавления к командлету `New-VM` простых дополнительных переключателей можно настраивать параметры конфигурации виртуальной машины, такие как описание, объем ОЗУ, количество ЦП и виртуальный диск. Как и в случае со всеми командлетами PowerShell, ввод `Get-Help` перед этим командлетом позволяет отобразить все доступные параметры `New-VM`, которые необходимы для быстрого развертывания виртуальных машин в Hyper-V. По следующей ссылке находится полезная статья, состоящая из трех частей, которая посвящена работе с этим командлетом: `http://blogs.technet.com/b/heyscriptingguy/archive/2013/06/14/create-a-new-virtual-machine-with-windows-powershell-part-1.aspx`.

Установкой новой виртуальной машины работа далеко не заканчивается. Если только ваша виртуальная машина не функционирует под управлением той же самой ОС и пакета обновлений, что и система хоста, то ее службы Integration Services не будут соответствовать таким службам хоста Hyper-V. Тем не менее, модернизировать Integration Services довольно легко с применением встроенного файла ISO программного обеспечения Integration Services. Детали могут несколько различаться в зависимости от версии ОС и/или ранее установленных версий Integration Services.

1. Войдите в систему виртуальной машины от имени учетной записи администратора.
2. В консоли этой виртуальной машины выберите пункт меню Action⇨Insert Integration Services Setup Disk (Действие⇨Вставить установочный диск Integration Services).

Спустя короткое время на экране появится диалоговое окно Autoplay (Автозапуск), которое должно предложить запуск программы установки (рис. 27.37). Если этого не произошло, возможно, из-за отключенной функции автозапуска, вы можете запустить программу установки непосредственно из виртуального DVD-привода в виртуальной машине.

3. Запустите программу установки.

   Далее установка проходит по накатанной дорожке. Может потребоваться одна или более перезагрузок. Если службы Integration Services уже актуальны, отобразится диалоговое окно с соответствующим уведомлением.

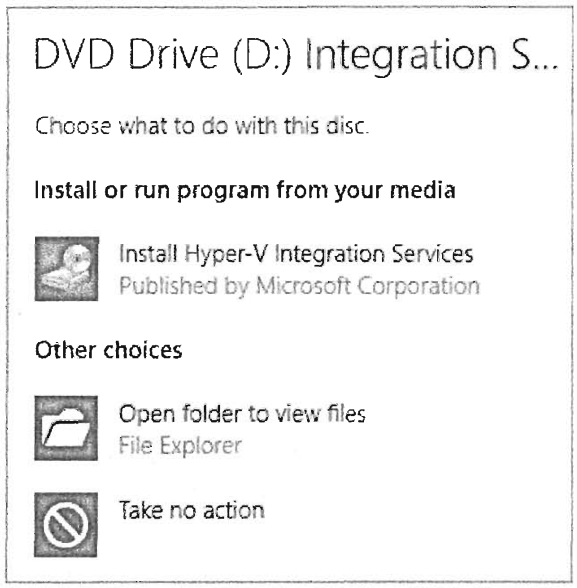


Рис. 27.37. Диалоговое окно Autoplay для установки Integration Services

---

Поддержание служб Integration Services в актуальном состоянии

Рекомендуется поддерживать службы Integration Services гостевой ОС в актуальном состоянии тем же способом, каким вы регулярно обновляете ОС своего хоста с применением пакетов обновлений и исправлений от Microsoft. При обновлении хоста службы Integration Services не обновляются до более новой версии автоматически, поэтому вы должны делать это вручную или автоматизировать процесс посредством инструмента, подобного System Center 2012 — Orchestrator. Чтобы выяснить, нуждаются ли службы Integration Services в обновлении, проверьте их версию с помощью замечательного сценария, который разработал известный специалист по Hyper-V Дидье Ван Хой: `http://workinghardinit.wordpress.com/2012/12/07/checking-host-integration-services-version-on-all-nodes-of-a-windows-server-2012-hyper-v-cluster-with-powershell/`.

И последнее замечание относительно состояний питания виртуальной машины. Физическую машину можно загружать, завершать, переводить в режим сна, приостанавливать и сбрасывать. Однако у виртуальной машины имеется еще одно состояние питания: она может находиться в *сохраненном состоянии*. Для тестовой среды это просто замечательная возможность. Оно подобно состоянию сна, но инициированному со стороны хоста. Это означает, что такое состояние работает всегда вне зависимости от того, какая ОС установлена на виртуальной машине. Действие Save

(Сохранить) можно обнаружить на обычном месте в консоли управления Hyper-V или в виртуальной консоли виртуальной машины, и после щелчка на нем вы увидите состояние Saving (Сохранение) с процентным счетчиком, показывающим ход выполнения. Запустите виртуальную машину снова, и сохраненное состояние будет перезагружено, чтобы обеспечить возобновление работы виртуальной машины в точности с того места, где она была оставлена.

Для некоторых тестов виртуальную машину удобно заморозить в определенном месте. Это отличается от сохраненного состояния, поскольку никакие данные на диске не сохраняются. Замораживание (или *пауза*, как оно называется в Hyper-V) просто немедленно останавливает работу виртуальной машины. Это еще одна возможность, которую вы вряд ли найдете на физической машине. На рис. 27.38 показаны кнопки состояний питания в консоли Hyper-V.

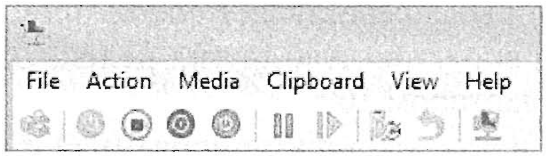


Рис. 27.38. Кнопки состояний питания виртуальной машины в консоли Hyper-V

С помощью этих кнопок (слева направо) можно выполнять следующие действия.

- Отправить виртуальной машине последовательность <Ctrl+Alt+Del>.
- Запустить виртуальную машину после прекращения работы или сохраненного состояния.
- Завершить работу виртуальной машины напрямую. ОС Windows спросит у вас, действительно ли вы хотите сделать это. Хост Hyper-V будет взаимодействовать с виртуальной машиной, чтобы инициировать обычную последовательность завершения. Это очень полезная возможность! Для этого больше не требуется входить в консоль.
- Сохранить текущее состояние виртуальной машины. При проведении тестирования это вероятно самое часто используемое действие.
- Приостановить (заморозить) виртуальную машину. Чтобы возобновить работу виртуальной машины, щелкните на этой кнопке еще раз.
- Сбросить виртуальную машину подобно аппаратному сбросу на физическом хосте.
- Создать контрольную точку для виртуальной машины: сохранить все текущее состояние и конфигурацию и создать соответствующую закладку. Виртуальная машина продолжает работать, но позже к сохраненному снимку можно возвратиться. Это чрезвычайно полезная возможность; вместе с тем, как будет показано ниже, она потенциально опасна.
- Возвратиться к сохраненной контрольной точке.
- Возвратиться к базовому сеансу. Если вы включили для своей виртуальной машины режим расширенного сеанса, то щелчок на этой кнопке перенесет виртуальную машину обратно в базовый сеанс, подобно тому, как было предусмотрено в предшествующих версиях Hyper-V.

Работа с виртуальными локальными сетями

Ранее мы уже обсуждали виртуальные коммутаторы и организацию сетей с помощью Hyper-V. Теперь, когда вы понимаете, как конфигурировать и устанавливать новую виртуальную машину, настало время углубиться в детали подключения виртуальных машин к разным подсетям сети. В мире физических сетей, если вы хотите изолировать подсети по причинам, связанным с безопасностью или масштабируемостью, то, скорее всего, воспользуетесь технологией виртуальных локальных сетей (virtual LAN — VLAN). Сеть VLAN создается на сетевом устройстве (обычно коммутаторе или маршрутизаторе) и обеспечивает изоляцию сетей посредством назначения сетевых идентификаторов.

Сети VLAN действуют на сетевом уровне 2 модели OSI. Точное определение протокола известно как 802.1Q. Каждый сетевой пакет, принадлежащий сети VLAN, имеет идентификатор, который представляет собой просто число в диапазоне от 0 до 4095, где 0 и 4095 резервируются для других целей. Давайте предположим, что есть сеть VLAN с идентификатором 100.

Сетевая интерфейсная плата, сконфигурированная с идентификатором VLAN, равным 100, будет отбирать сетевые пакеты с таким же идентификатором, игнорируя все остальные идентификаторы. Особенность сетей VLAN заключается в том, что коммутаторы и маршрутизаторы, активизированные для 802.1Q, могут представлять сети VLAN разным портам коммутаторов в сети. Другими словами, в то время как обычная IP-подсеть ограничена набором портов на физическом коммутаторе, подсеть, определенная в сети VLAN, может быть представлена на любом порте коммутатора — разумеется, если она соответствующим образом сконфигурирована.

С помощью виртуального коммутатора Hyper-V можно задействовать подключения к VLAN и назначение идентификаторов, присваивая эти идентификаторы виртуальным сетевым интерфейсным платам. Физическая сетевая плата внутри хоста должна быть подсоединена к магистральному порту VLAN на физическом коммутаторе (или на любом другом физическом сетевом устройстве, которое управляет сетью VLAN); при этом создается внешний виртуальный коммутатор Hyper-V, который назначается этой физической сетевой плате. Сконфигурировав подобным образом сеть, останется только выполнить описанные ниже шаги.

1. В настройках виртуальной машины выберите Network Adapter (Сетевой адаптер) в панели Hardware (Оборудование).
2. Подключите свою виртуальную машину к созданному ранее внешнему виртуальному коммутатору, выбрав его в раскрывающемся списке Virtual Switch (Виртуальный коммутатор).
3. В области VLAN ID (Идентификатор VLAN) отметьте флажок Enable virtual LAN identification (Включить идентификацию виртуальной локальной сети), а затем введите идентификатор VLAN в расположенном ниже поле (рис. 27.39).
4. Щелкните на кнопке OK, чтобы закрыть диалоговое окно и сохранить настройки идентификатора VLAN.

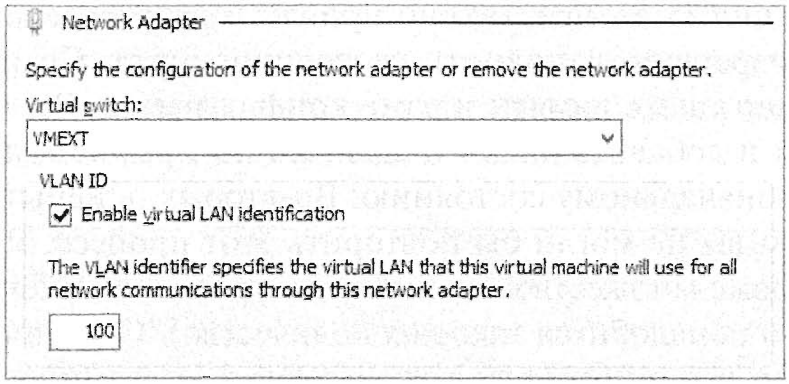


Рис. 27.39. Назначение идентификатора VLAN

Путешествие во времени с помощью контрольных точек

Как вы видели, многие возможности Hyper-V могут быть очень полезными, когда вы работаете в испытательной среде либо у себя дома, либо в своей организации. Динамические диски экономят ценное дисковое пространство, а разностные диски позволяют быстро развертывать новые виртуальные машины. Но разве не было бы замечательно, если бы можно было подготовить виртуальную машину для тестирования и легко сохранить ее, чтобы возвратиться к ней, когда что-то пойдет не так? Именно эту и другие возможности предлагают контрольные точки.

Контрольную точку лучше всего представлять себе как копию виртуальной машины в определенный момент времени. Эта копия включает виртуальные диски, память, состояние процессора и конфигурацию виртуальной машины. Виртуальная машина может быть выключена, функционировать или находиться в сохраненном состоянии — это не имеет значения. Конечно, в действительности виртуальная машина не копируется полностью; Hyper-V сохраняет только самое необходимое. При создании контрольной точки виртуальной машины гипервизор Hyper-V выполняет следующие действия.

1. Для каждого виртуального диска, подключенного к виртуальной машине, он создает новый разностный диск.
2. Он отделяет виртуальные диски от виртуальной машины и заменяет их соответствующими разностными дисками.

   С этого момента вы будете наблюдать медленное снижение производительности виртуальной машины.
3. Он копирует файлы, содержащие конфигурацию виртуальной машины.
4. Hyper-V позволяет виртуальной машине возобновить работу. Обычно в этой точке происходит простой, не превышающий одной секунды.
5. Во время работы виртуальная машина записывает содержимое своей памяти на диск. Если виртуальная машина выполняет запись в память, Hyper-V перехватывает операцию записи и первоначальное содержимое памяти быстро записывается на диск. Затем Hyper-V разрешает виртуальной машине продолжить операцию записи. Подобным образом Hyper-V сохраняет содержимое всей памяти на момент создания снимка, одновременно позволяя виртуальной машине продолжать функционирование.
6. Когда Hyper-V создание дампа памяти завершено, контрольная точка готова.

Взглянув на это внимательнее, можно прийти к ряду интересных выводов. Во-первых, Hyper-V разрешает выполнять настоящий откат. Сохраняется не только содержимое диска, но также памяти и даже конфигурации. Вы могли бы изменить содержимое памяти и добавить диски и сети, но по-прежнему иметь возможность возвратиться к первоначальному состоянию. Во-вторых, в испытательной среде нет причин, по которым вы не могли бы повторить этот процесс. Вы можете располагать цепочкой или даже множеством цепочек контрольных точек вплоть до 50 (хотя вряд ли вам когда-то понадобится такое их количество). Ограничение этого процесса заключается в том, что он работает только с виртуальными дисками. Если виртуальная машина использует диски прямого доступа, то создавать для нее контрольные точки невозможно.

Наконец, несмотря на то, что создание контрольной точки не требует много времени и является весьма соблазнительной во многих сценариях, мы настоятельно рекомендуем применять эту возможность осмотрительно, ограничившись лишь их созданием в испытательной среде. Любой, использующий в производственной среде виртуальную машину с крупными файлами контрольных точек, заметит значительное снижение производительности до тех пор, пока контрольные точки не будут удалены.

Подобно изменению состояний питания, создавать контрольную точку можно разными способами. Чтобы сделать это в консоли управления Hyper-V, щелкните правой кнопкой мыши на виртуальной машине и выберите в контекстном меню пункт Checkpoint (Контрольная точка). На рис. 27.40 показан раздел Checkpoints (Контрольные точки) диспетчера Hyper-V. Базовой контрольной точкой является Base OS Install (Базовая установка ОС); у нее есть два поддерева, которые называются After Domain Join (После присоединения к домену) и Before Service Pack (Перед применением пакета обновлений).

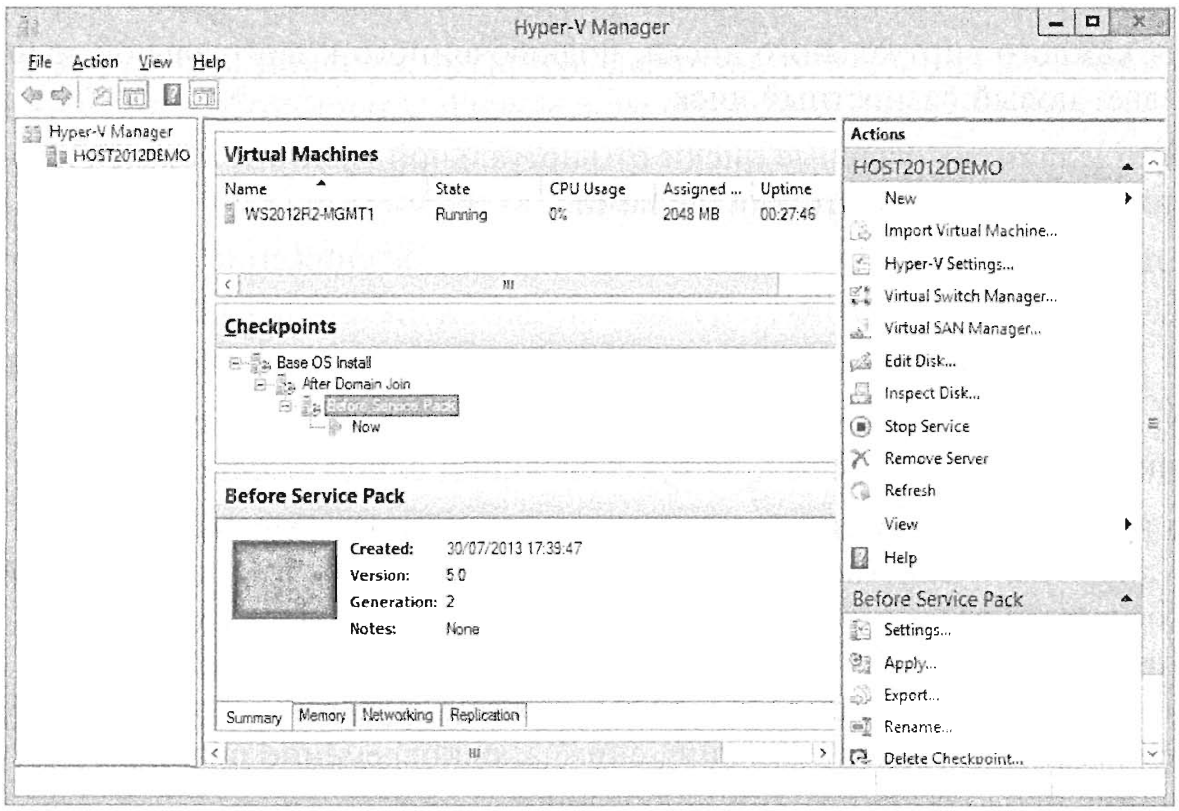


Рис. 27.40. Виртуальная машина с множеством деревьев контрольных точек

В этом примере уже имеется несколько контрольных точек. Текущая контрольная точка выделена. Ее значок отличается от значков других контрольных точек. Стандартным именем для новой контрольной точки является текущее время и дата, но разумно ее переименовать сразу же после создания.

Создание контрольные точки с помощью PowerShell

Если вам нужно снабдить сценариями процесс создания контрольных точек, то отправным пунктом является новый командлет `Checkpoint-VM`. Чтобы создать новую контрольную точку виртуальной машины со специальным именем, введите следующую команду:

```
Checkpoint-VM -Name "WS2012R2-SRV"
  -SnapshotName "Before Service Pack Install"
```

Перемещаться между контрольными точками не составляет труда. Тем не менее, если вы хотите сохранить текущее состояние, нужно сначала создать новую контрольную точку. Если этого не сделать, то самым последним сохраненным состоянием окажется состояние наиболее поздней контрольной точки. Таким образом, чтобы перейти на другую контрольную точку во время действия текущей контрольной точки, понадобится выполнить описанные ниже шаги.

1. Выберите контрольную точку, на которую хотите перейти.

   Выбрать можно любую желаемую контрольную точку, даже из тех, что находятся в середине цепочки.

2. Выберите пункт Apply (Применить) в меню Checkpoint (Контрольная точка).

   Откроется диалоговое окно с тремя переключателями: Create Checkpoint and Apply (Создать и применить контрольную точку), выбранный по умолчанию, Apply (Применить) и Cancel (Отмена).

3. Выберите подходящий переключатель, и спустя несколько секунд желаемая контрольная точка вступит в действие.

Аналогичным способом можно удалить любую контрольную точку. С позиции консоли управления это действие выглядит простым, но "за кулисами" происходит немало интересного. Ключевым фактором контрольных точек является использование разностных дисков. Так что же произойдет, если вы удалите контрольную точку из середины цепочки? В этом случае разностные диски удаленной контрольной точки сохраняются, поддерживая цепочку дисков незатронутой. Удаляются только конфигурационные файлы. В Hyper-V версии Windows Server 2012 контрольные точки можно удалять, не останавливая работу виртуальной машины, и хост объединит висячие разностные диски с их родительскими дисками безо всякого простоя. Консоль управления Hyper-V отобразит статус Merging (Объединение) и будет указывать процент выполнения этой операции. Здесь возможны и другие сценарии, однако ключевым моментом является то, что гипервизор Hyper-V осведомлен о них и будет делать то, что необходимо.

Одним из конкретных примеров может служить ситуация, когда вы удаляете виртуальную машину, которая содержит контрольные точки. Открывшееся диалоговое окно сообщит о том, что связанные с этой виртуальной машиной виртуальные

диски удаляться не будут. Однако это верно лишь отчасти. Когда вы действительно удалите виртуальную машину, действие займет больше времени, чем можно было бы ожидать. На экране остается диалоговое окно, которое указывает на то, что выполняется операция удаления (Destroying), и отображает процент ее выполнения. При этом происходит не удаление дисков, а объединение активной контрольной точки с ее родительскими дисками, оставляя вам лишь один файл `.vhdx`. Вероятно, это правильно, т.к. вам остается только один файл `.vhdx`, который представляет все данные удаленной виртуальной машины.

Контрольные точки являются великолепным средством тестирования. Вы можете экспериментировать со своей средой, как вам заблагорассудится, и у вас под рукой будет спасательный круг, который не позволит пойти на дно. Всегда ли можно рассчитывать на его помощь? К сожалению, нет. Существуют обстоятельства, когда применение какой-то более ранней контрольной точки может привести к серьезным проблемам. Для автономного компьютера, не связанного с другими, контрольные точки совершенно безопасны. В любой другой ситуации, при которой компьютеры совместно используют определенную конфигурацию, необходимо соблюдать осторожность. Самым показательным примером можно считать Active Directory.

При наличии Active Directory контрольные точки могут создавать проблемы несколькими способами. Самый очевидный пример касается контрольной точки сервера-члена, полученной, скажем, 40 дней тому назад. Как вам известно, сервер, который является членом домена, меняет свой пароль каждые 30 дней. По прошествии 40 дней этот сервер сменил свой пароль в Active Directory, по меньшей мере, один раз, а то и два. В его локальной базе хранятся два пароля: текущий и предыдущий. Если пароль менялся два раза, то сервер, для которого была создана эта контрольная точка, больше не располагает подходящим паролем в Active Directory. Другими словами, он уже не является членом домена и его необходимо повторно присоединить к домену. Эта проблема аналогична проблеме, возникающей при регулярном резервном копировании. Однако существует менее заметная и вместе с тем более опасная проблема, которая оказывает влияние на любой контроллер домена с версией Active Directory, предшествующей Windows Server 2012 (RTM).

Чтобы контроллеры домена могли выполнять репликацию, они нуждаются в определенном администрировании, в результате которого сообщается о том, какая информация уже получена ими от своих партнеров, а какая все еще отсутствует. Такое администрирование полагается на порядковые номера обновлений (update sequence number — USN), которые генерирует каждый контроллер домена с каждой модификацией его базы данных. С любым изменением ассоциирован уникальный номер USN. Идея в том, что при восстановлении снимка контроллера домена также восстанавливается конфигурация USN на данный момент времени. Проблема связана с тем, что другие контроллеры домена совершенно не знают, что это произошло! Когда они просматривают контроллер домена, снимок которого был восстановлен, то считают, что уже обработали текущий номер USN этого контроллера домена. Таким образом, партнеры репликации этого контроллера домена не видят необходимости в репликации каких-либо данных. В сущности, этот контроллер домена не будет выполнять репликацию до тех пор, пока его номер USN в конце концов не превысит значение, которое обработали его партнеры. Все данные, которые контроллер домена сгенерировал за этот период, никогда не покинут его пределы.

Эта сложная и очень серьезная проблема, которой подвержены унаследованные контроллеры домена, известна как *откат USN* и документирована в статье 875495 базы знаний Microsoft (`http://support.microsoft.com/kb/875495`). К счастью, если контроллер домена обнаруживает, что это происходит, он немедленно останавливает всю деятельность Active Directory и фиксирует проблему в журнале событий службы каталогов. Вы должны быть осведомлены о том, что использование контрольных точек может привести к неожиданным проблемам даже в системах, которые, как вам кажется, вы хорошо знаете. Лучший способ избежать таких проблем — создавать контрольные точки для компьютеров как группы после завершения их работы и восстанавливать их также как группу. Возможно, вас интересует, почему подобные проблемы не возникают при регулярном резервном копировании и восстановлении контроллера домена. Причина в том, что операциям восстановления Windows известно о настройке репликации Active Directory, поэтому они сбрасывают ее. Перейдя в онлайновый режим после непринудительного восстановления, восстановленный контроллер домена сигнализирует своим партнерам о том, что он должен трактоваться так, как если бы репликация никогда раньше не происходила. Ранее уже упоминалось, что проблеме отката USN подвержены контроллеры домена, на которых функционирует более ранняя версия Active Directory, чем Windows Server 2012 (RTM). В следующей главе мы обсудим усовершенствования виртуализации посредством Hyper-V, которые препятствуют возникновению такой проблемы в контроллерах домена Windows Server 2012.

В завершение раздела, посвященного контрольным точкам Hyper-V, можно сделать два важных вывода:

- контрольные точки являются великолепным средством тестирования, которое способно существенно облегчить вам жизнь;
- контрольные точки не должны использоваться в производственных сетях, если только вы полностью не осведомлены о рисках, связанных с их применением, но даже тогда по возможности их следует избегать.

Резюме

Уясните, что собой представляет виртуализация сервера. Вы закупаете новые серверы, главной ролью которых будет запуск Hyper-V. Однако вас заботит вопрос, способны ли новые серверы обеспечить работу Hyper-V, т.е. удовлетворяют ли они минимальным требованиям, предъявляемым Hyper-V.

> *Контрольный вопрос.* Каковы базовые требования к ЦП и BIOS для запуска Hyper-V?

Исследуйте нововведения Hyper-V в Windows Server 2012 R2. Специалисты Microsoft разработали большой набор новых возможностей и внесли множество усовершенствований в Hyper-V версии Windows Server 2012 R2, которые должны значительно облегчить IT-специалистам, администраторам и консультантам работу по убеждению своих клиентов и руководителей в необходимости использования Hyper-V в своих производственных средах.

> *Контрольный вопрос.* В ранних версиях Hyper-V сложное копирование и вставка в виртуальные машины могло быть обеспечено только с применением под-

ключения Remote Desktop и вообще не работало при отсутствии подключения к сети. Как называется новое средство, которое делает возможными копирование и вставку в виртуальную машину безо всякого сетевого подключения за счет использования VMBus?

Уясните архитектуру Hyper-V. Когда вы разворачиваете роль Hyper-V на своем компьютере, то тем самым создаете архитектуру гипервизора. *Гипервизор* — это программный уровень, который располагается между оборудованием и операционными системами, функционирующими на хосте. Такой подход называется "голым железом", т.е. виртуализация реализуется на самом низком из возможных уровней. Главная цель гипервизора заключается в создании изолированных сред выполнения (разделов) для всех операционных систем. В полном соответствии с этой функцией гипервизор отвечает за арбитраж доступа к оборудованию.

Контрольный вопрос. Во время развертывания роли Hyper-V хост пару раз перезапускается, чтобы обеспечить размещение Hyper-V поверх оборудования. На уровне какого кольца оно находится?

а. Кольцо 3

б. Кольцо 0

в. Кольцо -1

г. Кольцо 2

Установите и сконфигурируйте хост Hyper-V. Едва ли не единственным решением, которое понадобится принять перед установкой роли Hyper-V, является выбор сетевой интерфейсной платы, предназначенной для управления хостом Hyper-V. Идея в том, чтобы на хосте было, по меньшей мере, две сетевых интерфейсных платы, хотя можно обойтись и одной, если так сложились обстоятельства. В таком случае не рассчитывайте на высокую производительность. При наличии двух сетевых интерфейсных плат, выделите одну из них для управления хостом, а другую — для сетевого трафика виртуальной машины.

Контрольный вопрос. Если вы располагаете в своей среде Hyper-V двумя или большим количеством сетевых интерфейсных плат, то какой параметр, включенный по умолчанию, вы должны отключить на виртуальном сетевом адаптере?

Сконфигурируйте и установите операционную систему на виртуальной машине. Концептуально создание виртуальной машины с нуля выполняется в два этапа. Сначала вы конфигурируете виртуальное оборудование виртуальной машины, затем загружаете виртуальную машину и приступаете к установке на ней операционной системы. Когда эти два этапа будут завершены, вы можете с помощью диспетчера Hyper-V или PowerShell управлять виртуальной машиной.

Контрольный вопрос. При управлении виртуальной машиной с применением графического пользовательского интерфейса консоль может "захватывать" клавиатуру и мышь. Для этого нужно щелкнуть на виртуальном экране. После захвата весь ввод с клавиатуры и мыши отправляется виртуальной машине. В начальной стадии нельзя освободить виртуальную машину от управления клавиатурой и мышью, просто переместив курсор мыши. Какая клавиатурная комбинация сконфигурирована по умолчанию для возврата управления клавиатурой и мышью обратно операционной системе хоста?

Глава 28

Управление виртуальными машинами

В предыдущей главе вы узнали основные сведения о гипервизоре Hyper-V: процесс его установки, программную архитектуру, а также детали, связанные с виртуальными дисками и сетями. Мы также обсудили начало работы с виртуальными машинами и требования для их конфигурирования и установки. Однако это далеко не исчерпывающая информация, касающаяся Hyper-V, и в этой главе мы рассмотрим такие темы, как виртуализация контроллеров домена, живая миграция, управление виртуальными машинами и восстановление в аварийных ситуациях. Некоторые из этих тем мы обсудим лишь вкратце (просто чтобы вы получили какое-то представление о них), а о других поговорим подробнее.

В этой главе вы изучите следующие темы:

- виртуализация контроллеров домена;
- перемещение виртуальных машин;
- управление виртуальными машинами;
- восстановление в аварийных ситуациях с помощью Hyper-V.

Контроллеры домена и Hyper-V

Хотя к настоящему времени виртуализация охватила большинство аспектов серверных вычислений, виртуализация контроллеров домена всегда таила в себе определенную опасность. Однако давайте быть честными: учитывая гибкость и экономию затрат, обеспечиваемые виртуализацией, у большинства из нас возникает огромный соблазн виртуализировать контроллеры домена, и в наше время можно встретить множество виртуальных контроллеров домена, установленных на разнообразных гипервизорных платформах. До появления Windows Server 2012 при виртуализации контроллеров домена приходилось преодолевать немало препятствий и ведомственной волокиты, чтобы гарантировать поддержание целостности Active Directory.

Учитывая зависимость аутентификации Kerberos от надежного хронометража, для обеспечения работоспособности Active Directory при виртуализации контроллеров домена первостепенными становятся такие аспекты, как точная синхронизация времени внутри виртуальной машины.

Чтобы проиллюстрировать возможные проблемы, рассмотрим реальный пример — виртуальную машину, на которой функционирует контроллер домена Active Directory. Эта виртуальная машина действует на автономном хосте Hyper-V, который не присоединен к домену. Хост получает показания времени от какого-то сетевого компонента, например, централизованного коммутатора. При проведении обслуживания прошивка коммутатора обновляется, и он случайно устанавливает время, опережающее на год текущее. Хост получает это показание и также устанавливает время с опережением на год. Затем то же самое происходит с виртуальным контроллером домена. С этого момента он прекращает выполнение репликации со своими партнерами, поскольку нарушена аутентификация Kerberos, и вскоре вам начнут звонить пользователи, жалуясь на проблемы с входом в систему. Еще одна проблема с неудовлетворительной синхронизацией времени внутри виртуальных контроллеров домена связана с тем, что внутренняя процедура администрирования Active Directory в отношении удаленных объектов начинает идти вкривь и вкось, если показание времени скачкообразно изменяется слишком далеко вперед. Некоторые объекты будут удалены безвозвратно, другие — нет. В результате получится изрядно поврежденный лес. Если задуматься о возможных последствиях, то их список будет расти и расти. Вывод очевиден: в производственной среде очень важно обеспечить корректную настройку синхронизации времени, особенно для виртуальных машин.

Должна ли быть отключена служба синхронизации времени?

По мнению многих, чтобы справиться с проблемами синхронизации времени в виртуальных контроллерах домена, достаточно отключить службу синхронизации времени (Time Synchronization), входящую в состав компонентов интеграции, для виртуальной машины посредством консоли Hyper-V. К сожалению, это не так, а в долгосрочной перспективе появятся еще и дополнительные проблемы.

Лучше всего никогда не блокировать службу Time Synchronization, а вместо этого дополнить ее функциональность внешним источником показаний времени. В следующей статье Бена Армстронга объясняется рекомендуемый способ управления синхронизацией времени: `http://blogs.msdn.com/b/virtual_pc_guy/archive/2010/11/19/time-synchronization-in-hyper-v.aspx`.

После ознакомления с этой статьей перейдите по указанной ниже ссылке от Microsoft, чтобы автоматически сконфигурировать надежный внешний источник времени, щелкнув на кнопке Microsoft Fix It или на ссылке Устранить проблему в нижней части страницы: `http://support.microsoft.com/kb/816042`.

Синхронизация времени — не единственный аспект, о котором нужно помнить, имея дело с виртуальными контроллерами домена. В главе 27 мы обсуждали проблему отката USN, которая оказывала влияние на контроллеры домена с версиями Active Directory, предшествующими Windows Server 2012, при использовании контрольных точек. При наличии в кластере Hyper-V с обходом отказа виртуального контроллера домена, функционирующего под управлением Windows Server 2008, могла возникать еще одна проблема. Если только вы не развернули его *весьма* спе-

цифическим способом, то необходимо было позаботиться о существовании за пределами кластера, по меньшей мере, одного физического контроллера домена, чтобы обеспечить перезапуск всех компонентов после перезагрузки кластера. В следующей статье базы знаний Microsoft подытоживаются некоторые из этих проблем и описана политика Microsoft по поддержке виртуальных контроллеров домена:

`http://support.microsoft.com/kb/888794`

В данный момент у вас может возникнуть вполне закономерный вопрос: зачем заниматься виртуализацией контроллеров домена, если это создает такие проблемы? К счастью, как будет показано в следующем разделе, средства Hyper-V и Active Directory в версии Windows Server 2012 R2 прошли долгий путь в разрешении многих проблем.

Виртуальные контроллеры домена, которые работают без проблем

Начиная с версии Windows Server 2012, виртуальные контроллеры домена получили новый встроенный идентификатор, который называется *VM-Generation ID* (Идентификатор поколения виртуальной машины). Этот новый идентификатор предназначен для защиты в ситуациях, когда виртуальный контроллер домена откатывается назад во времени с применением контрольных точек, что приводит к возникновению проблемы отката USN (update sequence number — порядковый номер обновления), как описано по ссылке `http://tinyurl.com/USNRollback`.

Когда виртуальный контроллер домена Windows Server 2012 развернут, идентификатор VM-Generation ID сохраняется в базе данных Active Directory как атрибут *`msDS-GenerationID`* вновь созданной учетной записи компьютера (рис. 28.1). Драйвер Windows внутри виртуальной машины гарантирует, что идентификатор VM-Generation ID постоянно отслеживается независимым образом.

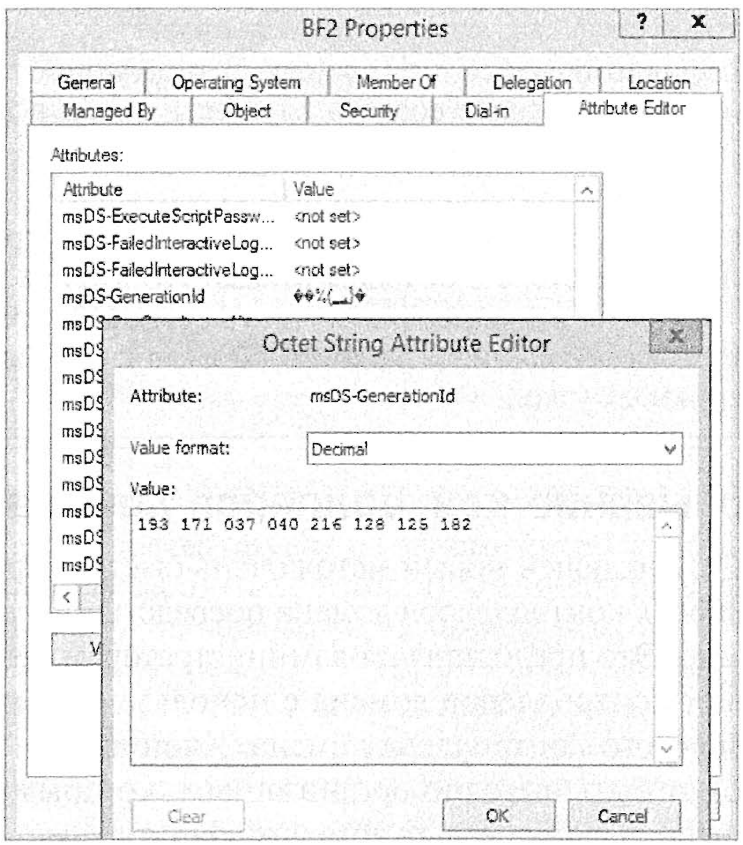


Рис. 28.1. Атрибут `msDS-GenerationID`

Например, если производится откат виртуального контроллера домена к предыдущей контрольной точке, то значение VM-Generation ID экземпляра контрольной точки сравнивается с текущим значением VM-Generation ID, которое хранится в базе данных Active Directory. Если эти два значения не совпадают, происходит сброс еще одного уникального идентификатора, известного как InvocationID, что, в свою очередь, предотвращает повторное использование номера USN, помогая избежать отката USN. Это определенно желанное изменение по сравнению с ранними версиями Active Directory, которое содействует более безопасной виртуализации контроллеров домена.

Другой целью, лежащей в основе решения с идентификаторами VM-Generation ID, было обеспечение их независимости от поставщиков гипервизоров, т.е. преимущества этих идентификаторов не ограничиваются виртуальными контроллерами домена, функционирующими под управлением Hyper-V. Эта возможность может применяться даже с виртуальными контроллерами домена, работающими на хосте VMware!

Самозагрузка кластера означает, что физические контроллеры домена больше не нужны

Если в прошлом вы конфигурировали кластер Hyper-V с обходом отказа на основе Windows Server 2008 R2, то наверняка знаете о наличии требования иметь физический контроллер домена или хотя бы контроллер домена, расположенный на автономном виртуальном хосте, который не является частью данного кластера. Причина этого требования заключалась в том, что кластеру с обходом отказа необходима была возможность аутентификации с помощью контроллера домена, прежде чем он мог бы произвести загрузку. Если единственный контроллер домена в среде представлял собой виртуальную машину, размещенную внутри кластера, который пытался загрузиться, то, фигурально выражаясь, вы оказывались в безвыходном положении.

В кластерах с обходом отказа Windows Server 2012 появилась возможность *самозагрузки кластера* — новое средство, которое позволяет кластеру загрузиться без предварительной аутентификации в Active Directory. Это делается за счет разрешения загружаемому узлу кластера сначала создать кластер и затем попытаться получить кворум. Как только это произойдет, будут загружены остальные узлы кластера — без необходимости в аутентификации на контроллере домена.

Самозагрузка кластера происходит по умолчанию, не требуя предварительно конфигурировать что-либо в кластере с обходом отказа. Но имейте в виду — это вовсе не означает, что вы не должны заранее располагать средой Active Directory, которая по-прежнему требуется для создания исходного объекта кластера, а также во время добавления в кластер новых узлов.

Быстрое развертывание контроллеров домена

В Windows Server 2012 включен новый метод очень быстрого развертывания любого количества виртуальных контроллеров домена посредством *клонирования виртуальных контроллеров домена*. Это предоставляет администраторам решение для оперативного ввода одинаковых контроллеров домена с использованием в качестве эталона существующего шаблонного контроллера домена. Клонирование виртуальных контроллеров домена может быть выгодно организациям, которым необходимо быстро развернуть много контроллеров в новых доменах. Данное средство также полезно в частных облачных средах при удовлетворении требований масштабируемости.

Однако вполне вероятно, что чаще всего эта функция будет применяться в тестовых и демонстрационных средах, где могут быть развернуты многочисленные конфигурации контроллеров домена для опробования новых средств и возможностей до их внедрения в производственной среде.

Предварительные условия для клонирования виртуальных контроллеров домена

В этом разделе мы обсудим предварительные условия, которые должны быть удовлетворены, чтобы можно было приступить к клонированию виртуальных контроллеров домена.

- Учетная запись пользователя, являющегося членом группы `Domain Admins` (Администраторы домена) в Active Directory.
- По меньшей мере, один хост Hyper-V (в нашем примере — `VMHOST1-SRV`), работающий под управлением Windows Server 2012 или последующей версии.
- Права локального администратора на сервере хоста Hyper-V.
- Должен быть заранее развернут контроллер домена Windows Server 2012 или выше, на котором функционирует роль FSMO эмулятора PDC (`WS2012R2-DC1`).

  Чтобы просмотреть, на каком сервере находится эта роль в существующей среде Active Directory, можно ввести команду **`netdom query fsmo`**. Этот сервер не будет частью процесса клонирования и применяется главным образом для аутентификации и аудита безопасности.
- Виртуальный контроллер домена, работающий под управлением Windows Server 2012 или последующей версии (`WS2012R2-DC2`), в том же самом домене, что и упомянутый выше эмулятор PDC. Это шаблонный контроллер домена, который вы будете использовать для клонирования. Данный шаблонный контроллер домена не должен иметь роли DHCP, Active Directory Certificate Services или Lightweight Directory Services, т.к. клонирование не поддерживает ни одну из них. Он может иметь установленную роль DNS-сервера, который хранит зоны, интегрированные с Active Directory, но вы должны давать себе отчет в том, что тогда клонируемый контроллер домена также будет развернут как DNS-сервер.
- Удостоверьтесь в том, что виртуальный привод гибких дисков (virtual floppy drive — VFD) на шаблонном виртуальном контроллере домена пуст, поскольку если оставить его подключенным, могут возникнуть проблемы при попытке выполнить импортирование новой виртуальной машины.

Требования к клонированию между несколькими хостами

Если вы клонируете контроллер домена из одного хоста Hyper-V и помещаете его на другой хост, вам нужно позаботиться о том, чтобы имена виртуальных сетевых коммутаторов были в точности одинаковыми на каждом узле, подверженном экспорту и импорту. Например, если на хосте `Host1` имеется виртуальный коммутатор по имени `VMEXT1`, то на хосте `Host2` также должен присутствовать виртуальный коммутатор по имени `VMEXT1`. Кроме того, если хосты располагают разными процессорами, удостоверьтесь, что на виртуальном контроллере домена, который вы собираетесь экспортировать первым, отмечен флажок Migrate to a physical computer with a different processor version (Перейти на физический компьютер с другой версией процессора).

Клонирование виртуального контроллера домена

После удовлетворения всех перечисленных выше предварительных условий вы готовы выполнить последовательность действий, описанную в этом разделе, и клонировать свой первый виртуальный контроллер домена.

1. Войдите в систему контроллера домена, на котором установлена роль PDC Emulator (Эмулятор PDC), с применением учетной записи администратора домена и в окне диспетчера серверов выберите пункт меню Tools⇨Active Directory Users and Computers (Сервис⇨Пользователи и компьютеры Active Directory).
2. Раскройте объект корня домена и затем щелкните на организационной единице `Users` (Пользователи).

   Вы должны увидеть группу доступа `Cloneable Domain Controllers` (Клонируемые контроллеры домена), как показано на рис. 28.2.

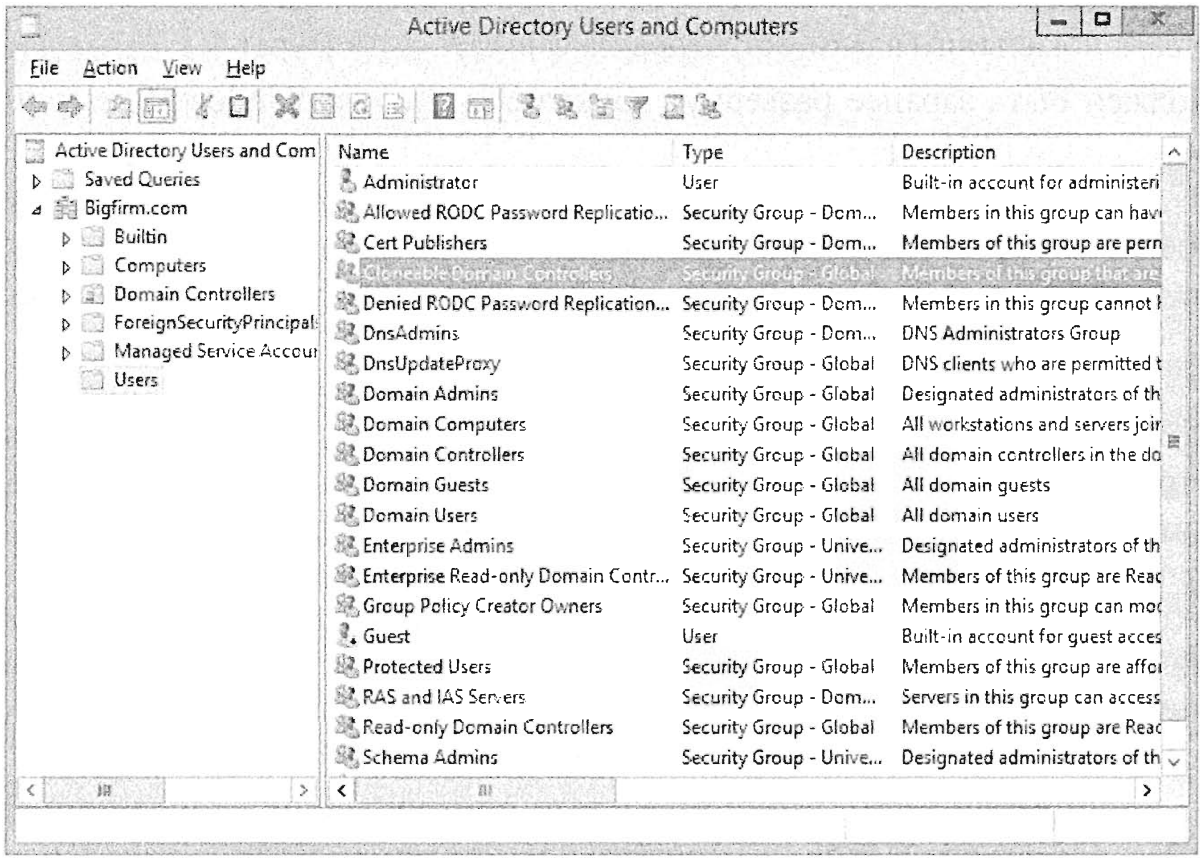


Рис. 28.2. Группа доступа `Cloneable Domain Controllers`

Эта группа управляется бригадой администраторов Active Directory и предназначена для контроля над тем, какие контроллеры домена будут клонироваться. Обычно в среде безопасности с низкими привилегиями бригады Active Directory и виртуализации будут отдельными сущностями, гарантируя то, что авторизацией на клонирование критически важного сервера, такого как контроллер домена, управляет бригада AD. Если вы не видите эту группу, значит, вы не используете контроллер домена Windows Server 2012 для размещения роли PDC Emulator, как упоминалось ранее.

3. Дважды щелкните на группе `Cloneable Domain Controllers`, в открывшемся диалоговом окне перейдите на вкладку Members (Члены) и щелкните на кнопке Add (Добавить).

4. Щелкните на кнопке Object Types (Типы объектов) и в открывшемся окне отметьте флажок Computers (Компьютеры); затем введите имя шаблонного виртуального контроллера домена (`WS2012R2-DC2`) и щелкните на кнопке Add.
5. Щелкните на кнопке OK, чтобы закрыть окно и подтвердить, что этот шаблонный виртуальный контроллер домена добавлен в группу.

   Теперь, когда шаблонный виртуальный контроллер домена авторизован для клонирования, необходимо удостовериться в том, что все выполняющиеся на нем приложения (если они есть) могут быть безопасно клонированы.
6. Для этого войдите в систему шаблонного виртуального контроллера домена под учетной записью с административными разрешениями и запустите командлет PowerShell по имени `Get-ADDCCloningExcludedApplicationList`.
7. Просмотрите результирующий список приложений и выясните у поставщика ПО, поддерживается ли клонирование этих приложений (если это уместно).
8. Чтобы подготовить эти приложения, в окне PowerShell с повышенными полномочиями введите команду `Get-ADDCCloningExcludedApplicationList -GenerateXML`. В результате создается новый XML-файл `CustomDCCloneAllowList.xml`, по умолчанию расположенный в `%windir%\NTDS` (рис. 28.3).

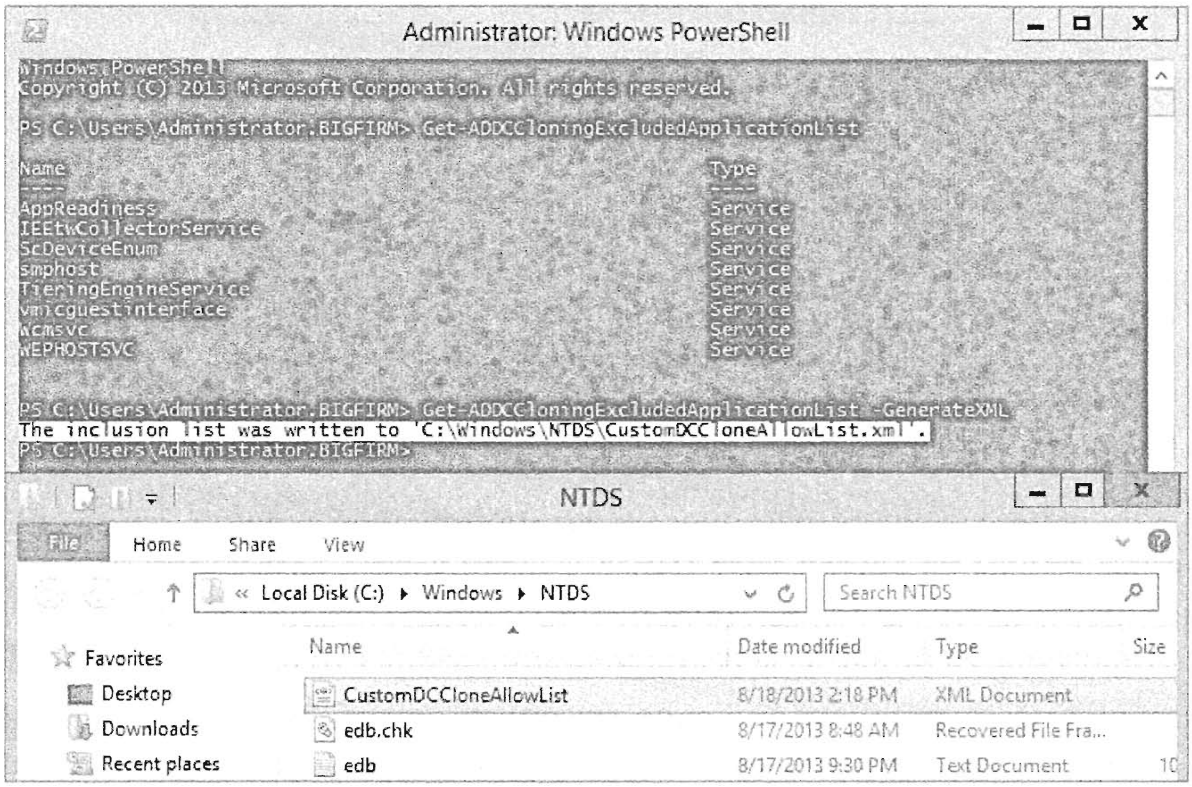


Рис. 28.3. Подготовка приложений для клонирования

9. Оставаясь в окне PowerShell на шаблонном виртуальном контроллере домена, вам теперь необходимо запустить командлет `New-ADDCCloneConfigFile` со всеми параметрами, требуемыми для нового клона контроллера домена (имя хоста, информация TCP/IP и т.д.). Выполнение этого командлета приведет к созданию файла `DCCloneConfig.xml`, который будет использоваться для запуска и обеспечения успешного выполнения клонирования. С полным синтаксисом этого командлета можно ознакомиться по ссылке `http://technet.microsoft.com/en-us/library/jj158947.aspx`.

10. Введите следующую команду, чтобы создать файл DCCloneConfig (подставив параметры, соответствующие вашей среде):

```
New-ADDCCloneConfigFile -Static
  -IPv4Address "192.168.0.210"
  -IPv4DNSResolver "192.168.0.100"
  -IPv4SubnetMask "255.255.255.0"
  -CloneComputerName "WS2012R2-DC3"
  -IPv4DefaultGateway "192.168.0.254"
  -SiteName "DUBLIN"
```

11. Теперь завершите работу шаблонного виртуального контроллера домена (в нашем примере — WS2012R2-DC2) и, прежде чем продолжить, удалите любые контрольные точки, которые вы могли создать ранее.

12. В диспетчере Hyper-V выберите остановленный шаблонный виртуальный контроллер домена и щелкните на элементе Export (Экспортировать) в панели Actions (Действия). В открывшемся диалоговом окне Export Virtual Machine (Экспортирование виртуальной машины) укажите место, куда будет экспортироваться эта виртуальная машина (рис. 28.4), и щелкните на кнопке Export (Экспорт).

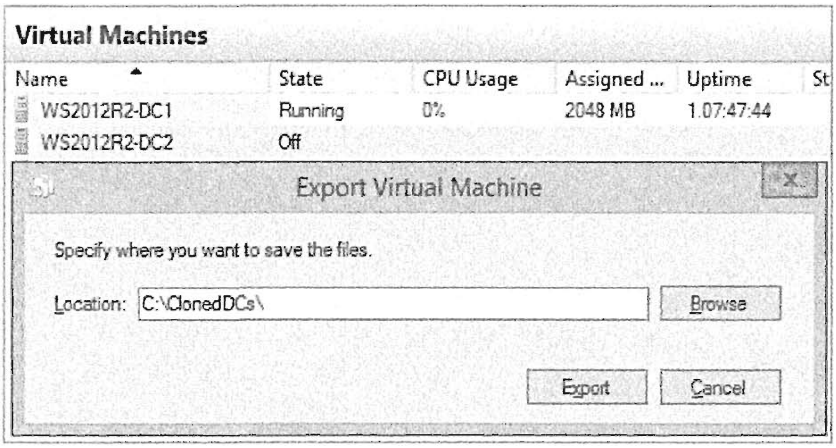


Рис. 28.4. Экспортирование шаблонного виртуального контроллера домена

Когда процесс экспорта завершится, вы можете либо скопировать экспортированные файлы на другой хост Hyper-V (если хотите развернуть на нем новый клон контроллера домена), либо просто оставить их там, куда они были экспортированы, если в вашем распоряжении имеется только один хост.

13. Независимо от того, где выбрано место для сохранения экспортированных файлов, находясь на хосте Hyper-V, разверните новый клон контроллера домена, откройте диспетчер Hyper-V и щелкните на элементе Import Virtual Machine (Импортировать виртуальную машину) в панели Actions.

14. В мастере Import Virtual Machine (Импортирование виртуальной машины) щелкните на кнопке Next (Далее), чтобы перейти на экран Locate Folder (Местонахождение папки), и укажите место хранения экспортированных файлов.

15. Щелкните на кнопке Next.

16. На экране Select Virtual Machine (Выбор виртуальной машины) убедитесь в том, что имя шаблонного виртуального контроллера домена выбрано как виртуальная машина, подлежащая импорту, и щелкните на кнопке Next.

17. На экране Choose Import Type (Выбор типа импортирования) понадобится выбрать переключатель Copy the virtual machine (create a new unique ID) (Копировать виртуальную машину (создать новый уникальный идентификатор)), как показано на рис. 28.5; затем щелкните на кнопке Next.

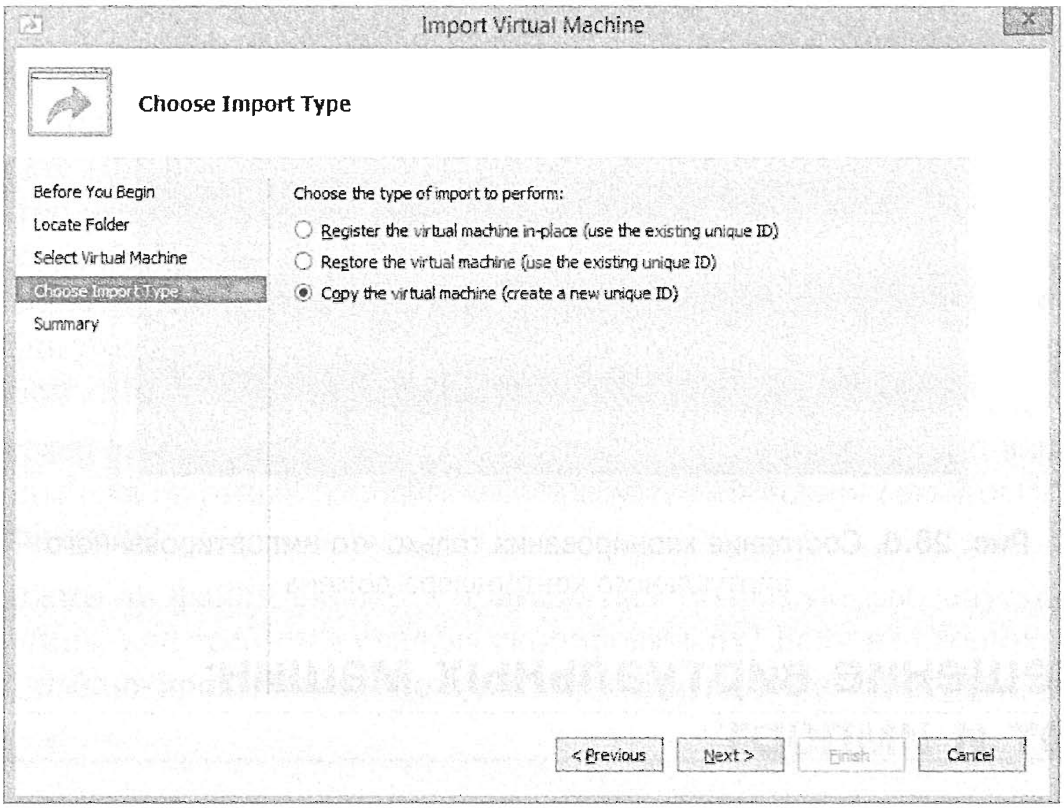


Рис. 28.5. Создание уникального идентификатора для импортированной виртуальной машины

Следующие два экрана позволяют выбрать папки для сохранения импортированных виртуальных машин и указать, хотите ли вы создать несколько клонов контроллера домена с помощью графического пользовательского интерфейса диспетчера Hyper-V.

18. Указывайте здесь новое местоположение папки каждый раз, когда выполняете импорт из шаблонного виртуального контроллера домена.
19. Щелкните на кнопке Next, чтобы продвинуться дальше в мастере; затем щелкните на кнопке Finish (Готово), чтобы начать импортирование.
20. Когда процесс импорта завершится, запустите шаблонный виртуальный контроллер домена (`WS2012R2-DC2`) снова, а когда он начнет работать, запустите только что импортированную виртуальную машину (`WS2012R2-DC3`).

    Как только новый контроллер домена запустится, вы должны увидеть сообщение, свидетельствующее о ходе клонирования контроллера домена (рис. 28.6).

После завершения клонирования нового виртуального контроллера домена вы увидите, что клонированный контроллер домена стал членом группы доступа `Cloneable Domain Controllers`. Это произошло потому, что он скопировал членство в группах из исходного шаблонного виртуального контроллера домена. В Microsoft рекомендуют оставлять эту группу доступа пустой до тех пор, пока вы не выполните операции клонирования, и по завершении клонирования понадобится удалить членов этой группы.

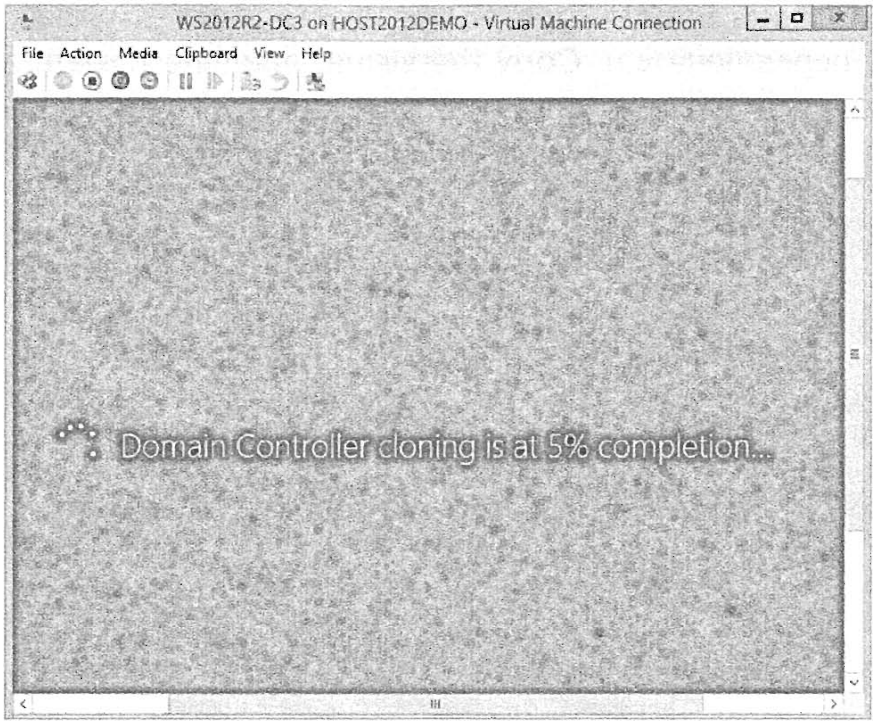


Рис. 28.6. Состояние клонирования только что импортированного виртуального контроллера домена

Перемещение виртуальных машин: экспорт и импорт

Одно из важнейших преимуществ технологии виртуализации серверов заключается в том, что поскольку виртуальные машины представляют собой всего лишь наборы файлов (включающие файлы виртуальных дисков и XML), вы можете легко перемещать их между физическими хостами; это не особо отличается от вырезания, копирования или вставки обычных файлов и папок.

Как обсуждалось ранее в разделе "Клонирование виртуального контроллера домена", гипервизор Hyper-V версии Windows Server 2012 предлагает функции относительно простого *экспорта* и *импорта* виртуальных машин между хостами. Это стало возможным благодаря тому факту, что все хосты Hyper-V предоставляют своим виртуальным машинам практически идентичное оборудование посредством компонентов интеграции и синтетических драйверов. Если вы хотели перемещать установленные копии ОС в мире физических серверов, то должны были переносить, по меньшей мере, физические диски, что возможно лишь в случае достаточного сходства оборудования (причем даже это не служило гарантией успеха). Если оборудование не было похожим, то, как правило, приходилось переустанавливать всю ОС. В этом разделе мы более подробно обсудим экспорт и импорт Hyper-V, на этот раз между двумя хостами. Все, что для этого понадобится — обычная высокоскоростная сеть между ними (из-за передачи большого объема данных). Сеть SAN в этом случае не требуется.

Виртуальная машина имеет три параметра: конфигурацию, текущее состояние и данные. При перемещении виртуальной машины на другой хост Hyper-V вам нужно обеспечить перенос всех этих трех параметров. В консоли управления Hyper-V доступен мастер экспорта виртуальной машины (Export Virtual Machine Wizard), который собирает все относящиеся к делу данные, включая контрольные точки, и копирует их в целевую папку. Такая возможность существует, начиная с самого пер-

вого выпуска Hyper-V. Важная особенность экспортирования виртуальной машины в Windows Server 2012 состоит в том, что это можно делать, когда она находится в онлайновом режиме — в противоположность тому, что в ранних версиях сначала требовалось завершить работу экспортируемой виртуальной машины. Это по-настоящему полезная возможность, которая позволяет быстро получить копию функционирующего сервера в производственной среде и поместить ее в испытательную среду для контроля обновлений программного обеспечения или поиска и устранения проблем в приложениях.

На хосте Hyper-V, где вы хотите разместить виртуальную машину, нужно запустить мастер импорта виртуальной машины (Import Virtual Machine Wizard) — и это почти все, что потребуется сделать.

Первый момент, о котором следует знать — операция экспорта просто копирует всю конфигурацию виртуальной машины, ее состояние и данные. Операция импорта отличается. Необходимо принять несколько решений.

- Должен ли быть сохранен уникальный идентификатор старой виртуальной машины (стандартный вариант) или требуется сгенерировать новый такой идентификатор?
- Должны ли файлы экспорта применяться напрямую для запуска виртуальной машины или требуется сначала скопировать их? Если не скопировать эти файлы, импортирование можно будет выполнить только один раз.

Идентификаторы виртуальных машин

Как известно большинству опытных администраторов Windows, многие объекты в мире Windows имеют несколько имен. Широко известным примером может служить объект Active Directory. Его настоящее имя — *глобально уникальный идентификатор* (globally unique identifier — GUID), но мы предпочитаем использовать такие читабельные для человека имена, как *отображаемое имя* или *общее имя*. То же самое касается виртуальных машин. Их настоящим именем также является идентификатор GUID, который не изменяется даже в результате переименования сервера. Вместе с тем, отображаемое имя может быть каким угодно. Другие объекты в мире виртуальных машин, например, виртуальные коммутаторы и сетевые интерфейсные платы, также могут иметь идентификаторы GUID.

Интересное свойство виртуальных машин заключается в том, что их идентификаторы должны быть уникальными, но отображаемые имена могут быть идентичными. Это обычно происходит, когда виртуальная машина импортируется на тот же хост, на котором она экспортировалась. До тех пор, пока при импорте применяется другой идентификатор, все работает без проблем.

Второй и более тонкий момент связан с конфигурацией виртуальной сети. Откуда виртуальной машине известно о том, какие виртуальные коммутаторы использовать на новом хосте? Внутренне каждый виртуальный коммутатор известен по своему идентификатору GUID, что позволяет назначать ему любое имя, не влияя на его отношения с виртуальными сетевыми интерфейсными платами. Но если вы создаете виртуальный коммутатор на другом хосте, он будет иметь другой GUID. Чтобы обойти это, гипервизор Hyper-V предпринимает небольшой трюк. При импортировании он ищет виртуальные коммутаторы с точно таким же отображаемым именем

(учитывая регистр символов), как у виртуальных коммутаторов, которые включены в файлы экспорта. Если такие коммутаторы обнаруживаются, то виртуальные сетевые интерфейсные платы подключаются, а если нет, то импортированная виртуальная машина будет иметь отключенные сетевые интерфейсные платы.

Давайте рассмотрим пример, в котором задействован экспорт и импорт виртуальной машины. Подошла бы любая виртуальная машина, но в этом случае мы будем использовать `WS2012R2-SRV1`. В идеальной ситуации вы должны располагать вторым хостом Hyper-V для импорта, но в примере мы обойдемся одним хостом.

Предположим, что у вас есть второй хост; для импортирования мы будем применять хост `VMHOST2-SRV` в качестве целевого. Создайте общую папку с описательным именем наподобие `ImportedVMs`. Разрешения на совместное использование этой папки несколько запутанны. Процесс экспорта выполняется от имени учетной записи `SYSTEM`, а не вашей. Таким образом, общая папка должна иметь разрешения, которые позволяли бы учетной записи компьютера хоста производить запись данных. Предоставьте доступ по записи либо учетной записи компьютера исходного хоста (в нашем примере — `VMHOST1-SRV`), либо участнику безопасности `Everyone`. Затем начните процесс экспорта на исходном хосте.

1. В консоли управления Hyper-V выберите виртуальную машину, которую хотите экспортировать (в рассматриваемом примере это `WS2012R2-SRV1`).
2. Не останавливая работу выбранной виртуальной машины, щелкните на элементе Export (Экспортировать) в панели Actions (Действия).
3. Введите целевой путь для экспорта.

   Это может быть локальный диск, устройство USB или удаленное сетевое местоположение. На этот раз мы будем экспортировать напрямую на другой хост Hyper-V: `\\vmhost2-srv\ImportedVMs`. Если этот путь не существует, мастер создаст его. Независимо от указанного здесь пути, мастер создаст подкаталог с именем виртуальной машины.

После завершения процедуры экспорта вы займетесь импортированием виртуальной машины. Это можно сделать в консоли управления Hyper-V на исходном сервере, добавив целевой хост как дополнительную управляемую машину, но в этом примере вы напрямую войдете в систему целевого хоста.

1. Войдите в систему `VMHOST2-SRV` с применением административной учетной записи и откройте консоль управления Hyper-V.
2. Если вы хотите, чтобы виртуальные сетевые интерфейсные платы подключались автоматически при импорте, удостоверьтесь в наличии на обоих хостах виртуальных коммутаторов с полностью одинаковыми именами.

   В нашем примере для управления используется `MGMTNIC`, а для внешних сетевых подключений — `VMEXT1`.
3. Щелкните на элементе Import Virtual Machine (Импортировать виртуальную машину) в панели Actions (Действия) консоли управления Hyper-V. В открывшемся окне мастера щелкните на кнопке Next (Далее).
4. На экране Locate Folder (Местонахождение папки) укажите путь к месту хранения экспортированной виртуальной машины, такой как `D:\ImportedVMs\WS2012R2-SRV1`, и щелкните на кнопке Next.

5. На экране Select Virtual Machine (Выбор виртуальной машины) убедитесь в том, что для импорта выбрана корректная версия виртуальной машины, затем щелкните на кнопке Next.

   Переключатели на экране Choose Import Type (Выбор типа импортирования), который был показан ранее на рис. 28.5, заслуживают определенного внимания.

   - **Register the virtual machine in-place (use the existing unique ID) (Зарегистрировать виртуальную машину на месте (использовать существующий уникальный идентификатор)).** Если вы регистрируете виртуальную машину, то Hyper-V переведет ее в онлайновый режим и предположит, что вас устраивает сохраненное местоположение файлов виртуальной машины. Это не всегда оказывается идеальным вариантом, т.к., скорее всего, файлы будут находиться в папке вроде `ImportedVMs` и, возможно, вы захотите хранить все свои виртуальные машины вместе в библиотеке или на определенном томе. Прежде чем выбирать этот переключатель, удостоверьтесь в том, что файлы виртуальной машины хранятся именно там, где нужно и удобно вам.
   - **Restore the virtual machine (use the existing unique ID) (Восстановить виртуальную машину (использовать существующий уникальный идентификатор)).** В случае выбора этого переключателя понадобится выбрать место для хранения файлов виртуальной машины (рис. 28.7).
   - **Copy the virtual machine (create a new unique ID) (Копировать виртуальную машину (создать новый уникальный идентификатор)).** Выбор этого переключателя позволяет многократно импортировать виртуальную машину из какого-то шаблона, причем для каждой скопированной виртуальной машины будет создан новый уникальный идентификатор.

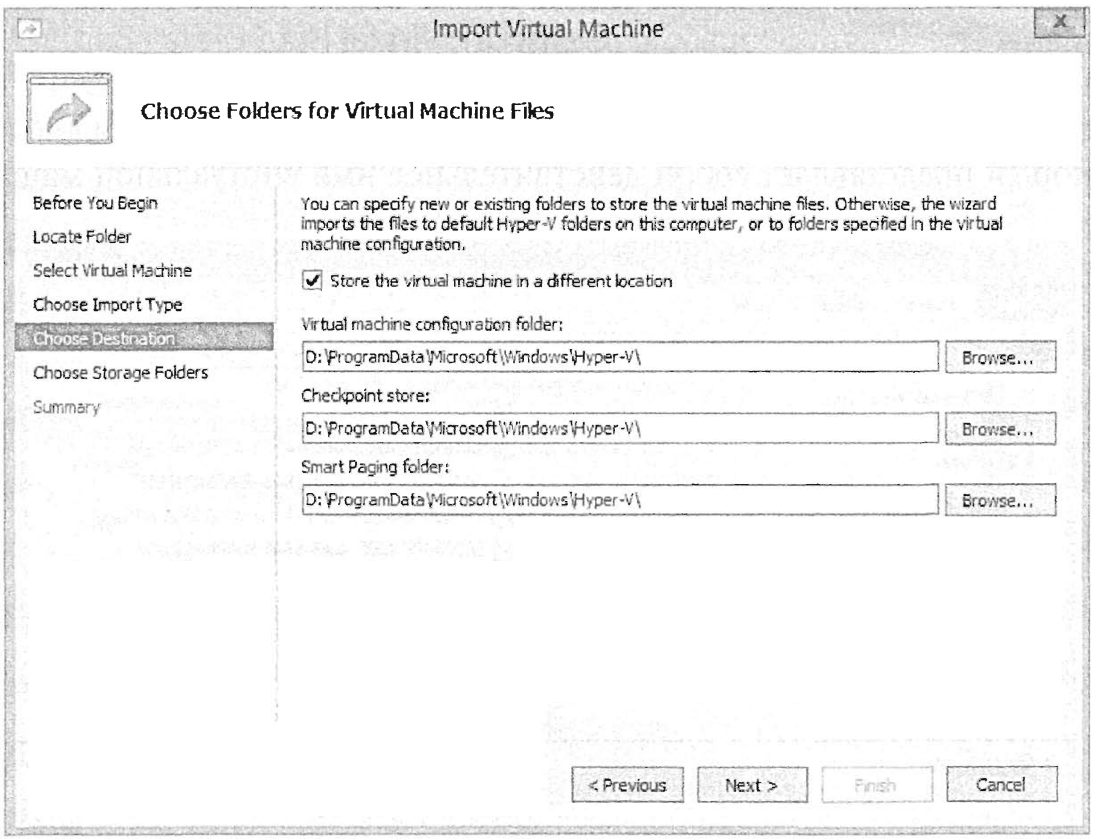


Рис. 28.7. Выбор типа импортирования Restore the virtual machine позволяет выбирать местоположения для файлов виртуальной машины

6. Выберите подходящий вариант и для продолжения щелкните на кнопке Next.
7. На экране Summary (Сводка) щелкните на кнопке Finish (Готово), чтобы начать процесс импорта.

   Процесс импорта займет всего несколько секунд и завершится обновлением состояния. Если возникла какая-то проблема, вы должны просмотреть журнал событий. Распространенной проблемой является невозможность найти совпадающий виртуальный коммутатор, в результате чего сетевые интерфейсные платы останутся неподключенными.
8. Выберите только что импортированную виртуальную машину. Вы обнаружите, что все существующие контрольные точки также были импортированы.
9. Проверьте свойства виртуальной машины и обратите внимание на пути к виртуальным дискам.
10. Проверьте состояние подключения сетевых интерфейсных плат.
11. Щелкните на элементе Start (Пуск) в панели Actions, чтобы перевести виртуальную машину в онлайновый режим.

    Имейте в виду, что вы на самом деле клонировали старую виртуальную машину. Если она по-прежнему функционирует на другом хосте, а вы перевели только что импортированную виртуальную машину в онлайновый режим, то в сети окажутся две идентичных машины, что определенно вызовет проблемы!

Возможно, вам интересно знать, каким образом Hyper-V отслеживает конфигурацию виртуальных машин. С действительной конфигурацией виртуальной машины все довольно просто. Когда вы создаете виртуальную машину, то сообщаете ей, куда поместить папку верхнего уровня, содержащую конфигурацию. На рис. 28.8 показана конфигурация виртуальной машины на хосте Hyper-V по имени `VMHOST1-SRV`.

Здесь видны три папки: Snapshots (Снимки), Virtual Hard Disks (Виртуальные жесткие диски) и Virtual Machines (Виртуальные машины). Зарегистрированы две виртуальные машины. С каждой из них связана одна папка с именем ее идентификатора GUID, который представляет собой действительное имя виртуальной машины.

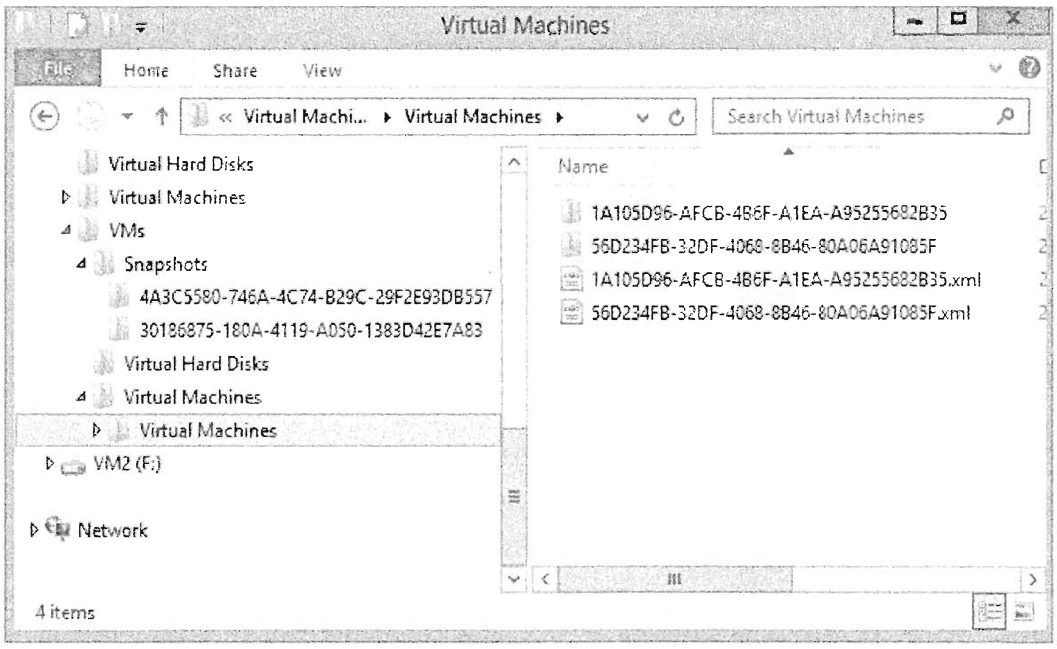


Рис. 28.8. Файлы конфигурации виртуальной машины

Например, имя папки 1A105D96-AFCB... соответствует виртуальной машине `WS2012R2-SRV1`. Эта папка содержит текущее состояние памяти, если вы сохранили ее состояние. У каждой виртуальной машины имеется XML-документ, также названный согласно идентификатору GUID виртуальной машины. Данный документ является полностью читабельным, хотя, вероятно, вы не должны редактировать его вручную. Если вы просмотрите его, то найдете полную конфигурацию виртуальной машины. К примеру, этот XML-файл содержит все виртуальные коммутаторы, к которым подключена виртуальная машина, перечисленные в виде своих идентификаторов GUID, а не описательных имен.

Папка Snapshot (ее имя отражает старый термин, который использовался для обозначения контрольной точки) содержит подпапки GUID с информацией о состоянии каждой контрольной точки: текущая конфигурация процессов и виртуального оборудования в файле `.vsv` и вся виртуальная память в файле `.bin`. Разностные файлы контрольных точек хранятся в виде файлов `.avhdx` внутри папки Virtual Hard Disks.

При создании виртуальной машины или виртуального диска их можно поместить по существу в любое желаемое место. Откуда Hyper-V известно, где искать все необходимое? Для этого Hyper-V использует *символические ссылки*, представляющие собой очень маленькие файлы, которые ссылаются на другие файлы способом, прозрачным для приложений. В данном случае все важные символические ссылки находятся в центральном месте хранения конфигурации для Hyper-V: `%systemdrive%\ProgramData\Microsoft\Windows\Hyper-V`. Папка `ProgramData` является скрытой: ее можно увидеть, указав в проводнике Windows на необходимость отображения скрытых и системных файлов. Начиная с версии Windows Server 2008 R2, в проводнике Windows вы можете видеть символические ссылки подобного рода.

На рис. 28.9 в описании внутри столбца Type (Тип) можно заметить, что это именно символические ссылки (SymLink), а не обычные файлы. Кроме того, это подтверждает размер файла, равный 0 байтов. В предшествующих версиях Windows Server вам пришлось бы прибегнуть к командной строке, чтобы увидеть разницу между символическими ссылками и обычными файлами.

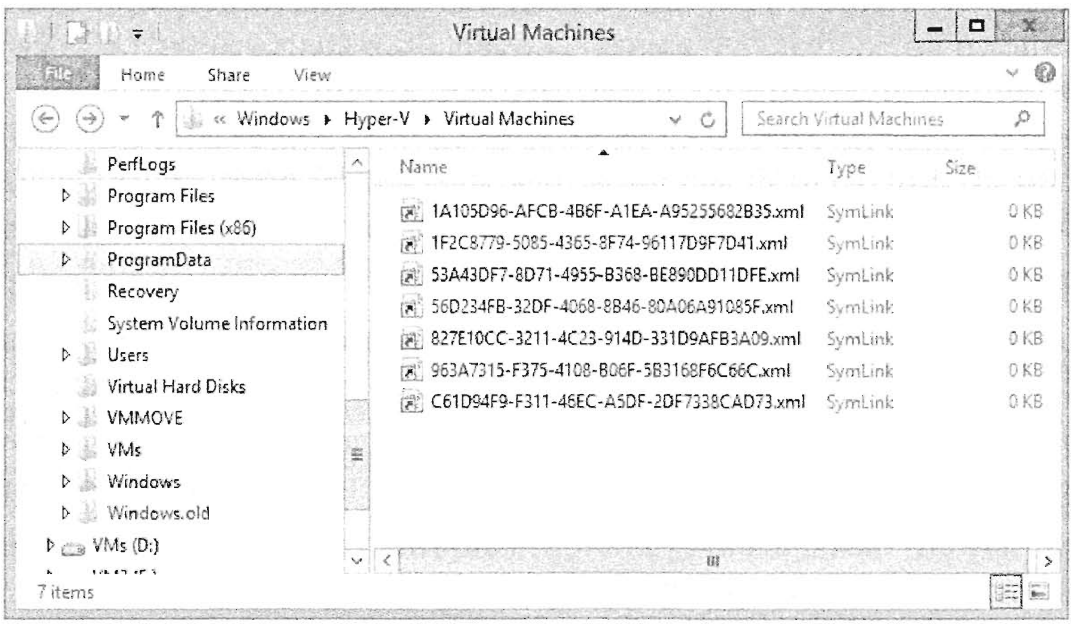


Рис. 28.9. Отправная точка для файлов конфигурации Hyper-V. Все файлы здесь являются символическими ссылками, указывающими на физические местоположения XML-файлов, которые определяют виртуальные машины

Знание того, как действует этот механизм ссылок, может оказаться весьма полезным во время исправления конфигурации Hyper-V после аварийной ситуации. Не забывайте об этом!

Быстрая миграция и живая миграция

Полноценное обсуждение виртуализации сервера невозможно себе представить без упоминания о быстрой миграции и живой миграции. Это связанные, но разные технологии перемещения виртуальных машин между хостами. В предыдущих версиях Hyper-V вам приходилось применять общее хранилище с совместно используемыми высокоскоростными сетями, но в Hyper-V версии Windows Server 2012 R2 появилась возможность иметь дело с хранилищем и сетями, не находящимися в общем пользовании. В этом разделе мы представим введение в технологии быстрой миграции и традиционной живой миграции, а позже обсудим новую функциональность Shared Nothing Live Migration (Живая миграция без совместного использования ресурсов).

- **Быстрая миграция.** Быстрая миграция работает путем сохранения состояния виртуальной машины, передачи управления другому узлу и ее перезапуска на этом узле. Этот процесс является предсказуемым и надежным, но не настолько быстрым, чтобы протекать незаметно для пользователя. При сохранении и восстановлении состояния виртуальной машины происходят потери времени, которые в случае виртуальных машин с большим объемом памяти могут исчисляться минутами.

- **Живая миграция.** Еще одна технология — это живая миграция, которая так называется из-за ее скорости, достаточно высокой для того, чтобы перемещать виртуальную машину в другой узел без потери обслуживания. В главе 27 мы обсуждали ряд усовершенствований живой миграции в текущем выпуске Windows Server, включая неограниченное количество одновременных живых миграций, готовую возможность сжатия, SMB Multichannel и SMB Direct. Ее ключевая особенность состоит в том, что период недоступности виртуальной машины во время фактического перемещения является очень коротким и может измеряться долями секунды. Это достаточно короткое время для поддержания непрерывности сеансов TCP/IP. Другими словами, пользователь перемещаемой виртуальной машины, как максимум, заметит микроскопическую задержку, но все компоненты продолжат работать обычным образом.

  Живая миграция схематически функционирует так, как описано ниже.

  1. Процесс миграции начинается. Конфигурация виртуальной машины перемещается на целевой хост, где строится скелетная виртуальная машина.
  2. Хранилище памяти виртуальной машины блокируется и начинается другой файл. В этот файл записываются все изменения, вносимые в память.
  3. Хранилище памяти виртуальной машины переносится в целевой узел по совместно используемой сети.

     Понятно, что эта сеть должна быть настолько быстрой, насколько возможно. Целевой узел начинает загрузку этой памяти в скелетную виртуальную машину.

4. Первый разностный файл блокируется, а второй начинается. Первый разностный файл передается в целевой узел. Этот процесс повторяется до тех пор, пока размеры разностных файлов не станут небольшими.
5. До этого момента виртуальная машина продолжала функционировать, однако в данной точке она замораживается и перемещается последний разностный файл.
6. Управление файлами VHDX виртуальной машины передается целевому узлу. Это происходит очень быстро.
7. Конфигурация виртуальной машины удаляется из исходного узла и регистрируется в целевом узле.
8. Виртуальная машина начинает работать в целевом узле.

По очевидным причинам из двух указанных технологий чаще всего применяется живая миграция. Возможность такого быстрого перемещения виртуальных машин между хостами открывает простор для ряда интересных сценариев.

- **Очистка виртуальных машин по завершении работы.** Если у вас функционирует кластер Hyper-V, то эта возможность может оказаться весьма полезной. Каждый раз, когда на хосте необходимо выполнить какую-то работу, которая предполагает его простой, вы можете переместить все виртуальные машины на другой хост, избежав перерыва в обслуживании. Для этого используется новая возможность очистки виртуальных машин по завершении работы (Virtual Machine Drain on Shutdown), реализованная в Hyper-V версии Windows Server 2012 R2. Это исключительно удобно при обслуживании оборудования, скажем, при добавлении модулей памяти, применении исправлений и т.д. По существу, когда вы завершаете работу хоста Hyper-V, который является частью кластера с обходом отказа (даже не переводя его в режим обслуживания), все виртуальные машины, размещенные на этом узле, автоматически подвергаются живой миграции на другой хост.
- **Выделение ресурсов по запросу.** У вас могут быть виртуальные машины, которые функционируют в нагруженном режиме и используют значительные ресурсы ЦП или дискового ввода-вывода. С помощью живой миграции вы можете быстро переместить эти виртуальные машины на менее загруженный хост или в качестве альтернативы уступить дорогу другим виртуальным машинам. Если вы развернули средство System Center 2012, то можете сконфигурировать его на автоматическое перемещение таких виртуальных машин в период их высокой загрузки.
- **Включение энергосберегающих информационных технологий.** Благодаря живой миграции, у вас есть возможность останавливать работу хостов с низким коэффициентом использования, хотя в реальности вам понадобились бы дополнительные инструменты, такие как System Center 2012. Идея заключается в том, чтобы переместить виртуальные машины со слабо загруженных хостов на хосты с высокой утилизацией, например, со средним коэффициентом использования времени ЦП, который составляет не менее 60% или равен любой другой желаемой величине. Затем можно завершить функционирование хостов, не имеющих виртуальных машин, до тех пор, пока они снова не понадобятся, что в итоге означает экономию электроэнергии.

Все основные поставщики средств виртуализации серверов предлагают похожие возможности, которые могут иметь другие названия. Однако общее хранилище подразумевает сети SAN, контроллеры iSCSI и другие технологии хранения, которые мы не будем обсуждать здесь подробно. Тем не менее, мы раскроем базовые принципы и дадим краткий обзор, предполагая, что вы способны самостоятельно настроить базовую инфраструктуру хранения. На тот случай, если ранее вам не приходилось работать с удаленным хранилищем, мы предложим несколько рекомендаций, которые помогут ориентироваться в дальнейшем.

Живая миграция полагается на роль Failover Clustering (Кластеризация с обходом отказа) в Windows Server 2012 R2. *Кластеризация с обходом отказа* — это возможность перемещения между хостами функционирующих приложений, включая все их данные и текущее состояние. Такое перемещение (также известное как *событие обхода отказа*) может инициироваться пользователем, но обычно указывается несколько условий, которые будут запускать обход отказа. Хорошими примерами таких условий могут служить зависимости приложения: диски, сети, определенные службы, которые должны действовать, и т.п. Если какой-то зависимости не хватает, то кластеризация с обходом отказа инициирует этот обход. Приложение должно знать, что оно функционирует на кластере, и предпринимать соответствующее действие, когда поступает на него запрос. Широко известными примерами решений кластеризации с обходом отказа, помимо Hyper-V, могут служить SQL Server, Exchange Server, File and Print Services и т.д. Вы можете видеть, где в игру вступает общее хранилище: диск данных для приложения, выполняющегося на одном узле, должен переместиться на другой узел, если это приложение обходит отказ.

В традиционном сценарии живой миграции понадобилось бы иметь, по меньшей мере, два хоста Hyper-V, которые используют общее хранилище и сетевую конфигурацию, подобную показанной на рис. 28.10.

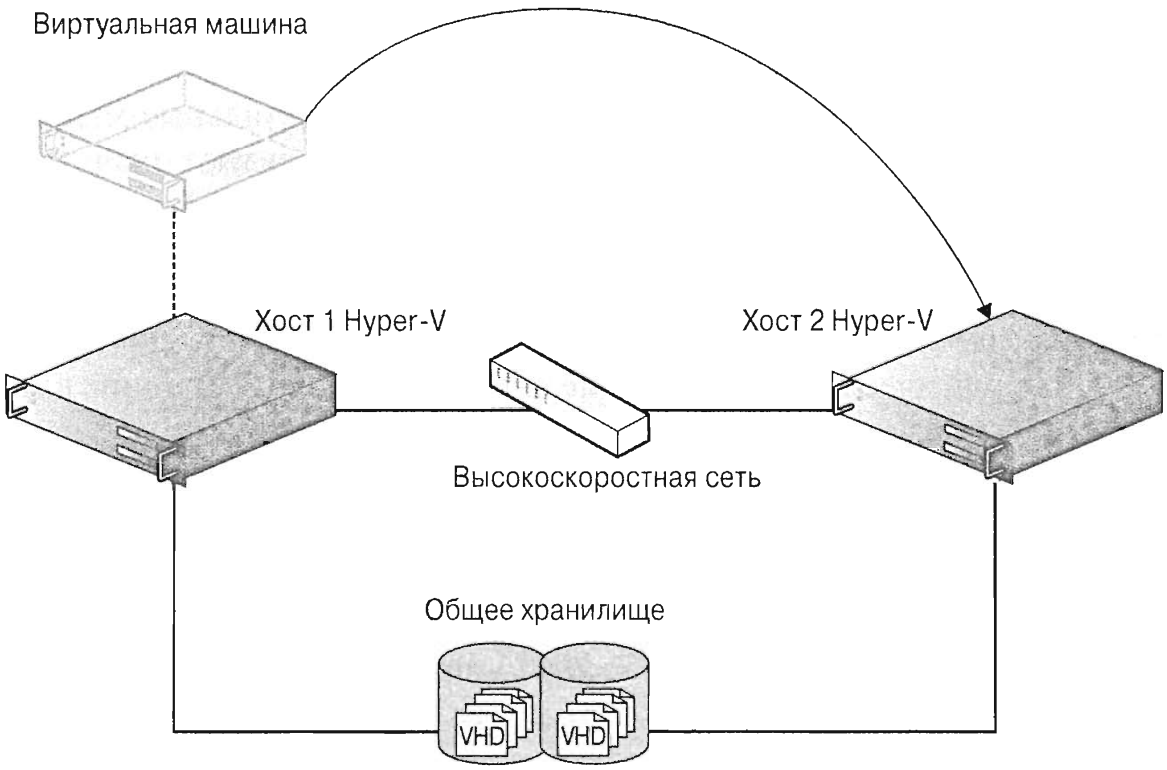


Рис. 28.10. Перемещение виртуальных машин между хостами посредством живой миграции требует наличия высокоскоростной сети и общего хранилища

Каждый сервер хоста, принимающий участие в кластерной конфигурации, является узлом. В Windows Server 2012 R2 максимальное количество узлов было доведено до 64, что является значительным увеличением по сравнению с ограничением в 16 узлов, присущим версии Windows Server 2008 R2. Основная цель кластеризации с обходом отказа заключается в обеспечении высокой готовности: если один хост останавливается, либо запланировано, либо неожиданно, службы кластеризации гарантируют, что приложение перезапустится на другом узле.

Выбор между живой и быстрой миграцией

Зачем вообще может понадобиться быстрая миграция, если в вашем распоряжении есть живая миграция? Одна из причин связана с тем, что живая миграция иногда терпит неудачу. Если внимательно взглянуть на способ ее работы, удастся заметить теоретически слабое место: живая миграция должна переместить память на целевой хост быстрее, чем виртуальная машина успеет внести в нее изменения. При наличии приложения, которое очень быстро записывает в память большой объем данных и продолжает делать это, живая миграция может оказаться невозможной. Очевидно, чтобы живая миграция была надежной, требуется высокоскоростная сеть. Но это также свидетельствует о преимуществе метода быстрой миграции: она является детерминированной, поскольку сохраняет и восстанавливает состояние виртуальной машины между миграциями. Таким образом, если для отдельной виртуальной машины живая миграция не срабатывает, попробуйте воспользоваться быстрой миграцией.

Бескластерные живые миграции

Как упоминалось ранее, в Windows Server 2012 имеется расширение, посредством которого можно выполнять миграцию функционирующих виртуальных машин между хостами безо всякого простоя и — что очень важно — без общих кластерных конфигураций! Такая возможность известна как *Shared Nothing Live Migration* (Живая миграция без совместного использования ресурсов). Все, что понадобится — это два хоста и кабель высокоскоростной сети, как показано на рис. 28.11.

Это стало доступным за счет использования процесса, очень похожего на обсуждавшуюся выше функциональность онлайнового экспортирования виртуальных машин, и еще одного нового средства Windows Server 2012 R2, которое называется *Live Storage Migration* (Живая миграция хранилища).

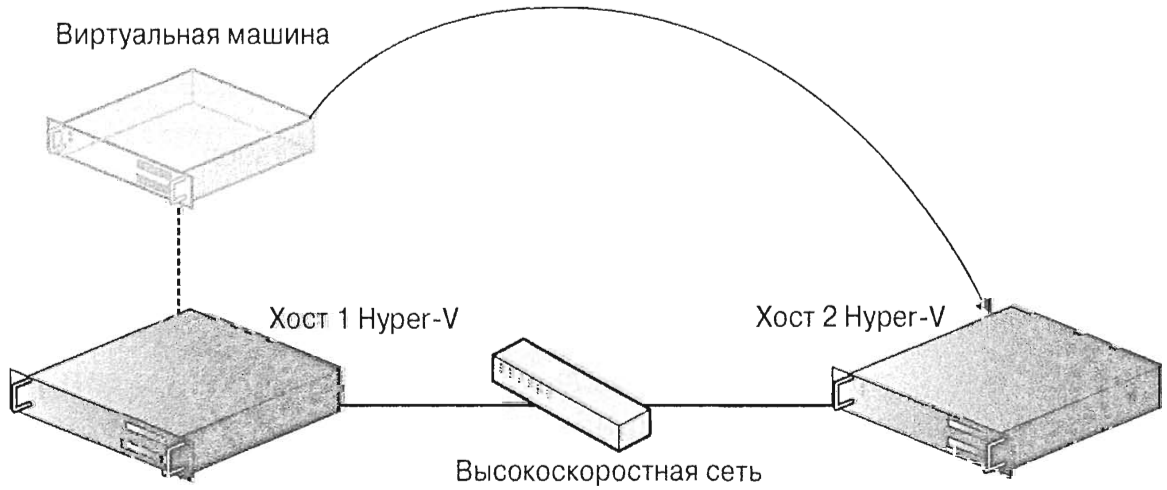


Рис. 28.11. Перемещение виртуальных машин с помощью Shared Nothing Live Migration

Благодаря Live Storage Migration, хранилище (виртуальные диски) виртуальной машины можно перемещать в другое местоположение, такое как новая структура папок на локальном хосте или хранилище, находящееся на удаленном хосте. Даже одна эта возможность является весьма долгожданным дополнением к Hyper-V, поскольку ее отсутствие остро ощущалось в предыдущих выпусках и означало необходимость планирования простоя виртуальной машины, когда требовалось провести миграцию ее хранилища.

После всех этих объяснений давайте рассмотрим саму процедуру. В приведенных ниже шагах предполагается наличие у вас доступа к двум хостам (один из них будет источником, а другой — получателем), которые работают под управлением ОС Windows Server 2012 R2 с установленной ролью Hyper-V. Эти два хоста должны быть частью одного и того же домена Active Directory.

1. Войдите в систему исходного сервера хоста Hyper-V от имени учетной записи с разрешениями администратора.
2. Откройте диспетчер Hyper-V, убедитесь, что в левой панели выбран исходный хост, и щелкните на элементе Hyper-V Settings (Настройки Hyper-V) в панели Actions (Действия).
3. Щелкните на узле Live Migrations (Живые миграции) и затем отметьте флажок Enable incoming and outgoing live migrations (Включить входящие и исходящие живые миграции), чтобы активизировать эту возможность (рис. 28.12).

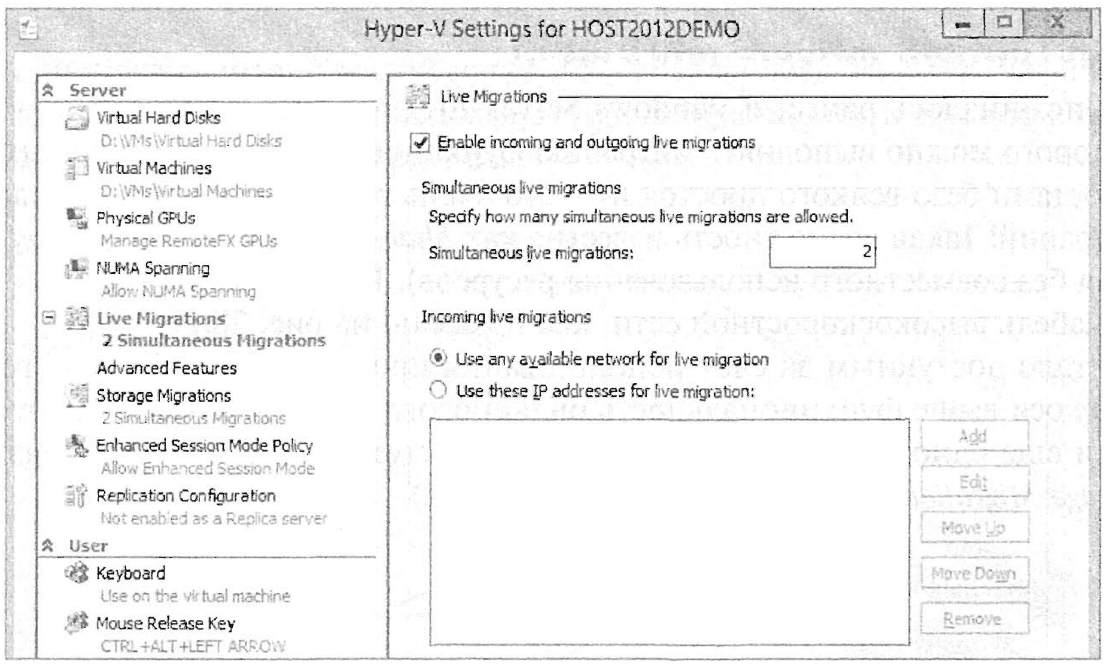


Рис. 28.12. Включение Shared Nothing Live Migration

4. В поле Simultaneous live migrations (Количество одновременных живых миграций) введите количество живых миграций, которые должны одновременно выполняться на данном сервере, или просто оставьте стандартное значение 2.
5. Если вы хотите использовать для живых миграций конкретную сеть, то выберите ее в области Incoming live migrations (Входящие живые миграции).
6. В разделе Server (Сервер) слева раскройте узел Live Migrations и щелкните на элементе Advanced Features (Расширенные возможности).

На рис. 28.13 видно, что в области Authentication protocol (Протокол аутентификации) выбран переключатель Use Credential Security Support Provider (CredSSP) (Использовать поставщик поддержки учетных данных безопасности (CredSSP)), а в разделе Performance options (Параметры производительности) — переключатель Compression (Сжатие). В нижней части окна вы могли также обратить внимание на предупреждающее сообщение, указывающее на необходимость выхода из системы и затем входа в нее снова, чтобы разрешить применение выбранного протокола аутентификации CredSSP. Сейчас подходящее время сделать это.

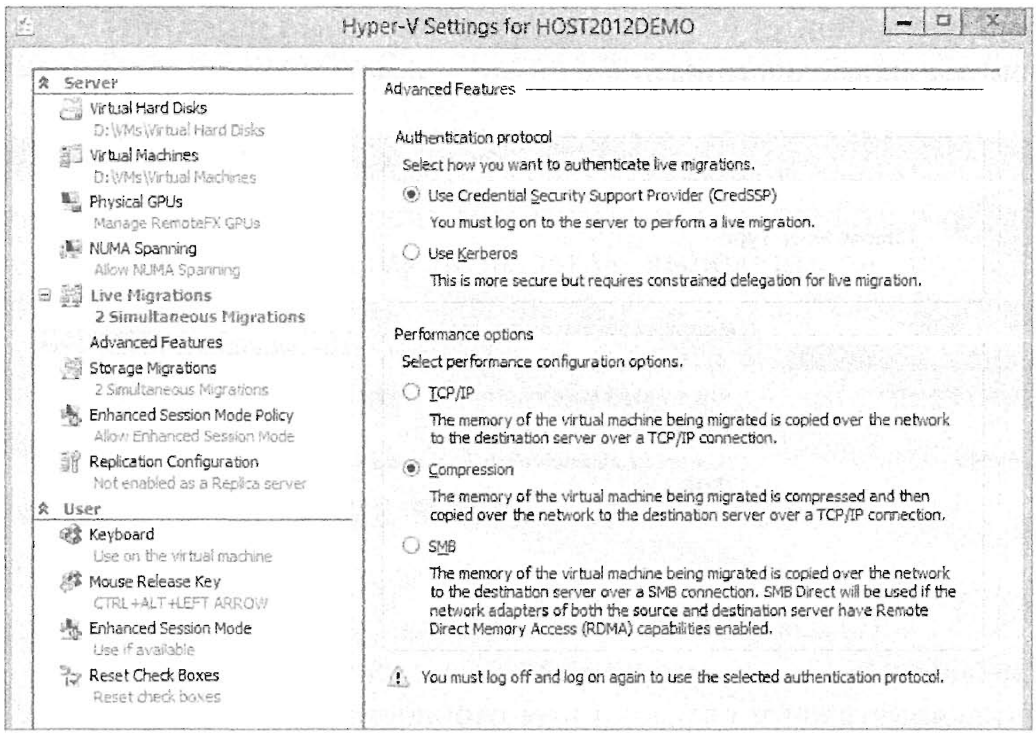


Рис. 28.13. Расширенные возможности для живых миграций

7. Повторите те же шаги на целевом хосте Hyper-V, и в конце процесса конфигурирования обязательно выйдите из системы и снова войдите в нее.

Если вы хотите некоторого разнообразия, то для выполнения того же самого процесса вместо графического пользовательского интерфейса можно применить следующие команды PowerShell:

```
Enable-VMMigration
Set-VMHost -UseAnyNetworkForMigration $true
```

Удаленный запуск Shared Nothing Live Migration

Если вы хотите запустить живую миграцию виртуальных машин между хостами, использующую Shared Nothing Live Migration, из удаленного сервера или рабочей станции (не с исходного или целевого хоста), то понадобится включить ограниченное делегирование Kerberos (Kerberos Constrained Delegation) в оснастке Active Directory Users and Computers, после чего на экране Live Migrations⇨Advanced Settings (Живые миграции⇨Дополнительные параметры) в окне Hyper-V Settings (Настройки Hyper-V) выбрать переключатель Use Kerberos (Использовать Kerberos). Более подробные сведения доступны по ссылке `http://technet.microsoft.com/en-us/library/jj134199.aspx#BKMK_Step1`.

Когда настройки живой миграции сконфигурированы на исходном и целевом хостах, можно приступить к тестированию и переместить виртуальную машину между этими двумя хостами.

1. Войдите в систему исходного сервера хоста Hyper-V от имени учетной записи с разрешениями администратора.
2. Щелкните правой кнопкой мыши на функционирующей виртуальной машине и выберите в контекстном меню пункт Move (Переместить).

   На экране Choose Move Type (Выбор типа перемещения), показанном на рис. 28.14, предлагаются переключатели Move the virtual machine (Перенести виртуальную машину) и Move the virtual machine's storage (Перенести хранилище виртуальной машины).

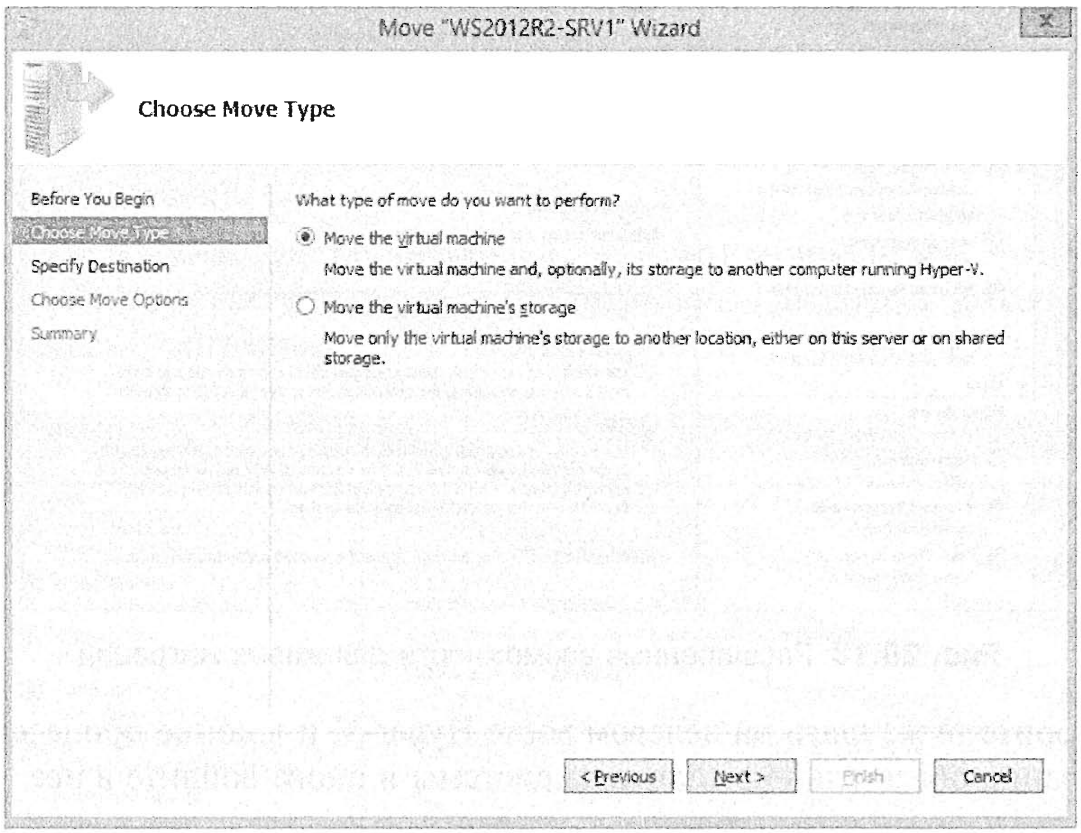


Рис. 28.14. Выбор типа перемещения

3. Оставьте выбранным переключатель Move the virtual machine и щелкните на кнопке Next (Далее).
4. Укажите имя целевого хоста и щелкните на кнопке Next.
5. На экране Choose Move Options (Выбор параметров перемещения) выберите место, где будут храниться данные виртуальной машины (или просто оставьте здесь стандартную настройку), и щелкните на кнопке Next.
6. Если на предыдущем шаге вы приняли стандартную настройку, то теперь понадобится указать на целевом сервере хоста место, куда будет помещена перенесенная виртуальная машина. Щелкните на кнопке Next.
7. На экране Summary (Сводка) просмотрите сконфигурированные настройки и щелкните на кнопке Finish (Готово), чтобы начать перенос Shared Nothing Live Migration виртуальной машины на целевой хост.

Перевод живой миграции на новый уровень

С применением SMB 3.0, RDMA и Multichannel в Windows Server 2012 R2 можно действительно улучшить показатель готовности и устранить ограничения на мобильность виртуальных машин в центре обработки данных — конечно, если вы располагаете соответствующим бюджетом. Дидье Ван Хой написал статью по этой теме, с которой можно ознакомиться по ссылке `http://workinghardinit.wordpress.com/2013/06/04/complete-vm-mobility-across-the-data-center-with-smb-3-0-rdma-multichannel-windows-server-2012-r2/`.

После этого не упустите возможность прочитать статью Айдана Финна, посвященную установке границ полосы пропускания SMB 3.0 в Windows Server 2012 R2: `http://www.aidanfinn.com/?p=15262`.

Обслуживание виртуальных машин

Хотя виртуализация привносит множество новых средств и значительную степень гибкости, вам по-прежнему необходимо выполнять ряд более традиционных задач обслуживания виртуальных машин, таких как резервное копирование, управление защитой от вредоносного программного обеспечения и своевременное применение обновлений. В этом разделе мы обсудим возможности, доступные для проведения таких работ.

Резервное копирование и восстановление виртуальных машин

С точки зрения управления системами виртуальные машины должны трактоваться, как если бы они были физическими машинами, но с несколькими исключениями. Когда дело доходит до резервного копирования и восстановления, нужно учитывать несколько особенностей. Глядя на хост Hyper-V, на котором функционирует множество виртуальных машин, вас наверняка интересует, можно ли выполнить резервное копирование всех этих машин за один раз. В идеальном мире мы могли бы поступать так, как описано ниже.

- Создавать резервные копии всех виртуальных машин, делая это пошагово.
- Информировать все виртуальные машины о наличии резервных копий, чтобы они знали, как действовать при восстановлении. Это особенно важно для Active Directory и Exchange Server.
- Восстанавливать виртуальные машины на индивидуальной основе.

Все это принципиально возможно. Тем не менее, реальность отличается. Мы кратко рассмотрим, как работает резервное копирование в современной версии Windows Server.

Начиная с версии Windows Server 2003, в нашем распоряжении была служба теневого копирования томов (Volume Shadow Copy Service — VSS). Для процесса резервного копирования этот компонент решает две задачи.

- **Замораживание дискового тома.** Во-первых, служба VSS может заморозить дисковый том, получить снимок и снова разморозить диск (это выполняется по такому же принципу, что и создание контрольной точки виртуальной машины на уровне хоста, как обсуждалось в главе 27). Снимок остается на томе.

Принцип его построения основан на алгоритме определения различий, поэтому снимок занимает мало места.

- **Взаимодействие с приложениями.** Во-вторых, во время резервного копирования служба VSS взаимодействует с приложениями, предоставляя им возможность провести очистку и подготовку, такую как сброс буферов, стабилизация структур данных и т.д. Это очень важно в случае сложных приложений. Служба VSS позволяет быстро создавать резервные копии приложений, не затрагивая структуры данных. К числу таких приложений относятся Active Directory, SQL Server, Exchange Server и, конечно же, Hyper-V.

Таким образом, чтобы заставить VSS работать в виртуальной среде, вам необходим поставщик VSS для Hyper-V и компонент в виртуальной машине, который интегрируется с этим поставщиком. Как по-другому приложения в виртуальной машине могли бы узнать о том, что выполняется резервное копирование? Это представляет собой двухэтапную процедуру: во время резервного копирования процессу VSS на хосте необходимо запустить процесс VSS в виртуальной машине, используя в качестве коммуникационного канала поставщика VSS для Hyper-V. В самой виртуальной машине о координации заботятся службы Integration Services. Этот момент важно подчеркнуть: без функционирующих служб Integration Services не может быть реального резервного копирования с хоста. Действительно, с помощью VSS можно создать резервные копии файлов `.vhdx`, образующих виртуальную машину, но эта виртуальная машина не будет осведомлена о резервных копиях. Это было бы ничуть не лучше создания резервной копии живого образа со всеми его ограничениями и отсутствием функциональности на уровне приложений.

Давайте подведем краткие итоги сказанному выше. У вас есть два варианта создания резервных копий операционной системы и приложений в виртуальной машине.

- Запустить резервное копирование с хоста, применив для этого какой-то инструмент резервного копирования, осведомленный о службе VSS, например, Windows Server Backup (Резервное копирование сервера Windows) или System Center 2012 — Data Protection Manager (Диспетчер защиты данных системного центра). Внутри виртуальной машины обязательно должны функционировать службы Integration Services.
- Трактовать виртуальную машину как физическую и запустить программу резервного копирования из виртуализированной ОС.

Оба варианта обладают своими достоинствами.

- **Резервное копирование из хоста.** При выполнении резервного копирования виртуальной машины на уровне хоста вы гарантированно получаете полную резервную копию всей виртуальной машины, которая позволит ее восстановить, когда возникнет такая потребность. В случае отказа сервера вам не придется заниматься восстановлением с нуля и повторной установкой приложений. Этот вариант также хорошо вписывается в сценарий дистанционного восстановления в аварийных ситуациях, когда вся виртуальная машина реплицируется за пределами своего сайта. Однако недостаток резервного копирования на уровне хоста заключается в том, что в зависимости от размера виртуальной машины оно может занимать очень много времени, даже при наличии плана инкрементального резервного копирования. Вдобавок вам нужно

располагать диском большой емкости, т.к. создание резервных копий только на магнитных лентах сейчас считается устаревшим, и в любом случае оно было бы непрактичным при построении полных копий большого количества виртуальных машин. К тому же необходимо учитывать потенциальное снижение производительности хоста во время резервного копирования множества виртуальных машин, но этого легко избежать за счет надлежащего планирования и выбора проектного решения.

- **Резервное копирование в виртуализированной ОС.** Этот вариант удачно впишется в существующую систему резервного копирования, ничего не нарушая, к тому же вам хорошо известно, как это делать. Скорее всего, вам понадобится развернуть агент резервного копирования в гостевой операционной системе каждой виртуальной машины, и наряду с файлами, папками и приложениями выполнять резервное копирование состояния системы. В таком случае хост можно рассматривать как черный ящик, который может быть заменен по своему усмотрению. Однако если вы потеряете хост со всеми функционирующими на нем виртуальными машинами, и у вас останутся только резервные копии, созданные внутри машин, будьте готовы потратить немало времени на их восстановление в рамках другого хоста. Кроме того, вы должны понимать, что резервное копирование, запущенное изнутри виртуальной машины, генерирует большой объем операций дискового ввода-вывода. Если 10 виртуальных машин на одном хосте начнут одновременно создавать свои резервные копии, то нагрузка на этот хост возрастет десятикратно. Справиться с такой нагрузкой сумеет только очень хорошее оборудование!

Если вы хотите располагать полным спектром возможностей, доступных для резервного копирования Hyper-V, мы рекомендуем установить диспетчер защиты данных системного центра (System Center 2012 — Data Protection Manager (DPM)). Если по какой-либо причине это сделать не удается, то, как упоминалось ранее, можно воспользоваться встроенным инструментом для резервного копирования Hyper-V — Windows Server Backup (WSB). Данный инструмент более подробно обсуждается в главе 32, но чтобы вы получили общее представление о том, как с его помощью создаются резервные копии виртуальных машин, мы кратко рассмотрим здесь базовую процедуру. Первым делом потребуется установить WSB. Проще всего это сделать, открыв окно командной строки PowerShell от имени учетной записи администратора и введя в нем следующую команду:

```
Install-WindowsFeature Windows-Server-Backup
```

После установки WSB можно заняться резервным копированием виртуальной машины.

1. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите в меню Tools (Сервер) пункт Windows Server Backup (Резервное копирование сервера Windows), чтобы открыть оснастку консоли MMC.
2. В левой панели дерева щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) и выберите в контекстном меню пункт Backup Schedule (Расписание резервного копирования), чтобы открыть мастер расписания резервного копирования (Backup Schedule Wizard).
3. На экране Getting Started (Начало работы) щелкните на кнопке Next (Далее).

4. В качестве типа резервного копирования выберите Custom (Специальный) и щелкните на кнопке Next.
5. Щелкните на кнопке Add Items (Добавить элементы), чтобы открыть диалоговое окно Select Items (Выбор элементов).
6. Раскройте узел Hyper-V и отметьте флажок возле имени виртуальной машины, для которой необходимо создать резервную копию (рис. 28.15).

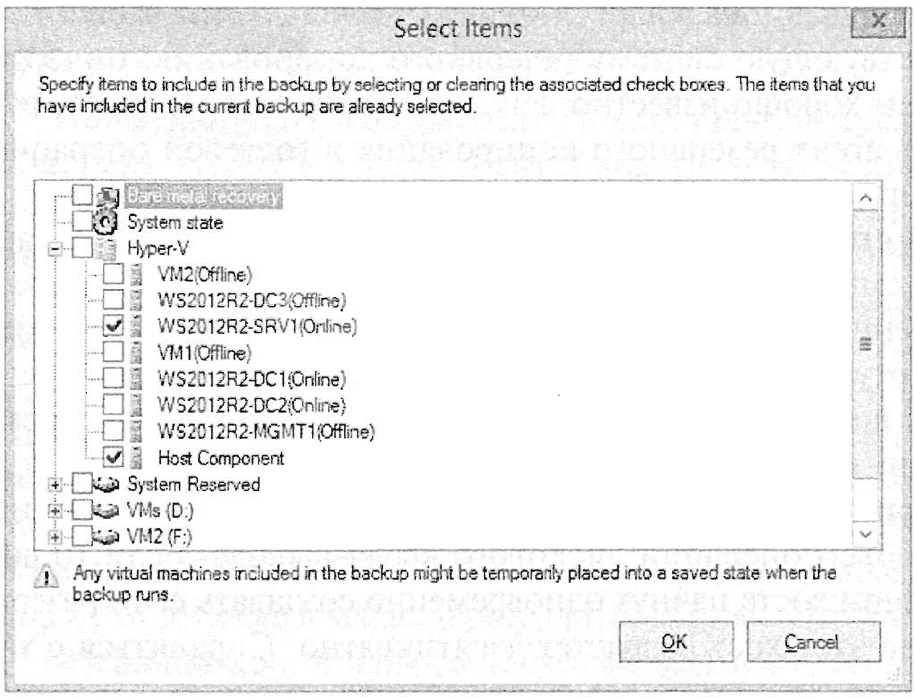


Рис. 28.15. Резервное копирование виртуальных машин с помощью WSB

Обратите внимание, что отмечен также и флажок Host Component (Компонент хоста), поскольку это защищает виртуальные коммутаторы, пулы ресурсов и диспетчер авторизации Windows (Windows Authorization Manager) на хосте. Щелкните на кнопке OK.

7. На экране Select Items for Backup (Выбор элементов для резервного копирования) щелкните на кнопке Advanced Settings (Дополнительные настройки) и в открывшемся диалоговом окне перейдите на вкладку VSS Settings (Настройки VSS).
8. Выберите переключатель VSS full backup (Полное резервное копирование VSS), если вы не используете другой продукт для резервного копирования, чтобы защитить свои виртуальные машины, или переключатель VSS copy backup (Резервное копирование копии VSS), если вы располагаете другим решением резервного копирования и хотите сохранить файлы журнала приложений.
9. Щелкните на кнопке OK, чтобы закрыть это диалоговое окно; затем щелкните на кнопке Next, чтобы продолжить работу мастера.
10. Укажите время для запуска резервного копирования.

    В вашем распоряжении есть следующие переключатели:

    - Once a day (Раз в сутки) — в этом случае выбирается время суток для запуска резервного копирования;
    - More than once a day (Более одного раза в сутки) — в этом случае выбирается доступное время.

11. Щелкните на кнопке Add (Добавить), чтобы добавить выбранное время в список Scheduled time (Запланированное время).

    Переключатель More than once a day позволяет запланировать столько сеансов резервного копирования, сколько нужно, при условии, что вы оставите интервал времени между сеансами, достаточный для того, чтобы текущий сеанс резервного копирования успел завершиться до запуска следующего сеанса.

12. Щелкните на кнопке Next.
13. Выберите переключатель Back up to a hard disk that is dedicated for backups (recommended) (Создать резервную копию на жестком диске, который выделен для резервных копий (рекомендуется)).

    Чтобы можно было применять этот вариант, к серверному компьютеру должен быть присоединен, по меньшей мере, один диск, не имеющий томов. Это должен быть неформатированный диск без разделов или файловой системы.

14. Щелкните на кнопке Next.
15. Выберите диск, который будет использоваться для тома резервных копий, и щелкните на кнопке Next.

    Откроется диалоговое окно с предупреждением о том, что по завершении работы мастера выбранный диск будет сформатирован, а любые существующие на нем данные утеряны.

16. Если вы уверены, что указали подходящий диск, щелкните на кнопке Yes (Да), чтобы продолжить.
17. Просмотрите выбранные настройки и щелкните на кнопке Finish (Готово), чтобы сформатировать диск для резервных копий и запланировать процесс резервного копирования.

Возможно, вам приходилось использовать результат выполнения экспорта в качестве резервной копии. Тем не менее, экспортированная виртуальная машина не эквивалентна нормальной резервной копии из-за отсутствия интеграции с VSS. Когда вы импортируете виртуальную машину, ей не известно, что она была "восстановлена". Недостатком работы с экспортированными копиями является то, что их импортирование обычно выполняется поодиночке и может требовать предварительного удаления текущей виртуальной машины (если она по-прежнему существует). Если вы хорошо понимаете, что делаете, то при крайней необходимости средство экспорта/импорта применять допускается. В противном случае, поскольку оно не является решением для резервного копирования, масштабное его использование не рекомендуется.

Защита от вредоносного программного обеспечения и применение исправлений

Само собой разумеется, что наличие на серверах какого-то типа защиты от вредоносного программного обеспечения является весьма разумным решением. Вопрос больше касается того, до каких пределов должна распространяться такая защита. Вам необходимо непрерывное сканирование или устроит ежедневное либо еженедельное сканирование? До тех пор, пока вы в состоянии противостоять новым угрозам, скорее всего, все будет в порядке.

Виртуализация может привнести дополнительную сложность. Во внимание должен приниматься не только хост, но и дисковый ввод-вывод, который представляет собой ценный ресурс на любой платформе виртуализации. Если на хосте размещено 10 виртуальных машин, и все они выполняют непрерывное сканирование на предмет вредоносного ПО, то система ввода-вывода хоста подвергается в 10 раз большей нагрузке, чем та, с которой имел бы дело одиночный сервер. На практике это нечасто является ограничивающим фактором. Современным инструментам, предназначенным для борьбы с вредоносным программным обеспечением (естественно, серверного класса), известно, каким образом бережно обращаться с полосой пропускания ввода-вывода. Поэтому для виртуальных машин рекомендация очевидна: устанавливайте инструменты сканирования вредоносного ПО на всех виртуальных машинах. Рассматривайте виртуальную машину как физический сервер и позаботьтесь о внедрении документированных антивирусных программ, соответствующих рабочей нагрузке.

А что можно сказать о хосте Hyper-V? Если на нем не функционируют никакие другие службы, кроме Hyper-V, то есть ли потребность в сканировании на предмет вредоносного ПО? Если говорить о Server Core, то для вредоносного ПО там не особо много целей. Однако это не значит, что защищать вообще нечего. Любая операционная система, подключенная к сети, потенциально уязвима к атакам. Даже небольшой изъян в стеке TCP/IP может привести к компрометации всей системы. Таким образом, если вам необходима полноценная защита, то придется сканировать и хост. Имейте в виду, что преобладающая доля дисковых операций выполняется виртуальными машинами, и вы увидите, что влияние на производительность хоста со стороны инструмента для сканирования вредоносного ПО будет низкой. Разумеется, вам понадобится исключить из процесса сканирования виртуальные диски и процессы Hyper-V. Точнее говоря, нужно исключить стандартную папку конфигурации виртуальных машин (`VM Configuration`), папку VHD, папку снимков (`Snapshot`), файлы `VMMS.exe` и `VMWP.exe`. Если не исключить их из процесса сканирования вредоносного ПО с онлайновым доступом, вы можете обнаружить, что некоторые виртуальные машины не запустятся или даже не будут видны в диспетчере Hyper-V.

В то время как сканирование на предмет вредоносного программного обеспечения является прямой формой защиты, своевременное применение обновлений и исправлений представляет собой косвенную, но от этого не менее важную, форму защиты. Не стоит и говорить, что вы должны применять исправления к виртуальным машинам и хосту — иначе вы неминуемо создадите себе проблему. Применение исправлений к хосту может предусматривать перезагрузку с переводом всех виртуальных машин в автономный режим. Это требует планирования и может вызвать проблемы, если у вас нет возможности надежно завершить работу виртуальных машин. Именно поэтому службы Integration Services настолько важны. Одной из их функций является запуск внутри виртуальной машины процедуры сохранения состояния, когда это запрашивает хост. На каждой виртуальной машине сконфигурировано стандартное действие, которое заключается в сохранении ее состояния, когда автономный хост прекращает работу. Помочь в решении проблемы может наличие нескольких хостов, т.к. это позволит использовать средство Shared Nothing Live Migration и сохранять виртуальные машины в онлайновом режиме.

Если у вас имеется среда кластера Hyper-V с обходом отказа, функционирующая под управлением Windows Server 2012 или последующей версии, вы можете задействовать средство обновления, осведомленное о кластерах (Cluster-Aware Updating — CAU), которое позволит применять исправления к серверам с минимальным временем простоя в процессе развертывания обновлений. Средство CAU интегрируется со встроенным агентом обновления Windows (Windows Update Agent) и службами обновления сервера Windows (Windows Server Update Services — WSUS) для загрузки и установки обновлений. Когда необходимо применить исправления к кластерному узлу Hyper-V с работающим Windows Server 2012 R2, понадобится всего лишь остановить хост, после чего активизируется новая функция Virtual Machine Drain on Shutdown (упомянутая ранее в этой главе), которая выполнит миграцию всех виртуальных машин на любой другой доступный хост. Если вы имеете дело с Windows Server 2012 (т.е. не Windows Server 2012 R2), то для получения того же самого результата сначала необходимо приостановить хост с помощью диспетчера кластера с обходом отказа (Failover Cluster Manager), а затем выбрать опцию Drain Roles (Очистить роли). Дополнительные сведения о средстве CAU можно получить в документе TechNet по ссылке `http://tinyurl.com/ws2012cua`.

Восстановление в аварийных ситуациях

Объем информации и новостей со всего мира, которые обрушиваются в наши дни на среднестатистического пользователя Интернета, потрясает воображение. Практически ежедневно то из одного, то из другого уголка мира приходят сообщения о катаклизмах (природных или техногенных), случившихся в какой-то стране, городе, деревне или предприятии. Примером такой катастрофы может служить удар цунами, обрушившийся в апреле 2011 года на западное побережье Японии и повлекший за собой разрушительные последствия на значительной территории. Буквально весь мир горячо откликнулся на эту трагедию, были проведены многочисленные кампании по сбору пожертвований, а многие страны отправили в Японию значительную гуманитарную помощь. Глобальные поставщики IT-услуг также не остались безучастными к этой трагедии населения Японии, открыв для них бесплатный доступ к своим центрам хранения и обработки данных и облачным службам. Когда японцы приступили к ликвидации последствий стихийного бедствия и восстановлению жилищного фонда и экономики, они использовали облачную платформу как один из эффективных способов быстрого налаживания нормального функционирования страны. После того как организации заново отстроили свои офисы и восстановили местную инфраструктуру, многие из них решили сохранить свое присутствие в облаке, вместо того чтобы возвращать все обратно в офисы, полагая, что это смягчит последствия возможных стихийных бедствий в будущем.

Виртуализация является ключевой опорой облачных вычислений, и с развитием таких технологий, как Hyper-V, восстановление в аварийных ситуациях (disaster recovery — DR) значительно упростилось и удешевилось по сравнению с прошлыми временами.

Самое время упомянуть, что концепции DR и высокой готовности (high availability — HA) не являются тождественными. Они разделяют некоторые характеристики, но служат разным целям. Высокая готовность сфокусирована на постоянной доступности вашей среды, что в терминах Hyper-V означает доступность

виртуальных машин. Вы обеспечиваете высокую готовность для виртуальных машин посредством кластеризации с обходом отказа (Hyper-V Failover Clustering) и предоставляете избыточность для хостов, развертывая в кластере достаточное количество физических серверов, чтобы избежать простоев в случае выхода из строя хоста. С другой стороны, назначение DR заключается в гарантировании того, что организация может поддерживать функционирование своих IT-систем (и в конечном итоге своего бизнеса) посредством дистанционной репликации и отказоустойчивых сайтов DR. Восстановление в аварийных ситуациях можно представлять себе как некий "план Б", который вступает в действие после удара стихии.

В этом разделе мы рассмотрим новую возможность DR в Windows Server 2012, которая называется Hyper-V Replica (Реплика Hyper-V).

Недорогое решение по восстановлению в аварийных ситуациях с помощью Hyper-V Replica

Средство Hyper-V Replica (HVR) — это новая возможность, появившаяся в Windows Server 2012, которая позволяет выполнять репликацию виртуальных машин, основанную на хостах, без необходимости в наличии каких-то общих кластерных компонентов. По существу вы можете взять виртуальную машину, работающую внутри хоста Hyper-V на одном сайте, и просто реплицировать ее на другой сайт с возможностью использования до двух дополнительных сайтов. В Microsoft разработали HVR для работы с коммерческими широкополосными подключениями, поэтому наличие дорогостоящих высокоскоростных волоконно-оптических каналов на сайте DR не является жизненно необходимым для того, чтобы происходила репликация. На рис. 28.16 представлен базовый сценарий HVR.

Для обеспечения безопасности HVR использует либо Active Directory, либо аутентификацию на основе сертификатов между хостами. Вы можете выбрать, какие виртуальные диски в виртуальной машине должны реплицироваться, а какие — нет (например, виртуальный диск, содержащий большой файл подкачки).

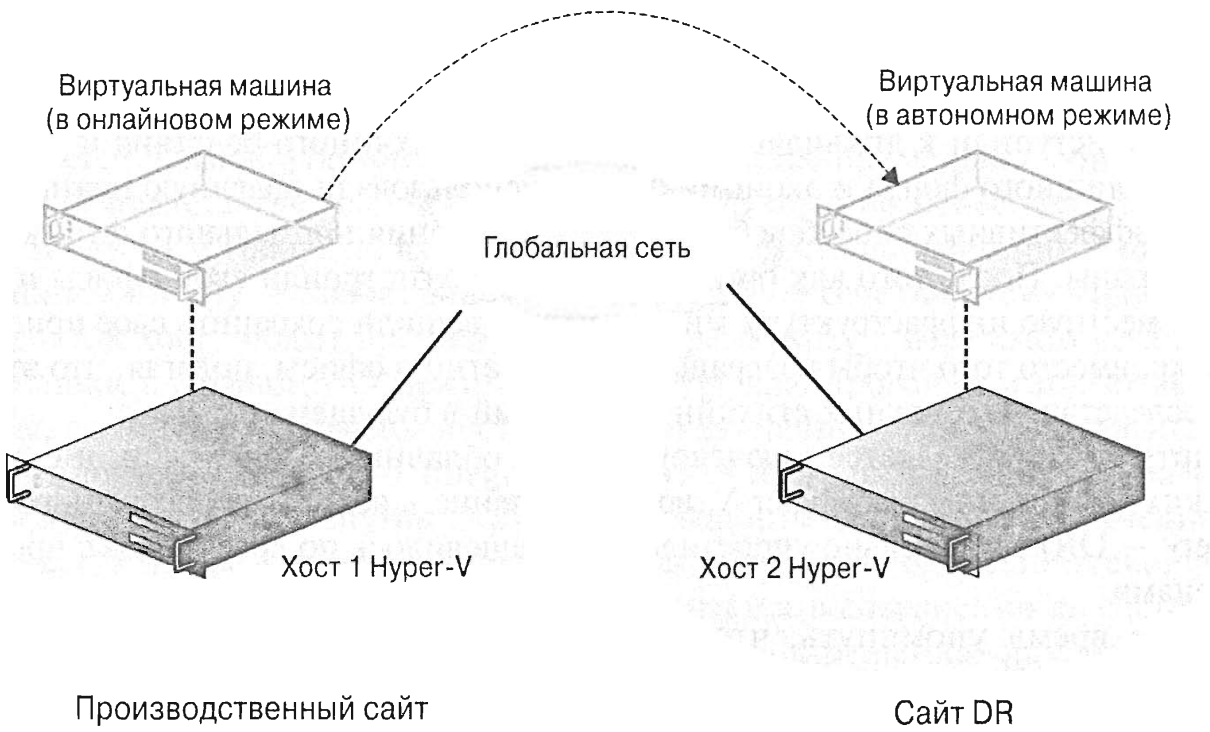


Рис. 28.16. Базовый сценарий Hyper-V Replica

Когда вы впервые конфигурируете репликацию, между исходным и целевым хостами выполняется "начальная" синхронизация, по завершении которой в действие вступает асинхронная репликация. Реплицированная виртуальная машина на целевом хосте будет выключена, и при необходимости вы должны вручную запустить плановый или внеплановый обход отказа, чтобы включить ее. Со средством HVR связана одна интересная особенность. Если вам необходимо было реализовать план DR и вы передали управление всеми реплицированными виртуальными машинами сайту DR, то после возвращения производственного сайта в онлайновый режим вы можете относительно легко перенаправить процесс репликации обратно на исходный сайт.

Предварительные условия для работы Hyper-V Replica

На исходном и целевом хостах должен функционировать гипервизор Hyper-V под управлением одной из перечисленных ниже операционных систем:

- Windows Server 2012 редакции Standard/Datacenter
- Windows Server 2012 R2 редакции Standard/Datacenter
- Hyper-V Server 2012 (бесплатная версия)
- Hyper-V Server 2012 R2

Для нормальной работы средства HVR на обоих хостах должна действовать одна и та же версия Hyper-V; например, вы не сможете реплицировать виртуальную машину, функционирующую на хосте с Windows Server 2012 R2, на хост с Windows Server 2012. В целях аутентификации вам нужно позаботиться о том, чтобы исходный и целевой хосты находились в одном и том же лесе Active Directory. В противном случае вам придется вручную импортировать сертификаты X.509 v3 согласно требованиям, изложенным по ссылке `http://blogs.technet.com/b/virtualization/archive/2012/03/13/hyper-v-replica-certificate-requirements.aspx`.

После того как вы удовлетворите требования к хостам для HVR, необходимо удостовериться в том, что на гостевых виртуальных машинах работает операционная система, которая поддерживается Hyper-V. Это означает, что вы не ограничены применением для HVR только виртуальных машин Windows Server 2012 и последующих версий, поэтому HVR становится очень привлекательным средством восстановления в аварийных ситуациях для более старых виртуальных машин.

Планирование технических характеристик для Hyper-V Replica

Без дополнительной помощи попытка оценить влияние HVR на ЦП, память, IOPS и полосу пропускания может оказаться довольно непростой задачей. В Microsoft разработали утилиту, назначение которой полностью отражается ее названием — Capacity Planner for Hyper-V Replica (Планировщик технических характеристик для Hyper-V Replica); она доступна по ссылке (`http://www.microsoft.com/en-us/download/details.aspx?id=39057`).

Эта утилита поможет правильно выбрать характеристики сервера, хранилища и сетевой инфраструктуры, которые необходимы для нормального функционирования HVR. Все, что потребуется — это загрузить и запустить данный инструмент из

хоста Hyper-V, работающего под управлением Windows Server 2012. После запуска появится диалоговое окно мастера, который проведет вас по процедуре начального конфигурирования. На рис. 28.17 видно, что мастер предлагает ввести имена хостов для первичного и вторичного серверов или точки клиентского доступа к брокеру Hyper-V Replica (Hyper-V Replica Broker Client Access Point — CAP), если применяется конфигурация кластера с обходом отказа. Здесь также нужно указать примерную ширину полосы пропускания WAN и продолжительность времени сбора метрик.

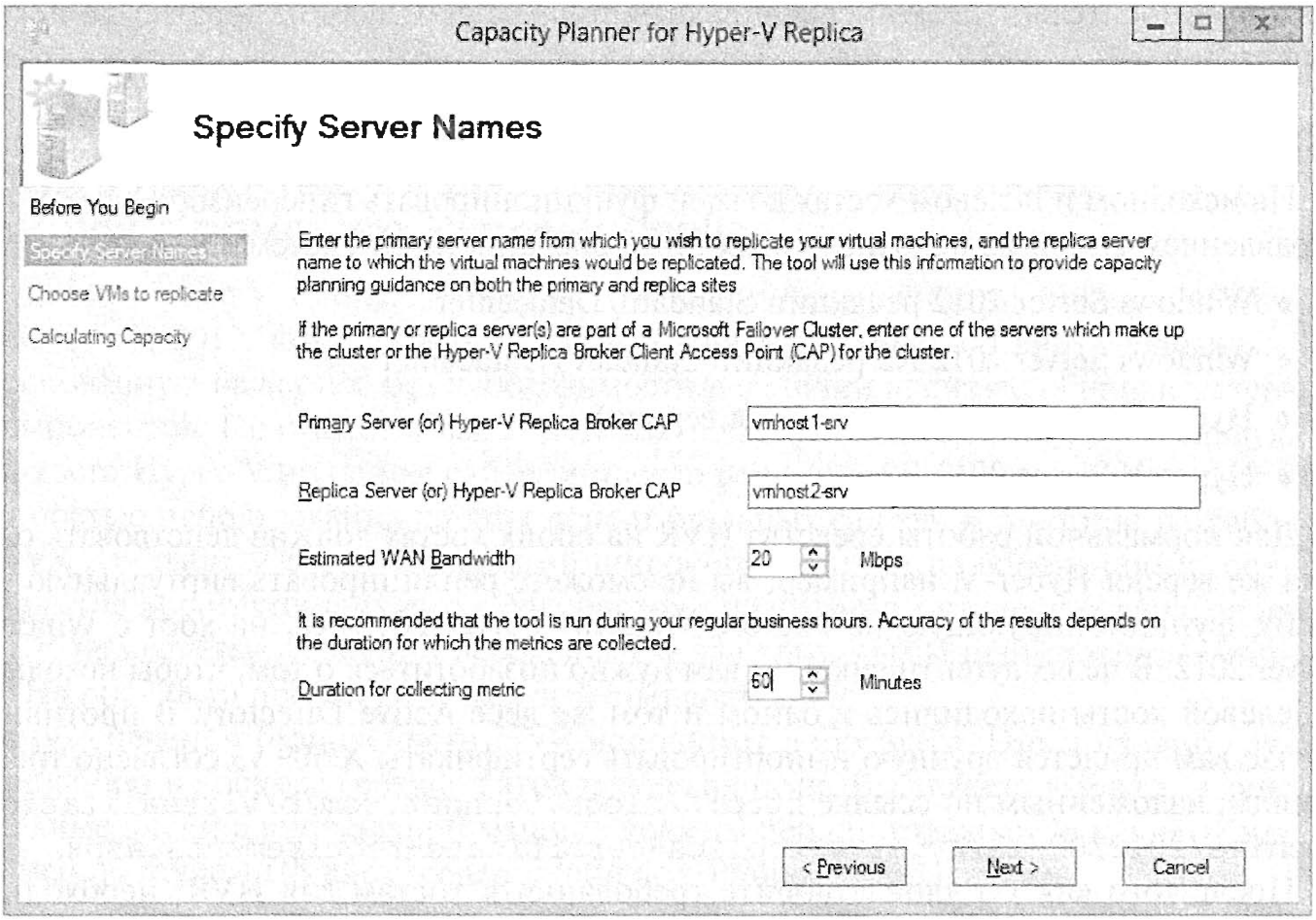
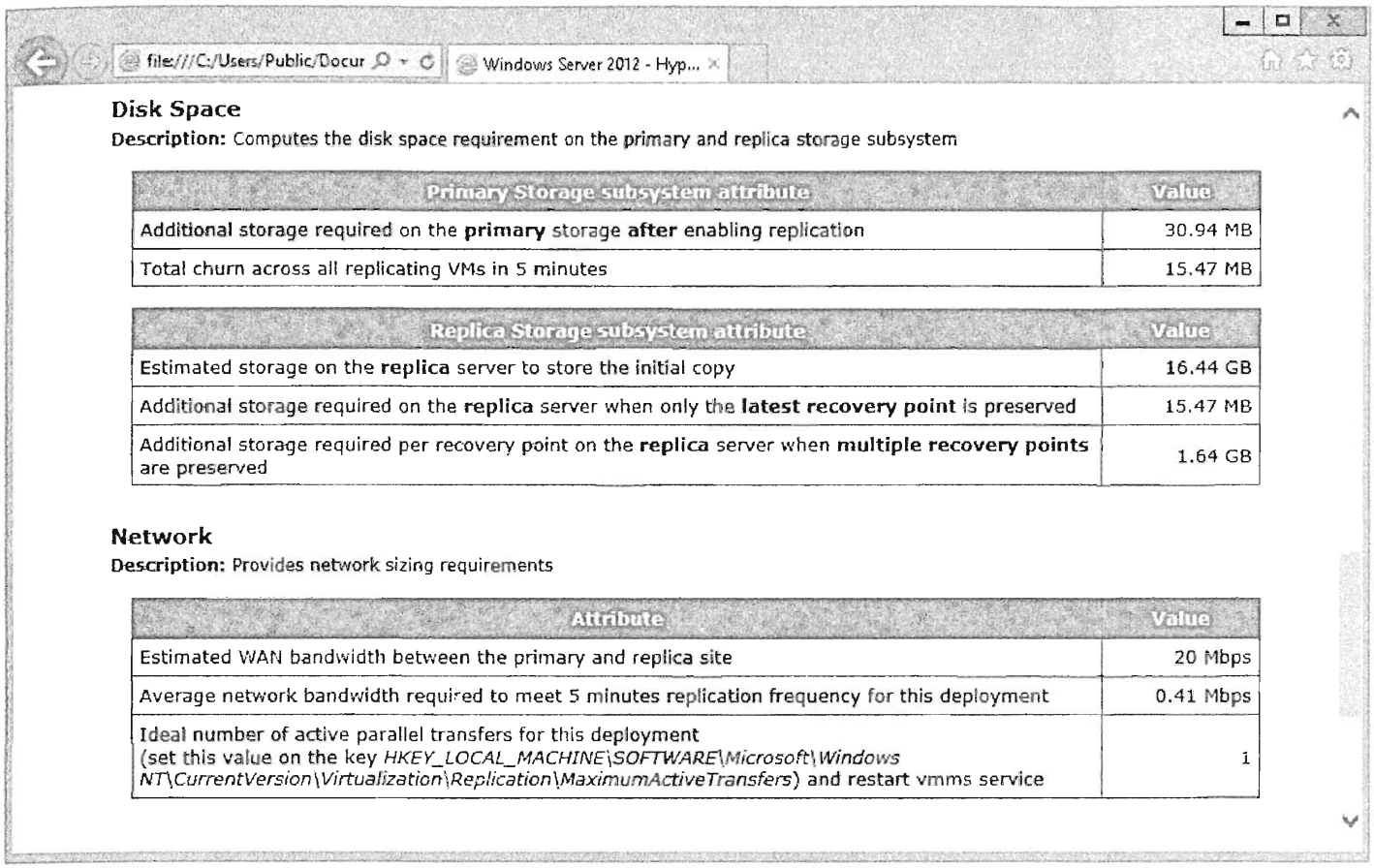


Рис. 28.17. Планировщик технических характеристик для HVR

Предоставив этой утилите параметры хоста HVR и полосы пропускания, вы должны выбрать временное место, где планировщик сможет создать и реплицировать тестовую виртуальную машину. Эта тестовая виртуальная машина используется для определения требований к развертыванию сети между первичным сервером и сервером реплики. После ввода всей необходимой информации утилита приступит к вычислению требуемых технических характеристик и выдаст отчет, подобный показанному на рис. 28.18.

Поддерживаемые сценарии для Hyper-V Replica

Средство Hyper-V Replica может выполнять не только репликацию между двумя хостами, не входящими в кластер, но также и репликацию с хоста, не входящего в кластер, на узел в кластере Hyper-V и наоборот. Это может оказаться полезным, если вы хотите гарантировать, что определенная кластеризованная виртуальная машина будет перемещена на хост, не входящий в кластер, внутри сайта DR.



file:///C:/Users/Public/Docur ... Windows Server 2012 - Hyp...

Disk Space

Description: Computes the disk space requirement on the primary and replica storage subsystem

Primary Storage subsystem attribute	Value
Additional storage required on the **primary** storage **after** enabling replication	30.94 MB
Total churn across all replicating VMs in 5 minutes	15.47 MB

Replica Storage subsystem attribute	Value
Estimated storage on the **replica** server to store the initial copy	16.44 GB
Additional storage required on the **replica** server when only the **latest recovery point** is preserved	15.47 MB
Additional storage required per recovery point on the **replica** server when **multiple recovery points** are preserved	1.64 GB

Network

Description: Provides network sizing requirements

Attribute	Value
Estimated WAN bandwidth between the primary and replica site	20 Mbps
Average network bandwidth required to meet 5 minutes replication frequency for this deployment	0.41 Mbps
Ideal number of active parallel transfers for this deployment (set this value on the key *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\Replication\MaximumActiveTransfers*) and restart vmms service	1

Рис. 28.18. Отчет о технических характеристиках

Включение Hyper-V Replica

Теперь, когда вы получили представление о том, что такое HVR, в этом разделе мы рассмотрим конфигурирование репликации виртуальной машины между двумя не входящими в кластер хостами Hyper-V, которые функционируют под управлением Windows Server 2012 R2. Мы будем применять `VMHOST1-SRV` в качестве исходного сервера, а `VMHOST2-SRV` в качестве целевого сервера реплики. Оба хоста в данном примере входят в состав одного и того же леса Active Directory и могут распознавать DNS-имена друг друга через WAN. По умолчанию средство HVR отключено, поэтому сначала его необходимо включить на целевом сервере.

1. Войдите в систему целевого сервера от имени учетной записи с административными разрешениями, откройте диспетчер Hyper-V, щелкните правой кнопкой мыши на хосте и выберите в контекстном меню пункт Hyper-V Settings (Настройки Hyper-V).

2. В разделе Server (Сервер) открывшегося окна Hyper-V Settings (Настройки Hyper-V) щелкните на элементе Replication Configuration (Конфигурация репликации) и отметьте флажок Enable this computer as a Replica server (Включить этот компьютер как сервер Hyper-V Replica), как показано на рис. 28.19.

   Обратите внимание на два флажка в области Authentication and ports (Аутентификация и порты): Use Kerberos (HTTP) (Использовать Kerberos (HTTP)) и Use certificate-based Authentication (HTTPS) (Использовать аутентификацию на основе сертификатов (HTTPS)); поскольку для аутентификации мы применяем Active Directory, в этом случае подойдет Kerberos.

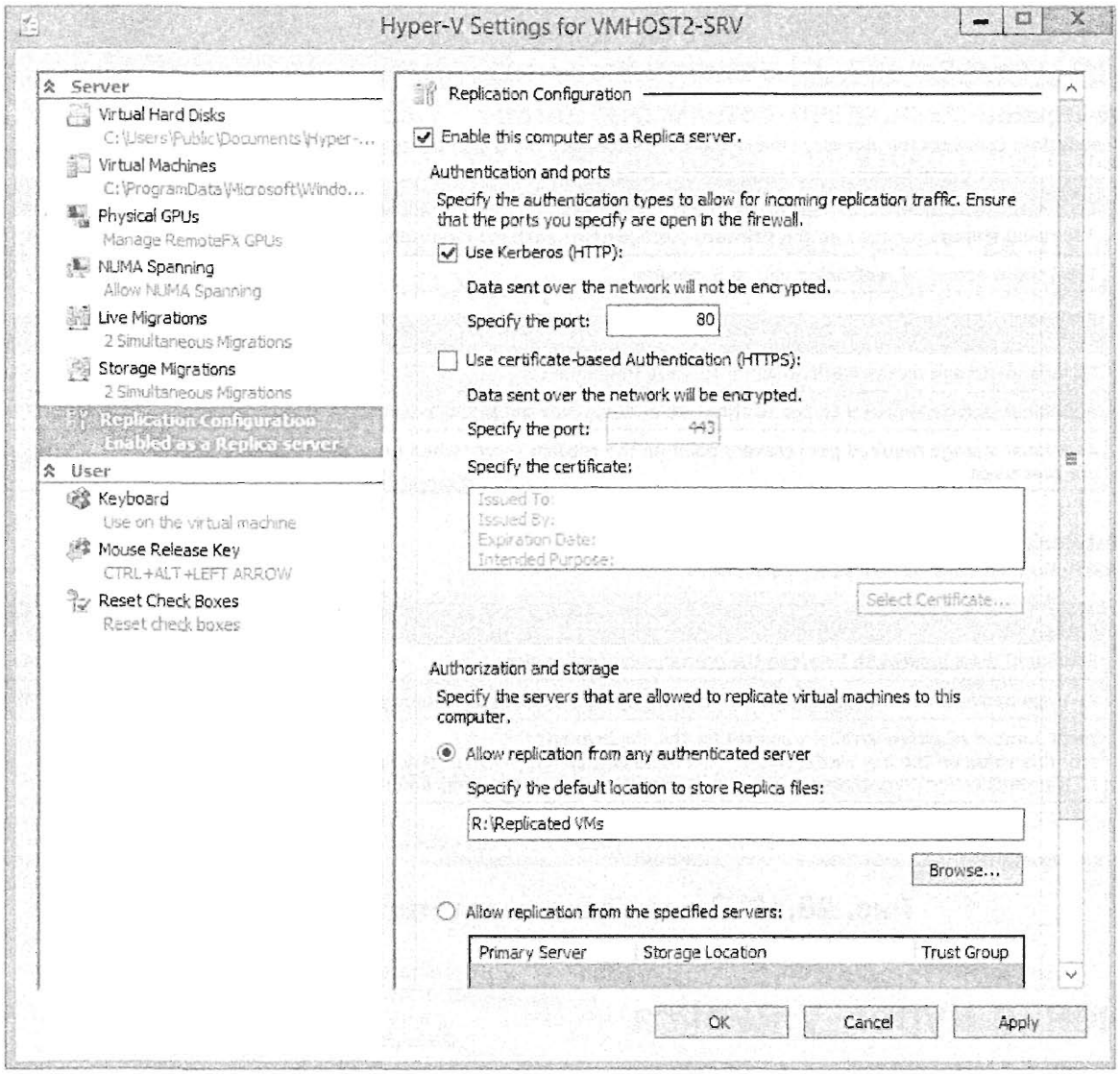


Рис. 28.19. Включение HVR на целевом хосте

3. Выберите переключатель Allow replication from any authenticated server (Разрешить репликацию из любого аутентифицированного сервера) и укажите местоположение на целевом хосте для сохранения реплицированных виртуальных машин (удостоверившись в наличии там достаточного свободного дискового пространства для поддержки реплик).

4. Щелкните на кнопке OK, чтобы закрыть окно Hyper-V Settings.

5. Появится всплывающее диалоговое окно с предупреждением о конфигурировании входящих правил брандмауэра для поддержки репликации. После этого проверьте, включено ли соответствующее правило для прослушивателя Hyper-V Replica (Hyper-V Replica Listener) в брандмауэре Windows на целевом хосте (рис. 28.20). Если вы модифицировали стандартные настройки портов HTTP и HTTPS, то должны будете создать специальные правила.

Конфигурирование репликации виртуальных машин

После включения HVR необходимо сконфигурировать репликацию виртуальных машин. Это делается индивидуально для каждой виртуальной машины. При первом включении репликации для какой-то виртуальной машины понадобится решить, каким образом будет создаваться "начальная" копия.

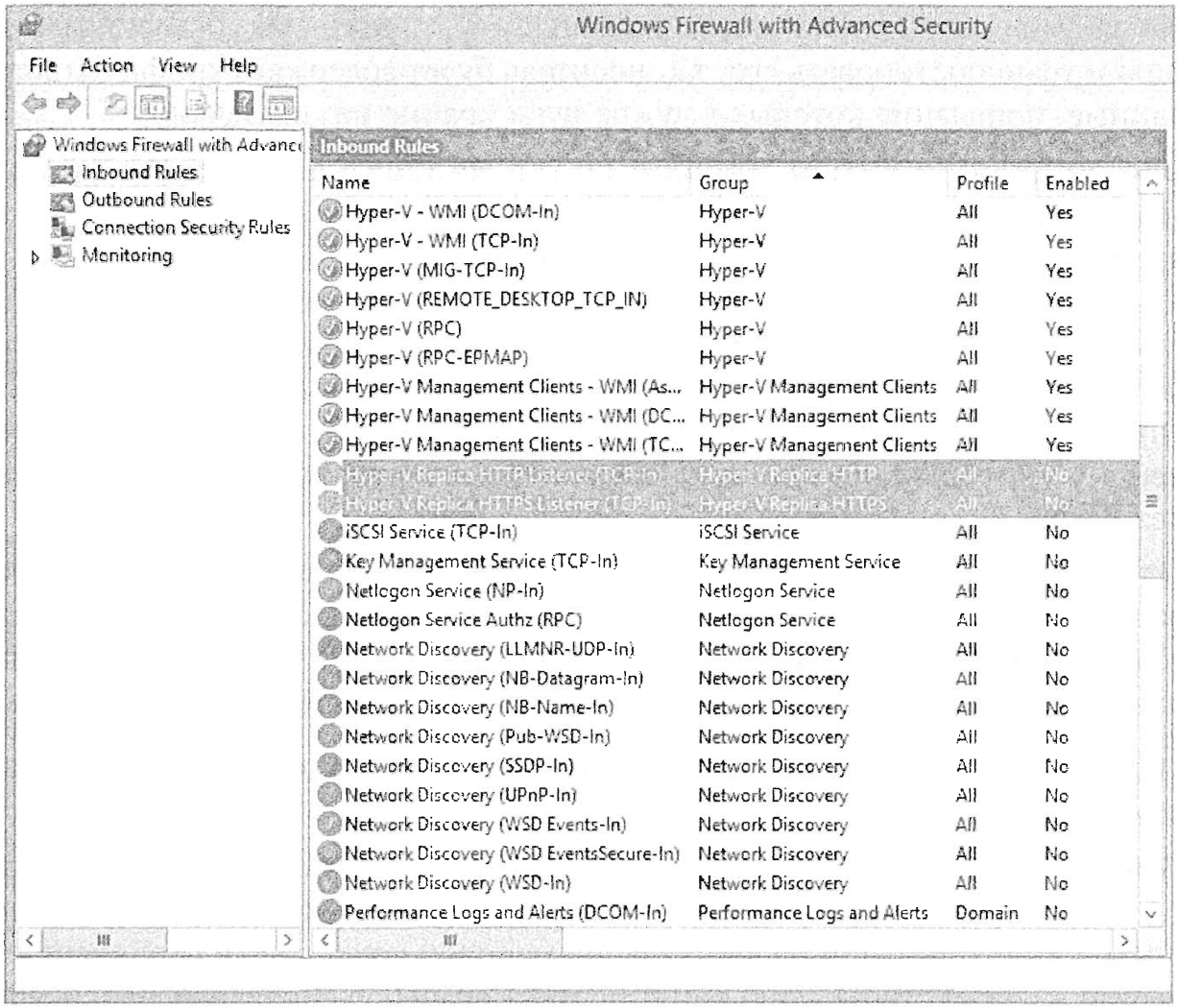


Рис. 28.20. Правила брандмауэра для Hyper-V Replica

Поскольку эта начальная копия будет довольно большой (в зависимости от размера реплицируемой виртуальной машины), для указания метода синхронизации на выбор доступны три разных переключателя.

- **Send Initial Copy over the Network (Передать начальную копию по сети).** Это самый простой вариант, который можно выбрать для начальной копии, но он зависит от наличия достаточно хорошего канала для выгрузки данных из производственного сайта на сайт DR. Если вы не располагаете выделенным подключением WAN для репликации между сайтами, то этот вариант может оказаться не самым подходящим. Однако такой метод весьма популярен, если конфигурация Hyper-V Replica создается, когда производственный хост и хост DR находятся на одном и том же сайте — возможно как временная мера для поддержки процесса начального копирования.
- **Send Initial Copy Using External Media (Передать начальную копию с помощью внешнего носителя).** С помощью этого варианта можно создать онлайновую экспортированную копию виртуальной машины и сохранить ее на внешнем носителе, таком как устройство USB. Затем вы доставляете этот внешний носитель на сайт DR и импортируете копию на целевой хост. Такой вариант хорошо подходит для организаций, которые имеют каналы WAN с небольшими скоростями выгрузки, и которым иначе понадобились бы недели на копирование реплик на сайт DR.

Не забудьте зашифровать съемный носитель, прежде чем помещать туда копию и транспортировать его, т.к. носитель будет содержать конфиденциальные данные, попадание которых в чужие руки крайне нежелательно.

- **Use an Existing Virtual Machine on the Replica Server as the Initial Copy (Использовать в качестве начальной копии существующую виртуальную машину на сервере Hyper-V Replica).** Интересным последним вариантом для вашей начальной копии является возможность использования существующей виртуальной машины, которую можно было бы восстановить с помощью какого-то решения по удаленному резервному копированию (наподобие DPM) и импортировать ее на целевой сервер. Когда вы включите репликацию на восстановленной виртуальной машине, HVR синхронизирует ее с исходным хостом через WAN.

  Однако этим вариантом нужно пользоваться крайне осторожно, поскольку если вы восстановите виртуальную машину из резервной копии и переведете ее в онлайновый режим, имея функционирующую виртуальную машину на производственном сайте, то очень быстро столкнетесь с серьезными проблемами.

В следующей процедуре для передачи начальной копии по сети будет применяться первый вариант.

1. Войдите в систему исходного сервера (`VMHOST1-SRV`) от имени учетной записи с административными разрешениями, откройте диспетчер Hyper-V, щелкните правой кнопкой мыши на виртуальной машине, подлежащей репликации, и выберите в контекстном меню пункт Enable Replication (Включить репликацию).
2. На экране Specify Replica Server (Указание сервера Hyper-V Replica) введите имя целевого сервера (или перейдите к нему), на котором вы ранее включили HVR.
3. Выберите тип аутентификации для виртуальной машины реплики или оставьте здесь стандартные настройки и щелкните на кнопке Next (Далее).
4. На экране Choose Replication VHDs (Выбор файлов VHD для репликации), представленном на рис. 28.21, отметьте флажки возле файлов VHD, которые хотите реплицировать, и снимите отметку возле тех из них, которые реплицировать не нужно, например, возле выделенного файла подкачки. Щелкните на кнопке Next.

   Следующий экран позволяет указать частоту передачи изменений на целевой сервер — 30 секунд, 5 минут и 15 минут.
5. Сделав выбор, щелкните на кнопке Next.
6. На экране Configure Additional Recovery Points (Конфигурирование дополнительных точек восстановления) выберите сохранение только самой последней точки восстановления реплицированной виртуальной машины или создайте дополнительные точки восстановления, чтобы иметь возможность восстановить ее в какой-то более ранней точке.
7. Для продолжения щелкните на кнопке Next.

   Предпоследний экран мастера показан на рис. 28.22. Именно здесь выбирается метод репликации начальной копии (как обсуждалось ранее), а также время передачи начальной копии.

8. Сделав выбор, щелкните на кнопке Next.
9. На экране Summary (Сводка) просмотрите настройки конфигурации и щелкните на кнопке Finish (Готово), чтобы завершить работу мастера.

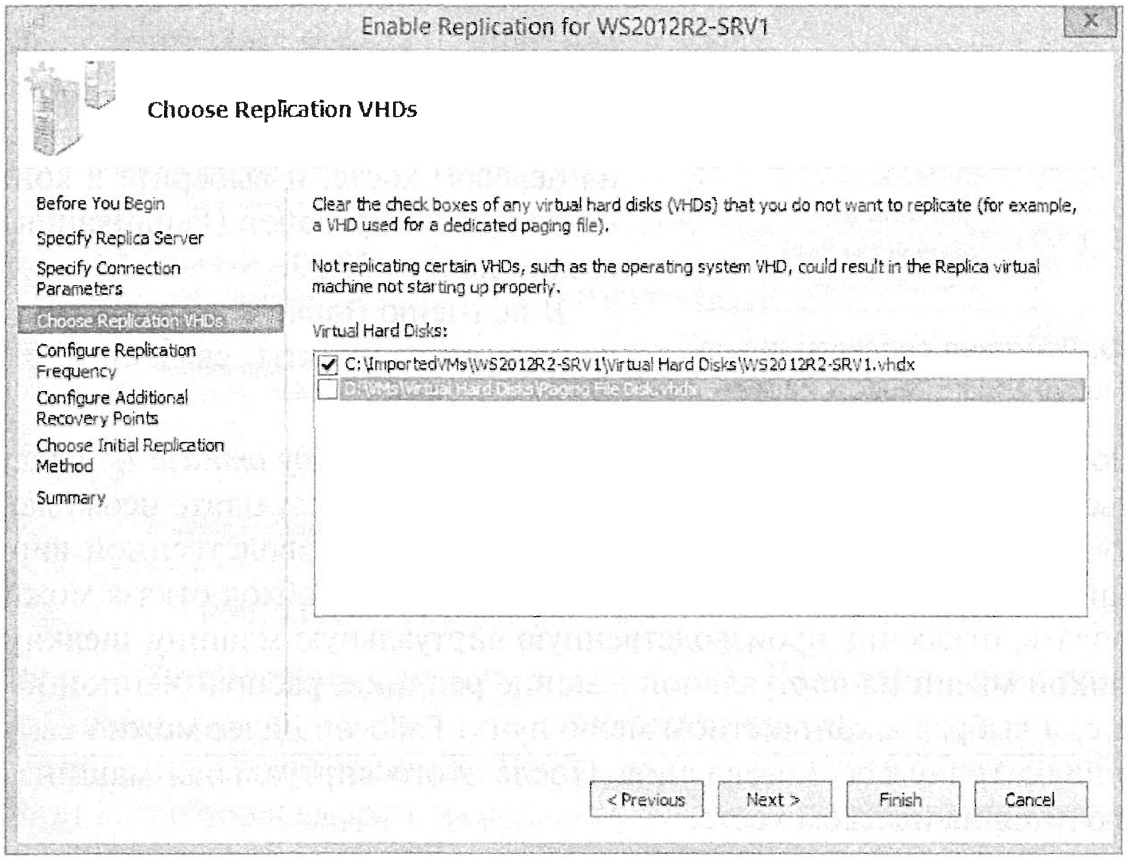


Рис. 28.21. Выбор файлов VHD, подлежащих репликации

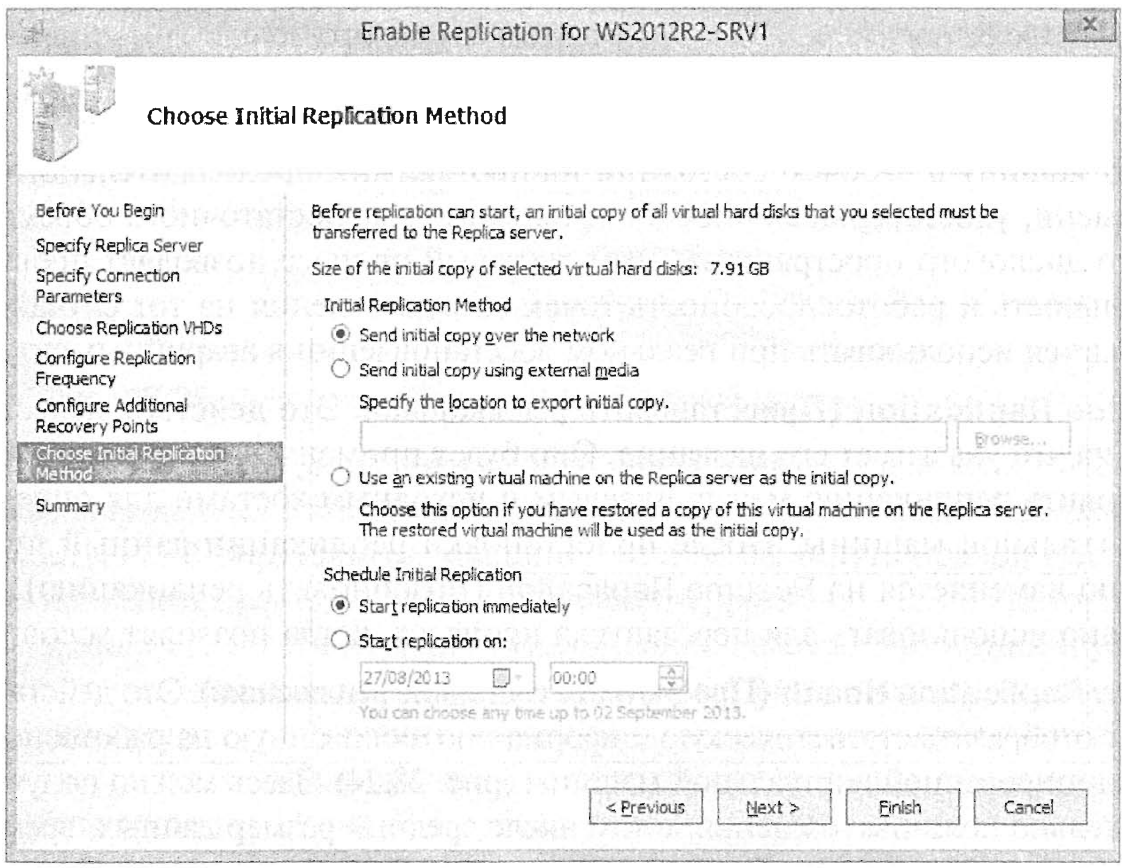


Рис. 28.22. Выбор метода репликации начальной копии

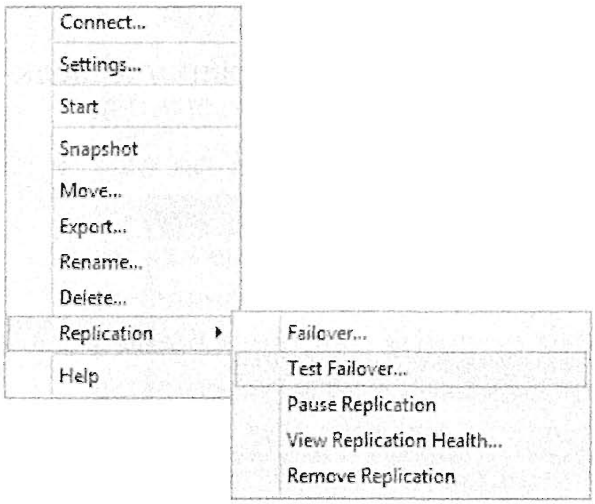


Рис. 28.23. Действия репликации виртуальной машины на целевом хосте

Управление репликами виртуальных машин

Имея сконфигурированные реплики виртуальных машин, с ними можно выполнять действия. Для этого щелкните правой кнопкой мыши на реплицированной виртуальной машине в автономном режиме, размещенной на целевом хосте, и выберите в контекстном меню пункт Replication (Репликация), как показано на рис. 28.23.

В подменю Replication доступны перечисленные ниже пункты, связанные с задачами обхода отказа.

- **Failover (Обход отказа).** К *незапланированному обходу отказа* не следует относиться необдуманно. Здесь предполагается, что в результате неожиданного отключения или выхода из строя обращение к производственной виртуальной машине стало невозможным. Незапланированный обход отказа можно смоделировать, отключив производственную виртуальную машину, щелкнув правой кнопкой мыши на виртуальной машине реплики, расположенной на целевом хосте, и выбрав в контекстном меню пункт Failover. Далее можно выбрать подходящую точку восстановления. После этого виртуальная машина реплики включится на целевом хосте.
- **Test Failover (Тестовый обход отказа).** *Тестовый обход отказа* создает копию виртуальной машины путем ее клонирования и сохранения клона на разностном виртуальном диске с использованием хранилища виртуальной машины реплики в качестве ее родителя. Поскольку в этом случае применяется хранилище виртуальной машины реплики, разностный диск будет сохранен на том же томе, что и реплика. Таким образом, если вы намерены поддерживать тестовую виртуальную машину в рабочем состоянии на протяжении продолжительного периода времени, удостоверьтесь в наличии на этом томе достаточного объема свободного дискового пространства. Этот тестовый процесс позволяет проверить актуальность и работоспособность точек восстановления на тот случай, если их придется использовать при реальном восстановлении в аварийных ситуациях.
- **Pause Replication (Приостановить репликацию).** Это действие делает именно то, на что указывает его название. Оно будет применяться, когда нужно приостановить репликацию между целевым и исходным хостами для определенной виртуальной машины. После приостановки репликации данный пункт подменю изменяется на Resume Replication (Возобновить репликацию), который можно использовать для перезапуска процесса, когда позволят условия.
- **View Replication Health (Просмотреть состояние репликации).** Это действие позволяет отобразить статистическую информацию, основанную на работоспособности реплицированной виртуальной машины (рис. 28.24). Здесь можно получить действительно полезные сведения, в том числе средний размер данных, время ожидания, обнаруженные ошибки и время последней синхронизации. С этого пункта меню всегда удобно начинать поиск и устранение неполадок в репликах HVR.

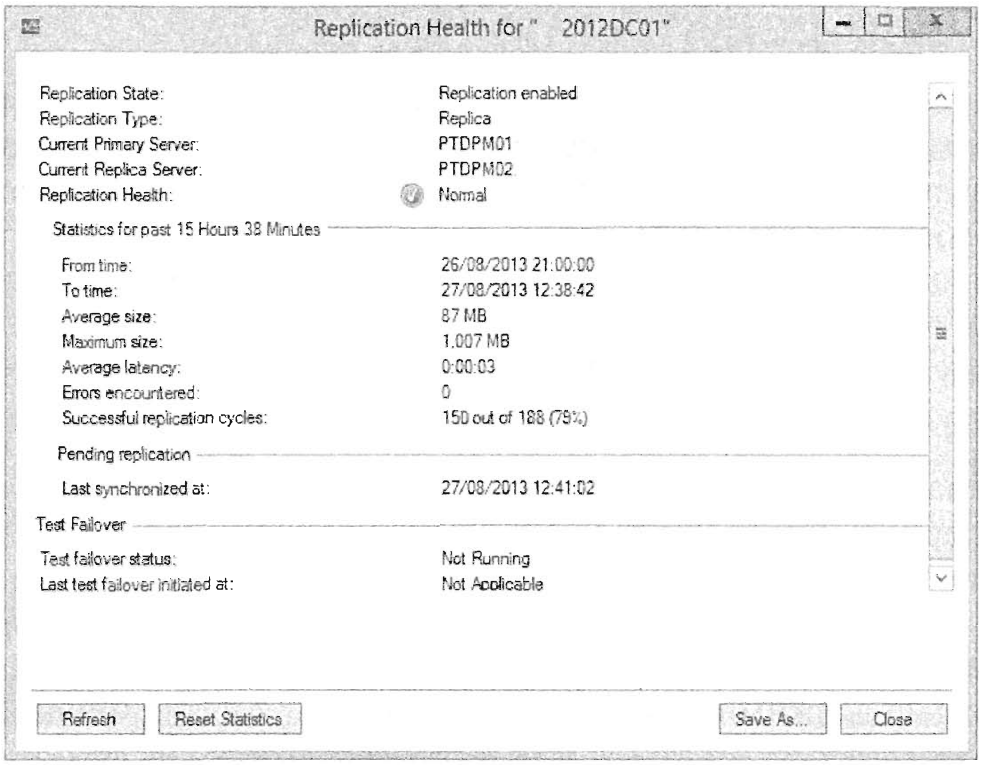


Рис. 28.24. Проверка работоспособности репликации

- **Remove Replication (Удалить репликацию).** Еще одно очевидное действие. Выбирайте этот пункт подменю, если хотите удалить репликацию для отдельно взятой виртуальной машины. Чтобы полностью удалить репликацию, данный пункт потребуется выбрать на репликах исходной и целевой виртуальных машин.

Если щелкнуть правой кнопкой мыши на производственной виртуальной машине, которая размещена на исходном хосте, и выбрать в контекстном меню подменю Replication, то вместо пунктов Failover и Test Replication в нем появится пункт Planned Failover (Запланированный обход отказа), как показано на рис. 28.25.

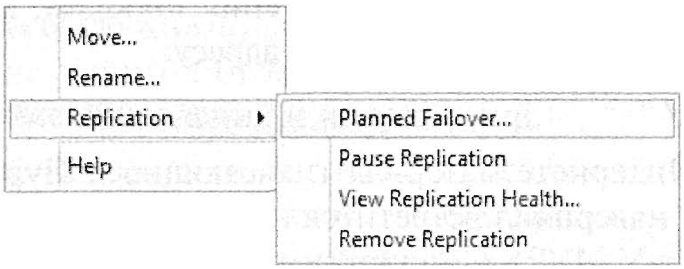


Рис. 28.25. Действия репликации виртуальной машины на исходном хосте

- **Planned Failover (Запланированный обход отказа).** Если вы хотите выполнить *запланированный обход отказа*, то должны сначала завершить работу производственной виртуальной машины, а затем щелкнуть правой кнопкой мыши на производственной виртуальной машине, размещенной на исходном хосте, и выбрать в контекстном меню пункт Planned Failover. Это инициирует проверку, действительно ли данная производственная виртуальная машина выключена, а направление репликации может быть изменено на противоположное после завершения запланированного обхода отказа. Когда проверка завершится, файлы журнала Hyper-V Replica будут помещены на целевой хост реплики и применены. Наконец, виртуальная машина реплики будет автоматически включена на целевом хосте и готова к использованию.

Онлайновые ресурсы по Hyper-V

В этом разделе приведен чрезвычайно полезный список онлайновых ресурсов, к которым вы можете обращаться при работе с Hyper-V в Windows Server 2012 R2. Ссылки включают официальные источники Microsoft, блоги сообщества, а также социальные сети.

Бен Армстронг — руководитель программы Hyper-V в Microsoft, а его блог по виртуализации является именно тем местом, где вы найдете по-настоящему полезные материалы, касающиеся Hyper-V:

```
http://blogs.msdn.com/b/virtual_pc_guy/
```

Блог Айдана Финна является одним из наиболее посещаемых ресурсов по Hyper-V в Интернете. Айдан Финн — обладатель звания Hyper-V MVP в Ирландии; он написал многочисленные книги, доклады и статьи по всем версиям Hyper-V. Он был ведущим автором книги *Hyper-V Installation and Configuration Guide*, опубликованной издательством Sybex. Если вы хотите изучить Hyper-V действительно глубоко, то обязательно должны прочитать эту книгу. Блог Айдана Финна доступен по ссылке:

```
http://www.aidanfinn.com
```

Дидье Ван Хой — обладатель звания Hyper-V MVP в Бельгии; его блог посвящен вопросам развертывания и управления Hyper-V в крупных организациях. Некоторые из предложенных им эталонных тестов для решений Hyper-V и организации хранилищ уровня предприятия пользуются огромной популярностью и заслуживают ознакомления:

```
http://workinghardinit.wordpress.com/
```

Еще одним обладателем звания MVP и знатоком всевозможных тонкостей Hyper-V является Ханс Фредевоорт. Он регулярно публикует материалы, посвященные сложным вопросам поиска и устранения проблем, а также интеграции с Hyper-V и System Center. Его можно найти по адресу:

```
http://hyper-v.nu/
```

Если вы ищете в Интернете материалы, касающиеся Hyper-V версии Windows Server 2012 R2, то вам наверняка встретится несколько статей из блога швейцарца Томаса Маурера (Hyper-V MVP). С некоторыми его статьями можно ознакомиться по следующему адресу:

```
http://www.thomasmaurer.ch/
```

Наконец, когда обнаружится, что вам нужна помощь в понимании виртуализации сетей Hyper-V и таких аспектов, как сходящаяся фабрика, NVGRE и виртуальные шлюзы, то вам определенно следует почитать блог Дамиана Флинна (Cloud and Datacenter MVP). Дамиан был соавтором книги *Hyper-V Installation and Configuration Guide* и среди специалистов, не работающих в Microsoft, является одним из тех, к кому можно обратиться за квалифицированной консультацией по этим вопросам. Его блог доступен по адресу:

```
http://www.damianflynn.com/
```

Резюме

Виртуализируйте контроллеры домена. В Windows Server 2012 предлагается новый метод очень быстрого развертывания любого количества виртуальных контроллеров домена посредством *клонирования виртуальных контроллеров домена*. Он позволяет администраторам оперативно вводить в действие копии контроллеров домена, используя в качестве эталона существующий шаблонный контроллер домена. Клонирование виртуальных контроллеров домена может быть выгодно организациям, которым необходимо быстро развернуть много контроллеров в новых доменах. Эта функция также полезна в частных облачных средах при удовлетворении требований масштабируемости.

> *Контрольный вопрос.* Какова минимальная поддерживаемая версия Active Directory, которую можно использовать с клонированием виртуальных контроллеров домена?

Уясните, как перемещать виртуальные машины. Средство Hyper-V в Windows Server 2012 позволяет относительно просто *экспортировать* и *импортировать* виртуальные машины между хостами. Это стало возможным за счет того, что все хосты Hyper-V предоставляют своим виртуальным машинам практически идентичное оборудование посредством компонентов интеграции и синтетических драйверов. Если требовалось перемещать установленные копии ОС в мире физических серверов, то нужно было, как минимум, переносить физические диски, что работало только в случае достаточного сходства оборудования, но при этом далеко не всегда гарантировало успех.

> *Контрольный вопрос.* Какие три параметра необходимо перенести при перемещении виртуальной машины на другой хост Hyper-V?

Управляйте виртуальными машинами. Хотя виртуализация привносит множество новых средств и добавляет гибкости, вам по-прежнему приходится выполнять более традиционные задачи по обслуживанию виртуальных машин, такие как резервное копирование, управление защитой от вредоносного программного обеспечения и своевременное применение обновлений и исправлений.

> *Контрольный вопрос.* Какую технологию вы использовали бы для применения исправлений к производственным виртуальным машинам, если вы располагаете кластером с обходом отказа Hyper-V, который функционирует под управлением Windows Server 2012 R2?

Уясните, как выполняется восстановление в аварийных ситуациях с помощью Hyper-V. Средство Hyper-V Replica (HVR) доступно в Windows Server 2012 и последующих версиях. Оно делает возможной репликацию виртуальных машин на основе хоста, не требуя создания общих кластерных компонентов для поддержки сценариев восстановления в аварийных ситуациях.

> *Контрольный вопрос.* На какое количество сайтов, находящихся за пределами производственного сайта, можно реплицировать виртуальные машины, имея функционирующее средство Hyper-V Replica в Windows Server 2012 R2?

Глава 29

Установка, использование и администрирование служб удаленного рабочего стола

Службы удаленного рабочего стола (Remote Desktop Services — RDS), ранее известные как терминальные службы (Terminal Services — TS) — это роль в Windows Server 2012 R2, которая позволяет пользователям подключаться к рабочим столам, приложениям и виртуальным рабочим столам на основе сеансов.

Приложения, которые выполняются на хост-сервере сеансов удаленных рабочих столов (RD Session Host), называются приложениями RDS RemoteApp. С точки зрения конечного пользователя эти приложения выглядят так, словно они выполняются на его локальной системе. Нажатия клавиш и перемещения курсора мыши, совершаемые пользователем, передаются серверу. Изображения отправляются обратно в систему пользователя. Даже "тонкие" клиенты способны без проблем выполнять сложные приложения, хотя приложения RDS RemoteApp чаще всего функционируют на обычных настольных системах.

Старые терминальные службы бывали двух разновидностей: TS для администраторов и TS в режиме приложения. Службы TS для администраторов в настоящее время известны как Remote Desktop for Administration (Удаленный рабочий стол для администрирования), а TS в режиме приложения — как Remote Desktop Services с сервером RD Session Host. Службы Remote Desktop for Administration обсуждались в главе 17, а в настоящей главе рассматриваются службы Remote Desktop Services с сервером RD Session Host.

В этой главе вы изучите следующие темы:

- ограничение максимального количества подключений;
- добавление приложения на сервер RD Session Host;
- добавление приложений RemoteApp для доступа посредством веб.

Потребность в службах удаленного рабочего стола

Службы удаленного рабочего стола могут применяться для предоставления конечным пользователям возможности запуска на удаленном сервере Windows-программы со своих настольных компьютеров. Сервер, размещающий приложение, называется *хост-сервером сеансов удаленных рабочих столов* (Remote Desktop Session Host — RD Session Host). Конечные пользователи также могут получать доступ к сеансу полнофункционального рабочего стола на сервере RD Session Host и, если этого недостаточно, то теперь можно использовать хост виртуализации служб удаленного рабочего стола (Remote Desktop Services Virtualization Host) для инфраструктуры виртуальных рабочих столов (Virtual Desktop Infrastructure — VDI).

Как администратор вы можете решать следующие задачи.

- Разворачивать и управлять приложениями на нескольких серверах RDS вместо сотен или тысяч клиентских компьютеров.
- Предоставлять приложения конечным пользователям, которых невозможно легко поддерживать из-за того, что они находятся в другом офисе или даже в другой стране.
- Снижать влияние отказов клиентского оборудования, сохраняя все приложения на центральном сервере. Если какой-то из клиентских компьютеров выходит из строя, достаточно подключить новый клиентский компьютер, и работа будет возобновлена.
- Избегать неправильно сконфигурированных компьютеров, например, если для корректной работы какого-то приложения требуется определенный набор двоичных файлов, но пользователи установили другие приложения и в результате переписали эти двоичные файлы.
- Отказаться от погони за все более новым и совершенным оборудованием, что требует постоянных обновлений для поддержки новейшего программного обеспечения.
- Применять компьютеры в окружающих средах, неприемлемых для настольных компьютеров, например, в промышленном производстве, где загрязнение воздуха может стать причиной выхода из строя ПК.
- Упростить работу служб технической поддержки и обучения.

Если любые из этих задач важны для вас, то вы должны всерьез рассмотреть возможность использования Remote Desktop Services с сервером RD Session Host.

Централизованное развертывание приложений

Одно из крупных достоинств служб Remote Desktop Services заключается в том, что они упрощают развертывание приложений. Вместо того чтобы развертывать приложение на всех клиентах с помощью групповой политики или диспетчера конфигурации системного центра Microsoft (Microsoft System Center Configuration Manager — SCCM), достаточно один раз установить это приложение на сервере RD Session Host.

Например, ваша компания может располагать производственным приложением, доступ к которому должны иметь 100 пользователей. Вместо установки его на всех 100 настольных компьютерах вы можете воспользоваться сервером RD Session Host. На такой сервер приложение устанавливается однократно, и затем каждый пользователь сможет обращаться к нему дистанционно. Более того, когда приложение понадобится обновить или применить к нему исправления, это придется делать только в одном месте — на сервере RD Session Host.

Поддержка удаленных пользователей

Службы Remote Desktop Services можно использовать для дистанционного доступа или доступа из офисов филиалов. Некоторые приложения испытывают трудности с работой через медленные подключения или нуждаются в открытии специальных портов на брандмауэре. Вместо запуска таких приложений через медленные подключения вы можете разместить их на сервере RD Session Host внутри высокоскоростной сети.

Клиенты могут по-прежнему подключаться через VPN или низкоскоростные коммутируемые линии. Однако поскольку приложения выполняются на сервере RD Session Host в быстродействующей сети, более медленные подключения не влияют на их производительность.

Все большее и большее число людей выполняют свою работу дистанционно как минимум пару дней в неделю. Многие государственные учреждения в США официально разрешают своим сотрудникам работать в подобной манере, причем у многих таких работников зачастую даже нет собственного рабочего места в офисе. Вместо того чтобы пытаться обеспечить настольными компьютерами всех своих сотрудников, многие компании предоставляют пользователям возможность брать компьютеры домой и обращаться к нужным приложениям посредством удаленных серверов.

Поддержка окружающих сред, неблагоприятных для ПК

Мечта о "ПК на каждом рабочем столе" так и останется мечтой в случаях, когда окружающая среда оказывается неподходящей для настольного ПК или настольный ПК не соответствует имеющимся условиям. Другими словами, когда размещение где-нибудь настольного ПК не представляется возможным.

Некоторые среды оказывают вредное воздействие на ПК. Персональные компьютеры плохо переносят пыль, высокую температуру и вибрацию. Вряд ли вам понравится обслуживать ПК в подобных окружающих средах. Разумеется, некоторые ПК приспособлены для работы в экстремальных условиях, например, при повышенных температурах или даже под водой. Для компаний и людей, которым приходится эксплуатировать ПК в таких экстремальных средах, предусмотрены соответствующие конструктивные решения, но стоят они совсем недешево. Когда цена является критическим фактором, а тонкий клиент способен справиться с работой, то оптимальным решением могут оказаться службы Remote Desktop Services.

Нам приходилось видеть терминалы в кафе при спортивных клубах и в кофейнях, которые были устроены так, что виден только монитор. Это уменьшало шансы попадания бутербродных крошек и капель фруктовых коктейлей внутрь корпуса. Если все же кто-то умудрится пролить коктейль внутрь корпуса терминала, то из-за того, что приложения установлены и функционируют на сервере RD Session

Host, замена устройства для предоставления идентичной среды сводится к простому отключению вышедшего из строя терминала и подключению нового. Если пролить коктейль на системный блок компьютера, то восстановление идентичной рабочей среды будет значительно более сложной задачей.

Что можно сказать о ситуации, когда настольный ПК не соответствует имеющимся условиям? Стерильные помещения, в которых изготавливаются микросхемы и платы, являются хорошими кандидатами на установку терминалов Windows. В стерильном помещении не должно быть пыли, а вентиляторы внутри системного блока выдувают из него пыль. Вдобавок санитарную обработку перед входом в стерильное помещение нельзя назвать простой или недорогой; вряд ли целесообразно использовать в таком помещении устройства, которые требуют регулярного ухода и обслуживания со стороны IT-персонала. Еще один фактор применим ко многим ситуациям, а не только к стерильным помещениям: любое помещение, пространство которого пользуется большим спросом, будет подходящим кандидатом для применения терминалов Windows.

На клиентской стороне могут функционировать тонкие клиенты или практически любая настольная операционная система, включая Windows, Linux и Macintosh (хотя безопасность оптимизирована в случае Windows Vista или Windows 7/8).

В этом разделе мы не намерены рекламировать идею использования терминалов Windows. Мы просто хотим подчеркнуть, что иногда их применение бывает полезным и даже необходимым, к тому же их нельзя использовать без сервера RD Session Host.

Пример из практики

Борьба за снижение потребления энергии

Еще один аспект недружественного к окружающей среде ПК касается потребляемой настольным компьютером энергии. Опубликованы результаты многочисленных исследований, посвященных экономии затрат тонкими клиентами по сравнению с настольными ПК. Учитывая высокую стоимость электроэнергии в наши дни, экономия может оказаться весьма существенной.

Одно исследование, результаты которого доступны по адресу `www.thinclient.net/pdf/Thin_Client_Benefits_Paper.pdf`, демонстрирует определенные возможности в плане экономии. Оно проводилось достаточно давно, но принципы остались действительными и в наше время. Например, одиночный тонкий клиент потребляет в среднем 10 Вт в день, тогда как среднее потребление настольного ПК составляет 69 Вт. Этот показатель не включает потребление монитора, однако и тонкие клиенты, и ПК могут использовать маломощные LCD-мониторы вместо старых весьма прожорливых мониторов с электронно-лучевыми трубками.

В исследованиях принималась цена электроэнергии между $0,10 и $0,20 за 1 кВт/час, что является довольно точным диапазоном тарифов в США. Для 100 клиентов годовая экономия составит от $3000 до $6000.

Экономия затрат на электроэнергию не является единственной причиной применения терминалов Windows, но если вы обдумываете идею замены ПК терминалами, то это убедительный аргумент в ее пользу.

Сокращение количества обновлений оборудования

Требуется ли для проверки электронной почты, решения бухгалтерских задач и блуждания в Интернете процессор Core i5 с тактовой частотой 2,5 ГГц и 4 Гбайт оперативной памяти? Конечно же, нет, однако по состоянию на середину 2013 года такой профиль оборудования для настольного компьютера не является редкостью. Не то, чтобы такие компьютеры стоили слишком дорого в абсолютном выражении, но мы успокаиваем себя тем, что каждый раз, когда покупаем новый компьютер, мы выкладываем меньшую сумму за более мощную систему, чем та, которая приобреталась в последний раз.

И все же, несмотря на то что новые компьютеры не являются чересчур дорогими в абсолютном выражении, они не всегда стоят этих затрат, т.к. выполняемые вами задачи не предъявляют слишком больших требований к оборудованию. По иронии судьбы, если только вы не занимаетесь работой, предъявляющей действительно высокие требования к оборудованию, скажем, автоматизированным проектированием, то более мощный компьютер, скорее всего, понадобится дома, а не на работе, учитывая требования к оборудованию со стороны компьютерных игр. Чтобы сыграть несколько стремительных раундов последней версии Warcraft, потребуется более высокая вычислительная мощность, чем для написания этой главы. (Сражение с орками — работа не из легких!)

Проблема в том, что иногда вам действительно необходимо иметь более мощные компьютеры, если вы намерены шагать в ногу с существующими технологиями ПО. Да, вам не нужен самый быстрый в мире компьютер, чтобы выполнять текстовую обработку. Однако вам может понадобиться более быстрый компьютер, чем тот, которым вы располагаете, если вы собираетесь следить за развитием самого нового и мощного пакета текстовой обработки, которым пользуется большинство. Если вы хотите иметь возможность читать все схемы и диаграммы, то это будет удаваться не всегда, если применяемому текстовому редактору уже исполнилось шесть лет, хотя он по-прежнему удовлетворяет домашним нуждам. К тому же вы не всегда сможете запустить этот новый текстовый редактор, если компьютер был куплен шесть лет тому назад.

Вы должны также принимать во внимание современные устройства, предлагаемые на рынке в настоящее время. Потребление энергии играет в них первостепенную роль, чтобы сделать их легкими, мобильными и имеющими достаточно продолжительный срок службы. Чтобы снизить потребление энергии, производителям также приходится уменьшать вычислительную мощность устройств, поэтому сейчас для выполнения функций, требующих интенсивных вычислений, важность сервера RD Session Host возрастает. Это также справедливо в случае, если компания использует стратегию BYOD; клиенты Remote Desktop доступны практически для каждой платформы. Это обеспечивает пользователям необходимую гибкость в вопросах приобретения и работы с требуемыми им устройствами, в то время как администраторы корпорации сохраняют контроль над корпоративной системой и настольными приложениями.

Подводя итоги, можно сказать, что если вы применяете службы Remote Desktop Services с сервером RD Session Host, то клиент только отображает приложения, выполняющиеся на сервере RD Session Host, вместо того чтобы запускать их локально.

Вас не беспокоит вопрос, смогут ли эти приложения выполняться на клиентском компьютере; вас интересует лишь сервер. Если приложение может быть запущено на сервере RD Session Host, а клиент имеет доступ к этому серверу, то приложение будет отображаться на стороне клиента независимо от платформы.

Упрощение пользовательского интерфейса

Еще одно потенциальное преимущество служб Remote Desktop Services связано с тем, что они способствуют упрощению пользовательского интерфейса. Иметь дело с компьютером не настолько легко, как уверяют в мире маркетинга. Опытные пользователи находят простым настройку интерфейса под свои нужды, но менее опытные при взаимодействии со своими компьютерами сталкиваются со всеми возможными видами ловушек: слишком много параметров, чтобы легко запутаться, и слишком много способов нарушить работу каких-то компонентов. Красочные значки со скругленными углами не делают пользовательский интерфейс простым.

Если поддерживаемым вами пользователям требуется только одно приложение, то вы можете существенно упростить жизнь себе и им, предоставив подключение, которое запускает это приложение на удаленном рабочем столе и ничего другого не делает. Это особенно справедливо в отношении терминалов на основе Windows, которые представляют собой немногим более чем монитор, системный блок, клавиатуру и мышь.

Если пользователи уже работают в среде настольной ОС, то вы можете применять приложения RemoteApp. Пользоваться приложениями RemoteApp, развернутыми через RDS, так же просто, как любыми другими приложениями на компьютере конечного пользователя. Приложения RemoteApp можно запускать через меню Start (Пуск), посредством значка рабочего стола (файл `.rdp`) либо из веб-страницы.

Обеспечение службы технической поддержки

Наконец, службы Remote Desktop Services могут облегчить поддержку приложений, причем не только в отношении установки новых приложений и применения исправлений, но и в плане оказания людям помощи в освоении этих приложений. Технология *Remote Desktop Shadowing* (Теневое использование удаленного рабочего стола), которая раньше называлась Remote Control (Удаленное управление), позволяет персоналу технической поддержки или администраторам подключаться к удаленному сеансу другого человека, чтобы либо наблюдать за его работой, либо взаимодействовать с удаленным сеансом. Это не происходит автоматически и требует определенных действий от администратора и пользователя. Кроме того, с помощью объекта GPO можно управлять некоторыми аспектами его поведения.

При наличии удаленного управления сеансом другого пользователя вы можете или наблюдать за его действиями и направлять их (возможно, по телефону), или реально взаимодействовать с сеансом с целью демонстрации процесса пользователю. Это лучше, чем стоять за спиной у человека и говорить ему: “Щелкните на кнопке Файл в верхнем левом углу. Нет, Файл. Кнопка Файл!” либо пытаться определить, что он делает, когда единственным источником информации является сам этот человек, пытающийся рассказать о том, что у него появляется на экране.

Развертывание приложений RDS RemoteApp

Программы RemoteApp — это приложения, которые выполняются на сервере RD Session Host, но для конечного пользователя все выглядит так, будто они функционируют на его рабочем столе. Именно таким образом удобно представлять этот процесс конечному пользователю. Он не обязан управлять множеством рабочих столов, а вместо этого может просто запустить еще одно приложение со своего рабочего стола.

Программы RemoteApp были введены в Windows Server 2008 и впоследствии совершенствовались в каждом новом поколении Windows, включая Windows Server 2012 R2. Ниже описаны некоторые усовершенствования, появившиеся в этом выпуске.

- **Чередование приложений RemoteApp.** Улучшенное разрешение и чередование выполнения на клиентских машинах, включая изменение настроек разрешения для удаленного сеанса.
- **Установка/удаление монитора на ходу.** Если вы добавляете монитор, то эта функция позволяет перенести в него приложение и выполнить перенастройку, если монитор удаляется.
- **Поддержка приложений ClickOnce.** Пользователи могут теперь устанавливать приложения прямо из браузера, вместо того чтобы просить администратора предоставить и развернуть их, как это было в предыдущих версиях.
- **Полноценные графические приложения RemoteApp.** Это позволяет Windows RT поддерживать приложения, которые используют диспетчер окон рабочего стола (Desktop Window Manager). Кроме того, теперь вы получаете всплывающие уведомления с эффектом постепенного исчезновения.

Учтите, что для обеспечения поддержки программ RemoteApp требуется определенное конфигурирование. Однако после того как вы сконфигурируете все необходимые элементы, пользователи смогут обращаться к программам RemoteApp с помощью перечисленных ниже методов.

- **Посредством веб-браузера.** Если у вас сконфигурирован сервер RD Web Access, то для запуска приложения пользователи могут зайти на веб-страницу и щелкнуть на ссылке.
- **С помощью файла Remote Desktop Protocol.** Чтобы запустить приложение RemoteApp, пользователь может просто дважды щелкнуть на сконфигурированном надлежащим образом файле `.rdp`.
- **Посредством меню Start (Пуск) или значка программы.** Приложения RemoteApp можно установить с применением традиционных пакетов Windows Installer (`.msi`), которые также называют пакетами Microsoft Installer. После их установки пользователи смогут запускать приложения точно так же, как любое другое установленное приложение. Кроме того, они могут воспользоваться новым методом развертывания ClickOnce.

Вы узнаете, как устанавливать все компоненты и развертывать приложения RemoteApp для каждого из этих методов, в разделе "Добавление служб Remote Desktop Services" далее в этой главе.

Модель обработки в службах Remote Desktop Services

Под *сетью тонких клиентов* или *вычислениями на базе сервера* (что представляет собой одно и то же, но с разными акцентами) подразумевается любая вычислительная среда, в которой бо́льшая часть обработки приложений происходит не на клиенте, а на сервере, открытом для многопользовательского доступа. Эти термины ссылаются на сеть по определению, поэтому не включают автономные малые вычислительные устройства, подобные смартфонам и планшетным компьютерам, хотя к некоторым из них можно добавить поддержку тонких клиентов.

"Тонкими" сети тонких клиентов и вычисления делает не размер операционной системы и не сложность приложений, запускаемых на клиенте, а то, как эта обработка распределяется. В сети тонких клиентов большая часть, а то и вся обработка происходит на сервере. Инструкции для создания видео-вывода перемещаются из сервера на клиент, щелчки кнопками мыши и нажатия клавиш передаются из клиента на сервер, а весь видео-вывод визуализируется на клиенте.

Последователь мейнфрейма?

Вы могли встречаться с описанием сети тонких клиентов как "возврата к пагадигме мейнфреймов". (Нам приходилось слышать это и в менее вежливой форме: "Вы заново изобрели мейнфрейм, глупцы!") Такое сравнение является частично уместным, а частично — обманчивым. Действительно, приложения хранятся и выполняются на центральном сервере, а на клиенте только отображается вывод.

Планшет и тонкие клиенты

В наши дни наблюдается резкий рост популярности планшетов, и вас наверняка интересует, почему мы упоминаем о них здесь. На тот случай, если вы только что прибыли с необитаемого острова: планшет — это небольшой (с экраном от 7 до 10 дюймов) переносной компьютер, предназначенный главным образом для коммуникаций через Интернет, но также привлекаемый для достижения самых разных целей в повседневной жизни. Обычно планшеты имеют больше ресурсов, чем тонкий клиент, однако значительно меньше, чем полнофункциональный настольный компьютер. В силу своего размера они чрезвычайно мобильны. Планшеты обладают меньшей вычислительной мощностью, меньшим объемом ОЗУ и упрощенной графикой (правда, с беспрецедентной скоростью догоняют по этим характеристикам настольные ПК), что позволяет снизить энергопотребление и продлить срок службы аккумулятора.

Такие устройства вполне допустимо использовать как часть решения Remote Desktop. Их можно подключать к серверу Remote Desktop либо напрямую через Интернет с применением RD Gateway, либо посредством VPN. Приложения или рабочие столы могут выполняться на сервере Remote Desktop, чтобы не перегружать аппаратные ресурсы устройства.

Тем не менее, приложения, выполняемые в среде тонких клиентов, отличаются от приложений, запускаемых в среде мейнфрейма; мейнфреймы не поддерживают пакеты для текстовой обработки или демонстрации слайдов, а требования к видео на графическом клиенте Windows, безусловно, выше, чем они были при использо-

вании текстового терминала. Однако степень контроля, предлагаемая сетью тонких клиентов, примерно такая же, как у мейнфрейма. Мы слышали, как один человек называл сеть тонких клиентов и управление, которое она обеспечила для его пользователей, "возвратом к золотым временам мейнфреймов".

В чем причина перехода от централизованных вычислений к персональным компьютерам и обратно? Бизнес-приложения стимулировали развитие ПК — новые приложения просто не могли работать в среде мейнфрейма. Разумеется, не все мейнфреймы были отправлены на свалку, но проектные решения более новых приложений слишком интенсивно использовали оборудование, чтобы хорошо работать в разделяемой вычислительной среде. Тем не менее, эти приложения возвратились к централизованной модели вычислений, когда стало ясно, что модель с мейнфреймом может предложить функции, отсутствующие у локальной сети на основе ПК:

- группирование вычислительных ресурсов, чтобы ни один из них не простаивал впустую;
- централизованное распространение и обслуживание приложений;
- отсутствие необходимости для клиентов запускать у себя самую современную операционную систему и располагать новейшим оборудованием, которое ее поддерживает;
- отсутствие необходимости для клиентских машин в установке источников бесперебойного питания, поскольку они не выполняют ни одного приложения локально.

В общем, "изобретение заново мейнфрейма" имеет свои преимущества. Точно так же, как ПК не заменили собой мейнфреймы, серверные вычисления не являются заменой ПК. Тем не менее, неплохо располагать возможностью применения серверных вычислений, когда это более разумно, чем установка приложений на настольном компьютере.

Структура сеанса тонкого клиента

Сетевой сеанс тонкого клиента состоит из трех частей.

- **Сервер RDS.** Выполняет многопользовательскую операционную систему.
- **Remote Desktop.** Многоканальный протокол, который позволяет передавать по отдельным каналам разнообразную информацию (включая презентационные данные, управляющую информацию, лицензионную информацию и т.д.).
- **Клиент.** Может выполнять любую операционную систему, которая поддерживает этот терминальный клиент.

Все они подробно обсуждаются в последующих разделах.

Сервер RDS

Службы Remote Desktop Services являются одним из необязательных компонентов, которые можно устанавливать в Windows Server 2012 R2. Если вы добавили роль Remote Desktop Services, то сразу после начальной загрузки сервера и загрузки ядра операционной системы службы RDS приступают к прослушиванию TCP-порта 3389 на предмет поступления от клиентов входящих запросов на подключение. Не забудьте сконфигурировать брандмауэр, разрешив этот порт.

Понятие сеансов

Когда клиент запрашивает подключение к серверу и сервер принимает этот запрос, уникальное представление клиента о сервере RDS называется его *сеансом*. В дополнение к удаленным сеансам создается специальный клиентский сеанс для консоли.

Службы RDS не могут функционировать на настольных ПК

Некоторые интересуются, есть ли возможность превратить компьютер с Windows XP, Windows Vista, Windows 7 или Windows 8 в многопользовательский сервер (или нечто подобное). Ответ отрицательный — ни одна настольная операционная система Microsoft не включает в себя полноценные службы Remote Desktop Services, и способа их добавления не существует. В состав Windows XP, Windows Vista, Windows 7 и Windows 8 входит средство Remote Desktop, которое позволяет подключаться к компьютеру через протокол отображения RDP. Тем не менее, в каждый момент времени поддерживается только одно соединение. Средство Remote Desktop Services, обсуждаемое в этой главе, является возможностью исключительно серверного класса.

Все сеансы имеют уникальные идентификаторы сеанса, который сервер использует для различения процессов, выполняющихся внутри разных сеансов RDS на том же самом компьютере. В этом контексте процессы примерно эквивалентны исполняемым файлам. Когда клиент подключается к серверу RDS, для сеанса создается идентификатор сеанса.

На рис. 29.1 показано окно консоли Remote Desktop Services в диспетчере серверов, в котором выполняется мониторинг сеансов, выполняющихся на сервере RDS.

Внутри каждого сеанса рабочего стола выполняется несколько базовых процессов, которые поддерживают пользователя. Наличие дополнительных процессов в сеансе будет зависеть от приложений, запускаемых пользователем.

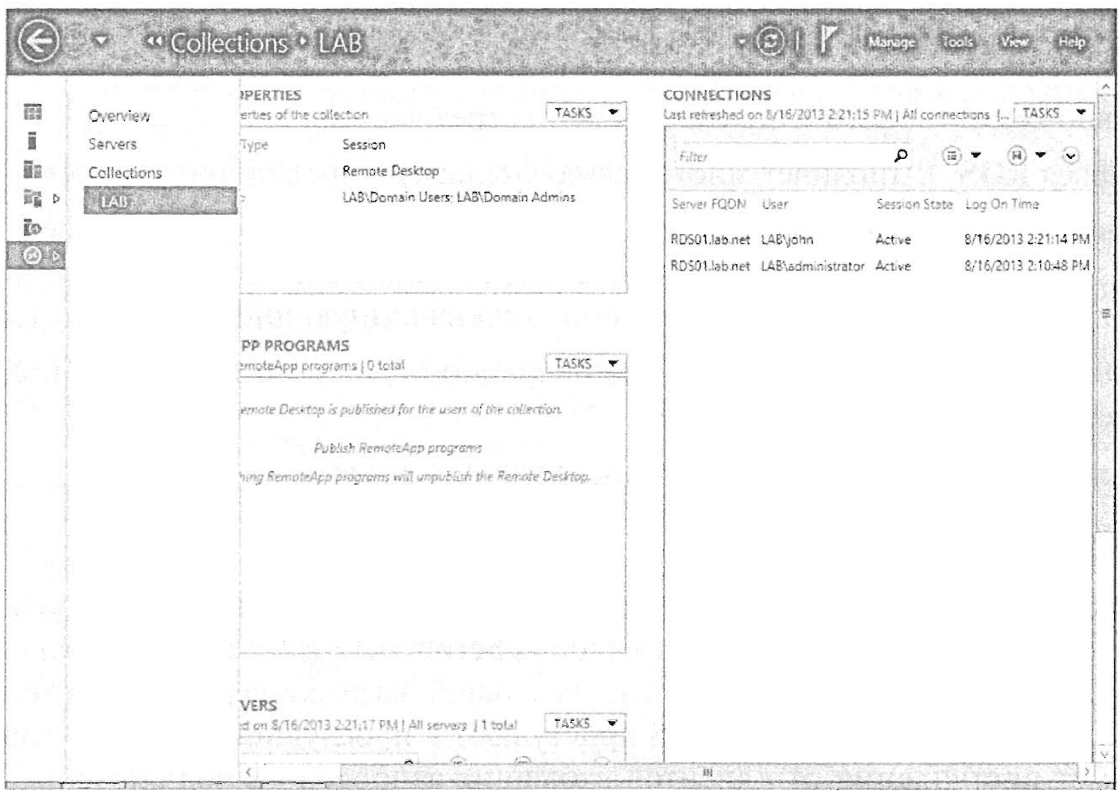


Рис. 29.1. Консоль Remote Desktop Services

Исполняемые файлы, образы и потоки

В операционных системах Windows исполняемый файл внутренне известен как *образ*. Причина в том, что формально приложение является не фрагментом кода, получающим рабочие циклы процессора, а коллекцией команд, называемых *потоками*, которые тратят процессорное время на выполнение необходимых задач. Потоки имеют среду, называемую *процессом*, который сообщает потокам, где сохранять и откуда извлекать их данные. Часть процесса, которая что-то делает, собирательно называется *образом* или *исполняемым файлом*. Ради согласованности программы, выполняющиеся на сервере RDS, мы будет называть *процессами*.

Сеанс не позволяет своим внутренним процессам разрушать или видеть данные друг друга. Однако хотя сеансам разрешено игнорировать друг друга, они по-прежнему должны сосуществовать. Все сеансы работают с одними и теми же ресурсами — процессорным временем, памятью и функциями операционной системы, — поэтому операционной системе приходится разделять использование таких ресурсов между всеми сеансами. Для этого сервер RDS опознает процессы, инициированные в каждом сеансе, не только по идентификаторам процесса, но и по идентификаторам сеанса.

Каждый сеанс имеет высокоприоритетный поток, зарезервированный для ввода с клавиатуры и мыши и для отображения вывода, но обычные приложения выполняются с приоритетом, которым бы они располагали в однопользовательской среде. Поскольку все потоки сеанса обладают одним и тем же приоритетом, планировщик обрабатывает пользовательский ввод циклическим образом, с предоставлением потоку ввода каждого сеанса определенной порции времени для обработки данных, прежде чем управление процессора будет передано другому потоку. Если сеансы очень активны, возникает гораздо более высокая конкуренция за процессорное время.

Количество сеансов, которые может поддерживать сервер RDS, зависит от того, сколько сеансов способно поддерживать оборудование (в основном это касается памяти, но также учитывается процессорное время, полоса пропускания сети и доступ к дискам) и сколько доступно лицензий. Когда клиент выходит из своего сеанса, виртуальные каналы к этой клиентской машине закрываются, а ресурсы, выделенные данному сеансу, освобождаются.

"За кулисами" протокола удаленного рабочего стола

Вы можете запустить все желаемые сеансы на сервере RDS, но от этого будет мало толку, если вы не сможете просматривать вывод сеанса на удаленном компьютере и выгружать свой ввод на терминальный сервер для его обработки. Механизмом, который позволяет решать обе задачи (а также делать многое другое), является *протокол удаленного рабочего стола* (Remote Desktop Protocol).

Особенности работы протокола удаленного рабочего стола

Протокол Remote Desktop Protocol (RDP) загружает инструкции для визуализации графических изображений из сервера RDS на клиент и выгружает ввод с клавиатуры и мыши из клиента на сервер. Службы Remote Desktop Services изначально поддерживают протокол Remote Desktop Protocol. Протокол RDP обеспечивает зависимое от TCP/IP двухточечное соединение, которое отображает либо рабочий стол, либо одиночное приложение на рабочем столе клиента, выполняющего RDP.

Требования к вычислительной мощности клиента снижаются за счет применения средства, которое называется *кешированием на стороне клиента* и позволяет "запоминать" изображения, уже загруженные в ходе сеанса. При использовании кеширования во время каждого обновления на клиент загружаются только измененные части экрана. Например, если значок Microsoft Word уже был загружен, то при обновлении изображения рабочего стола нет необходимости загружать этот значок еще раз. Кеш на жестком диске хранит данные в течение ограниченного периода и со временем отбрасывает данные с применением алгоритма удаления наиболее давно использовавшихся элементов (least recently used — LRU). Когда кеш становится полным, он отбрасывает данные, к которым дольше других не было обращения, в пользу размещения новых данных.

Как упоминалось ранее, за годы своего существования протокол RDP претерпел немало изменений. Полное понимание Remote Desktop Protocol даст следующая статья:

```
http://support.microsoft.com/kb/186607
```

Периодичность автоматического обновления

Когда сеанс активен, изображение на экране обновляется через очень короткие интервалы. Если пользователь, открывший этот сеанс, перестает отправлять серверу щелчки кнопками мыши и нажатия клавиш, то сервер RDS отмечает это отсутствие активности и снижает частоту обновления до тех пор, пока активность снова не восстановится.

Обратите внимание, что в дополнение к каждому клиентскому сеансу имеется также сеанс, используемый сервером. Все локально запущенные службы и исполняемые файлы действуют в контексте этого серверного сеанса.

Версии протокола RDP

Протокол RDP существует со времен NT 4.0 (первой его версией была RDP 4.0) и с тех пор претерпел множество модернизаций. Текущей версией, доступной в Windows Server 2012 R2, является 8.1.

Хотя в протокол было внесено много постепенных изменений, в его версии Windows Server 2012 и Windows Server 2012 R2 основное внимание сосредоточено на оптимизации работы с WAN, обеспечении более легкого администрирования всех компонентов, сокращении затрат на хранилище и сеть с применением онлайновой дедупликации данных (Data Deduplication — Dedup) и полной поддержке пространств хранения данных и многоуровневых хранилищ. Как видите, протокол RDP прошел долгий путь развития с момента своего появления в NT 4.0.

Клиент

Усовершенствования клиента соответствуют тому, о чем шла речь при обсуждении Remote Desktop Protocol. Вы должны удостовериться, что клиент поддерживает самую последнюю версию RDP, поддерживаемую сервером RDS. В противном случае вы не сможете воспользоваться всеми замечательными возможностями и преимуществами последних версий протокола.

Требования к серверу и клиентам

Модель вычислений для сети тонких клиентов означает, что практически вся вычислительная мощность сконцентрирована на серверной, а не на клиентской стороне. Так как сервер будет поддерживать десятки или, возможно, сотни пользователей, это не тот случай, когда следует экономить на мощности.

Оборудование сервера

Предложение использовать более мощный сервер, чтобы можно было сэкономить на оборудовании клиентской стороны, далеко не ново. Именно в этом заключается сущность файлового сервера, как компьютера, снабженного быстродействующим жестким диском большой емкости, который позволяет избежать приобретения таких дисков для каждого пользователя в офисе. Серверы RDS построены по аналогичному принципу: если большая часть обработки сосредоточена в одном месте, здесь можно сосредоточить аппаратные ресурсы, необходимые для поддержки такой обработки, не особо беспокоясь о вычислительной мощности на клиентской стороне.

Использование мощного сервера RD Session Host

Поскольку сервер RD Session Host будет обслуживать приложения или полноценные рабочие столы клиентов, вам понадобится приобрести или собрать мощный сервер. (Хотя согласно передовому опыту лучше иметь множество менее мощных хостов, чтобы можно было распределять нагрузку.) Наиболее важными ресурсами являются вычислительная мощность и ОЗУ. В зависимости от типов и количества поддерживаемых сеансов полезно также рассмотреть возможность ускорения доступа к дискам и полосы пропускания сети. На первый взгляд, определение потребностей в ресурсах представляется довольно простым. Достаточно выполнить следующие действия.

1. Подсчитайте ресурсы, необходимые для операционной системы.
2. Подсчитайте ресурсы, нужные для небольшого количества сеансов (скажем, 5).
3. Получите объем ресурсов, необходимых для всех сеансов, на основе общего количества сеансов, которые планируется поддерживать.

   Например, если вы намерены поддерживать 100 сеансов, и оценили объем ресурсов, необходимый для поддержания 5 сеансов, то этот объем понадобится умножить на 20, чтобы получить показатели для 100 сеансов (20 5 = 100). Таким образом, если для поддержки 5 сеансов нужно 4 Гбайт ОЗУ, то для поддержки 100 сеансов требуется 4 Гбайт × 20 = 80 Гбайт ОЗУ. Множитель 20 получается делением суммарного количества необходимых сеансов (100) на количество сеансов, для которых проводилась оценка объема ресурсов (5).
4. Просуммируйте объем ресурсов, необходимых для общего числа сеансов, и объем ресурсов, необходимых для операционной системы.

Хотя подсчет выглядит совершенно простым, вряд ли вы будете поступать подобным образом. Совместное действие нескольких факторов часто трудно предсказать. Вдобавок совместное действие нескольких факторов (когда целое больше суммы его частей) часто приводит к несколько неожиданным результатам. Кроме того, если развертывание прошло успешно и пользователи довольны тем, что они могут делать, то в конечном итоге они смогут извлечь из среды гораздо больше, чем вы ожидали.

Лучше заранее предусмотреть запас на случай неожиданностей и запланировать расширение, но только не рассказывайте об этом ответственным за смету. Некоторые поставщики публикуют “эталонные архитектуры” для своих аппаратных платформ, которые также помогут принять правильное решение по ресурсам для платформы.

Основные аппаратные ресурсы

Чтобы обеспечить эффективное функционирование сервера RD Session Host, абсолютного минимума, требуемого для запуска Windows Server 2012 R2, будет недостаточно. Несмотря на отсутствие четких спецификаций для сервера RDS, ниже приведены рекомендации общего характера по выбору технических характеристик сервера.

- **Процессор.** Правило о том, что чем выше быстродействие, тем лучше, соблюдается лишь до определенной степени. Достаточно большой объем кеша процессора важнее его высокой скорости, т.к. ему не придется часто обращаться к (медленной) системной памяти за кодом и данными. Находясь перед необходимостью выбора между большим объемом кеша и высоким быстродействием, отдавайте предпочтение кешу. В наши дни большинство серверов RDS являются многопроцессорными, и эти процессоры имеют по нескольку ядер. Хотя в действительности только многопоточные приложения способны использовать одновременно более одного процессора, при наличии нескольких процессоров потоки, требующие выполнения, могут выстраиваться в очередь к ним.

- **Память.** Как правило, ограничения серверов RDS связаны с памятью, а не процессорами. Применяйте высокоскоростную память с коррекцией ошибок, устанавливайте ее как можно больше и будьте готовы к ее наращиванию по мере увеличения количества пользователей и приложений на сервере RDS. Однако иногда лучше добавить еще один компьютер, чтобы снизить нагрузку, т.к. наращивать память можно лишь до определенного предела, после чего это начинает негативно сказываться на работе системы. Объем необходимой памяти зависит от используемых приложений, количества параллельных сеансов и потребности в памяти со стороны файлов, открытых в этих сеансах: программы автоматизированного проектирования будут подвергать систему более высокой нагрузке, чем, скажем, приложение Notepad. К счастью, 64-разрядная операционная система не ограничена пределом памяти в 4 Гбайт. Начинайте свои подсчеты объема памяти для сервера минимум с 8 Гбайт и увеличивайте этот объем на основе количества пользователей и памяти, требуемой приложениям, которые будут выполняться на сервере. ОС Windows Server 2012 R2 способна поддерживать до 4 Тбайт ОЗУ.

- **Диск.** По возможности применяйте на сервере RDS диски SCSI (Small Computer System Interface — интерфейс малых вычислительных систем). Контроллер дисков SCSI может работать в многозадачном режиме для всех устройств в цепочке SCSI. Большинство пользователей уверено, что диски SCSI работают гораздо быстрее, чем SATA (Serial Advanced Technology Attachment — последовательный интерфейс для подключения внешних устройств) и EIDE (Enhanced Integrated Drive Electronics — расширенный параллельный интерфейс подключения накопителей), хотя некоторые обнаруживают, что высокопроизводительные решения SATA работают лучше низкопроизводительных решений SCSI. Производительность диска является важной характеристикой на любом сервере, но особенно — на сервере RDS.

Кроме того, рассмотрите возможность использования решения RAID (Redundant Array of Inexpensive Disks — избыточный массив недорогих дисков) с целью повышения производительности и/или отказоустойчивости дисковых устройств. В случае высокопроизводительного сервера RDS решение RAID 1+0 обеспечивает выигрыш как в производительности, так и в избыточности. В случае развертывания в виртуализированной среде обдумайте также применение многоуровневого хранилища. Когда возможно, используйте для операционной системы высокопроизводительный диск SSD и файл VHDX фиксированного размера.

- **Сеть.** На загруженном сервере RDS рассмотрите возможность объединения высокоскоростных сетевых интерфейсных плат (NIC Teaming), что позволит назначать нескольким таким платам один и тот же IP-адрес и в результате распределять сетевой трафик. Альтернативным вариантом может быть многоадресный сервер с одной сетевой интерфейсной платой, выделенной для трафика сеансов RDS. С точки зрения скорости сети пересылка туда и обратно вывода приложения и ввода клиентской стороны требует небольшой полосы пропускания, но клиентские печатные задания, отправляемые на отображенные принтеры, могут занимать довольно значительную часть полосы пропускания. Отображаемые диски также могут увеличивать нагрузку, делая возможным копирование файлов туда и обратно через подключение RDP.

Использование монитора производительности

Монитор производительности (Performance Monitor) помогает получить сведения о том, какую нагрузку сеансы RDS оказывают на сервер. Нагрузка на сервер должна масштабироваться в близкой зависимости от количества людей, использующих сервер. Таким образом, выбрав репрезентативную группу примерно из пяти человек, потребности можно было бы экстраполировать на группы пользователей бо́льших размеров. Ключевые объекты и счетчики, применяемые для измерения общей нагрузки на сервер, можно найти в рамках бесплатного инструмента, который называется Performance Analysis of Logs (Анализ производительности по журналам) и доступен по ссылке `http://pal.codeplex.com`; они помогут определить характеристики серверов RDS. Но пара объектов монитора производительности заслуживает более пристального внимания, т.к. с их помощью можно получить детальную информацию о сервере RDS.

Объекты монитора производительности по-прежнему называются Terminal Services

Несмотря на то что со времени появления Windows Server 2012 R2 название Terminal Services было изменено на Remote Desktop Services, объекты в мониторе производительности по-прежнему содержат Terminal Services в своих именах. Хоть это может выглядеть опечаткой, но эти два объекта действительно называются Terminal Services и Terminal Services Session.

Объект Terminal Services имеет счетчики, представляющие количество активных сеансов (сеансов, в которых пользователь подключился к серверу RD Session Host и успешно вошел в систему), неактивных сеансов (сеансов, в которых пользователь все еще остается в системе сервера RDS, но перестал пользоваться сеансом) и общее количество сеансов.

Помимо простого мониторинга активности, указанные счетчики можно применять для выдачи оповещений, когда количество активных сеансов достигнет определенного порога. Допустим, вы хотите знать, когда сервер будет размещать более 100 сеансов. Это можно сделать с помощью группы сборщиков данных.

В мониторе производительности можно настроить простую группу сборщиков данных с оповещением. Для этого нужно создать вручную (не с помощью шаблона) группу сборщиков данных, определенную пользователем, выбрать в качестве типа Performance Counter Alert (Оповещение счетчика производительности) и задать пороговое значение для количества активных сеансов. Затем для этого оповещения можно определить задачу, которая будет уведомлять вас с помощью базового сценария или фиксировать событие в журнальном файле.

Хотя вы можете получить некоторую информацию уровня сеанса в диспетчере Remote Desktop Services, объект монитора производительности под названием Terminal Services Session предоставляет намного больше данных. Воспользуйтесь диспетчером Remote Desktop Services для нахождения сеанса, который вы хотите отслеживать (сеансы идентифицируются в мониторе производительности по своим номерам, а не по входным именам пользователей), а затем добавьте счетчики для мониторинга этого сеанса.

Каждый объект сеанса имеет счетчики процессора и памяти, которые выглядят вполне знакомо для каждого, кому приходилось работать с монитором производительности, но также и счетчики, специфичные для сеанса, вроде перечисленных в табл. 29.1. Здесь описаны не все счетчики, а только те, которые отражают информацию, полезную при вычислении нагрузки на сервер и анализе текущей производительности сеансов.

Не торопитесь с настройкой сервера лицензий

При проведении экспериментов с сеансами Remote Desktop для выяснения, какое количество пользователей удастся поддерживать в каждом сеансе, не настраивайте сервер лицензий; для этой цели позвольте серверу RDS выпустить свои временные 120-дневные лицензии. Хотя это может звучать несколько неожиданно, применение временных лицензий предотвращает непреднамеренное назначение лицензий устройств тестовому оборудованию. В разделе "Режим лицензирования" далее в главе подробно объясняется работа лицензирования и выделения лицензий.

Клиентское оборудование

При подключении к серверу RD Session Host посредством собственного клиента RDP чаще всего вы будете использовать ПК с загруженной операционной системой Windows, т.е. терминал Windows.

Таблица 29.1. Ключевые счетчики производительности объекта Terminal Services Session

Счетчик	Описание	См. также
% Processor Time (Процент процессорного времени)	Процент времени, в течение которого все потоки в сеансе использовали процессор для выполнения инструкций. На многопроцессорных машинах максимальное значение этого счетчика равно произведению 100% на количество процессоров	–
Total Bytes (Общее количество байтов)	Общее количество байтов, отправленных в и из этого сеанса, включая все накладные расходы протокола	Input Bytes (Входных байтов), Output Bytes (Выходных байтов)
Total Compressed Bytes (Общее количество сжатых байтов)	Общее количество байтов после сжатия. Отношение Total Compressed Bytes к Total Bytes представляет собой коэффициент сжатия	Total Compression Ratio (Общий коэффициент сжатия)
Total Protocol Cache Hit Ratio (Общий коэффициент попаданий в кеш протокола)	Общее количество попаданий во все кеши протокола, содержащие объекты Windows с высокой вероятностью повторного использования. Попадания в кеш представляют объекты, которые не нуждаются в повторной пересылке, поэтому более высокий коэффициент попаданий означает более интенсивное повторное использование кеша и, возможно, меньшее время ожидания ответа от сеанса	Protocol Save Screen Bitmap Cache Hit Ratio (Коэффициент попаданий в кеш растровых изображений хранителя экрана протокола), Protocol Glyph Cache Hit Ratio (Коэффициент попаданий в кеш глифов протокола), Protocol Brush Cache Hit Ratio (Коэффициент попаданий в кеш кистей протокола)
Working Set (Рабочий набор)	Текущее количество байтов в рабочем наборе этого сеанса	Virtual Bytes (Виртуальных байтов), Page Faults/Sec (Страничных отказов в секунду)

Собственный клиент RDP

В этом контексте под собственным клиентом RDP понимается клиент, доступный от Microsoft, что подразумевает Windows. Хотя компания Microsoft не поддерживает другие платформы (за исключением своего клиента OS X Macintosh, который можно загрузить на странице `http://www.microsoft.com/mac/downloads`), по адресу `www.hobsoft.com/products/connect/jwt.jsp` у компании Hobsoft можно приобрести межплатформенный (Windows, Mac, Linux, DOS) клиент Java; кроме того, есть бесплатный клиент RDP для Linux, доступный для загрузки на сайте `www.rdesktop.org`.

Терминалы Windows

В самом узком определении *терминал Windows* — это зависимое от сети устройство, работающее под управлением ОС Windows CE, которая поддерживает один или более протоколов отображения, таких как RDP или ICA (Independent Computing Architecture — независимая вычислительная архитектура), представляющий собой протокол отображения для подключения к серверам Presentation Server. Многие терминалы Windows также поддерживают некоторую форму эмуляции терминала.

В этом разделе мы будем представлять терминал Windows как любое терминальное устройство, спроектированное для подключения к серверу Windows RD Session

Host; он может функционировать под управлением любой ОС, в которой имеется клиент RDP. Таким устройством является терминал на основе Windows (Windows-based terminal — WBT), который локально выполняет ОС Windows и соответствует системным требованиям Microsoft в отношении терминалов WBT.

Главной определяющей характеристикой терминала Windows является его тонкий аппаратный профиль: поскольку основная работа большинства терминалов Windows связана с функционированием протокола отображения, им не требуется большой объем памяти или вычислительная мощность, и они не пользуются внешней памятью. Терминал Windows включает процессор, оперативную память небольшого объема, сетевую плату и поддержку видео, а также устройства ввода, такие как клавиатура (или эквивалент) и мышь (или эквивалент). Обычно терминалы не снабжаются жесткими дисками, приводами CD-ROM или проигрывателями DVD. Операционная система хранится в локальной памяти. Помимо указанных похожих черт физически терминалы Windows варьируются от "тостерного" форм-фактора до панели или небольшого блока, который можно подключать с тыльной стороны монитора — либо даже быть частью самого монитора. Некоторые модели терминалов Windows являются беспроводными планшетными компьютерами, предназначенными для таких пользователей, как врачи и медсестры, которые обычно используют для хранения информации папки с зажимом для бумаги и скоросшиватели.

Несмотря на то что большинство терминалов Windows всецело зависят от своего сервера RDS, небольшая их часть может выполнять приложения локально. У них по-прежнему отсутствуют жесткие диски; подобно операционной системе, приложения хранятся в ПЗУ. Типы доступных приложений зависят от операционной системы терминала, поскольку локально хранящиеся приложения должны выполняться локально, а не просто отображать свои результаты. Тем не менее, в плане приложений терминалы Windows чаще всего зависят от своего сервера RDS.

Терминалы Windows наиболее популярны в средах, где люди используют единственное приложение, где обеспечение поддержки ПК было бы затруднительно или где применение ПК не очень хорошо подходит. Однако ПК по-прежнему превосходят по численности терминалы Windows в качестве тонких клиентов. Частично это объясняется тем, что многие среды не могут всецело полагаться на серверные вычисления. Компании уже располагают ПК, и если только они не проводят полное обновление своего парка настольных систем, то изъятие из работы мощного ПК с целью его замены менее мощным терминалом Windows в действительности имеет мало смысла.

Клиенты в виде ПК

В настоящее время люди применяют ПК в качестве клиентских машин сервера RDS более чем в два раза чаще терминалов Windows. В этом нет ничего удивительного.

- Во-первых, если только все не начинается с нуля, люди уже имеют ПК. Хотя терминалы WBT несколько дешевле низкопроизводительных ПК, все равно их приобретение приводит к дополнительным расходам.
- Во-вторых, не все приложения работают удовлетворительно в среде сервера RDS. Зачастую одни приложения лучше выполнять на сервере RDS, а другие — локально.

Если вы не приобретаете новое оборудование и предвидите необходимость в будущем выполнять какие-то приложения локально, то, скорее всего, должны использовать ПК хотя бы для некоторых терминальных клиентов.

Чтобы работать со службами Remote Desktop Services, на ПК должна функционировать операционная система Windows, в них должен быть установлен протокол отображения RDP и они должны иметь действующее сетевое подключение, которое использует TCP/IP и допустимый IP-адрес.

Планшетные компьютеры

Учитывая удобство пользования планшетными компьютерами, неудивительно, что они настолько популярны в наши дни. Они являются прекрасной заменой для ноутбуков благодаря своей дешевизне, небольшому весу и малому энергопотреблению, так что те, кому приходится совершать дальние перелеты, могут работать с ними в течение всего перелета, а не только пару часов после взлета. (К тому же вы можете пользоваться планшетным компьютером в самолете, не опасаясь, что человек, сидящий перед вами, внезапно откинет спинку своего кресла и сломает дисплей ноутбука.) Обычно планшетные компьютеры функционируют под управлением Windows, Android или Apple IOS. Для подключения к серверу RDS можно применять проводные или беспроводные соединения с VPN или без.

Внешний вид планшетного компьютера зависит от производителя. Некоторые планшеты выглядят как "младшие братья" ноутбуков, к примеру, Microsoft Surface. Другие складываются в виде папки либо имеют вид плоской плитки. Некоторые планшеты настолько малы, что работать с ними не особенно удобно. У одних планшетов — именно им мы отдаем предпочтение — имеется клавиатура, тогда как другие снабжены только перьями для ввода. Со всего этого можно сделать вывод, что планшетный компьютер не в состоянии заменить настольный ПК, хотя встречаются исключения наподобие Microsoft Surface Pro, который представляет собой планшет с клавиатурой и обладает вычислительной мощностью, сопоставимой с настольным ПК. Планшетный компьютер обычно используется в сочетании с основной машиной, выступая в качестве ее партнера благодаря применению, например, OneNote или SkyDrive.

Добавление служб Remote Desktop Services

Роль Remote Desktop Services можно добавить к любому серверу Windows Server 2012 R2, присоединенному к домену, с помощью диспетчера серверов. В диспетчере серверов есть мастера, которые позволяют добавлять многие роли, и, скорее всего, вам уже приходилось пользоваться этим диспетчером.

При добавлении роли RDS мастер добавления ролей и компонентов (Add Roles and Features Wizard) сначала предлагает меню, показанное на рис. 29.2. После этого он задает дополнительные вопросы, относящиеся непосредственно к роли RDS.

В последующих разделах приведена информация, которая вам понадобится для ответа на эти вопросы и успешного добавления роли RDS. Ниже перечислены темы, касающиеся установки сервера RD Session Host:

- дополнительные службы роли;
- аутентификация на уровне сети;

- режим лицензирования;
- членство в группе `Local Remote Desktop Users`;
- добавление приложений.

После установки этой роли понадобится сконфигурировать сервер. В этом разделе приведено подробное описание процесса принятия решений, а также действия по добавлению и конфигурированию сервера.

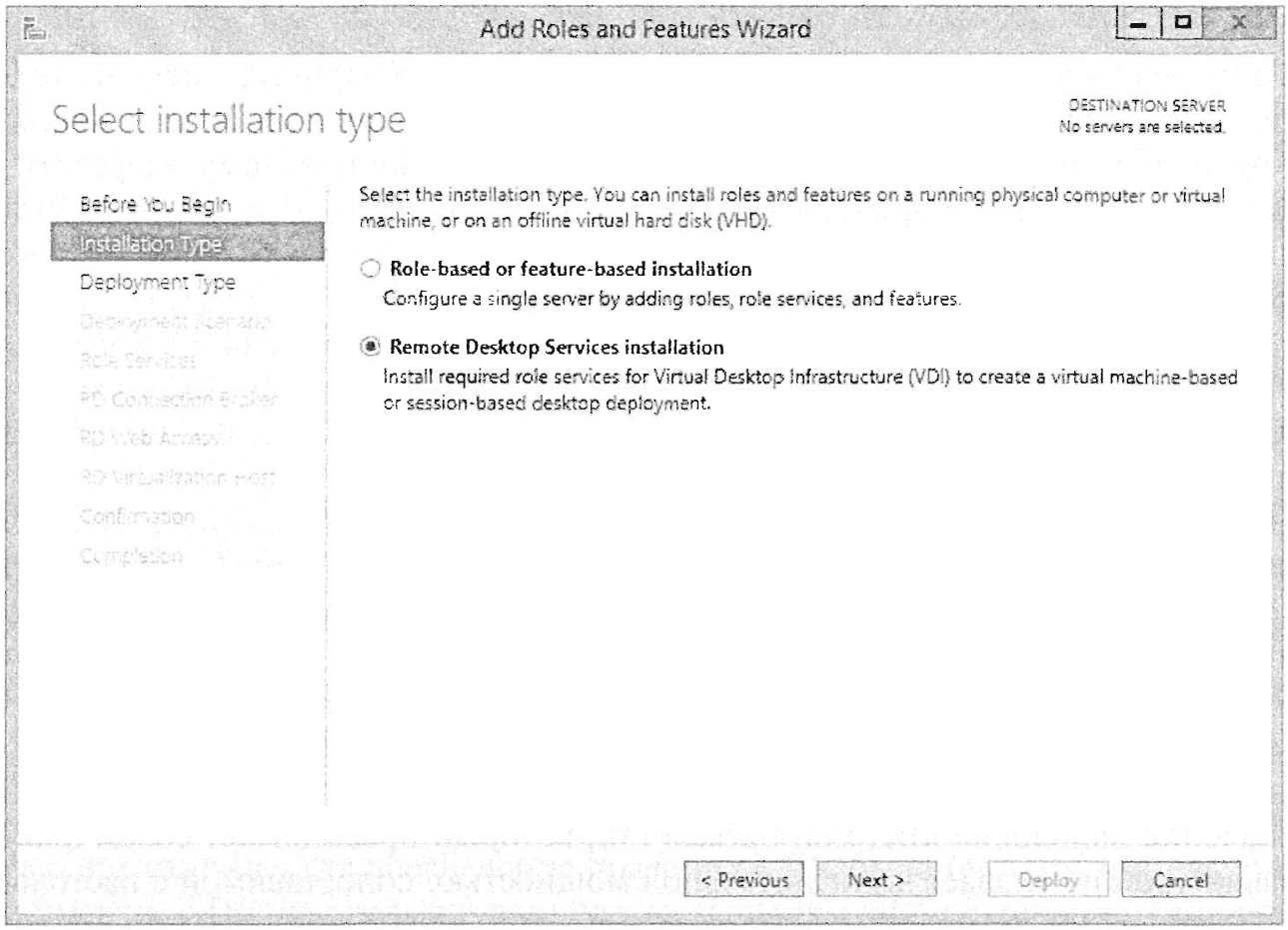


Рис. 29.2. Мастер Add Roles and Features Wizard

Службы Remote Desktop Services не требуются для подключения администраторов

Для подключения к серверу администраторов службы Remote Desktop Services не нужны. В главе 17 рассказывалось о дистанционном подключении к серверу с помощью Remote Desktop Connection (RDC) или Remote Desktops. Чтобы можно было пользоваться этими инструментами, устанавливать службы Remote Desktop Services необязательно. Вместо этого понадобится разрешить подключения к удаленному рабочему столу на сервере.

Существенная разница между дистанционным подключением с целью администрирования и применением сервера RD Session Host заключается в том, что для подключения администраторов лицензии не требуются. Любой сервер может поддерживать два удаленных подключения администраторов без лицензии. Тем не менее, для подключения к серверу RD Session Host лицензии обязательны и они выдаются по принципу “один к одному”. Другими словами, для каждого подключения необходима лицензия.

Обязательные службы роли

Серверная роль Remote Desktop Services включает несколько служб роли. Далеко не все эти службы требуются при каждой установке. Чтобы определить, какие службы добавлять, вы должны оценить, какие задачи собираетесь решать.

- **Remote Desktop Session Host (Хост сеансов удаленного рабочего стола).** Служба RD Session Host позволяет серверу размещать Windows-программы или полный рабочий стол Windows. Она является обязательной для роли Remote Desktop Services.
- **Remote Desktop Virtualization Host (Хост виртуализации удаленного рабочего стола).** Служба RD Virtualization Host интегрирована с Hyper-V, чтобы предоставить пользователям возможность подключения к виртуальной машине на сервере, размещающем Hyper-V. Ее можно сконфигурировать так, чтобы пользователи подключались к собственным уникальным виртуальным машинам, и позволяет им запускать одновременно несколько операционных систем. Этой службе требуется служба роли Hyper-V, и она необходима, если вы используете службу роли Hyper-V.
- **Remote Desktop Licensing (Лицензирование удаленного рабочего стола).** Служба RD Licensing управляет лицензиями клиентского доступа RDS (Client Access Licenses — CAL), которые нужны для подключения к серверу RD Session Host. В течение ограниченного льготного периода (120 дней) службами Remote Desktop Services можно пользоваться без лицензий. Это дает вам время для развертывания, конфигурирования и тестирования сервера.
- **Remote Desktop Connection Broker (Брокер подключений удаленного рабочего стола).** Служба RD Connection Broker применяется для балансирования нагрузки сеансов и повторного подключения к сеансам внутри фермы серверов RD Session Host. Она также обязательна для поддержки приложений RDS RemoteApp, которые позволяют пользователям запускать приложения на сервере RD Session Host через Internet Explorer.

  Если вы используете несколько серверов RD Session Host, то служба RD Connection Broker может перенаправлять подключения на серверы с минимальной загруженностью, предоставляя балансирование нагрузки. Кроме того, если пользователь теряет подключение, то служба RD Connection Broker обеспечивает его повторное подключение с тем же сервером, на котором активен сеанс этого пользователя.
- **Remote Desktop Gateway (Шлюз удаленного рабочего стола).** Служба RD Gateway применяется для того, чтобы предоставить пользователям возможность подключаться к серверам RD Session Host и удаленным рабочим столам через Интернет. Этой службе требуются дополнительные службы роли, включая Web Server (IIS) (Веб-сервер (IIS)), Network Policy and Access Services (Службы сетевых политик и доступа), RPC over HTTP Proxy (Прокси RPC поверх HTTP) и Remote Server Administration Tools (Инструменты дистанционного администрирования сервера).

  Подробное описание службы Remote Desktop Gateway было приведено в главе 17, в том числе добавление обязательных служб и ее включение.

- **Remote Desktop Web Access (Доступ к удаленным рабочим столам посредством веб).** Служба RD Web Access позволяет пользователям получать доступ к RemoteApp и Remote Desktop Connection посредством веб-браузера. Если клиенты работают под управлением Windows 7, то они могут обращаться к RemoteApp и Remote Desktop Connection через меню Start (Пуск) своих систем. Этой службе требуются дополнительные поддерживающие службы роли, в том числе Web Server (IIS) и Remote Server Administration Tools. Аббревиатура IIS означает Internet Information Services (Информационные службы Интернета) производства Microsoft.

Совместимость приложений

Если вы собираетесь применять сервер RD Session Host для размещения приложений, предназначенных конечным пользователям, то должны *сначала* установить RDS и только затем необходимые приложения. Приложения, которые установлены перед добавлением роли RD Session Host, могут не работать корректно в многопользовательской среде.

Хотя некоторые приложения будут функционировать в многопользовательском режиме, даже если они уже были установлены, многие приложения работать откажутся. Если вы уже установили приложения, которые хотите использовать с сервером RD Session Host, то перед добавлением роли Remote Desktop Services должны удалить их.

Технология Easy Print

Начиная с версии Windows Server 2008, стала доступной замечательная возможность под названием Easy Print. Технология Easy Print гарантирует, что клиентские принтеры всегда установлены в удаленных сеансах, не требуя установки их драйверов на терминальном сервере. Со времен Windows Server 2008 R2 никакие изменения в Easy Print не вносились.

На первый взгляд Easy Print не предлагает особых удобств, но в прошлом от вас требовалось установить на терминальном сервере драйверы печати для всех принтеров, используемых клиентами. При наличии 50 клиентов, которые работают с 10 разными устройствами печати, вам понадобилось бы установить на сервере драйверы принтеров для всех 10 устройств печати, даже если они уже были установлены в системах клиентов.

Теперь вас может интересовать, что необходимо сделать для поддержки Easy Print. Вообще говоря, практически ничего. Если на сервере Windows Server 2008 R2 или в более поздней версии установлены службы Remote Desktop Services, то поддержка Easy Print обеспечивается автоматически.

У клиентов должны быть запущены средства RDC 6.1 и Microsoft .NET Framework 3.0 с SP1. Как упоминалось ранее, RDC 6.1 обеспечивает обратную совместимость с Windows XP SP3. Компонент Microsoft .NET Framework 3.0 с SP1 можно загрузить для клиентов XP из сайта загрузок Microsoft по адресу `www.microsoft.com/downloads`. Выполните на нем поиск "Microsoft .NET Framework 3.0 Service Pack 1".

Механизм единого входа

Механизм единого входа (single sign-on — SSO) позволяет пользователям предоставлять свои учетные данные только раз и пользоваться ими на протяжении всего сеанса. При условии, что эти учетные данные имеют подходящие разрешения, у пользователей они повторно не запрашиваются. Без механизма единого входа пользователям пришлось бы указывать одно и то же имя и пароль несколько раз.

Механизм единого входа может быть реализован для пользователей, которые получают доступ к серверу RDS с применением клиентов Windows XP SP3, Windows Vista и Windows 7 либо из серверов Windows Server 2008 или Windows Server 2008 R2.

В свойствах подключения RDP TCP/IP понадобится установить две настройки.

- На вкладке General (Общие) диалогового окна свойств подключения RDP TCP/IP для уровня безопасности должно быть указано либо Negotiate (Согласовывается), либо SSL (TLS 1.0).
- На вкладке Log on (Вход) диалогового окна свойств подключения RDP TCP/IP флажок Always prompt for password (Всегда запрашивать пароль) не должен быть отмечен.

В Windows Server 2008 настройка SSO была довольно сложной. В Windows Server 2012 (и Windows Server 2012 R2) процедура активизации SSO была изначально упрощена. Однако простота включения таит в себе небольшую ловушку: обращающийся клиент должен поддерживать RDP 8.0, инфраструктурой виртуального рабочего стола должна быть ОС Windows 8, а на серверах должна функционировать ОС Windows Server 2012 или выше. Если вам по-прежнему нужна смешанная среда, то конфигурировать SSO придется традиционным способом.

Ниже приведены две ссылки, которые помогут включить механизм SSO:

```
http://blogs.msdn.com/b/rds/archive/2009/08/11/introducing-web-single-sign-on-for-remoteapp-and-desktop-connections.aspx
```

```
http://blogs.msdn.com/b/rds/archive/2012/06/25/remote-desktop-web-access-single-sign-on-now-easier-to-enable-in-windows-server-2012.aspx
```

Аутентификация сетевого уровня

Аутентификация сетевого уровня (Network Level Authentication — NLA) может использоваться в сеансах Remote Desktop для обеспечения повышенной безопасности. При добавлении роли Remote Desktop Services понадобится указать, требуется ли NLA. Решение должно приниматься на основе клиентов, которые будет поддерживать сервер RD Session Host.

Средство NLA гарантирует, что аутентификация выполнится до установления полноценного подключения Remote Desktop. В отсутствие NLA со стороны злоумышленника или вредоносного программного обеспечения существует небольшая возможность для атаки, даже если аутентификация не прошла.

В Windows Vista, Windows 7 и Windows 8 аутентификация сетевого уровня доступна по умолчанию. Она полагается на поставщика поддержки учетных данных безопасности (Credential Security Support Provider — CredSSP). Если все клиенты функционируют под управлением Windows Vista, Windows 7 или Windows 8, вы должны затребовать NLA на сервере RD Session Host.

Поддержка NLA не заложена в Windows XP. Однако если вы модернизируете Windows XP с помощью пакета обновлений SP3 и включите CredSSP, то NLA можно будет использовать. Для применения CredSSP в Windows XP SP3 необходимо модифицировать реестр. Дополнительную информацию по этому вопросу ищите в следующих двух статьях базы знаний Microsoft:

- статья KB 951608, "Description of the Credential Security Support Provider (CredSSP) in Windows XP Service Pack 3" ("Описание поставщика поддержки учетных данных безопасности (CredSSP) в Windows XP Service Pack 3"): `http://support.microsoft.com/kb/951608/`
- статья KB 951616, "Description of the Remote Desktop Connection 6.1 client update for Terminal Services" ("Описание обновления клиента Remote Desktop Connection 6.1 для терминальных служб"): `http://support.microsoft.com/kb/951616/`

Если ваши клиенты старше Windows XP SP3, то они не смогут подключаться с использованием NLA, поэтому аутентификация сетевого уровня включаться не должна.

Режим лицензирования

При конфигурировании служб Remote Desktop Services потребуется выбрать режим лицензирования, который указывает, какой тип лицензий клиентского доступа к Remote Desktop Services (Remote Desktop Services Client Access Licenses — RDS CAL) будет использоваться. На выбор есть три варианта.

- **Configure Later (Конфигурировать позже).** Вы получите льготный период 120 дней, чтобы сконфигурировать лицензирование и выбрать режим лицензирования. Этот вариант обычно выбирают на ранней стадии цикла развертывания, а после устранения всех проблем в среде RD настраивают RDS CAL.
- **Per Device (Индивидуально на устройство).** Индивидуальная лицензия клиентского доступа для устройства выдается клиентскому компьютеру или устройству. Если режим лицензирования установлен в Per Device и сервер лицензирования сконфигурирован, то этот сервер выдаст устройству временную лицензию, когда оно подключится первый раз. При подключении устройства второй раз сервер лицензирования попытается выдать ему постоянную лицензию.

  Сервер лицензирования будет принудительно применять лицензии клиентского доступа для устройств. Другими словами, если для устройства не существует индивидуальной лицензии CAL, а RDS CAL не доступна для выдачи, то подключение будет заблокировано.

  Если для подключения к серверу RD Session Host множество пользователей будут применять одно и то же устройство, вы должны выбрать вариант выдачи индивидуальных лицензий CAL для устройств.
- **Per User (Индивидуально на пользователя).** Индивидуальная лицензия клиентского доступа для пользователя позволяет ему подключаться к серверу RD Session Host из любого количества устройств. Интересно отметить, что сервер лицензирования не отслеживает индивидуальные лицензии CAL для пользователей. С одной стороны, такой подход упрощает ситуацию, а с другой сто-

роны, усложняет ее. Это упрощает ежедневное управление, потому что сервер RD Session Host не препятствует подключению пользователей. Тем не менее, администраторы по-прежнему должны отвечать за то, что соответствующие лицензии CAL приобретены, а это требует проведения дополнительных работ по администрированию. Индивидуальные лицензии CAL для пользователей необходимо применять, если пользователи будут подключаться к серверу RD Session Host с многих устройств.

Сервер Remote Desktop Licensing должен быть сконфигурирован на установку, выдачу и отслеживание лицензий RDS CAL. Клиенты не смогут подключаться к серверу RD Session Host, если по истечении льготного периода лицензии RDS CAL не были приобретены и добавлены на сервер лицензирования.

Группа Remote Desktop Users

Чтобы пользователи могли подключаться к серверу RD Session Host, они должны быть членами локальной группы `Remote Desktop Users` (Пользователи удаленного рабочего стола). Вы можете добавить их туда при добавлении роли Remote Desktop Services или сделать это позже. Группа `Administrators` добавляется в группу `Remote Desktop Users` по умолчанию.

Существуют две группы `Remote Desktop Users`: группа домена и локальная группа на сервере RD Session Host. Для предоставления доступа к серверу RD Session Host необходимо добавлять пользователей и группы в *локальную* группу `Remote Desktop Users`.

Нередко бывает так, что администратор добавляет пользователей в группу `Remote Desktop Users` домена, ошибочно полагая, будто это обеспечит им доступ к серверу RD Session Host. Спустя какое-то время, администратор обнаруживает, что не обратил внимания на слово *локальная*. После того как пользователи будут добавлены в локальную группу, все начинает работать именно так, как было заявлено. Всего этого можно избежать за счет надлежащего планирования, размещения и установки.

Добавление роли Remote Desktop Services

Ниже описаны шаги по установке роли Remote Desktop Services. Однако помните, что она должна устанавливаться на компьютере, который не является контроллером домена. В нашем примере среды один сервер (по имени `AD-01`) используется в качестве контроллера домена, а два других (`RDS01` и `RDS02`) — как серверы RDS в домене под названием lab.net.

1. Войдите в систему сервера-члена.
2. Если диспетчер серверов не запустился автоматически, запустите его, выбрав в меню Start (Пуск) пункт Administrative Tools⇨Server Manager (Администрирование⇨Диспетчер серверов).
3. В окне диспетчера серверов выберите пункт меню Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты).

   Откроется мастер добавления ролей и компонентов (Add Roles and Features Wizard).

4. Щелкните на кнопке Next (Далее), чтобы продолжить.

   Как упоминалось ранее в настоящей главе, вместо выбора роли, как это делалось в предыдущих версиях Windows, вы можете выбрать вариант установки Remote Desktop Services.

5. Выберите этот вариант и щелкните на кнопке Next.

   Далее необходимо выбрать тип развертывания. Доступны два варианта: стандартное развертывание, которое позволит развернуть службы Remote Desktop Services на множестве серверов, и быстрый запуск.

6. Выберите стандартное развертывание и щелкните на кнопке Next.

7. Теперь понадобится выбрать сценарий развертывания.

   В этом примере мы выбираем развертывание рабочего стола на базе сеансов. Позже в главе мы продемонстрируем варианты развертывания рабочего стола на основе виртуальных машин.

   В ходе стандартного развертывания устанавливаются три роли:
   - Remote Desktop Connection Broker (Брокер подключений удаленного рабочего стола)
   - Remote Desktop Web Access (Доступ к удаленным рабочим столам посредством веб)
   - Remote Desktop Session Host (Хост сеансов удаленного рабочего стола)

8. Для продолжения щелкните на кнопке Next.

   При выполнении нескольких следующих шагов потребуется добавить нужные серверы, которые вы хотите сконфигурировать.

9. Повторите шаг 8 для каждой роли.

10. Ознакомьтесь с информацией на экране Confirmation (Подтверждение).

    Прежде чем можно будет щелкнуть на кнопке Deploy (Развернуть), понадобится отметить флажок Restart the destination server automatically if required (При необходимости перезапустить целевой сервер автоматически).

    Перезапуск сервера будет выполнен как часть процесса развертывания (к сожалению, программа установки не настраивает автоматический вход в систему, поэтому для завершения процесса установки вам придется снова войти в систему).

    После входа вы получите информационные сообщения, имеющие отношение к серверу лицензирования, т.к. он еще не установлен и не сконфигурирован (при его наличии внутри предприятия).

    Мастер Add Roles and Features Wizard перезапустится и установка завершится.

11. Проверьте, что все роли успешно установлены.

    В Windows Server 2012 (включая Windows Server 2012 R2) службы Remote Desktop Services конфигурируются непосредственно из диспетчера серверов.

12. В окне диспетчера серверов щелкните на элементе Remote Desktop Services.

    Появится экран Overview (Обзор), показанный на рис. 29.3. Конфигурирование RDS в Windows Server 2012 (R2) несколько отличается от того, как это делалось в предыдущих версиях, а параметры, которые обычно настраивались посредством мастера Add Roles and Features Wizard, теперь конфигурируются отдельно.

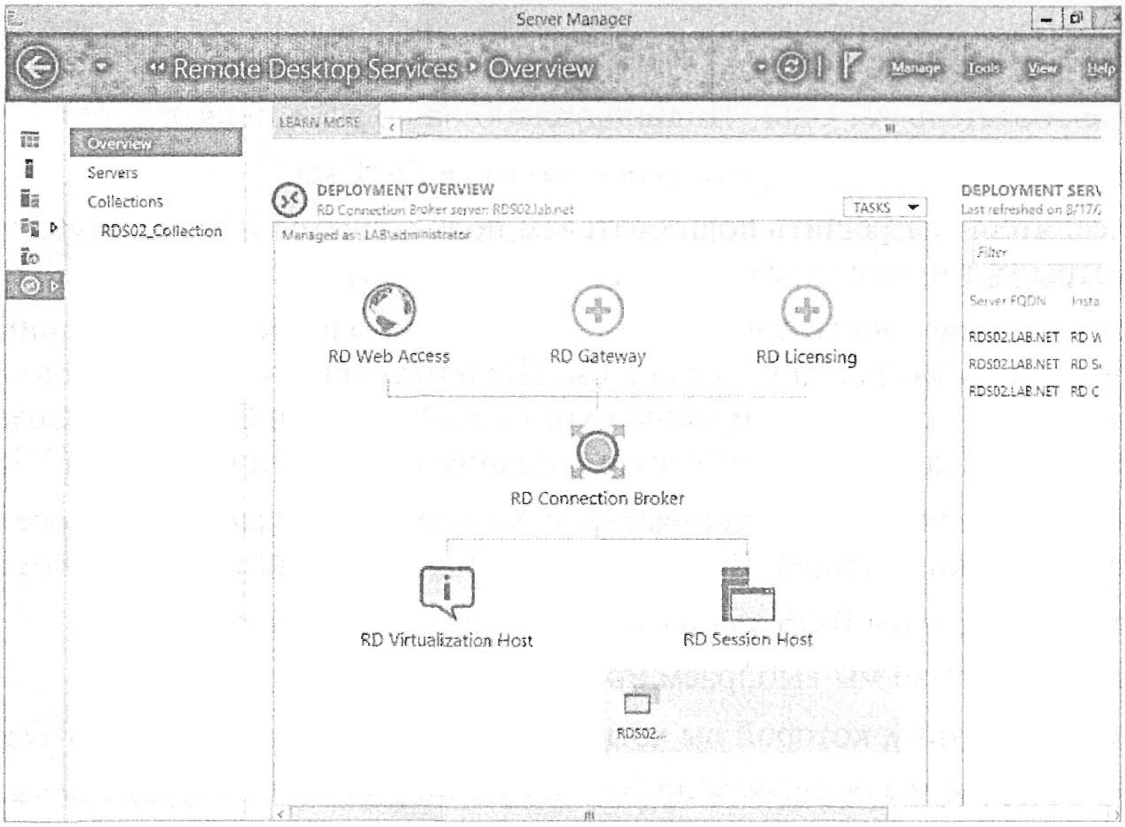


Рис. 29.3. Обзор служб Remote Desktop Services

13. Щелкните на кнопке Tasks (Задачи) рядом с разделом Deployment Overview (Обзор развертывания) и выберите пункт Edit Deployment Properties (Редактировать свойства развертывания).

    Свойства развертывания включают несколько параметров, самым интересным из которых является конфигурация лицензирования (рис. 29.4).

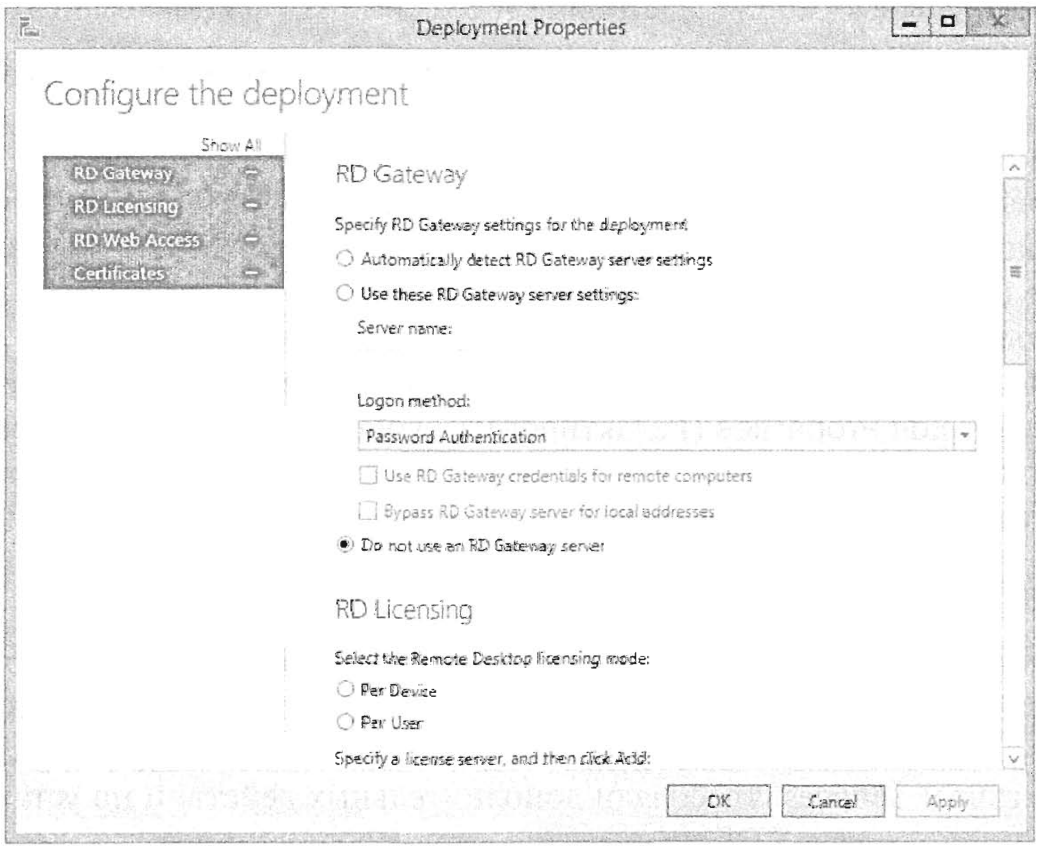


Рис. 29.4. Свойства развертывания

Именно здесь производится выбор между лицензиями CAL для устройств (переключатель Per Device (Индивидуально на устройство)) и для пользователей (переключатель Per User (Индивидуально на пользователя)).

14. В данном примере выберите переключатель Per User.

    Далее, чтобы разрешить пользователям подключиться и сконфигурировать параметры (в том числе разрешенные группы), потребуется создать коллекцию.

15. В окне Deployment Overview (см. рис. 29.3) выполните прокрутку вниз, чтобы добраться до значка RD Session Host. Щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Create Session Collection (Создать коллекцию сеанса). Откроется мастер создания коллекции (Collection Wizard).

16. Пропустите начальный экран мастера и введите описательное имя в поле Collection Name (Имя коллекции). В этом примере мы вводим **`RDS02_Collection`**.

17. Выберите серверы RDS для развертывания в них этой коллекции.

    В данном случае мы выбираем `RDS02`.

18. Выберите группу, которой вы хотите разрешить доступ к серверу RDS.

    В этом случае мы оставляем предлагаемую по умолчанию группу `Domain Users` (Пользователи домена), но может быть указана любая другая группа.

19. Выберите местоположение и лимит на размер пользовательских профилей на сервере RDS.

    В предыдущих версиях это было огромной проблемой, т.к. все обычно сохранялось на системном диске.

20. Поскольку мы имеем дело с демонстрационной средой, лимит на размер можно пока отключить.

21. Просмотрите выбранные настройки и создайте коллекцию сеанса.

На этом завершается базовое конфигурирование, которое позволит пользователям подключаться к серверу RDS.

Возможно, вы обратили внимание, что перед помещением сервера в производственную среду традиционно приходилось конфигурировать и просматривать значительное количество параметров. В окне диспетчера серверов для служб Remote Desktop Services теперь предусмотрено меню Collections (Коллекции), в котором вы увидите только что сконфигурированную коллекцию (рис. 29.5).

В разделе Properties (Свойства) этого окна щелкните на кнопке Tasks (Задачи) и выберите пункт Edit Properties (Редактировать свойства). Это позволит сконфигурировать дополнительные группы, параметры сеанса и ряд других настроек. Пример настроек, которые можно конфигурировать, приведен на рис. 29.6.

Добавление приложений

Хотя многие приложения (такие как Paint, Calculator и Notepad) будут работать в многопользовательском режиме автоматически, другие приложения придется устанавливать. Предшествующие версии Remote Desktop Services (которые ранее назывались Terminal Services) требовали дополнительных действий по установке таких приложений, но в случае RDS процесс значительно упростился.

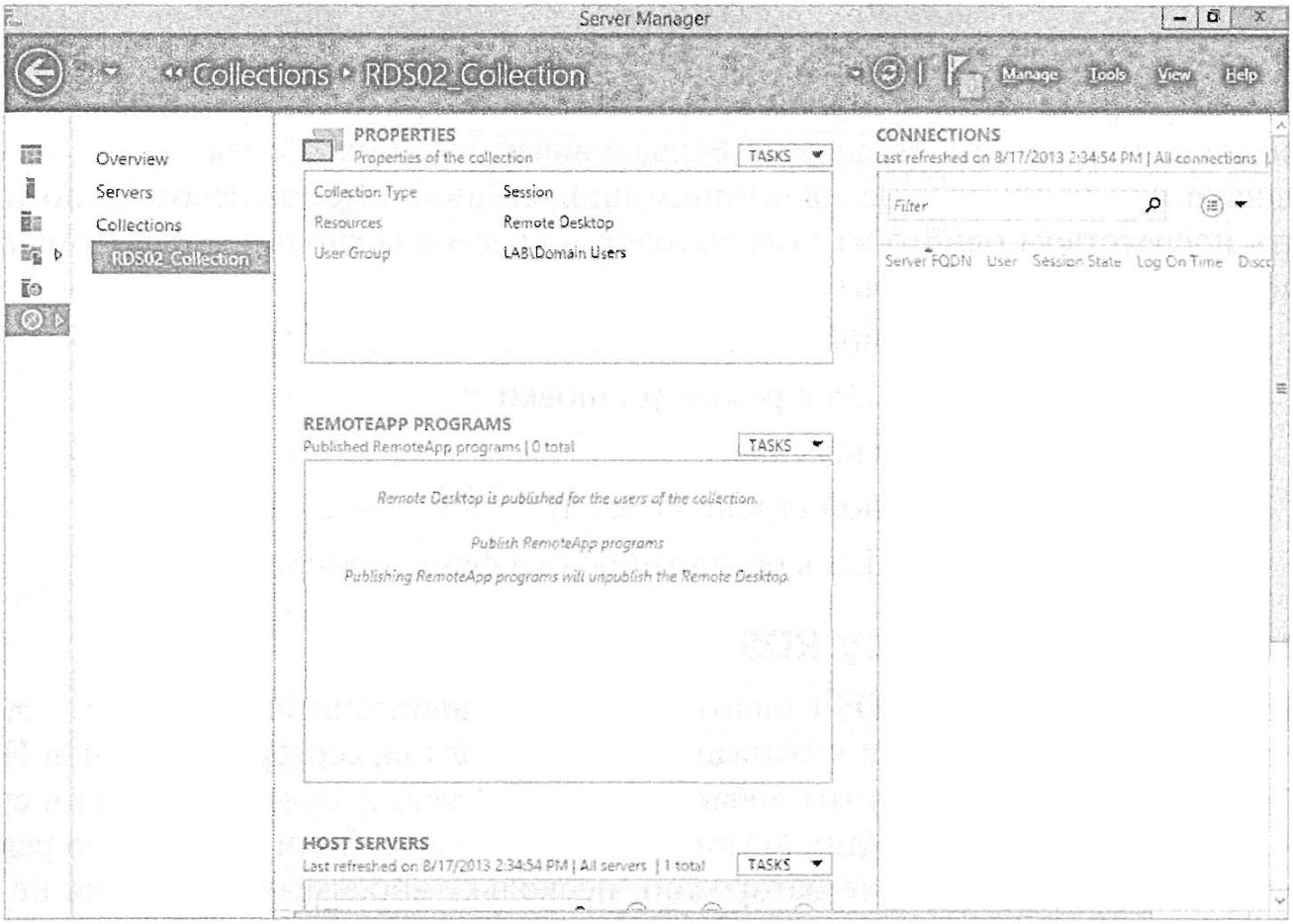


Рис. 29.5. Конфигурация коллекции

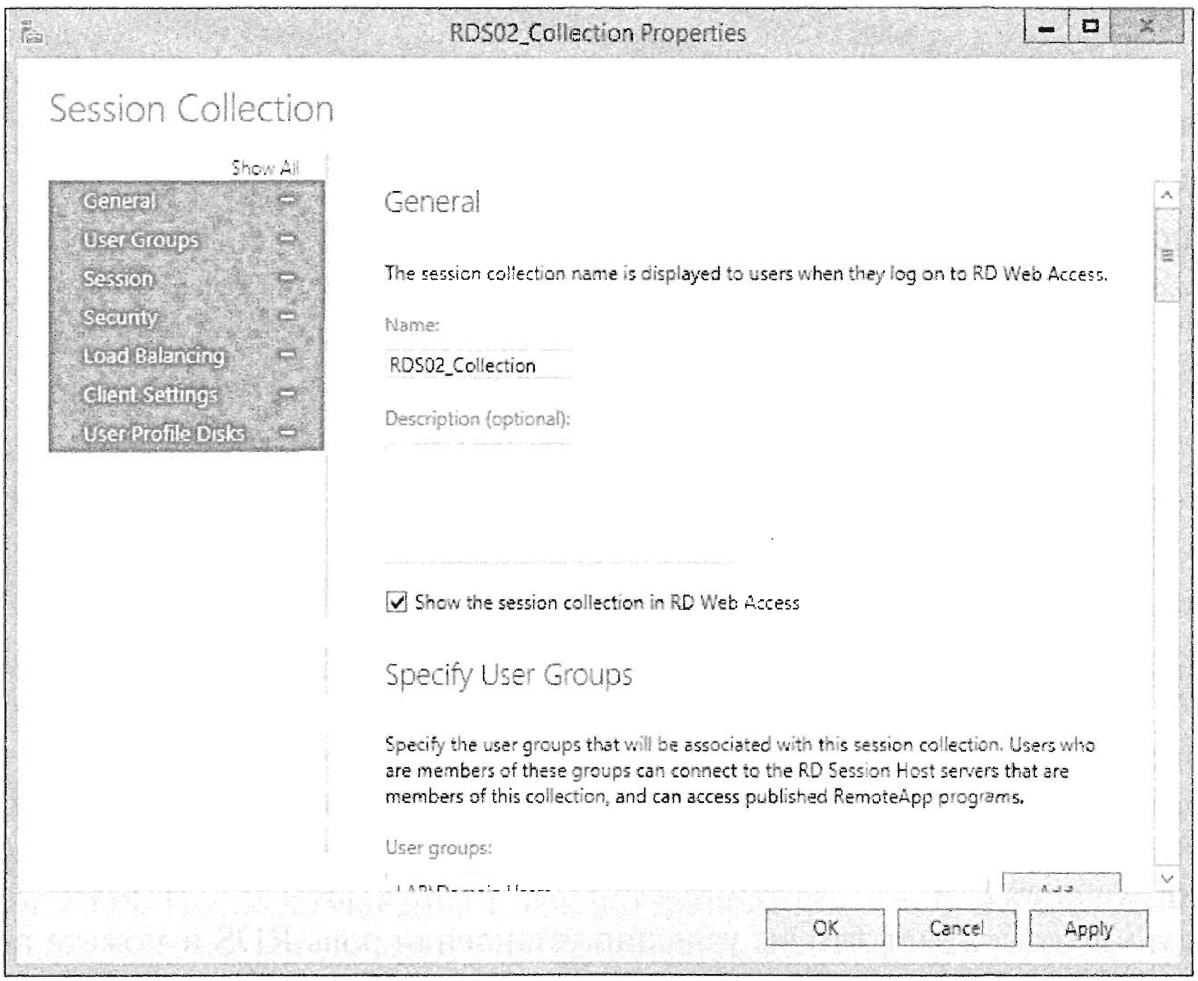


Рис. 29.6. Свойства коллекции

После добавления роли Remote Desktop Services любое приложение можно установить с применением файла `.msi` (Windows Installer) или функции установки и удаления программ панели управления. Если приложение будет устанавливаться с помощью одного из этих методов, то больше ничего не понадобится.

Однако при наличии унаследованного приложения, которое невозможно установить посредством одного из этих методов, придется воспользоваться командой `Change User`. Процесс состоит из трех действий.

1. Введите в окне командной строки команду `Change User /install`.

   Это переведет сервер RDS в режим установки.

2. Установите нужное приложение.

3. Введите в окне командной строки команду `Change User /execute`.

   Это возвратит сервер RDS в обычный режим функционирования.

Подключение к сеансу RDS

После добавления роли RDS клиенты, которые являются членами группы `Domain Users`, могут получать доступ к сеансам рабочего стола на сервере RD Session Host. Во время конфигурирования мы добавили группу `Domain Users`, которая в свою очередь была добавлена в группу `Remote Desktop Users`. Если вы вручную редактируете эту группу, действуйте осторожно, поскольку вносимые изменения не отражаются в пользовательском интерфейсе Remote Desktop Services. Теперь давайте подключимся к только что созданному серверу RD Session Host и коллекции.

1. Щелкните на кнопке Start (Пуск), введите **MSTSC** в поле поиска и нажмите <Enter>. Это приведет к запуску консоли Remote Desktop Connection. Полное описание всех параметров, доступных в этом инструменте, было приведено в главе 17.

2. Щелкните на кнопке Options (Параметры).

3. В поле Computer (Компьютер) введите имя компьютера, размещающего роль RDS, а в поле User name (Имя пользователя) укажите имя пользователя из локальной группы `Remote Desktop Users`.

   Окно будет подобно показанному на рис. 29.7.

4. Щелкните на кнопке Connect (Подключиться).

   Появится окно Windows Security (Безопасность Windows), где будет предложено ввести пароль для пользователя.

5. Введите пароль и щелкните на кнопке OK.

   Учетные данные пользователя будут проверены, и через короткое время вы будете подключены к рабочему столу.

В зависимости от того, как сконфигурирован инструмент MSTSC, подключение может быть начато в окне на рабочем столе или в полноэкранном режиме. Такое подключение представлено на рис. 29.8. Обратите внимание, что оно имеет внешний вид Windows 8.

Хотя это подтверждает, что вы успешно установили роль RDS и можете подключаться к сеансам RDS, сеансы по-прежнему являются обычными рабочими столами. Вы можете устанавливать приложения на сервере RD Session Host и делать их до-

ступными всем пользователям либо использовать приложения RD RemoteApp, чтобы разрешить пользователям запускать их в среде Windows на своих рабочих столах.

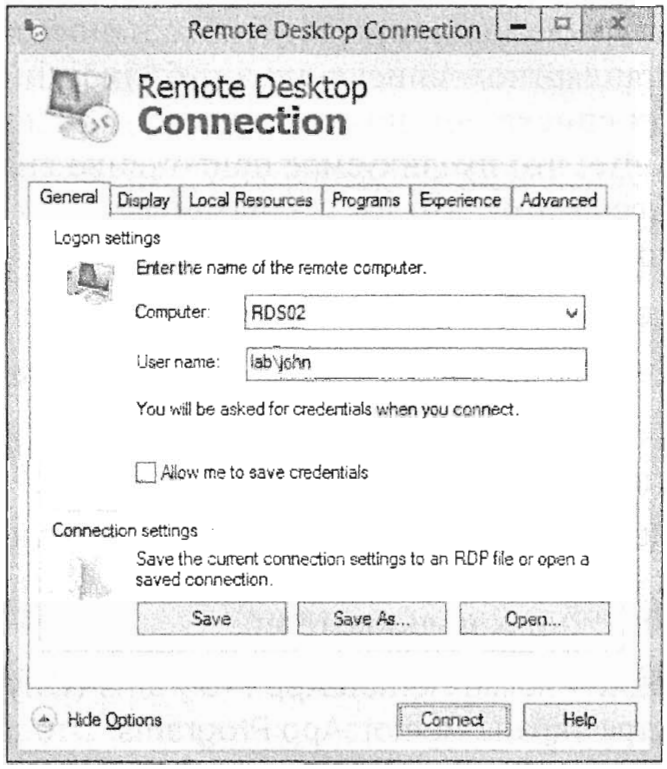


Рис. 29.7. Подключение с помощью Remote Desktop Connection

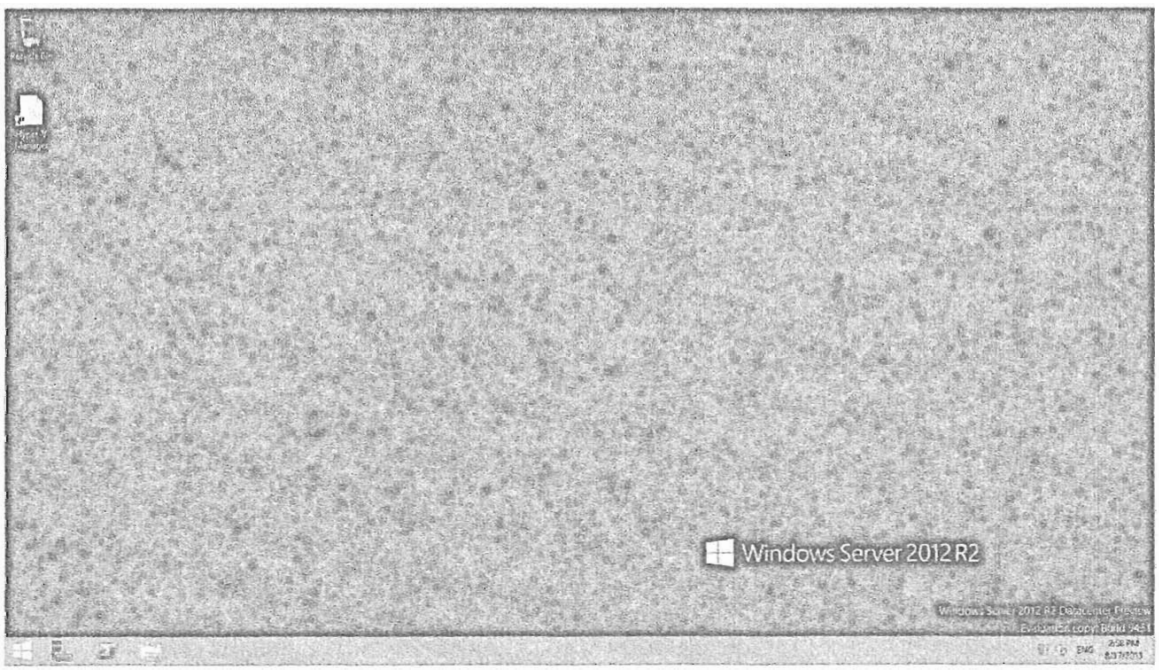


Рис. 29.8. Результат подключения к серверу RD Session Host с применением Remote Desktop Connection

Добавление приложения RD RemoteApp

Приложения RD RemoteApp представляют собой очень удобное средство, обеспечиваемое RDS. После добавления и конфигурирования они будут выполняться в собственных окнах на компьютере конечного пользователя. В отличие от запуска пользователем полного рабочего стола другой операционной системы, запуск на выполнение приложения RemoteApp выглядит подобно любому другому приложению.

Приложения RemoteApp стали частью процесса конфигурирования коллекции, тогда как в предыдущих версиях для обеспечения их работоспособности требовалось значительное количество действий. Сейчас это относительно простая задача. Описанная ниже процедура демонстрирует публикацию приложения калькулятора, которое находится в стандартном списке для опубликования, и окна командной строки, которого в этом списке нет, но мы покажем, как добавить интересующее приложение. Не забывайте, что публикуемое приложение сначала должно быть установлено. Удостоверьтесь в том, что вы устанавливаете его в многопользовательском режиме, иначе оно может не заработать.

1. Откройте диспетчер серверов и перейдите к службам Remote Desktop Services.
2. Щелкните на элементе Collections (Коллекции) для служб Remote Desktop Services.
3. Выберите коллекцию `RDS02_Collection`.

   Появится экран RemoteApp Programs (Программы RemoteApp), который можно применять для быстрого добавления новых приложений RemoteApp и опубликования их в коллекциях пользователей.
4. Щелкните на кнопке Publish RemoteApp Programs (Опубликовать программы RemoteApp) в центре экрана RemoteApp Programs. Это приведет к вызову мастера для опубликования нового приложения RemoteApp.
5. На экране мастера публикации программ RemoteApp (Publish RemoteApp Programs Wizard), показанном на рис. 29.9, отметьте флажок возле приложения Calculator, чтобы опубликовать его. Щелкните на кнопке Next (Далее).
6. Просмотрите путь и имя программы RemoteApp и щелкните на кнопке Publish (Опубликовать).

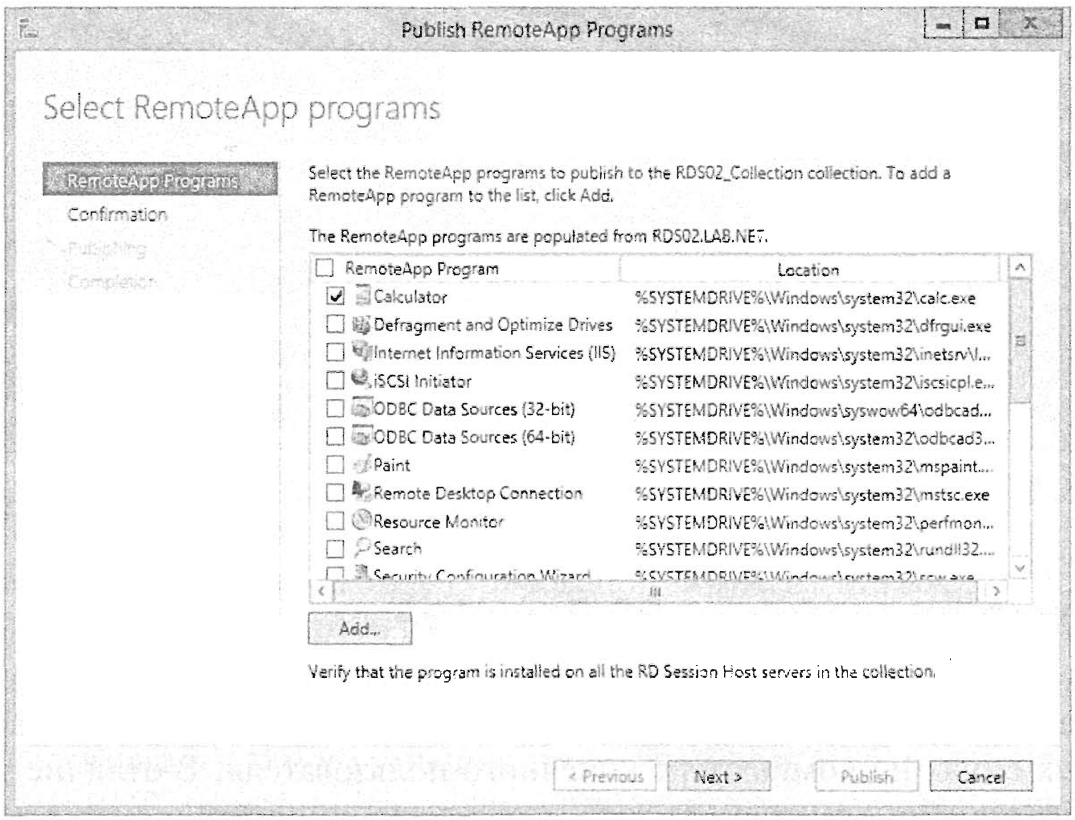


Рис. 29.9. Выбор приложения для опубликования

Итак, публикация приложения завершена; это оказалось значительно легче, чем в предыдущих версиях RemoteApp.

Давайте теперь рассмотрим другой пример. Предположим, что пользователям требуется возможность запуска программ из окна командной строки на сервере. Здесь мы покажем, как опубликовать окно командной строки. Разумеется, все это только примеры, и вы можете опубликовать на сервере любое приложение.

1. Если вы хотите добавить программу, не включенную в стандартный список, щелкните на кнопке Tasks (Задачи) рядом с разделом RemoteApp Programs (Программы RemoteApp) в диспетчере серверов (см. рис. 29.5) и выберите пункт Publish RemoteApp Programs (Опубликовать программы RemoteApp).
2. На экране Select RemoteApp Programs (Выбор программ RemoteApp) щелкните на кнопке Add (Добавить).
3. Перейдите к исполняемому файлу, который хотите опубликовать, и выберите его.

   В нашем демонстрационном примере мы публикуем окно командной строки, которое находится в `c:\windows\system32\cmd.exe`.
4. Завершите публикацию данного приложения, как было описано в предыдущей процедуре.

По умолчанию приложение RemoteApp публикуется для каждого, кто авторизован в коллекции; в нашем случае доступ получает вся группа `Domain Users` в испытательной среде. Однако может понадобиться ограничить доступ к приложению RemoteApp единственным пользователем или другой группой. Для этого выполните следующие шаги.

1. Щелкните правой кнопкой мыши на нужном приложении RemoteApp в списке программ RemoteApp.
2. Отредактируйте его свойства.
3. Измените назначение пользователей.

Запуск приложения RemoteApp из Internet Explorer

С помощью описанной ниже последовательности действий приложение RemoteApp можно запустить с помощью Internet Explorer. Это делается из сервера RDS либо из другого компьютера в сети.

1. Запустите Internet Explorer.
2. Введите в поле адреса следующий URL: **`https://localhost/rdweb`**.

   Если вы обращаетесь по этому URL из удаленного хоста, укажите вместо `localhost` имя сервера. Например, именем нашего сервера является `RDS02`, так что URL будет выглядеть как **`https://rds02/rdweb`**.

   Поскольку сервер использует самозаверяющий сертификат, вы увидите сообщение об ошибке.
3. Щелкните на ссылке Continue to This Website (Not Recommended) (Продолжить с этим веб-сайтом (не рекомендуется)).

4. Если появился запрос от средства расширенной конфигурации безопасности (Enhanced Security Configuration) браузера Internet Explorer, щелкните на кнопке Add (Добавить), чтобы указать, что вы доверяете этому веб-сайту.
5. Щелкните на кнопке Add еще раз, а затем щелкните на кнопке Close (Закрыть). Появится страница RemoteApp and Desktop Connection (Подключение к приложению RemoteApp и рабочему столу).
6. Введите имя пользователя в формате домен\имя пользователя и пароль для учетной записи, которая находится в локальной группе `Remote Desktop Users` сервера RDS. Мы создали в испытательном домене учетную запись по имени `John`, поэтому ввели имя пользователя в виде **`lab\john`** (рис. 29.10).

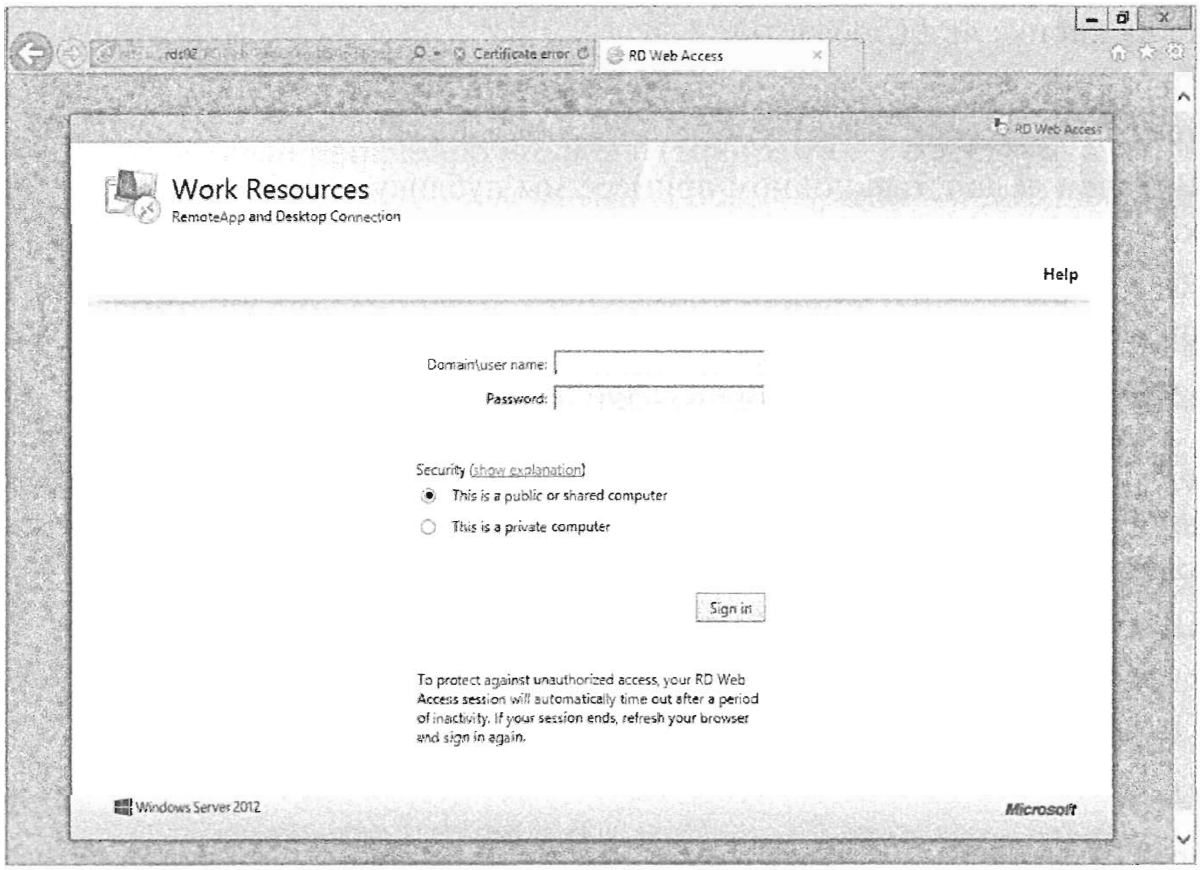


Рис. 29.10. Вход на веб-сайт удаленного доступа предприятия

Обратите внимание, что вы можете также выбрать, из какого компьютера будет осуществляться доступ к приложению RemoteApp — общественного или частного. Вариант с частным компьютером разрешает более длительный период активности, прежде чем сеанс будет прекращен. Настоятельно рекомендуется, чтобы по завершении работы пользователи закрывали сеансы; это позволит сбрасывать любые данные, оставшиеся в сеансе.

7. Введите пароль пользователя и щелкните на кнопке Sign in (Войти).

   Отобразятся программы RemoteApp, которые были опубликованы на данном сервере (рис. 29.11).
8. Щелкните на значке приложения Calculator (Калькулятор). На экране появится сообщение, предупреждающее о запуске программы RemoteApp.
9. Щелкните на кнопке Connect (Подключиться).

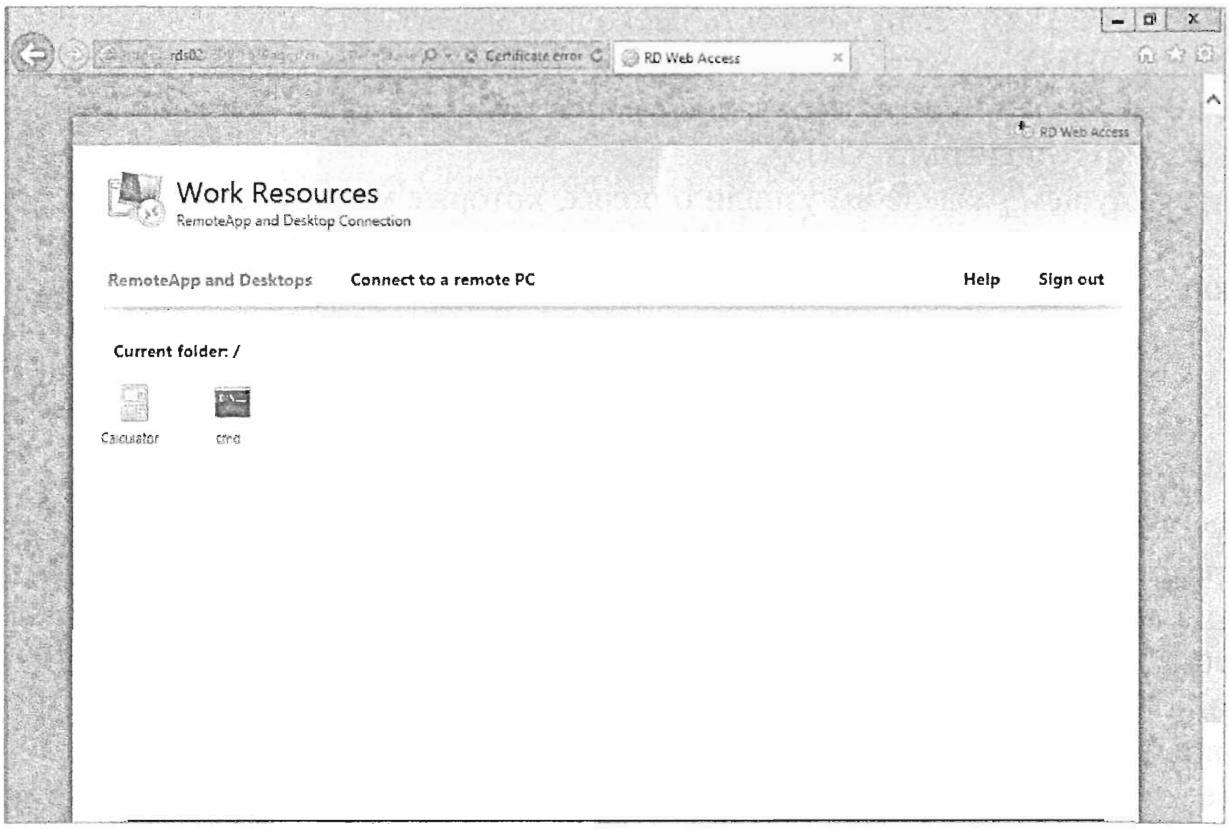


Рис. 29.11. Доступ к программам RemoteApp посредством Internet Explorer

Обратите внимание, что вы не обязаны вводить учетные данные (в предыдущих версиях для запуска приложения вам пришлось бы вводить учетные данные несколько раз).

10. Запустите также приложение `cmd` и щелкните на кнопке Connect, когда выдается соответствующее приглашение.
11. В окне командной строки введите **`hostname`**; должно возвратиться имя сервера RDS, на котором происходит выполнение.
12. Закройте все приложения и закройте Internet Explorer.

В предыдущих версиях RemoteApp существовала возможность упаковки приложения в файл RDP или MSI для распространения. В Windows Server 2012 R2 эта возможность объявлена устаревшей.

Инфраструктура виртуальных рабочих столов

Инфраструктура виртуальных рабочих столов (Virtual Desktop Infrastructure — VDI) используется уже достаточно давно. Существует много разных реализаций и подходов к ее внедрению. VDI — это объединенная в пул коллекция клиентских операционных систем (обычно Windows XP, Windows Vista, Windows 7 или Windows 8), размещенная на платформе виртуализации. Подключениями к этому пулу управляет служба брокера. Это позволяет клиентам распространять жизненный цикл актива на все предприятие и сосредоточить свои основные приложения в центре хранения и обработки данных. В Windows Server 2012 это рассматривается как часть стека Remote Desktop с добавлением Hyper-V.

Ключевым усовершенствованием в Windows Server 2012 R2, которое в большей степени касается хранилища, но приносит пользу также VDI, является дедупликa-

ция данных (Dedup). Если у вас есть несколько идентичных образов из копий главного файла VHDX, можете воспользоваться средством Dedup и сэкономить место на диске, не жертвуя при этом производительностью. Дедупликация данных поддерживается только в сценариях VHDX.

В предыдущем разделе вы узнали о ролях, которые можно выбирать при развертывании Remote Desktop Services. При рассмотрении VDI мы сосредоточимся на следующих трех ролях:

- RD Virtualization Host
- RD Connection Broker
- RD Web Access

С учетом того, что мы уже обсудили, в чем заключаются функции этих ролей, нам предстоит ознакомиться с предварительными условиями, которые должны быть приняты во внимание, прежде чем можно будет продолжить. Первое решение, которое необходимо принять при использовании Windows Server 2012 R2, касается клиентской ОС, которой вы будете оперировать в своей инфраструктуре VDI. В настоящее время Microsoft поддерживает Windows 7 SP1, Windows 8 и Windows 8.1. При выборе клиентской ОС вам потребуется построить шаблон; этот шаблон должен представлять собой стандартную сборку этой ОС с необходимыми приложениями (например, Office, Adobe Reader и т.д.). Как только все приложения будут установлены, а ОС надлежащим образом настроена, для этого образа понадобится запустить команду `sysprep`. Чуть позже мы покажем, как это делать.

Прежде всего, мы объясним, как сконфигурировать VDI на сервере Windows Server 2012 R2 и развернуть два типа коллекций: коллекцию в виде пула (где все пользуются общими ресурсами) и персональную коллекцию виртуальных рабочих столов (где машину VDI можно выделить только для одного пользователя). Образ в нашей испытательной среде будет основан на Windows 8. В среде также будет присутствовать контроллер домена под названием `AD-01` и хост (по имени `VDIHOST02`) с возможностью виртуализации, работающий под управлением Windows Server 2012. На хост `VDIHOST02` также скопирован ISO-образ Windows 8 для использования в дальнейшем. Ниже описаны шаги, которые необходимо выполнить.

1. Войдите в систему `VDIHOST02` и откройте диспетчер серверов.
2. Выберите пункт меню Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты).
3. На экране Before You Begin (Прежде чем начать) мастера добавления ролей и компонентов (Add Roles and Features Wizard) Щелкните на кнопке Next (Далее).
4. Выберите установку роли Remote Desktop Services и щелкните на кнопке Next.
5. Укажите для типа развертывания Standard Deployment (Стандартное развертывание) и щелкните на кнопке Next.
6. В качестве сценария развертывания выберите Virtual machine based desktop deployment (Развертывание рабочего стола на основе виртуальной машины).

   В результате стандартного развертывания будут добавлены следующие роли:

- Remote Desktop Connection Broker
- Remote Desktop Web Access
- Remote Desktop Virtualization Host

7. Для ролей Remote Desktop Connection Broker и Remote Desktop Web Access добавьте хост VDIHOST02 и щелкните на кнопке Next.
8. Для роли Remote Desktop Virtualization Host выберите еще раз хост VDIHOST02, но удостоверьтесь в том, что флажок Create a new virtual switch on the selected servers (Создать новый виртуальный коммутатор на выбранных серверах) отмечен, как показано на рис. 29.12.

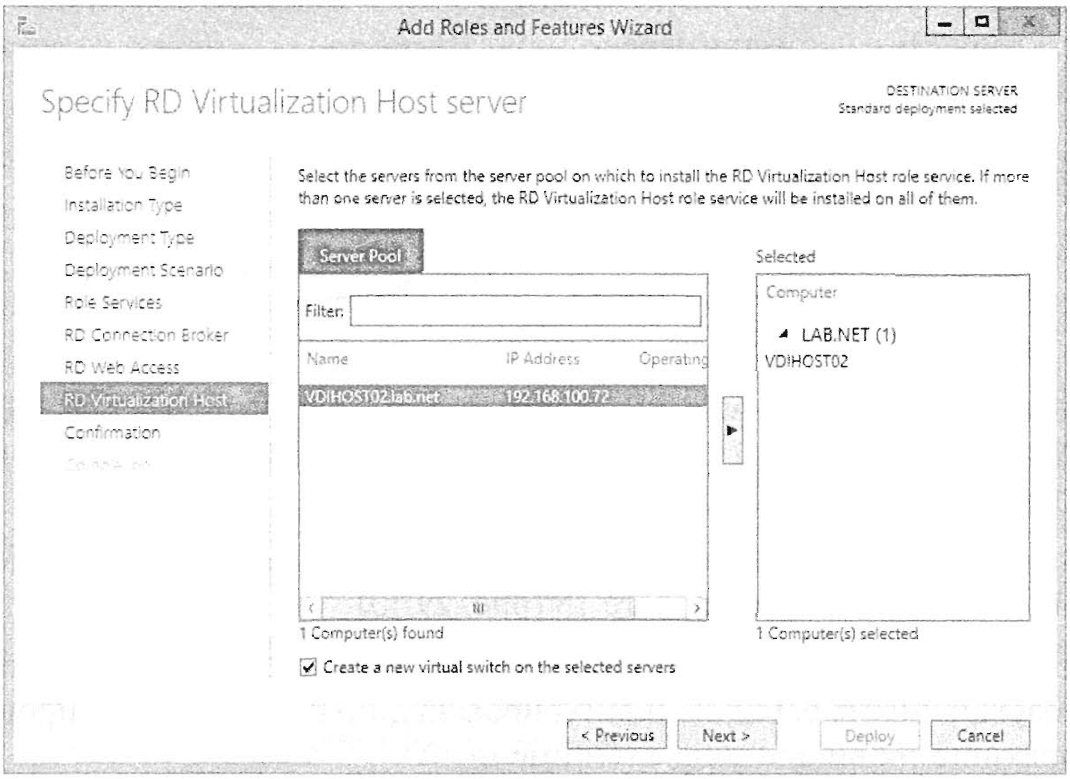


Рис. 29.12. Параметры Remote Desktop Virtualization Host

9. Просмотрите только что сконфигурированные параметры, отметьте флажок Restart the destination server automatically if required (При необходимости перезапустить целевой сервер автоматически) и щелкните на кнопке Deploy (Развернуть).

   Сервер развернет эти роли и перезагрузится один или два раза; причина перезагрузки в том, что добавляется также роль Hyper-V. Процедура установки в целом может занять 10–15 минут, так что есть время выпить чашку кофе.
10. После выполнения перезагрузок снова войдите в систему VDIHOST02; мастер Add Roles and Features Wizard перезапустится и завершит свою работу.

    Как и в случае описанной ранее установки хоста сеансов, на данном этапе можно не обращать внимания на сообщения о лицензиях.

    Далее на контроллере домена AD-01 необходимо создать организационную единицу, в которой будут храниться учетные записи компьютеров VDI.
11. Войдите в систему AD-01 и запустите оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory).

12. Создайте организационную единицу для хранения учетных записей компьютеров VDI.

    В нашей испытательной среде мы создали организационную единицу по имени `VDI Computers` (Компьютеры VDI).

13. Выберите пункт меню View⇨Advanced Features (Вид⇨Дополнительные возможности).

14. Щелкните правой кнопкой мыши на организационной единице `VDI Computers` и выберите в контекстном меню пункт Attribute Editor (Редактор атрибутов).

15. Выполните прокрутку вниз до атрибута `distinguishedname` и скопируйте его содержимое. В нашем примере атрибут `distinguishedname` содержит `OU=VDI Computers,OU=LAB,DC=lab,DC=NET`.

16. Снова войдите в систему `VDIHOST02`; если диспетчер серверов закрыт, откройте его и щелкните на Remote Desktop Services.

17. В разделе Deployment Overview (Обзор развертывания) щелкните на кнопке Tasks (Задачи) и выберите пункт Edit Deployment Properties (Редактировать свойства развертывания).

18. Щелкните на элементе Active Directory и затем выберите переключатель Specify the distinguished name of the organizational unit (Указать отличительное имя организационной единицы).

19. В поле ниже переключателя введите отличительное имя организационной единицы, как упоминалось на шаге 15 (рис. 29.13).

    Обратили ли вы внимание в нижней части экрана на предупреждение о том, что разрешения не были сконфигурированы, но будут скорректированы, когда вы щелкнете на кнопке Apply (Применить)?

20. Щелкните на кнопке Apply, и будет предпринята попытка установки разрешений. Предупреждающее сообщение должно измениться на сообщение, информирующее о том, что настройки были применены и подходящие разрешения активны. Теперь нам предстоит немного отвлечься и создать образ, который будет использоваться для развертывания VDI.

21. Откройте диспетчер Hyper-V на хосте `VDIHOST02`.

    Поскольку вам уже приходилось иметь дело с виртуальными машинами и Hyper-V в главах 27 и 28, мы предполагаем, что вы знаете, как создавать виртуальную машину Windows 8, монтировать образ ISO и устанавливать операционную систему. В этом примере виртуальная машина названа `Win8-Gold` и размещена локально на диске `C` в папке по имени `VMSTORE`.

22. После установки операционной системы и развертывания желаемых приложений откройте окно командной строки с повышенными разрешениями и введите **`c:\windows\system32\sysprep\sysprep`**.

23. Выберите параметры, как показано на рис. 29.14.

24. После того как виртуальная машина отключится в Hyper-V, щелкните правой кнопкой мыши на ее имени и выберите в контекстном меню пункт Export

(Экспортировать). Вам будет предложено указать путь. По умолчанию инфраструктура VDI на сервере Windows Server 2012 R2 требует помещения экспортированной копии виртуальной машины в `c:\RDVirtualDesktopTemplate`.

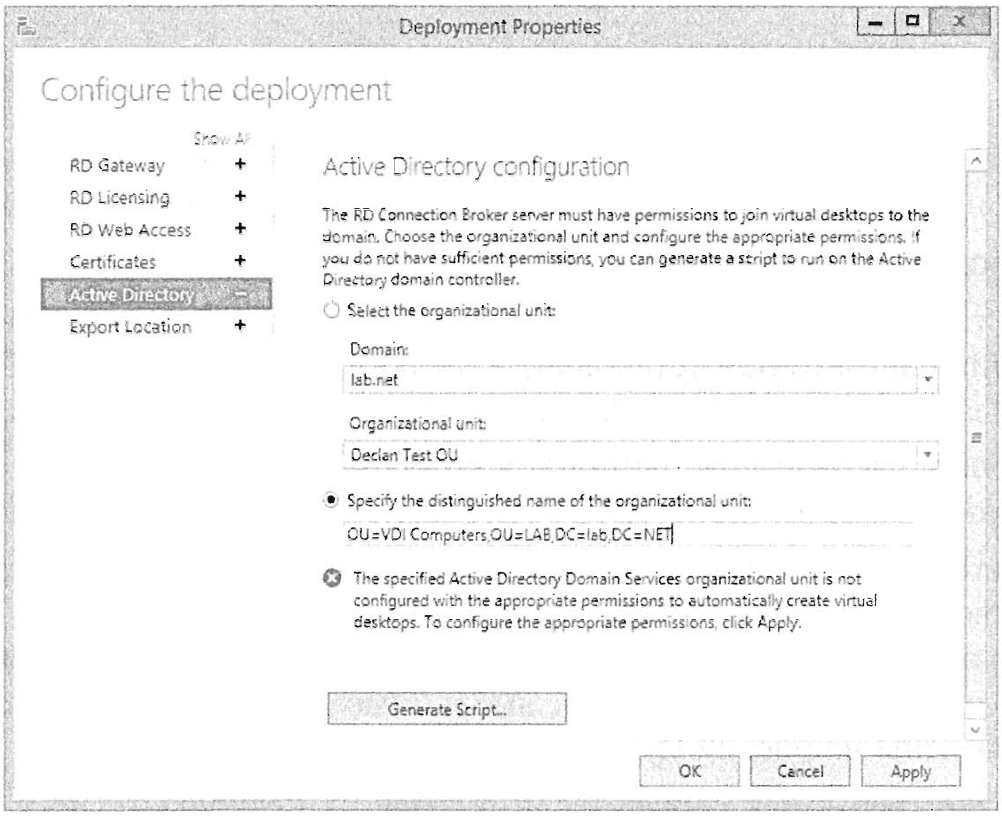


Рис. 29.13. Указание свойств организационной единицы Active Directory

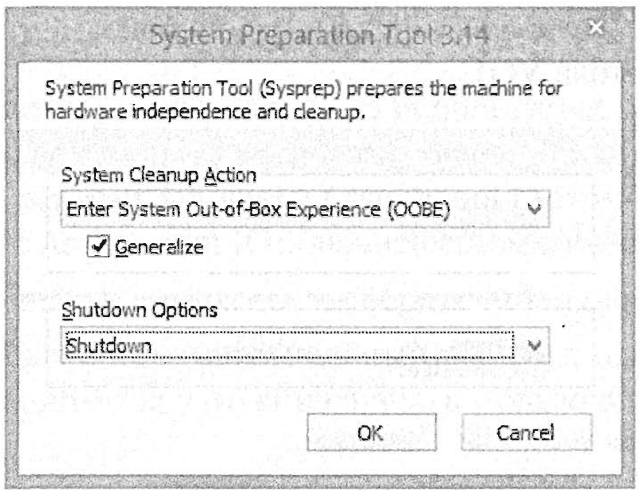


Рис. 29.14. Параметры утилиты `sysprep`

25. Сконфигурируйте этот путь посредством PowerShell, используя командлеты `Get-RDVirtualDesktopTemplateExportPath` и `Set-RDVirtualDesktop TemplateExportPath`.
26. Дождитесь завершения экспорта и удалите виртуальную машину.
27. Импортируйте только что экспортированную виртуальную машину из `C:\RDVirtualDesktopTemplatePath\Win8-Gold`.
28. Возвратитесь в окно диспетчера серверов и выберите элемент Remote Desktop Services⇨Collections (Службы удаленного рабочего стола⇨Коллекции).

29. Щелкните на кнопке Tasks и выберите пункт Create Virtual Desktop Collection (Создать коллекцию виртуального рабочего стола).
30. Щелкните на кнопке Next на экране Before You Begin.
31. Введите имя коллекции и щелкните на кнопке Next.

    В этом примере мы ввели `Win8-VDI-Pooled`.
32. Выберите переключатель Pooled Virtual Desktop Collection (Коллекция виртуального рабочего стола в виде пула) и щелкните на кнопке Next.

    Шаблон, сконфигурированный вами ранее, сейчас появляется в этом списке.
33. Для продолжения щелкните на кнопке Next.
34. Выберите переключатель Provide unattended installation settings (Использовать настройки автономной установки) и щелкните на кнопке Next. Если в вашей организации подготовлен файл ответов `sysprep`, можете воспользоваться им.
35. Установите часовой пояс региона, в котором находитесь, укажите записанное вами ранее значение атрибута `distinguishedname` и щелкните на кнопке Next.
36. Добавьте группы, которым вы авторизуете доступ к пулу VDI. Определите количество рабочих столов VDI, которые необходимо иметь в пуле (не забывайте, что это количество должно соответствовать возможностям оборудования), и укажите префикс. Параметры, выбранные для рассматриваемого примера, представлены на рис. 29.15.
37. Выберите требуемый сервер (если в среде их несколько), но уделите время просмотру информации, касающейся памяти и процессора, а также любых существующих виртуальных машин. По завершении щелкните на кнопке Next.

    Вы можете указать, где должны быть размещены виртуальные жесткие диски нового рабочего стола VDI.

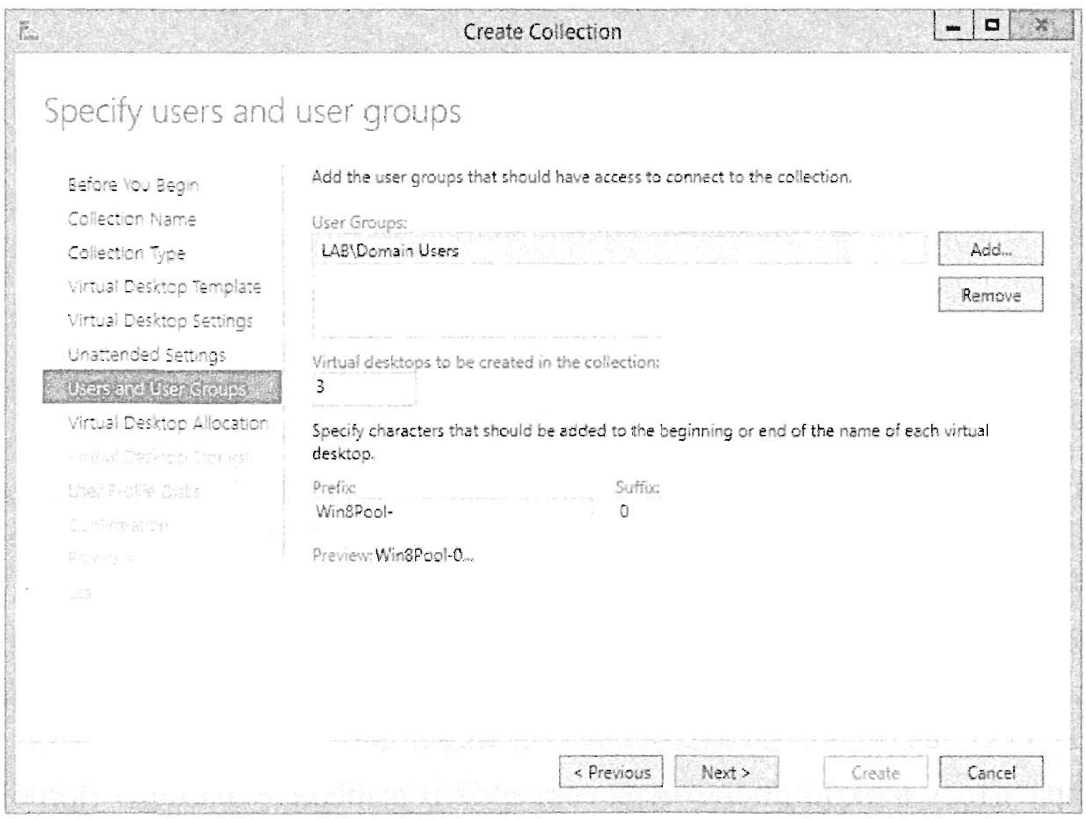


Рис. 29.15. Указание пользователей и групп

38. В данном случае выберите вариант, предлагаемый по умолчанию, т.к. на демонстрационном сервере имеется только один жесткий диск.

    В производственной среде вам следует рассмотреть другие варианты, зависящие от инфраструктуры. В самом крайнем случае, если вы выберете переключатель Specify a separate path on which to store the parent disk (Указать отдельный путь, по которому будет находиться родительский диск), то это будет следовать рекомендуемой практике и обеспечит оптимальную производительность хранилища.

39. Снимите отметку с флажка Enable User Profiles Disk (Включить диск пользовательских профилей), поскольку в нашей среде такой диск использоваться не будет. Обратите внимание, что в большинстве предприятий, работающих с инфраструктурой VDI, обычно реализовано перенаправление пользовательских профилей на общий файловый ресурс, поэтому в данном параметре нет необходимости.

40. Просмотрите все настройки и щелкните на кнопке Create (Создать).

    В зависимости от оборудования этот процесс занимает в среднем от 5 до 30 минут.

41. Щелкните на кнопке Close (Закрыть), чтобы можно было создать вторую коллекцию для персональных подключений.

42. Создайте новую коллекцию виртуальных рабочих столов.

43. Назовите эту коллекцию `Win8-VDI-Personal`.

44. Выберите переключатель Personal Virtual Desktop Collection (Персональная коллекция виртуальных рабочих столов) и щелкните на кнопке Next.

45. Выберите образ `Win8-Gold` еще раз.

    Вы получите уведомление о том, что образ используется другими коллекциями. Поскольку в данном случае речь идет о персональной коллекции рабочих столов, можете выбрать вариант Automatic Assignment (Автоматическое назначение) или Disable Automatic Assignment (Отключить автоматическое назначение).

46. Чтобы сократить накладные расходы, выберите Automatic Assignment.

    Автоматическое назначение — оптимальный вариант, однако встречаются ситуации, когда необходимо вручную назначать пользователя виртуальной машине.

    Как и ранее, вы можете указать существующий файл ответов `sysprep`, если организация им располагает.

47. Выберите переключатель Provide unattended installation settings и щелкните на кнопке Next.

48. Как и ранее, укажите часовой пояс региона и организационную единицу.

49. Сконфигурируйте подходящую группу для доступа и назначения виртуальному рабочему столу. Сконфигурируйте нужное количество рабочих столов для развертывания и префикс.

    На рис. 29.16 показаны параметры, выбранные для данного примера.

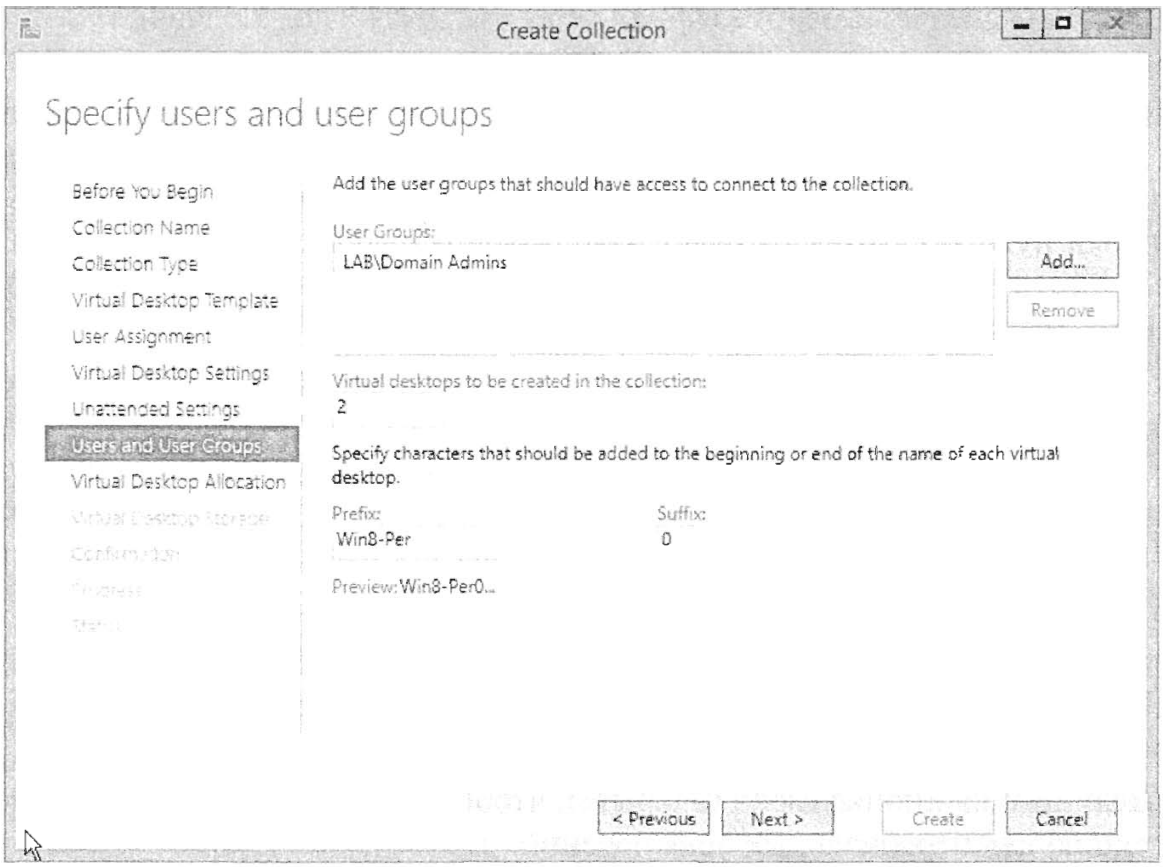


Рис. 29.16. Параметры, сконфигурированные для персональной коллекции VDI

50. Просмотрите все настройки, как уже делали ранее, и щелкните на кнопке Next.

    При выборе хранилища виртуального рабочего стола обратите внимание на то, как изменился вариант, предлагаемый по умолчанию; количество доступных вариантов уменьшилось.

51. Выберите переключатель Store on Each RD Virtualization Host Server (Сохранить на каждом хост-сервере виртуализации RD).

52. Просмотрите и подтвердите выбранные настройки, после чего щелкните на кнопке Create.

53. Закройте этот экран и следите за ходом развертывания.

54. Из удаленного клиента войдите в `https://vdihost02.lab.net/rdweb` (это наш URL).

    Не обращайте внимания на сообщения об ошибках, касающиеся сертификата, т.к. по умолчанию развертывается самозаверяющий сертификат.

55. Введите учетные данные пользователя домена, в данном случае `lab\john`.

    На рис. 29.17 представлен пример веб-страницы, которую мы получили.

56. Во-первых, протестируйте подключение к коллекции `Win8-VDI-Pooled`, щелкнув на ее значке.

    Вам будет предложено подтвердить подключение.

57. Щелкните на кнопке Connect (Подключиться).

    В результате вы войдете в систему виртуальной машины VDI из пула.

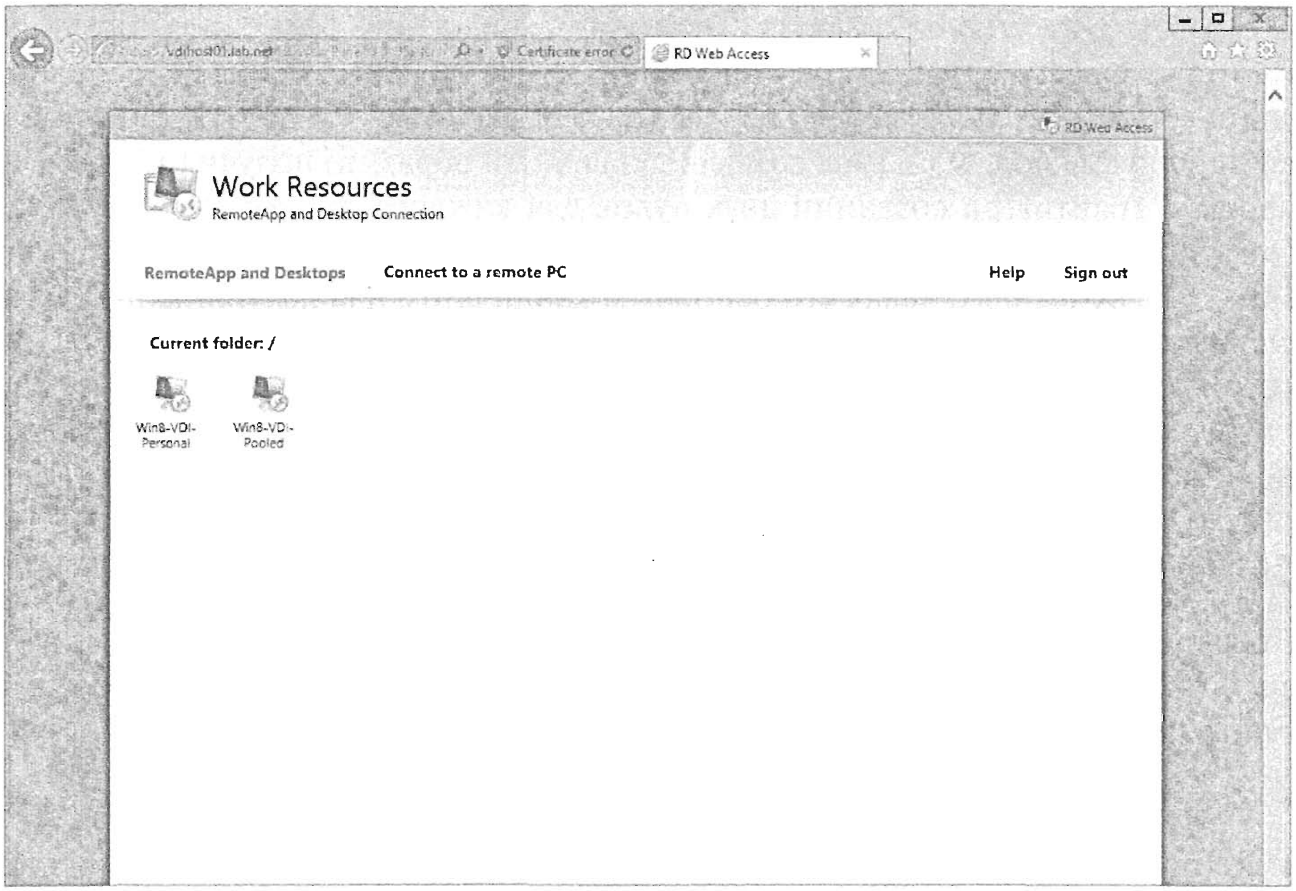


Рис. 29.17. Веб-страница для VDI

58. После проверки приложений и возможности подключения к сети выйдите из системы.
59. Во-вторых, протестируйте подключение к коллекции `Win8-VDI-Personal`, щелкнув на ее значке.
60. Получив приглашение, щелкните на кнопке Connect.

    По существу здесь не окажется ничего нового, но теперь каждый раз вы будете входить в систему той же самой виртуальной машины.

На рис. 29.18 показаны виртуальные машины, связанные с развертыванием VDI. Обратите внимание, что одна из них находится в состоянии Saved (Сохранена); это происходит автоматически, сохраняя ресурсы, когда они не используются.

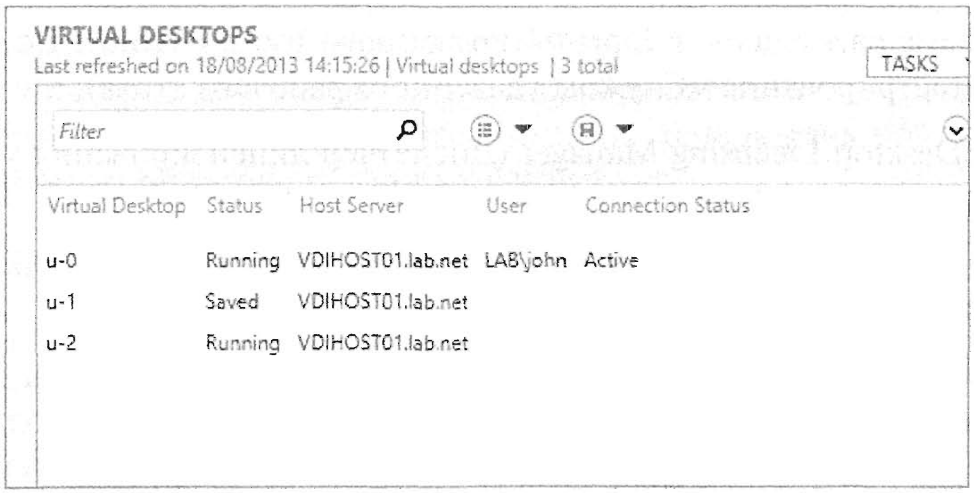


Рис. 29.18. Виртуальные машины, связанные с развертыванием VDI

Теперь мы имеем полностью работоспособное решение VDI. Ранее упоминалось о том, что инфраструктура VDI в Windows Server 2012 оптимизирована для работы с дедупликацией данных хранилища. Рассмотрим это немного подробнее, чтобы вы уловили общую идею. Когда мы создали первичный образ, то получили VHDX-файл размером 8 Гбайт. При создании двух пулов для каждого их них была создана копия этого первичного образа. В сумме это составило примерно 24 Гбайт хранилища только в VHDX-файлах, делая его основным кандидатом для дедупликации данных. За счет одного лишь включения функции Dedup можно было бы сэкономить около 60% стоимости внешней памяти. Однако не следует размещать файлы VDI на корневом томе, т.к. на нем нельзя включать Dedup. Начиная с шага 25, мы показали, как сконфигурировать путь таким образом, чтобы он не находился на корневом томе.

Мониторинг служб Remote Desktop Services

После развертывания и запуска служб Remote Desktop Services вам понадобится обеспечить их мониторинг и управление. В предшествующих версиях Windows было доступно несколько инструментов RDS:

- Remote Desktop Services Manager (Диспетчер служб удаленного рабочего стола)
- Remote Desktop Session Host Configuration (Конфигурация хоста сеансов удаленных рабочих столов)
- RemoteApp Manager (Диспетчер приложений RemoteApp)
- Remote Desktop Web Access Configuration (Конфигурация доступа к удаленным рабочим столам посредством веб)
- Remote Desktop Licensing Manager (Диспетчер лицензирования удаленных рабочих столов)
- Remote Desktop Connection Manager (Диспетчер подключений к удаленным рабочим столам)
- Remote Desktops (Удаленные рабочие столы)

В Windows Server 2012 R2 все инструменты администрирования, за исключением двух, расположены непосредственно в пользовательском интерфейсе диспетчера серверов внутри раздела Remote Desktop Services. Двумя инструментами, которые по-прежнему размещены в Start⇨Administrative Tools⇨Remote Desktop Services (Пуск⇨Администрирование⇨Службы удаленного рабочего стола), являются:

- Remote Desktop Licensing Manager (Диспетчер лицензирования удаленных рабочих столов)
- новый инструмент RD Licensing Diagnoser (Средство диагностики лицензирования удаленных рабочих столов)

Инструмент RD Licensing Diagnoser помогает определить, возникнут ли в вашей среде проблемы с лицензированием. На рис. 29.19 показан вывод RD Licensing Diagnoser для среды, где лицензии пока не опубликованы, но льготный период еще не закончился.

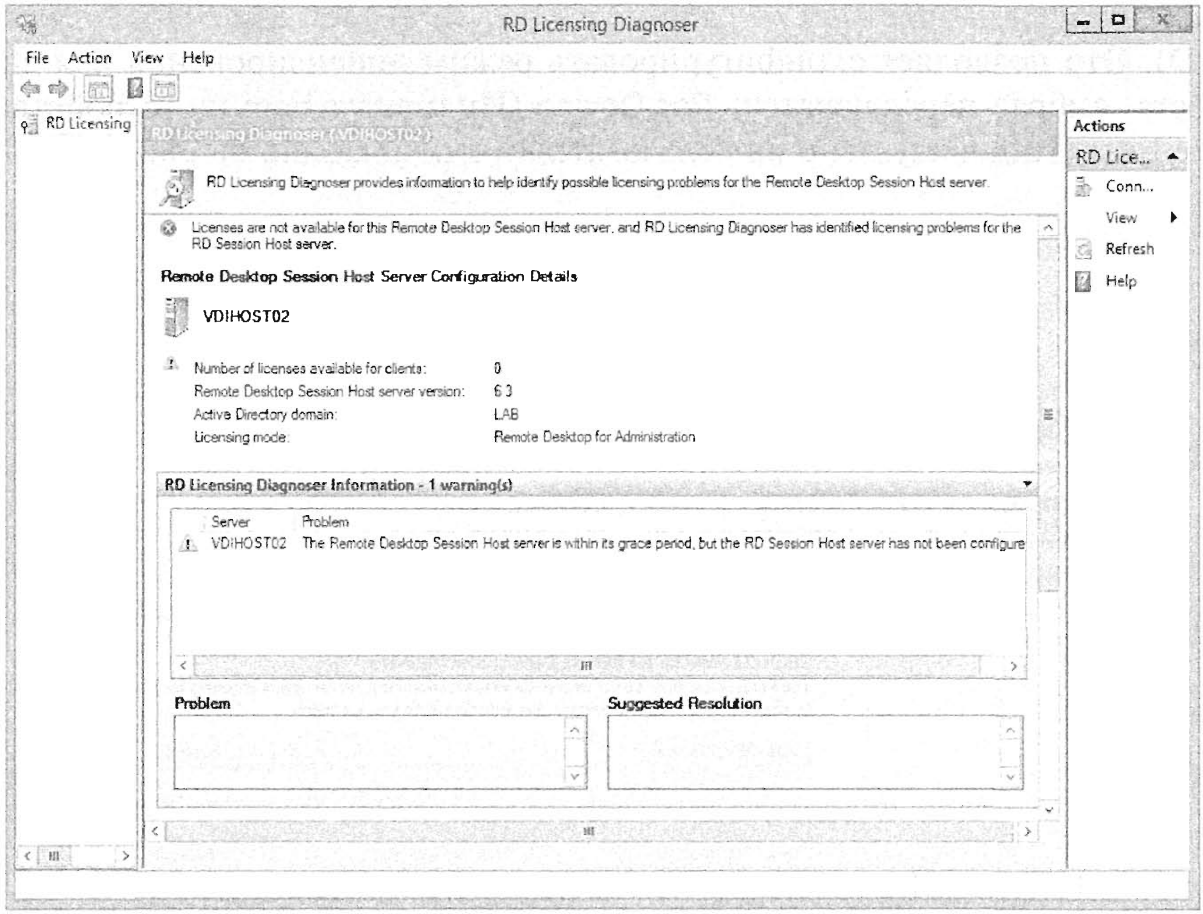


Рис. 29.19. Инструмент RD Licensing Diagnoser

Инструмент Remote Desktop Licensing Manager в действительности остался без изменений и по-прежнему выполняет те же функции, что и ранее. Требование предварительной активации сервера лицензирования на Microsoft Clearinghouse (Расчетная палата Microsoft) осталось в силе, и все еще необходимо устанавливать подходящие лицензии CAL. Теперь доступно удобное средство генерации отчетов по использованию CAL, но кроме этого набор возможностей является таким же, как в предыдущих версиях.

Выполнение распространенных задач

Как уже упоминалось, все унаследованные инструменты для мониторинга и даже конфигурирования Remote Desktop Services до версии Windows Server 2012 находятся внутри пользовательского интерфейса (разумеется, за исключением PowerShell). При описании процесса развертывания Remote Desktop и VDI мы предоставили экранные снимки, которые демонстрировали, как обращаться к элементам информации, обычно требующимся во время развертывания. Теперь речь пойдет о нескольких распространенных областях, о которых следует знать.

Пример 1. Конфигурирование лицензирования для RD Session Host или Virtualization Host

1. В разделе Remote Desktop Services диспетчера серверов щелкните на элементе Overview (Обзор).
2. Перейдите в область Deployment Overview (Обзор развертывания), щелкните на кнопке Tasks (Задачи) и выберите пункт Edit Deployment Options (Редактировать параметры развертывания).

3. Щелкните на значке "плюс" рядом с элементом RD Licensing (Лицензирование RD). Это позволяет сконфигурировать режим лицензирования для данного хоста, выбрав переключатель Per Device (Индивидуально на устройство) или Per User (Индивидуально на пользователя), как показано на рис. 29.20.

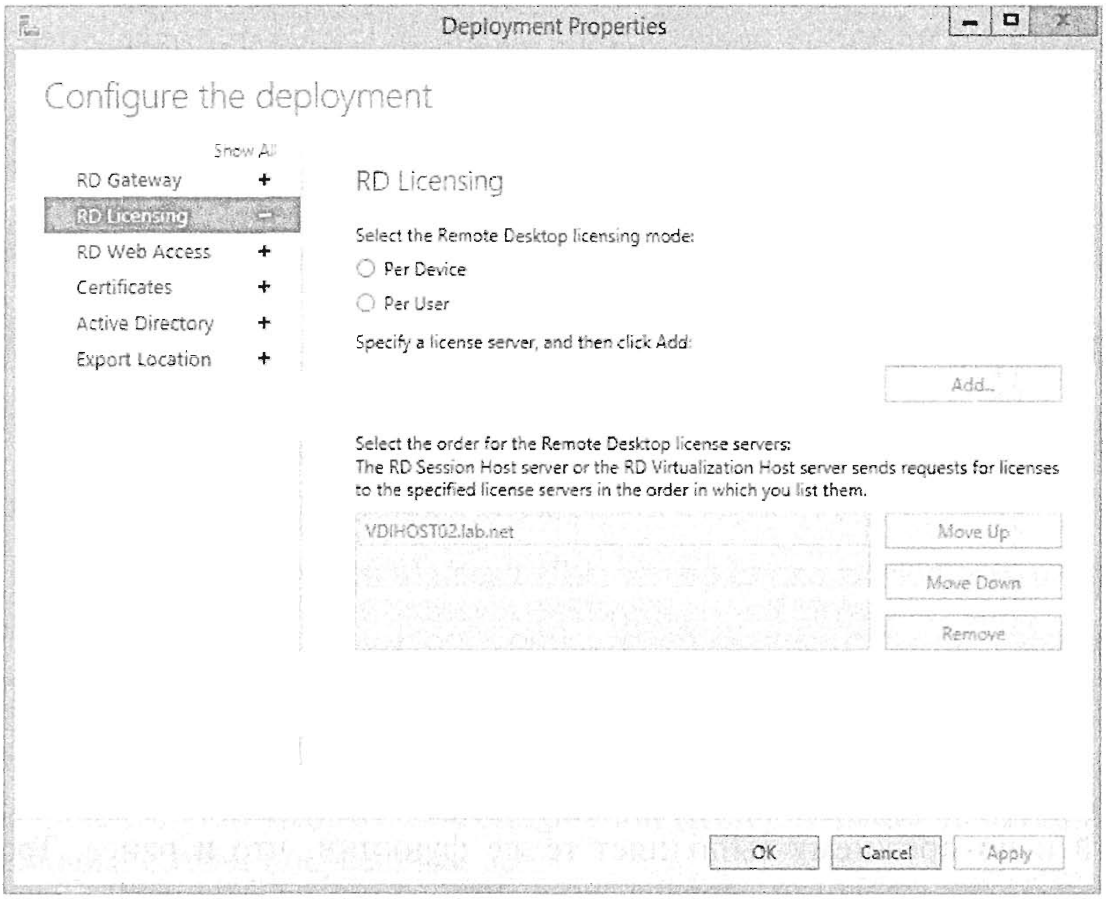


Рис. 29.20. Конфигурирование режима лицензирования RD

Пример 2. Изменение местоположения для экспорта шаблона виртуального рабочего стола

1. На рис. 29.20 в нижней части левого столбца вы увидите элемент Export Location (Местоположение экспорта). Он имеет отношение к местоположению шаблона.
2. Откройте окно командной строки с повышенными разрешениями и введите `net share`. Это позволит вам быстро отобразить данный общий ресурс на физический путь.
3. Просто укажите другой сконфигурированный путь.

Пример 3. Изменение уровня шифрования RDS на FIPS Compliant

1. В окне диспетчера серверов выберите Remote Desktop Services⇨Collections⇨Name of your Collection (Службы удаленного рабочего стола⇨Коллекции⇨Имя вашей коллекции).
2. Взгляните на окно свойств, щелкните на кнопке Tasks (Задачи) и выберите пункт Edit Properties (Редактировать свойства).
3. Выберите в списке слева элемент Security (Безопасность) и в раскрывающемся списке Encryption Level (Уровень шифрования) выберите вариант FIPS Compliant (Совместимый с FIPS), как показано на рис. 29.21.

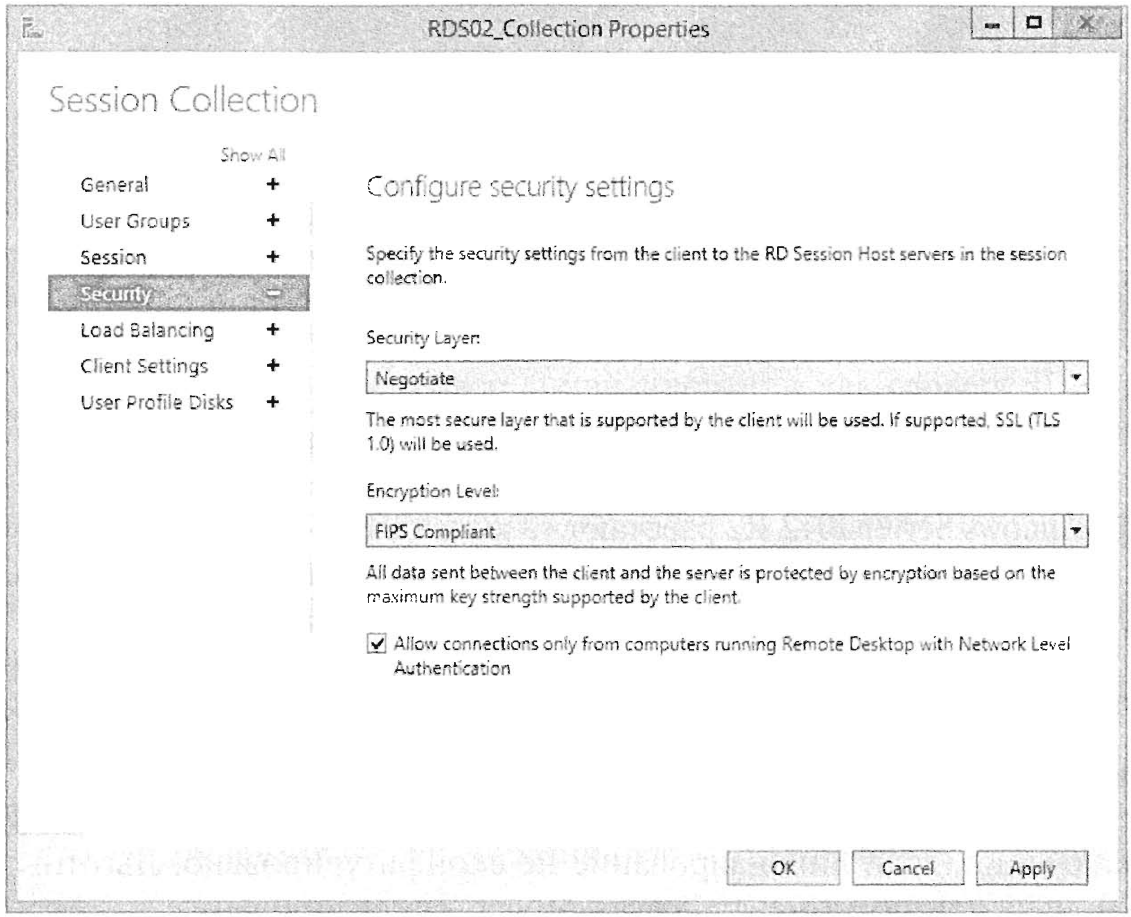


Рис. 29.21. Изменение уровня шифрования RDS

Пример 4. Изменение клиентских настроек для RD Session Host

1. Выберите элемент Client Settings (Клиентские настройки) в списке слева (см. рис. 29.21). Обратите внимание на то, что вы можете включать и отключать различные параметры, оказывая влияние на функции клиентов.
2. Отобразите диски посредством RDS из локальной машины.
3. Скопируйте данные в буфер обмена и вставляйте из буфера обмена.
4. Отключите воспроизведение аудио и видео.

Пример 5. Выяснение, кто в систему какой виртуальной машины вошел

1. В окне диспетчера серверов выберите Remote Desktop Services⇨Collections⇨Name of your Collection (Службы удаленного рабочего стола⇨Коллекции⇨Имя вашей коллекции).
2. Взгляните на рис. 29.22.

   Здесь показан пример вывода, который позволяет выяснить, кто в систему какой виртуальной машины вошел в рамках персонального пула VDI.

Это лишь несколько примеров выполнения ряда распространенных задач, которые обычно вам пришлось бы выполнять при развертывании Remote Desktop Services. Они применимы к сценариям VDI и RDS.

Все эти возможности доступны и в PowerShell. Полный список командлетов, имеющихся на вашей машине, можно получить с использованием следующего командлета:

```
get-command -module RemoteDesktop
```

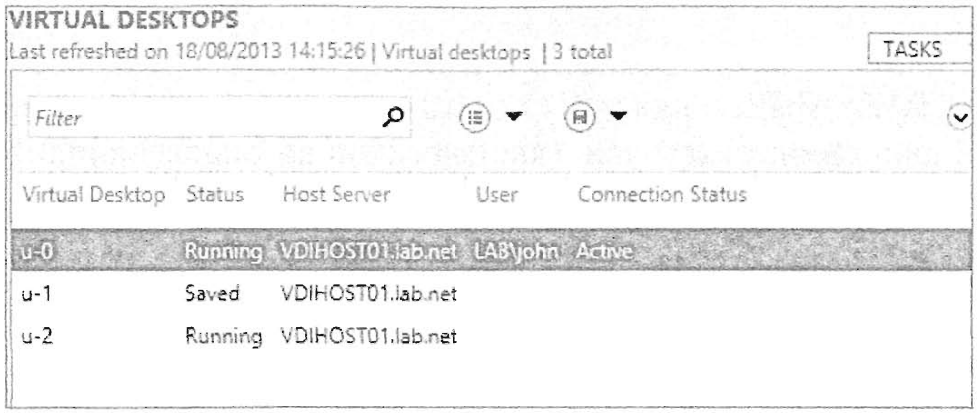


Рис. 29.22. Кто в систему какой виртуальной машины вошел

В среде Windows Server 2012 R2 работают 73 командлета. С полным списком и справочной информацией по всем этим командлетам можно ознакомиться по ссылке:

`http://technet.microsoft.com/en-us/library/jj215451.aspx`

Диспетчер лицензирования удаленных рабочих столов

Хотя вам предоставляется льготный период, в течение которого службы RDS будут нормально функционировать, по его окончании службы RDS перестанут принимать подключения, если лицензирование не сконфигурировано. Льготный период длится 120 дней или до момента, когда сервер лицензирования выпустит первую постоянную лицензию RDS CAL, в зависимости от того, что случится раньше.

Как уже было указано, вы можете выбрать между индивидуальными лицензиями для устройств и индивидуальными лицензиями для пользователей. Чтобы можно было устанавливать лицензии, сначала необходимо активировать сервер лицензирования.

После конфигурирования среды RDS понадобится сконфигурировать сервер лицензирования. Диспетчер лицензирования удаленных рабочих столов (RD Licensing Manager) применяется для установки, выпуска и отслеживания доступности лицензий RDS CAL на сервере лицензирования Remote Desktop. Лицензии можно приобретать разнообразными методами в зависимости от отношений вашей компании с Microsoft; различают следующие виды лицензий:

- Enterprise Agreement (Соглашение предприятия)
- Campus Agreement (Соглашение университетского городка)
- School Agreement (Соглашение школы)
- Services Provider License Agreement (Лицензионное соглашение поставщика услуг)
- Other Agreement (Другое соглашение)

При наличии одного из таких соглашений с Microsoft оптимальным способом получения лицензий будет именно оно. Лицензии можно приобрести по каналам розничной торговли в виде лицензионного пакета. Подробная информация о том, как купить лицензии, приведена по следующей ссылке:

`http://www.microsoft.com/en-us/server-cloud/windows-server/buy.aspx`

Сервер лицензирования может находиться на том же сервере, что и сервер RD Session Host. В случае более крупных реализаций Remote Desktop Services с несколькими серверами один сервер лицензирования будет управлять лицензиями для множества серверов RDS.

Более старые серверы лицензирования Terminal Services применяли область обнаружения, чтобы позволить серверам TS находить сервер лицензирования. В установке сервера лицензирования в Windows Server 2012 R2 нет необходимости. Вместо этого вы должны воспользоваться инструментом Remote Desktop Session Host Configuration и указать сервер лицензирования для сервера RD Session Host. Это делается на вкладке Licensing (Лицензирование) диалогового окна RDP-TCP Connections Properties (Свойства подключений RDP-TCP), где идентифицируется тип лицензий RDS CAL, применяемых для данного сервера (индивидуально для устройств или для пользователей).

Сконфигурировать диспетчер лицензирования удаленных рабочих столов можно с помощью описанных ниже действий.

1. Запустите диспетчер лицензирования удаленных рабочих столов, выбрав в меню Start (Пуск) пункт Administrative Tools⇨Remote Desktop Services⇨Remote Desktop Licensing Manager (Администрирование⇨ Службы удаленного рабочего стола⇨Диспетчер лицензирования удаленных рабочих столов).
2. Щелкните на значке “плюс”, чтобы раскрыть узел All Servers (Все серверы).

   Вы увидите свой сервер помеченным красным кружочком с белым символом X внутри.
3. Выберите свой сервер; щелкните на его значке правой кнопкой мыши и выберите в контекстном меню пункт Activate Server (Активировать сервер).
4. Просмотрите информацию на экране приветствия мастера и щелкните на кнопке Next (Далее).
5. На экране Connection Method (Метод подключения) примите вариант, предложенный по умолчанию — Automatic Connection (Recommended) (Автоматическое подключение (рекомендуется)).

   Используйте этот метод, если у сервера RDS имеется доступ в Интернет. В противном случае подключиться можно с помощью другого компьютера через Интернет или по телефонной линии.
6. Щелкните на кнопке Next.

   Появится экран Company Information (Информация о компании).
7. Введите свое имя, фамилию, название компании и страну.

   Эта информация используется, когда вы нуждаетесь в помощи от Microsoft.
8. Щелкните на кнопке Next.
9. Введите дополнительную информацию, запрашиваемую на экране Optional Company Information (Необязательная информация о компании). Щелкните на кнопке Next.

Отобразится диалоговое окно с индикатором хода работ. Сервер подключается к Microsoft Clearinghouse и активируется. По завершении этой процедуры появится экран завершения.

10. Снимите отметку с флажка Start Install Licenses Wizard Now (Запустить мастер установки лицензий) и щелкните на кнопке Finish (Готово).

    В этот момент сервер лицензирования активирован, но не установлено ни одной лицензии RDS CAL.

Установка индивидуальных лицензий для устройств или для пользователей

Может потребоваться возврат в консоль Remote Desktop Session Host Configuration с целью установки режима лицензирования для удаленных рабочих столов. После запуска этой консоли дважды щелкните на режиме лицензирования удаленных рабочих столов, чтобы получить доступ к странице свойств. В зависимости от типа приобретенных лицензий выберите переключатель Per Device или Per User и введите имя сервера лицензирования.

---

11. Щелкните правой кнопкой мыши на значке своего сервера и выберите в контекстном меню пункт Install Licenses (Установить лицензии).

    Это приведет к запуску мастера для установки ваших лицензий. В зависимости от типа приобретенных лицензий и от того, у кого вы их купили, мастер может следовать множеством путей.

Резюме

Ограничьте максимальное количество соединений. Вы можете изменить режим лицензирования сервера, чтобы гарантировать соответствие лицензионному соглашению и существующим назначениям.

Контрольный вопрос. Вы хотите знать, в каком режиме лицензирования находится сервер. Что вы предпримете?

Добавьте приложения к серверу RD Session Host. После добавления роли RDS и конфигурирования сервера RD Session Host можно приступить к добавлению приложений, чтобы сделать их доступными этому серверу.

Контрольный вопрос. Ваша компания приобрела приложение, которое поддерживает многопользовательский доступ. Вы хотите установить его на сервере RD Session Host. Что потребуется сделать?

Добавьте приложения RemoteApp для доступа через веб. Приложения RemoteApp могут быть сконфигурированы так, чтобы пользователи могли получать доступ к ним из веб-браузера. Пользователям просто необходимо обратиться к подходящей странице и выбрать приложение для запуска.

Контрольный вопрос. Предположим, что вы уже сконфигурировали среду для поддержки приложений RemoteApp. Теперь вы хотите добавить приложение RemoteApp. Что потребуется сделать?

Глава 30

Мониторинг Windows Server 2012 R2

О существовании проблемы лучше всего знать до того, как она проявится. К миру информационных технологий это относится в той же степени, как и ко всему остальному. Если вы хотите знать о потенциальных проблемах, касающихся серверов, до их перерастания в полномасштабный кризис, необходимо позаботиться о мониторинге серверов.

С помощью небольшого объема упреждающего мониторинга и корректно подобранного набора инструментов можно выявлять мелкие ошибки и негативные тенденции перед тем, как они превратятся в серьезные проблемы.

В этой главе мы сначала обсудим ряд базовых инструментов, встроенных в Windows Server 2012 R2, которые помогают получить представление о любых ошибках или проблемах с производительностью. Этими инструментами мониторинга являются консоль диспетчера серверов (Server Manager), анализатор передового опыта (Best Practices Analyzer), средство просмотра событий (Event Viewer), монитор производительности (Performance Monitor) и монитор ресурсов (Resource Monitor). Когда вы научитесь пользоваться этими инструментами, мы поговорим о двух дополнительных (и малоизвестных), сторонних инструментах, PAL и PerfView, которые можно применять для углубленного анализа производительности. Наконец, мы обсудим решение мониторинга, рекомендованное Microsoft — диспетчер операций системного центра 2012 R2 (System Center 2012 R2 Operations Manager). Мы покажем, как это решение может помочь вам быстро выяснить первопричину проблем с рабочими нагрузками сервера Windows Server 2012 R2.

В этой главе вы изучите следующие темы:

- использование диспетчера серверов для мониторинга нескольких серверов;
- работа с Event Viewer;
- исследование монитора производительности;
- исследование инструментов PAL и PerfView;
- ознакомление с диспетчером операций системного центра 2012 R2.

Использование диспетчера серверов для мониторинга нескольких серверов

Новая консоль диспетчера серверов в Windows Server 2012 R2 предлагает готовое решение мониторинга и проверки работоспособности локальной и удаленной серверной инфраструктуры. В разделе "Диагностика ролей и компонентов" главы 2 вы узнали, как с помощью диспетчера серверов проводить мониторинг отдельно взятого сервера и связанных с ним ролей. В данном разделе мы тщательно разберем эту информацию и обсудим вопросы применения диспетчера серверов для мониторинга нескольких серверов и закрепленных за ними ролей — причем все это в одной центральной консоли.

Добавление серверов для управления

Чтобы добавить дополнительные серверы для управления и мониторинга посредством диспетчера серверов, выполните следующие шаги.

1. Войдите в систему компьютера Windows Server 2012 R2 от имени учетной записи с административными разрешениями.
2. В окне диспетчера серверов выберите пункт меню Dashboard (Инструментальная панель).
3. На вкладке Quick Start (Быстрый запуск) щелкните на ссылке Add other servers to manage (Добавить другие серверы для управления).
4. На вкладке Active Directory диалогового окна Add Servers (Добавление серверов) выполните фильтрацию по местоположению и операционной системе; затем либо введите начало имени для серверов, которые хотите добавить, либо просто щелкните на кнопке Find Now (Найти сейчас), чтобы отобразить все серверы для выбранных вами вариантов.
5. Дважды щелкните (или щелкните при нажатой клавише <Ctrl>) на каждом сервере, который необходимо добавить в столбец Selected (Выбранные), и щелкните на кнопке OK.

   Теперь внутри представления Dashboard вы должны увидеть значение Servers total (Всего серверов) в области Roles and Server Groups (Роли и группы серверов), которое отражает количество серверов, добавленных для мониторинга.
6. В окне диспетчера серверов выберите в меню View (Вид) пункт 75%, чтобы увидеть сжатое представление всех ролей из выбранных серверов, которые теперь подвергаются мониторингу (рис. 30.1), с ролью каждого отдельно взятого сервера и его состоянием работоспособности (зеленый цвет — работоспособен, красный цвет — неработоспособен).

Создание группы серверов для мониторинга

Когда вы добавляете к консоли диспетчера серверов несколько серверов, каждая роль сервера отображается в сегментированном представлении, как было показано на рис. 30.1. Однако вам может понадобиться видеть объединенное состояние работоспособности для общих ролей на множестве серверов, и как раз здесь пригодятся группы серверов в диспетчере серверов.

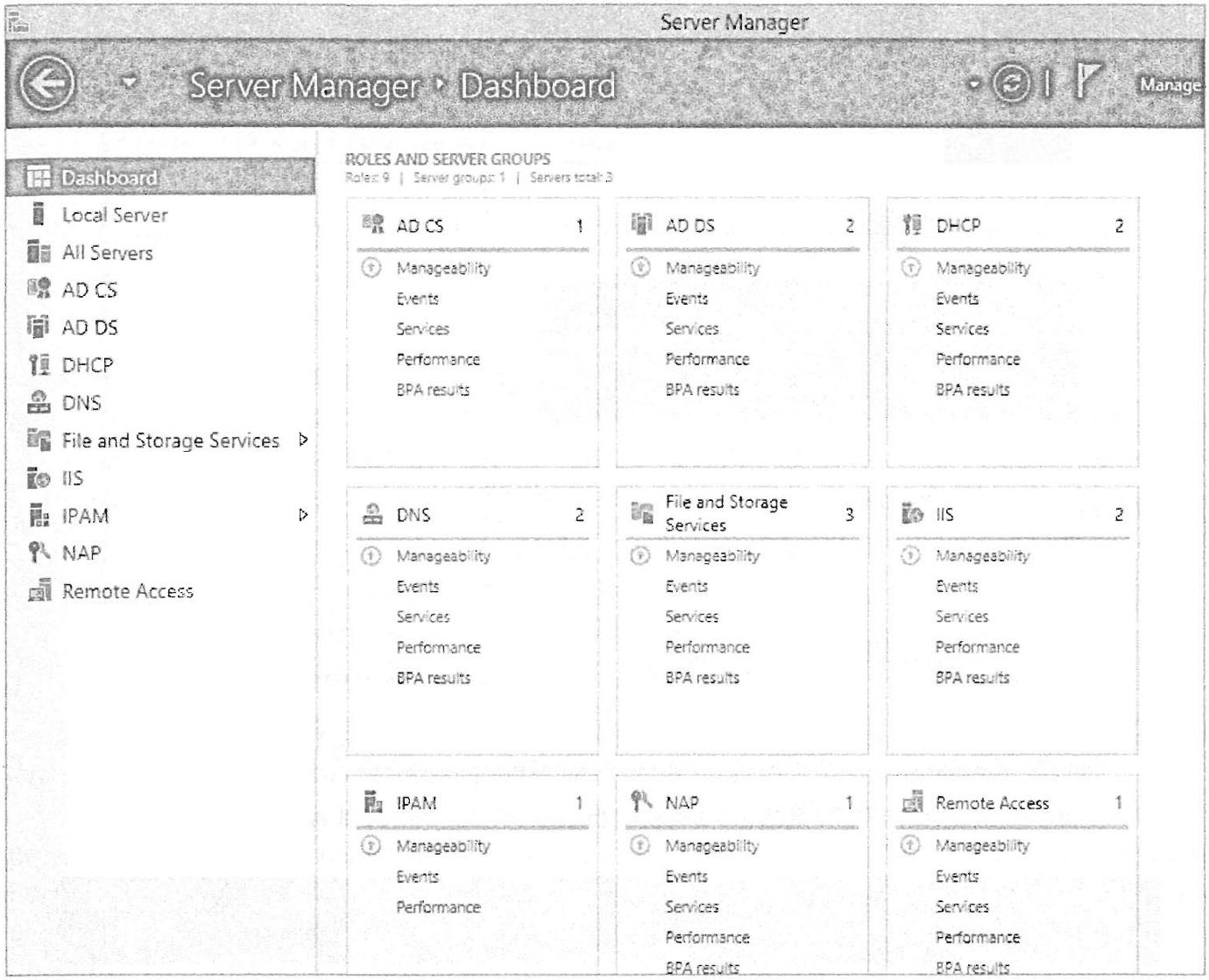


Рис. 30.1. Мониторинг множества серверов

Чтобы создать группу серверов, включающую все серверы, для которых необходимо проводить мониторинг из консоли, выполните описанные ниже действия.

1. Войдите в систему компьютера Windows Server 2012 R2 от имени учетной записи с административными разрешениями.
2. В окне диспетчера серверов выберите пункт меню Dashboard (Инструментальная панель).
3. На вкладке Quick Start (Быстрый запуск) щелкните на ссылке Create a server group (Создать группу серверов).
4. В диалоговом окне Create Server Group (Создание группы серверов) введите в поле Server Group Name (Имя группы серверов) имя, которое должно быть назначено новой группе серверов. На вкладке Server Pool (Пул серверов), Active Directory, DNS или Import (Импортирование) выберите несколько серверов для добавления в эту группу (мы использовали вкладку Server Pool, как показано на рис. 30.2) и щелкните на кнопке OK.

Теперь в представлении Dashboard можно видеть новую группу серверов, которая отображает свернутое состояние работоспособности всех содержащихся внутри нее серверов (рис. 30.3).

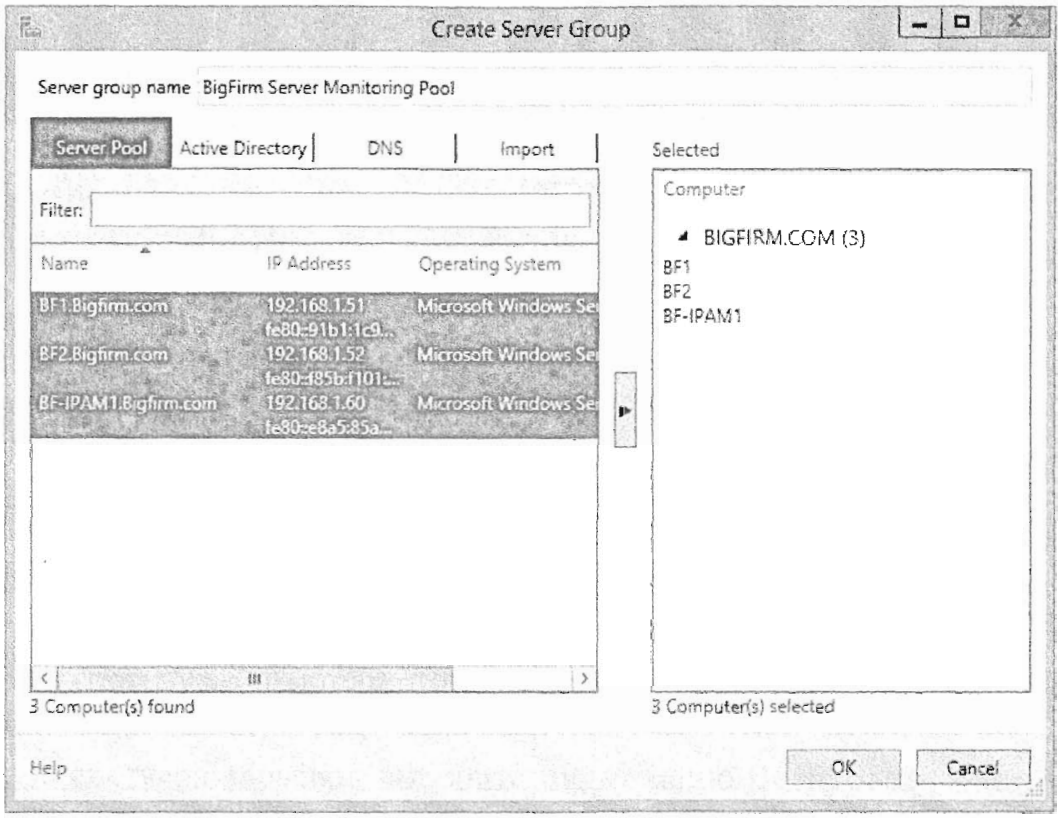


Рис. 30.2. Добавление нескольких серверов в группу

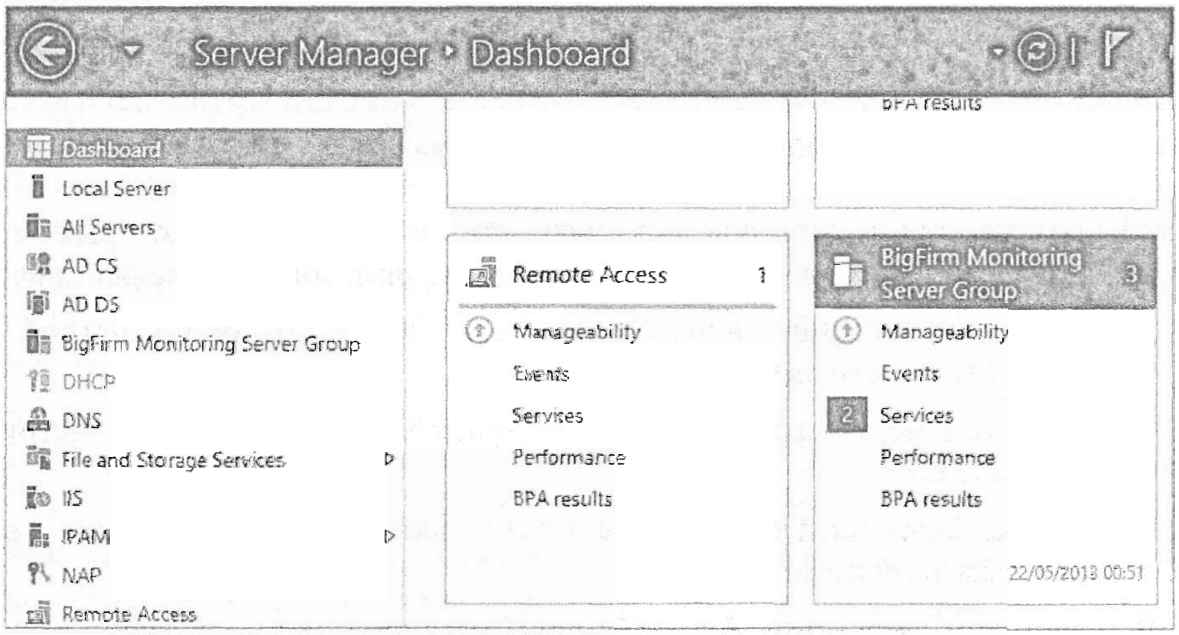


Рис. 30.3. Новая группа серверов

Мониторинг с использованием групп серверов

Когда вы сконфигурировали нужные группы серверов в консоли диспетчера серверов, то можете быстро идентифицировать наличие проблемы с любым из серверов в этих группах, касающейся перечисленных ниже ключевых областей.

- **Manageability (Управляемость).** Здесь вы можете видеть некоторые стандартные метрики мониторинга, которые определяют, удовлетворен ли критерий ошибки управляемости сервера.

- **Events (События).** Эта область предоставляет централизованное представление всех событий типа Critical (Критическое), Error (Ошибка) и Warning (Предупреждение), которые происходят на серверах.
- **Services (Службы).** Здесь приводится обзор служб, которые функционируют (или не функционируют) на выбранных серверах.
- **Performance (Производительность).** В этой области отображаются результаты мониторинга таких ресурсов, как центральный процессор и оперативная память, на выбранных серверах.
- **BPA Results (Результаты BPA).** Эта область предоставляет разные уровни безопасности (Information, Warning и Error), которые генерируются после выполнения анализатора передового опыта (Best Practices Analyzer — BPA).

Рис. 30.4. Группа серверов, с которой связаны проблемы

Взглянув на группу серверов, созданную в предыдущем разделе, можно заметить, что имеется несколько проблем, которые требуют решения (рис. 30.4).

Щелчок на одной из выделенных областей с проблемами, позволит быстро определить, на каком из серверов возникли проблемы и какие причины вызывают появление предупреждений в консоли диспетчера серверов. Если щелкнуть на области Services группы BigFirm Monitoring Server Group, откроется диалоговое окно Services Detail View (Детальное представление служб), где мы можем четко видеть проблему с двумя службами, остановленными на двух разных серверах (рис. 30.5).

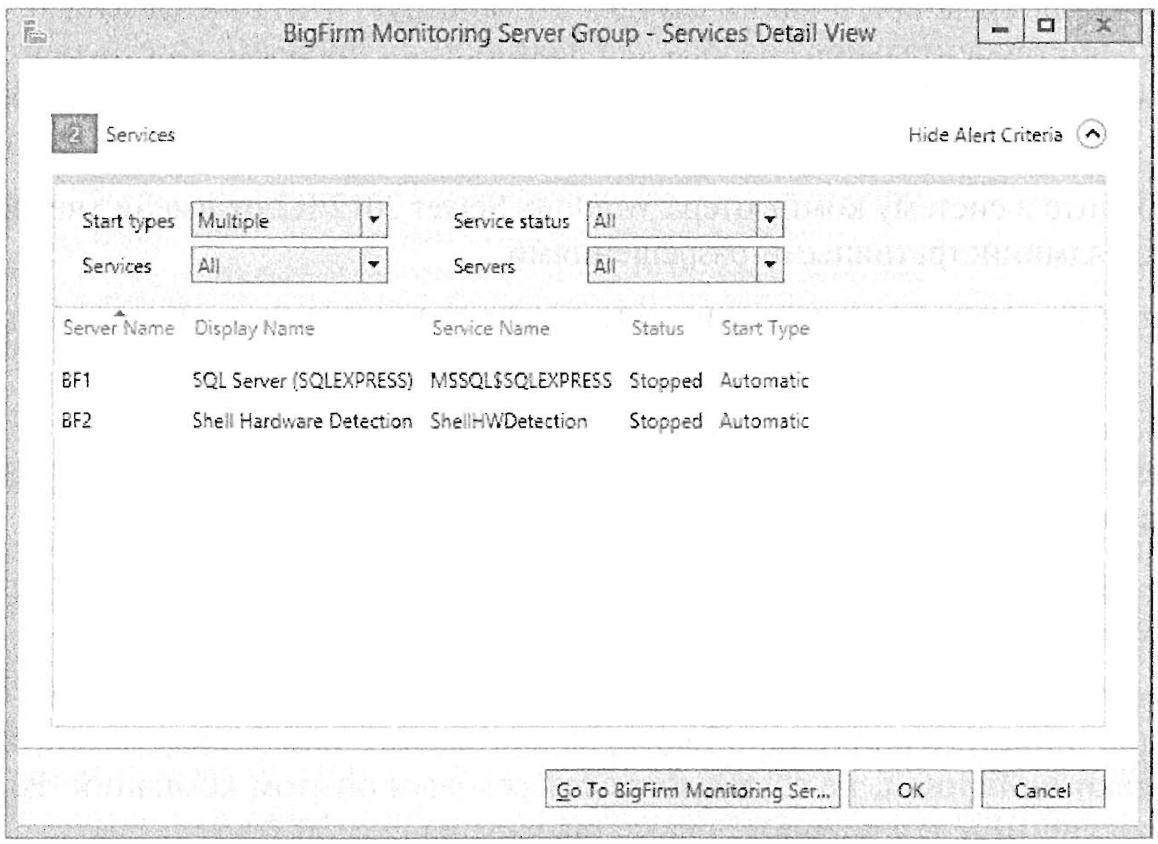


Рис. 30.5. Идентификация проблемы

Представление группы серверов

Если вместо представления Dashboard в диспетчере серверов вы хотите получить более детализированное представление для своей группы серверов, просто щелкните на имени этой группы в навигационной панели слева. Появится прокручиваемое окно, содержащее несколько разделов для каждой из обсуждавшихся ранее ключевых областей. В каждом разделе присутствует кнопка Tasks (Задачи), которая в зависимости от выбранной области будет предоставлять доступ к разным задачам.

Использование анализатора передового опыта

На протяжении нескольких лет сотрудники Microsoft, входящие в состав группы Solution Accelerator (Ускоритель решений), периодически выпускали инструменты анализатора передового опыта (Best Practices Analyzer), служившие дополнением некоторых ключевых продуктов. Одним из самых известных таких инструментов был Microsoft Exchange BPA (ExBPA), который позволял системным администраторам и консультантам со всего мира удостоверяться в том, что их среды сконфигурированы оптимально и в соответствии с рекомендациями Microsoft, основанными на передовом опыте. Поначалу BPA были инструментами, отдельными от приложений, но с учетом огромного успеха ExBPA в Microsoft приняли решение включать BPA в состав Windows Server (начиная с Windows Server 2008), чтобы можно было анализировать каждую роль, развернутую в операционной системе. Важное преимущество такого подхода заключается в том, что инструменты BPA обновляются посредством Windows Update тем же способом, что и ОС, обеспечивая наличие актуальных рекомендаций, когда они понадобятся.

Тот факт, что с появлением Windows Server 2012 R2 в вашем распоряжении оказывается настолько много новых ролей и богатая функциональность, обусловливает важность понимания, в каких случаях эти инструменты BPA следует применять как часть инструментального набора для диагностики проблем. Инструменты BPA в Windows Server 2012 R2 можно легко запускать из консоли диспетчера серверов для каждой конкретной роли. Ниже описано, как это делать.

1. Войдите в систему компьютера Windows Server 2012 R2 от имени учетной записи с административными разрешениями.

2. Откройте диспетчер серверов и щелкните на интересующей роли в навигационной панели слева. В этом примере мы будем использовать роль DNS.

3. Выполните прокрутку до области Best Practices Analyzer (Анализатор передового опыта), щелкните на кнопке Tasks (Задачи) и выберите пункт Start BPA Scan (Начать сканирование BPA), как показано на рис. 30.6.

4. Выберите сервер (или несколько серверов), которые хотите просканировать, и щелкните на кнопке Start Scan (Начать сканирование).

После завершения сканирования будут выведены результаты сканирования, позволяющие вникнуть в суть ошибок, предупреждений или информации, которые, как считают в Microsoft, не согласуются с передовым опытом компании. Результаты сканирования BPA для роли DNS представлены на рис. 30.7.

Рис. 30.6. Запуск анализатора передового опыта

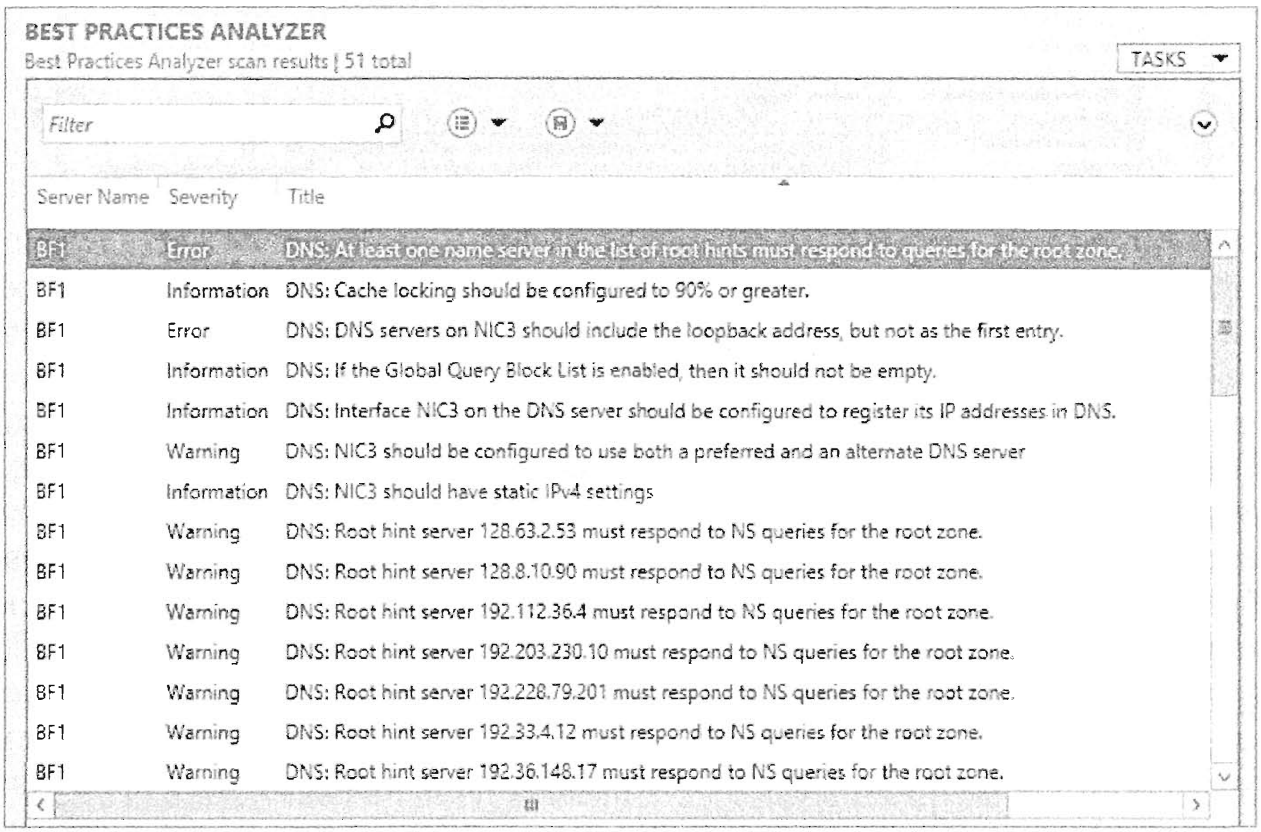


Рис. 30.7. Результаты сканирования BPA

Мониторинг системы с помощью Event Viewer

Средство просмотра событий (Event Viewer) в Windows Server 2012 R2 является одним из важнейших инструментов, применяемых для мониторинга системы. Часто он оказывается одним из первых инструментов, к которым вы обращаетесь, когда обнаруживаете, что на сервере имеется проблема, но средство Event Viewer можно также использовать для упреждающего мониторинга серверов. Средство просмотра событий может помочь быстро выявить источник проблемы или, по крайней мере, получить достаточный объем информации для понимания, в каком направлении продолжать поиск.

Запустить Event Viewer можно из начального экрана Windows Server 2012 R2, набрав **eventvwr** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.

На рис. 30.8 показано окно Event Viewer (Просмотр событий) и несколько журналов событий, с которыми вам придется сталкиваться на практике.

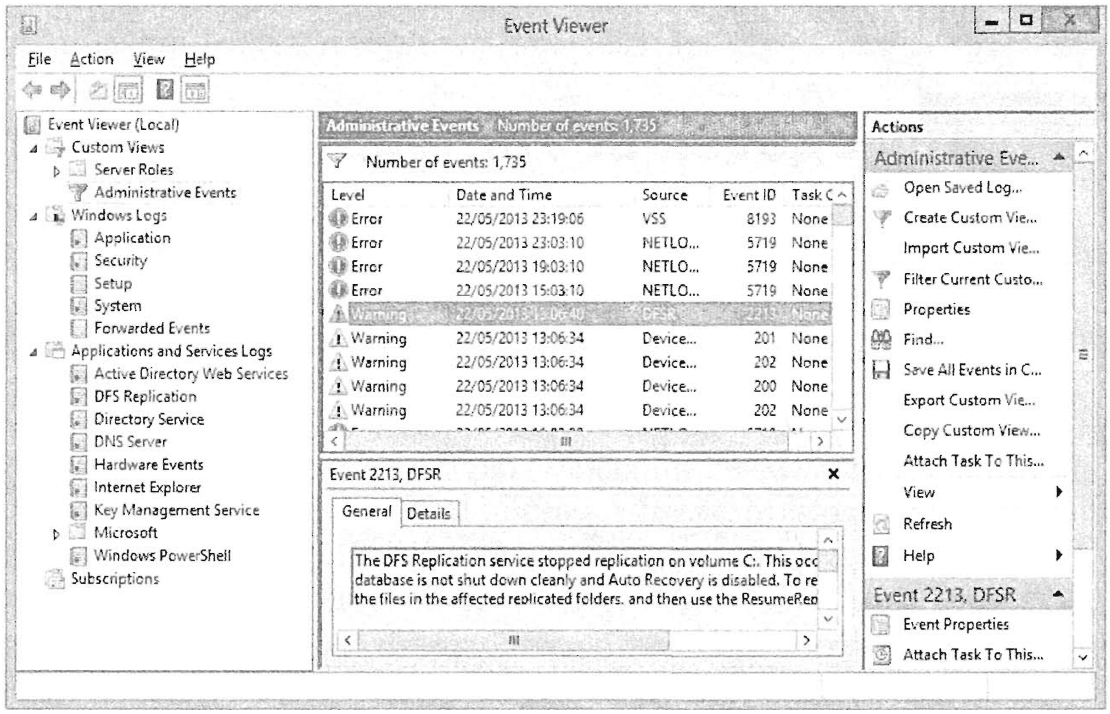


Рис. 30.8. Окно Event Viewer

В левой панели перечислены все журналы событий, доступные для выбора. В центральной панели отображаются события из выбранного журнала, а также информация о выбранном событии в нижней части. В правой панели представлены все действия, которые можно выполнить для выбранного журнала или события.

Обратите внимание, что не все журналы используются постоянно, а некоторые из них могут применяться только для специфичной цели. В качестве простого примера, журнал Setup (Установка) используется для регистрации событий только во время установки. Если этот журнал очищен, вы не больше не увидите в нем какие-то события. Просмотрев содержимое некоторых из таких нечасто применяемых журналов, вы можете обнаружить, что они пусты, но это вовсе не указывает на наличие проблемы.

Просмотр события

Двойной щелчок на любом событии в центральной панели приводит к отображению диалогового окна с подробной информацией об этом событии. Детали многих событий содержат полезные сведения, которые помогают выявить и распознать причину возникновения ошибки. Пример события ошибки показан на рис. 30.9.

На рис. 30.9 информация о событии, приведенная на вкладке General (Общие), четко указывает на возникновение проблемы с установлением безопасного сеанса с помощью контроллера домена в домене ECOAST. Вдобавок здесь приводятся рекомендации по устранению этой проблемы, а также дополнительные сведения о работе безопасного сеанса.

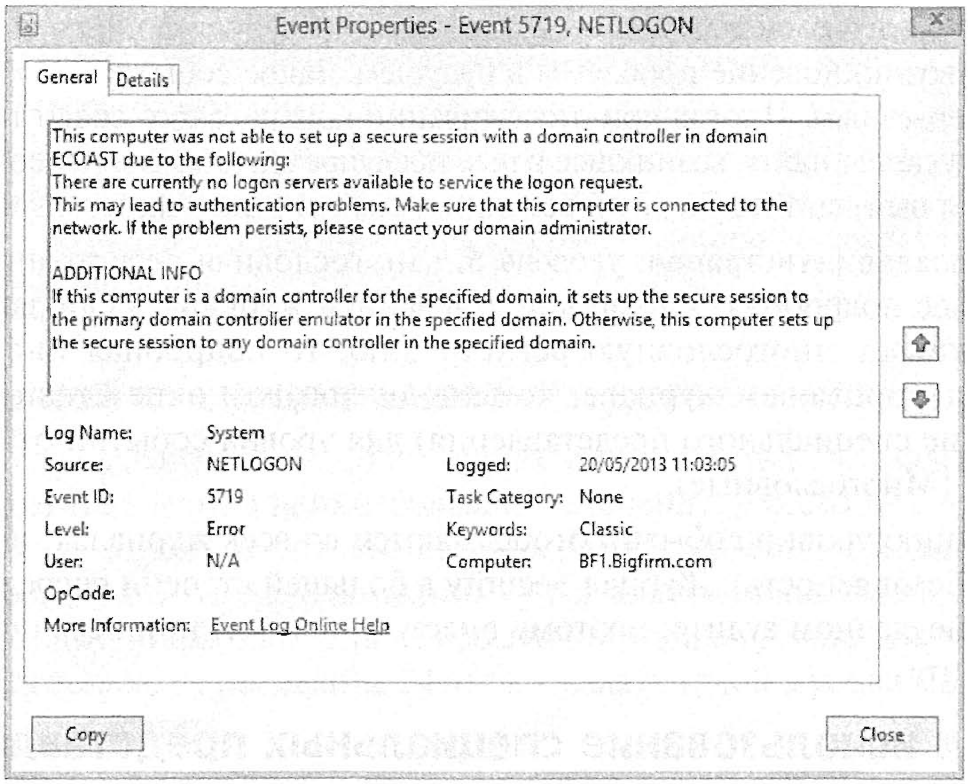


Рис. 30.9. Диалоговое окно с информацией об ошибке, доступное в средстве Event Viewer

На вкладке General можно также щелкнуть на ссылке Event Log Online Help (Онлайновая справка по журналу событий). Если у сервера имеется доступ в Интернет, он отправит информацию об ошибке и отобразит страницу Microsoft TechNet, связанную с этой ошибкой. Для ряда распространенных ошибок такая онлайновая справка оказывается весьма полезной.

Еще одним удобным средством является возможность щелкнуть на кнопке Copy (Копировать) и скопировать всю подробную информацию в буфер обмена. Затем эту информацию можно вставить в документ для последующего просмотра либо в журнал или базу данных диагностики проблем.

Уровни событий

События классифицируются по уровням, с которыми связаны имена и номера. Просматривая события, вы можете видеть их уровни, идентифицируемые именами и значками, но в случае конфигурирования специальных представлений можно использовать номера уровней из XML-файла.

- **Информационные события: уровень 0 и уровень 4.** Эти записи применяются для указания на произошедшее изменение или на успешное завершение операции. Значок информационного события выглядит как буква *i* в кружочке.
- **Критические события: уровень 1.** Критическое событие — это событие, из которого приложение или компонент не может восстановиться автоматически. Критические события являются наиболее серьезными. Значок критического события выглядит как белая буква *x* в красном кружочке.
- **События ошибок: уровень 2.** События ошибок указывают на возникновение проблемы, внешней по отношению к приложению или компоненту, которая может повлиять на функциональность данного приложения или компонента. Значок события ошибки выглядит как белый восклицательный знак в красном кружочке.

- **События предупреждений: уровень 3.** События предупреждений указывают на возможное возникновение проблемы в будущем. Такое событие не обязательно является серьезным. Иногда при отслеживании критического события или события ошибки удается найти возникшее ранее предупреждение. Значок события предупреждения выглядит как черный восклицательный знак в желтом треугольнике.
- **Многословная регистрация: уровень 5.** Многословная регистрация предоставляет более подробную информацию в записи журнала. Если запись журнала поддерживает многословную регистрацию, то подробная информация будет зафиксирована в журнале, когда в диалоговом окне Create Custom View (Создание специального представления) для уровня событий отмечен флажок Verbose (Многословные).

По умолчанию уровни событий отображаются во всех журналах, исключая журнал Security (Безопасность). Журнал Security в большей степени сосредоточен на успешном или неудачном аудите, поэтому вместо уровней в нем перечислены ключевые слова аудита.

Создание и использование специальных представлений

Часто при просмотре журналов вы ищете специфичные события или, во всяком случае, события, связанные с конкретной проблемой. Узел Custom Views (Специальные представления) в окне Event Viewer предлагает заранее определенные специализированные представления событий и позволяет создавать собственные представления. Данная возможность весьма удобна, поскольку не требует воссоздания представления каждый раз, когда необходимо просмотреть эти события.

Некоторые специальные представления созданы автоматически.

- **Server Roles (Серверные роли).** Каждый раз, когда вы добавляете серверную роль, автоматически создается связанное с ней специальное представление. Например, если вы повышаете сервер до контроллера домена, в узел Server Roles добавляется специальное представление под названием Active Directory Domain Services (Службы домена Active Directory), чтобы отобразить системные события для служб Active Directory Domain Services.
- **Administrative Events (Административные события).** Специальное представление Administrative Events отображает критические события, а также события ошибок и предупреждений из всех административных журналов. Другими словами, это специальное представление показывает все события кроме информационных. Данное представление включает базовые административные журналы (Application (Приложения), Security (Безопасность) и System (Система)), встречающиеся в любой системе. Оно также содержит журналы в узле Applications and Services Logs (Журналы приложений и служб) и некоторые из журналов в узле Applications and Services Logs⇨Microsoft⇨Windows.

  Когда сервер сконфигурирован с новой ролью или компонентом и добавлены дополнительные журналы, специальное представление Administrative Events модифицируется для учета этих дополнительных журналов.

Хотя вы не можете изменять эти предварительно определенные специальные представления, вы можете создавать собственные специальные представления и модифицировать их. В следующем разделе будет показано, как создавать собственные специальные представления, допускающие внесение изменений.

Предварительно определенные специальные представления фильтроваться не могут

Ни специальное представление Administrative Events, ни любое из специальных представлений для серверных ролей фильтроваться не могут. Если вы хотите фильтровать эти журналы, то должны сначала создать копию соответствующего специального представления.

Создание копии специального представления

Вам может подходить какое-то из заранее определенных специальных представлений, но вы хотите внести в него небольшое изменение. Вместо того чтобы начинать с нуля, вы можете создать копию специального представления и модифицировать ее.

Например, вы хотите использовать журнал Administrative Events в качестве шаблона, но добавить информационные события и отфильтровать его, чтобы отображались события только за последние 24 часа. Создать такой журнал можно с помощью описанных ниже шагов.

1. Запустите средство Event Viewer из начального экрана Windows Server 2012 R2, набрав **eventvwr** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Щелкните правой кнопкой мыши на специальном представлении Administrative Events (Административные события) и выберите в контекстном меню пункт Copy Custom View (Копировать специальное представление).
3. Измените имя на `Today's Core Log Events`.
4. Щелкните на кнопке New Folder (Создать папку). В текстовом поле Name (Имя) введите `My Custom Views` и щелкните на кнопке OK.
5. Щелкните на кнопке OK, чтобы создать копию специального представления Administrative Events в папке `My Custom Views`.
6. Щелкните правой кнопкой мыши на журнале Today's Core Log Events и выберите в контекстном меню пункт Properties (Свойства).
7. Щелкните на кнопке Edit Filter (Редактировать фильтр).

   Обратите внимание, что свойства совпадают со свойствами исходного специального представления Administrative Events, но их можно редактировать.
8. В раскрывающемся списке Logged (Зарегистрированные в журнале) и выберите вариант Last 24 Hours (Последние 24 часа).
9. В области Event Level (Уровень событий) отметьте флажок Information (Информационные).

   Флажки Critical (Критические), Warning (Предупреждения) и Error (Ошибки) уже должны быть отмечены.
10. Щелкните на раскрывающемся списке Event Logs (Журналы событий).

    Флажок Application and Services Logs (Журналы приложений и служб) отображается серым цветом, указывая на то, что некоторые журналы выбраны.

11. Щелкните на флажке Application and Services Logs один раз, чтобы выбрать все журналы. Щелкните на нем еще раз, чтобы снять с него отметку, в результате чего снимутся отметки со всех журналов.

    Вы должны видеть на экране примерно то, что показано на рис. 30.10. Здесь был произведен щелчок на значке "плюс" для узла Application and Services Logs, чтобы отобразить все доступные журналы, но выбрано только три журнала в узле Windows Logs (Журналы Windows).

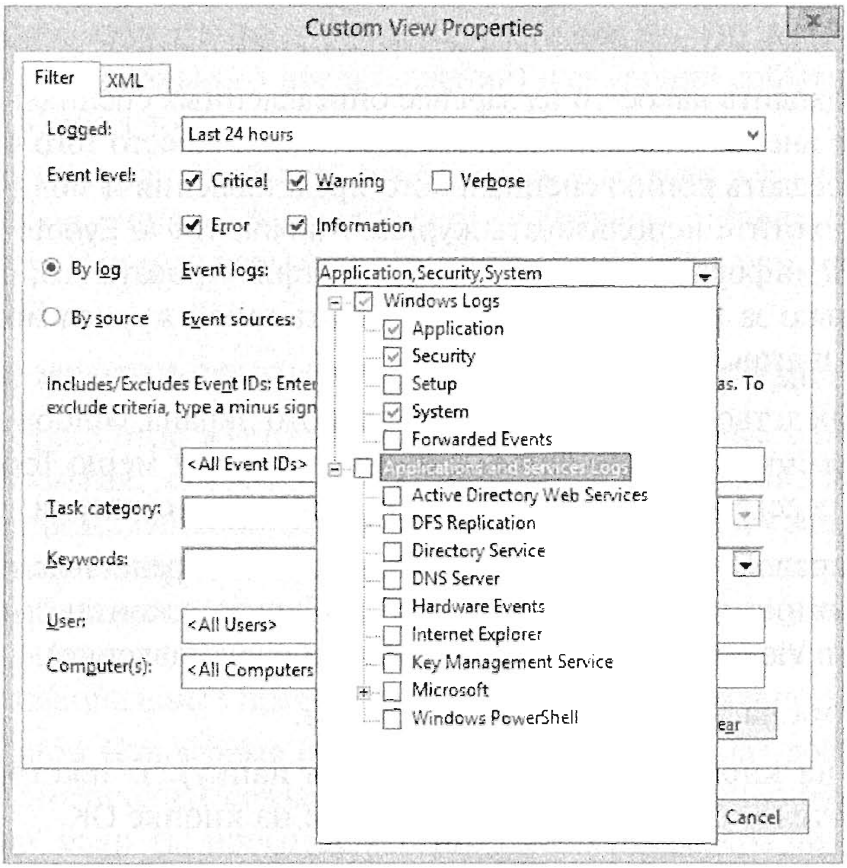


Рис. 30.10. Изменение специального представления

12. Два раза щелкните на кнопке OK, чтобы сохранить свое новое специальное представление.

Создание нового специального представления

Специальные представления можно также создавать с нуля. Это удобно при проведении диагностики специфичных проблем. Например, может понадобиться мониторинг запуска и останова служб.

Чтобы создать специальное представление, которое позволит быстро просмотреть все события, касающиеся запуска или останова какой-то службы, выполните следующие действия.

1. Запустите средство Event Viewer из начального экрана Windows Server 2012 R2, набрав **`eventvwr`** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Щелкните правой кнопкой мыши на узле Custom Views (Специальные представления) и выберите в контекстном меню пункт Create Custom View (Создать специальное представление).

3. В области Event Level (Уровень событий) отметьте флажки Critical (Критические), Warning (Предупреждения), Error (Ошибки) и Information (Информационные).
4. Выберите переключатель By Source (По источнику).
5. Щелкните на раскрывающемся списке Event Sources (Источники событий), выполните прокрутку вниз и отметьте флажки Service Control Manager (Диспетчер управления службами) и Service Control Manager Performance Diagnostic Provider (Поставщик диагностики производительности диспетчера управления службами). Обратите внимание, что два журнала выбраны автоматически: System и Microsoft-Windows-Services/Diagnostic.
6. Щелкните на кнопке OK. Введите `Monitor Services` в качестве имени специального представления. Щелкните на кнопке OK.

Созданное специальное представление будет отображать только события, связанные с Service Control Manager.

Фильтрация специального представления

Специальные представления можно фильтровать подобно любому обычному журналу событий. Журнал может содержать сотни или даже тысячи событий. Если вас интересует конкретное событие, то его поиск может занять немало времени, но с помощью фильтра круг поиска удастся значительно сузить.

Фильтрация журналов

Хотя в этом разделе рассказывается о том, как фильтровать специальное представление, те же действия применимы для фильтрации любого журнала внутри Event Viewer.

Описанные ниже шаги демонстрируют выполнение фильтрации журнала. При этом используется журнал, созданный ранее в этой главе (по имени `Today's Core Log Events`); тем не менее, данная последовательность действий может служить руководством по фильтрации любого журнала.

1. Запустите средство Event Viewer из начального экрана Windows Server 2012 R2, набрав **`eventvwr`** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Раскройте узел Custom Views (Специальные представления).
3. Выберите ранее созданное специальное представление, например, `Monitor Services`, которое создавалось в предыдущем разделе.
4. Создайте фильтр для отображения разных уровней событий.
   а. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Filter Current Custom View (Фильтровать текущее специальное представление).
   б. В области Event Level (Уровень событий) снимите отметку с флажков Warning (Предупреждения), Error (Ошибки) и Information (Информационные), оставив выбранным только флажок Critical (Критические).
   в. Щелкните на кнопке OK. Теперь журнал будет отображать только критические события.

г. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Clear Filter (Очистить фильтр).

5. Создайте фильтр для отображения специфичных источников событий.
   а. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Filter Current Custom View.
   б. Щелкните на раскрывающемся списке Event Sources (Источники событий) и отметьте флажок Service Control Manager (Диспетчер управления службами). Можете выбирать столько источников событий, сколько пожелаете.

Выбор фильтрации по журналу или по источнику

Переключатели By Log (По журналу) и By Source (По источнику) могут вводить в заблуждение. Переключатели обычно применяются для выбора только одного варианта, поэтому By Log и By Source наталкивают на мысль, что фильтровать допускается либо по журналу, либо по источнику, но в действительности можно использовать оба вида фильтрации.

Когда выбран переключатель By Log, вы можете выбрать журналы событий, а затем сузить поиск, отметив флажки для конкретных источников событий в раскрывающемся списке Event Sources.

Если вы выбрали переключатель By Source и указали какой-то источник событий в раскрывающемся списке Event Sources, то перечень доступных журналов в раскрывающемся списке Event Logs изменится, отображая только журналы, которые включают этот источник событий.

   в. Щелкните на кнопке OK. Теперь журнал будет отображать только события, имеющие отношение к службам.
   г. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Clear Filter.

6. Создайте фильтр для отображения только специфичных идентификаторов событий.
   а. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Filter Current Custom View.
   б. Щелкните в текстовом поле, в котором отображается <All Event IDs> (Все идентификаторы событий).
   в. Введите `7000-7999,8224`, чтобы выбрать событие с идентификатором 8224 и все события с идентификаторами в диапазоне от 7000 до 7999.

Выбор идентификаторов событий

Вы можете выбирать диапазоны идентификаторов событий с использованием дефиса (как в `7000-7999`). Выбрать несколько диапазонов можно, разделяя их запятыми (например, `7000-7999,8050-8059`). Фильтровать для любых конкретных идентификаторов событий можно путем их разделения запятыми (скажем, `7036,7042`). Допускается также комбинировать эти методы (как в случае `7000-7999,8050-8059,8042,636`).

г. Щелкните на кнопке OK, чтобы просмотреть отфильтрованный журнал.

д. Щелкните правой кнопкой мыши на журнале и выберите в контекстном меню пункт Clear Filter.

В приведенных выше действиях фильтр изменяется по конкретным причинам, но в зависимости от потребностей фильтрацию можно осуществлять на основе других критериев.

Экспортирование и импортирование специальных представлений

Не следует забывать об одной интересной особенности — специальные представления, созданные на одном сервере, можно экспортировать, а затем импортировать на другой сервер. Хотя определенно допускается вручную создать нужное специальное представление в другой системе, безошибочное воспроизведение фильтра может быть сопряжено с трудностями или, по крайней мере, требовать немалых затрат времени. Однако процесс экспортирования и импортирования позволит сделать это быстро и точно.

Журналы, основанные на XML

Начиная с Windows Vista, все журналы событий совместно используют инфраструктуру, основанную на XML. Крупное достоинство языка XML связано с тем, что он является общим форматом, предполагающим хранение в простом текстовом файле. Специальные представления экспортируются как XML-файлы и затем могут копироваться подобно любому другому файлу.

Для экспортирования специального представления выполните перечисленные ниже шаги. С их помощью экспортируется заранее определенное специальное представление Administrative Events, но их можно было бы применить для любого специального представления, которые вы создали самостоятельно.

1. Запустите средство Event Viewer из начального экрана Windows Server 2012 R2, набрав **`eventvwr`** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Раскройте узел Custom Views (Специальные представления).
3. Щелкните правой кнопкой мыши на специальном представлении Administrative Events (Административные события) и выберите в контекстном меню пункт Export Custom View (Экспортировать специальное представление).
4. На своем компьютере перейдите к местоположению, где хотите сохранить этот файл. Введите имя этого файла, такое как `ExportedCustomView`, и щелкните на кнопке Save (Сохранить).

Полученный XML-файл можно скопировать на другой сервер или общий ресурс, доступный другому серверу. Его можно даже импортировать на тот же самый сервер, если исходный файл оказался разрушенным.

Для импортирования XML-файла выполните следующие действия.

1. Если средство Event Viewer не открыто, запустите из начального экрана Windows Server 2012 R2, набрав `eventvwr` и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Щелкните правой кнопкой мыши на узле Custom Views (Специальные представления) и выберите в контекстном меню пункт Import Custom View (Импортировать специальное представление).
3. На своем компьютере перейдите к местоположению, где хранится экспортированный XML-файл.
4. Выберите этот XML-файл и щелкните на кнопке Open (Открыть).
5. Введите другое имя для импортируемого представления.

   На рис. 30.11 показано диалоговое окно Import Custom View File (Импорт файла специального представления).

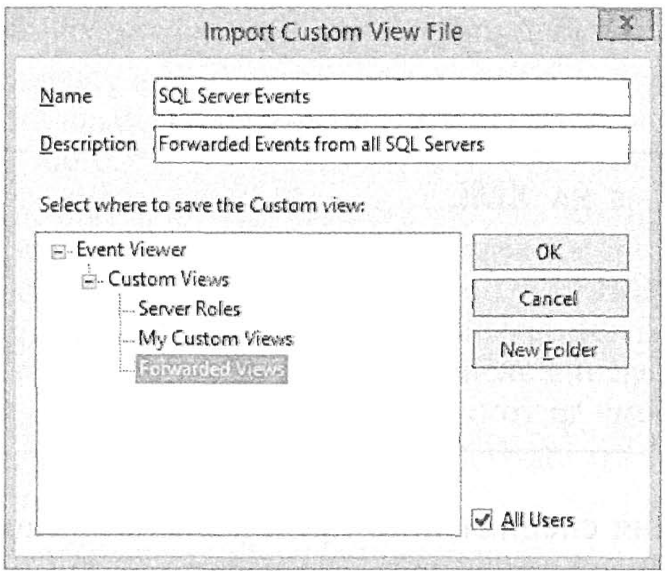


Рис. 30.11. Импортирование специального представления

При желании можете дать этому файлу новое описание. Можете также упорядочить свои специальные представления, создав для них папки.

После импортирования специального представления манипулировать фильтром можно точно так же, как любыми другими специальными представлениями. Изменение специального представления не оказывает влияния на исходный XML-файл, который применялся для импортирования.

Журналы Windows

Журналы Windows — это традиционные журналы, которые были доступными в прошлых версиях Windows, а также журналы Setup и Forwarded Events.

- **Application (Приложения).** Журнал Application используется для регистрации событий из приложений. Разработчик приложения может регистрировать события в этом журнале или создать дополнительный журнал специально для своего приложения. Например, SQL Server будет регистрировать события в журнале Application, а приложение Windows PowerShell будет их записывать в раздел Applications and Services Logs журнала Windows PowerShell.

- **Security (Безопасность).** В журнале Security будут фиксироваться все события аудита. К числу событий аудита относится использование входов в систему, файлов и других объектов, а также любые аналогичные события, включенные администратором. События аудита могут быть как успешными, так и неудачными. В Windows Server 2012 R2 включен аудит определенных событий по умолчанию, поэтому журнал Security будет содержать события, даже если администратор не вносил изменения в настройки аудита.
- **Setup (Установка).** Журнал Setup включает события, относящиеся к установке операционной системы или приложений. Этот журнал включает добавление и удаление любых ролей или компонентов.
- **System (Система).** В журнале System фиксируются события, связанные с операционной системой. Он включает информацию, касающуюся системных драйверов и служб.
- **Forwarded Events (Переадресованные события).** Если включены подписки, то в журнале Forwarded Events будут фиксироваться все события, переадресованные этому компьютеру. Прежде чем события начнут появляться в этом журнале, должны быть сконфигурированы подписки на события.

Журналы приложений и служб

Папка Applications and Services Logs (Журналы приложений и служб) включает журналы для специфичных приложений или компонентов. Представления журналов событий динамически добавляются сюда по мере добавления в Windows Server 2012 R2 ролей и компонентов, а специальные представления помещаются в узел Server Roles (Серверные роли).

Например, когда сервер повышается до контроллера домена, в эту папку добавляются дополнительные журналы, в том числе журнал Active Directory Web Services, журнал DFS Replication и журнал Directory Service.

Журналы этих типов предназначены для предоставления целевому персоналу важной информации, имеющей отношение к делу, а не информации общего характера, которая используется каждым.

Посредством этой папки можно также получить доступ к множеству полезных журналов Windows, к которым исторически невозможно было обратиться из Event Viewer, и вместо этого они были доступны только как текстовые или XML-файлы. Эти журналы находятся в представлении Microsoft\Windows. Журналы в этой папке разделены на четыре категории.

- **Admin (Администратора).** Журналы Admin ориентированы на администраторов и персонал поддержки. Цель их в том, чтобы идентифицировать проблемы и предложить решение, которое администратор может применить для разрешения проблемы.
- **Operational (Операционные).** Журналы Operational используются для анализа или диагностики или наступившего события.
- **Analytic (Аналитические).** Журналы Analytic применяются для регистрации и описания деталей операции программы или компонента. Обычно аналитический журнал содержит большое количество событий, которые фиксируют каждый шаг операции.

- **Debug (Отладки).** Журналы Debug предназначены для использования разработчиками приложений совместно с программами отладки на стадии разработки.

Конфигурирование свойств журнала событий

С каждым журналом событий связана страница свойств, идентифицирующих подробные сведения о журнале. Здесь можно сконфигурировать местоположение журнала, максимальный размер журнала и действие, которое должно предприниматься, когда максимальный размер достигнут.

На рис. 30.12 представлена страница свойств журнала System. Чтобы получить доступ к этой странице, щелкните правой кнопкой мыши на файле журнала и выберите в контекстном меню пункт Properties (Свойства).

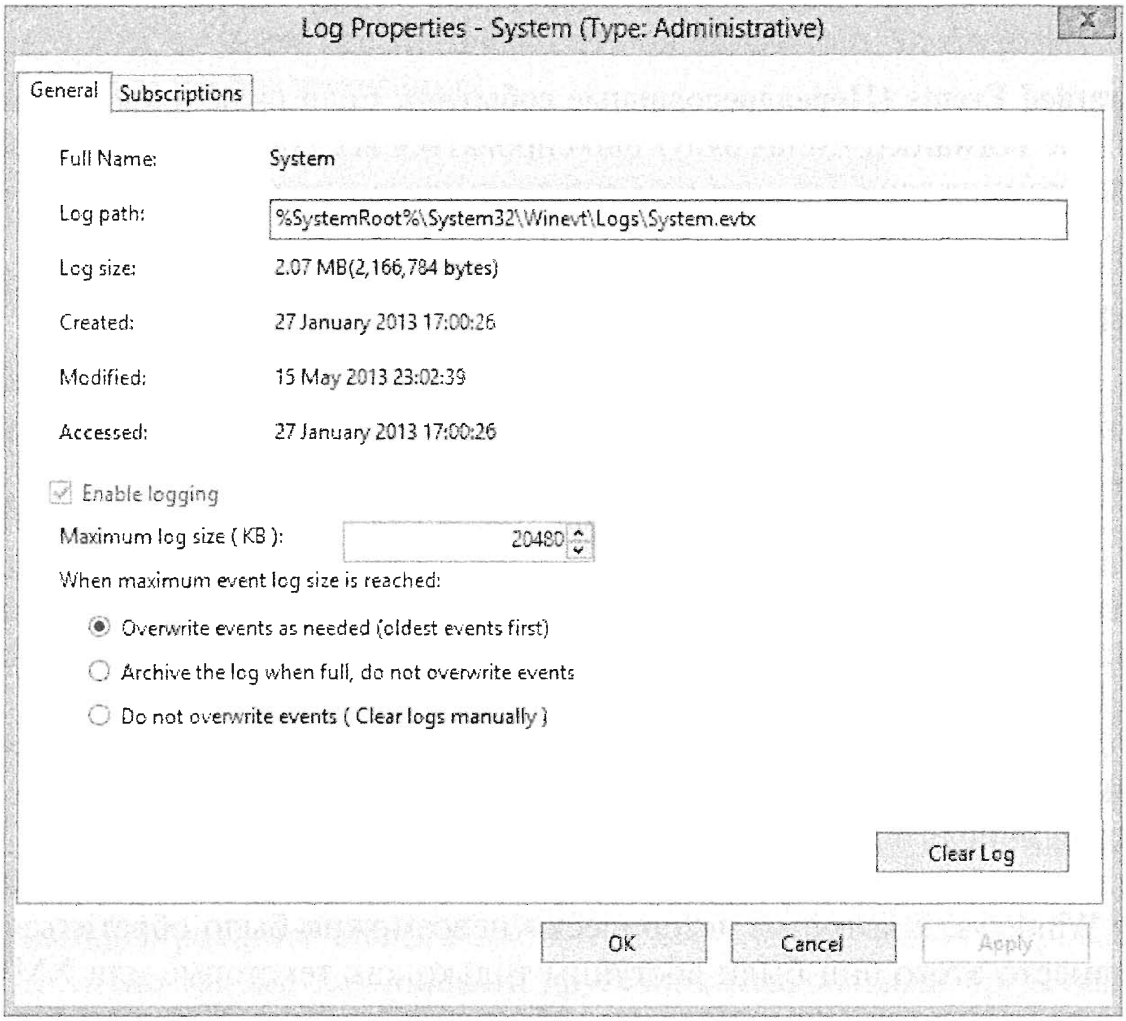


Рис. 30.12. Страница свойств журнала System

Размеры журналов в специальных представлениях не могут быть сконфигурированы

Максимальный размер журнала в специальном представлении конфигурировать нельзя. Причина в том, что специальное представление в действительности не является файлом, а просто отфильтрованной формой одного или нескольких существующих файлов. Каждый раз, когда вы выбираете специальное представление, оно извлекает данные из исходных журнальных файлов.

В поле Log path (Путь журнала) указано местоположение журнального файла. Перенос местоположения журнального файла просто означает ввод в этом поле нового пути.

Интересно отметить, что при переносе журнала существующие события сохраняются в первоначальном месте, а все новые события помещаются в новое место. Однако средство Event Viewer помнит, где находятся первоначальные события, и отображает события с обоих мест. Если после переноса журнала щелкнуть на кнопке Clear Log (Очистить журнал), будет предложено сохранить содержимое файла этого журнала.

На этой странице можно установить максимальный размер журнала. Разные журнальные файлы имеют разные стандартные размеры. Например, размер журнала System по умолчанию составляет 20 Мбайт, а размер журнала Security — около 130 Мбайт. Устанавливайте максимальный размер журнала таким, чтобы он не потреблял слишком много пространства на жестком диске, но вместе с тем, чтобы он позволял видеть важные события.

Наконец, понадобится определить, что делать, когда достигнут максимальный размер журнала. Ниже перечислены соответствующие переключатели.

- Overwrite events as needed (oldest events first) (При необходимости перезаписывать события (сначала самые старые события))
- Archive the log when full, do not overwrite events (Архивировать журнал, когда он полон, не перезаписывать события)
- Do not overwrite events (Clear logs manually) (Не перезаписывать события (очищать журналы вручную))

Сохранение файла журнала

Политики многих организаций предусматривают обязательное архивирование журнальных файлов. В результате архивирования исходный файл сохраняется и может быть просмотрен позже, а новые события не перезаписывают архивированные события.

Щелкните правой кнопкой мыши на файле журнала в Event Viewer и выберите в контекстном меню пункт Clear Log (Очистить журнал); будет предложено сохранить содержимое этого журнального файла. Щелкните на кнопках Save (Сохранить) и Clear (Очистить). После этого можете назначить файлу имя и указать место, где он должен быть сохранен.

Можно также щелкнуть правой кнопкой мыши на файле журнала и выбрать в контекстном меню пункт Save All Events As (Сохранить все события как). Снова будет предоставлена возможность назначить файлу имя и указать место, где его необходимо сохранить. Разница лишь в том, что в этом случае сохраняемые события останутся в журнале, а не будут очищены.

Может быть также выдан запрос на сохранение отображаемой информации. Если вы работаете в двуязычной среде, это обеспечит надлежащее отображение данных на компьютерах с другим языком, установленным по умолчанию.

Отображение сохраненного файла журнала

Средство Event Viewer позволяет открывать любой сохраненный журнал. Щелкните правой кнопкой мыши на любом узле в Event Viewer и выберите в кон-

текстном меню пункт Open Saved Log (Открыть сохраненный журнал). После этого перейдите в место, где хранится интересующий журнал, выберите его и щелкните на кнопке Open (Открыть).

Стандартным местом для отображения сохраненного журнала является новая папка с подходящим именем Saved Logs (Сохраненные журналы). Можете использовать эту папку в качестве места для отображения сохраненного журнала или создать новую папку для отображения новых журналов.

В случае применения стандартного места появится новая папка Saved Logs. Перемещаться между действующим журналом и сохраненным журналом можно с помощью обычных щелчков.

Подписка на события

Подписка на события позволяет сконфигурировать отдельный сервер для сбора копий событий из множества систем. Одиночный сервер, собирающий события, называется *компьютером-сборщиком*, и на него переадресуются события из компьютеров-источников-источников.

На рис. 30.13 показано, как работают компьютеры-источники и компьютер-сборщик с помощью подписок на события. Здесь компьютер-сборщик собирает копии событий, фиксируемых в журналах событий, с нескольких компьютеров-источников.

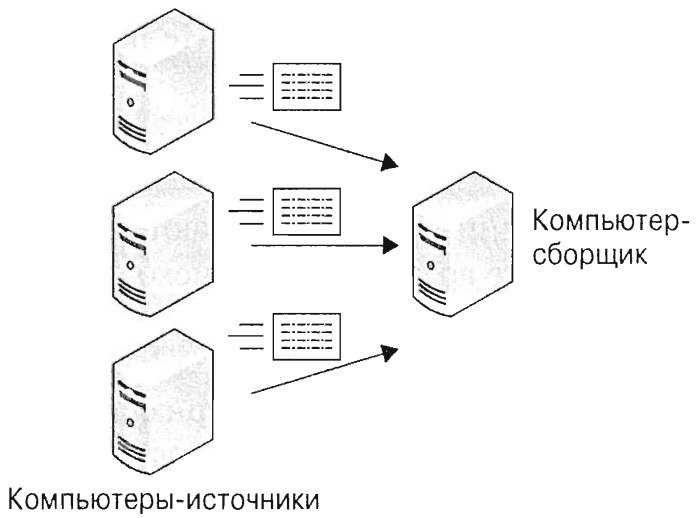


Рис. 30.13. Компьютеры-источники и компьютер-сборщик

Настройка мониторинга событий на центральном сервере позволяет существенно облегчить обслуживание и администрирование множества серверов. Например, предположим, что вы занимаетесь администрированием нескольких экземпляров Microsoft SQL Server. Вы можете создать подписки, чтобы переадресовать события из каждого экземпляра SQL Server на центральный сервер мониторинга.

После того, как компьютер-сборщик захватит события, ими можно манипулировать и фильтровать подобно любым другим событиям на этом компьютере. Для переадресованных событий можно также создавать специальные представления.

Типы подписки

Подписки могут инициироваться либо компьютером-сборщиком, либо компьютерами-источниками. Подписка, инициируемая коллектором, идентифицирует все

компьютеры, от которых коллектор будет принимать события, и извлекает события из этих компьютеров. При подписке, инициируемой компьютерами-источниками, компьютеры-источники помещают события в коллектор.

Подписки, инициируемые коллектором

В подписках, инициируемых коллектором, перечислены все компьютеры, которые будут переадресовывать события (источники событий). Это самый распространенный тип подписки, используемый администраторами серверов.

На рис. 30.14 показана страница конфигурации для подписки, инициируемой коллектором, под названием `CollectSQLEvents`.

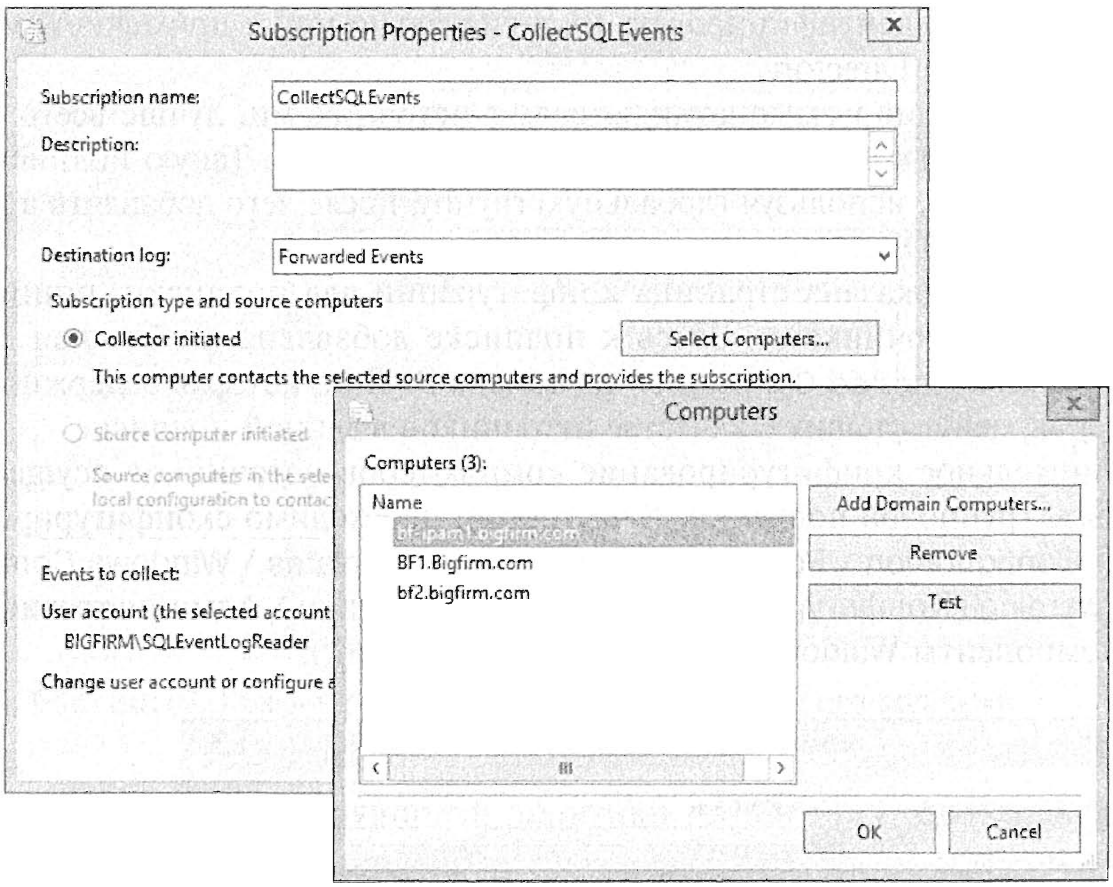


Рис. 30.14. Создание подписки, инициируемой коллектором

При конфигурировании подписки, инициируемой коллектором, понадобится добавить компьютеры-источники, щелкнув на кнопке Select Computers (Выбрать компьютеры). Если компьютеры-источники остаются одними и теми же, то подписка, инициируемая коллектором, является наилучшим вариантом. Вы составляете список компьютеров-источников и модифицируете его, только когда требуется добавить или удалить компьютер из подписки.

Подписки, инициируемые коллектором, также должны конфигурироваться с применением учетной записи, которая имеет разрешения по чтению (Read) на исходных журналах. Поскольку подписки будут включать события, поступающие из нескольких компьютеров, потребуется использовать доменную учетную запись, которой легко выдать разрешение Read на нескольких компьютерах.

На рис. 30.14 видно, что была создана доменная учетная запись по имени `SQLEventLogReader`. Эта учетная запись была добавлена в группу `Event Log Readers` (Считыватели журналов событий).

Группа Event Log Readers

Простейший способ предоставить разрешение Read на исходных журналах предусматривает добавление учетной записи пользователя в группу `Event Log Readers`. Учетную запись пользователя можно добавить в группу `Event Log Readers`, локальную для каждого компьютера, или в доменную группу `Event Log Readers`, находящуюся во встроенном контейнере.

Подписки, инициируемые компьютерами-источниками

При использовании подписки, инициируемой компьютерами-источниками, компьютеры-источники передают события компьютеру-сборщику. Компьютеры-источники можно идентифицировать индивидуально или с применением глобальной группы в Active Directory.

Подписки, инициируемые компьютерами-источниками, лучше всего подходят, когда список компьютеров-источников часто изменяется. Такую подписку можно создать однократно, используя глобальную группу, после чего добавлять в нее и удалять группы Active Directory.

На рис. 30.15 показана страница конфигурации для подписки, инициируемой компьютерами-источниками. Здесь к подписке добавлена глобальная группа по имени `Event Monitored Computers` из домена Bigfirm, которая содержит перечень компьютеров, действующих в качестве источников в данной подписке.

Дополнительное конфигурирование компьютеров-источников осуществляется посредством групповой политики. В частности, необходимо сконфигурировать узел Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Event Forwarding (Конфигурация компьютера \ Политики \ Административные шаблоны \ Компоненты Windows \ Переадресация событий).

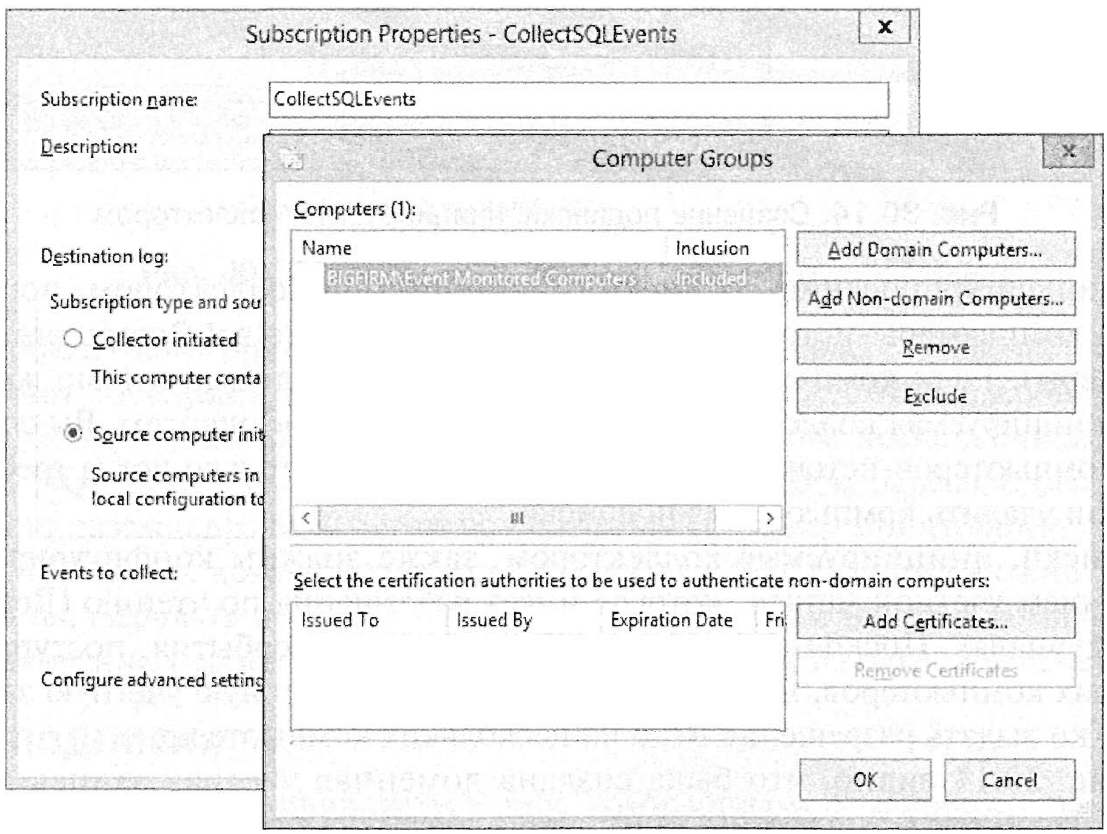


Рис. 30.15. Создание подписки, инициируемой компьютерами-источниками

Настройкой групповой политики, которая должна быть сконфигурирована, является Configure target Subscription Manager (Конфигурировать целевой диспетчер подписки).

В качестве диспетчера подписки понадобится указать полное доменное имя компьютера-сборщика. После выбора переключателя Enabled (Включена) для включения этой настройки, можете щелкнуть на кнопке Show (Показать) и добавить имя сервера на странице Subscription Managers (Диспетчеры подписки).

Например, сервер по имени `BF2` в домене Bigfirm.com идентифицируется с помощью значения `BF2.BigFirm.com` (рис. 30.16).

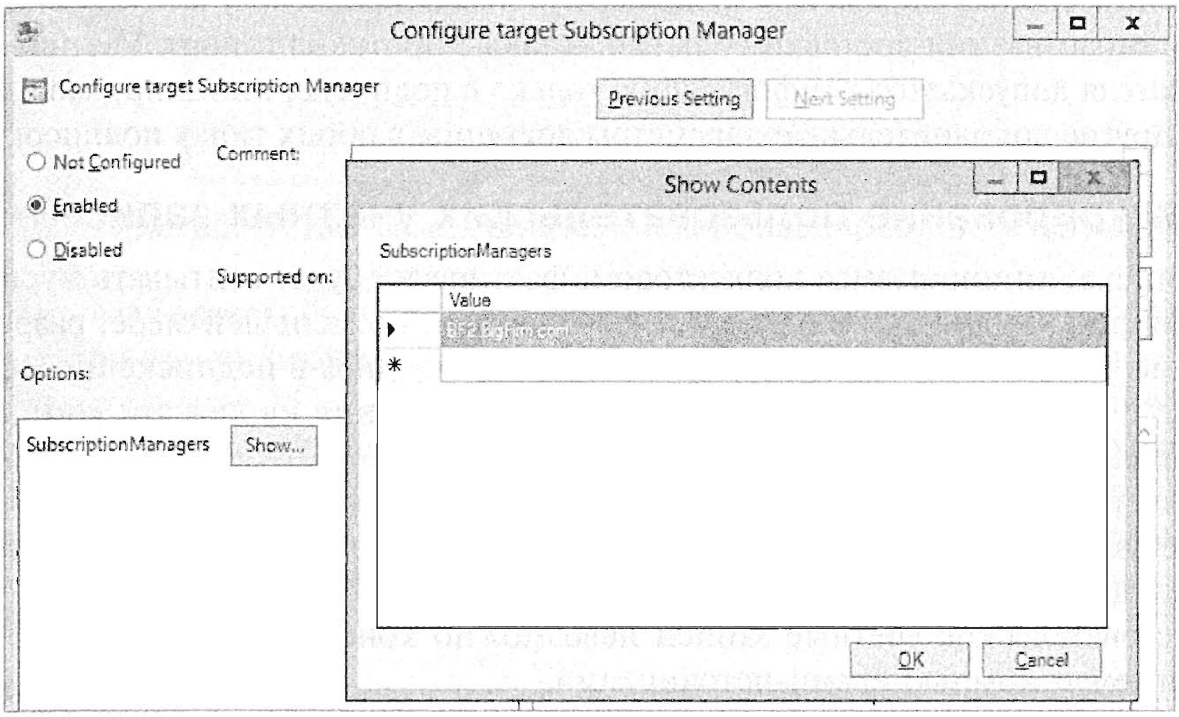


Рис. 30.16. Конфигурирование групповой политики для подписки, инициируемой компьютерами-источниками

Вспомните, что объекты групповой политики (GPO) могут быть привязаны к сайтам, доменам и организационным единицам. В рассматриваемом сценарии имеет смысл поместить все серверы, которыми вы хотите управлять, в организационную единицу, а затем связать объект GPO с этой организационной единицей.

Настройку Configure target Subscription Manager допускается также конфигурировать на каждом компьютере-источнике вручную, если он не находится в домене. Если компьютеры входят в рабочую группу, а не в домен, то для аутентификации также придется применять сертификаты, выпущенные каким-то центром сертификации.

Учитывая дополнительные требования к подпискам, инициируемым компьютерами-источниками, внутри рабочей группы, в недоменных средах эффективнее пользоваться подписками, инициируемыми коллектором.

Выбор событий

При конфигурировании подписки на события необходимо идентифицировать события, которые будут переадресовываться. Выбор событий производится одинаково для подписок, инициируемых коллектором, и для подписок, инициируемых компьютерами-источниками.

Вы можете переадресовывать все события, фиксируемые в определенных журналах, или только специфичные события. Щелчок на кнопке Select Events (Выбрать события) приводит к отображению той же самой страницы, которую вы применяете для фильтрации любого журнала в Event Viewer или создания специального представления.

Создать подписку можно и в командной строке. При использовании командной строки события выбираются с помощью XML-запроса.

Установка дополнительных параметров

Дополнительные параметры включают пользовательскую учетную запись, настройки оптимизации доставки событий, а также протокол и порт. Учетная запись пользователя допускается конфигурацию только в подписке, инициируемой коллектором. Другие дополнительные параметры доступны в обоих типах подписок.

Конфигурирование пользовательских учетных записей

Подписка, инициируемая коллектором, фактически будет считывать журналы на компьютерах-источниках и должна иметь для них, по меньшей мере, разрешение на чтение. Вы должны сконфигурировать учетную запись в подписке и обеспечить наличие у этой учетной записи подходящего разрешения на каждом компьютере-источнике.

Удовлетворить эти требования внутри домена проще всего, создав доменную учетную запись и добавив ее во встроенную локальную группу домена под названием `Event Log Readers`.

Пользовательские учетные записи невозможно конфигурировать в подписках, инициируемых компьютерами-источниками.

Оптимизация доставки событий

При конфигурировании подписок вы можете оптимизировать их для сред с различными полосами пропускания или разными требованиями в отношении времени задержки. Эти настройки могут быть сконфигурированы как для подписок, инициируемых коллектором, так и для подписок, инициируемых компьютерами-источниками.

На рис. 30.17 показано диалоговое окно Advanced Subscription Settings (Дополнительные настройки подписки) для подписки, инициируемой коллектором. Обратите внимание на три переключателя в области Event Delivery Optimization (Оптимизация доставки событий): Normal (Нормальная), Minimize Bandwidth (Минимизировать полосу пропускания) и Minimize Latency (Минимизировать время задержки).

В диалоговом окне Advanced Subscription Settings для подписки, инициируемой компьютерами-источниками, предусмотрены точно такие же переключатели Event Delivery Optimization, но отсутствуют настройки в области User Account (Пользовательская учетная запись). При использовании подписки, инициируемой компьютерами-источниками, компьютер-сборщик не считывает журналы на компьютере-источнике, а просто принимает события, поэтому учетная запись с соответствующими разрешениями не требуется.

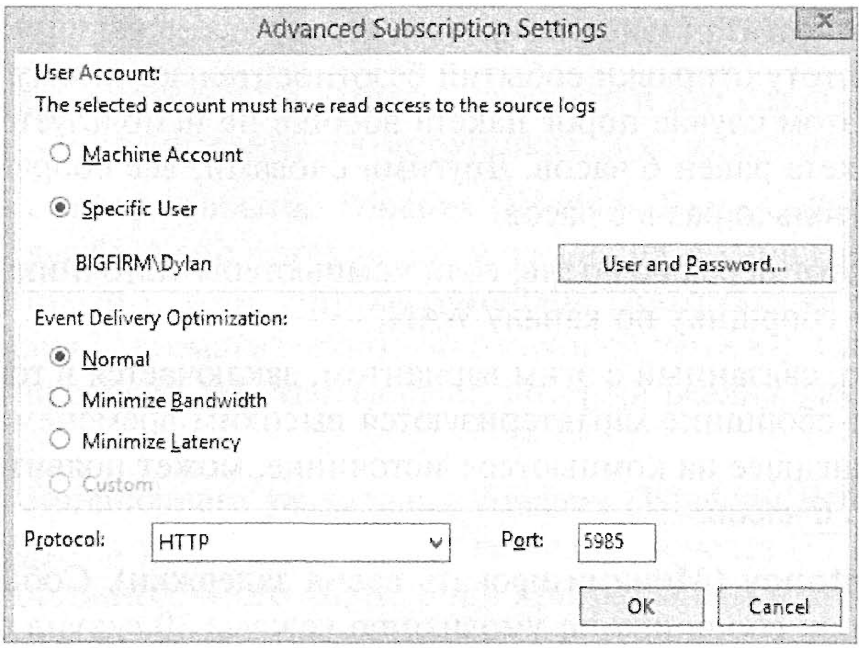


Рис. 30.17. Диалоговое окно Advanced Subscription Settings

Обычно все серверы будут находиться в среде с высокоскоростными подключениями внутри одной локальной сети и работать в режиме Normal. События переадресуются в течение 15 минут и не требуют интенсивного использования полосы пропускания. Однако если серверы разделены каналами WAN или необходимо пересылать события коллектору быстрее, можно оптимизировать доставку событий.

Разные режимы доставки событий имеют дело с пакетами и тайм-аутами пакетов. Прежде чем можно будет понять режимы доставки, необходимо уяснить основы пакетов и тайм-аутов пакетов.

- **Пакеты.** События можно пересылать по одному за раз, хотя обычно они отправляются пакетами. Пакет — это несколько событий, сгруппированных вместе для передачи. Разные режимы оптимизации имеют разные пороговые количества событий, объединяемых в пакет. Например, в режиме Normal приходится ждать, пока не будет получено пять событий, из которых формируется пакет для передачи.
- **Тайм-аут пакета.** Тайм-аут пакета задает максимальное время ожидания системой момента начала отправки событий, даже если порог формирования пакета не был достигнут. Например, в режиме Normal тайм-аут пакета составляет 15 минут. Если в подписке указано, что каждый пакет содержит пять событий, но за 15 минут было принято только три события, то по истечении 15 минут эти три события будут переданы в виде пакета.

Каждый из трех переключателей в области Event Delivery Optimization связан с различным применением пакетов и тайм-аутов пакетов. Ниже приведены описания этих переключателей.

- **Normal (Нормальная).** Используется в типичной локальной сети с высокоскоростными подключениями. Никакие попытки экономии полосы пропускания не предпринимаются и события отправляются часто. По умолчанию порог для пакетов составляет 5 событий, а тайм-аут пакета — 15 минут.

- **Minimize Bandwidth (Минимизировать полосу пропускания).** Значительно ограничивает частоту отправки событий безотносительно к тому, сколько событий собрано. В этом случае порог пакета вообще не используется, а стандартный тайм-аут пакета равен 6 часов. Другими словами, все собранные события отправляются только раз в 6 часов.

  Выбирайте этот переключатель, если компьютеры-источники подключаются к компьютеру-сборщику по каналу WAN.

  Компромисс, связанный с этим вариантом, заключается в том, что события на компьютере-сборщике характеризуются высоким временем задержки. Событие, произошедшее на компьютере-источнике, может появиться на коллекторе только через 6 часов.

- **Minimize Latency (Минимизировать время задержки).** События отправляются компьютеру-сборщику по умолчанию каждые 30 секунд с использованием режима доставки выталкиванием. Порог пакета не отслеживается, но вместо этого применяется тайм-аут пакета, составляющий 30 секунд.

Протоколы подписки на события

Подписки используют протокол HTTP для незашифрованной передачи и протокол HTTPS для зашифрованной передачи. Хотя протоколы HTTP и HTTPS работают со стандартными портами 80 и 443 в Интернете, подписки на события для этих протоколов применяют другие порты.

Вот стандартные порты, которые используются подписками на события:

- HTTP: 5985
- HTTPS: 5986

Единственной причиной изменения стандартных портов является конфликт с другим приложением в сети. Иными словами, если порт 5985 или 5986 уже используется в сети, вы можете выбрать какой-то другой порт.

Если вы изменили порты в конфигурации подписки, то серверы, задействованные в этой подписке, понадобится переконфигурировать с помощью команды `WinRM`. Вот формат этой команды:

```
Winrm set winrm/config/listener?Address=*+Transport=HTTP @{Port="8888"}
```

Поскольку подписки на события используют не те порты, которые обычно применяются с протоколами HTTP и HTTPS, они не должны конфликтовать с установленным сервером IIS.

Конфигурирование подписок на события

Ниже перечислены общие требования к конфигурированию подписок на события.

- Позаботьтесь о включении обязательных служб на компьютерах-источниках и коллекторе.
- Сконфигурируйте компьютеры-источники и коллектор.
- Сконфигурируйте подписку.

Включение обязательных служб

Для поддержки подписок на события требуются две службы, которые должны функционировать и на компьютерах-источниках, и на коллекторе.

- **Служба коллектора событий Windows (Windows Event Collector; `wecutil`).** Это основная служба, используемая для управления подписками. Для нее должен быть установлен режим запуска Automatic (Автоматический) или Automatic (Delayed Start) (Автоматический (отсроченный запуск)). Служба `wecutil` поддерживает протокол WS-Management, который реализован в Windows с помощью службы WinRM.
- **Служба дистанционного управления Windows (Windows Remote Management — WinRM).** Служба WinRM использует веб-службы через HTTP и HTTPS для реализации дистанционного управления программным и аппаратным обеспечением. Для нее должен быть установлен режим запуска Automatic или Automatic (Delayed Start). Служба WinRM не зависит от роли Web Services (IIS) и может сосуществовать с ней, если эта роль установлена на том же самом сервере.

Конфигурирование компьютеров

Прежде чем можно будет создавать подписки на события, вы должны сконфигурировать компьютеры-источники и коллектор. Чтобы настроить компьютер-источник для приема событий, выполните описанные ниже шаги. В результате на компьютере-источнике будет сконфигурирована служба WinRM.

1. Откройте окно командной строки с административными разрешениями.
2. Введите следующую команду:

```
winrm quickconfig
```

Служба Windows Event Collector

Когда вы первый раз выберете узел Subscriptions (Подписки) в Event Viewer или перейдете на вкладку Subscription (Подписка) в окне свойств журнала, отобразится диалоговое окно, информирующее о том, что у вас должна функционировать сконфигурированная служба Windows Event Collector. После этого выдается запрос о том, хотите ли вы запустить и сконфигурировать эту службу. Если вы щелкнете на кнопке Yes (Да), служба запустится, а тип ее запуска изменится с Manual (Ручной) на Automatic (Delayed Start). Это приведет к тому, что данная служба будет запускаться каждый раз при загрузке Windows.

Если служба WinRM еще не сконфигурирована, вам будет предложено выполнить следующие действия:

- создать прослушиватель WinRM на `HTTP://*`, чтобы принимать запросы WS-Management к любому IP-адресу на этой машине;
- добавить исключение брандмауэра для WinRM.

Если служба WinRM уже сконфигурирована, вы увидите сообщение о том, что эта служба функционирует и сконфигурирована для дистанционного управления.

3. Чтобы принять эти изменения, введите `Y` и нажмите <Enter>.

   Система отреагирует указанием на то, что служба WinRM была обновлена для дистанционного управления.

Следующая далее последовательность действий позволяет настроить компьютер-сборщик на прием событий. В результате на компьютере-сборщике будет сконфигурирована служба Windows Event Collector (`wecutil`).

1. Откройте окно командной строки с административными разрешениями.
2. Введите следующую команду:

   ```
   wecutil qc
   ```

   Вы получите сообщение о том, что режим запуска этой службы будет изменен на Automatic (Delayed Start), и предложено ввести `Y` или `N`.

3. Чтобы внести эти изменения, введите `Y` и нажмите <Enter>.

   Система отреагирует указанием на то, что служба Windows Event Collector была успешно сконфигурирована.

Создание подписки, инициируемой коллектором

Воспользуйтесь описанными ниже шагами, чтобы создать в доменной среде подписку, инициируемую коллектором.

1. Запустите средство Event Viewer из начального экрана Windows Server 2012 R2, набрав **`eventvwr`** и нажав <Enter>, или через пункт меню Tools⇨Event Viewer (Сервис⇨Средство просмотра событий) диспетчера серверов.
2. Щелкните правой кнопкой мыши на узле Subscriptions (Подписки) и выберите в контекстном меню пункт Create Subscription (Создать подписку).
3. В поле Subscription Name (Имя подписки) введите `Collector Initiated`.

   Обратите внимание, что в поле Destination Log (Целевой журнал) указан журнал Forwarded Events (Переадресованные события).

4. Удостоверьтесь в выборе переключателя Collector Initiated (Инициируемая коллектором) и щелкните на кнопке Select Computers (Выбрать компьютеры).
5. Щелкните на кнопке Add Domain Computers (Добавить компьютеры домена). Введите `LocalHost` в качестве имени компьютера и щелкните на кнопке OK.

   Имя `LocalHost` будет преобразовано в действительное имя вашего компьютера. В реальной среде не было бы никакой необходимости создавать подписку для собственного компьютера. Тем не менее, это позволяет точно следовать процедуре создания подписки.

6. При желании добавьте другие компьютеры.
7. Щелкните на кнопке Test (Проверить). Это проверит возможность подключения к серверу.
8. Щелкните на кнопке OK, чтобы закрыть диалоговое окно Connectivity Test Succeeded (Проверка соединения завершилась успешно). Щелкните на кнопке OK в диалоговом окне Computers (Компьютеры).

FQDN или входное имя

Когда вы добавляете сервер, система пытается достичь его, и если это удается, она отображает полное доменное имя (fully qualified domain name — FQDN) этого сервера (вроде `BF1.Bigfirm.com`). Если же сервер системой недостижим, она отобразит имя в формате входа в систему вида `домен\учетная_запись` (наподобие `Bigfirm\BF3`). Если сервера в Active Directory не существует, он не может быть добавлен.

9. Щелкните на кнопке Select Events (Выбрать события). Отметьте флажки Critical (Критические), Warning (Предупреждения), Error (Ошибки) и Information (Информационные). Выбирайте уровни событий, которые соответствуют вашим нуждам.
10. Щелкните на раскрывающемся списке Event Logs (Журналы событий).
11. Щелкните на значке "плюс" рядом с узлом Windows Logs (Журналы Windows) и отметьте флажки для журналов Application и System.

    Можете также отметить флажки для любых журналов в узле Application and Services Logs (Журналы приложений и служб).

Выбирайте менее 10 журналов

Каждый раз, когда вы выбираете более 10 журналов, появляется предупреждение, указывающее на непродуманность такого действия. Выбор слишком большого количества журналов может привести к чрезмерному расходованию ресурсов сервера и отрицательно сказаться на производительности системы. Избегайте соблазна проводить мониторинг абсолютно всего, вместо того чтобы отслеживать только то, что действительно необходимо.

12. Щелкните на кнопке OK, чтобы закрыть окно выбора Query Filter (Фильтр запросов).
13. Щелкните на кнопке Advanced (Дополнительно).

    Обратите внимание, что учетная запись машины выбрана по умолчанию. Ей не понадобится разрешение для чтения исходных журналов на любых удаленных серверах.
14. Выполните следующие действия, чтобы создать доменную учетную запись и выдать ей разрешение для чтения исходных журналов на удаленных системах.
    а. Запустите оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory).
    б. Щелкните правой кнопкой мыши на узле Users (Пользователи) и выберите в контекстном меню пункт New⇨User (Создать⇨Пользователь).
    в. В текстовых полях First Name (Имя) и User Logon Name (Входное имя пользователя) введите **`EventLogReader`**. Щелкните на кнопке Next (Далее).
    г. В текстовых полях Password (Пароль) и Confirm Password (Подтвердите пароль) введите пароль, который удовлетворяет требованиям по сложности, принятым в домене.

д. Снимите отметку с флажка User Must Change Password at Next Logon (Пользователь должен изменить пароль при следующем входе).

е. Отметьте флажки User Cannot Change Password (Пользователь не может изменять пароль) и Password Never Expires (Срок действия пароля никогда не истекает).

Учетная запись считывателя журналов событий

Учетная запись считывателя журналов событий должна трактоваться как учетная запись службы. Учетные записи служб часто конфигурируются так, чтобы срок действия их паролей никогда не истекал. Тем не менее, учетными записями служб (и учетной записью считывателя журналов событий) по-прежнему необходимо управлять. Другими словами, вы должны располагать процессом для периодического изменения паролей этих учетных записей или, что еще лучше, использовать средство Managed Service Accounts (Учетные записи управляемых служб), доступное в Windows Server 2012 R2.

ж. Щелкните на кнопке Next, а затем на кнопке Finish (Готово), чтобы создать учетную запись.

з. Дважды щелкните на учетной записи `EventLogReader`, чтобы открыть диалоговое окно ее свойств.

и. Перейдите на вкладку Member Of (Членство в группах) и щелкните на кнопке Add (Добавить).

й. Введите **`Event Log Readers`** и щелкните на кнопке OK, чтобы добавить эту учетную запись в группу `Event Log Readers`.

15. Возвратитесь в диалоговое окно Advanced Subscription Settings (Дополнительные настройки подписки) и выберите переключатель Specific User (Конкретный пользователь).

16. Щелкните на кнопке User and Password (Пользователь и пароль).

17. В открывшемся диалоговом окне Credentials (Учетные данные) введите имя пользователя и пароль только что созданной учетной записи. Имя пользователя должно вводиться в формате `домен\имя_пользователя`. Щелкните на кнопке OK.

18. Просмотрите переключатели в области Event Delivery Optimization (Оптимизация доставки событий) и удостоверьтесь в том, что выбран переключатель Normal (Нормальная).

19. Просмотрите протоколы и порты. Стандартным портом для HTTP является 5985, а для HTTPS — 5986. Порт для HTTPS можно увидеть, выбрав элемент HTTPS в раскрывающемся списке Protocol (Протокол).

20. Щелкните на кнопке OK, чтобы принять внесенные изменения.

21. Щелкните на кнопке OK, чтобы завершить создание подписки.

Ошибки при создании подписки

Если при создании подписки вы получаете какие-то сообщения об ошибках, проверьте, что компьютеры, добавленные в эту подписку, работоспособны и достижимы из вашего сервера. Это легко сделать, щелкнув на кнопке Select Computers (Выбрать компьютеры), выбрав каждый из компьютеров и щелкнув на кнопке Test (Проверить).

После того как подписка создана, вы можете щелкнуть на ней правой кнопкой мыши и выбрать в контекстном меню пункт Properties (Свойства), чтобы переконфигурировать большинство свойств этой подписки. Изменять тип подписки (инициируемая коллектором или инициируемая компьютерами-источниками), а также ее имя нельзя, но можно модифицировать любые другие ее свойства.

Поиск и устранение проблем, связанных с переадресацией событий

Наиболее распространенными проблемами, которые вызывают появление ошибок, связанных с переадресацией событий, являются невозможность доступа через сеть к серверам, задействованным в подписке, некорректное конфигурирование подписки или отсутствие надлежащих разрешений у пользовательской учетной записи.

Проверка состояния времени выполнения

Полезно проверять состояние времени выполнения подписки на события. Для этого щелкните правой кнопкой мыши на подписке и выберите в контекстном меню пункт Runtime Status (Состояние времени выполнения).

На рис. 30.18 показано состояние времени выполнения подписки, имеющей проблемы с учетной записью. Когда состояние выбрано, в нижней панели отображается подробная информация об ошибке.

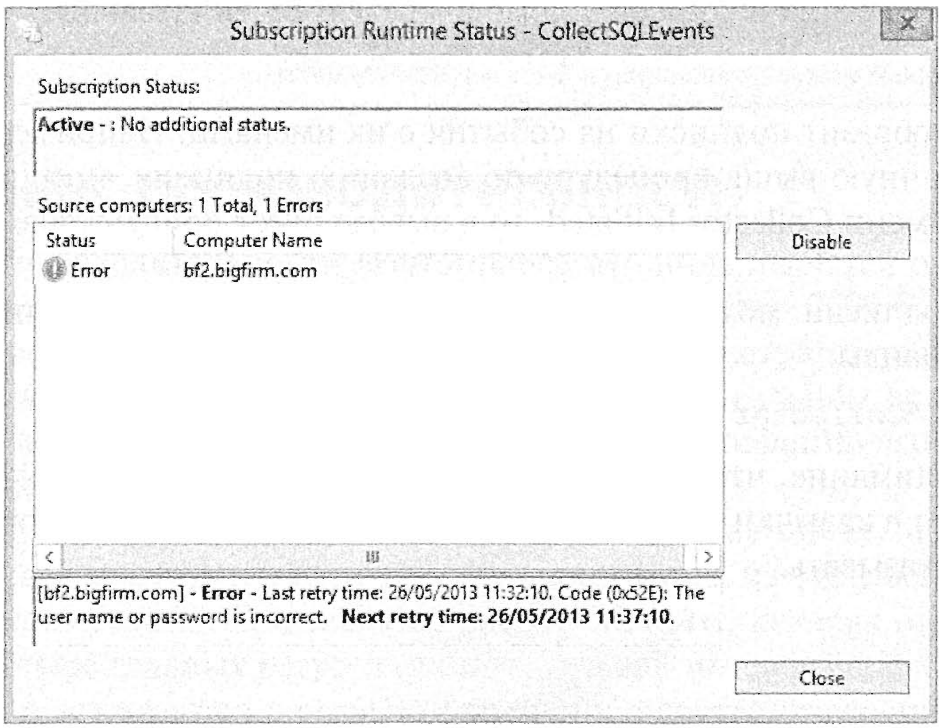


Рис. 30.18. Просмотр состояния времени выполнения

В этом случае ошибка связана с отказом во входе. Учетная запись, использованная для этой подписки, не имеет разрешения для чтения журналов на удаленном компьютере из-за некорректно указанного имени пользователя или пароля. Проблему можно решить, проверив правильность имени пользователя и пароля и убедившись в том, что данная пользовательская учетная запись была добавлена в группу `Event Log Readers`.

Использование утилиты Windows Event Collector

Для конфигурирования и диагностики проблем, связанных с переадресацией событий, можно также запустить утилиту Windows Event Collector в командной строке.

С помощью графического пользовательского интерфейса Event Viewer и команды `wecutil` можно решать в основном те же самые задачи. Таким образом, возникает вполне естественный вопрос: зачем применять именно команды `wecutil`? Для этого есть две причины.

- Первая и самая важная причина заключается в том, что команды `wecutil` можно запускать дистанционно с использованием команды `WinRS`. Если служба WinRS сконфигурирована, то любую команду `wecutil` можно выполнять в командной строке на удаленном компьютере.
- Вторая причина касается того, что команды `wecutil` можно применять в сценариях. Любую команду, которую допускается вводить в командной строке, можно поместить в пакетный файл или сценарий PowerShell и очень просто выполнить. Например, если вы создали подписку с помощью пакетного файла, то можете легко создать ее еще раз, запустив этот же пакетный файл повторно. В табл. 30.1 перечислены разнообразные переключатели, доступные для `wecutil`.

Самый распространенный способ использования этих команд для поиска и устранения проблем, связанных с подписками на события, предусматривает первоначальный вывод перечня подписок с помощью следующей команды:

```
wecutil es
```

Команда отобразит подписки на события с их именами. Например, если вы выполнили описанную выше процедуру по созданию подписки, инициируемой коллектором, по имени Collector Initiated, то в выводе будет присутствовать `Collector Initiated`.

Зная имя подписки, можно получить ее состояние времени выполнения посредством такой команды:

```
wecutil gr "Collector Initiated"
```

Обратите внимание, что имя подписки содержит пробел, поэтому оно должно быть заключено в кавычки. Если же в имени подписки пробелы отсутствуют, кавычки можно не указывать.

Таблица 30.1. Команды `wecutil`

Команда `wecutil`	Комментарий
`wecutil /?`	Получение справки. Отображает базовые команды. Можно запросить дополнительную справку по любой команде, указав после команды переключатель `/?` (например, `wecutil es /?`)
`wecutil es`	Перечисление подписок. Вы можете вывести перечень всех подписок в системе. Применяйте эту команду для получения идентификатора подписки, используемого в других командах
`wecutil gs` *<идентификатор подписки>*	Получение подписки. Команда `gs` выводит все параметры и опции для созданной подписки
`wecutil gr` <идентификатор подписки>	Получение состояния времени выполнения для подписки. Этой командой удобно пользоваться при поиске и устранении проблем с подписками. Если подписка не работает, то результаты выполнения команды `gr` будут включать детали последнего сообщения об ошибке. Доступ к этой информации можно также получить, щелкнув правой кнопкой мыши на подписке в Event Viewer и выбрав в контекстном меню пункт Runtime Status (Состояние времени выполнения)
`wecutil ss`	Установка подписки. Эту команду можно применять для установки параметров подписки. Для нее можно получить значительный объем дополнительной справочной информации. Чтобы поместить ее вывод в текстовый файл `sshelp.txt`, воспользуйтесь следующей командой: `wecutil ss /? > sshelp.txt`. Результирующий файл можно открыть так: `Notepad sshelp.txt`
`wecutil cs`	Создание подписки. Эту команду можно применять для создания подписки. Для нее можно получить значительный объем дополнительной справочной информации, добавив переключатель `/?`
`wecutil ds` <идентификатор подписки>	Удаление подписки
`wecutil rs` <идентификатор подписки>	Повторение попытки подписки. Эта команда инициирует попытку установить подключение и отправить удаленный запрос на подписку. Затем можно выполнить команду `gr`, чтобы получить текущее состояние
`wecutil qc`	Переключатель `qc` (quick configure — быстрое конфигурирование) используется для конфигурирования службы Windows Event Collector

Мониторинг производительности

Монитор производительности (Performance Monitor) является одним из краеугольных камней операционных систем со времен Windows 2000 Server, и он стал важным компонентом набора инструментов для администраторов по всему миру. Его можно применять для наблюдения за системой в реальном времени или для создания журнальных файлов, которые позволяют идентифицировать изменения в производительности.

Окно монитора производительности показано на рис. 30.19. В левой панели отображаются все инструменты, доступные для запуска из этой оснастки. В центральной панели представлена сводка о работе системы, которая отображается по умолчанию. Четыре главных ресурса (память, сетевой интерфейс, физический диск и процессор) отслеживаются в реальном времени, а соответствующие счетчики сообщают подробности их функционирования.

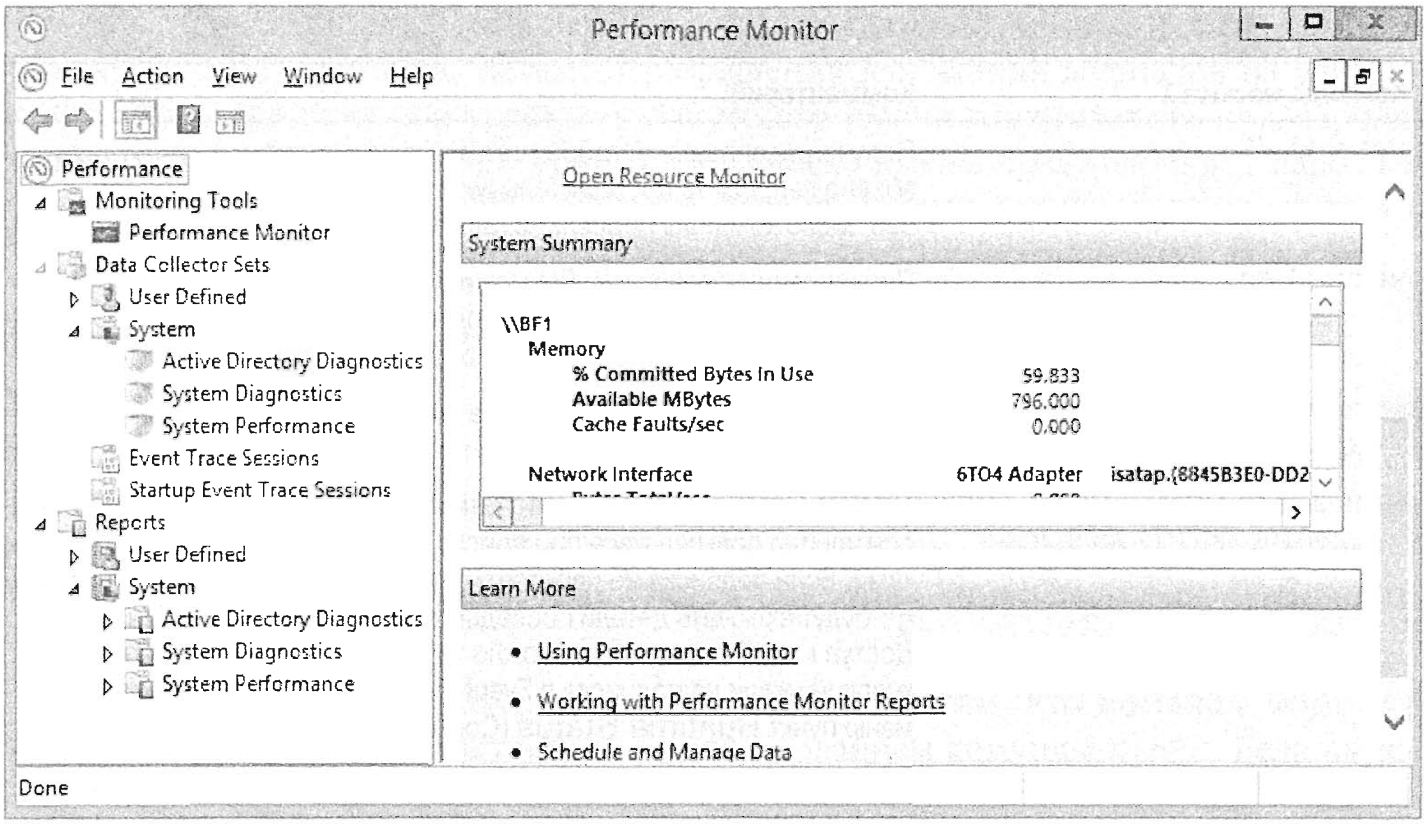


Рис. 30.19. Монитор производительности

Основной функциональностью монитора производительности являются группы сборщиков данных, которые позволяют накапливать и просматривать ключевые данные производительности системы, сгруппированные по категории диагностики и производительности.

Как все-таки называется инструмент: "Производительность" или "Монитор производительности"?

В разных версиях Windows этот инструмент назывался и "Производительность" (Performance), и "Монитор производительности" (Performance Monitor). В Windows Server 2012 R2 встречаются оба названия. Он запускается как монитор производительности (путем открытия начального экрана, ввода **`perfmon`** и щелчка на значке Performance Monitor). Его можно также запустить путем ввода **`perfmon`** в окне PowerShell или в командной строке.

После запуска в заголовке окна отображается название Performance Monitor (Монитор производительности).

Однако верхний узел в навигационной панели (слева) называется Performance (Производительность). В узле Monitoring Tools (Инструменты мониторинга) вы увидите знакомый элемент Performance Monitor, которым вы могли пользоваться в предыдущих редакциях Windows. Мысль, которую мы пытаемся донести, заключается в том, что монитор производительности эволюционировал в комплект инструментов, который представляет собой нечто большее, чем традиционный инструмент `Perfmon.exe`, доступный в более ранних версиях Windows. В этой главе мы будем ссылаться на полный комплект инструментов как на *монитор производительности*, а на более старый инструмент Performance Monitor (из узла Monitoring Tools) — как на *унаследованный монитор производительности*.

Использование инструментов мониторинга

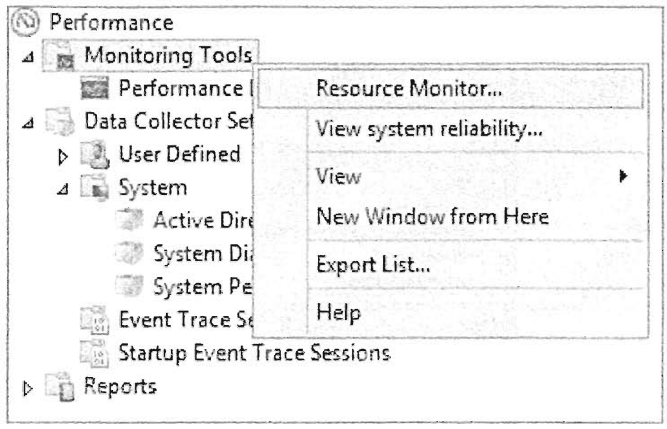


Рис. 30.20. Доступ к дополнительным инструментам мониторинга

В этом разделе приведена информация об унаследованном мониторе производительности, мониторе ресурсов и отчете о стабильности системы.

Унаследованный монитор производительности отображается по умолчанию. Если вы щелкнете правой кнопкой мыши на узле Monitoring Tools (Инструменты мониторинга), то увидите в контекстном меню доступные для выбора пункты Resource Monitor (Монитор ресурсов) и View system reliability (Просмотр сведений о стабильности системы), как показано на рис. 30.20.

Монитор производительности

Если вам приходилось иметь дело с предшествующими версиями Windows, то вы, скорее всего, пользовались монитором производительности. Монитор производительности с помощью объектов и счетчиков обеспечивает наблюдение за системами в реальном времени. Ниже приведены краткие пояснения.

- **Объекты.** Объекты монитора производительности — это особые ресурсы, которые могут быть измерены. Распространенными измеряемыми объектами являются Processor (Процессор), Memory (Память), Network Interface (Сетевой интерфейс) и Physical Disk (Физический диск).
- **Счетчики.** Счетчики — это индивидуальные метрики внутри объекта. Например, объект Processor включает такие счетчики, как % Processor Time (% процессорного времени), % User Time (% пользовательского времени) и Interrupts/Sec (Прерываний/с).

Счетчики, наблюдаемые в этом мониторе производительности, применяются по всему комплекту инструментов монитора производительности, включая группы сборщиков данных.

Монитор ресурсов

Монитор ресурсов (Resource Monitor) выполняется постоянно и собирает информацию счетчиков по четырем основным ресурсам системы. Для доступа к нему щелкните правой кнопкой мыши на узле Monitoring Tools (Инструменты мониторинга) и выберите в контекстном меню пункт Resource Monitor (Монитор ресурсов). Обратиться к монитору ресурсов можно также через окно диспетчера задач (Task Manager), перейдя на вкладку Performance (Быстродействие) и щелкнув на кнопке Resource Monitor (Монитор ресурсов).

На рис. 30.21 показано окно Resource Monitor (Монитор ресурсов) с выбранной вкладкой Overview (Обзор). В левой панели отображается подробная информация о каждом ресурсе, а в правой панели приведено графическое представление для каждого ресурса.

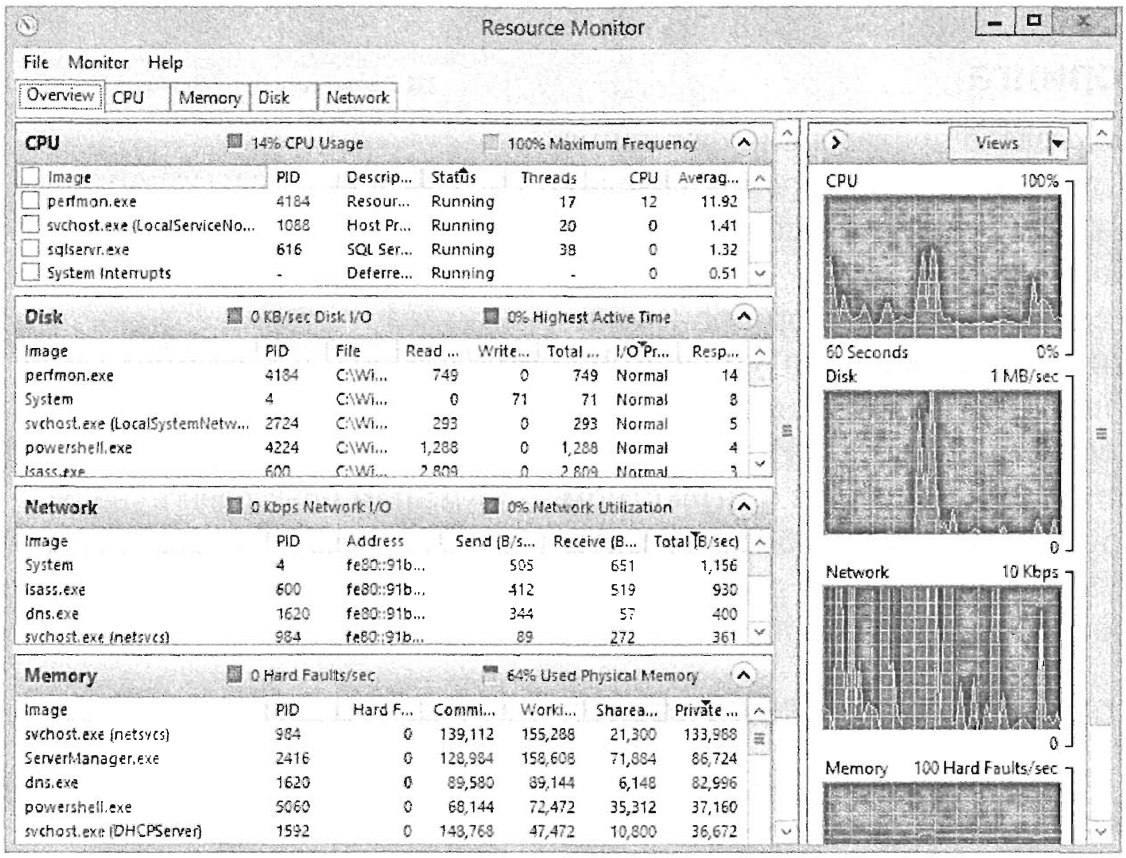


Рис. 30.21. Доступ к дополнительным инструментам мониторинга

Вы можете перейти на вкладку для любого из четырех ресурсов и получить дополнительную информацию о функционировании процессора, памяти, дисковой подсистемы или сетевого интерфейса.

Одним из главных преимуществ монитора ресурсов является его способность фильтровать результаты в соответствии с конкретными процессами или службами. Например, если вы хотите выяснить нагрузку, создаваемую каким-то приложением на систему, можете выбрать только процессы этого приложения.

Монитор ресурсов можно также использовать для выяснения, какой процесс блокирует определенный файл или библиотеку DLL. Например, вредоносное ПО часто предотвращает удаление файла, блокируя его. Когда вы попытаетесь удалить такой файл, система не позволит это сделать, сообщив, что файл заблокирован. Тем не менее, с помощью монитора ресурсов вы можете выяснить, что происходит в действительности.

Перейдите на вкладку CPU (ЦП) и откройте раздел Associated Handles (Связанные дескрипторы). В поле поиска введите имя нужного файла и щелкните на значке рядом с полем. Отобразится подробная информация о дескрипторе. Щелкните правой кнопкой мыши на полученном результате и выберите в контекстном меню пункт End Process (Завершить процесс), после чего должна появиться возможность удаления файла.

Иногда могут требоваться более детальные сведения. Определите идентификатор процесса (в столбце PID (ИД процесса)), перейдите на вкладку Overview и просмотрите раздел CPU (ЦП). Второй столбец обозначен как PID (ИД процесса), и щелчок на нем позволяет сортировать процессы в возрастающем или убывающем порядке, чтобы упростить нахождение интересующего процесса. В результате первого щелчка значок в виде стрелки вверх будет указывать на возрастающий порядок, а после второго щелчка отобразится значок в виде стрелки вниз, обозначающий убывающий порядок.

Соблюдайте осторожность при завершении процессов

Завершение процессов может привести к нестабильной работе системы. Вы должны останавливать процессы только в крайнем случае. Иногда это хорошее решение, но его не следует выбирать самым первым. Вдобавок некоторые процессы являются живучими, и после останова они автоматически перезапускаются. Это характерно для ряда системных ресурсов и определенных вредоносных программ.

Найдя нужный процесс, можете щелкнуть на нем правой кнопкой мыши и завершить его здесь или собрать о процессе дополнительную информацию. Если вы выберете в контекстном меню пункт Analyze Wait Chain (Анализ цепочки ожидания), то отобразятся все процессы, которые используют или ожидают использования одного и того же ресурса.

Просмотр сведений о стабильности системы

Стабильность системы отслеживается с помощью монитора стабильности (Reliability Monitor). Для оценки стабильности системы он применяет индекс стабильности со шкалой от 1 до 10, где 10 соответствует высокой надежности.

Монитор стабильности наблюдает за отказами оборудования, приложений, операционной системы Windows, а также за другими сбоями и предупреждениями. Когда происходит отказ, индекс стабильности снижается в зависимости от степени серьезности проблемы. Чем дольше система работает без сбоев, тем выше индекс стабильности.

Данные отображаются на графике, на котором представлены значки информационных сообщений, предупреждений и отказов. Можете выбрать любой из этих значков и ознакомиться с подробной информацией об отказе.

Монитор стабильности может быть удобен при выявлении тенденций в системах. Большинство ваших серверов должны иметь похожие индексы стабильности. Однако если вы обнаружите сервер со значительно более низким индексом стабильности, это может быть свидетельством наличия проблем, связанных с несовместимостью оборудования или ошибочной работой приложений.

Использование групп сборщиков данных

Группы сборщиков данных — это замечательное средство, доступное в комплекте монитора производительности, которое впервые появилось в Windows Server 2008. Каждая группа сборщиков данных представляет собой предварительно определенный набор счетчиков производительности, данных трассировки событий и конфигурационной информации, применяемый для мониторинга ключевых элементов системы.

Монитор производительности включает заранее сформированные системные группы сборщиков данных, которые можно использовать для мониторинга системы. Эти системные группы сборщиков данных можно также применять в качестве шаблонов для создания собственных групп сборщиков данных.

Для запуска или доступа к группам сборщиков данных требуется членство в группе `Administrators` (Администраторы) на локальной системе. Хотя группа `Performance Log Users` (Пользователи журнала производительности) существует

в Windows Server 2012 R2, ее пользователи располагают только минимальным доступом к инструментам внутри комплекта монитора производительности.

Системные группы сборщиков данных

Двумя предварительно сформированными группами сборщиков данных являются System Diagnostics (Диагностика системы) и System Performance (Производительность системы). В случае повышения сервер до контроллера домена добавляется группа сборщиков данных Active Directory Diagnostics (Диагностика Active Directory).

В отличие от монитора ресурсов, который функционирует постоянно, группы сборщиков данных не сконфигурированы на автоматический запуск. Чтобы запустить любую группу сборщиков данных, щелкните не ней правой кнопкой мыши и выберите в контекстном меню пункт Start (Запустить).

Данные, собираемые этими группами сборщиков данных, хранятся в папке `c:\Perflogs`.

- **System Diagnostics.** Группа сборщиков данных System Diagnostics предоставляет подробные сведения о локальных аппаратных ресурсах, показателях времени реакции системы и процессах на локальном компьютере. Она включает информацию о системе и данные конфигурации. Результирующий отчет содержит предложения по увеличению производительности и рационализации функционирования системы. Эта группа сборщиков данных работает в течение 10 минут после ее запуска.
- **System Performance.** Группа сборщиков данных System Performance может использоваться для идентификации возможных причин возникновения проблем с производительностью. Она включает информацию о локальных аппаратных ресурсах, показателях времени реакции системы и процессах. Эта группа сборщиков данных работает в течение 1 минуты после ее запуска.
- **Active Directory Diagnostics.** Группа сборщиков данных Active Directory Diagnostics накапливает данные, касающиеся Active Directory, в том числе счетчики производительности, данные трассировки событий и ключи реестра, которые можно применять для поиска и устранения проблем с производительностью Active Directory. Эта группа сборщиков данных работает в течение 5 минут после ее запуска.

Детали конфигурации и свойства каждой предварительно сформированной группы сборщиков данных можно просматривать, не модифицировать.

Чтобы запустить группы сборщиков данных System Performance и System Diagnostics и ознакомиться с их результатами, выполните следующие шаги.

1. Запустите комплект монитора производительности из начального экрана Windows Server 2012 R2, набрав **`perfmon`** и нажав <Enter>, или через пункт меню Tools⇨Performance Monitor (Сервис⇨Монитор производительности) диспетчера серверов.
2. Перейдите к узлу Data Collector Sets⇨System (Группы сборщиков данных⇨Система), чтобы получить доступ к предварительно сформированным группам сборщиков данных.

3. Щелкните правой кнопкой мыши на группе сборщиков данных System Performance (Производительность системы) и выберите в контекстном меню пункт Start (Запустить).

   Эта группа сборщиков данных будет работать в течение 1 минуты. Когда она завершит работу, вы сможете просмотреть отчет.

4. Щелкните правой кнопкой мыши на группе сборщиков данных System Diagnostics (Диагностика системы) и выберите в контекстном меню пункт Start.

   Эта группа сборщиков данных будет работать, пока вы просматриваете отчет, сгенерированный группой сборщиков данных System Performance.

5. Перейдите к узлу Reports⇨System⇨System Performance (Отчеты⇨Система⇨Производительность системы). Выберите нужный отчет. Окно монитора производительности будет подобным показанному на рис. 30.22.

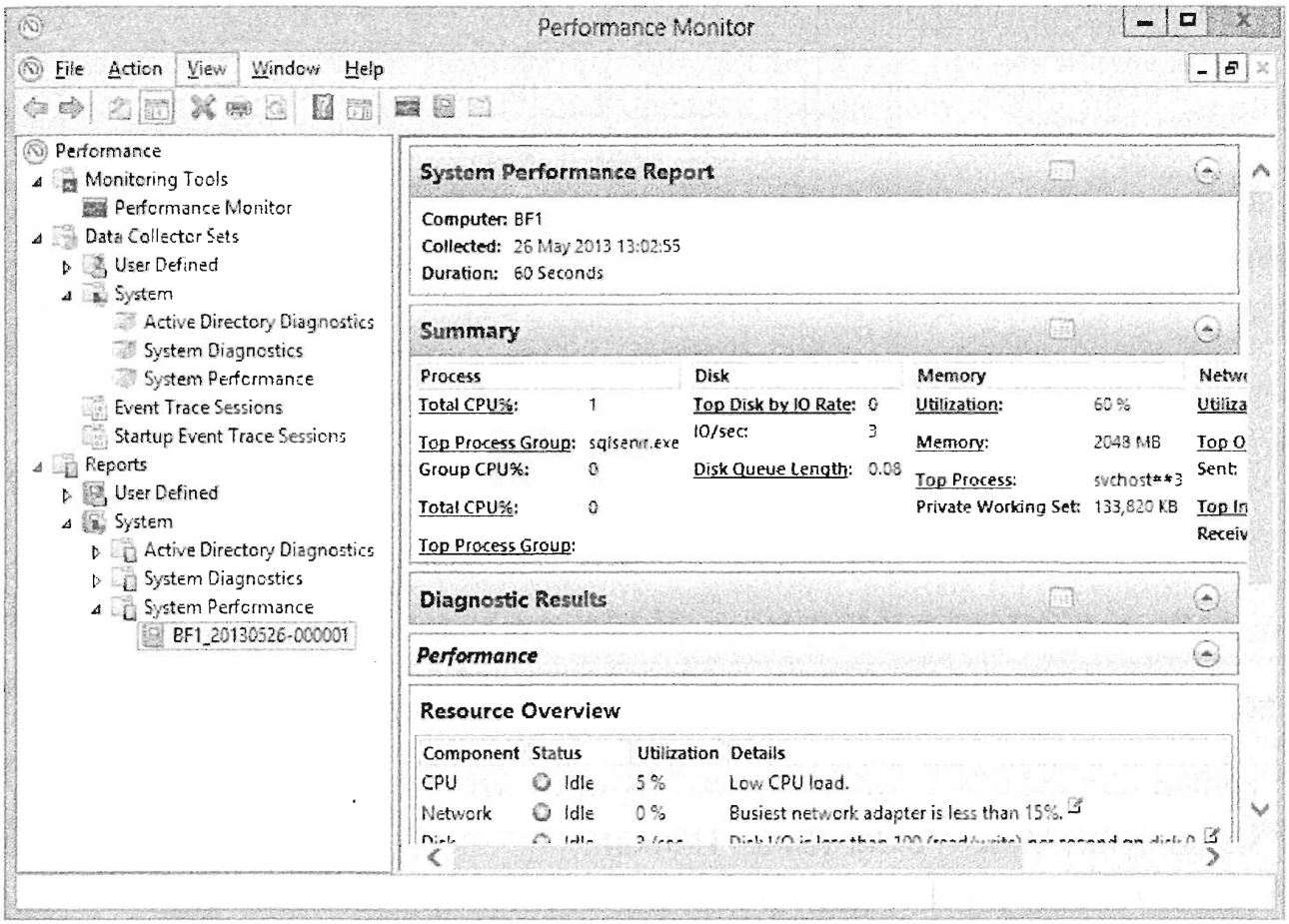


Рис. 30.22. Отчет о выполнении группы сборщиков данных

6. Ознакомьтесь с деталями этого отчета.

   Отчет включает подробные сведения об общей производительности системы, а также ресурсов ЦП, сети, дисков и памяти. В конце отчета приводятся совокупные статистические данные.

7. Щелкните правой кнопкой мыши на этом отчете и выберите в контекстном меню пункт View⇨Performance Monitor (Вид⇨Монитор производительности).

   Окно монитора производительности будет выглядеть похожим на то, что представлено на рис. 30.23. Здесь отображаются те же отчетные данные, что и на шаге 6, но на этот раз внутри унаследованного монитора производительности.

Как видите, разобраться здесь непросто и вообще воспринимается он нелегко. Хотя, как говорят, лучше один раз увидеть, чем сто раз услышать, составить отчетливое представление о функционировании системы на основе графика в унаследованном мониторе производительности довольно затруднительно. В Microsoft провели великолепную работу по прояснению этих данных и отображению их в виде отчета.

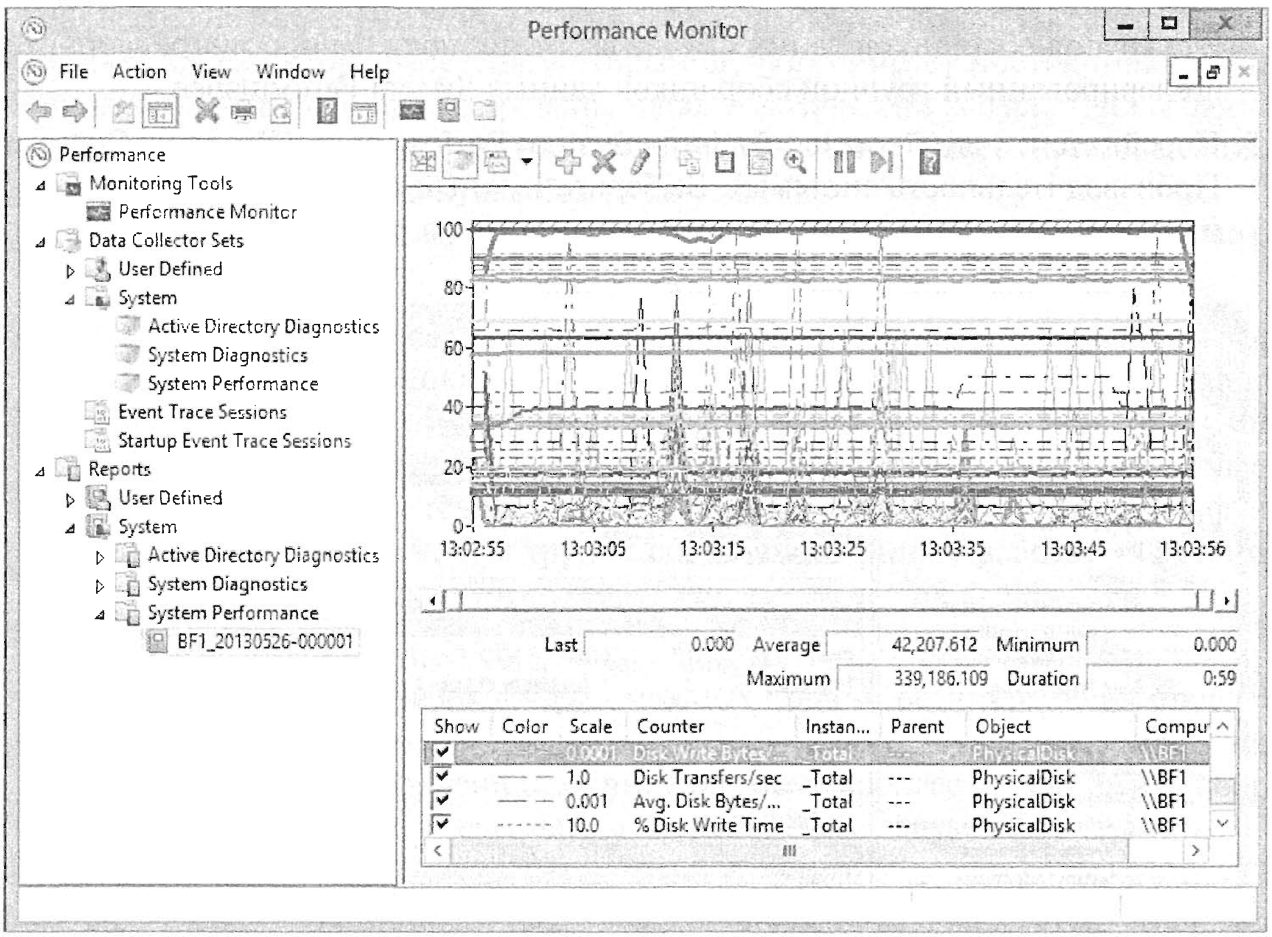


Рис. 30.23. Просмотр отчета о выполнении группы сборщиков данных в графическом режиме

8. Щелкните правой кнопкой мыши на этом отчете и выберите в контекстном меню пункт View⇨Folder (Вид⇨Папка).

   Это приводит к отображению представления проводника Windows с файлами, которые были задействованы при создании отчета. По умолчанию группы сборщиков данных System Performance хранятся в папке `c:\Perflogs\System\Performance`. Каждый отчет будет содержаться в отдельной папке.

9. Когда группа сборщиков данных System Diagnostics завершит работу, щелкните на ней правой кнопкой мыши и выберите в контекстном меню пункт Latest Report (Самый последний отчет).

10. Просмотрите этот отчет.

Обратите внимание, что раздел Warnings (Предупреждения) включает симптомы, причину, подробности и предлагаемый способ устранения каждой ошибки. Кроме того, в разделе Related (Связанная информация) часто предоставляется ссылка на веб-сайт, где можно найти информацию, имеющую отношение к данной ошибке.

Группы сборщиков данных, определяемые пользователем

Вы можете создавать собственные группы сборщиков данных, удовлетворяющие конкретным потребностям. В отличие от предварительно сформированных групп сборщиков данных, любые свойства группы сборщиков данных, определяемой пользователем, допускают модификацию. В число этих свойств входит продолжительность времени выполнения и график, применяемый для запуска.

При создании группы сборщиков данных, определяемой пользователем, вы обычно начинаете с шаблона, в качестве которого может выступать любая предварительно сформированная группа сборщиков данных. Группу сборщиков данных можно также создать с нуля, хотя это несколько напоминает попытку повторно изобрести колесо. Шаблоны предоставляют хорошую отправную точку.

Существуют две наиболее распространенных причины для создания группы сборщиков данных, определяемой пользователем.

- **Создание базового уровня.** Базовый уровень будет документировать работу системы в определенный момент времени. Если позже производительность снизится, вам будет легко идентифицировать, какой ресурс или приложение вызвало эту проблему.
- **Планирование запуска группы сборщиков данных.** Запуск группы сборщиков данных, определяемой пользователем, можно запланировать на регулярной основе. Например, вы можете создать две группы сборщиков данных на основе встроенных шаблонов System Diagnostics и System Performance, после чего спланировать их запуск раз в день. Затем вы можете регулярно просматривать их отчеты, и если на сервере возникнет какая-то проблема, то в вашем распоряжении будет простая для анализа хронология.

Две описанные ниже процедуры продемонстрируют создание базового уровня и настройку расписания для запуска группы сборщиков данных на регулярной основе.

Воспользуйтесь следующими шагами, чтобы создать группу сборщиков данных, которая может применяться в качестве базового уровня.

1. Запустите комплект монитора производительности из начального экрана Windows Server 2012 R2, набрав **`perfmon`** и нажав <Enter>, или через пункт меню Tools⇨Performance Monitor (Сервис⇨Монитор производительности) диспетчера серверов.
2. Перейдите к узлу Data Collector Sets⇨User Defined (Группы сборщиков данных⇨Определяемые пользователем), чтобы получить доступ к предварительно сформированным группам сборщиков данных.
3. Щелкните правой кнопкой мыши на узле User Defined и выберите в контекстном меню пункт New⇨Data Collector Set (Создать⇨Группа сборщиков данных).
4. Введите `Baseline` для имени своей группы сборщиков данных.
5. Удостоверьтесь в том, что выбран переключатель Create From a Template (Recommended) (Создать из шаблона (рекомендуется)), и щелкните на кнопке Next (Далее).
6. Выберите шаблон System Performance и щелкните на кнопке Next.

7. Примите стандартное место для хранения данных и щелкните на кнопке Next.

   На производственном сервере вы можете изменить этот путь, указав место на другом разделе, чтобы не соперничать за дисковый ввод-вывод с операционной системой.

8. На экране Create the Data Collector Set (Создание группы сборщиков данных) можно назначить другую учетную запись для запуска группы сборщиков данных.

   По умолчанию выбирается встроенная учетная запись `System`, которую можно использовать для локальной системы.

9. Щелкните на кнопке Finish (Готово).

10. Щелкните правой кнопкой мыши на группе сборщиков данных Baseline и выберите в контекстном меню пункт Start (Запустить).

    Эта группа сборщиков данных проработает в течение 1 минуты и завершится. Во время ее выполнения на экране отображается значок, похожий на кнопку Play (Воспроизведение). По завершении работы значок исчезнет.

11. Перейдите к узлу Reports⇨User Defined⇨Baseline (Отчеты⇨Определяемые пользователем⇨Baseline). Выберите отчет из группы Baseline и просмотрите его.

    На данном этапе нет никакой разницы между вашей определяемой пользователем группой сборщиков данных и группой сборщиков данных System Performance.

12. Щелкните правой кнопкой мыши на группе сборщиков данных Baseline и выберите в контекстном меню пункт Properties (Свойства).

13. В открывшемся диалоговом окне свойств группы Baseline перейдите на вкладку Stop Condition (Условие останова).

14. В поле со списком Units (Единицы измерения) возле флажка Overall Duration (Общая продолжительность) выберите вместо Minutes (Минуты) вариант Weeks (Недели).

    Диалоговое окно свойств группы Baseline будет подобным показанному на рис. 30.24.

15. Перейдите на вкладке Directory (Каталог).

    Обратите внимание, что место хранения отчета и формат имени отчета можно изменять. По умолчанию отчеты именуются в соответствии со следующим соглашением: `ИмяСервера_ггггммдд-порядковый номер`. По мере модификации настроек на этой вкладке, в нижней ее части отображается пример имени.

16. Просмотрите остальные вкладки диалогового окна свойств группы Baseline.

    Как видите, можно конфигурировать много свойств, но ни на одной из вкладок не представлен интервал выборки.

17. Щелкните на кнопке OK, чтобы сохранить внесенные изменения.

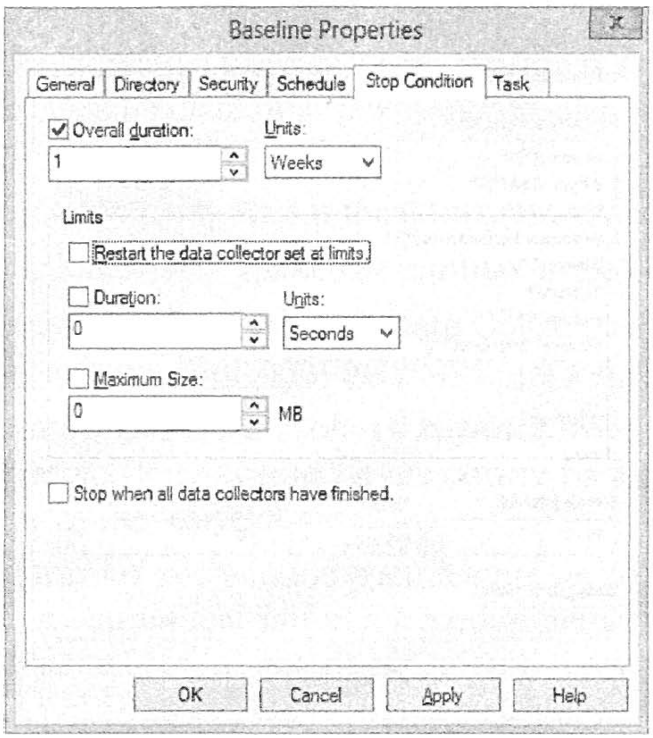


Рис. 30.24. Изменение свойств группы сборщиков данных

Измените стандартный интервал выборки

Стандартный интервал выборки составляет 1 секунду, т.е. группа сборщиков данных будет захватывать все метрики каждую секунду. В случае захвата данных на протяжении 60 секунд ежесекундная выборка вполне уместна. Тем не менее, когда данные захватываются в течение полной недели как часть построения базового уровня, для получения точной картины производительности системы достаточно производить выборки каждые 30–45 минут.

18. При выбранной группе сборщиков данных Baseline щелкните правой кнопкой мыши на элементе Performance Counter (Счетчик производительности) и выберите в контекстном меню пункт Properties.

    В открывшемся диалоговом окне Performance Counter Properties (Свойства счетчика производительности) можно добавлять и удалять счетчики производительности. Например, при выполнении мониторинга сервера, на котором функционирует SQL Server, возможно, к основным счетчикам ресурсов понадобится добавить некоторые счетчики производительности SQL Server.

19. Измените значение в поле Sample Interval (Интервал выборки) с `1` на `45` и выберите в поле со списком Units (Единицы измерения) вместо Seconds (Секунды) вариант Minutes (Минуты).

    Диалоговое окно Performance Counter Properties представлено на рис. 30.25.

20. Щелкните на кнопке OK.

К этому моменту вы располагаете группой сборщиков данных, которая будет выполняться на протяжении недели и производить выборки каждые 45 минут. Ее можно запускать вручную или модифицировать свойства с целью установки расписания для запуска группы в определенный день. В любом случае она будет работать в течение семи дней и создаст отчет базового уровня по системе.

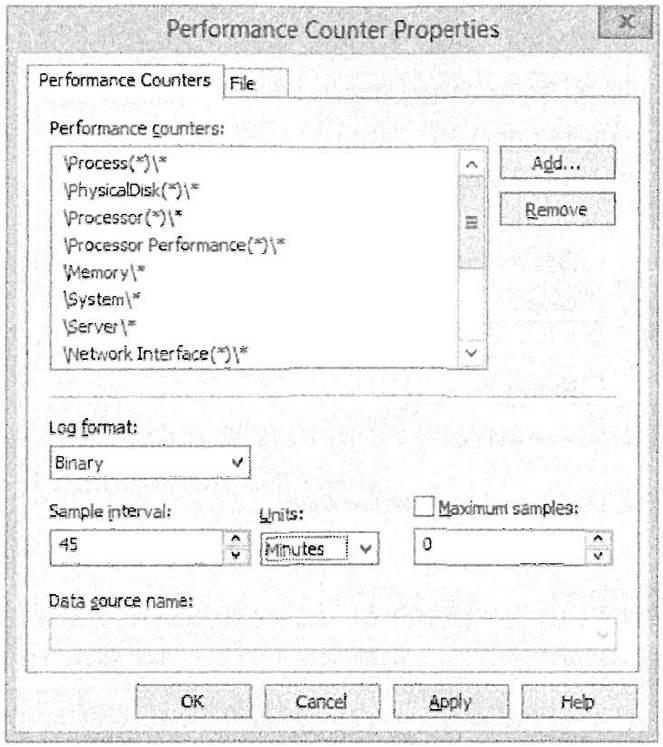


Рис. 30.25. Изменение свойств счетчиков производительности

Вы можете также вручную остановить любую группу сборщиков данных. Щелкните правой кнопкой мыши на выполняющейся группе сборщиков данных и выберите в контекстном меню пункт Stop (Остановить).

Только одна группа сборщиков данных за раз

Группам сборщиков данных требуется монопольный доступ к некоторым системным ресурсам. По этой причине за раз можно выполнять только одну группу сборщиков данных. Если одна группа функционирует, а вы пытаетесь запустить другую группу, то получите сообщение об ошибке. Как только выполнение первой группы сборщиков данных завершится, можно запускать другую группу, но учтите, что группы в очередь не ставятся.

Если вы создали в предыдущем упражнении группу базового уровня и запустили ее, то эту группу понадобится остановить, прежде чем получится запустить группу сборщиков данных, которая будет построена в следующем упражнении.

Чтобы создать группу сборщиков данных диагностики системы и запланировать ее на запуск раз в день, выполните перечисленные ниже действия.

1. Запустите монитор производительности, выбрав в меню Start (Пуск) пункт Administrative Tools⇨Performance Monitor (Администрирование⇨Монитор производительности).
2. Перейдите к узлу Data Collector Sets⇨User Defined (Группы сборщиков данных⇨Определяемые пользователем), чтобы получить доступ к предварительно сформированным группам сборщиков данных.
3. Щелкните правой кнопкой мыши на узле User Defined и выберите в контекстном меню пункт New⇨Data Collector Set (Создать⇨Группа сборщиков данных).

4. Введите `Routine Diagnostics` для имени своей группы сборщиков данных. Удостоверьтесь в том, что выбран переключатель Create From a Template (Recommended) (Создать из шаблона (рекомендуется)), и щелкните на кнопке Next (Далее).
5. Выберите шаблон System Diagnostics и щелкните на кнопке Next.
6. Примите стандартное место для хранения данных и щелкните на кнопке Next.
7. Отметьте флажок Open Properties for this Data Collector Set (Открыть свойства для этой группы сборщиков данных) и щелкните на кнопке Finish (Готово).
8. В открывшемся диалоговом окне свойств группы Routine Diagnostics перейдите на вкладку Schedule (Расписание) и щелкните на кнопке Add (Добавить), чтобы добавить расписание запуска.

   Обратите внимание, что по умолчанию расписание не создается. Тем не менее, можно добавлять расписания для запуска в любой день недели, в любое время суток, в любой день календаря и для прекращения своего действия по достижении любой даты.
9. Щелкните на кнопке OK, чтобы принять стандартное расписание, предусматривающее запуск в полночь каждого дня недели.
10. Щелкните на кнопке OK, чтобы завершить создание группы сборщиков данных Routine Diagnostics.

Теперь вы располагаете группой сборщиков данных, определяемой пользователем, которая будет запускаться ежедневно.

Обслуживание отчетов

Регулярное создание отчетов предполагает наличие определенных политик сохранения важных данных. Наихудшим сценарием является ситуация, когда отчеты занимают все больше и больше дискового пространства и система прекращает работу, что, конечно же, крайне нежелательно. К счастью, имеются встроенные защитные механизмы, которые предотвращают ситуации подобного рода. Однако эти защитные механизмы способны также удалить отчеты, которые могут понадобиться в будущем.

Отчеты объединяются для каждой группы сборщиков данных и управляются индивидуальными политиками сохранения данных. Каждый раз, когда вы запускаете группу сборщиков данных, в том же самом узле или папке создается еще один отчет и проводится анализ остальных отчетов для выяснения необходимости в их удалении или архивировании. Управление политикой сохранения данных осуществляется на вкладках Data Manager (Диспетчер данных) и Actions (Действия) диалогового окна свойств отчетов.

На рис. 30.26 показана вкладка Data Manager для определяемой пользователем группы сборщиков данных Routine Diagnostics. Чтобы получить доступ к этому окну, необходимо щелкнуть правой кнопкой мыши на нужной группе отчетов и выбрать в контекстном меню пункт Properties (Свойства). Группа отчетов будет иметь такое же имя, как и группа сборщиков данных. В этом примере группа отчетов находится в Reports⇨User Defined⇨Routine Diagnostics (Отчеты⇨Определяемые пользователем⇨Routine Diagnostics).

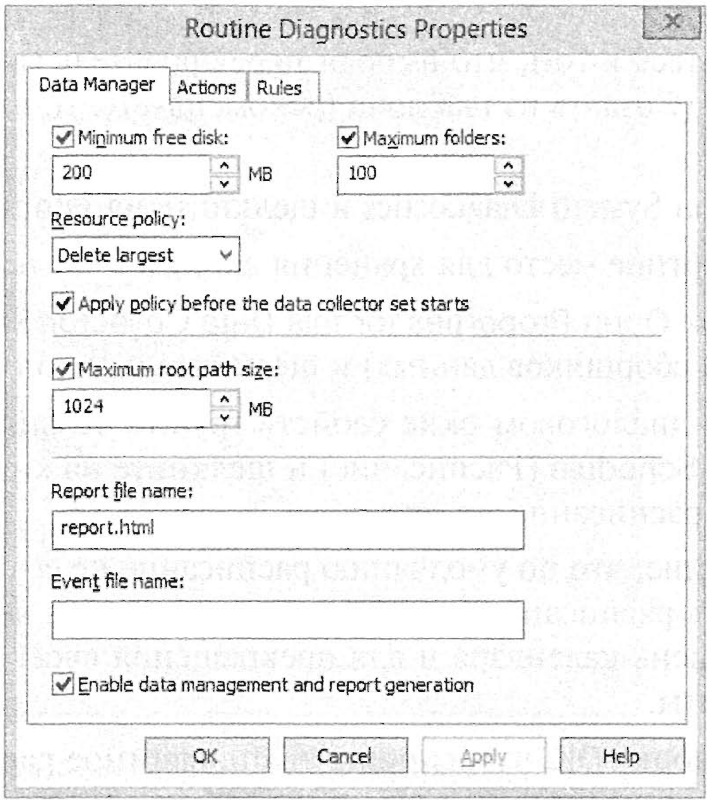


Рис. 30.26. Управление отчетами

Вкладка Data Manager предоставляет детали того, когда будут удаляться отчеты на основе степени использования диска. Перечисленные ниже настройки призваны предотвратить потребление отчетами целиком всего диска.

- **Minimum Free Disk (Минимум места на диске) и Maximum Folders (Максимум папок).** Если объем свободного пространства на диске опускается ниже минимального порогового значения (200 Мбайт по умолчанию) или количество папок превышает максимальное пороговое значение (100 отчетов по умолчанию), то политика инициирует удаление отчетов до тех пор, пока занимаемый объем не перестанет превышать порог. Каждый отчет содержится в отдельной папке, поэтому в данном контексте папка является синонимом отчета.
- **Resource Policy (Политика ресурсов).** Когда достигается определенное пороговое значение, можно выбрать между удалением либо самых больших отчетов (по умолчанию), либо самых старых отчетов.
- **Apply Policy Before The Data Collector Starts (Применить политику перед запуском группы сборщиков данных).** Отметка этого флажка приведет к тому, что данные будут удалены перед запуском группы сборщиков данных. Если этот флажок не отмечен, то ограничения, установленные на вкладке Data Manager, будут игнорироваться. Сохранение данных будет управляться исключительно правилами, определенными на вкладке Actions.
- **Maximum Root Path Size (Максимальный размер корневого пути).** Относится ко всем данным отчетов в этом общем пути. Например, общим путем по умолчанию является `c:\Perflogs`. Если объем всех данных отчетов превышает 1 Гбайт, то применение этой политики приведет к удалению или архивированию файлов. Настройка Maximum Root Path Size имеет более высокий приоритет, чем настройки Minimum Free Disk и Maximum Folders.

Папка Perflogs

При необходимости вы можете получать доступ к отчетам непосредственно с использованием проводника Windows. Если вы перейдете в папку `c:\Perflogs`, то увидите в ней две папки: `Admin` и `System`. В папке `Admin` содержатся данные отчетов от всех групп сборщиков данных, определяемых пользователем. В папке `System` находятся данные отчетов от всех системных групп сборщиков данных. Также есть возможность выбрать для любых групп сборщиков данных, созданных пользователем, другой путь, в том числе другой раздел.

На вкладке Actions находятся детали того, как отчеты архивируются и удаляются, даже если степень использования диска не превысила определенные пороговые значения. Если щелкнуть здесь на кнопке Add (Добавить) или Edit (Редактировать), откроется окно Folder Action (Действие для папки), которое применяется для создания условий, связанных с любым запланированным действием. Для отчетов, которые были созданы на основе шаблонов, доступны три стандартных действия для папки.

- **1 Day (1 дн.).** Спустя день будет создан файл CAB, а исходные данные удалены. Файл CAB — это формат архива, который может использоваться пользователем для восстановления исходных данных. Прежде чем данные можно будет просматривать в отчете, они должны быть сначала извлечены из файла CAB. Данные, архивированные в файл CAB, перестанут отображаться в представлении Reports (Отчеты) монитора производительности. Однако вы можете извлечь эти данные в другую папку и дважды щелкнуть на файле `report.html`, чтобы просмотреть отчет.
- **8 Weeks (8 нед.).** Файл CAB будет удален. Останется файл `report.xml`, который содержит необработанные данные из отчета.
- **24 Weeks (24 нед.).** Отчет будет удален. Это правило также будет проверяться в отношении исходных данных и файла CAB. Если исходные данные или файл существует, он также будет удален.

Сохраните свой отчет

Если вы хотите сохранить любой отчет и гарантировать, что он не будет удален в результате применения политик сохранения данных, то должны скопировать всю папку в другое место с помощью проводника Windows. Когда возникнет необходимость просмотреть этот отчет, откройте созданную папку и дважды щелкните на документе `report.html`. Полностью этот отчет можно увидеть в Internet Explorer. Кроме того, вы можете изменить политику сохранения данных так, чтобы она не приводила к автоматическому удалению этого отчета.

Инструменты PAL и PerfView

Теперь, когда вы знаете, как пользоваться комплектом встроенных инструментов монитора производительности для анализа функционирования развернутых копий Windows Server, настало время изучить несколько дополнительных внешних инструментов, которые могут быть полезны при выполнении углубленных исследований производительности, недоступных с помощью только встроенных инструментов.

Инструменты PAL (Performance Analysis of Logs — Анализ производительности по журналам) и PerfView помогут упростить сбор и анализ данных о производительности, а также создать всеобъемлющие базовые уровни производительности для существующих приложений, которые выполняются под управлением Windows Server 2012 R2.

Введение в PAL

Инструмент PAL был разработан примерно в 2007 году сотрудником Microsoft Клинтом Хаффманом и доступен для бесплатной загрузки по ссылке `http://pal.codeplex.com/`. Запускаемый в окне PowerShell, он позволяет анализировать существующие журналы счетчиков производительности и генерировать отчеты, позволяющие получить базовые уровни с использованием пороговых значений, которые были определены Microsoft и касаются производительности ваших приложений и систем. Инструмент PAL может быть очень полезным, когда применяется в сочетании с журналами счетчиков (файлы `*.blg`), генерируемыми группами сборщиков данных монитора производительности, которые мы обсуждали ранее.

В следующем разделе мы обсудим предварительные условия для работы инструмента PAL и опишем процедуру его установки.

Предварительные условия

Перед установкой PAL удостоверьтесь в том, что собираетесь запускать этот инструмент на клиенте, функционирующем под управлением минимум 64-разрядной версии Windows 7. Это единственная клиентская операционная система, для которой разработчик протестировал самый последний выпуск своего инструмента, однако PAL успешно работает в средах Windows 8 и Windows Server 2012 R2. Кроме того, на компьютере, где будет выполняться PAL, должны быть установлены следующие программные продукты:

- PowerShell v2.0 или выше;
- Microsoft .NET Framework 3.5 Service Pack 1;
- Microsoft Chart Controls (Элементы управления диаграммами Microsoft) для Microsoft .NET Framework 3.5.

Установка

После того как все перечисленные выше предварительные условия для установки PAL удовлетворены, а инструмент загружен, установите его с помощью перечисленных далее действий.

1. Войдите в систему компьютера, где вы собираетесь установить PAL, с использованием административной учетной записью.
2. Перейдите в папку, где находятся загруженные двоичные файлы, щелкните правой кнопкой мыши на `setup.exe` и выберите в контекстном меню пункт Run as administrator (Запуск от имени администратора), чтобы начать установку.
3. На экране приветствия мастера ознакомьтесь с предупреждением о настройке политики выполнения PowerShell и щелкните на кнопке Next (Далее).
4. Укажите папку для установки и два раза щелкните на кнопке Next.
5. На экране Installation Complete (Завершение установки) щелкните на кнопке Close (Закрыть), чтобы завершить работу мастера.

Использование PAL

Теперь, когда инструмент PAL установлен, настало время подготовить его к эффективному применению. В этом разделе мы рассмотрим процедуру первоначального конфигурирования, необходимую для генерации вашего первого отчета. Если вы еще не проработали задачи из раздела "Системные группы сборщиков данных", то займитесь этим сейчас, т.к. мы будем использовать журнальный файл счетчиков производительности, который сгенерирован как цель для инструмента PAL.

1. Войдите в систему компьютера, где был установлен инструмент PAL, с применением административной учетной записи и запустите инструмент PAL.

   После запуска PAL откроется мастер PAL (PAL Wizard), начальный экран которого показан на рис. 30.27. Этот мастер поможет быстро сконфигурировать PAL.

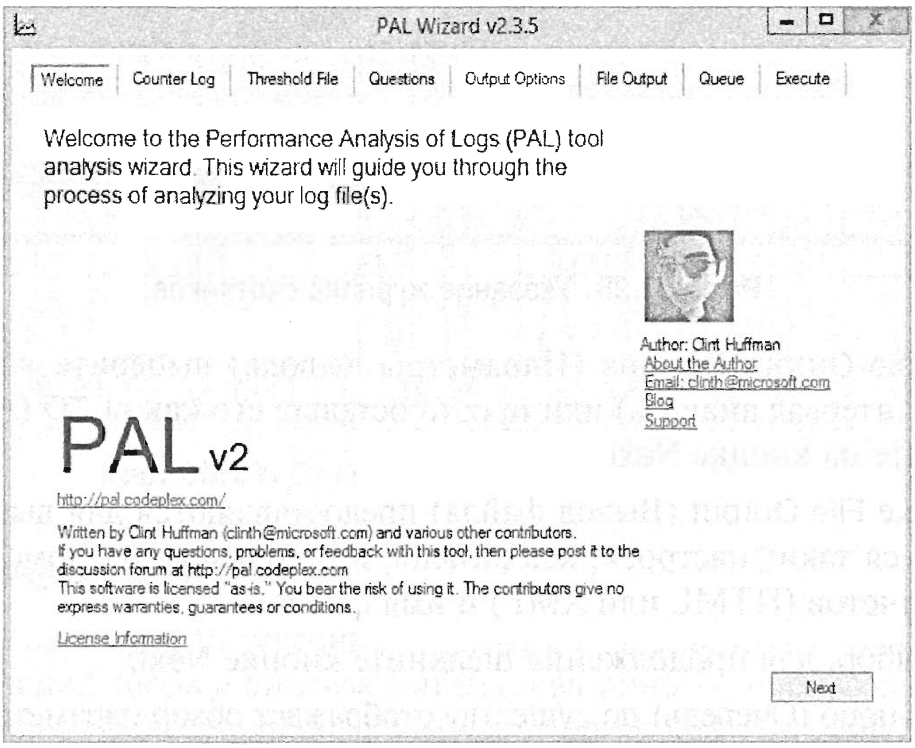


Рис. 30.27. Мастер PAL Wizard

2. Щелкните на кнопке Next (Далее), чтобы приступить к конфигурированию.
3. На вкладке Counter Log (Журнал счетчиков) укажите местоположение журналов счетчиков, которые хотите применять для анализа.

   Мы собираемся использовать сгенерированный ранее журнал счетчиков System Performance, который находится в `c:\Perflogs\System\Performance`. Вкладка вкладке Counter Log представлена на рис. 30.28. Здесь также можно выбрать диапазон даты и времени, на котором будет сфокусирован этот отчет.
4. Для продолжения щелкните на кнопке Next.
5. На вкладке Threshold File (Файл пороговых значений) выберите System Overview (Обзор системы) в качестве заголовка файла и щелкните на кнопке Next.
6. На вкладке Questions (Вопросы) щелкните на каждом вопросе и введите запрашиваемую информацию, основываясь на компьютере, где были сгенерированы журналы счетчиков (Number of Processors (Количество процессоров), Total Memory (Общий объем памяти) и т.д.), а затем щелкните на кнопке Next.

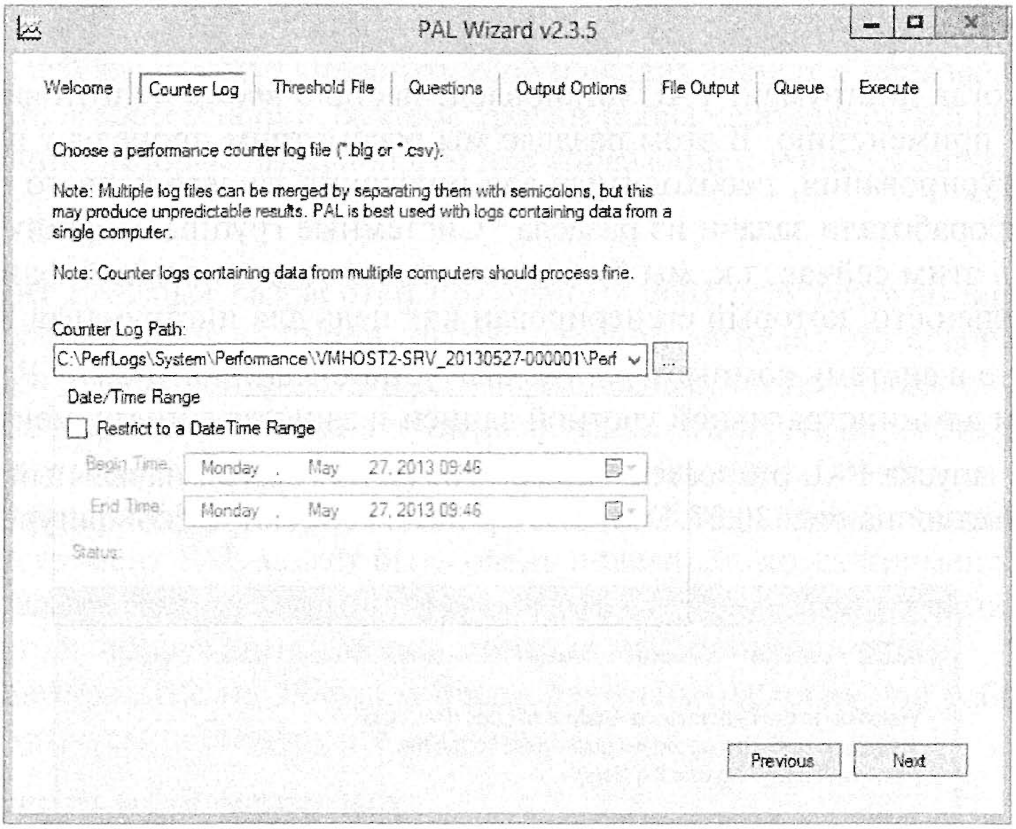


Рис. 30.28. Указание журнала счетчиков

7. На вкладке Output Options (Параметры вывода) выберите вариант Analysis Interval (Интервал анализа) или просто оставьте его как AUTO (Автоматически) и щелкните на кнопке Next.
8. На вкладке File Output (Вывод файла) предоставляются для выбора варианты, касающиеся таких настроек, как каталог, в который будут помещаться отчеты, формат отчетов (HTML или XML) и имя файла.
9. Сделав выбор, для продолжения щелкните кнопке Next.

   Вкладка Queue (Очередь) по существу отображает обзор параметров, выбранных в мастере до сих пор, и позволяет удалить элементы из очереди выполнения.
10. Щелкните на кнопке Next.
11. На вкладке Execute (Выполнить) можно выбрать немедленное выполнение анализа, добавление в очередь новых элементов либо выполнение анализа перед перезапуском мастера с теми же настройками для удобства.
12. Щелчок на кнопке Finish (Готово) приводит к запуску сценария, который работает с журналами счетчиков, указанными для генерации вашего отчета. После нескольких минут функционирования PowerShell вы должны увидеть результаты анализа, которые будут выглядеть примерно так, как показано на рис. 30.29.

Этот отчет является лишь одним примером углубленной информации, которую можно получить при использовании PAL в сочетании с комплектом инструментов монитора производительности, встроенных в Windows Server 2012 R2. Дополнительные сведения о PAL доступны в блоге Клинта Хаффмана; в частности, обратите внимание на статью, посвященную сценарию сборки данных PAL:

```
http://tinyurl.com/ws2012pal
```

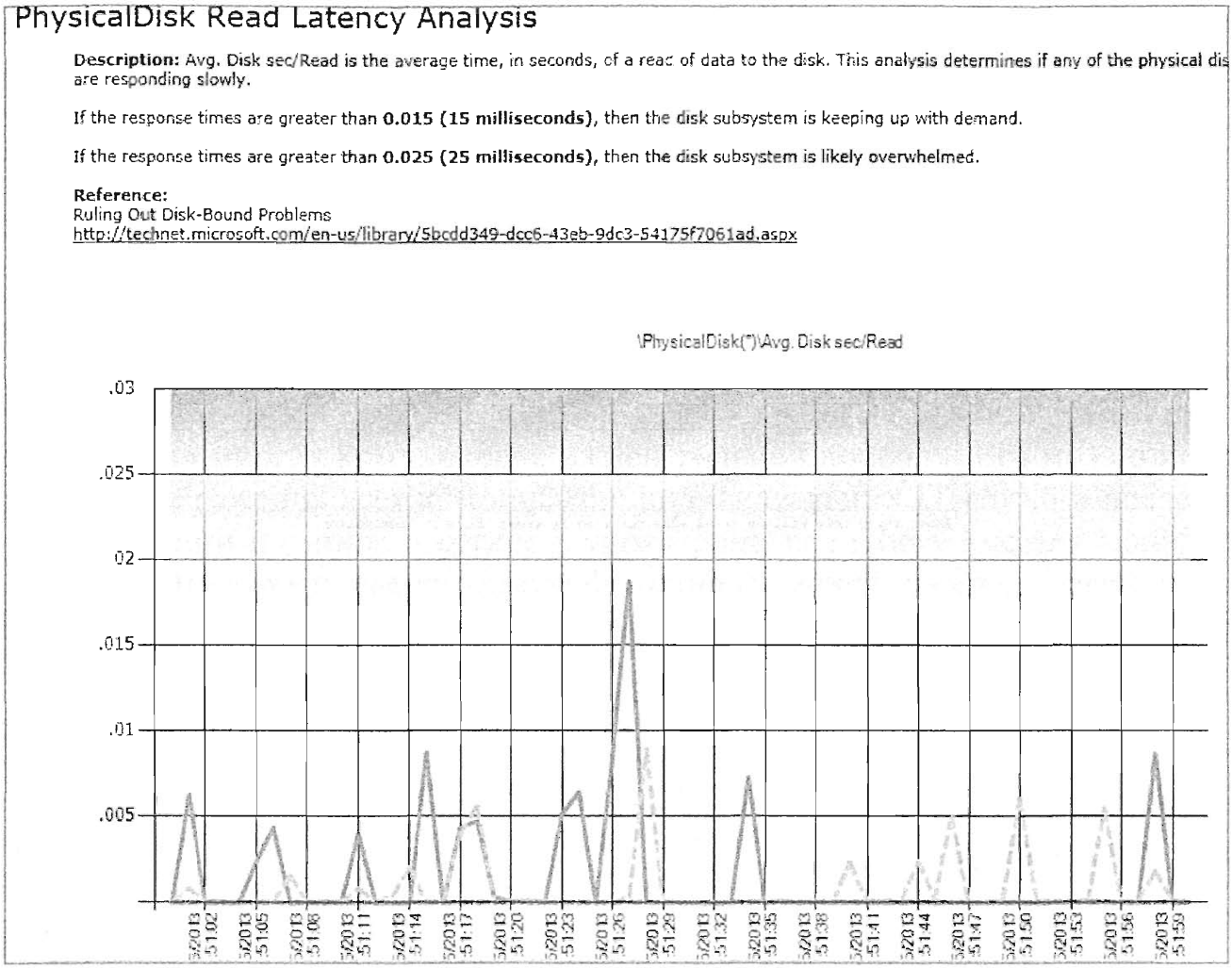


Рис. 30.29. Отчет с результатами анализа

Инструмент PerfView

PerfView — это еще один интересный инструмент анализа, который можно применять для упрощения сбора и анализа данных, связанных с производительностью. Он работает на более глубоком уровне, чем монитор производительности или PAL, и при сборе информации использует средство трассировки событий для Windows (Event Tracing for Windows — ETW) операционной системы Windows Server 2012 R2. Обычно информация ETW такого типа может показаться слишком специфичной, но для специалистов по мониторингу производительности из группы Windows Performance в Microsoft, которые имеют дело с этим инструментом, она транслируется в понятный и простой в применении формат. На рис. 30.30 приведен пример инструмента PerfView в действии.

Этот гибкий инструмент позволяет углубиться в стеки ЦП и дискового ввода-вывода, если вы испытываете такую потребность. Из-за того, что данный инструмент ориентирован на разработчиков, вопросы его развертывания и использования выходят за рамки настоящей книги, однако он, несомненно, стоит добавления в арсенал средств анализа производительности. Инструмент PerfView доступен для бесплатной загрузки в Microsoft Download Center:

```
http://tinyurl.com/ws2012perfview
```

Обязательно ознакомьтесь с сопутствующими руководствами пользователя и примерами применения PerfView.

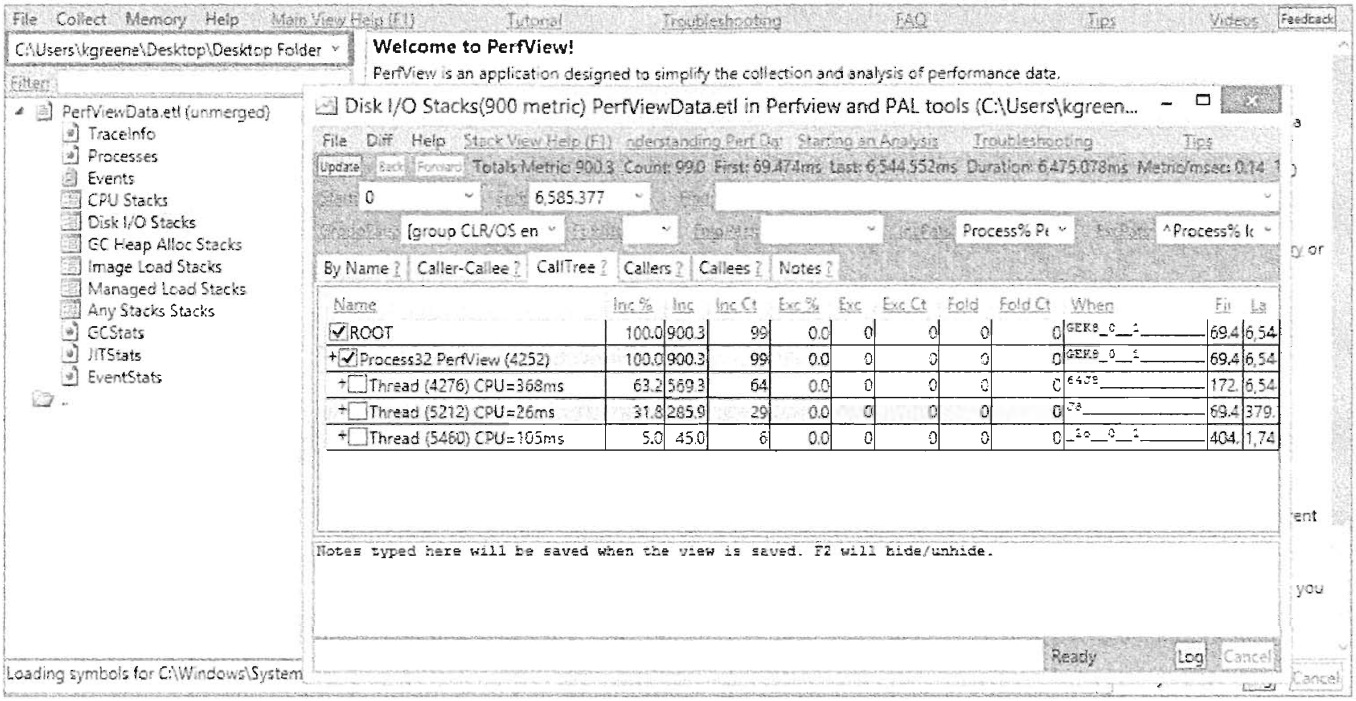


Рис. 30.30. Инструмент PerfView

Расширенный мониторинг с помощью System Center 2012 R2

Если вы тщательно проработали все главы этой книги и уже перенесли свои развертывания Windows Server, Failover Clustering, Hyper-V и т.д. из испытательной среды в производственную, вам наверняка понадобится дополнить эти развертывания решением по управлению и мониторингу уровня предприятия. Это требование удовлетворяется Microsoft предоставлением комплекта инструментов System Center 2012 R2 (Системный центр 2012 R2).

В состав System Center 2012 R2 входят следующие восемь основных продуктов:

- Operations Manager (мониторинг)
- Virtual Machine Manager (управление структурой)
- Service Manager (управление инцидентами, изменениями и службами)
- Orchestrator (автоматизация)
- Data Protection Manager (резервное копирование)
- App Controller (управление гибридным облаком)
- Configuration Manager (управление устройствами)
- Endpoint Protection (защита от вредоносного ПО и вирусов)

Каждый из этих продуктов играет свою роль в рамках истории облачной ОС от Microsoft, которая воплотила в себе средства управления частным и открытым облаком. Продуктом, о котором мы собираемся рассказать в этом разделе, является Operations Manager (Диспетчер операций), поскольку его можно задействовать для обеспечения полной прозрачности мониторинга развертываний Windows Server 2012 R2 и связанных с ними соглашений об уровне обслуживания (service-level agreement — SLA).

Operations Manager — довольно крупный продукт, чтобы с ним можно было с ходу разобраться, и мы не можем раскрыть здесь все его возможности и функциональность. Если вы хотите получить дополнительные сведения об Operations Manager, почитайте книгу *Mastering System Center 2012 Operations Manager* (Sybex, 2012 г.).

Введение в Operations Manager

Диспетчер операций (Operations Manager, также известный как OpsMgr или SCOM) представляет собой решение сквозного мониторинга, которое охватывает среду Microsoft и 19 других межплатформенных сред. Диспетчер операций позволяет централизованно проводить мониторинг серверов, приложений, оборудования и операций для многих компьютеров из центральной консоли. Его можно использовать для отображения всех компонентов индивидуальных IT-служб и последующей их организации в единое и легкое в управлении представление для мониторинга. Представляйте его как расширенную функциональность групп серверов, о которой шла речь ранее в этой главе, за исключением того, что вместо простого группирования серверов вы размещаете в одном месте все свои компоненты служб.

В качестве примера того, что можно делать с помощью Operations Manager, возьмем службу электронной почты в любой организации. Отдел информационных технологий должен иметь возможность наблюдать не только за серверами Microsoft Exchange, которые обрабатывают электронную почту для своей компании, но и за такими компонентами, как сеть SAN, хосты Hyper-V, операционная система Windows Server, сетевые коммутаторы и маршрутизаторы. Все эти компоненты вместе образуют службу электронной почты в целом, и если какой-то из них выходит из строя, то вся служба электронной почты потенциально может прекратить работу. Это называется *моделированием IT-службы* или *IT как служба*.

Располагая возможностью управления и проведения мониторинга своей службы как единого целого, вы можете получить представление по общей работоспособности этой службы. Индикатор состояния службы будет отображаться зеленым цветом, если она работает нормально, красным цветом, когда служба имеет критические ошибки, и желтым цветом при появлении предупреждения. По сравнению с рядом более традиционных методов мониторинга такой подход позволяет значительно быстрее вскрывать глубинные причины ухудшения работоспособности IT-служб. На рис. 30.31 показан пример IT как службы с использованием Operations Manager.

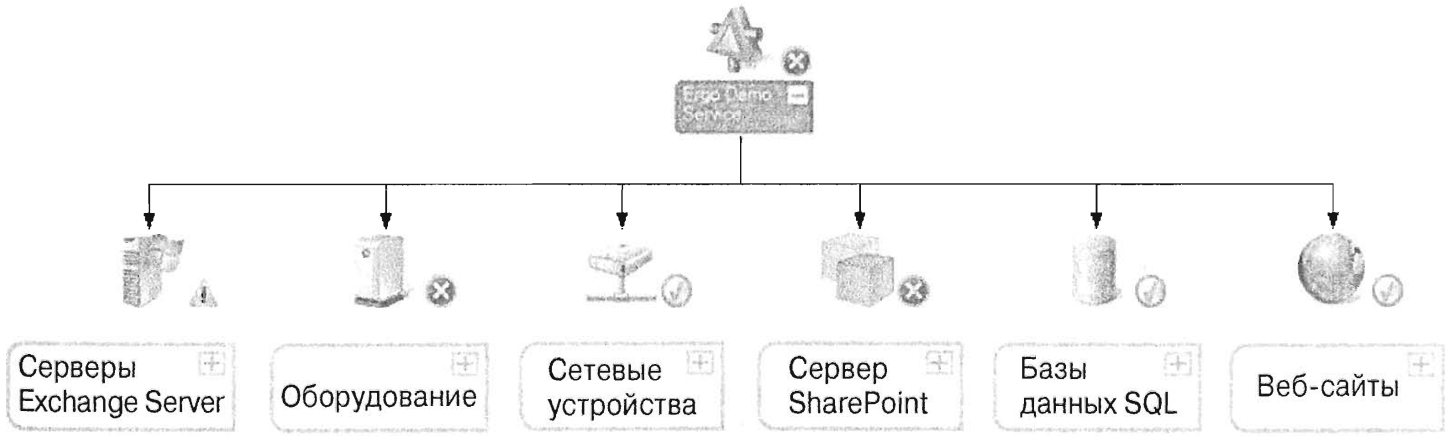


Рис. 30.31. IT как служба

Обзор пакетов управления

В отличие от ряда других доступных на рынке решений мониторинга, пытающихся наблюдать за всеми компонентами с самого начала, когда вы впервые развертываете Operations Manager и решаете поместить агент на сервер, он будет видеть этот сервер как сущность, которая либо функционирует, либо нет. Например, Operations Manager не будет знать, что агент развернут на компьютере Windows Server 2012 R2 или что он выполняется на сервере, имеющем установленную роль Hyper-V.

Диспетчеру операций известно, что он должен выполнять мониторинг на каждом агенте через специальные пакеты управления, которые были разработаны и сделаны доступными либо поставщиком приложения/продукта, либо сообществом System Center. Эти пакеты управления проливают свет на инфраструктуру Operations Manager и позволяют агентам воспринимать компоненты, которые необходимо взять под контроль мониторинга.

Мониторинг Windows Server 2012 R2

В Microsoft выпустили для Windows Server 2012 R2 большое количество пакетов управления (management pack — MP), охватывающих практически все важные роли, которые могут быть развернуты в среде этой операционной системы. Ниже перечислены примеры:

- Windows Server Active Directory MP (Пакет управления для Active Directory сервера Windows)
- Windows Server Base Operating System MP (Пакет управления для базовой операционной системы сервера Windows)
- Windows Server Cluster Management MP (Пакет управления для администрирования кластеров сервера Windows)
- Windows Server DNS 2012 MP (Пакет управления для DNS 2012 сервера Windows)
- Windows Server DHCP 2012 MP (Пакет управления для DHCP 2012 сервера Windows)
- Windows Server File and iSCSI Services MP (Пакет управления для файловых служб и служб iSCSI сервера Windows)
- Windows Server Group Policy MP (Пакет управления для групповой политики сервера Windows)
- Windows Server Hyper-V 2012 MP (Пакет управления для Hyper-V 2012 сервера Windows)
- Windows Server Internet Information Services MP (Пакет управления для информационных служб Интернета сервера Windows)
- Windows Server Network Load Balancing MP (Пакет управления для балансировки сетевой нагрузки сервера Windows)
- Windows Server Print Server MP (Пакет управления для сервера печати сервера Windows)
- Windows Server Remote Desktop Services 2012 MP (Пакет управления для служб удаленных рабочих столов сервера Windows)
- Windows Terminal Services MP (Пакет управления для терминальных служб Windows)

Каждый из этих пакетов управления содержит собственные оповещения, мониторы, правила, задачи, диаграммы, управляющие панели и даже отчеты, основанные на связанной технологии, для мониторинга которой пакет был предназначен. Тот факт, что каждый пакет управления разрабатывался вместе с реальной группой продуктов Microsoft, реализующей роль или компонент, означает наличие оптимального решения мониторинга, учитывающего все рекомендации передового опыта, которые вы получили бы в результате поиска в Интернете, если бы понадобилась помощь.

С полным перечнем всех доступных пакетов управления Microsoft для Operations Manager можно ознакомиться по ссылке `http://tinyurl.com/ws2012scom`.

Исследование пакета управления Windows Server Base Operating System MP

Если ранее вам не приходилось иметь дело с Operations Manager, то прежде чем развертывать любой пакет управления, вы должны прочитать руководство по этому пакету. Эти руководства похожи на обычные руководства пользователя: они предоставляют много полезной информации о том, что может и чего не может делать пакет управления. Объем руководства по пакету Windows Server Base Operating System MP приближается к 60 страницам, но если вы уделите время его изучению, то узнаете обо всех компонентах Windows Server, которые данный пакет может обнаруживать и отслеживать, таких как диски, ЦП, память и сетевые адаптеры.

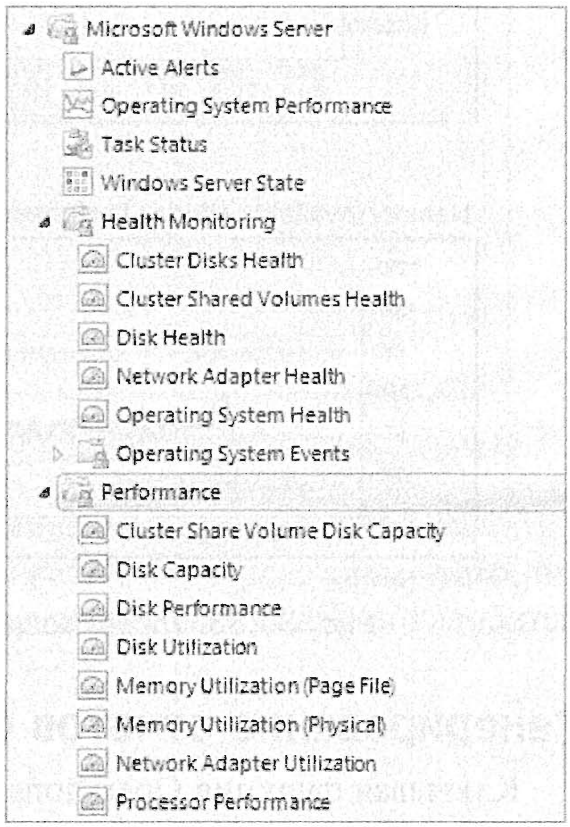


Рис. 30.32. Пакет управления Windows Server Base Operating System MP

Вдобавок с этим пакетом поступает большое количество отчетов, которые позволяют создавать базовые уровни производительности, а также проверять степень использования и конфигурацию. Кроме того, эти отчеты помогают контролировать возникновение повседневных ситуаций вроде нехватки дискового пространства на всех серверах. На рис. 30.32 показаны все представления, имеющие отношение к мониторингу работоспособности и производительности, которые доступны при мониторинге Windows Server 2012 R2 с помощью Operations Manager.

Мониторинг производительности

Диспетчер операций использует базу данных SQL, которая хранит данные мониторинга и производительности для одного года. Такой объем данных означает, что она будет одной из самых крупных баз данных SQL, с которыми вам придется иметь дело как IT-администратору. Однако это также означает, что вы можете быстро создавать управляющие панели и представления базовых уровней, охватывающие любой желаемый период за последний год. Наличие доступа к такой углубленной информации является великолепным способом понять функционирование приложений и служб, критически важных для ведения бизнеса.

Функциональность управляющих панелей в Operations Manager облегчает выявление этих данных и представление их на экране для обеспечения наилучшей визуализации среды, подвергаемой мониторингу. На рис. 30.33 приведен пример управляющей панели мониторинга производительности в действии.

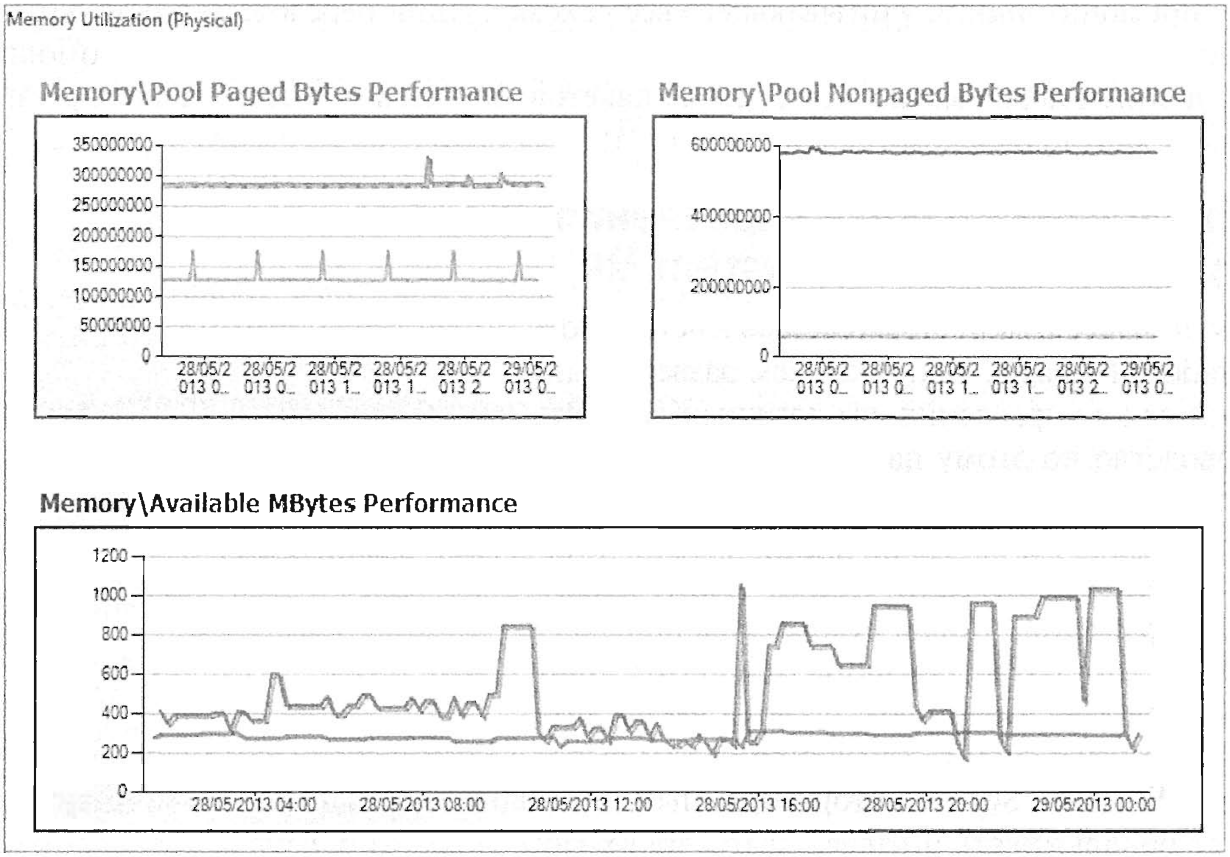


Рис. 30.33. Управляющая панель мониторинга производительности

Генерирование отчетов с помощью Operations Manager

Ключевая функция Operations Manager заключается в получении всей информации о компьютерах, приложениях и устройствах, которая находится в хранилище данных, и затем в предоставлении вам возможности быстро сгенерировать широкое разнообразие отчетов, помогающих упрочить свою роль как IT-администратора. Вы можете сконфигурировать отчеты так, чтобы они генерировались по мере необходимости либо на основе расписания с отправкой результатов по электронной почте. Такое средство настройки расписания является отличным способом своевременного предоставления владельцам и руководству разных подразделений требуемой информации, которая оформлена в удобном для них виде (рис. 30.34).

Резюме

Используйте диспетчер серверов для мониторинга множества серверов. Новая консоль диспетчера серверов в Windows Server 2012 R2 обеспечивает мониторинг и проверку работоспособности инфраструктуры локальных и удаленных серверов. Ее можно применять для мониторинга нескольких серверов и ролей, за которые они отвечают, причем все это из одной центральной консоли.

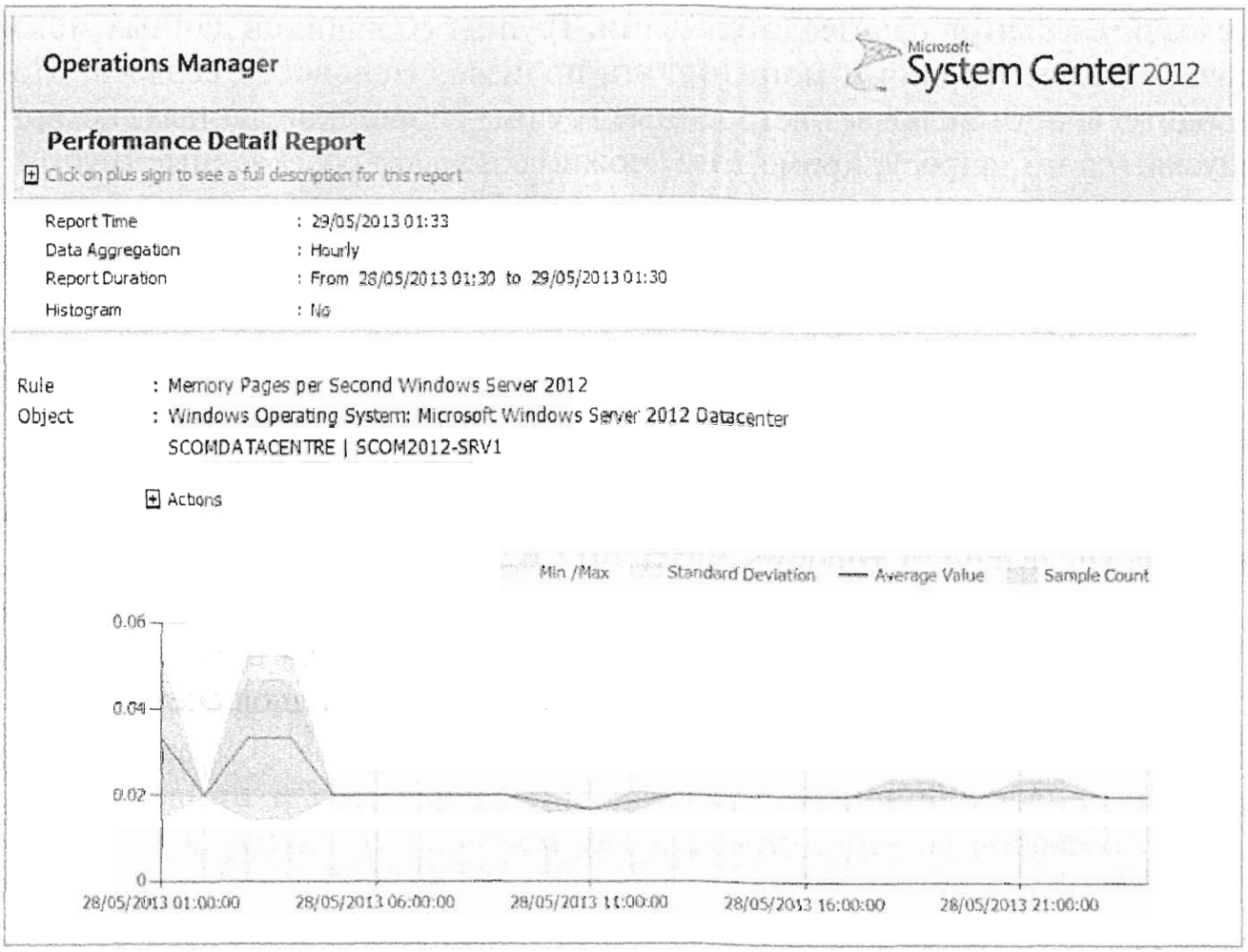


Рис. 30.34. Пример отчета, сгенерированного в Operations Manager

Контрольный вопрос. Вам необходимо знать комплексное состояние работоспособности для коллективных ролей на множестве серверов; кроме того, вы хотите управлять ими посредством диспетчера серверов. Что вам понадобится развернуть?

а. Группы доступа

б. Группы серверов

в. Группы рассылки

г. Административные группы

Научитесь пользоваться средством Event Viewer. Средство Event Viewer в Windows Server 2012 R2 является одним из важнейших инструментов, используемых для мониторинга системы. Часто он оказывается одним из первых мест, куда вы будете заглядывать, когда обнаружите, что в сервере имеется проблема, однако Event Viewer можно также применять и для упреждающего мониторинга серверов. Средство Event Viewer может помочь в быстрой идентификации источника проблемы или, по крайней мере, в получении достаточного объема информации, чтобы знать, куда двигаться дальше.

Контрольный вопрос. Вы только что развернули роль Hyper-V на своем компьютере Windows Server 2012 R2. Где вы будете искать журнал событий, связанный с этой ролью?

Исследуйте монитор производительности. Группы сборщиков данных можно использовать для измерения и мониторинга производительности сервера. Монитор производительности включает встроенные группы сборщиков данных, которые могут запускаться по запросу; кроме того, можно создавать собственные группы сборщиков данных.

Контрольный вопрос. Запустите группу сборщиков данных System Performance и просмотрите результирующий отчет.

Исследуйте инструменты PAL и PerfView. Инструменты Performance Analysis of Logs (PAL) и PerfView являются двумя дополнительными внешними средствами, которые помогают упростить сбор и анализ данных о производительности, а также создать всеобъемлющие базовые уровни производительности для приложений, функционирующих под управлением Windows Server 2012 R2.

Контрольный вопрос. Инструмент PAL может быть очень полезным, когда применяется в сочетании с журналами счетчиков монитора производительности. Какое расширение используется для файлов этих журналов счетчиков?

а. `.chk`

б. `.perf`

в. `.blg`

г. `.evnt`

Изучите диспетчер операций, входящий в состав System Center 2012 R2. Диспетчер операций (Operations Manager, также известный как OpsMgr или SCOM) представляет собой решение сквозного мониторинга, которое охватывает среду Microsoft и 19 других межплатформенных сред. Диспетчер операций позволяет централизованно проводить мониторинг серверов, приложений, оборудования и операций для многих компьютеров из центральной консоли. Его можно использовать для отображения всех компонентов индивидуальных IT-служб и последующей их организации в единое и легкое в управлении представление для мониторинга.

Контрольный вопрос. Когда вы впервые развертываете Operations Manager и решаете поместить агент на сервер, он будет видеть этот сервер как сущность, которая либо функционирует, либо нет. Как заставить Operations Manager видеть разные роли и приложения на серверах?

Глава 31

Управление исправлениями

Управление исправлениями было процессом снижения до минимума уязвимостей организации за счет управления и развертывания обновлений программного обеспечения. С течением временем оно переместилось на поддержку обновлений компонентов и продукта в целом. Обновления могут развертываться и управляться с помощью нескольких продуктов и инструментов; примером может служить System Center Configuration Manager (Диспетчер конфигурации системного центра). В этой главе мы сосредоточим внимание на комплекте инструментов, встроенном в инфраструктуру Windows Server 2012 R2, и рассмотрим предлагаемые им возможности. В современном мире информационных технологий, основами которого являются Интернет и сотрудничество, внесение изменений в программное обеспечение стало повседневной задачей. Частота, с которой вы развертываете и проверяете актуальность обновлений, может означать разницу между тратой выходных на восстановление скомпрометированных или разрушенных систем и проведением их в кругу семьи или друзей.

Обновление программного обеспечения выглядит как бесконечный процесс, и если только вы не предпочитаете лично подходить к каждому компьютеру для установки обновлений, то вам понадобятся инструменты, которые помогут справиться с этой работой. Помимо инструментов необходим также надежный процесс управления исправлениями. Вам нужно знать, применимо ли каждое обновление к компьютерам в сети, совместимо ли оно с существующими приложениями и насколько срочно следует развертывать данное обновление.

В настоящей главе мы обсудим установку и конфигурирование роли Windows Server Update Services для Windows Server 2012 R2 и расскажем, что должно приниматься во внимание при развертывании этого процесса управления исправлениями. Кроме того, мы проанализируем обновления безопасности и подробно рассмотрим службу обновления сервера Windows (Windows Server Update Services — WSUS), которая теперь интегрирована в операционную систему в виде серверной роли. Вдобавок мы объясним, как перейти от WSUS версии Windows Server 2008 R2 к WSUS версии Windows Server 2012 R2. Наконец, мы представим обзор доступных командлетов PowerShell.

В этой главе вы изучите следующие темы:

- использование автоматических обновлений Windows (Windows Automatic Updates) для проверки наличия новых обновлений на компьютере, работающем под управлением Windows 8;
- применение автономной программы установки обновлений Windows (Windows Update Standalone Installer) для молчаливой установки обновления безопасности;
- идентификация четырех фаз управления исправлениями.

Что нового в Windows Server Update Services версии Windows Server 2012 R2

Служба Windows Server Update Services (WSUS) теперь интегрирована в Windows Server 2012 R2. Эта новая роль позволяет администраторам использовать диспетчер серверов для конфигурирования и управления обновлениями; в новую версию WSUS включены те же возможности генерации отчетов и обновления состояния, что и ранее, а также несколько новых средств и модификаций предыдущей функциональности.

Новые возможности WSUS v6 в Windows Server 2012 R2

В версию WSUS v6 было добавлено несколько новых возможностей, базовый перечень которых приведен ниже.

- Службы можно добавлять или удалять с помощью диспетчера серверов.
- Доступны командлеты PowerShell для управления десятком наиболее важных задач в службе WSUS.
- Для обеспечения дополнительной безопасности добавлена возможность хеширования SHA256.
- Обеспечивается разделение клиента и сервера. Версии агента обновления Windows (Windows Update Agent — WUA) могут поставляться независимо от WSUS.

Требования к программному обеспечению для серверов и клиентов WSUS

Прежде чем устанавливать WSUS в существующей среде, вы должны удостовериться в том, что сервер (серверы) и клиенты WSUS удовлетворяют минимальным требованиям к программному обеспечению.

На серверах WSUS должно быть установлено, как минимум, следующее программное обеспечение:

- операционная система Windows Server 2012 R2;
- службы Internet Information Services (IIS);
- инфраструктура .NET Framework 4.0 или более новая версия;
- если вы используете отдельный сервер базы данных, то должны иметь компьютер, на котором функционирует SQL Server 2012 R2 либо SQL Server 2008 R2 с пакетом обновлений SP1 или более новая версия.

Конечные точки WSUS должны быть основаны на версии 7.8 агента Windows Update Agent (WUAgent 7.8). Клиенты WSUS должны работать под управлением одной из перечисленных далее операционных систем:

- Windows 8
- Windows RT
- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 с пакетом обновлений SP1
- Windows Vista

Ниже приведен список баз данных, поддерживаемых WSUS:

- Windows Internal Database (WID)
- Microsoft SQL Server 2012 R2 Standard Edition
- Microsoft SQL Server 2012 R2 Enterprise Edition
- Microsoft SQL Server 2012 R2 Express Edition
- Microsoft SQL Server 2008 R2 SP1 Standard Edition
- Microsoft SQL Server 2008 R2 SP1 Enterprise Edition
- Microsoft SQL Server 2008 R2 SP 1 Express Edition

Предельный размер базы данных в SQL Server Express 2012 и SQL Server Express 2008 R2 составляет 10 Гбайт; для многих сред его может оказаться достаточно, но это ограничение очень важно учитывать при определении подходящего предельного размера для вашей системы. Размышления по поводу размера всегда должны начинаться с числа клиентов, которое вы собираетесь поддерживать, и количества платформ.

Сценарии развертывания

Версия WSUS в Windows Server 2012 R2 была изменена так, чтобы сценарии развертывания фокусировались не столько на размере предприятия, сколько на требованиях в отношении емкости и местоположения. Тремя основными вариантами развертывания являются одиночный сервер WSUS, несколько серверов WSUS и отключенный сервер WSUS. Для организаций средних и крупных размеров или сложной инфраструктуры вы должны подумать о применении какого-то продукта из семейства System Center (`www.microsoft.com/systemcenter`).

Сценарий с развертыванием единственного экземпляра предполагает использование одного главного сервера WSUS, который синхронизируется непосредственно со службой Microsoft Update. Клиенты WSUS могут быть разбросаны по разным географическим регионам, но все они находятся за одним и тем же брандмауэром (рис. 31.1).

Многие организации средних и крупных размеров эксплуатируют многосерверную инфраструктуру, которая состоит из нескольких серверов WSUS, обслуживающих множество географически распределенных клиентов. Один сервер WSUS может синхронизироваться с другим (рис. 31.2) или они могут получать обновления от Microsoft Update по отдельности.

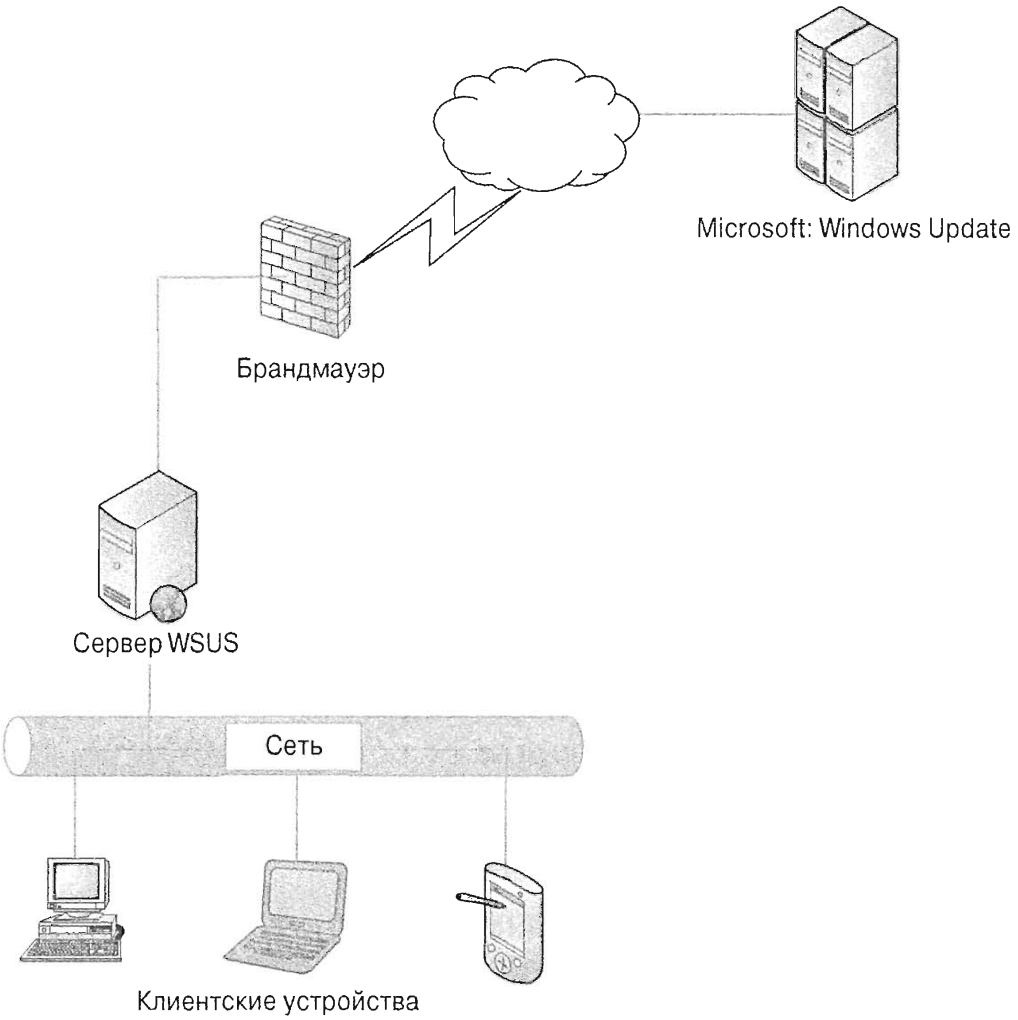


Рис. 31.1. Развертывание с одиночным сервером WSUS

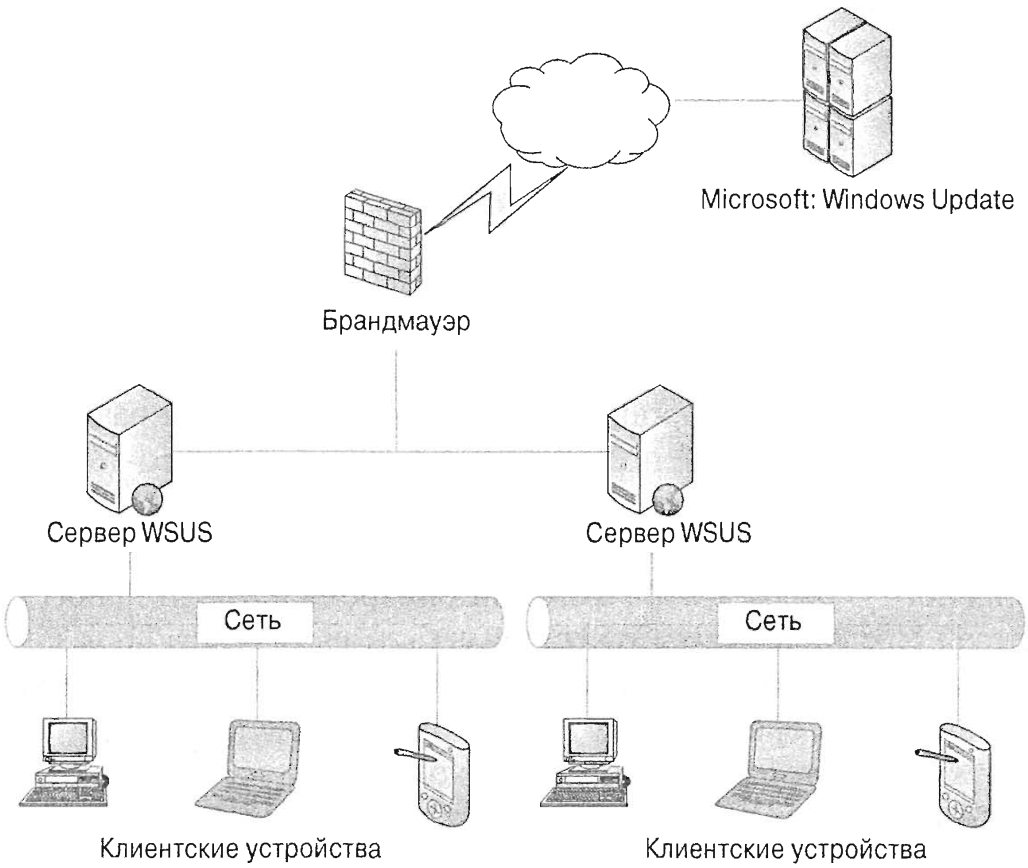


Рис. 31.2. Развертывание с несколькими серверами WSUS, в котором один сервер WSUS синхронизируется с другим

В этой конфигурации только один сервер виден из Интернета, а остальные настроены как нижестоящие серверы, которые должны синхронизироваться с первым сервером. Преимущество наличия единственного сервера, синхронизирующегося с Microsoft Update, заключается в том, что другие серверы WSUS из Интернета не видны.

Сценарий с отключенной инфраструктурой предназначен для компьютеров, которым не разрешен доступ в Интернет или которые располагают только ограниченным доступом к нему. Получать обновления для компьютеров, подключенных к такой изолированной сети, можно путем настройки в этой отключенной сети сервера WSUS. После обработки всех исправлений для производственной сети их можно экспортировать на устройства наподобие USB-дисков. Ниже описаны базовые шаги этого процесса.

1. Экспортируйте исправления из консоли WSUS на USB-диск. Для их экспорта необходимо воспользоваться командой `WSUTIL.exe`.
2. Импортируйте исправления на отключенный сервер WSUS.
3. Настройте расписание и разверните исправления.

Как только исправления будут экспортированы, их можно импортировать на отключенный сервер WSUS, как показано на рис. 31.3, а развертывание может производиться на основе расписания для этого сервера WSUS.

Рис. 31.3. Развертывание с отключенным сервером WSUS

Построение сложных иерархий с использованием WSUS

В зависимости от типа развертывания сервера и нужд организации существуют дополнительные преимущества применения новой версии Windows Server. Это помогает минимизировать развертывания серверного оборудования (или виртуальные развертывания), требуемые для управления средой. Используя возможности Windows Server 2012 R2 и WSUS, вы можете сконфигурировать автономный (Autonomous) режим, режим реплики (Replica), а также настроить клиентов в филиалах и блуждающих клиентов.

Автономный режим, обычно называемый распределенным режимом, является стандартным вариантом установки для WSUS. В этой конфигурации (показанной на рис. 31.4) вышестоящий сервер используется для обмена обновлениями с одним или несколькими нижестоящими серверами, и за счет внедрения средств управления доступом вы можете предоставить локальным администраторам возможность управления собственными средами.

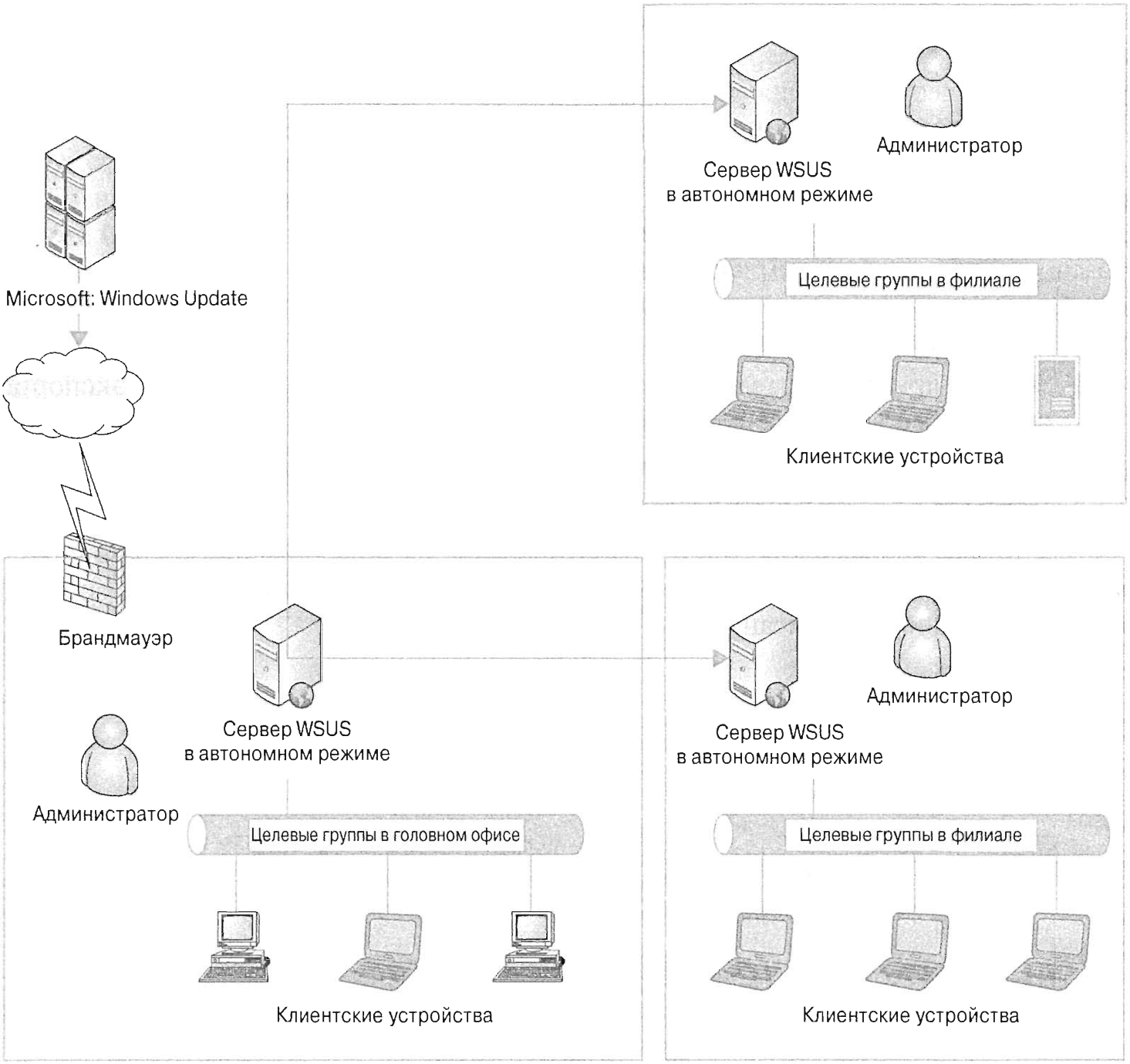


Рис. 31.4. Автономный режим в многосайтовой среде

Режим реплики (рис. 31.5) представляет собой проектное решение с централизованным администрированием и позволяет вышестоящему серверу обмениваться своими обновлениями, клиентскими группами и другими компонентами с нижестоящими серверами.

Серверы реплики — это просто нижестоящие серверы, которые управляются посредством главного вышестоящего сервера. Такая конфигурация оказывается самой удобной, когда центральный IT-отдел управляет обновлениями в сценарии с несколькими сайтами или офисами филиалов.

Офисы филиалов — один из новейших сценариев, введенных в Windows Server 2012 R2. В этой конфигурации используется средство BranchCache, доступное в Windows Server 2012 R2 (`http://tinyurl.com/BranchCache`). С помощью средств BranchCache и Branch Office, реализованных в Windows, можно сократить нагрузку на канал WAN и улучшить показатель времени реакции системы.

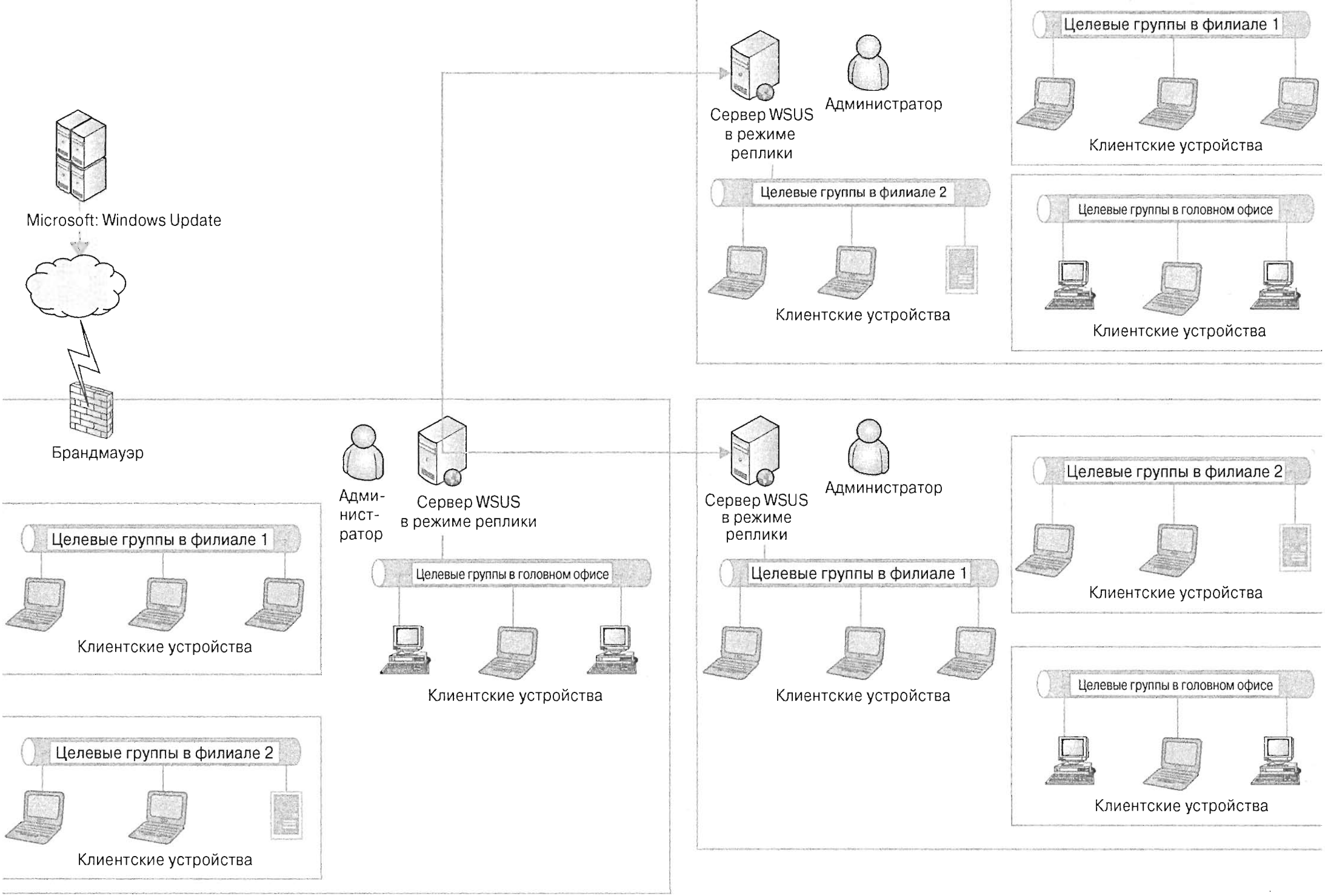


Рис. 31.5. Режим реплики в сценарии с несколькими офисами филиалов

Установка и конфигурирование управления исправлениями

Установка обновлений на компьютерах в сети вашей организации критически важна для обеспечения безопасности этой сети и оптимального функционирования клиентских компьютеров организации. Распространение обновлений требует планирования и тестирования, гарантирующего успешную их установку. В Microsoft рекомендуют применять поэтапный подход к управлению исправлениями; каждый этап подробно обсуждается на веб-сайте Microsoft TechNet по ссылке:

```
https://technet.microsoft.com/en-us/library/cc700845.aspx
```

Установка роли WSUS в Windows Server 2012 R2

Одним из новых средств Windows Server 2012 R2 является возможность установки серверной роли с автоматическим добавлением всех обязательных компонентов как части процесса установки. В предыдущих версиях Windows Server многие роли и компоненты приходилось конфигурировать как отдельные задачи.

Чтобы установить роль WSUS в Windows Server 2012 R2, выполните следующие шаги.

1. Откройте управляющую панель диспетчера серверов и щелкните на ссылке Add roles and features (Добавить роли и компоненты), как показано на рис. 31.6.
2. Войдите в систему компьютера с использованием учетной записи из локальной группы `Administrators` или администратора домена.
3. Запустите диспетчер серверов (по умолчанию в Windows Server 2012 R2 он запускается автоматически).

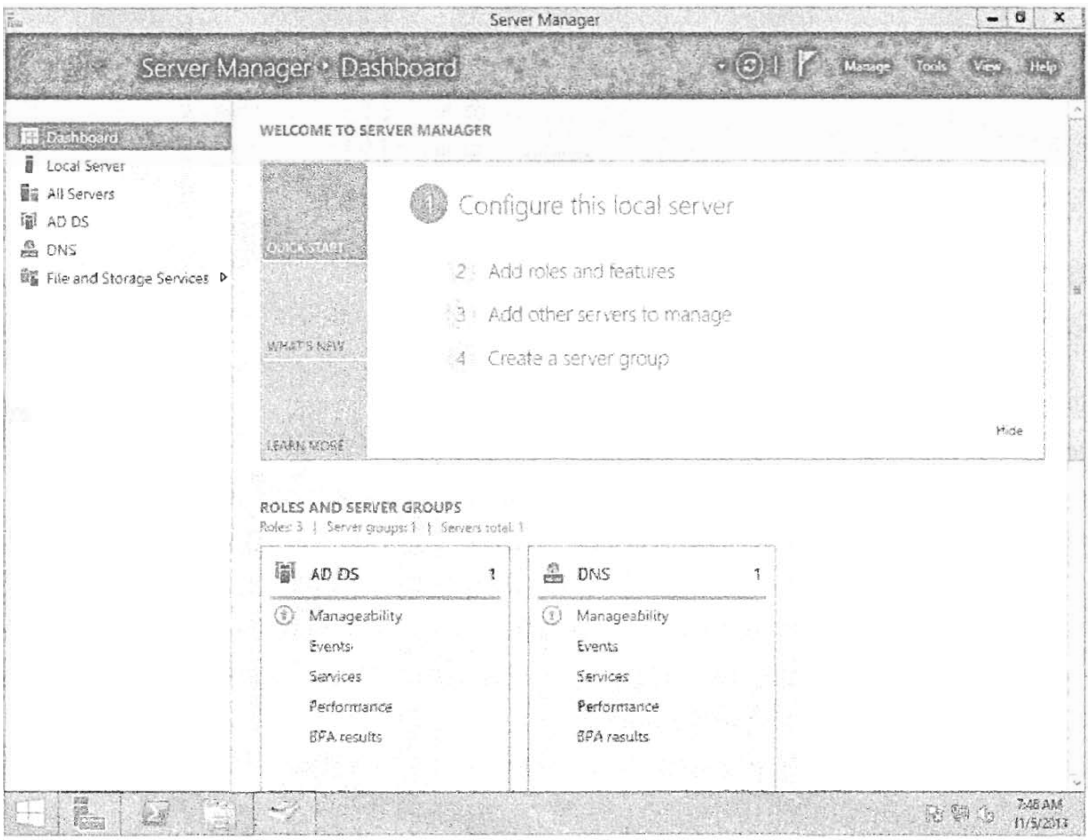


Рис. 31.6. Добавление ролей в Windows Server 2012 R2

4. В разделе Configure this local server (Конфигурировать этот локальный сервер) щелкните на ссылке Add Roles and Features.
5. На экране Before You Begin (Прежде чем начать) щелкните на кнопке Next (Далее).
6. Выберите переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) для типа установки и щелкните на кнопке Next.
7. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным ваш сервер, как предлагается по умолчанию, и щелкните на кнопке Next.

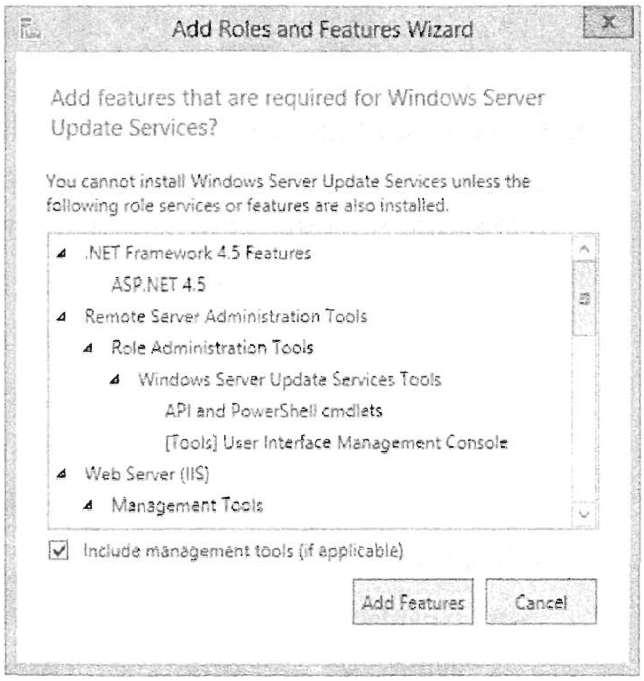


Рис. 31.7. Обязательные компоненты для Windows Server Update Services

8. Выполните прокрутку вниз до роли Windows Server Update Services, отметьте флажок рядом с ней и щелкните на кнопке Next.
9. Для продолжения установки будет предложено добавить дополнительные компоненты, как показано на рис. 31.7.
10. Щелкните на кнопке Add Features (Добавить компоненты). Вы заметите, что компонент Web Server (IIS) также выбран; щелкните на кнопке Next.

    Откроется экран Features (Компоненты) с заранее отмеченными флажками для следующих компонентов:

    - Remote Server Administration Tools (Инструменты дистанционного администрирования серверов)
    - Windows Internal Database (Внутренняя база данных Windows)
    - Windows Process Activation (Активация процессов Windows)
11. Просмотрите выбранные параметры и щелкните на кнопке Next.
12. Откроется экран Windows Server Update Services (Службы обновления сервера Windows); щелкните на кнопке Next.

    В разделе Role Services (Службы роли) по умолчанию отмечены флажки WID Database (Windows Internal Database) (База данных WID (внутренняя база данных Windows)) и WSUS Services (Службы WSUS). Кнопка Database (База данных) предусмотрена на тот случай, если вы намерены использовать базу данных SQL на другом сервере; она предоставит дополнительные параметры.
13. Оставьте все без изменений и щелкните на кнопке Next.

    Следующий экран позволяет выбрать местоположение файлов Windows Update (если вы решили сделать их доступными локально); в рассматриваемом примере снимите отметку с этого флажка. Тем самым вы получаете возможность сохранить все обновления на сервере Microsoft Update и применять их, когда это необходимо.

14. После снятия отметки с флажка Store updates in the following location (Сохранять обновления в следующем месте) щелкните на кнопке Next.
15. Откроется экран Web Server Role (IIS); щелкните на кнопке Next.

    После этого отобразится экран Role Services (Службы роли), где будут заранее выбраны перечисленные ниже флажки.

    - Common HTTP Features (Общие компоненты HTTP):
      - Default Document (Стандартный документ)
      - Static Content (Статическое содержимое)
    - Performance (Производительность):
      - Dynamic Content Compression (Динамическое сжатие содержимого)
    - Security (Безопасность):
      - Request Filtering (Фильтрация запросов)
      - Windows Authentication (Аутентификация Windows)
    - Application Development (Разработка приложений):
      - .NET Extensibility 4.5 (.NET Extensibility 4.5)
      - ASP.NET 4.5
      - ISAPI Extensions (Расширения ISAPI)
      - ISAPI Filters (Фильтры ISAPI)
    - Management Tools (Инструменты управления):
      - IIS Management Console (Консоль управления IIS)
      - IIS 6 Management Compatibility (Совместимость с управлением IIS 6)
      - IIS 6 Metabase Compatibility (Совместимость с метабазой IIS 6)
16. Просмотрите выбранные параметры и щелкните на кнопке Next.
17. Подтвердите выбранные параметры установки и щелкните на кнопке Install (Установить).

Операционная система Windows Server 2012 R2 позволяет выбирать и экспортировать любые настройки конфигурации, сделанные в ходе установки ролей и компонентов (рис. 31.8). Вы найдете ссылку Export configuration settings (Экспортировать настройки конфигурации) в нижней части экрана очень удобной, когда вы создаете множество идентичных конфигураций серверов или настроили специфичную конфигурацию и хотите ее сохранить.

Конфигурирование WSUS для развертывания

После завершения установки серверной роли WSUS вы можете запустить службу Windows Server Update Services из начального экрана (рис. 31.9) и приступить к конфигурированию.

Чтобы начать конфигурирование сервера WSUS, необходимо настроить обновления, требуемые для вашей среды. После открытия консоли Update Services запустится мастер конфигурирования службы обновления сервера Windows (Windows Server Update Services Configuration Wizard), который проведет через последовательность шагов по настройке параметров обновлений для последующего развертывания.

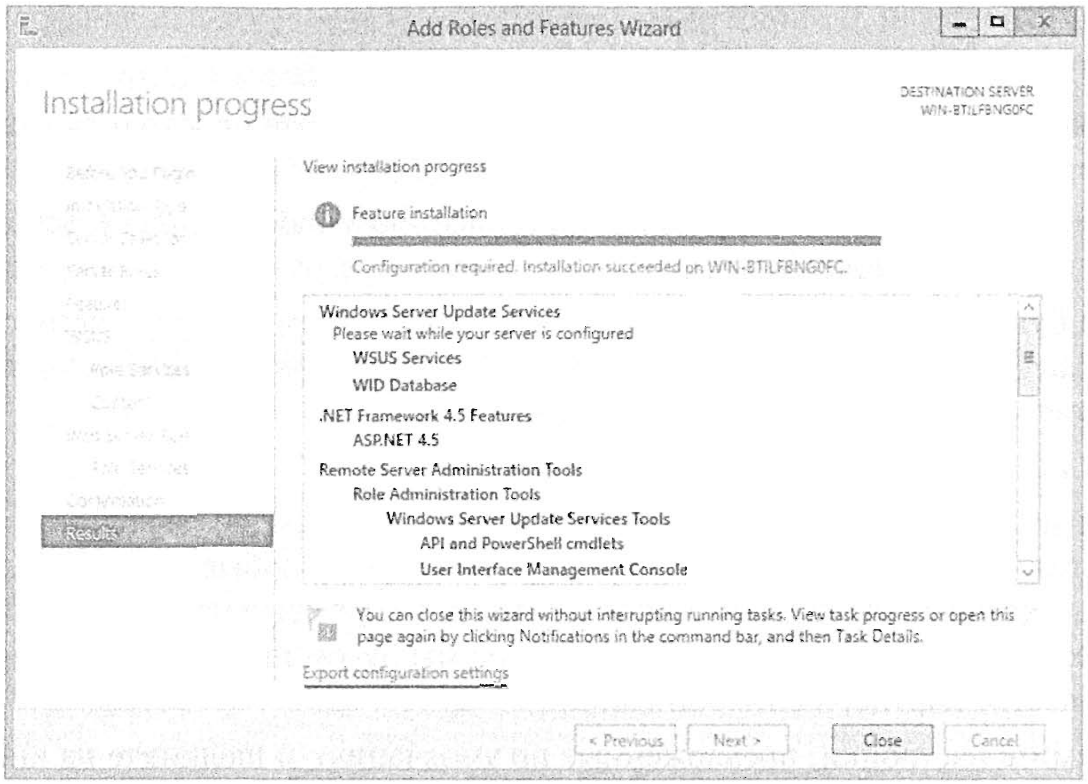


Рис. 31.8. Экспорт настроек конфигурации

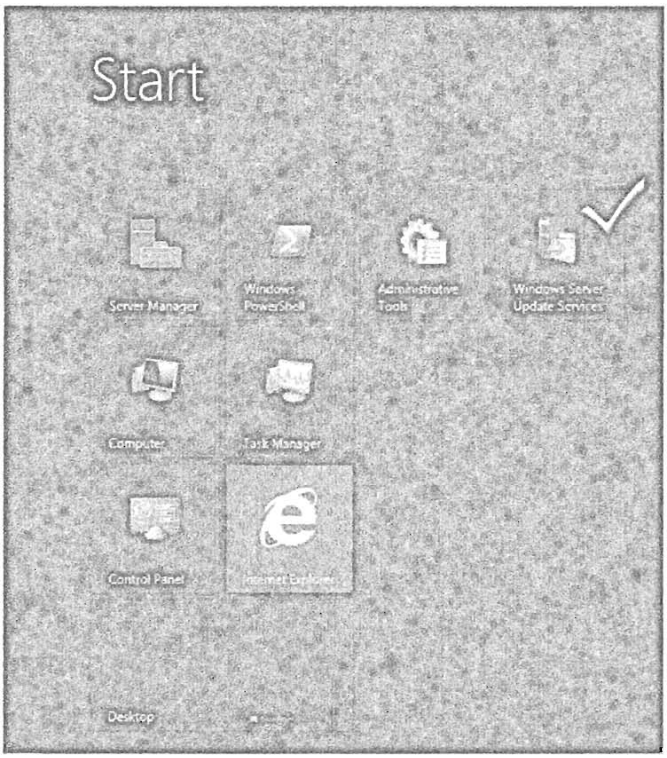


Рис. 31.9. Доступ к службе Windows Server Update Services на начальном экране

Первым экраном мастера является Before You Begin (Прежде чем начать); до начала процесса вы должны удостовериться в том, что удовлетворены перечисленные ниже условия.

- Сконфигурирован ли брандмауэр сервера на разрешение клиентам доступа к серверу?
- Может ли этот компьютер подключиться к вышестоящему серверу (такому как Microsoft Update)?

- Располагаете ли вы пользовательскими учетными данными для прокси-сервера, если в этом есть необходимость?

Убедившись в том, что эти условия выполнены, можете переходить к следующим действиям.

1. Приступите к начальному конфигурированию Windows Update Services, щелкнув на кнопке Next (Далее).

   Вам будет предложено присоединиться к программе по улучшению Microsoft Update (Microsoft Update Improvement Program); при желании можете оставить соответствующий флажок отмеченным.

2. Для продолжения щелкните на кнопке Next.

   Вам понадобится выбрать вышестоящий сервер, и вы задействуете на нем Microsoft Update, если это самый первый сервер. Любые дополнительные серверы, которые вы добавите впоследствии, могут ссылаться на этот сервер для синхронизации с ним. В нашем примере мы будем применять Microsoft Update в качестве партнера синхронизации.

3. Примите настройки, предложенные по умолчанию, и щелкните на кнопке Next.

4. Укажите прокси-сервер. Если в организации используется прокси-сервер, заполните все обязательные поля, как показано в примере на рис. 31.10, и щелкните на кнопке Next.

   Теперь вы подключитесь к вышестоящему серверу, чтобы можно было начать получение доступных обновлений продуктов, языков и других типов обновлений для вашего сервера обновлений.

5. Чтобы начать этот процесс, щелкните на кнопке Start Connecting (Начать подключение), представленной на рис. 31.11. Процесс подключения к вышестоящему серверу в первый раз может занять несколько минут.

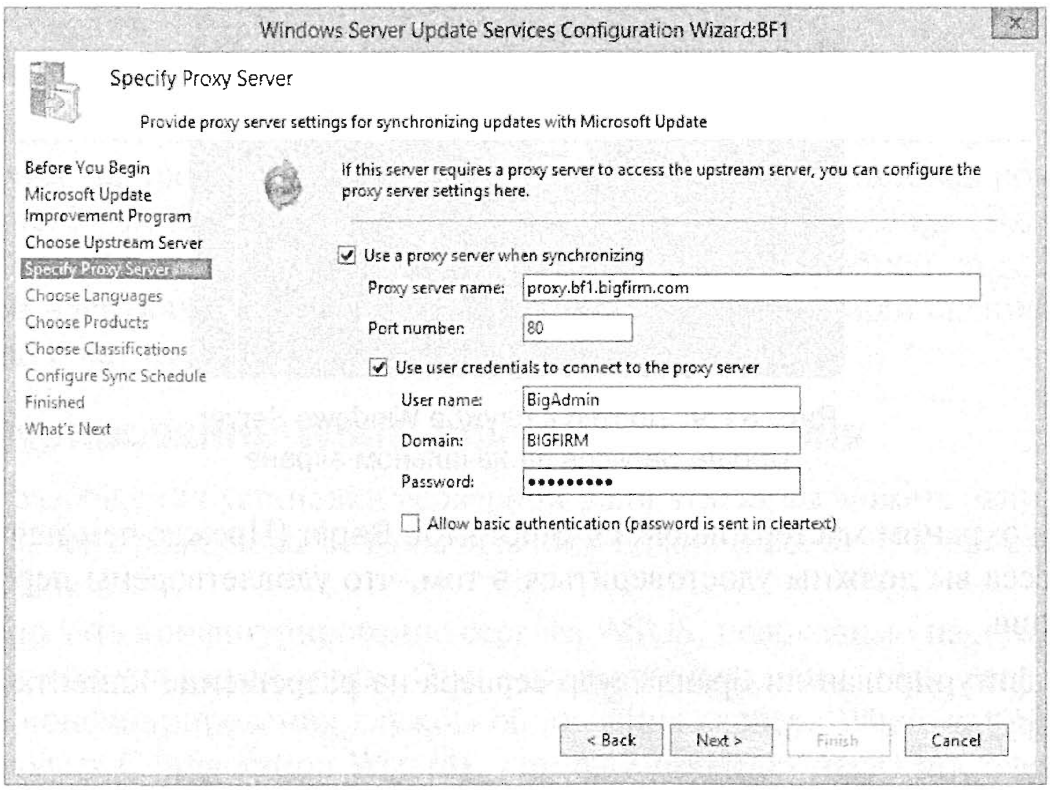


Рис. 31.10. Конфигурирование прокси-сервера

6. Когда этот процесс завершится, щелкните на кнопке Next.

   На экране Product Updates (Обновления продуктов) будет приведен список всех продуктов, доступных на вашем вышестоящем сервере. Вы можете выбрать целый продукт или конкретную его версию.

7. В этом примере мы отметили флажки только для Office 2013 и всех версий Silverlight (рис. 31.12). Выберите желаемые продукты и щелкните на кнопке Next.

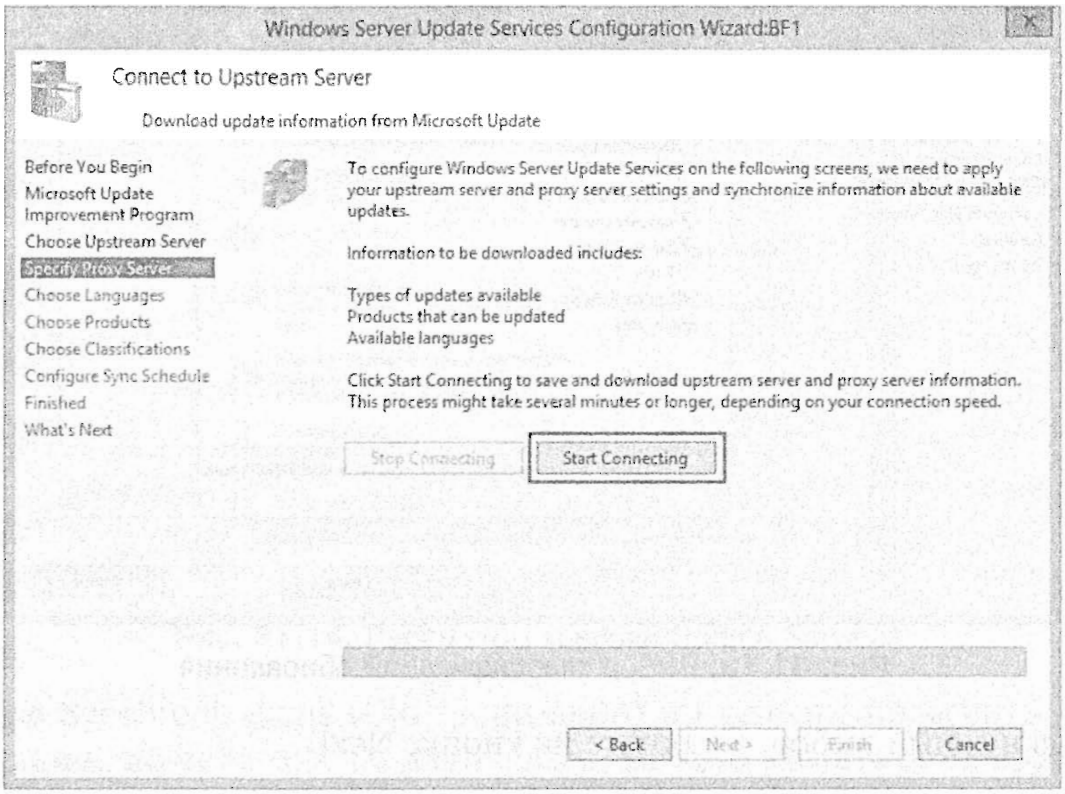


Рис. 31.11. Подключение к вышестоящему серверу

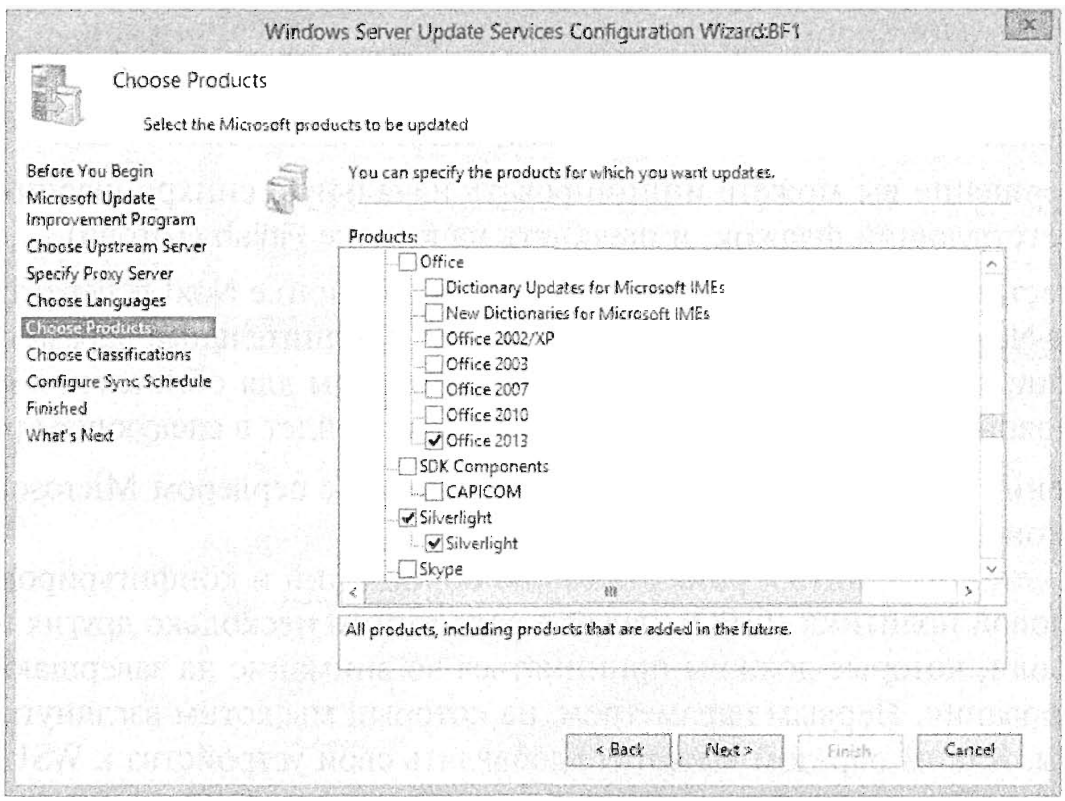


Рис. 31.12. Выбор продуктов для обновления

Далее понадобится выбрать классификации ваших обновлений для синхронизации. Перечень простирается от важных обновлений (Critical Updates) до обычных обновлений (Updates), как показано на рис. 31.13.

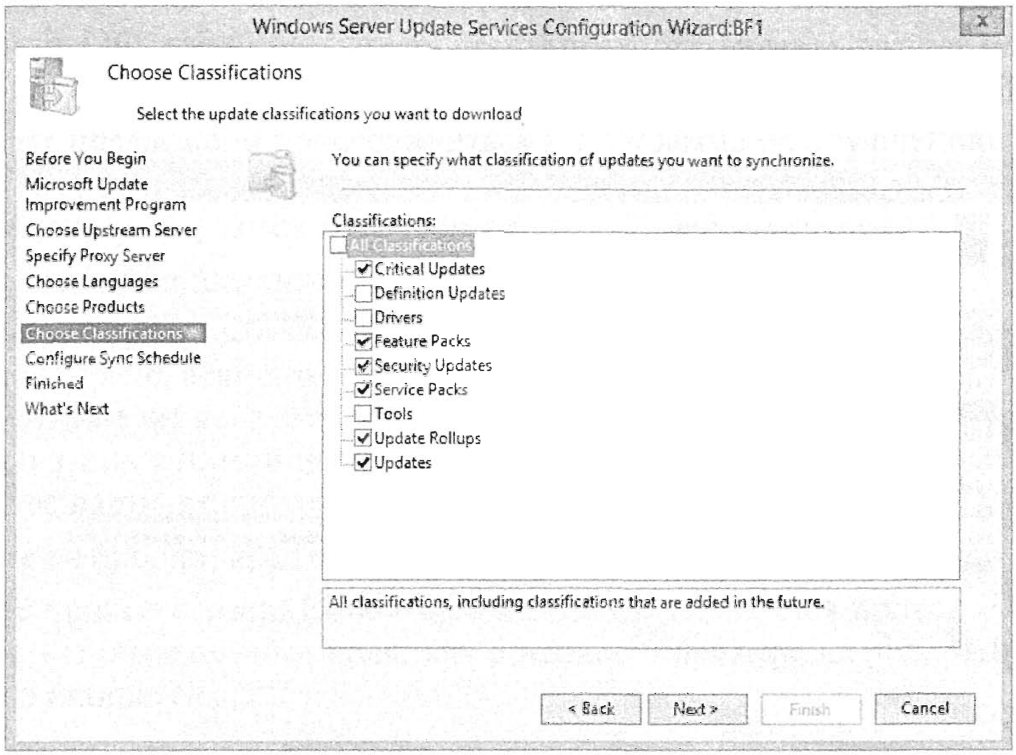


Рис. 31.13. Выбор классификаций обновления

8. Сделав нужный выбор, щелкните на кнопке Next.

   Следующий экран позволяет настроить расписание синхронизации. Здесь есть два варианта: первым является ручная синхронизация, которую можно выполнять посредством консоли службы обновления, а вторым — автоматическая синхронизация в определенный день и время. (За день можно также выполнять несколько синхронизаций.)

9. Установив расписание синхронизации, щелкните на кнопке Next.

10. В завершение вы можете инициировать начальную синхронизацию, отметив соответствующий флажок, и щелкнуть на кнопке Finish (Готово).

    В качестве альтернативы можете щелкнуть на кнопке Next и перейти на экран What's Next (Что дальше), где можно задать дополнительные параметры конфигурации, такие как SSL, и назначить компьютеры для обновления с помощью групповой политики (подробнее об этом речь пойдет в следующем разделе).

Обновления Windows начнут синхронизироваться с сервером Microsoft Update и заполнять консоль Update Services.

Прежде чем приступить к развертыванию обновлений и конфигурированию объектов групповой политики (GPO), давайте рассмотрим несколько других параметров в этой консоли, которые должны приниматься во внимание на завершающих шагах конфигурирования. Первым параметром, на который мы хотим взглянуть, являются компьютеры. Каким образом вы хотите добавлять свои устройства к WSUS? Открыв раздел Options (Параметры) консоли Update Services (рис. 31.14), вы можете выбрать объект Computers (Компьютеры); это позволит либо использовать консоль Update

Services для распределения компьютеров по группам, либо применять для назначения компьютеров групповую политику (или настройки реестра).

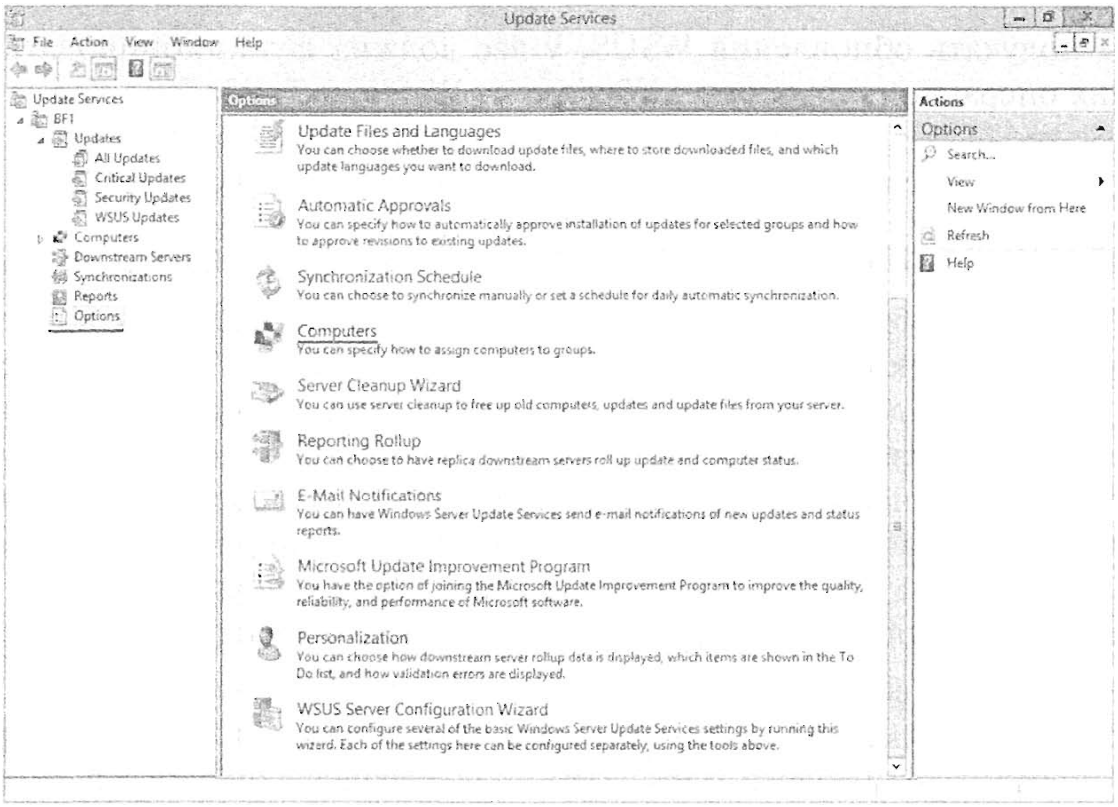


Рис. 31.14. Параметры консоли Update Services

В разделе Synchronizations (Синхронизации) вы должны проверить успешность синхронизации, но если она не начиналась, можете запустить ее вручную, щелкнув на элементе Synchronize Now (Синхронизировать сейчас) в панели Actions (Действия). Дополнительные детали приведены на рис. 31.15.

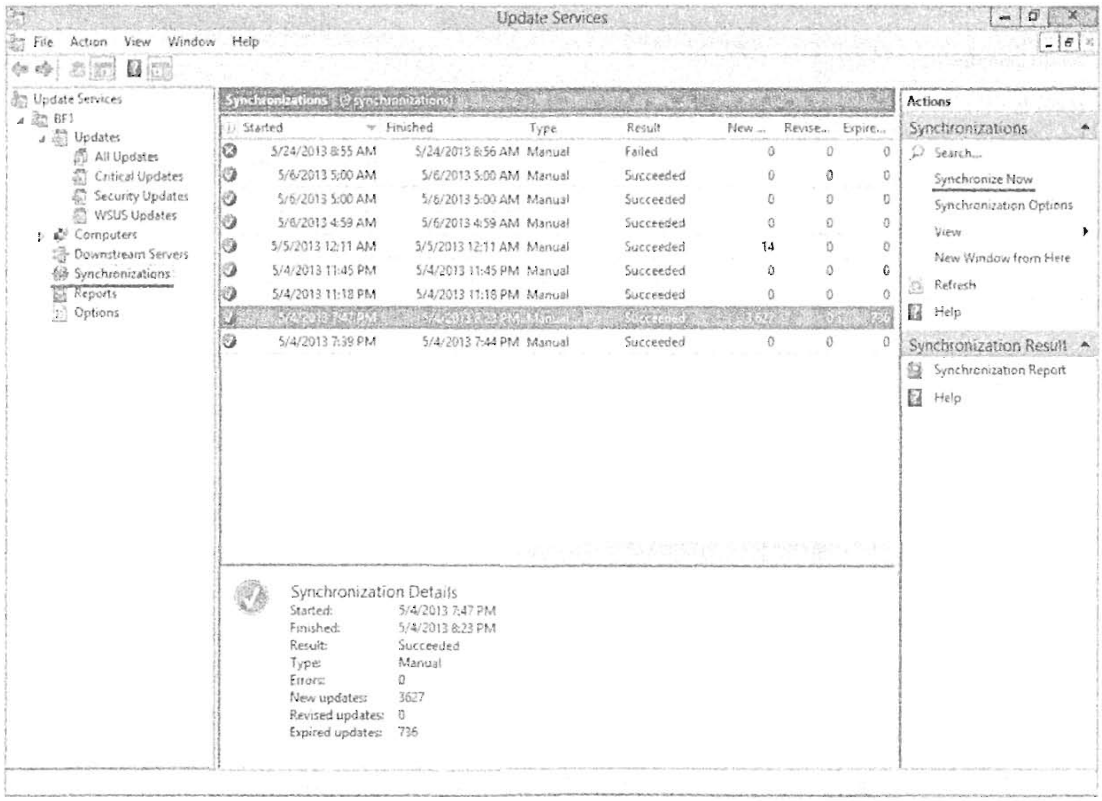


Рис. 31.15. Консоль Update Services, параметры синхронизации и задачи

Развертывание обновлений и миграция для WSUS

Чтобы получать обновления WSUS, у вас должна функционировать одна из следующих операционных систем: Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2, Windows Vista, Windows Server 2008 или Windows Server 2003. Также поддерживается Windows 8 RT, но с ограниченными возможностями.

Конфигурирование групповой политики для Windows Update

Использование объектов групповой политики (GPO) является наиболее распространенным и рекомендуемым подходом к управлению Windows Server Update Services. В этом разделе вы сконфигурируете параметры, необходимые для того, чтобы вытолкнуть обновления Windows с помощью объекта GPO. Для этого примера мы создаем совершенно новый объект GPO и применяем его к организационной единице `Workstations` (Рабочие станции) в Active Directory. Этот вновь созданный объект GPO называется `BigFirmUpdates` (рис. 31.16). Чтобы сконфигурировать настройки автоматического обновления Windows, выполните перечисленные ниже шаги.

1. Щелкните правой кнопкой мыши на объекте GPO и выберите в контекстном меню пункт Edit (Редактировать), чтобы открыть редактор управления групповыми политиками (Group Policy Management Editor), как показано на рис. 31.17.

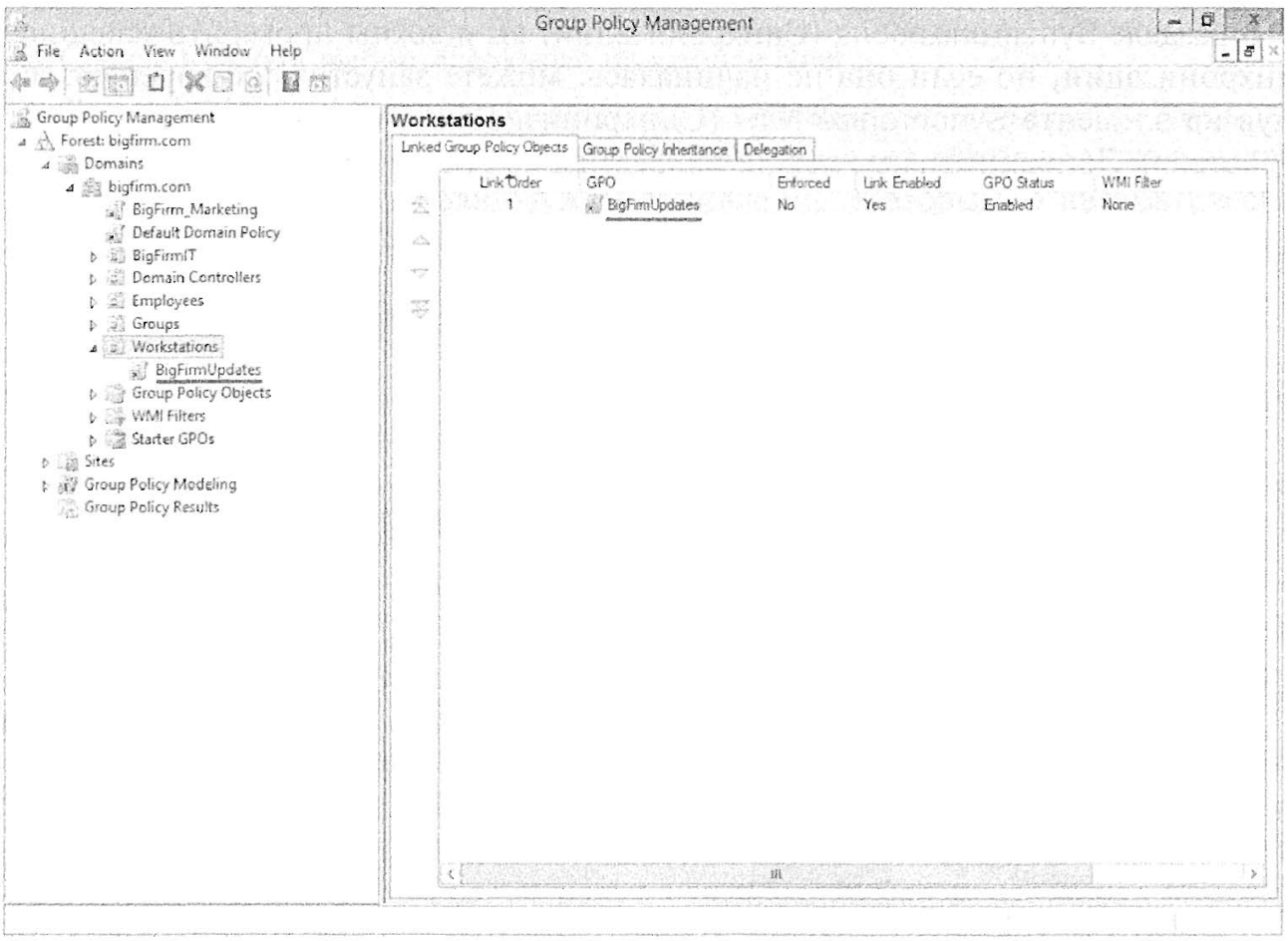


Рис. 31.16. Консоль Group Policy Management

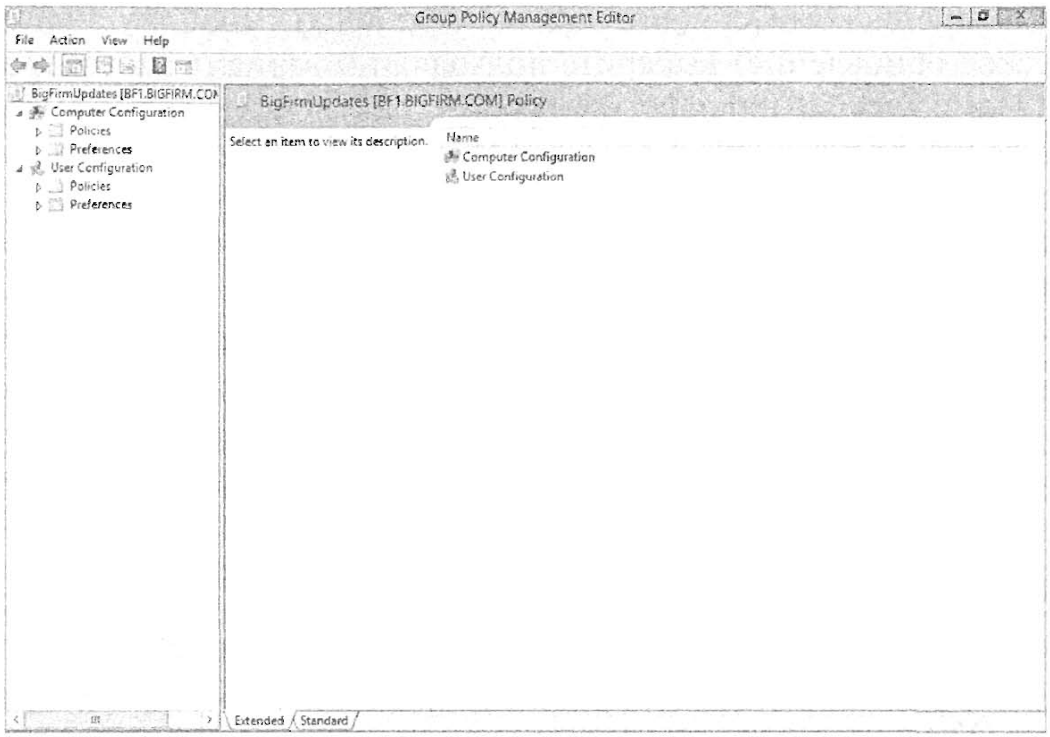


Рис. 31.17. Редактор Group Policy Management Editor

2. В редакторе Group Policy Management Editor перейдите в папку Computer Configuration \ Administrative Templates \ Windows Components \ Windows Update (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Обновление Windows).
3. Дважды щелкните на настройке Configure Automatic Updates (Конфигурировать автоматические обновления), показанной на рис. 31.18, и выберите для нее переключатель Enabled (Включить).

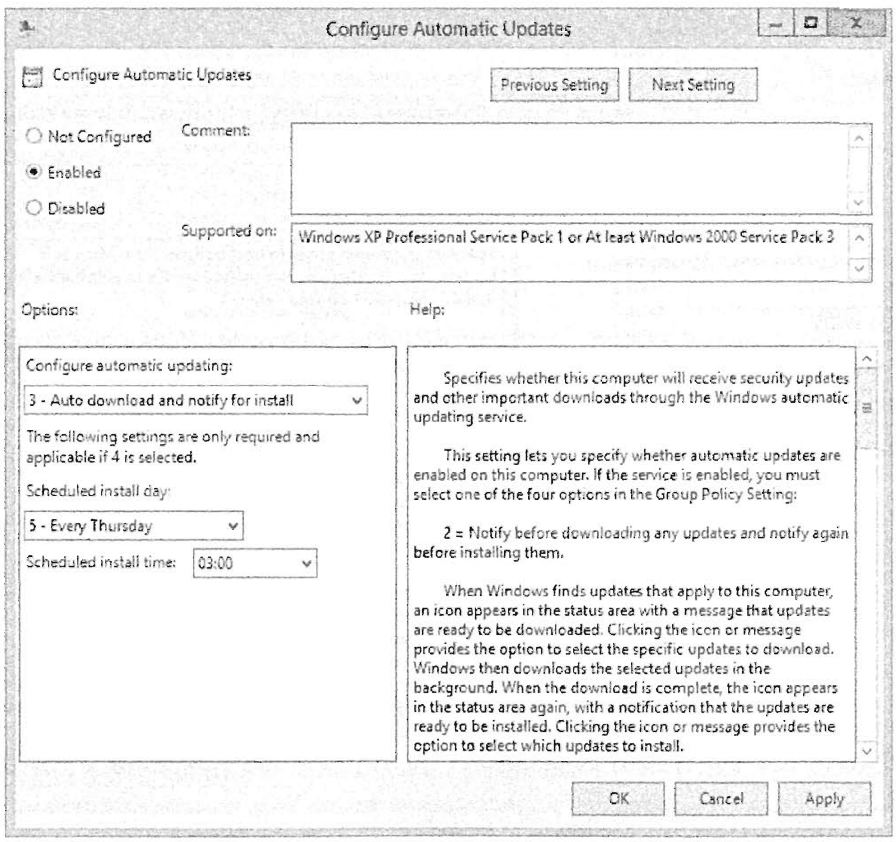


Рис. 31.18. Конфигурирование автоматических обновлений

а. В поле со списком Configure automatic updating (Конфигурировать автоматическое обновление) выберите подходящий вариант из числа доступных: Notify for download and notify for install (Уведомления о загрузке и установке), Auto download and notify for install (Автоматическая загрузка и уведомление об установке), Auto download and schedule the install (Автоматическая загрузка и установка по расписанию), Allow local admin to choose setting (Локальный администратор может менять параметр).

б. Если вы выбрали вариант Auto download and schedule the install, то должны указать день и время установки по расписанию.

4. Выберите настройку Specify intranet Microsoft update service location (Указать размещение службы обновлений Microsoft в интрасети). Здесь вам предстоит указать клиентам WSUS на сервер WSUS.

а. Выберите переключатель Enabled (Включить).

б. В полях Set the intranet update service for detecting updates (Укажите службу обновлений в интрасети для поиска обновлений) и Set the intranet statistics server (Укажите сервер статистики в интрасети) введите имя сервера WSUS, как показано на рис. 31.19.

в. Щелкните на кнопке OK.

Все это условия, которые обеспечат выталкивание обновлений на ваши клиентские устройства и использование только что созданной инфраструктуры WSUS.

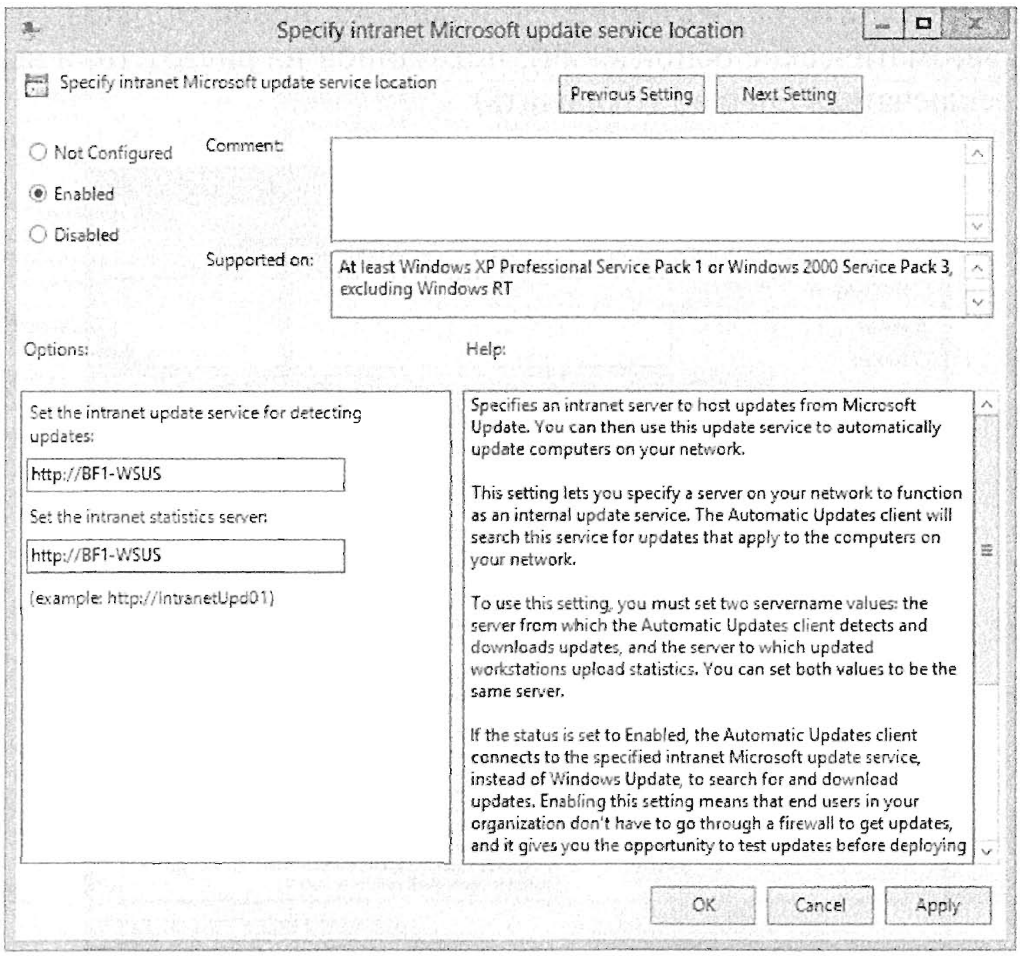


Рис. 31.19. Конфигурирование сервера WSUS

В разделе Windows Update редактора Group Policy Object Editor (рис. 31.20) легко заметить несколько других настроек, которые помогают существенно повысить эффективность администрирования и применения Windows Update. Они предоставляют возможность изменять график автоматических обновлений, включать выбор целей на клиентской стороне и отключать отображение на клиентах параметра установки обновлений, когда они доступны.

Конфигурирование клиентов для обновлений Windows

В этом разделе мы расскажем о конфигурировании и проверке того, что компьютер Windows 8 (по имени `WIN8CLIENT`), получает обновления из нашего сервера WSUS версии Windows Server 2012 R2. Настройка на клиентской стороне очень проста и требует только наличия самих обновлений или конфигурирования объекта GPO для получения этих обновлений. Если вы провели модернизацию до нового сервера Windows Server 2012 R2, то останется лишь модифицировать объекты GPO из предыдущего раздела.

Вообще говоря, внесение изменений в объекты GPO является единственной серьезной задачей для конфигурирования клиентов на получение обновлений из нового сервера WSUS. Ниже мы раскроем некоторые основы проверки и гарантии того, что клиент получает свои обновления и нацелен на правильный сервер.

Обновление групповой политики, которое происходит после указания клиентам нового сервера WSUS, может занять от 90 до 120 минут. Стандартное обновление объекта GPO занимает 90 минут.

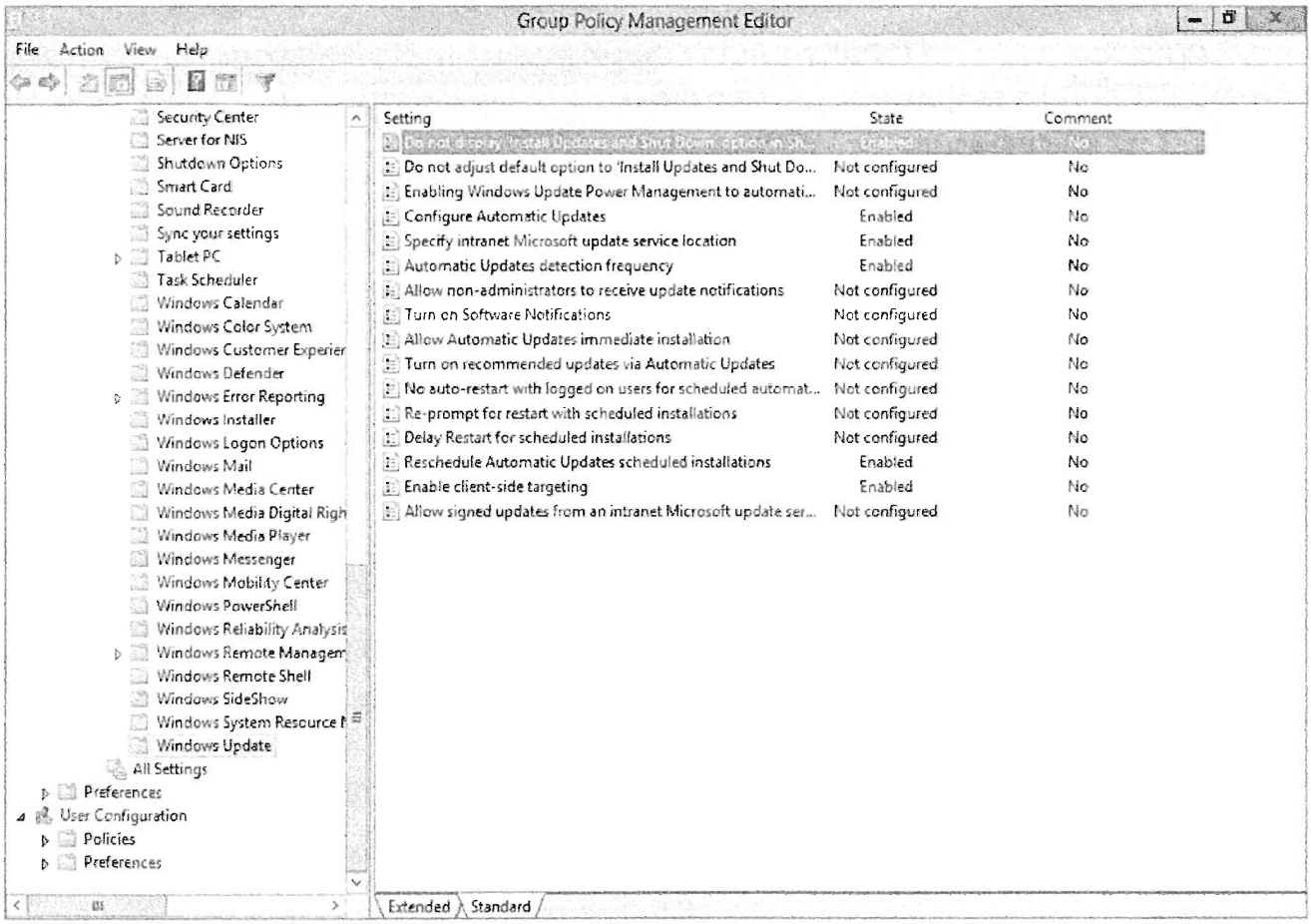


Рис. 31.20. Дополнительные настройки групповой политики Windows Update

Если вы хотите протестировать клиент, выполните следующие шаги.

1. На клиентском компьютере Windows откройте окно командной строки.
2. Введите команду `wuauclt.exe /detectnow /reportnow`.

   Это приведет к немедленному переходу клиента на сервер WSUS, проверке доступности его обновлений и выдаче отчета, по сути, подтверждающего их существование.

Чтобы проверить наличие ошибок или проблем с локальным клиентом, вы можете запустить средство Event Viewer локальной системы и перейти в нем к узлу \ Applications and Services Logs \ Microsoft \ Windows \ Windows Update Client \ (\ Журналы приложений и служб \ Microsoft \ Windows \ Клиент обновлений Windows \). Здесь вы увидите информационные сообщения, сообщения об ошибках и предупреждения клиентской системы, касающиеся обновлений (рис. 31.21).

Вдобавок вы всегда можете открыть инструмент Windows Update (Центр обновления Windows) из панели управления на клиенте и проверить, получает ли клиентский компьютер обновления. Средство Windows Update отобразит, когда выполнялись самые последние проверки наличия обновлений, укажет, какие обновления были установлены и как производится управление обновлениями (рис. 31.22).

В следующем разделе собираемся перейти от клиентских настроек к обзору процесса миграции вашей текущей реализации WSUS в Windows Server 2012 R2 и встроенной роли для Windows Server Update Services.

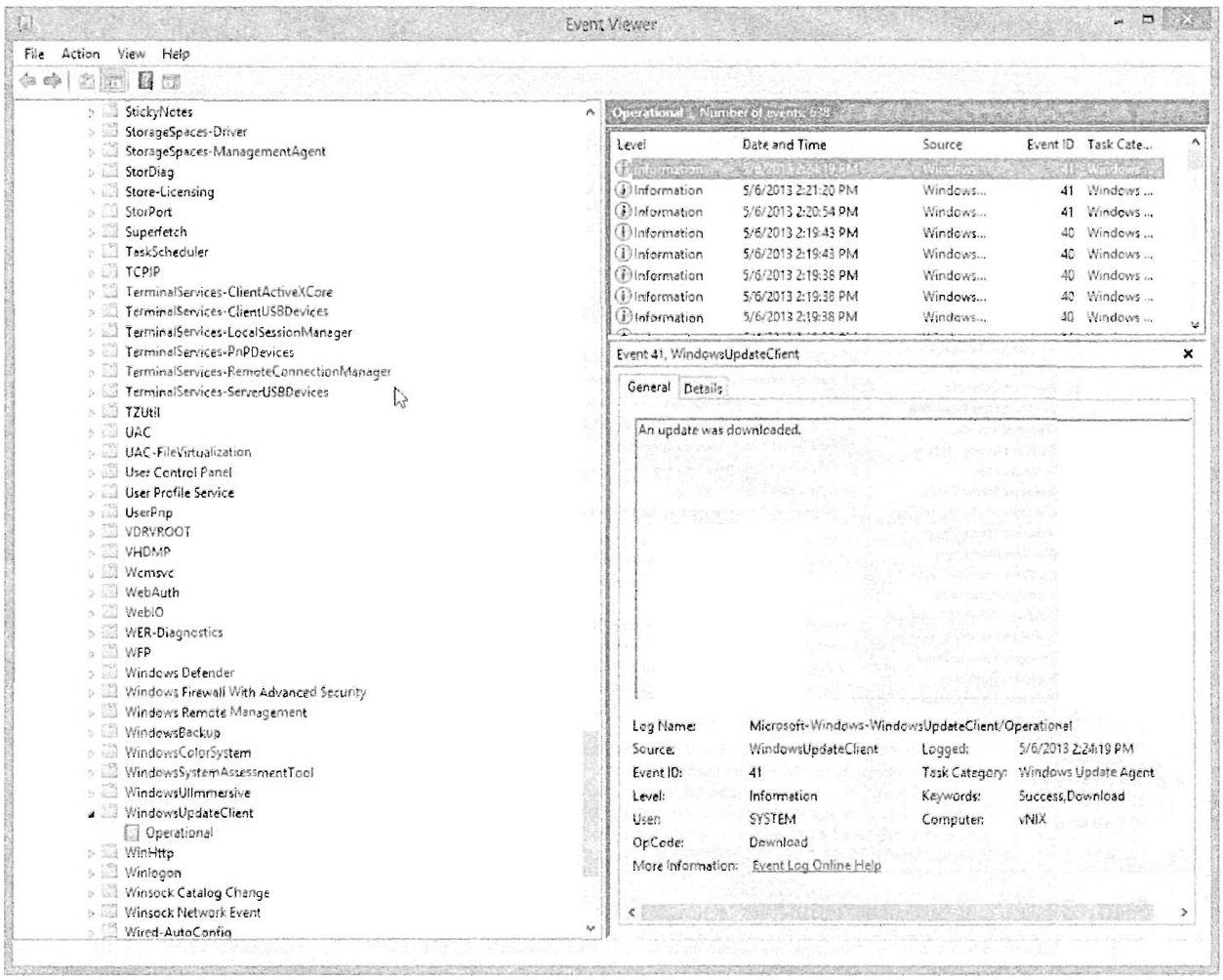


Рис. 31.21. Журнал Windows Applications and Services для обновлений клиентской стороны

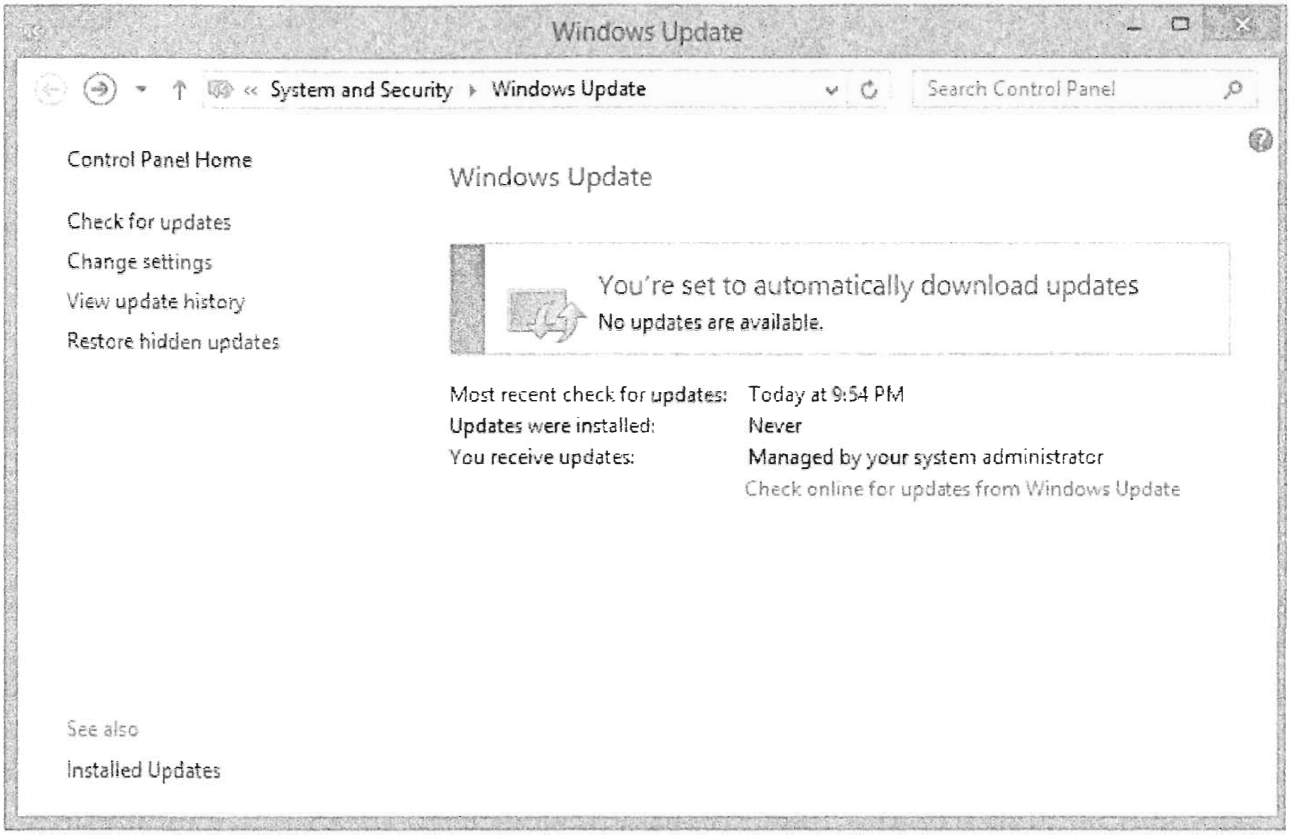


Рис. 31.22. Инструмент Windows Update в Windows 8

Миграция из WSUS 3.0 на Windows Server 2012 R2

Служба WSUS 3.0 упакована как автономный модуль установки, доступный в центре загрузки Microsoft (Microsoft Download Center), тогда как служба WSUS v6 (или WSUS 4.0, как иногда на нее ссылаются) представляет собой встроенную роль в Windows Server 2012 R2. В этом разделе вы узнаете, каким образом перейти от текущей установки WSUS 3.0 к новой встроенной платформе Windows Server 2012 R2.

В Microsoft предоставили четырехэтапный процесс для выполнения миграции из существующей реализации WSUS на новый целевой сервер, функционирующий под управлением Windows Server 2012 R2. Описание этого процесса можно найти в TechNet по ссылке:

```
https://technet.microsoft.com/ru-ru/library/hh852339.aspx
```

Прежде чем выполнять любой переход в производственной среде, понадобится принять во внимание множество разных факторов. Наличие достоверной исходной информации и перечня всех имеющихся серверов уступает по своей значимости лишь знанию вами всех возможных сценариев перехода.

Редакции Windows Server 2012 R2 Standard и Datacenter поддерживаются в качестве целевых серверов; возможен также переход с физической операционной системы на виртуальную. Модернизация будет поддерживать переход от SQL или Windows Internal Database (WID) как составную часть этого процесса миграции. Вдобавок можно переходить от WID к SQL Server.

Процесс перехода от службы WSUS 3.0 SP2 на инфраструктуру WSUS в Windows Server 2012 R2 требует определенных усилий, и очень важно иметь план резервного копирования/отката, если что-то не заработает, как ожидалось. При запуске процесса миграции, прежде всего, необходимо переместить все обновления WSUS

со старого исходного сервера на новый целевой сервер Windows Server 2012 R2. Использование инструментов вроде XCopy или Robocopy является жизнеспособным вариантом, но гораздо важнее понимать командлеты и управление с помощью PowerShell. Применение PowerShell для переноса таких объектов, как двоичные файлы, более подробно объясняется здесь:

```
https://technet.microsoft.com/ru-ru/library/hh852349.aspx
```

Создание резервной копии базы данных WSUS

Прежде чем приниматься за решение серьезной задачи миграции, вы должны позаботиться о создании резервной копии конфигурации, примененных исправлений и баз данных. Перед выполнением любых крупных задач модернизации или миграции, понадобится протестировать процесс резервного копирования и восстановления.

Частью рекомендуемой стратегии миграции является резервное копирование базы данных WSUS 3.0 SP2 и последующее восстановление этих данных на новом целевом сервере. После восстановления базы данных WSUS 3.0 SP2 на новом сервере WSUS v6 в Windows Server 2012 R2 процесс переноса должен завершиться успешно и вам не придется решать проблемы с утраченными отчетами, совместимостью данных или отменой примененных ранее исправлений.

Резервные копии информации и базы данных WSUS будут зависеть от типа выполняемого резервного копирования. Существует один процесс для резервного копирования и восстановления Windows Internal Database и другая последовательность действий, если в качестве сервера базы данных используется SQL Server. Создание резервной копии базы данных SQL Server описано по ссылке:

```
https://technet.microsoft.com/ru-ru/library/ms175477.aspx
```

Базу данных WID можно просмотреть в проводнике объектов (Object Explorer); после того как вы раскроете узлы баз данных, она будет обозначаться во всех экземплярах как SUSDB.

За дополнительной информацией о создании резервных копий WSUS и пошаговым руководством по этому процессу обращайтесь по ссылке:

```
http://tinyurl.com/c31widbackup
```

Дополнительные соображения

Помимо разработки плана резервного копирования для новой среды WSUS и подтверждения того, что все клиенты в организации получают обновления от нового сервера WSUS на основе Windows Server 2012 R2, вам необходимо разработать исчерпывающую документацию по всем настройкам, определенным для вашей организации. Уделите время включению сценариев PowerShell, приведению ссылок на любые компоненты и перечислению предварительных условий.

Как вы видели во многих приведенных ранее примерах, основными соображениями являются интенсивное использование PowerShell и количество новых процессов, выполняемых в его командной строке. Удостоверьтесь в том, что располагаете четким планом тестирования и списком задач в той или иной форме, что поможет создать контрольные точки на всем пути миграции.

Еще одно важное соображение касается построения собственного плана миграции и документации, чтобы иметь определенный процесс с указанием всех основных предварительных условий и диаграммы существующей инфраструктуры. Наличие такой документации становится исключительно полезным, если в будущем вам понадобится перейти на более крупный сервер или вы решили перейти с WID на SQL.

Операционное управление и инструменты

Клиентские компьютеры используют для получения обновлений WSUS клиент автоматического обновления Windows и могут быть сконфигурированы с применением объекта групповой политики. Объект GPO резко сокращает административные накладные расходы, поскольку один такой объект можно однократно развернуть на всех компьютерах в среде Active Directory. Конфигурирование автоматического обновления Windows посредством GPO производится с помощью редактора объекта групповой политики (Group Policy Object Editor).

PowerShell и WSUS

Управлять всеми аспектами WSUS можно посредством PowerShell, который предоставляет великолепный набор инструментов, ориентированных на повседневное управление обновлениями. Замечательным примером того, что можно делать с помощью этих инструментов, а также функций PowerShell в WSUS является возможность перехода от установки роли WSUS на сервере Windows Server 2012 R2, как показано здесь:

```
...\Install-WSUSServ.ps1 -ComputerName BF1 -StoreUpdatesLocally
-ContectDirectory "E:\Packages\WSUS" -InstallDatabasePatch "E:\"
-CreateDatabase -Verbose
```

к управлению клиентом и настройками реестра с помощью командлетов `Get-WSUSClientSettings` и `Set-ClientWSUSSettings`. Получить более подробную информацию о любом из этих командлетов можно по команде `Get-Help` или в Интернете. По ссылке `http://tinyurl.com/c31pswsus` доступна отличная статья по управлению WSUS и PowerShell.

Обновление с учетом кластеров

В Windows Server 2012 R2 предлагается новый компонент, который называется обновлением с учетом кластеров (Cluster-Aware Updating — CAU). Этот компонент позволяет обновлять кластеры без потери доступности в рамках окна обновлений. Когда компонент CAU запускается внутри окна обновлений, он переводит первый узел в режим обслуживания и передает рабочую нагрузку другим серверам в кластере, пока выполняется установка обновлений и при необходимости перезагрузка. После того как первый узел возвращается в рабочее состояние, CAU выводит данный сервер из режима обслуживания, возвращает ему исходные роли и переходит к следующему узлу. Например, при наличии кластера из двух узлов все роли или серверы из узла 1 будут перенесены в узел 2. После внесения исправлений в узел 1 и его перезагрузки он вернется к исполнению своих исходных ролей, а затем примет роли, размещенные в узле 2. Узел 2 будет переведен в режим обслуживания и перенесет свои серверы в узел 1.

Дополнительные инструменты управления исправлениями, предоставляемые Microsoft

Хотя в этом разделе внимание было сосредоточено на WSUS, доступно еще несколько инструментов производства Microsoft, которые могут содействовать в управлении обновлениями внутри организации.

- **Microsoft Update** (Центр обновления Microsoft). Компонент Microsoft Update теперь включен в панель управления и позволяет просматривать текущие настройки, выяснять, когда применяются обновления, и видеть действие, которое предпринимается при обнаружении обновлений.
- **Microsoft Update Catalog** (Каталог центра обновления Microsoft). Все файлы, доступные в Microsoft Update, имеются и в Microsoft Update Catalog, в том числе драйверы, исправления, безопасность и другие обновления продуктов Microsoft. Важной особенностью Microsoft Update Catalog является возможность добавления нескольких в корзину и загрузки их всех за раз. Каталог центра обновления Microsoft находится по ссылке `http://catalog.update.microsoft.com`.
- **Командлеты PowerShell для службы Windows Server Update Services.** В Windows Server 2012 R2 доступна обширная библиотека командлетов PowerShell, которые применяются для решения общих и повторяющихся задач внутри инфраструктуры WSUS. С полным списком этих командлетов PowerShell можно ознакомиться в TechNet (`http://tinyurl.com/c31pscmdlets`). Возможность управления компонентами и классификациями исправлений из PowerShell позволяет дополнительно автоматизировать процесс управления многосерверными инфраструктурами и оказывать более тонкое влияние на процесс обновления (например, запрещать применение определенного исправления к конкретному развертыванию).
- **Инструменты для поддержки безопасности Microsoft.** В клиентах Windows Server 2012 R2 и Windows 8 вместо MBSA (Microsoft Baseline Security Analyzer — анализатор базовых уровней безопасности Microsoft) используются инструменты оценки безопасности (Security Assessment Tools), которые обеспечивают поддержку Windows 7, Windows Server 2008, Windows XP, Windows Vista и Windows Server 2008 R2.

  Доступно несколько инструментов: Microsoft Security Assessment Tool 4.0, Microsoft Baseline Security Analyzer 2.2 и Microsoft Security Compliance Manager. Все эти инструменты и дополнительные сведения о них можно найти на вебсайте Microsoft.
- **Блог центра реагирования на проблемы безопасности Microsoft.** Центр реагирования на проблемы безопасности Microsoft (Microsoft Security Response Center — MSRC) предназначен для выдачи обновлений безопасности для продуктов Microsoft. Этот сайт также предоставляет сводки о проблемах, которые еще не решены, но изучаются. Блог MSRC можно использовать для получения текущей информации. Он доступен по ссылке `http://blogs.technet.com/b/msrc/`.

  Отслеживание этой группы в Твиттере (`@MSFTSecResponse`) позволит быть в курсе актуальных обновлений.

Инструменты Cluster-Aware Updating можно устанавливать на компьютерах Windows Server 2012 R2 и Windows 8. После установки инструментов вы конфигурируете нужный сценарий CAU; примеры таких сценариев можно найти по ссылке `http://tinyurl.com/c31cluster`.

В руководствах по сценариям Cluster-Aware Updating вы заметите, что компонент CAU работает в двух основных режимах.

- **Самообновление.** Эта конфигурация выполняется на узле кластера, который вы хотите обновить. Вам понадобится только настроить расписание обновления и позволить CAU обновить кластер.
- **Дистанционное обновление.** Вы запускаете CAU из автономного сервера или клиента, не входящего в кластер, например, из настольного компьютера Windows 8 с установленными инструментами CAU. Затем вы подключаетесь к нужному кластеру и обновляете его согласно расписанию.

В ходе установки и управления компонентом Cluster-Aware Updating вы обнаружите набор командлетов PowerShell, которые помогут выяснить, готов ли сервер, запустить необходимый процесс и проверить общее состояние кластеров. Выбрав подходящий метод применения компонента CAU, а также установив расписание, вы получите в свое распоряжение расширенные возможности Windows Server 2012 R2 и новую роль WSUS v6.

Диспетчер конфигурации системного центра

Диспетчер конфигурации системного центра (System Center Configuration Manager — SCCM) — это инструмент централизованного управления, построенный на основе комплекта программного обеспечения System Center (Системный центр) от Microsoft. В число основных областей внимания SCCM входит управление клиентами (серверами и рабочими станциями), применение исправлений, защита конечных точек, развертывание приложений и автоматизированная доставка операционных систем.

Анализ самой последней версии этого продукта, SCCM 2012 SP1, можно найти по ссылке:

```
https://www.microsoft.com/ru-ru/server-cloud/products
  /system-center-2012-r2-configuration-manager/default.aspx
```

Диспетчер конфигурации системного центра предлагает более широкие возможности генерирования отчетов и поддержания совместимости по сравнению с WSUS. Для любой средней и крупной организации обычно рекомендуется использовать SCCM в качестве основного инструмента применения исправлений. Ниже перечислены некоторые дополнительные преимущества внедрения SCCM.

- Возможность централизованного отката исправления, которое уже было развернуто.
- Оценка совместимости, позволяющая выполнять поиск программного обеспечения или обновлений, которые необходимы для обеспечения совместимости.
- Один унифицированный клиент: вы можете использовать клиент SCCM для установки обновлений, управления или регулировки обновлений и существенного упрощения единичных развертываний.
- Усовершенствованные отчеты и возможность определять подписки, которые помогают оценивать совместимость.

- Возможность определения окон обслуживания для выталкивания исправлений; использование групповой политики обеспечивает только строгий подход в стиле "все или ничего" к применению исправлений в системах. С помощью SCCM и окон обслуживания вы можете вносить исправления в подгруппы компьютеров только на протяжении определенных часов.
- Издатель обновлений системного центра (System Center Update Publisher) позволяет собирать загрузочные файлы исправлений от Adobe, Java и производителей оборудования. Эти исправления легко интегрируются в развертывание и расписание.
- Автономное обслуживание позволяет обновлять файл WIM (Windows Image File Format — файловый формат для образа Windows) после его сохранения, избавляя от необходимости развертывать и обновлять образ вручную. Это гарантирует, что образы развертывания ОС всегда развертываются с самыми последними исправлениями.

Резюме

Используйте Windows Automatic Updates для проверки наличия новых обновлений на компьютере, работающем под управлением Windows 8. Компонент Windows Automatic Updates входит в состав панели управления и применяется для проверки наличия на сайте Microsoft Update любых обновлений для вашего компьютера.

Контрольный вопрос. Воспользуйтесь Windows Automatic Updates на компьютере Windows 8, чтобы проверить наличие для него доступных обновлений.

Применяйте Windows Update Standalone Installer для молчаливой установки обновлений безопасности. Инструмент Windows Update Standalone Installer применяется для установки обновлений безопасности во всех операционных системах Windows, начиная с Windows Vista и Windows Server 2008.

Контрольный вопрос. Установите в молчаливом режиме обновление безопасности и отложите требуемую перезагрузку с использованием Windows Update Standalone Installer.

Идентифицируйте четыре фазы управления исправлениями. Согласно рекомендациям Microsoft, существуют четыре фазы при планировании стратегии управления исправлениями.

Контрольный вопрос. Какое из перечисленных ниже действий не имеет отношения к четырем фазам управления исправлениями?

1. Идентификация
2. Поиск и устранение проблем
3. Оценка и планирование
4. Оценка
5. Развертывание

Глава 32

Резервное копирование и обслуживание Windows Server 2012 R2 и Active Directory

Резервное копирование и восстановление представляют собой задачи, хорошо знакомые большинству администраторов серверов. Защита данных и приложений достаточно важна, но восстановление Active Directory может оказаться даже более жизненно необходимой мерой, направленной на поддержание непрерывного функционирования среды.

В этой главе мы рассмотрим различные типы резервного копирования и восстановления, доступные в Windows Server 2012 R2, и покажем, как их применять к Active Directory. Вы также узнаете о корзине Active Directory (Active Directory Recycle Bin), диспетчере защиты данных системного центра 2012 R2 (Microsoft System Center 2012 R2 Data Protection Manager) и новом инструменте онлайнового резервного копирования для Windows Server 2012 R2, который поддерживает создание резервной копии с помощью продукта Microsoft Windows Azure.

Вдобавок мы опишем ряд задач обслуживания Active Directory, таких как возможность останова и перезапуска Active Directory без необходимости в перезапуске серверного компьютера. Возможность останова Active Directory позволяет проводить автономное обслуживание базы данных Active Directory, в том числе дефрагментацию и проверку целостности. В этой главе вы изучите следующие темы:

- использование Windows Server Backup для резервного копирования и восстановления компьютера Windows Server 2012 R2;
- дефрагментация AD DS в автономном режиме;
- установка Active Directory Recycle Bin;
- создание и восстановление резервной копии состояния системы для Active Directory.

Введение в Windows Server Backup

Резервное копирование уже давно является частью Windows Server, а в Windows Server 2012 R2 задачи резервного копирования выполняются с помощью Windows Server Backup. Хотя инструмент Windows Server Backup может не предоставлять абсолютно все функции, которые желательно иметь в производственной среде, он довольно хорошо справляется с резервным копированием и восстановлением сервера Windows Server 2012 R2 и может оказаться надежным решением для сред малых и средних размеров. Инструмент Windows Server Backup можно использовать для резервного копирования удаленных компьютеров, но лучше всего он подходит для резервного копирования локального сервера.

Инструмент Windows Server Backup, входящий в состав Windows Server 2012 R2, содержит несколько важных усовершенствований по сравнению с предыдущей версией, включенной в Windows Server 2008 R2. Ниже приведен перечень этих усовершенствований.

- Теперь поддерживается резервное копирование и восстановление отдельных виртуальных машин из хост-сервера Hyper-V.
- Улучшено управление версиями и хранение резервных копий, к тому же можно указывать политики удаления, что помогает контролировать используемое дисковое пространство.
- Устранено ограничение, связанное с возможностью резервного копирования только томов, объем которых не превышает 2 Тбайт, а размер сектора составляет 512 байтов. Теперь можно создавать резервные копии больших томов или устройств, имеющих новый формат виртуального жесткого диска объемом до 64 Тбайт (`.VHDX`); кроме того, поддерживается размер сектора в 4 Кбайт.
- В настоящее время поддерживаются общие тома кластера (Cluster Shared Volume — CSV), хотя и с несколькими ограничениями: скажем, нельзя выполнять резервное копирование виртуальных машин, размещенных на томах CSV, и восстанавливать полный том CSV.
- Более точная конфигурация выдачи отчетов о компонентах состояния системы (System State) позволяет системному средству записи (System Writer) сообщать о том, что файлы служб Win32 теперь являются частью только клиентской операционной системы Windows 8, а не Windows Server 2012 R2. Это означает более эффективное резервное копирование состояния системы.

Резервное копирование на ленту с помощью Windows Server Backup

Инструмент Windows Server Backup не поддерживает резервное копирование на ленту (начиная с версии Windows Server 2008 R2). Если организации необходим более традиционный метод резервного копирования на ленту, понадобится развернуть продукт, подобный диспетчеру защиты данных системного центра 2012 R2 (System Center 2012 R2 Data Protection Manager), предлагаемый Microsoft.

Установка Windows Server Backup

Инструмент Windows Server Backup устанавливается как компонент операционной системы Windows Server 2012 R2 и состоит из трех отдельных частей:

- оснастка консоли управления Microsoft (Microsoft Management Console — MMC);
- инструменты командной строки (`Wbadmin.exe`);
- командлеты Windows PowerShell.

По умолчанию Windows Server Backup не устанавливается, поэтому придется выполнить следующие шаги.

1. Войдите в систему сервера Windows Server 2012 R2, присоединенного к домену, с помощью учетной записи с разрешениями администратора домена. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты).
2. На экране Before You Begin (Прежде чем начать) щелкните на кнопке Next (Далее).
3. Удостоверьтесь, что на экране Select Installation Type (Выбор типа установки) выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов), и щелкните на кнопке Next.
4. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов), убедитесь, что ваш сервер выделен в разделе Server Pool (Пул серверов), и щелкните на кнопке Next.
5. На экране Select Server Roles (Выбор серверных ролей) просто щелкните на кнопке Next, чтобы продолжить.
6. На экране Select Features (Выбор компонентов) выполите прокрутку вниз до тех пор, пока не найдете в списке Roles (Роли) элемент Windows Server Backup (Резервное копирование сервера Windows), отметьте флажок рядом с ним и щелкните на кнопке Next.
7. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) просмотрите выбранные варианты, щелкните на кнопке Install (Установить), чтобы начать процесс установки, и затем на кнопке Close (Закрыть), когда мастер завершит работу.

Резервное копирование и восстановление полного сервера

Самая большая разница между сохранением резервных копий в общей сетевой папке и применением для этой цели локального диска связана с тем, что на локальном диске инструмент Windows Server Backup будет хранить множество версий резервных копий, а в удаленном расположении — только самую последнюю версию резервной копии. Наличие нескольких резервных копий для конкретного серверного компьютера означает возможность восстановления с отказом от изменений, внесенных на определенные даты, а также возможность восстановления после полной утери данных. Это особенно полезно при восстановлении файлов, которые могли измениться или были удалены до создания самой последней резервной копии.

При выполнении резервного копирования на диски подумайте об использовании съемного диска какого-то типа, скажем, внешнего жесткого диска USB или eSATA. Еще более эффективным вариантом является применение нескольких съемных дисков, которые можно было по очереди менять с внешним хранилищем, чтобы обеспечить более высокий уровень защиты на случай аварийных ситуаций. Инструмент Windows Server Backup может идентифицировать диски, предназначенные для резервного копирования, и автоматически использовать любой имеющийся диск, удаляя из него самую старую резервную копию с целью освобождения места под текущую резервную копию.

Создание полной резервной копии сервера является одним из наиболее простых для выполнения типов резервного копирования и вместе с тем самым эффективным типом с точки зрения последующего восстановления. Создание полной резервной копии сервера включает в себя следующие части:

- все локальные тома (виртуальные диски, расположенные на локальных томах, не будут копироваться, если они находятся в онлайновом режиме);
- критически важные тома;
- состояние системы.

При наличии полной резервной копии сервера вы можете восстанавливать индивидуальные файлы и папки, а также целые тома в случае отказа диска. Вы можете также выполнить восстановление с нуля, при котором полностью заменяется серверный компьютер (или, по меньшей мере, жесткие диски, содержащие операционную систему и состояние системы) и отсутствует установленная операционная система. Недостатками полной резервной копии сервера являются ее размер и время, требуемое для проведения резервного копирования.

Создание полной резервной копии сервера

В описанных ниже действиях предполагается, что вы будете создавать полную резервную копию сервера на локальном диске и определять расписание для автоматического повторения этой операции резервного копирования.

1. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Windows Server Backup (Сервис⇨ Резервное копирование сервера Windows), чтобы открыть эту оснастку MMC.
2. В окне оснастки MMC щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) в левой панели дерева и выберите в контекстном меню пункт Backup Schedule (Расписание резервного копирования), чтобы открыть мастер расписания резервного копирования (Backup Schedule Wizard).
3. На экране Getting Started (Начало работы) щелкните на кнопке Next (Далее).
4. Для указания типа резервного копирования выберите переключатель Full server (recommended) (Полный сервер (рекомендуется)), как показано на рис. 32.1; затем щелкните на кнопке Next.
5. Установите время суток, чтобы начать резервное копирование (рис. 32.2).

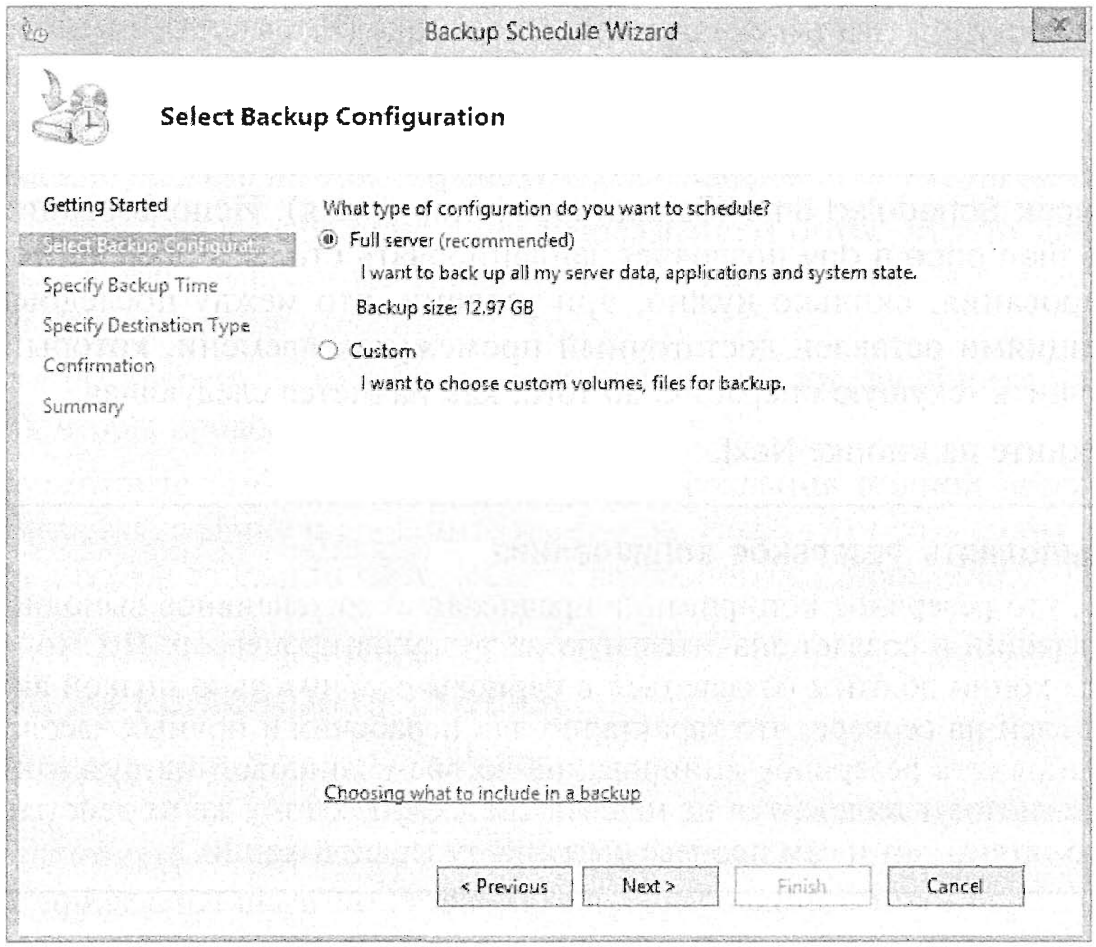


Рис. 32.1. Выбор типа резервного копирования

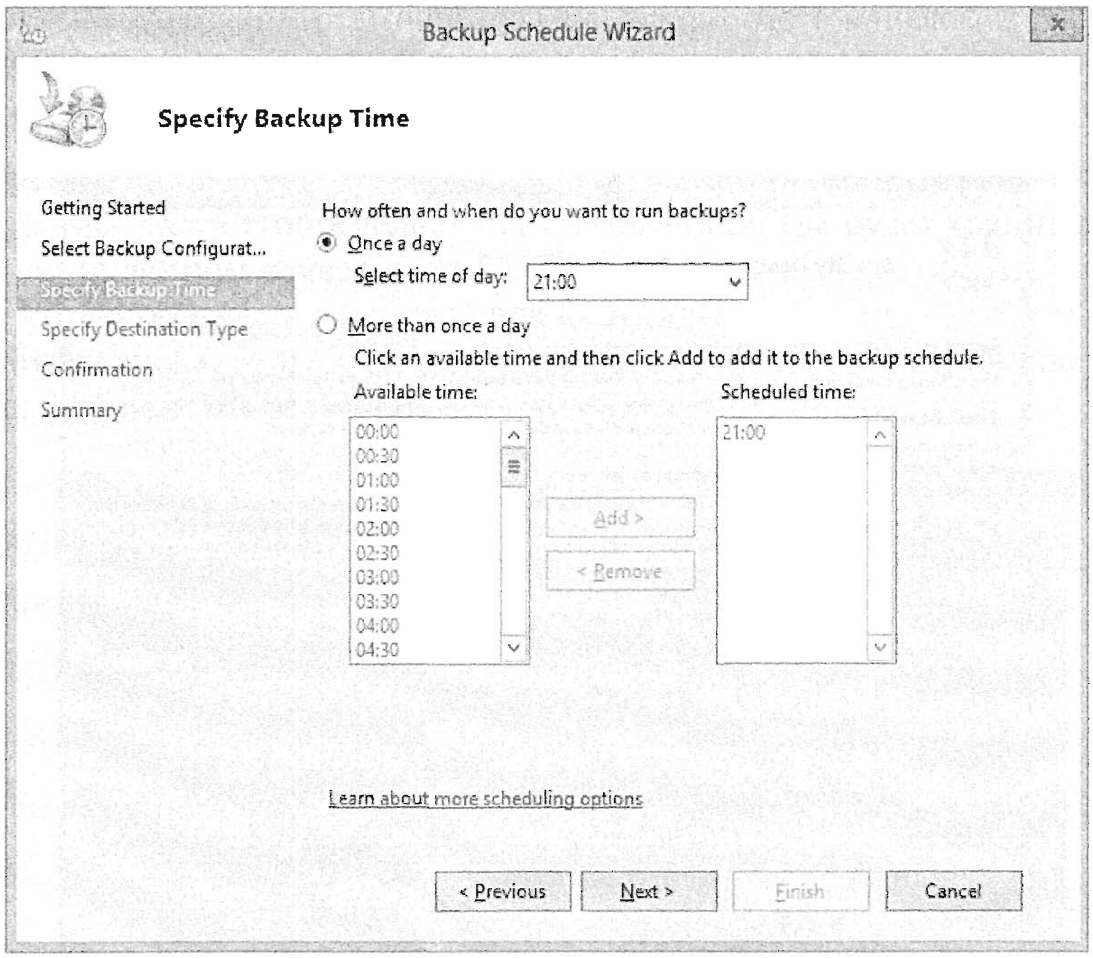


Рис. 32.2. Выбор времени суток

Здесь доступны два переключателя: Once a day (Раз в сутки); в этом случае вы должны выбрать время суток, когда начнется резервное копирование; и More than once a day (Более одного раза в сутки); в этом случае вы должны выбрать подходящее время и щелкнуть на кнопке Add (Добавить), чтобы поместить его в список Scheduled time (Запланированное время). Использование варианта More than once a day позволяет запланировать столько операций резервного копирования, сколько нужно, при условии, что между последовательными операциями оставлен достаточный промежуток времени, который позволит завершить текущую операцию до того, как начнется следующая.

6. Щелкните на кнопке Next.

Когда выполнять резервное копирование

Помните, что резервное копирование предполагает интенсивное выполнение дисковых операций и создает значительную нагрузку на процессор. По этой причине резервные копии должны создаваться в периоды сравнительно низкой активности пользователей на сервере, что характерно для нерабочих и ночных часов. Если вы будете выполнять резервное копирование во время пиковой нагрузки на сервер, пользователи могут жаловаться на медленный доступ, к тому же их действия на сервере часто затягивают и сам процесс создания резервной копии.

---

7. Выберите переключатель Back up to a hard disk that is dedicated for backups (recommended) (Создать резервную копию на жестком диске, который выделен для резервных копий (рекомендуется)), как показано на рис. 32.3.

   Для использования этого варианта к серверному компьютеру должен быть подключен, по меньшей мере, один диск, который не имеет тома. Диск должен быть неформатированным, т.е. не содержать разделов или файловую систему.

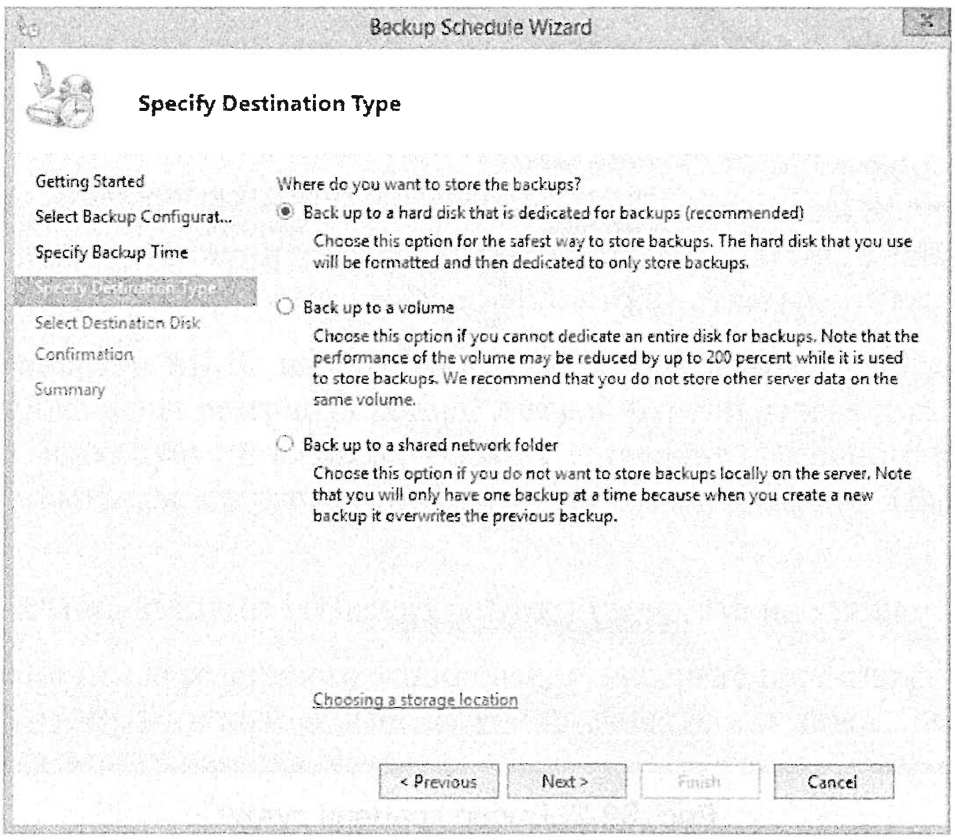


Рис. 32.3. Выбор типа диска

8. Щелкните на кнопке Next.
9. Выберите диск для применения в качестве тома для резервных копий. Чтобы использовать систему чередующейся смены дисков, хранящихся за пределами организации, укажите на этом экране несколько дисков. Щелкните на кнопке Next.

   Откроется диалоговое окно с предупреждением о том, что по завершении работы мастера выбранные диски будут сформатированы, а любые существующие на них данные утеряны.
10. Если вы уверены, что указали подходящие диски, щелкните на кнопке Yes (Да), чтобы продолжить.
11. Просмотрите выбранные настройки для создания полной резервной копии сервера по графику и щелкните на кнопке Finish (Готово), чтобы сформатировать диски и запланировать процесс резервного копирования.

Создание полной резервной копии сервера из командной строки

Компонент командной строки Windows Server Backup, `Wbadmin.exe`, можно использовать в случаях, когда вы хотите снабдить резервное копирование сценариями или предпочитаете обслуживать серверный компьютер с помощью командной строки. Ниже приведены шаги по созданию запланированной полной резервной копии сервера с применением командной строки.

1. Откройте окно командной строки с повышенными разрешениями. Для этого необходимо быть членом группы `Administrators` или `Backup Operators`.
2. Введите следующую команду:

```
Wbadmin.exe enable backup -vssFull -schedule:02:00
  -addtarget:E: -include:C:\
```

   Переключатель `-vssFull` отражает создание полной резервной копии сервера, а `-addtarget` определяет путь назначения, где будет храниться резервная копия (в данном случае диск E). Переключатель `-include:C:\` указывает на то, что должен быть включен диск C. Каждый раз когда `-include` используется буква диска, ее необходимо завершать символом обратной косой черты. На рис. 32.4 показан результат выполнения этой команды.

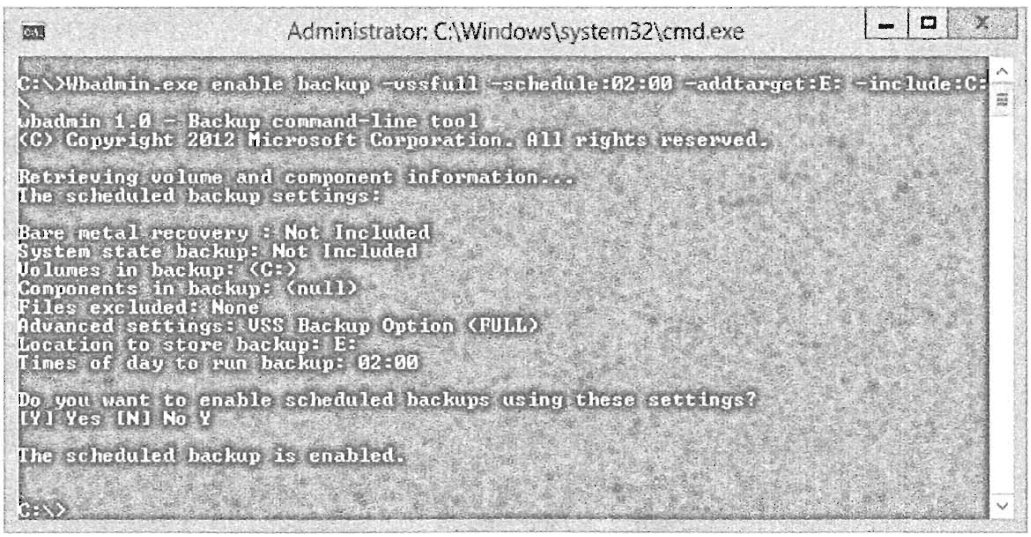


Рис. 32.4. Создание новой запланированной резервной копии

3. Введите следующую команду, чтобы запустить только что созданную задачу резервного копирования:

```
Wbadmin.exe start backup
```

Создание резервной копии с помощью PowerShell

В главе 27 вы узнали, как создавать виртуальные машины на хосте Windows Server 2012 R2. Здесь мы собираемся обсудить резервное копирование виртуальной машины Hyper-V с помощью PowerShell как альтернативы `wbadmin.exe`. Вы можете воспользоваться командлетами PowerShell для Windows Server Backup, чтобы создать свою политику резервного копирования (`New-WBPolicy`), указать место хранения резервной копии (`New-WBBackupTarget`), добавить виртуальную машину (`Add-WBVirtualMachine`) и сконфигурировать расписание, в соответствии с которым будет запускаться резервное копирование (`Set-WBSchedule`).

1. Откройте окно PowerShell с повышенными разрешениями. (Для этого необходимо быть членом группы `Administrators` или `Backup Operators`.)
2. Сконфигурируйте политику выполнения сценариев, чтобы разрешить запуск недоверяемых сценариев, для чего введите следующую команду (и введите `Y` в ответ на запрос):

```
Set-ExecutionPolicy Unrestricted
```

3. Введите следующий сценарий PowerShell, приведя значения для командлетов `New-WBBackupTarget` и `Get-WBVirtualMachine` в соответствие со своей средой:

```
# Создание новой политики резервного копирования
$BackupPolicy = New-WBPolicy

# Указание целевого местоположения
$BackupTarget = New-WBBackupTarget -VolumePath F:

# Добавление целевого местоположения к политике
Add-WBBackupTarget -Policy $BackupPolicy -Target $BackupTarget

# Указание имени виртуальной машины
$VMs = Get-WBVirtualMachine | where vmname -like "ws2012r2*"
Add-WBVirtualMachine -Policy $BackupPolicy -VirtualMachine $VMs

# Конфигурирование расписания
$BackupTime = [datetime] "23:00"
Set-WBSchedule -Policy $BackupPolicy -Schedule $BackupTime

# Активизация политики
Set-WBPolicy -Policy $BackupPolicy -AllowDeleteOldBackups
```

4. После выполнения этого сценария ваша политика резервного копирования будет сконфигурирована для запуска в запланированное время. Вы можете просмотреть задание резервного копирования в консоли Windows Server Backup (рис. 32.5).

Командлеты PowerShell для Windows Server Backup

Полный список и описание всех командлетов PowerShell для Windows Server Backup доступен по ссылке `http://tinyurl.com/ws2012R2wsb`.

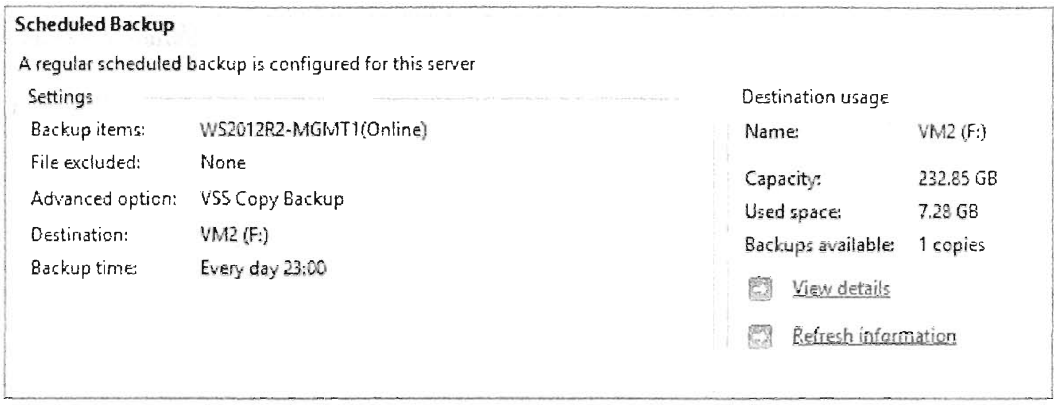


Рис. 32.5. Просмотр задания резервного копирования, созданного с помощью PowerShell

Выполнение полного восстановления сервера

Восстанавливать сервер можно с применением разных методов в зависимости от объема данных, которые должны быть восстановлены, и от времени, которое вы готовы потратить на восстановление. Рассмотрим самый худший сценарий, когда на сервере утеряны все данные либо в результате отказа оборудования, либо по причине повреждения данных. В этом случае можно было бы переустановить операционную систему Windows Server 2012 R2 и затем провести полное восстановление сервера с помощью Windows Server Backup. В качестве альтернативы можно было бы выполнить восстановление с нуля, используя установочный носитель Windows Server 2012 R2 и полную резервную копию сервера. Этот процесс ориентирован на небольшие среды и не подойдет, если вы управляете крупной организацией с несколькими контроллерами домена.

В описанной ниже последовательности действий предполагается, что данные на вашем серверном компьютере полностью утеряны и отказ оборудования вынудил заменить жесткие диски. Прежде всего, удостоверьтесь в том, что новые жесткие диски имеют, по крайней мере, не меньшую емкость, чем заменяемые. Обязательно подключите устройство, содержащее резервную копию, с которой будет производиться восстановление, чтобы программа Windows Setup была способна найти его. В качестве альтернативы можете обратиться к резервной копии, находящейся в открытой сетевой папке.

1. Загрузите компьютер из носителя Windows Server 2012 R2.
2. В диалоговом окне установки Windows выберите требуемые языковые параметры и щелкните на кнопке Yes (Да).
3. Щелкните на ссылке Repair your computer (Восстановить компьютер) внизу слева.
4. На экране Choose an Option (Выбор действия) щелкните на ссылке Troubleshoot (Поиск и устранение проблем), чтобы продолжить.
5. На экране Advanced Options (Дополнительные параметры восстановления) щелкните на ссылке System Image Recovery (Восстановление из образа системы), как показано на рис. 32.6.

   Программа Windows Setup попытается идентифицировать любые существующие установки Windows на жестких дисках и, если обнаружит их, то предложит восстановить. В случае восстановления на чистый жесткий диск вы получите сообщение об ошибке, указывающее на невозможность нахождения образа системы.

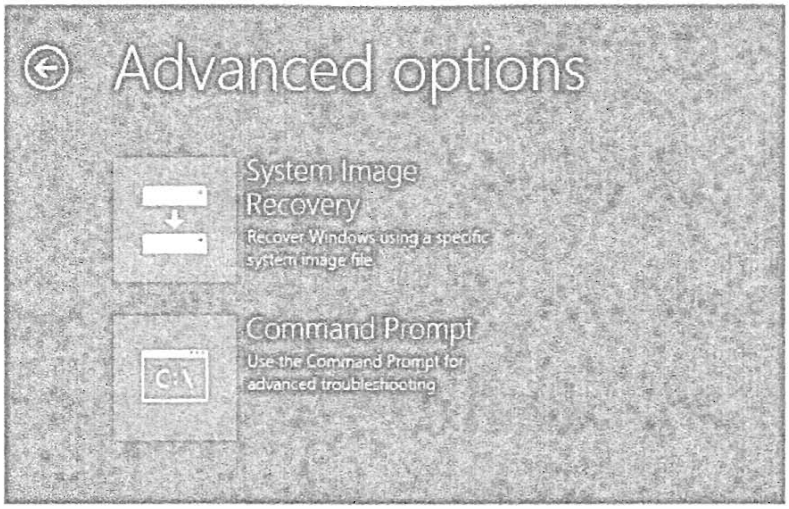


Рис. 32.6. Дополнительные параметры восстановления

6. Щелкните на кнопке Next (Далее).
7. В мастере повторного создания образа компьютера (Re-image your computer wizard) выберите один из переключателей Use the latest available system image (Использовать последний доступный образ системы) или Select a system image (Выбрать образ системы).

   Если выбран переключатель Select a system image, отобразится список образов, обнаруженный мастером, которые можно применять для восстановления сервера. Щелчок на кнопке Advanced (Дополнительно) предоставит возможность поиска образа в сети, а также установки драйвера для нового компьютера, который мог быть не включен в образ, созданный в результате резервного копирования.
8. Сделав необходимый выбор, щелкните на кнопке Next, чтобы продолжить.
9. На экране Select the date and time of system image to restore (Выбор даты и времени восстановления образа системы) выберите доступную резервную копию и щелкните на кнопке Next.
10. На экране Choose additional restore options (Выбор дополнительных параметров восстановления) выберите подходящие вам параметры.
    - Отметьте флажок Format and repartition disks (Форматировать диски и заново создать разделы), чтобы сформатировать и создать разделы на дисках, куда будет проводиться восстановление. Когда этот флажок отмечен, становится доступной кнопка Exclude disks (Исключить диски), щелкнув на которой можно исключить из процесса форматирования какие-то диски. Это особенно важно, когда вы восстанавливаете только диск, содержащий операционную систему, и не хотите затрагивать данные, хранящиеся на других томах.
    - Если вы не видите все диски, установленные на данном компьютере, может потребоваться установить недостающие драйверы. Щелкните на кнопке Install drivers (Установить драйверы).
    - Щелкнув на кнопке Advanced (Дополнительно), укажите, должен ли компьютер автоматически перезапускаться и нужно ли при перезапуске проверять диски на предмет наличия ошибок.
11. Просмотрите выбранные параметры и щелкните на кнопке Finish (Готово), чтобы начать восстановление.

При выполнении восстановления из сетевого расположения удостоверьтесь, что во время восстановления сервер не функционирует как контроллер домена. Сервер, содержащий резервные копии, должен быть доступен компьютерам, не входящим в домен, чтобы они могли к нему обращаться в ходе восстановления. По этой причине часто проще провести восстановление из локально подключенного внешнего диска.

Полное восстановление сервера наиболее полезно выполнять на серверном компьютере, который требует полного восстановления операционной системы и всех данных на каждом диске. В случае восстановления только операционной системы или всех данных на критически важных дисках (например, операционной системы и файлов реестра) процесс можно успешно выполнять из программы установки Windows при условии внимательного исключения дисков, не требующих восстановления.

Пример из практики

Когда возникают проблемы

Как администратор сервера вы предпринимаете меры по защите своих данных на тот случай, когда что-то пойдет не так. В связи с этим мы приведем показательный пример. Недавно мы узнали историю одного клиента, который сделал все необходимое, чтобы подготовиться к восстановлению данных. На контроллере домена в его небольшом офисе размещалась не только инфраструктура Active Directory для домена, но также несколько важных приложений и пользовательские данные. Операционная система, приложения и пользовательские данные хранились на комплекте RAID 5, состоящем из четырех физических дисков. Расписание резервного копирования предусматривало создание резервных копий каждую ночь, а полное резервное копирование проводилось вручную не реже одного раза в месяц с сохранением копий за пределами офиса.

Комплекты RAID 5 достаточно отказоустойчивы, чтобы выдержать выход из строя одного жесткого диска без простоя. Вы можете заменить отказавший диск новым и запустить автоматическую перестройку комплекта RAID 5, причем все это на лету. Однако на контроллере домена этого клиента как-то ночью отказали сразу два физических диска. Это была ненормальная ситуация, но восстановление оказалось невозможным.

После обнаружения проблемы на следующее утро администратору удалось восстановить контроллер домена, заменив вышедшие из строя диски, создав новый комплект RAID 5 и выполнив полное восстановление сервера. Процесс предусматривал начальную загрузку компьютера с установочного носителя при подключенном диске с резервной копией и применение этой резервной копии для восстановления с нуля. Работу сервера удалось возобновить всего за несколько часов.

Восстановление состояния системы

Сервер можно также восстановить, заново установив операционную систему и затем с помощью инструмента Windows Server Backup восстановив состояние системы. Такой метод восстановления может быть предпочтительным, если резервная копия хранится на доменном компьютере, к которому невозможно обратиться посредством программы установки Windows.

Чтобы восстановить состояние системы сервера с помощью инструмента Windows Server Backup, выполните перечисленные ниже действия.

1. Откройте консоль Windows Server Backup. Для этого либо в окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Windows Server Backup (Сервис⇨Резервное копирование сервера Windows), либо на начальном экране Windows Server 2012 R2 наберите **backup** и щелкните на значке инструмента Windows Server Backup.
2. Щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) в левой панели дерева и выберите в контекстном меню пункт Recover (Восстановить), чтобы открыть мастер восстановления (Recovery Wizard).
3. На экране Getting Started (Начало работы) выберите один из следующих переключателей.
   - This server (Этот сервер). Будет восстановлен локальный сервер.
   - A backup stored on another location (Резервная копия, хранящаяся в другом месте). Вы будете восстанавливать данные, находящиеся на удаленном сервере. После выбора этого переключателя будет предложено указать местоположение файлов с резервными копиями, которые должны использоваться — либо на локальном компьютере, либо в общей сетевой папке.
4. На экране Select Backup Date (Выбор даты резервного копирования) с помощью календаря выберите дату резервной копии для восстановления и время, если в этот день было создано более одной копии.
5. Для продолжения щелкните на кнопке Next (Далее).
6. На экране Select Recovery Type (Выбор типа восстановления) выберите переключатель System State (Состояние системы) и щелкните на кнопке Next.
7. Укажите место, куда будет выполняться восстановление, выбрав переключатель Original location (Исходное местоположение) или Alternate location (Альтернативное местоположение).

   В случае выбора восстановления в другое место либо введите вручную путь, куда будет выполняться восстановление, либо щелкните на кнопке Browse (Обзор), чтобы указать нужное местоположение.
8. Просмотрите все настройки и щелкните на кнопке Recover (Восстановить), чтобы начать восстановление.

В Windows Server 2012 R2 восстановить состояние системы можно также в командной строке с помощью инструмента `Wbadmin.exe` или в окне PowerShell с использованием командлета `Start-WBSystemStateRecovery`. Ниже приведен пример восстановления состояния системы с помощью `Wbadmin.exe`:

```
Wbadmin.exe start systemstaterecovery -version -backupTarget
  -machine -recoveryTarget -authsysvol -autoreboot
```

- **`-version`**. Определяет дату и время резервной копии. Например, чтобы указать резервную копию, созданную 12 мая 2015 г. в 23:00, используйте `-version:05/12/2015-23:00`.

- **-backupTarget**. Определяет компьютер, на котором хранится файл резервной копии, например, -backupTarget:\\server1\share.
- **-machine**. Определяет имя восстанавливаемого компьютера; применяйте этот переключатель в сочетании с -backupTarget, если в одном месте хранятся резервные копии для нескольких компьютеров, например: -machine:Server1.
- **-recoveryTarget**. Определяет, куда будет выполняться восстановление с резервной копии, если восстановление производится не в исходное местоположение.
- **-authsysvol**. Указывает, что должно быть выполнено авторитетное восстановление общей папки SYSVOL.
- **-autoreboot**. Сообщает процедуре восстановления о необходимости автоматического перезапуска компьютера после того, как восстановление состояния системы завершено.

Предостережение

После запуска восстановления состояния системы вы не должны останавливать его или перезагружать компьютер до тех пор, пока восстановление не будет завершено. Если процесс восстановления состояния системы прервать, серверный компьютер может остаться в состоянии, в котором начальная загрузка невозможна.

Резервное копирование и восстановление файлов и папок

В дополнение к созданию полных резервных копий сервера и состояния системы инструмент Windows Server Backup позволяет выполнять резервное копирование и восстановление индивидуальных файлов, папок и томов. Этот метод следует применять, когда вы больше заинтересованы в восстановлении данных, чем самой операционной системы, или если вы создаете промежуточные резервные копии важных данных, которые изменяются часто. Резервное копирование папок с данными может быть полезно в сценариях восстановления, в которых операционная система может восстанавливаться с использованием образов, а данные — с помощью резервных копий.

Создание резервной копии файлов и папок вручную

Резервное копирование данных (файлов и папок) в Windows Server Backup может выполняться либо по расписанию, либо вручную. Одна из распространенных конфигураций резервного копирования для сервера, на котором размещены важные данные, может предусматривать создание полной резервной копии сервера каждую ночь и дополнительных резервных копий файлов и папок с данными на протяжении дня.

В следующих шагах предполагается, что инструмент Windows Server Backup уже установлен, как обсуждалось ранее в этой главе, и у вас есть папки, которые содержат данные, подлежащие резервному копированию.

1. Откройте консоль Windows Server Backup. Для этого либо в окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Windows Server Backup (Сервис⇨Резервное копирование сервера Windows), либо на начальном экране Windows Server 2012 R2 наберите **backup** и щелкните на значке инструмента Windows Server Backup.
2. Щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) в левой панели дерева и выберите в контекстном меню пункт Backup Once (Однократное резервное копирование), чтобы открыть мастер однократного резервного копирования (Backup Once Wizard). Щелкните на кнопке Next (Далее).
3. На экране Select Backup Configuration (Выбор конфигурации резервного копирования) выберите переключатель Custom (Специальная), как показано на рис. 32.7, и щелкните на кнопке Next.

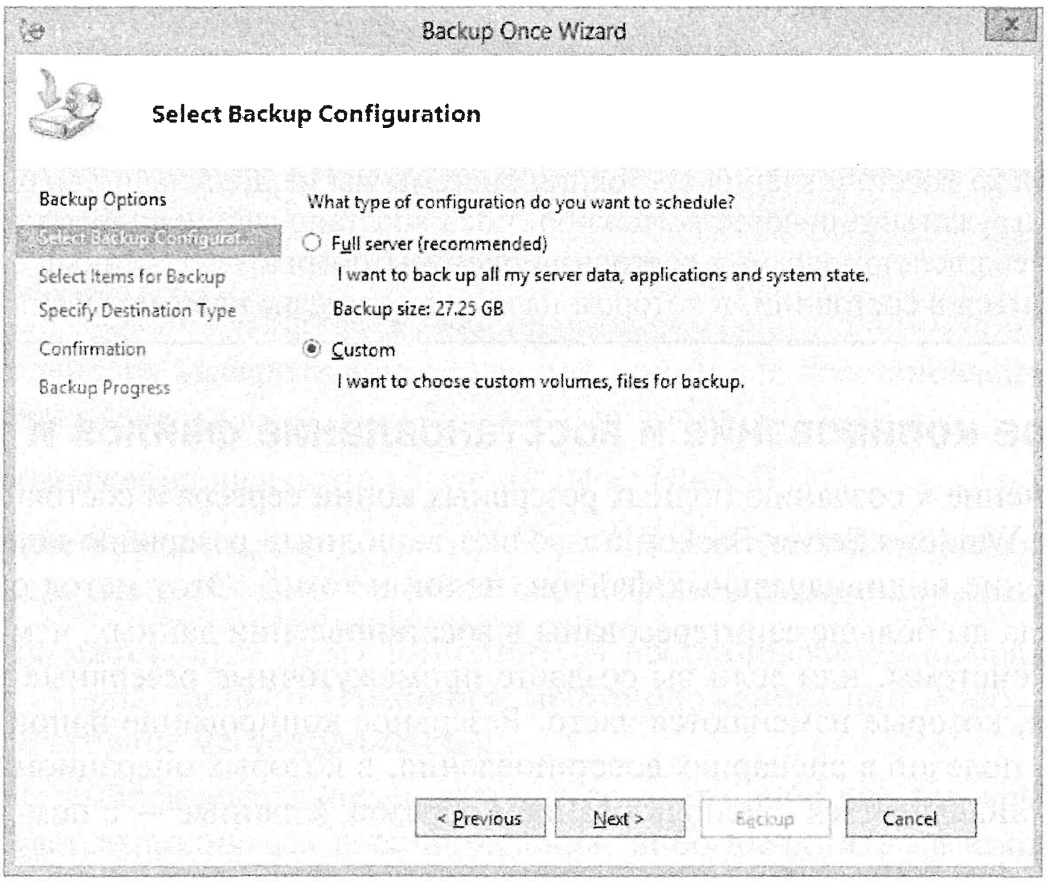


Рис. 32.7. Выбор переключателя Custom для создания резервной копии определенных файлов и папок

4. На экране Select Items for Backup (Выбор элементов для резервного копирования) щелкните на кнопке Add Items (Добавить элементы), чтобы выбрать файлы и папки, подлежащие резервному копированию.
5. Завершив выбор, щелкните на кнопке OK.
6. Щелкните на кнопке Advanced Settings (Дополнительные параметры).

   На вкладке Exclusions (Исключения) вы можете добавить типы файлов, чтобы не включать их в резервную копию. Это очень полезно при резервном копировании томов, на которых имеются файлы вроде MP3 или крупные видеофайлы, не предназначенные для помещения в резервную копию.

На вкладке VSS Settings (Настройки VSS) вы можете изменить поведение инструмента Windows Server Backup по отношению к журналам хронологии резервного копирования. Выберите переключатель VSS Full Backup (Резервная копия полной службы VSS), если Windows Server Backup является единственной программой резервного копирования, которую вы применяете с этими файлами и папками. Если же вы используете дополнительное программное обеспечение резервного копирования и хотите, чтобы журналы резервного копирования остались неизменными после этого ручного копирования, выберите переключатель VSS Copy Backup (Резервная копия копии службы VSS).

7. Щелкните на кнопке OK и затем на кнопке Next.
8. Укажите тип места назначения резервной копии — либо локальный диск, либо сетевое расположение. Щелкните на кнопке Next.
9. Укажите место назначения резервной копии.

   Вид этого экрана будет зависеть от выбранного ранее типа места назначения резервной копии. Если было выбрано сетевое расположение, то можно также указать, будет ли созданный файл резервной копии наследовать разрешения общей папки или к нему будут применены специальные разрешения.

   В случае выбора переключателя Do not inherit (Не наследовать) вам будет предложено предоставить пользовательские учетные данные для назначения разрешений этому файлу.
10. Щелкните на кнопке Next.
11. Просмотрите выбранные настройки и щелкните на кнопке Backup (Копировать), чтобы начать операцию резервного копирования.

На экране Backup Progress (Ход резервного копирования) отображается ход создания резервной копии, включая сообщения о любых возникших ошибках, и сообщение о завершении.

Восстановление папки из резервной копии

Восстановление индивидуальных файлов и папок является довольно распространенной задачей для многих администраторов. Стоит лишь вспомнить, насколько часто к вам обращаются пользователи по поводу случайно удаленной презентации или электронной таблицы, которая им требуется на предстоящей важной встрече. Эту задачу легко решить с помощью специального восстановления в Windows Server Backup (при условии доступности файлов резервных копий).

1. Откройте консоль Windows Server Backup. Для этого либо в окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Windows Server Backup (Сервис⇨Резервное копирование сервера Windows), либо на начальном экране Windows Server 2012 R2 наберите `backup` и щелкните на значке инструмента Windows Server Backup.
2. Щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) в левой панели дерева и выберите в контекстном меню пункт Recover (Восстановить), чтобы открыть мастер восстановления (Recovery Wizard).

3. Выберите местоположение файла резервной копии, который будет использоваться для этого восстановления (мы выбрали переключатель This server (Этот сервер)).

   В случае выбора удаленного местоположения на последующих шагах вам придется указать тип места назначения и путь к нему.

4. Щелкните на кнопке Next (Далее).
5. Выберите дату и время нужной резервной копии.

   При наличии только одной резервной копии по умолчанию дата и время будут соответствовать этой резервной копии. Если резервных копий несколько, то дата и время по умолчанию будут установлены в самую последнюю из них.

6. Щелкните на кнопке Next.
7. На экране Select Recovery Type (Выбор типа восстановления) выберите переключатель Files and Folders (Файлы и папки) и щелкните на кнопке Next.
8. Найдите папку, которую нужно восстановить, в древовидном представлении Available items (Доступные элементы).
9. Если вы пытаетесь восстановить отдельные файлы, выберите эти файлы в панели Items to recover (Элементы, подлежащие восстановлению) и щелкните на кнопке Next.
10. На экране Select Recovery Options (Выбор параметров восстановления) выберите место для восстановления, разрешения для восстанавливаемых файлов и папок и действие на случай, если в месте для восстановления существуют копии файлов. Щелкните на кнопке Next.
11. Просмотрите выбранные настройки и щелкните на кнопке Recover (Восстановить), чтобы начать восстановление.

Одиночную папку можно также восстановить в командной строке. В следующем примере восстанавливается папка `C:\Library`:

```
Wbadmin.exe START RECOVERY -version:05/12/2015-18:39
  -items:C:\Library -itemtype:File -backupTarget:E: -recursive
```

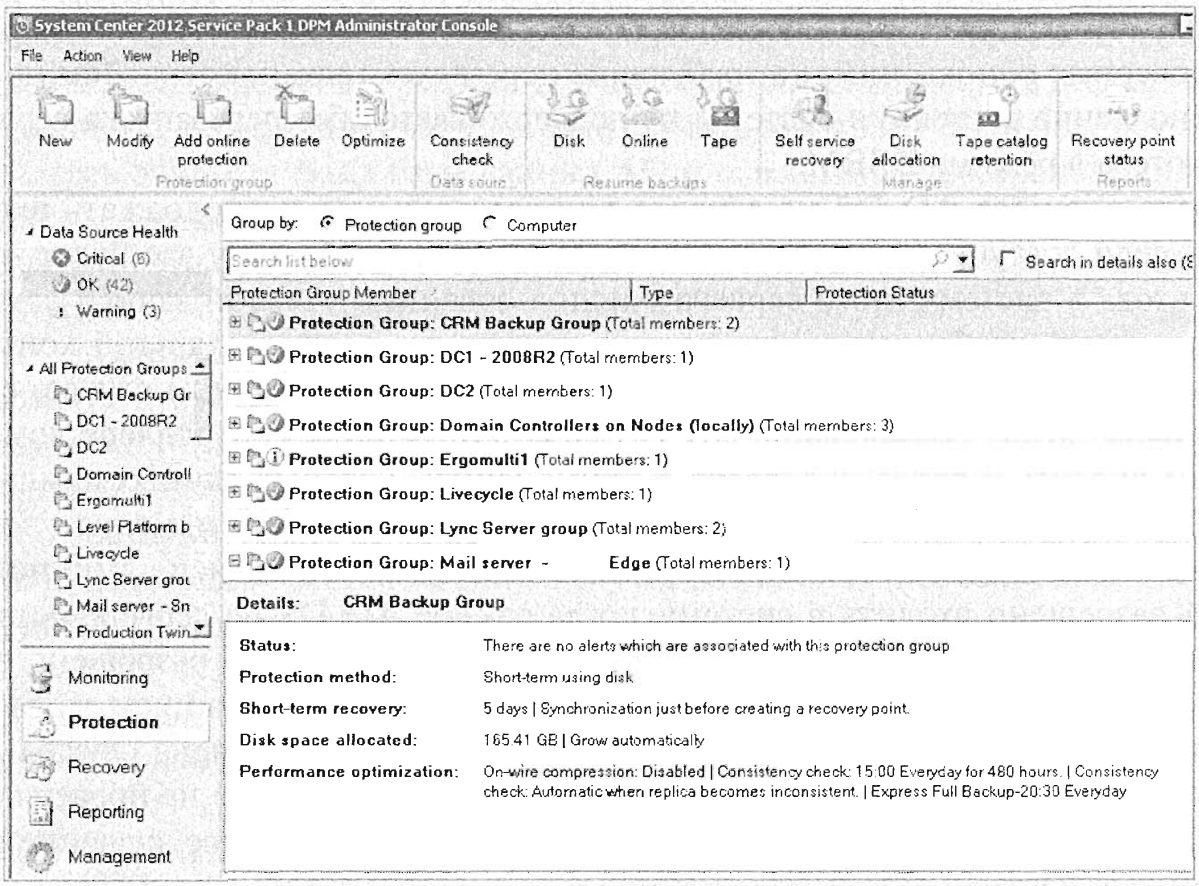
- **`START RECOVERY`**. Этот переключатель сообщает `Wbadmin.exe` о необходимости начать операцию восстановления.
- **`-version`**. Переключатель `-version` определяет версию резервной копии, которая будет использоваться для восстановления. Он задается в формате `ММ/ДД/ГГГГ-ЧЧ:ММ`. Чтобы получить список доступных версий резервной копии, введите команду `Wbadmin.exe GET VERSIONS`.
- **`-items`**. Этот переключатель предоставляет список разделяемых запятыми элементов, подлежащих восстановлению.
- **`-itemtype`**. Этот переключатель определяет тип объектов в списке `-items` и может включать `FILE`, `APP` и `VOLUME`. Для указания более одного типа объектов в операции восстановления применяйте отдельные переключатели.
- **`-backupTarget`**. Этот переключатель определяет местоположение файла резервной копии, который вы хотите использовать в операции восстановления.

Диспетчер защиты данных системного центра 2012 R2

В главе 30 вы узнали, что системный центр 2012 R2 (System Center 2012 R2) представляет собой основное решение по управлению системами, предлагаемое Microsoft. Диспетчер защиты данных (Data Protection Manager — DPM) — это продукт резервного копирования, входящий в комплект System Center 2012 R2, который является оптимальным решением для резервного копирования рабочих нагрузок Microsoft. С помощью DPM можно создавать резервные копии целых виртуальных машин либо только отдельных файлов или папок. Инструмент DPM можно интегрировать в такие приложения, как SQL, SharePoint и Exchange, обеспечивая высокоскоростное резервное копирование и восстановление данных, содержащихся внутри этих приложений.

Основным носителем резервных копий считается диск, но также предусмотрена возможность резервного копирования на внешнее ленточное устройство, если вам требуется долговременно хранить данные (вспомните, что инструмент Windows Server Backup не поддерживает резервные копии на лентах). Для восстановления в аварийных ситуациях (disaster recovery — DR) вы можете сконфигурировать главный сервер DPM на производственном сайте и дополнительный сервер DPM на сайте DR, после чего настроить репликацию наборов резервных копий (известных как группы защиты) через каналы WAN, чтобы предохранить свои данные.

Инструмент DPM производит резервное копирование Windows Server 2012 R2 с помощью агента, а все управление обеспечивается посредством консоли администрирования DPM (DPM Administrator Console), окно которой показано на приведенном ниже рисунке:



Если вы хотите получить дополнительные сведения о диспетчере защиты данных, загрузите его пробную версию по ссылке `http://www.microsoft.com/systemcenter`.

Резервное копирование в облако

Решением восстановления в аварийных ситуациях для резервных копий Windows Server 2012 R2, дополняющим инструмент DPM, является Windows Azure Backup. Это дополнение предоставляет маршрут в облачный продукт Microsoft Azure и делает возможным резервное копирование и восстановление файлов, папок и даже виртуальных машин, находящихся на компьютерах Windows Server 2012 R2. Его можно применять бок о бок с Windows Server Backup либо интегрировать в DPM. Когда решение Windows Azure Backup развернуто, его можно запускать из тех же самых оснасток управления.

Конечно, необходимо располагать подходящим подключением к Интернету — если вы все еще получаете доступ в веб по линии DSL со скоростью 1 Мбит/с, то забудьте о создании резервной копии в облаке! Кроме того, понадобится создать идентификатор онлайновой учетной записи Azure. С официальной документацией TechNet можно ознакомиться по ссылке `http://tinyurl.com/ws2012R2wab`. Если вы хотите посмотреть, как получить и запустить Windows Azure Backup, рекомендуем почитать следующую статью: `http://tinyurl.com/ws2012azurebackup`.

Останов и перезапуск Active Directory

Перезапускаемую службу Active Directory Domain Services (AD DS), которая появилась в Windows Server 2008, можно останавливать для проведения обслуживания на сервере без необходимости перезапуска сервера в режиме восстановления службы каталогов (Directory Services Restore Mode — DSRM). Преимущества возможности останова и перезапуска AD DS включают автономную дефрагментацию и применение серверных обновлений, не требующие перезапуска компьютера. Тем не менее, восстановление состояния системы не поддерживается без перезапуска серверного компьютера в режиме DSRM.

После останова AD DS на сервере пользователи могут продолжать входить в домен, если доступны другие контроллеры домена. Вдобавок у вас будет возможность входа в систему этого сервера с использованием учетной записи администратора домена, чтобы выполнить задачи на сервере, если есть другой контроллер домена, способный обработать ваш запрос на вход. В противном случае, если вы остановили функционирование AD DS на единственном контроллере домена, то должны входить в систему сервера с применением учетных данных администратора DSRM. Чтобы включить эту возможность, потребуется изменить значение `DSRMAdminLogonBehavior` в реестре либо на `1` (учетной записи администратора DSRM разрешено входить в систему, когда служба AD DS на сервере остановлена), либо на `2` (учетной записи администратора DSRM всегда разрешено входить в систему сервера). Вариант с разрешением учетной записи администратора DSRM всегда входить в систему сервера независимо о того, остановлена служба AD DS или нет, не является хорошей идеей, поскольку учетные данные не проверяются на предмет соблюдения политик в отношении паролей. Упомянутое значение реестра находится здесь:

```
HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior
```

Останов и запуск AD DS

Останов службы AD DS осуществляется точно так же, как любой другой службы в Windows, с помощью оснастки Services (Службы), доступной через меню Tools (Сервис) диспетчера серверов или в командной строке.

Чтобы выполнить описанные ниже действия, вы должны быть членом группы `Domain Administrators` (Администраторы домена).

1. В окне диспетчера серверов выберите пункт меню Tools⇨Services (Сервис⇨Службы).
2. Щелкните правой кнопкой мыши на элементе Active Directory Domain Services (Службы домена Active Directory) в панели подробностей и выберите в контекстном меню пункт Stop (Остановить).

   Вам будет предложено согласиться с остановом других служб, от которых зависит AD DS.
3. Примите приведенный список служб, и они также будут остановлены.

   Службы будут перезапущены, когда вы снова запустите AD DS.
4. Чтобы запустить AD DS, щелкните правой кнопкой мыши на элементе Active Directory Domain Services и выберите в контекстном меню пункт Start (Запустить).

Автономная дефрагментация Active Directory

Чтобы выполнить автономную дефрагментацию и проверку целостности базы данных Active Directory, в более ранних версиях Windows Server приходилось перезапускать контроллер домена в режиме DSRM. Хотя необходимость в дефрагментации AD возникает не особенно часто, в ряде случаев это может быть полезно, когда вы собираетесь очистить файл базы данных AD и освободить пространство на системном диске, а также потенциально улучшить производительность AD в крупных средах. В версии Windows Server 2012 R2 появилась возможность решать эти задачи, не перезапуская компьютер и не переходя в режим DSRM. Вместо этого вы можете остановить службу AD DS, а затем в окне командной строки с повышенными разрешениями запустить `Ntdsutil.exe`, чтобы выполнить автономную дефрагментацию и проверку целостности базы данных AD.

Прежде чем выполнять автономную дефрагментацию, разумно создать резервную копию состояния системы и критически важных дисков контроллера домена, обеспечив возможность восстановления в случае возникновения серьезных ошибок. На томе, который содержит базу данных AD DS (`Ntds.dit`), вы должны удостовериться в наличии достаточного свободного пространства для временного хранения данных. В Microsoft рекомендуют, чтобы свободное пространство для временного хранения составляло не менее 15% от размера файла `Ntds.dit`.

Active Directory автоматически выполняет онлайновую дефрагментацию с целью оптимизации хранения данных в файле `Ntds.dit` в ходе ежедневного процесса сборки мусора. Эта процедура помогает оптимизировать базу данных, но ничего не делает в плане сокращения размера файла базы данных. Автономная дефрагментация Active Directory является единственным эффективным способом сокращения размера файла базы данных.

Выполнение автономной дефрагментации файла Ntds.dit

В приведенных далее шагах предполагается, что вы остановили службу AD DS, как обсуждалось выше, и будете выполнять сжатие файла `Ntds.dit` в локальную папку. Если вы планируете дефрагментировать и сжимать базу данных в удаленную общую папку, то заранее отобразите на нее какую-то букву диска и указывайте ее в пути, где это необходимо.

1. Откройте окно командной строки с повышенными разрешениями.
2. Введите **`ntdsutil`** и нажмите <Enter>.
3. Введите **`Activate instance NTDS`** и нажмите <Enter>.
4. В приглашении `ntdsutil` введите **`Files`** (эта подкоманда чувствительна к регистру символов) и нажмите <Enter>.
5. В приглашении `file maintenance` введите **`compact to`** и путь к целевой папке для дефрагментации и нажмите <Enter>.

   Если в пути к целевой папке имеются пробелы, поместите путь в двойные кавычки (например, **`"c:\temp folder\"`**). Утилита `Ntdsutil.exe` будет отображать ход процесса дефрагментации. По завершении вам будет рекомендовано немедленно создать резервную копию исходного и сжатого файлов.
6. Скопируйте новый файл `Ntds.dit` в каталог `%systemroot%\NTDS\` (например, `c:\Windows\NTDS\Ntds.dit`).
7. Удалите все журнальные файлы в папке `NTDS` (например, введите **`del C:\Windows\NTDS\*.log`**).
8. Введите **`quit`** и нажмите <Enter>, чтобы выйти из режима обслуживания файла, после чего введите **`quit`** и нажмите <Enter> еще раз, чтобы выйти из `Ntdsutil.exe`.
9. Выполнив все эти действия, перезапустите AD DS.

Интересно отметить, что после останова AD DS вы не сможете обратиться к файлам и папкам на серверном компьютере, не предоставив учетные данные администратора DSRM.

Проверка целостности базы данных Active Directory

В Active Directory используется тот же самый механизм баз данных ISAM (Indexed Sequential Access Manager — диспетчер последовательного индексированного доступа), что и в Exchange Server, а версия, применяемая в Windows Server 2012 R2, называется *расширяемым механизмом хранения* (Extensible Storage Engine — ESE).

Встречаются ситуации, когда вам необходимо проверить целостность базы данных AD — возможно, чтобы устранить предпосылки к разрушению и сгенерировать отчеты об удаленных или фантомных записях, на которые имеются ссылки. Целостность файла `Ntds.dit` можно проверить двумя способами: в первом используется подкоманда `Files` утилиты `Ntdsutil.exe`, а во втором подкоманда `Semantic database analysis` той же утилиты. В Microsoft предупреждают, что подкоманда `Semantic database analysis` не должна применяться при нормальном управлении базой данных, т.к. ее некорректное использование может привести к серьезной утере данных Active Directory.

Подкоманду Semantic database analysis следует применять только во время поиска и устранения проблем при работе с поддержкой продуктов Microsoft. Но хотя в Microsoft не рекомендуют пользоваться подкомандой Semantic database analysis, каждый раз, когда вы вводите подкоманды integrity и recover в рамках Files, вам предлагается также запустить Semantic database analysis.

Проверка целостности файла Ntds.dit

Подкоманда Files утилиты Ntdsutil.exe позволяет проверить целостность файла базы данных и исправить любые обнаруженные искажения данных. Перед выполнением проверки целостности вы должны всегда применять команду recover. Команда recover сбрасывает все транзакции в файл базы данных, гарантируя наличие в файле самой актуальной информации. Она использует программу Esentutl.exe для выполнения мягкого восстановления базы данных Ntds.dit и фиксирует все незавершенные транзакции.

Чтобы проверить целостность Ntds.dit, после останова службы AD DS выполните следующие шаги.

1. Откройте окно командной строки с повышенными разрешениями.
2. Введите **ntdsutil** и нажмите <Enter>.
3. Введите **Activate instance NTDS** и нажмите <Enter>.
4. В приглашении ntdsutil введите **Files** (эта подкоманда чувствительна к регистру символов) и нажмите <Enter>.
5. В приглашении file maintenance введите **recover** и нажмите <Enter>.
6. Введите **integrity** и нажмите <Enter>.
7. Введите **quit** и нажмите <Enter>, чтобы выйти из режима обслуживания файла, после чего введите **quit** и нажмите <Enter> еще раз, чтобы выйти из Ntdsutil.exe.
8. Выполнив все эти действия, перезапустите AD DS.

Использование семантического анализа базы данных

Подкоманда Files в Ntdsutil.exe проверяет файл Ntds.dit на предмет наличия в нем обычных файловых повреждений. Подкоманда Semantic database analysis проверяет внутреннюю структуру Ntds.dit на ее соответствие нормальной семантике Active Directory и выводит отчет о количестве имеющихся в текущий момент записей, включая удаленные и фантомные записи. Отчет называется dsdit.dmp.x, где x — это число, которое увеличивается каждый раз, когда генерируется новый отчет.

Выполните описанные ниже действия после останова службы AD DS.

1. Откройте окно командной строки с повышенными разрешениями. Щелкните на кнопке Start (Пуск), щелкните правой кнопкой мыши на значке Command Prompt и выберите в контекстном меню пункт Run as Administrator (Запуск от имен администратора).
2. Введите **ntdsutil** и нажмите <Enter>.
3. Введите **Activate instance NTDS** и нажмите <Enter>.

4. Введите **Semantic database analysis** (эта подкоманда чувствительна к регистру символов) и нажмите <Enter>.
5. В приглашении semantic checker введите **Go**, чтобы запустить анализ. Используйте **Go Fixup**, чтобы запустить анализ и исправить семантические ошибки.
6. Введите **quit** и нажмите <Enter>, чтобы выйти из режима семантического анализа, а затем введите **quit** и нажмите <Enter> еще раз, чтобы выйти из Ntdsutil.exe.
7. Выполнив все эти действия, перезапустите AD DS.

Файл отчета, сгенерированный подкомандой Semantic database analysis, находится в текущей папке, из которой запускается Ntdsutil.exe; обычно это c:\Users%username%. Системная переменная %username% будет автоматически заменена именем вошедшего в систему пользователя.

Захват снимков Active Directory

Для создания снимка базы данных AD DS в Windows Server 2012 R2 можно применять службу теневого копирования томов (Volume Shadow Copy Service — VSS). Этот снимок можно затем использовать как автономную копию для просмотра данных или обработать для последующего применения в качестве базы данных каталога LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам). Снимки могут использоваться для просмотра текущих объектов в AD DS, не подвергая риску текущее состояние базы данных. Более простым методом восстановления удаленных объектов AD DS в Windows Server 2012 R2 является корзина Active Directory, которая описана в разделе "Восстановление удаленного объекта с помощью корзины Active Directory" далее в этой главе.

Создание снимка Active Directory

Создавать снимки AD DS можно с помощью утилиты Ntdsutil.exe, запущенной в окне командной строки с повышенными разрешениями. Поскольку перед созданием снимка останавливать AD DS не нужно, снимки идеально подходят для просмотра объектов из контроллера домена, не переводя его в автономный режим.

1. Откройте окно командной строки с повышенными разрешениями. Щелкните на кнопке Start (Пуск), щелкните правой кнопкой мыши на значке Command Prompt и выберите в контекстном меню пункт Run as Administrator (Запуск от имен администратора).
2. Введите **ntdsutil** и нажмите <Enter>.
3. Введите **Snapshot** и нажмите <Enter>.
4. В приглашении snapshot введите **Activate instance NTDS** и нажмите <Enter>.
5. Введите **Create** и нажмите <Enter>.
   Снимок создается с отображением его идентификатора GUID (рис. 32.8).
6. Введите **quit** и нажмите <Enter>, чтобы выйти из режима снимков, а затем введите **quit** и нажмите <Enter> еще раз, чтобы выйти из Ntdsutil.exe.

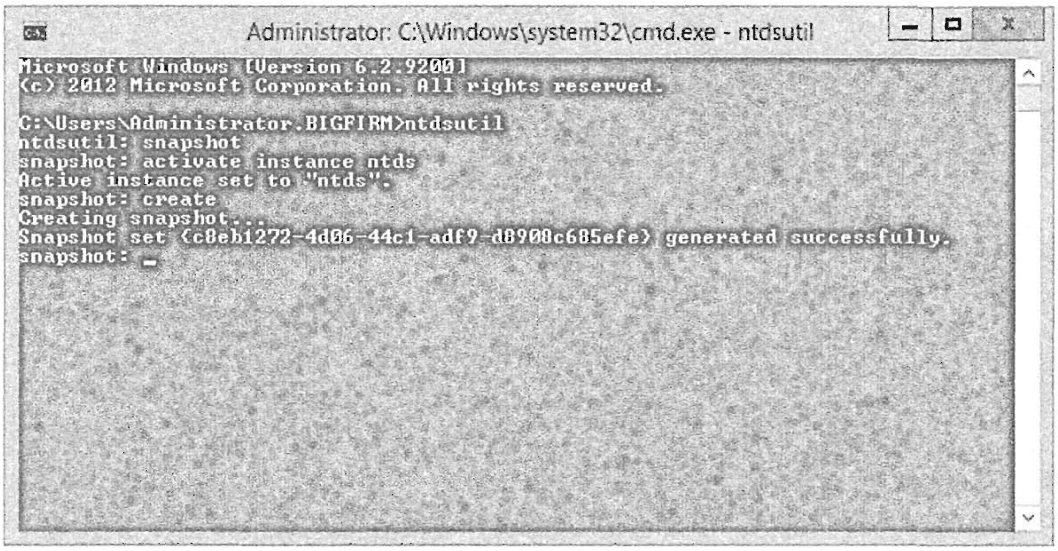


Рис. 32.8. Создание снимка Active Directory

Монтирование снимка Active Directory

Со снимком Active Directory можно работать только после его монтирования. Монтирование обеспечивает доступность снимка в виде локального пути на серверном компьютере. После того как снимок смонтирован, вы можете обращаться к файлам AD DS в папке NTDS под Windows.

1. Откройте окно командной строки с повышенными разрешениями.
2. Введите **ntdsutil** и нажмите <Enter>.
3. Введите **Snapshot** и нажмите <Enter>.
4. В приглашении `snapshot` введите **Activate instance NTDS** и нажмите <Enter>.
5. Введите **List All** и нажмите <Enter>.

   В результате отобразятся все снимки, имеющиеся на серверном компьютере. Для каждого из них указывается числовой индекс и идентификатор GUID.
6. Введите **mount x**, где `x` — это либо числовой индекс, либо идентификатор GUID снимка, подлежащего монтированию, и нажмите <Enter>.

   Если команда выполнится успешно, она возвратит локальный путь монтирования снимка, который обычно представляет собой папку, находящуюся в корневом каталоге диска C. Результат должен быть примерно таким, как показано на рис. 32.9.
7. Введите **quit** и нажмите <Enter>, чтобы выйти из режима снимков, а затем введите **quit** и нажмите <Enter> еще раз, чтобы выйти из `Ntdsutil.exe`.

Работа со смонтированными снимками Active Directory

После создания и монтирования снимка Active Directory необходимо обеспечить его доступность с помощью команды `Dsamain.exe`. Утилита `Dsamain.exe` устанавливается в Windows Server 2012 R2 вместе с ролью AD DS или Active Directory Lightweight Directory Services (AD LDS) и для своего использования требует членства в группе `Domain Administrators` (Администраторы домена) или `Enterprise Administrators` (Администраторы предприятия).

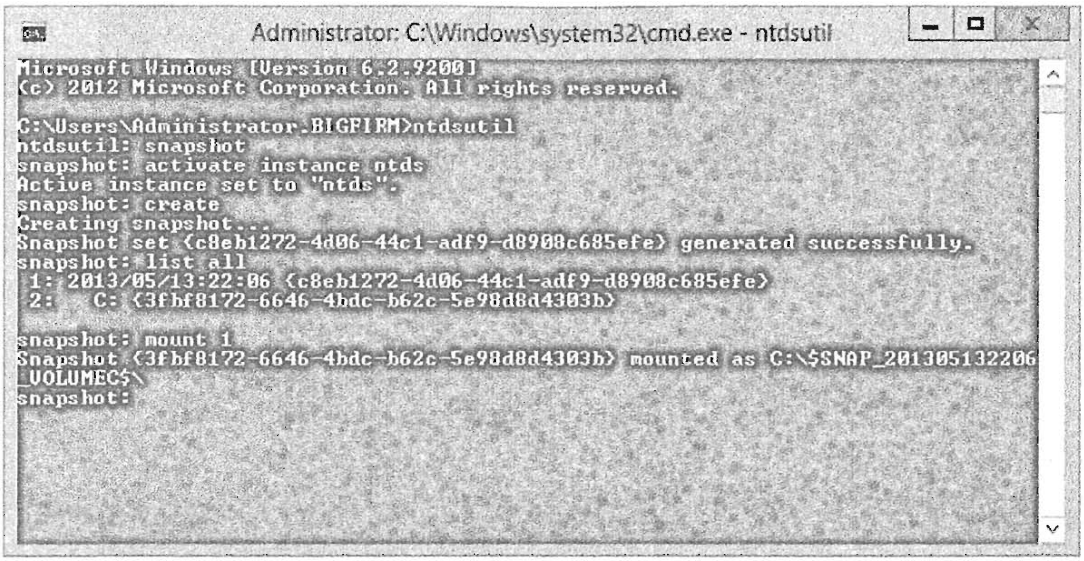


Рис. 32.9. Монтирование снимка Active Directory

Использование `Dsamain.exe`

Утилита `Dsamain.exe` делает доступной копию базы данных AD DS через LDAP из серверного компьютера. С помощью LDAP вы можете обращаться к этой версии AD DS с применением разнообразных инструментов, таких как `Ldp.exe` или любая оснастка Active Directory в Windows Server 2012 R2.

В приведенных ниже действиях предполагается, что вы уже создали и смонтировали снимок, используя описанные ранее процедуры.

1. В проводнике Windows перейдите к файлу `Ntds.dit` в смонтированном снимке. Путь может выглядеть примерно так: `c:\$SNAP_200906191422_VOLUMEC$\Windows\NTDS\Ntds.dit`.
2. Удерживая нажатой клавишу <Shift>, щелкните правой кнопкой мыши на файле `Ntds.dit` выберите в контекстном меню пункт Copy as path (Копировать как путь).
3. Откройте окно командной строки с повышенными разрешениями.
4. Введите команду **`dsamain /dbpath <путь> /ldapPort 10389`**. Чтобы указать значение `<путь>`, щелкните правой кнопкой мыши в окне командной строки и выберите в контекстном меню пункт Paste (Вставить), чтобы вставить скопированный ранее путь.

   Результат должен быть подобен показанному ниже:

   ```
   Dsamain /dbpath "C:\$SNAP_200906191422_VOLUMEC$\Windows\NTDS\Ntds.dit"
     /ldapPort 10389
   ```

5. Если команда выполнится успешно, оставьте окно командной строки открытым на время работы со смонтированным снимком.

   Закрыв окно командной строки, вы закроете сеанс `Dsamain.exe`.

6. Чтобы выйти из `Dsamain.exe`, нажмите <Ctrl+C>.

Имея смонтированный снимок, доступный как экземпляр LDAP, его можно просмотреть посредством любого инструмента, который способен подключаться к LDAP, например, `adsiedit`.

7. В окне командной строки с повышенными разрешениями введите `adsiedit` и нажмите <Enter>.
8. Выберите в меню Action (Действие) пункт Connect to (Подключиться к).
9. Щелкните на кнопке Advanced (Дополнительно).
10. В поле Port (Порт) введите номер порта, ранее назначенный в командной строке `Dsamain.exe`. Щелкните на кнопке OK.
11. Щелкните на кнопке OK, чтобы подключиться к экземпляру LDAP.

Инструмент `adsiedit` можно применять для просмотра содержимого снимка, скажем, с целью проверки, что объекты действительно были созданы.

Резервное копирование и восстановление Active Directory

Резервная копия Active Directory создается при резервном копировании состояния системы на контроллере домена с помощью Windows Server Backup, `Wbadmin.exe` или PowerShell. Как указывалось ранее в этой главе, чтобы инструмент Windows Server Backup можно было использовать для резервного копирования или восстановления серверного компьютера, он должен быть установлен как компонент в диспетчере серверов.

Выбираемый для контроллеров домена тип резервного копирования будет зависеть от частоты изменений в Active Directory и данных либо приложений, которые могут быть установлены на контроллере домена. Для защиты AD DS на контроллере домена понадобится, как минимум, создать резервную копию состояния системы. Состояние системы включает перечисленные ниже элементы, а также ряд дополнительных элементов в зависимости от установленных ролей:

- база данных Active Directory (`Ntds.dit`);
- реестр;
- регистрационная база данных COM+;
- база данных служб сертификатов Active Directory (Active Directory Certificate Services);
- файлы начальной загрузки;
- папка SYSVOL;
- информация службы кластеров;
- любые системные файлы, которые защищены посредством защиты ресурсов Windows;
- метакаталог информационных служб Интернета от Microsoft (Microsoft Internet Information Services).

Следующий уровень защиты резервным копированием обеспечивается созданием резервных копий критически важных томов, в число которых входят следующие тома:

- том, содержащий файлы начальной загрузки, включая Bootmgr и хранилище данных о конфигурации загрузки (Boot Configuration Data — BCD);
- том, содержащий операционную систему Windows и реестр;
- том, содержащий структуру папок;
- том, содержащий базу данных AD DS (`Ntds.dit`) и журнальные файлы.

Эти типы резервного копирования могут выполняться вручную по запросу или по расписанию либо с помощью Windows Server Backup, либо посредством `Wbadmin.exe` и запланированных задач (Scheduled Tasks).

Ограничения резервных копий Active Directory

Чтобы создать резервную копию Active Directory, можно использовать Windows Server Backup или `Wbadmin.exe` для резервного копирования состояния системы контроллера домена. В Microsoft рекомендуют применять для резервного копирования либо отдельный внутренний диск, либо внешний съемный диск, такой как жесткий диск USB. Преимущество внешних дисков заключается в том, что их можно использовать для хранения за пределами организации как часть обычного плана восстановления в аварийных ситуациях. Однако с точки зрения транспортировки они уступают традиционным магнитным лентам, поэтому позаботьтесь о наличии плана транспортировки носителей.

Для планирования запуска резервного копирования или восстановления состояния системы вы должны располагать административными учетными данными; операторы резервного копирования не обладают привилегиями, требуемыми для настройки расписаний резервного копирования. Резервные копии состояния системы будут включать зоны DNS, интегрированные в Active Directory, но не зоны DNS, основанные на файлах. Зоны DNS, основанные на файлах, должно сохраняться при резервном копировании на уровне томов, таком как резервное копирование критически важных томов или полное резервное копирование сервера.

Введение в корзину Active Directory

Если вам когда-либо приходилось по несчастливому стечению обстоятельств случайно удалять объект из Active Directory и затем восстанавливать его из резервных копий, то вы знаете, что это не самая приятная работа из числа тех, которыми приходится заниматься IT-специалистам. К счастью, в Windows Server 2008 R2 появилась корзина Active Directory (Active Directory Recycle Bin), предохраняющая удаленные объекты почти таким же способом, как это делает стандартная корзина Windows в отношении файлов и папок.

Однако недостаток версии корзины в Windows Server 2008 R2 для части пользователей заключался в том, что ей приходилось управлять полностью с помощью PowerShell. В Windows Server 2012 R2 появилась возможность управления корзиной посредством графического пользовательского интерфейса инструмента ADAC (Active Directory Administrative Center — центр администрирования Active Directory), что существенно облегчает обращение с удаленными объектами.

Корзина Active Directory или состояние системы?

Если вы размышляете, нужно ли вообще создавать резервную копию состояния системы, раз уж сконфигурирована корзина AD, то подумайте еще раз. Корзина AD призвана служить средством, дополняющим обычные резервные копии AD, и не должна использоваться в качестве основного метода восстановления. Это объясняется тем, что возможны ситуации, когда корзина AD оказывается недоступной. Для обращения к корзине AD у вас должна быть возможность входа в домен, а если домен отказал, то и доступа к корзине AD не будет.

В отсутствие корзины Active Directory и в более ранних версиях Windows Server, в которых она не поддерживается, когда вы удаляли объект, он не удалялся немедленно, а помечался как удаленный. Помеченные подобным образом объекты удалялись в ходе процесса сборки мусора.

Тем не менее, благодаря установленной в Windows Server корзине Active Directory процесс изменяется. Теперь, когда объект удаляется, он помечается как удаленный на промежуток времени, определенный свойством `msDS-DeletedObjectLifetime` в AD DS, значение которого по умолчанию является нулевым. Когда время жизни удаленного объекта истекает, этот объект помечается как помещенный в корзину и лишается большинства своих атрибутов. Он по-прежнему находится в контейнере Deleted Objects (Удаленные объекты) и может быть восстановлен в течение отведенного для этой цели срока, который задается атрибутом `tombstoneLifetime` в AD DS.

Что можно сказать об объектах, ранее помеченных как удаленные?

При установке корзины Active Directory все ранее существовавшие объекты, помеченные как удаленные, автоматически становятся объектами, помещенными в корзину, но после этого их невозможно восстановить так, как любые другие объекты, попадающие в корзину. Чтобы предотвратить такую ситуацию, перед установкой корзины Active Directory вы должны восстановить те объекты, помеченные как удаленные, которые желаете сохранить на будущее.

Необходимые условия для корзины Active Directory

Прежде чем переходить к обсуждению включения корзины Active Directory, мы должны рассмотреть условия, необходимые для ее функционирования. Эти условия перечислены ниже.

- Вы развернули минимум один контроллер домена, работающий под управлением Windows Server 2012 R2, с инструментом Active Directory Administrative Center.
- На всех других контроллерах домена в домене функционирует, по меньшей мере, ОС Windows Server 2008 R2 или последующей версии.
- Лес Active Directory должен работать на функциональном уровне Windows Server 2008 R2 или более высоком.

Включение корзины Active Directory

Корзина Active Directory по умолчанию отключена. Ниже представлены действия по включению корзины Active Directory из графического пользовательского интерфейса. Однако имейте в виду, что после включения корзина Active Directory не может быть отключена.

1. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Active Directory Administrative Center (Сервис⇨Центр администрирования Active Directory) и щелкните на своем (локальном) домене в панели навигации слева.
2. В панели Tasks справа щелкните на элементе Enable Recycle Bin (Включить корзину), как показано на рис. 32.10.
3. В диалоговом окне Enable Recycle Bin Confirmation (Подтверждение включения корзины) подтвердите свое согласие с тем, что данное изменение является необратимым, щелкнув на кнопке OK.
4. Щелкните на кнопке OK в открывшемся диалоговом окне, которое информирует о том, что корзина не будет доступна до тех пор, пока не завершится репликация всех контроллеров домена, и затем обновите окно центра администрирования Active Directory.

Включение корзины AD с помощью PowerShell

Используйте следующий сценарий PowerShell как альтернативный метод включения корзины AD:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=BigFirm,DC=COM' -Scope ForestOrConfigurationSet -Target 'BigFirm.com'
```

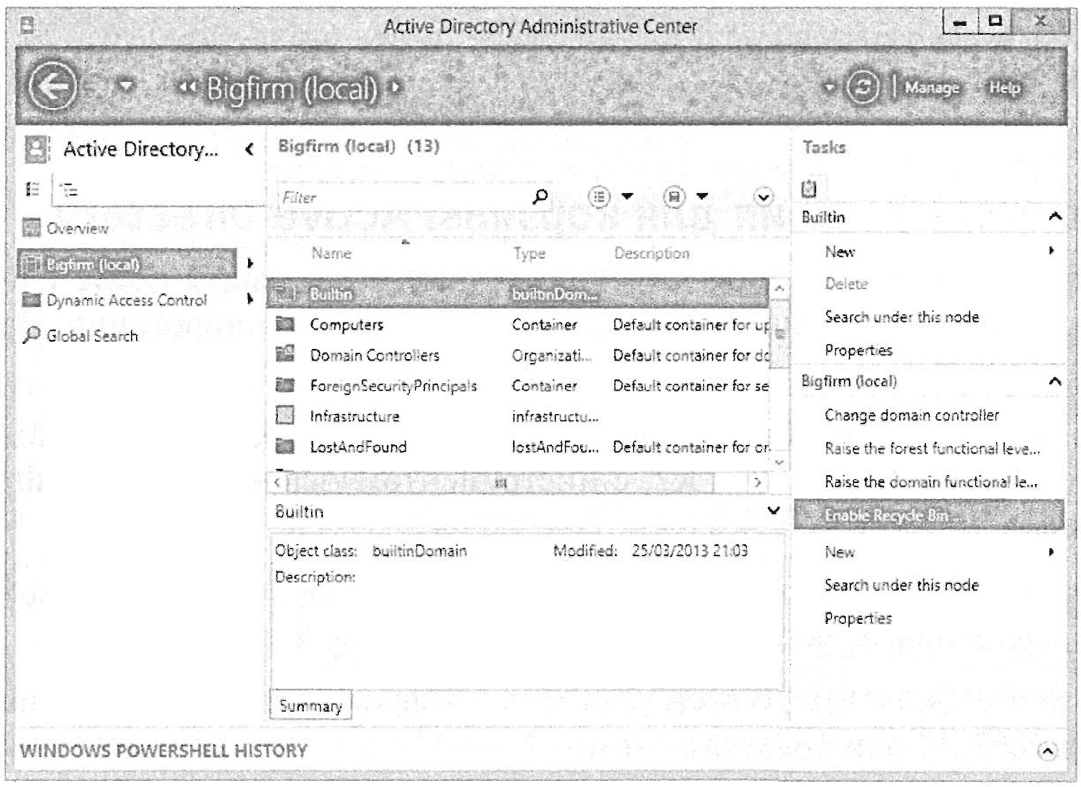


Рис. 32.10. Включение корзины

Восстановление удаленного объекта с помощью корзины Active Directory

Если вы случайно удалили какой-то объект в Active Directory, но имеете включенную корзину AD, выполните перечисленные далее шаги, чтобы быстро восстановить его. (В рассматриваемом примере мы удалили объект пользователя по имени `Sally` и теперь хотим его восстановить.)

1. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Active Directory Administrative Center (Сервис⇨Центр администрирования Active Directory) и щелкните на своем (локальном) домене в панели навигации слева.
2. Дважды щелкните на контейнере Deleted Objects (Удаленные объекты) в центральной панели.
3. Найдите удаленный объект, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Restore (Восстановить) или Restore To (Восстановить в), как показано на рис. 32.11.

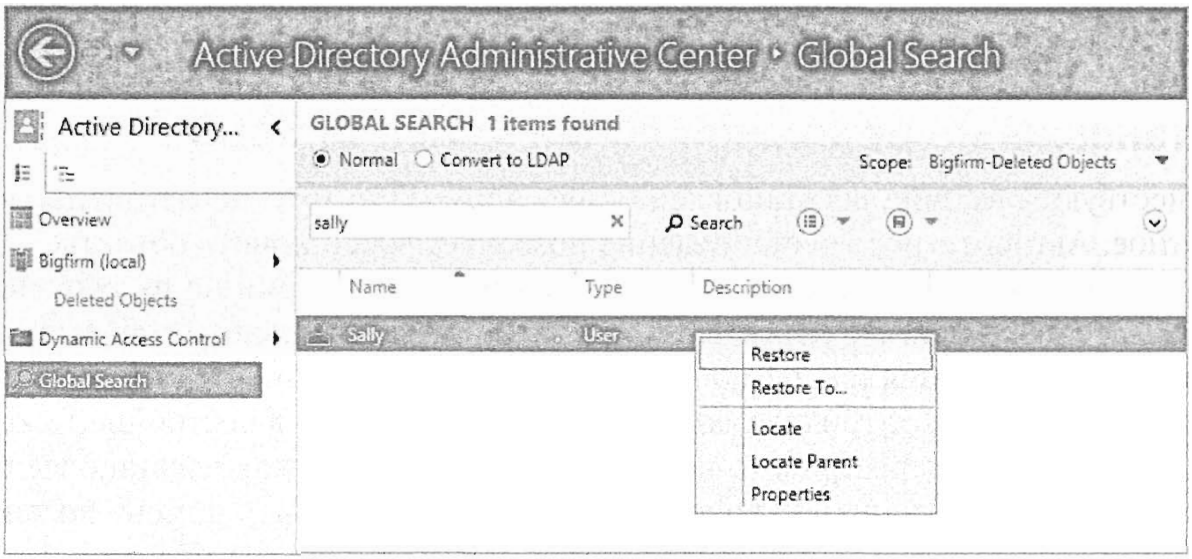


Рис. 32.11. Восстановление объекта с помощью корзины AD

Создание резервной копии Active Directory

Описанные ниже действия позволяют создать резервную копию состояния системы компьютера, которая содержит структуру и базу данных Active Directory.

1. В окне диспетчера серверов при выбранном элементе Local Server (Локальный сервер) выберите пункт меню Tools⇨Windows Server Backup (Сервис⇨Резервное копирование сервера Windows), чтобы открыть эту оснастку MMC.
2. Щелкните правой кнопкой мыши на элементе Local Backup (Локальная резервная копия) в левой панели дерева и выберите в контекстном меню пункт Backup Schedule (Расписание резервного копирования), чтобы открыть мастер расписания резервного копирования (Backup Schedule Wizard).
3. На экране Getting Started (Начало работы) щелкните на кнопке Next (Далее).
4. На экране Select Backup Configuration (Выбор конфигурации резервного копирования) выберите переключатель Custom (Специальная), как показано на рис. 32.7, и щелкните на кнопке Next.

5. На экране Select Items for Backup (Выбор элементов для резервного копирования) щелкните на кнопке Add Items (Добавить элементы), отметьте флажок рядом с элементом System State (Состояние системы) и щелкните на кнопке Next.

6. Продолжайте продвигаться по экранам мастера Backup Schedule Wizard, выбрав время для расписания резервного копирования и параметры сохранения, и затем щелкните на кнопке Finish (Готово), чтобы завершить работу мастера.

Позаботьтесь об обеспечении надлежащей безопасности для резервных копий Active Directory, т.к. они содержат полные копии объектов безопасности домена и учетных данных. Помните, что резервная копия состояния системы является самым надежным способом резервного копирования Active Directory. Если вам когда-либо придется обращаться в Microsoft для получения поддержки по отказавшей среде Active Directory, очень важно иметь рабочую резервную копию состояния системы.

Если для создания резервной копии состояния системы вы применяли продукт от стороннего поставщика, то за помощью в восстановлении вы должны обращаться к этому поставщику. Рекомендуется всегда иметь последнюю копию состояния системы на диске и затем использовать другой продукт резервного копирования, отличный от Microsoft, для создания резервных копий на удаленном диске или ленте.

Восстановление резервной копии Active Directory

Существуют два типа восстановления для Active Directory: авторитетное и неавторитетное. Авторитетное восстановление позволяет восстановить объекты, которые были удалены из Active Directory, но в этом случае репликации не разрешено переписывать восстановленные объекты. Вместо этого восстановленные объекты принудительно реплицируются на другие контроллеры домена в домене. При неавторитетном восстановлении контроллер домена восстанавливается в состояние, в котором он находился во время резервного копирования. После того как восстановление выполнено, вы разрешаете репликации обновить этот контроллер домена до текущего состояния остальной части Active Directory. В этом разделе мы обсудим неавторитетное восстановление. Оба метода выполняются в режиме DSRM, который требует перезапуска серверного компьютера и применения меню, доступного по нажатию клавиши <F8> во время загрузки, для выбора DSRM.

1. Включите питание серверного компьютера. После процедуры самотестирования нажмите клавишу <F8>, чтобы вызвать меню начальной загрузки Windows Server 2012 R2.

2. Выберите режим восстановления службы каталогов (Directory Services Repair Mode — DSRM) и нажмите <Enter>.

3. Нажмите комбинацию клавиш <Ctrl+Alt+Del>, чтобы войти в систему, введите имя пользователя и пароль DSRM и нажмите <Enter>.

   Это более быстрый и легкий процесс по сравнению с тем, что приходилось делать в более ранних версиях Windows Server, поскольку вы входите прямо в систему с отключенными службами Active Directory.

4. Откройте окно командной строки.

5. В окне командной строки введите **wbadmin get versions -backuptarget:<устройство>: -machine:<имя_компьютера>**, где <устройство> — буква диска, где находится резервная копия, а <имя_компьютера> — имя восстанавливаемого компьютера.

   Переключатель -machine является обязательным, только если на диске хранятся резервные копии для нескольких компьютеров.

6. Нажмите <Enter>.

   Обратите внимание, что идентификатор подлежащей восстановлению версии должен вводиться точно.

7. В окне командной строки введите **wbadmin start systemstaterecovery -version:<ММ:ДД:ГГГГ-ЧЧ:ММ> -backuptarget:<устройство>: -machine:<имя_компьютера> -quiet**.

   Переключатель -quiet подавляет выдачу запросов о том, хотите ли вы запустить восстановление, и о том, что состояние системы не изменилось. Команда должна выглядеть похожей на ту, что показана на рис. 32.12.

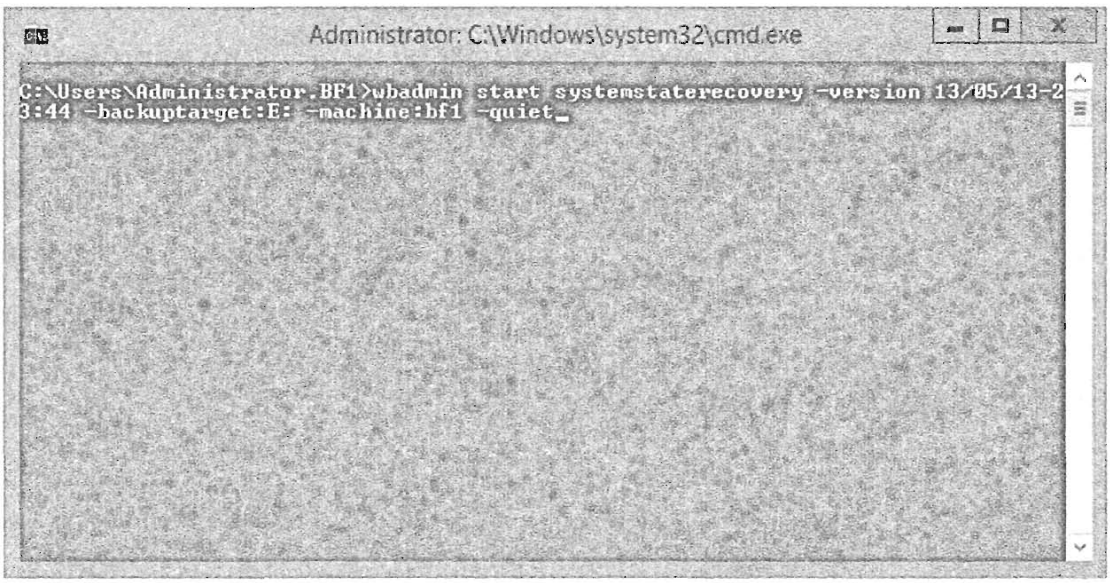


Рис. 32.12. Восстановление состояния системы

Если вы будете выполнять авторитетное восстановление после завершения неавторитетного восстановления, не перезапускайте сервер. Как только вы перезапустите контроллер домена, службы AD DS и Active Directory Certificate Services обнаружат, что произошло восстановление, и запустят автоматическую проверку целостности своих баз данных.

Очистка метаданных

В ситуации, когда из-за отказа оборудования или повреждения операционной системы вышел из строя контроллер домена, иногда быстрее с помощью команды ntdsutil metadata cleanup удалить отказавший контроллер домена, затем установить новый контроллер домена с тем же самым именем и позволить репликации Active Directory сделать все остальное.

Дополнительную информацию об очистке метаданных сервера в Active Directory можно получить по ссылке http://tinyurl.com/ws2012ntdsutil.

Выполнение авторитетного восстановления

Цель авторитетного восстановления заключается в восстановлении удаленных объектов AD DS путем пометки восстановленных объектов как авторитетных или путем пометки новой копии, которая должна быть реплицирована на другие контроллеры домена. Каждый раз, когда в AD DS вносится изменение, номер версии базы данных увеличивается. Выполнение авторитетного восстановления удаленных объектов AD DS предусматривает установку более высокого номера версии, чем текущая реплицируемая версия базы данных AD DS.

Когда только возможно, авторитетные восстановления должны проводиться на сервере глобального каталога, чтобы информация о группах могла быть полностью восстановлена. Если вы сумеете изолировать сервер глобального каталога до того, как он получит репликацию удаления, которое вы пытаетесь восстановить, то сможете восстановить эти объекты без предварительного неавторитетного восстановления. Другими словами, если вы достаточно сноровисты, чтобы успеть отсоединить сетевой кабель от сервера глобального каталога, то избежите необходимости в восстановлении из резервной копии. Чтобы провести авторитетное восстановление перед тем, как изменение будет реплицировано, выполните следующие шаги.

1. Изолируйте сервер, либо отсоединив сетевые кабели, либо введя команду **repadmin /options <имя_сервера> +DISABLE_INBOUND_REPL**.
2. Остановите службы AD DS. Для этого либо выберите пункт Services (Службы) в меню Tools (Сервис) диспетчера серверов, как было описано ранее в этой главе, либо введите команду **net stop ntds** в окне командной строки с повышенными разрешениями.
3. В окне командной строки с повышенными разрешениями введите **ntdsutil** и нажмите <Enter>.
4. В приглашении `ntdsutil` введите **authoritative restore** и нажмите <Enter>.
5. Введите команду, подходящую для типа восстанавливаемого объекта.
   - Чтобы восстановить поддерево наподобие целой организационной единицы, введите **restore subtree <DN>**, где <DN> — полное имя восстанавливаемого объекта. Например, для восстановления организационной единицы HR в домене Bigfirm.com введите **restore object "OU=HR,DC=bigfirm,DC=com"**.
   - Чтобы восстановить одиночный объект, такой как учетная запись пользователя, введите **restore object <DN>**, где <DN> — полное имя восстанавливаемого объекта.
6. Запомните имена любых сгенерированных файлов с расширениями `.txt` или `.ldif`, т.к. они могут использоваться при воссоздании обратных ссылок для восстанавливаемых объектов.
   - Обратные ссылки содержат информацию о членстве в группах.
   - Файлы `.txt` могут применяться при воссоздании членства в группах других доменов для восстановленных учетных записей пользователя с помощью команды `create ldif file from` утилиты `Ntdsutil`, запускаемой в других доменах.
   - Файлы `.ldif` могут использоваться при восстановлении членства в группах локального домена с применением утилиты `Ldifde.exe`.

7. Введите **quit**, чтобы выйти из режима авторитетного восстановления, а затем введите **quit** еще раз, чтобы выйти из `Ntdsutil.exe`. Перезапустите сервер обычным способом.

Выполнение авторитетного восстановления в случае, когда изменения уже были реплицированы, требует предварительного неавторитетного восстановления из резервной копии и затем проведения той же самой последовательности действий для авторитетного восстановления удаленных объектов.

Резюме

Используйте Windows Server Backup для резервного копирования и восстановления компьютера Windows Server 2012 R2. Инструмент Windows Server Backup устанавливается в виде компонента Windows Server 2012 R2 и может применяться для создания разнообразных типов резервных копий с целью защиты серверного компьютера. Полные резервные копии сервера содержат операционную систему, критически важные тома и все данные на сервере, тогда как резервные копии критически важных томов защищают все тома, от которых зависит операционная система, но не обязательно дополнительные данные, хранящиеся на сервере.

> *Контрольный вопрос.* Ваш сервер содержит два жестких диска: на первом находится операционная система, а на втором — пользовательские данные. Как с помощью Windows Server Backup можно защитить операционную систему и пользовательские данные?

Выполните автономную дефрагментацию AD DS. Версия Windows Server 2012 R2 предлагает возможность выполнения автономной дефрагментации и проверки целостности базы данных AD DS без необходимости в перезапуске компьютера и входе в режим DSRM. Вместо этого вы можете остановить AD DS и затем воспользоваться `Ntdsutil.exe` в окне командной строки с повышенными разрешениями для запуска автономной дефрагментации и проверки целостности.

> *Контрольный вопрос.* Вы хотите дефрагментировать базу данных AD DS, но не желаете прекращать работу сервера и перезапускать его в режиме DSRM. Как вы поступите?

Установите корзину Active Directory. Недостаток версии корзины в Windows Server 2008 R2 для части пользователей заключался в том, что ей приходилось управлять полностью с помощью PowerShell. В Windows Server 2012 R2 появилась возможность управления корзиной посредством графического пользовательского интерфейса.

> *Контрольный вопрос.* Вы хотите установить корзину Active Directory, не используя PowerShell. Как это можно сделать?

Создайте и восстановите резервную копию состояния системы для Active Directory. Поскольку контроллеры домена содержат всю информацию базы данных для Active Directory, восстановление вышедшего из строя сервера контроллера домена является чрезвычайно важной задачей. При использовании инструмента Windows Server Backup или утилиты командной строки `Wbadmin.exe` создавайте резервные копии, содержащие, как минимум, состояние системы, чтобы предохранить Active Directory.

> *Контрольный вопрос.* Вы хотите защитить данные Active Directory от возможного полного отказа оборудования серверного компьютера. Какие типы резервного копирования предоставят такую защиту?

Приложение

В конце глав этой книги предлагались упражнения, призванные усовершенствовать навыки и глубже понять материал, изложенный в главах. Временами имеется только одно возможное решение. Однако часто вам удастся задействовать свой опыт и творческий подход и получить решение, которое основано на том, что вы знаете, но позволяет исследовать одну из многочисленных возможностей.

Глава 2. Установка и модернизация до Windows Server 2012 R2

Проведите модернизацию старых серверов. В Microsoft предоставляют несколько вариантов модернизации до версии Windows Server 2012 R2.

Контрольный вопрос. Вы имеете файловый сервер Windows Server 2008 x86. Каким образом его модернизировать до Windows Server 2012 R2?

Решение. Операционная система Windows Server 2012 R2 доступна только как сборка x64. Вам придется подготовить новую машину с установленной операционной системой Windows Server 2012 R2. После этого вы перенесете нужные службы и данные из машины Windows Server 2008 на машину Windows Server 2012 R2.

Сконфигурируйте сервер. ОС Windows Server 2012 R2 позволяет использовать диспетчер серверов и PowerShell для добавления либо удаления ролей, служб ролей и компонентов.

Контрольный вопрос. Вы начали развертывать Windows Server 2012 R2 и планируете автоматизацию как можно большего количества действий для процесса развертывания. Каким инструментом вы будете пользоваться для добавления либо удаления ролей, служб ролей и компонентов?

Решение. Команда `Import-Module Servermanager` добавит следующие командлеты PowerShell. Командлет `Get-WindowsFeature` отображает состояние установки каждой роли, службы роли и компонента. Командлет `Add-WindowsFeature` позволяет установить компонент, а `Remove-WindowsFeature` — удалить компонент. Автоматизировать внесение изменений в конфигурацию можно с помощью сценариев PowerShell.

Постройте небольшую ферму серверов. Установка Windows Server обычно требует ответа на множество вопросов. Это отнимает много времени и отвлекает администраторов от решения других инженерных или проектных задач. Для применения доступны альтернативные приемы.

Контрольный вопрос. Вам поручено построить четыре новых сервера с ОС Windows Server 2012 R2. В вашей организации впервые будет развертываться версия Windows Server 2012 R2. В отделе не хватает персонала из-за отпускного периода. Вы хотите выполнить эту работу быстро и эффективно. Каким образом вы поступите?

Решение. Имея больше времени, можно было бы подготовить сервер с помощью службы развертывания Windows (Windows Deployment Services — WDS). Однако вам нужно работать быстрее. Вы можете загрузить с веб-сайта Microsoft и установить самую последнюю версию пакета автоматической установки Windows (Windows Automated Installation Kit). Вы должны с помощью диспетчера образов систем Windows (Windows System Image Manager — WSIM) подготовить файл ответов по имени `autounattend.xml`, скопировать этот файл на флэш-накопитель USB, вставить DVD-диск с Windows Server 2012 R2 в привод на каждом сервере и загрузить его с этого DVD-диска. Затем понадобится подключить флэш-накопитель USB с файлом ответов; программа установки Windows загрузит этот файл и автоматизирует процесс установки Windows. Вам останется только изменить пароль администратора и войти в систему.

Глава 3. Введение в Server Core

Используйте новую функциональность в Server Core. ОС Windows Server 2012 Server Core — это усеченная версия полной установки. Сокращение объема функционального кода уменьшает площадь атаки и также снижает требования к производительности оборудования. Основным интерфейсом для администрирования является командная строка. В Server Core могут функционировать некоторые, но не все роли, доступные в полной установке.

Контрольный вопрос. Версия Windows Server 2012 Server Core отличается от ее первоначального выпуска в Windows Server 2008. Каковы ключевые отличия, и каким образом это влияет на роли, которые может выполнять сервер?

Решение. Первоначальный выпуск не давал возможности переключаться между версией с графическим пользовательским интерфейсом (GUI) и Server Core. Версия Windows Server 2012 позволяет настроить свой сервер в режиме GUI, а затем просто переключиться на Server Core.

Установите и сконфигурируйте Server Core. Установка Server Core ничем не отличается от полной установки Windows Server 2012. Полная установка предоставляет список начальных задач конфигурирования, таких как присоединение к домену, включение автоматических обновлений и установка компонентов. Для каждой из этих операций предусмотрена соответствующая команда.

Контрольный вопрос. В Server Core имеется специальный сценарий для выполнения ряда общих задач, которые модифицируют реестр. Как называется этот сценарий? Какой параметр может предоставить список дополнительных команд для выполнения многих общих задач конфигурирования?

Решение. Сценарий `SCRegedit.wsf`, находящийся в `c:\windows\system32`, выполняет несколько конфигурационных задач, среди которых включение автоматических обновлений и удаленного рабочего стола. Список дополнительных команд для проведения начального конфигурирования можно получить с помощью параметра `/cli`.

Настройте Server Core для развертывания в офисе филиала. Развертывание в офисе филиала представляет собой один из возможных сценариев внедрения Server Core. На этом сервере можно установить и сконфигурировать роли инфраструктуры Active Directory Domain Services, DNS, DHCP, File Services и Print and Document Services и затем предоставлять их пользователям внутри небольшой офисной среды. Конфигурирование указанных служб можно проводить дистанционно.

Контрольный вопрос. Чтобы сконфигурировать Active Directory Domain Services и DNS, в командной строке запускается мастер установки Active Directory Domain Services Installation Wizard (`DCPromo`). Что необходимо для ввода параметров команды?

Решение. Утилите `DCPromo` требуется файл ответов для установки в системе Server Core. Из-за удаления многих графических возможностей из установки эта утилита не может выполняться в интерактивном режиме. Команда для использования файла ответов выглядит так: `dcpromo /unattend:answerFile.txt`.

Управляйте операционной системой дистанционно. Существуют три способа дистанционного управления Server Core. Доступно администрирование Remote Desktop, но может применяться только командная строка и инструменты с графическим пользовательским интерфейсом, предоставляемые Server Core. Можно подключить оснастки консоли MMC к службам на сервере и управлять ими с помощью стандартных инструментов Windows. Наконец, новая служба Windows Remote Shell позволяет подключаться к серверу для выполнения по одной команде.

Контрольный вопрос. Служба Windows Remote Shell предлагает опцию `quickconfig`. О каких проблемах безопасности должны знать системные администраторы при использовании этой опции? Что можно сделать для решения этих проблем?

Решение. Опция `quickconfig` настраивает службу Windows Remote Shell на прослушивание запросов на TCP-порте 5985 с использованием HTTP. Это означает, что команда и ее результаты будут передаваться в незашифрованном виде. Вдобавок сервер является неаутентифицированным, что может привести к конфигурированию не того сервера, который нужен. Одним из способов решения проблемы является настройка протокола IPSec между сервером и клиентами. Еще один способ предусматривает конфигурирование службы Windows Remote Shell для применения HTTPS с TCP-портом 5986, что обеспечит шифрование передаваемых данных и аутентификацию сервера.

Глава 4. Улучшения организации сетей в Windows Server 2012 R2

Освойте протокол IPv6. Переход с IPv4 на IPv6 определенно не могло произойти в короткие сроки, и проектировщикам IPv6 было очевидно, что в одной инфраструктуре возможно сосуществование и работа вместе обоих протоколов. Проблема в том, что IPv4 и IPv6 не могли естественным образом взаимодействовать друг с другом, и решение на переходный период требовало ликвидации коммуникационных барьеров между этими двумя протоколами.

Контрольный вопрос. Что из перечисленного ниже не является технологией перехода на IPv6?

а. ISATAP

б. DirectAccess

в. 6to4

г. Teredo

Решение. б. DirectAccess не является технологией перехода на IPv6.

Используйте PowerShell для лучшей управляемости сетями. В Windows Server 2012 R2 имеется около 2 500 командлетов PowerShell, среди которых буквально сотни предназначены для просмотра, конфигурирования и мониторинга всех компонентов и служб, связанных с сетями. С помощью этих командлетов вы можете выполнять широкий диапазон задач, начиная с простой настройки IP-адресов и заканчивая более специализированными функциями наподобие конфигурирования Quality of Service и установки параметров виртуализации сетей.

Контрольный вопрос. Какой новый командлет, встроенный в Windows Server 2012 R2, является реальным претендентом на замену традиционной команды `ping`?

Решение. Командлет `Test-NetConnection` встроен в Windows Server 2012 R2 и предоставляет гораздо больше информации, чем традиционная команда `ping`.

Реализуйте средство NIC Teaming. В современном "всегда подключенном" мире очень важно, чтобы сетевые подключения серверов оставались надежными и могли поддерживать безотказную работу в случае выхода из строя какого-либо адаптера. ОС Windows Server 2012 R2 помогает обеспечить такую отказоустойчивость путем использования средства NIC Teaming и сводит на нет необходимость в приобретении какого-либо дополнительного (и потенциально дорогого) оборудования или программного обеспечения.

Контрольный вопрос. Если вы хотите создать объединение NIC с применением PowerShell, то как вы поступите?

Решение. Чтобы создать новое объединение NIC, откройте окно PowerShell, воспользовавшись учетной записью с административными разрешениями, и введите следующую команду (подставив имена объединения и сетевых интерфейсных плат, которые соответствуют имеющейся среде): **`New-NetLbfoTeam Team1 NIC3,NIC4`**.

Изучите новые возможности QoS. Качество обслуживания (Quality of Service — QoS) позволяет администраторам конфигурировать и развертывать политики, которые заранее определяют, какие приложения или службы должны иметь приоритет при выделении полосы пропускания. Администраторы могут определять критически важные интерактивные службы наподобие Voice over IP (VoIP) и производственные (line-of-business — LOB) приложения, которые должны иметь приемлемые уровни и доступную полосу пропускания всякий раз, когда они в этом нуждаются.

Контрольный вопрос. В ранних операционных системах QoS можно было использовать только для установки максимального потребления полосы пропускания, что также было известно как ограничение скорости. Это больше было похоже на решение по регулировке полосы пропускания, а не на систему резервирования полосы пропускания. Каким средством QoS в Windows Server 2012 R2 можно воспользоваться, чтобы решить эту проблему?

Решение. Для решения этой проблемы в QoS версии Windows Server 2012 было включено новое средство под названием Minimum Bandwidth (Минимальная полоса пропускания). Оно предоставляет решение по резервированию полосы пропускания, отсутствовавшее в предшествующих версиях, и позволяет обеспечить для разных типов трафика требуемые ими детализированные конфигурации полосы пропускания.

Управляйте производительностью сети. Понимание методики управления производительностью сетевой среды Windows Server 2012 R2 имеет первостепенное значение для обеспечения оптимального уровня продуктивности организации.

Контрольный вопрос. Какие из перечисленных ниже инструментов можно использовать для управления производительностью сети в Windows Server 2012 R2? (Укажите два инструмента.)

а. `Ipconfig.exe`

б. `Perfmon.exe`

в. `Dfsrmon.exe`

г. Server Performance Advisor

д. `Networkview.exe`

Решение. Инструменты, которыми можно пользоваться для управления пропускной способностью сети в Windows Server 2012 R2, указаны в пунктах б) и г).

Глава 5. Компоненты IP Address Management и DHCP Failover

Реализуйте IPAM. Компонент IPAM — это интегрированный комплект инструментов, предназначенных для сквозного планирования, развертывания, управления и мониторинга инфраструктуры IP-адресов с развитым пользовательским интерфейсом. IPAM автоматически обнаруживает серверы инфраструктуры IP-адресов в сети и позволяет управлять ими из центрального интерфейса.

Контрольный вопрос. С компонентом IPAM связаны специфические предварительные условия, которые должны быть удовлетворены, прежде чем его можно будет развертывать. Каковы требования к Active Directory, о которых вы должны знать?

Решение. Сервер IPAM должен быть членом домена Active Directory; развертывание серверов IPAM, не присоединенных к домену, не поддерживается. Сервер IPAM может функционировать только в границах одиночного леса Active Directory, но внутри этого леса допускается иметь смесь доверенных и недоверенных доменов, которые могут управляться данным сервером IPAM. Кроме того, можно управлять только серверами, присоединенными к домену; любые серверы, не являющиеся членами домена Active Directory, средством IPAM не поддерживаются.

Эффективно используйте компоненты IPAM. Компонент IPAM образован из трех функциональных компонентов, интегрированных друг с другом для обеспечения целостного управления инфраструктурой IP-адресов. Эти три компонента предоставляют функциональность для Multi-Server Management and Monitoring (Многосерверное управление и мониторинг), Address Space Management (Управление адресным пространством) и Network Auditing (Аудит сети).

Контрольный вопрос. Какой компонент IPAM позволяет выполнять одновременное обновление всех серверов DHCP и DNS?

а. Multi-Server Management and Monitoring

б. Address Space Management

в. Network Auditing

Решение. а. Компонент Multi-Server Management and Monitoring (Многосерверное управление и мониторинг) средства IPAM обеспечивает автоматическое обнаружение поддерживающих управление серверов DHCP и DNS, а также предоставляет возможность централизации ресурсов, которые эти серверы обслуживают. Если вы не хотите применять метод автоматического обнаружения, можете по-прежнему добавлять или удалять серверы DHCP и DNS вручную. Результатом действия этого компонента является возможность одновременного обновления всех серверов DHCP и DNS.

Интегрируйте IPAM с System Center 2012. Со всей ориентацией на управление центрами данных и облаком именно здесь в Microsoft инвестировали самые большие средства в усовершенствование IPAM для Windows Server 2012 R2. Раздел Virtualized IP Address Space (Виртуализированное пространство IP-адресов) консоли IPAM упрощает управление пространствами физических и виртуальных адресов посредством нового интеграционного соединения с VMM. Эта интеграция открывает большие возможности по управлению IP-адресами между внутренними и облачными схемами IP-адресации.

Контрольный вопрос. Какие версии Windows Server и VMM должны функционировать, чтобы была доступной интеграция IPAM?

Решение. Чтобы можно было использовать интеграцию IPAM для эффективного управления физическими и виртуальными адресами, на сервере должна функционировать версия Windows Server 2012 R2 с диспетчером виртуальных машин системного центра 2012 R2 (System Center 2012 R2 Virtual Machine Manager).

Управляйте делегированием IPAM. В результате установки серверной роли IPAM автоматически создается несколько локальных групп доступа, которые могут использоваться для предоставления средства контроля доступа на основе ролей (Role-Based Access Control — RBAC) среды IPAM назначенным пользователям и администраторам. В зависимости от типа административных привилегий, которые вы хотите выдать своим пользователям, вам понадобится всего лишь добавить их учетные записи в подходящую группу доступа.

Контрольный вопрос. Существуют пять локальных групп доступа, которые IPAM создает для обеспечения RBAC. Какая группа из приведенного далее списка *не* является одной из них?

а. IPAM Administrators (Администраторы IPAM)

б. IPAM IP Audit Administrators (Администраторы аудита IP-адресов IPAM)

в. IPAM ASM Administrators (Администраторы IPAM ASM)

г. IPAM Advanced Users (Опытные пользователи IPAM)

д. IPAM MSM Administrators (Администраторы IPAM MSM)

е. IPAM Users (Пользователи IPAM)

Решение. г. Группа IPAM Advanced Users *не* является одной из пяти локальных групп доступа, которые IPAM создает для обеспечения RBAC и делегирования доступа.

Освойте DHCP Failover. Преимущество DHCP Failover в том, что теперь нет необходимости в наличии любых дорогостоящих хранилищ, таких как устройства SAN (Storage Area Network — сеть хранения данных), между серверами DHCP. Вместо этого данные об аренде непрерывно реплицируются между серверами. Учитывая, что оба сервера DHCP Failover содержат копию последних назначений IP-адресов и информацию об областях видимости, вы всегда будете иметь возможность защититься от отказа одного из серверов DHCP, не теряя функциональности DHCP.

Контрольный вопрос. Новая функциональность DHCP Failover позволяет конфигурировать два типа отношений обхода отказа. Как называются эти два отношения?

а. Failover clustering (active/active) (Кластеризация с обходом отказа (активный/активный))

б. Hot standby (active/passive) (Горячее резервирование (активный/пассивный))

в. Split-scope (active/passive) (Разделение области (активный/пассивный))

г. Seeded (active/active) (Начальное (активный/активный))

д. Load balance (active/active) ((активный/активный))

Решение. Двумя разными типами отношений DHCP Failover являются б) Hot standby (active/passive) и д) Load balance (active/active); при реализации обхода отказа между серверами вы можете выбрать подходящий вариант из этих двух.

Глава 6. DNS и преобразование имен в Windows Server 2012 R2

Освойте фундаментальные компоненты и процессы DNS. Система DNS опирается на интегрированные серверы, которые управляют иерархической структурой имен. В Интернете эта структура начинается с корневых серверов и затем продолжается серверами доменов верхнего уровня, которые делегируют поддомены другим DNS-серверам. Внутри DNS-сервера имеется база данных записей, которая называется зоной и может реплицироваться между другими DNS-серверами, обеспечивая распределенное преобразование для заданного пространства имен.

Контрольный вопрос. В этой главе обсуждались многие распространенные записи DNS. Записи SRV и MX имеют параметр по имени `priority`. При наличии двух записей SRV для одной службы с параметром `priority`, равным 10 и 20, какая из них будет выбрана первой?

Решение. Параметр `priority` в записях SRV может иметь значение от 0 до 65535. Однако наименьшее значение обладает самым высоким приоритетом. Следовательно, запись с параметром `priority`, имеющим значение 10, будет выбрана первой.

Конфигурируйте DNS для поддержки среды Active Directory. Для поддержки назначенного имени домена служба Active Directory требует доступного пространства имен DNS. В Windows Server 2012 R2 предлагается возможность автоматического создания требуемой структуры DNS посредством процесса поднятия контроллера домена. Зоны DNS могут храниться в базе данных Active Directory, которая обеспечивает для записей DNS репликацию с несколькими хозяевами. С помощью записей SRV и обновлений DDNS контроллеры доменов могут зарегистрировать свои службы в DNS для доступа к ним со стороны клиентов.

Контрольный вопрос. В DNS на контроллерах доменов можно создавать зоны, интегрированные с Active Directory. В какие места внутри базы данных Active Directory помещаются такие зоны? Какую область видимости эти места предоставляют?

Решение. Существуют четыре места, которые можно выбирать при создании новой зоны.

- Раздел домена, доступный для всех контроллеров домена в домене, включая контроллеры домена Windows 2000 Server.
- Раздел каталога приложений домена, доступный для всех контроллеров домена в домене.
- Раздел каталога приложений леса, доступный для всех контроллеров домена в лесе.
- Специальный раздел каталога приложений, доступный для всех контроллеров домена в лесе. Они должны быть включены в репликацию этого раздела, чтобы поддерживать его.

Управляйте и устраняйте неполадки в преобразовании имен DNS для внутренних и внешних имен. Преобразование внутренних и внешних имен полагается на подключаемость между DNS-серверами. Основными методами обеспечения для DNS-серверов возможности отправки между собой запросов являются переадресация и корневые подсказки. Для содействия в устранении проблем и мониторинге конфигурации и производительности DNS доступно несколько инструментов, в числе которых `NsLookup`, PowerShell и `DcDiag`.

Контрольный вопрос. Регистрация записей SRV для контроллеров доменов выполняется службой `netlogon`. Это очень сложная и ответственная задача, чтобы пытаться выполнить ее вручную. Какие тесты можно запустить для проверки, корректно ли зарегистрированы записи SRV внутри домена?

Решение. Утилита `DcDiag` предоставляет тесты для проверки доступности записей SRV внутри указанного домена. Команда `Dcdiag /registerindns` проверяет, может ли контроллер домена вносить обновления в зону домена с использованием обновлений DDNS.

Глава 7. Active Directory в Windows Server 2012

Создайте лес с единственным доменом. Любой сервер Windows Server 2012 может быть повышен до контроллера домена, чтобы создать лес с единственным доменом. На контроллере домена размещен экземпляр Active Directory Domain Services.

Контрольный вопрос. Вы хотите повысить сервер до контроллера домена и создать лес с единственным доменом. Что вы должны делать?

Решение. Установите роль Active Directory Domain Services и затем запустите мастер конфигурирования службы домена Active Directory (Active Directory Domain Services Configuration Wizard). Следуйте указаниям этого мастера по созданию нового леса.

Добавьте в домен второй контроллер домена. Единственный контроллер домена становится одиночной точкой потенциального отказа. Если это произойдет, домен перестанет функционировать. Чтобы такого не случилось, администраторы добавляют в домен второй контроллер домена.

Контрольный вопрос. Вы хотите добавить в свой домен второй контроллер домена. Что вы должны делать?

Решение. Установите роль Active Directory Domain Services и затем запустите мастер конфигурирования службы домена Active Directory (Active Directory Domain Services Configuration Wizard). Следуйте указаниям этого мастера, чтобы добавить второй контроллер домена в существующий домен.

Решите, добавлять ли глобальный каталог. На сервере глобального каталога размещена копия глобального каталога. Сервером глобального каталога может стать любой контроллер домена, но только первый контроллер домена является сервером глобального каталога по умолчанию.

Контрольный вопрос. Вы повышаете второй сервер до контроллера домена в лесе с единственным доменом. Должны ли вы его сделать сервером глобального каталога?

Решение. Да. В лесе с единственным доменом все контроллеры домена должны быть также серверами глобального каталога. Это обеспечивает избыточность в домене без дополнительных накладных расходов.

Создайте учетные записи. Любой домен должен содержать в себе учетные записи пользователей и компьютеров, представляющие пользователей и компьютеров, которые будут получать доступ к домену. Создавать учетные записи пользователей и компьютеров можно несколькими способами.

Контрольный вопрос. Назовите четыре метода для создания учетной записи пользователя. Два из них обладают графическим пользовательским интерфейсом, а другие два являются инструментами командной строки.

Решение. Этими четырьмя методами являются Active Directory Users and Computers, Active Directory Administrative Center, инструмент командной строки `DSAdd` и командлет PowerShell под названием `New-ADUser`.

Создайте детализированные политики паролей. В Windows Server 2012 введена возможность создания нескольких политик паролей внутри одного домена путем использования детализированных политик паролей. Детализированную политику паролей можно применять для назначения разных политик паролей пользователю или группе внутри домена.

Контрольный вопрос. Вы хотите создать детализированную политику паролей для группы администраторов в сети. Как и с помощью каких инструментов вы должны это делать?

Решение. Создайте объект настройки паролей (password-settings object — PSO) с помощью графического пользовательского интерфейса Active Directory Administrative Center. Применять PSO к пользователям или группам можно также с использованием Active Directory Users and Computers.

Изучите функциональный уровень леса Windows Server 2012. Каждый функциональный уровень леса традиционно предлагал новую функциональность для Active Directory. Например, функциональный уровень леса Windows Server 2008 R2 привнес в Active Directory поддержку средства Recycle Bin (Корзина).

Контрольный вопрос. Какое новое средство предлагается в функциональном уровне леса Windows Server 2012?

Решение. Новые средства в функциональном уровне леса Windows Server 2012 отсутствуют.

Модернизируйте свой домен до Windows Server 2012. В текущий момент вы располагаете лесом с единственным доменом Windows Server 2008 и выясняете, каким образом модернизировать этот лес. Вам нужен лес Windows Server 2012.

Контрольный вопрос. Какие методы модернизации или миграции леса подходят лучше всего?

Решение. В зависимости от предпочтений вы можете решить выполнять модернизацию на месте или постепенную миграцию. Миграция с использованием инструмента ADMT, скорее всего, не подойдет.

Глава 8. Создание и управление учетными записями

Управляйте локальными пользователями и группами. Локальные пользователи и группы хранятся на компьютере и не могут применяться для входа в систему или доступа к ресурсам на других компьютерах.

Контрольный вопрос. У вас есть 25 компьютеров с 25 пользователями в сети рабочей группы, другими словами, сеть без Active Directory или домена Windows. Вы устанавливаете два файловых сервера и хотите предоставить только авторизованный доступ к ресурсам на этих файловых серверах. Как вы сделаете это?

Решение. Вам понадобится создать учетные записи для каждого из 25 пользователей. Однако поскольку домен отсутствует, вам придется создать учетные записи и на ПК пользователей, и на каждом из двух серверов. Имя пользователя и пароль должны быть идентичными на ПК пользователей и на двух серверах. Процесс можно ускорить за счет написания сценария, в котором применяется команда `net user`.

Управляйте пользователями и группами в Active Directory. Пользователи и группы могут быть сохранены в Active Directory. Это означает, что администраторы могут создавать единственную копию каждого пользователя и группы, которая хранится в реплицируемой базе данных и может использоваться компьютерами-членами по всему лесу Active Directory. Для управления пользователями и группами в Windows Server 2012 можно применять оснастку Active Directory Users and Computers, командную строку, PowerShell и Active Directory Administrative Center.

Контрольный вопрос. Перечислите типы и области действия групп Active Directory. Для каждого вида группы укажите, когда вы будете его использовать.

Решение. Существуют два типа групп Active Directory.

- *Группа рассылки* используется для коллективного взаимодействия с ее членами через единственный почтовый адрес, который ассоциирован с этой группой.
- *Группа доступа* предназначена главным образом для управления разрешениями, назначенными коллекции пользователей.

Члены группы Active Directory могут быть объектами пользователей или других групп. Различают три области действия групп.

- *Локальная группа домена* предназначена для применения только внутри домена, в котором она была создана. Она может содержать учетные записи пользователей/компьютеров, глобальные группы и универсальные группы из любого домена в лесе, а также локальные группы из того же самого домена.
- Стандартной областью действия при создании группы в Active Directory является *глобальная группа*. Глобальная группа может использоваться компьютерами внутри домена, которые являются его членами, а также членами других доменов в лесе Active Directory. Она может содержать учетные записи пользователей/компьютеров из домена, в котором была создана.

- *Универсальная группа* является третьей и последней областью действия групп. Универсальная группа хранится на контроллерах домена, сконфигурированных в качестве глобального каталога. Универсальная группа реплицируется в домены по всему лесу. В результате появляется возможность не только использовать универсальную группу всеми компьютерами в лесе, но и помещать в нее члены из любого домена внутри леса. Универсальные группы могут содержать учетные записи пользователей и компьютеров, глобальные группы и другие универсальные группы из любого домена в лесе.

Управляйте пользователями и компьютерами в Windows Server 2012. Управлять пользователями и компьютерами можно с применением либо PowerShell, либо нового центра администрирования Active Directory (Active Directory Administrative Center — ADAC). Инструмент ADAC обеспечивает администраторам более быстрое и легкое выполнение ежедневных операций, таких как сброс паролей, разблокирование четных записей пользователей и нахождение объектов в лесе, которым они управляют. Модуль Active Directory для Windows PowerShell предлагает интерфейс командной строки и способ написания сценариев для задач управления Active Directory. Вы можете использовать это для автоматизации повторяющихся задач посредством сценариев или для выполнения сложных и крупных операций, которые требуют больших затрат времени в случае применения консоли администрирования.

Контрольный вопрос. Вы управляете лесом Windows Server 2012 Active Directory в международной корпорации. Руководство анонсировало скорое открытие нового сервисного центра с 5 000 служащих. Благодаря внештатным разработчикам, отдел кадров способен сгенерировать на основе своей базы данных файл с именами новых служащих. Вам необходимо как можно быстрее создать объекты пользователей с минимальными человеческими усилиями. Как вы поступите?

Решение. Вы можете договориться с внутренними разработчиками компании о том, чтобы экспорт данных о новых сотрудниках из системы управления кадрами осуществлялся в виде файла CSV. Строка заголовка внутри этого файла будет описывать записи в последующих строках. Каждая последующая строка будет содержать значения, которые можно было бы использовать в командлете PowerShell под названием `New-ADUser`, например:

```
Name,SamAccountName,GivenName,Surname,DisplayName,
Path,UserPrincipalName,AccountPassword
Rachel Kelly,RKelly,Rachel,Kelly,Rachel Kelly,
"OU=Users,OU=BigFirm,DC=bigfirm,DC=com",RKelly@bigfirm.com,NewPassw0rd
Ulrika Gerhardt,UGerhardt,Ulrika,Gerhardt,Ulrika Gerhardt,
"OU=Users,OU=BigFirm,DC=bigfirm,DC=com",UGerhardt@bigfirm.com,NewPassw0rd
Tomasz Kozlowski, TKozlowski,Tomasz,Kozlowski,Tomaz Kozlowski,
"OU=Users,OU=BigFirm,DC=bigfirm,DC=com",
TKozlowski@bigfirm.com,NewPassw0rd
```

Затем вы запустите команду PowerShell, которая читает каждую строку файла CSV и выполняет командлет `New-ADUser`, применяя значения в каждой строке для создания новых объектов пользователей, например:

```
PS C:\Users\Administrator> Import-CSV c:\users.csv | foreach {New-ADUser -Name
$_.Name -SamAccountName $_.SamAccountName -GivenName $_.GivenName -Surname
$_.Surname -DisplayName $_.DisplayName -Path $_.Path -UserPrincipalName
$_.UserPrincipalName -AccountPassword (ConvertTo-SecureString -AsPlainText
$_.AccountPassword -Force) -Enabled $true -ChangePasswordAtLogon 1}
```

Эта команда быстро прочитает файл и создаст все 5 000 объектов пользователей в выбранной вами организационной единице (или организационных единицах). Вместо того чтобы тратить дни, создавая объекты в консоли, вы потратите буквально минуты на ввод этой команды.

Делегируйте управление группами. Частью мощи Active Directory является возможность делегирования прав по администрированию. Вы можете выдать пользователям либо группам разрешения на управление любой организационной единицей или объектом в домене. Права могут быть ограничены так, что пользователи будут иметь разрешение делать только то, что соответствует их роли в организации.

Контрольный вопрос. Вы являетесь администратором домена в крупной организации. Ваша сеть содержит несколько файловых серверов. Файловые серверы защищены с использованием групп доступа домена. Права на управление этими группами вы делегировали персоналу службы поддержки. Организация полагается на службу поддержки в плане того, что там знают, кто должен иметь доступ по чтению или чтению/записи к общим файловым ресурсам или вообще не иметь его. Были допущены ошибки, а изменения заняли слишком много времени, что привело к утере сотрудниками доступа к критически важной информации. Вы ознакомились с бумажным документом, где владельцы общих файловых ресурсов указали, кто должен иметь доступ к этим ресурсам. Это проверенное, но непопулярное решение, поскольку оно замедляет работу. Вы предложили внедрить решение, которое обеспечит отсутствие простоев и получение доступа к важной информации только авторизованным персоналом.

Решение. Выполните перечисленные ниже шаги.

1. Создайте группы доступа домена с именами `Read Only` (Только чтение) и `Read and Write` (Чтение и запись) для каждого общего файлового ресурса.
2. Предоставьте каждой из этих групп соответствующие разрешения на общих ресурсах.
3. Создайте дополнительную группу доступа домена с именем `Owners` (Владельцы) для каждого общего файлового ресурса.
4. Добавьте в каждую группу `Owners` владельцев информации в общих файловых ресурсах.
5. Отредактируйте свойства групп `Read Only` и `Read and Write`.
6. На вкладке Managed By (Управляется) диалогового окна свойств групп `Read Only` и `Read and Write` добавьте в качестве руководителей соответствующие группы `Owners`.

В результате этого решения каждый, кто является членом группы `Management Owners` для общего ресурса `Management`, сможет управлять членством в группах `Management Read Only` и `Management Read and Write`. Владельцам информации известно, кто должен иметь доступ к их общим файловым ресурсам. Персонал службы

поддержки этими сведениями не располагает. Теперь у владельцев информации есть возможность вносить подходящие изменения в состав групп. Сотрудники IT-отдела больше не вовлечены в процесс. Такой подход упрощает процедуру коммуникаций и позволяет сотрудникам организации получать доступ к информации без задержек.

Обрабатывайте учетные записи пользователей, покидающих организацию. Важно понимать, что Windows отслеживает пользователей, группы и компьютеры посредством идентификаторов SID, а не по их дружественным отображаемым именам. Когда вы удаляете и затем повторно создаете объект, новый объект на самом деле является другим и не сохраняет права и разрешения старого объекта.

Контрольный вопрос. Отдел кадров сообщил вам, что служащий `BKavanagh` немедленно покидает организацию при неблагоприятных обстоятельствах. Сотрудник отдела безопасности информировал вас о наличии риска в плане безопасности. Вас попросили незамедлительно ликвидировать этот риск. Что вам делать? Два часа спустя вам сказали, что отдел кадров предоставил вам неправильное имя служащего. На самом деле имя выглядит как `BCavanagh`. Пользователь `BKavanagh` позвонил в службу поддержки и пожаловался, что он не может выполнять свою работу. Какие действия вы предпримете, чтобы исправить ситуацию?

Решение. Когда вы поначалу отключили пользователя `BKavanagh`, то должны были отключить его учетную запись. Это делает невозможным использование данной учетной записи. Когда вам сообщили о том, что учетная запись оказалась не той, что нужно, вы можете просто снова включить ее, и пользователь `BKavanagh` сможет приступить к работе.

Если у вас есть среда Active Directory в Windows Server 2012, и вы удалили учетную запись `BKavanagh`, то должны восстановить ее из корзины Active Directory.

Если вы удалили учетную запись пользователя, но среды Active Directory в Windows Server 2012 нет, вам придется заново создать ее и добавить этого пользователя во все группы, членом которых он был. Этот процесс займет некоторое время.

Чтобы выполнить требования службы безопасности и отдела кадров, вы должны заблокировать учетную запись `BCavanagh`. Если по истечении определенного времени данный пользователь не вернулся в организацию, можете удалить его учетную запись.

Глава 9. Групповая политика: инструменты и делегирование Active Directory

Усвойте понятие локальных политик и объектов групповой политики. Каждый компьютер Windows, начиная с Windows 2000 Professional и заканчивая современными версиями ОС, имеет локальную групповую политику. В Windows 8 есть много локальных групповых политик, которые можно приспосабливать под разнообразные ситуации нахождения компьютера. Существуют объекты групповой политики, хранящиеся также в Active Directory, которые делают возможным централизованное администрирование компьютеров и пользователей, ассоциированных с доменом.

Контрольный вопрос. Что из перечисленного ниже не является локальной групповой политикой?

- Local Computer Policy (Локальная политика компьютера)
- Administrators (Администраторы)
- Non-Administrators (Не администраторы)
- All Users (Все пользователи)

Решение. All Users не является локальной групповой политикой.

Создавайте объекты GPO. Объекты групповой политики могут и должны создаваться внутри домена Active Directory. Такие дополнительные объекты GPO позволят управлять настройками, программным обеспечением и безопасностью различных пользователей и компьютеров, которые находятся в домене. Объекты GPO обычно связаны с организационными единицами, но также могут связываться с узлом домена и сайтами AD. Объекты GPO создаются внутри AD с использованием консоли управления групповой политикой.

Контрольный вопрос. Создайте новый объект GPO и свяжите его с организационной единицей `HRUsers`.

Решение. Чтобы создать объект GPO и связать его с организационной единицей `HRUsers`, выполните перечисленные ниже шаги.

1. Создайте организационную единицу `HRUsers` внутри домена.
2. В консоли GPMC щелкните правой кнопкой мыши на организационной единице `HRUsers` и выберите пункт Create a GPO in this domain, and link it here (Создать объект GPO в этом домене и связать его).
3. Назначьте новому объекту GPO имя `HRUserSecurity`.

Ищите и устраняйте неполадки в групповых политиках. Иногда настройка объекта GPO или групповая политика отказывает во время применения. Причин может быть много, и для выявления проблем можно использовать множество инструментов. Некоторые инструменты, такие как `rsop.msc`, поддерживают графический пользовательский интерфейс, другие инструменты, подобные `gpresult.exe`, работают в командной строке. Независимо от применяемого инструмента, временами требуются поиск и устранение неполадок в групповой политике.

Контрольный вопрос. Каким инструментом вы воспользуетесь для проверки того, что все настройки во всех объектах GPO, связанных с Active Directory, были применены, даже если никакие изменения в объект GPO или настройку GPO не вносились?

Решение. Инструментом, с помощью которого можно обеспечить применение всех параметров к Active Directory, является команда `gpupdate /force`.

Делегируйте управление, используя организационные единицы. Делегирование является мощным средством в Active Directory, которое позволяет администраторам домена поручать выполнение задач младшим администраторам. Идея заключается в том, что область действия выданного делегирования сужается, предоставляя только ограниченные возможности в отношении Active Directory и содержащихся внутри объектов.

Контрольный вопрос. Установите для организационной единицы `HRUsers` делегирование, предоставив группе доступа `HRHelpDesk` возможность сброса паролей у всех пользователей указанной организационной единицы.

Решение. Выполните следующие шаги.

1. Создайте группу доступа `HRHelpDesk` внутри контейнера `Users`.
2. Создайте организационную единицу `HRUsers` внутри домена.
3. Щелкните правой кнопкой мыши на организационной единице `HRUsers` и выберите в контекстном меню пункт Delegate Control (Делегировать управление), чтобы открыть мастер делегирования управления (Delegation of Control Wizard).
4. Предоставьте разрешения группе `HRHelpDesk`.
5. Предоставьте разрешение на сброс пароля.
6. Завершите мастер делегирования управления.

Используйте расширенное делегирование для ручной установки индивидуальных разрешений. Для любого заданного объекта AD существуют тысячи отдельных разрешений. Расширенное делегирование предоставляет возможность установки любого из этих разрешений, чтобы открыть пользователю или группе доступ к объекту для указанного разрешения. Мастер Delegation of Control Wizard — это удобный инструмент для делегирования распространенных задач, но когда он не обеспечивает требуемый уровень детализации, вы должны выполнять делегирование вручную.

Контрольный вопрос. Для чего из перечисленного ниже делегирование является просто другим обозначением?

- Репликация базы данных AD
- Контроллер домена только для чтения
- Установка разрешений для объектов AD
- Использование групповой политики для установки настроек безопасности

Решение. Делегирование является другим обозначением установки разрешений для объектов AD.

Выясните, какие делегирования были установлены. К сожалению, мастер Delegation of Control Wizard — это инструмент, который может только выдавать разрешения, но не отчет о том, что было установлено. Чтобы выяснить, какие делегирования были установлены, необходимо использовать другие инструменты.

Контрольный вопрос. Назовите инструмент, с помощью которого можно просмотреть установленные делегирования.

Решение. Для просмотра детальных настроек делегирования используется утилита командной строки `dsacls`, входящая в состав Windows Server 2012 R2.

Глава 10. Службы федерации Active Directory

Установите на сервере роль AD FS. Установка роли AD FS на сервере является одним из первых шагов при реализации инфраструктуры AD FS. Установка и использование AD FS в Windows Server 2012 R2 теперь осуществляется как никогда просто.

Роль AD FS предоставляет доступ SSO внутри корпоративной сети, к партнерской организации, а также к веб-сайтам и приложениям, находящимся в Интернете.

Контрольный вопрос. Как вы будете устанавливать роль AD FS на сервере?

Решение. Установите роли и компоненты AD FS с помощью диспетчера серверов.

Сконфигурируйте первый сервер федерации внутри фермы серверов. Сервер федерации выступает как часть службы федерации и может выдавать, управлять и проверять запросы для маркеров безопасности, а также управлять удостоверениями. Несколько серверов федерации предлагают самую востребованную функциональность вроде высокой готовности и балансировки сетевой нагрузки в крупной инфраструктуре AD FS. Для обеспечения доступа SSO пользователям между вашей и партнерской организациями серверы федерации должны быть развернуты в обеих организациях.

Контрольный вопрос. Каким образом вы создадите первый сервер федерации внутри фермы таких серверов?

Решение. Находясь в оснастке AD FS Management (Управление AD FS), запустите мастер конфигурации сервера AD FS (AD FS Server Configuration Wizard) и следуйте его указаниям.

Настройте мониторинг производительности AD FS. Службы AD FS включают собственные счетчики производительности, которые помогают проводить мониторинг производительности на машинах серверов федерации и прокси-серверов федерации. Это небольшое и удобное дополнение, позволяющее упростить управление AD FS. Генерируемые отчеты предоставляют специфичные к AD FS детали, которые показывают, насколько хорошо эти службы функционирует в среде. Мониторинг производительности является важной частью планирования возможного расширения и масштабируемости. Высокие показатели утилизации могут означать необходимость в развертывании еще одного сервера федерации для более эффективной балансировки нагрузки.

Контрольный вопрос. Как вы собираетесь проводить мониторинг производительности своей инфраструктуры AD FS?

Решение. В мониторе производительности создайте новую группу сборщиков данных AD FS.

Глава 11. Введение в общее хранилище и кластеризацию

Используйте доступные опции хранения для кластеризации. С выпуском Windows Server 2012 R2 многие опции хранения стали доступными для решений кластеризации и высокой готовности.

Контрольный вопрос. Вы хотите построить решение JBOD и нуждаетесь в определении самого эффективного типа дисковой емкости. Для обхода отказа не играет особой роли пространство и скорость. На какую технологию вы должны обратить внимание?

Решение. Вы должны построить пространство хранения с виртуальным диском простого типа, который предназначен для увеличения пропускной способности и доведения до максимума емкости. Максимизируйте диски и доступ ним, чтобы сделать свое решение быстрым и эффективным.

Используйте кворумы для помощи в кластеризации. Кворум представляет собой минимальное количество членов, которое должно присутствовать на собрании или заседании, прежде чем оно законно может быть продолжено. Это определение остается справедливым и в случае применения термина "кворум" в отношении кластера.

Контрольный вопрос. Вы решили развернуть кластер с нечетным числом узлов, равным 5, и хотите использовать один узел в качестве свидетеля в форме открытого файлового ресурса. После того, как кластер запущен и функционирует, вы размещаете приложение. Но после установки приложения возникает серьезная утечка памяти, в результате чего работа серверов начинает стопориться и впоследствии вовсе прекращается. Сколько узлов утратят работоспособность до того, как кластер перейдет полностью в отключенное состояние?

Решение. Поскольку имеется четное число узлов кворума и запасной узел в качестве свидетеля, кластер будет оставаться в онлайновом режиме, пока самый последний узел не окажется на грани прекращения работы. Но при надлежащем мониторинге и оповещении вы не позволили бы зайти процессу настолько далеко, ведь так? Вполне возможно не позволили бы, однако преимущество узла-свидетеля заключается в том, что вы можете поддерживать свое приложение в рабочем состоянии на то время, пока возвращаете остальные серверы в онлайновый режим или направляете их на другую версию приложения.

Постройте хостовые и гостевые кластеры. Кластеризация — это сочетание программного обеспечения и оборудования, и она может охватывать физические серверы или виртуальные машины. В Windows Server 2012 R2 имеются встроенные компоненты и инструменты для развертывания кластеров, включая удобный мастер предварительных условий, который позволяет проверить, что для успешной настройки кластера присутствуют все компоненты и конфигурации.

Контрольный вопрос. При планировании хостовых и гостевых кластеров, исключая роль Hyper-V, о каком отличии между их настройкой следует знать?

Решение. Никаких отличий нет; когда вы приступаете к планированию оборудования и сетей, требования на стороне виртуальных машин и на стороне хоста процесса кластеризации совершенно одинаковы. Процесс прост и выполняется легко.

Глава 12. Хранилище Windows 2012 R2: пространства хранения, возможности SAN и улучшенные инструменты

Создайте пул хранения на виртуальном диске. Хранилище является постоянно растущим требованием при бизнес-деятельности. Если для удовлетворения этой потребности вы постоянно приобретали решения SAN, то знаете, что они отличаются высокой стоимостью. Кроме того, очень трудно предсказать, что вам может понадобиться

в течение года. Как управлять хранилищем, чтобы получить от него максимальную отдачу и удовлетворить будущие потребности в отношении хранения?

Контрольный вопрос. Создайте в испытательной среде пул хранения с тремя дисками, используя графический пользовательский интерфейс. Создайте виртуальный диск с размером в три раза больше общей полезной емкости диска. Сформатируйте его и подготовьте к работе.

Решение. В узле File and Storage Services (Службы файлов и хранилища) диспетчера серверов щелкните на папке Volumes⇨Disks (Тома⇨Диски). Щелкните правой кнопкой мыши на пуле Primordial (Первичный) и выберите в контекстном меню пункт New Storage Pool (Создать пул хранения). Введите имя для пула и затем выберите три физических диска (запомните объем каждого из них и сложите эти величины). Выберите свой пул хранения и создайте из него новый виртуальный диск. Назначьте ему описательное имя и выберите Parity (Контроль по четности) для компоновки и Thin (Тонкая) для типа настройки. В качестве размера используйте вычисленный совокупный объем дисковой памяти, умноженный на три. Создайте на этом виртуальном диске том и скопируйте в него несколько файлов.

Создайте дополнительное хранилище на виртуальном диске. Обычным явлением на современных предприятиях является запросы в последнюю минуту на настройку приложений, которые требуют хранилища большого объема. Часто хранилище, доступное локально на сервере, недостаточно велико, чтобы удовлетворить потребности в хранении. Как получить дополнительную емкость для хранения на сервере, не добавляя локальное хранилище?

Контрольный вопрос. Разверните в испытательной среде цель iSCSI, создайте виртуальный диск и затем подключите свой сервер к вновь созданному хранилищу.

Решение. В Windows Server 2012/2012 R2 было введено множество новых командлетов, которые помогут сконфигурировать цель iSCSI и клиентское программное обеспечение. Ниже описаны действия по конфигурированию этого решения посредством PowerShell.

1. В окне PowerShell на сервере, который вы выбрали в качестве сервера цели iSCSI, запустите следующий командлет:

```
Add-windowsfeature FS-iSCSITarget-Server -IncludeManagementTools
```

2. Создайте новую цель iSCSI следующим образом:

```
New-IscsiServerTarget -TargetName TestTarget01
-InitiatorID iqn.1991-05.com.microsoft:server01.contoso.com
```

(Замените имя `iqn` (определенное имя iSCSI) именем вашего удаленного сервера.)

3. Добавьте новый виртуальный диск с помощью следующего командлета:

```
New-IscsiVirtualDisk -path e:\newdisk.vhdx -SizeBytes 20GB
```

4. Добавьте диск к ранее созданной цели iSCSI, как показано здесь:

```
Add-IscsiVirtualDiskTargetMapping -TargetName TestTarget01
-path e:\newdisk.vhdx
```

5. На удаленном сервере, где необходима дополнительная дисковая память, в окне PowerShell с повышенными разрешениями запустите следующую команду:

```
Set-Service -Name msiscsi -StartupType Automatic
Start-Service msiscsi
```

6. Введите:

```
New-iscsitargetportal -targetportaladdress TestTarget01
```

7. Затем введите:

```
Get-IscsiTarget | Connect-IscsiTarget
```

8. В диспетчере дисков проверьте наличие только что добавленных дисков, после чего инициализируйте их и переведите в онлайновый режим.

Используйте технологии дедупликации для сокращения размера файлов. Одной из причин роста объемов данных в современных средах является доступность хранилища, но рано или поздно хранилище становится проблемой. Высокий процент этих файлов содержит большую долю идентичных шаблонов данных, но применение технологий дедупликации может значительно сократить объем требуемого дискового пространства и улучшить общие показатели использования на месте.

Контрольный вопрос. Скопируйте в испытательной среде файл ISO несколько раз в разные места и повторите это для документов Office, которые находятся не на системном томе. Включите дедупликацию на диске данных и добавьте исключение для важного общего ресурса в среде.

Решение. Дедупликацией в Windows Server 2012 R2 можно управлять через PowerShell. Ниже приведены действия по работе с дедупликацией, демонстрирующие применение ряда командлетов.

1. Включите дедупликацию посредством PowerShell:

```
Enable-DeDupVolume -Volume E:
```

Здесь `E:` — это том, на котором вы пытаетесь включить дедупликацию.

2. Исключите папку с помощью PowerShell:

```
Set-DedupVolume -Volume E: -ExcludeFolder E:\shares
```

3. Проверьте всю информацию:

```
Get-DeDupVolume -Volume E: | fl *
```

4. Установите поле возраста файла в `0`, чтобы все файлы сразу же рассматривались как кандидаты на дедупликацию:

```
Set-DedupVolume -Volume E: -MinimumFileAgeDays 0
```

5. Запустите задание оптимизации:

```
Start-Dedupjob -Type Optimization -Volume E:
```

6. Проверьте, удалось ли сэкономить дисковое пространство:

```
Get-DeDupStatus -Volume E:
```

Глава 13. Файлы, папки и базовые общие ресурсы

Установите дополнительные службы роли File and Storage Services на сервере. Роль File and Storage Services (Службы файлов и хранилища) включает службы, предназначенные для оптимизации обслуживания файлов на сервере. Важным добавлением является роль File Server Resource Manager (Диспетчер ресурсов файлового сервера), которая может применяться для управления квотами, добавления фильтров блокировки файлов и генерации всесторонних отчетов.

Контрольный вопрос. Как добавить роль FSRM на сервер?

Решение. Установите службу роли File Server Resource Manager с использованием диспетчера серверов.

Комбинируйте разрешения общего доступа и NTFS. Когда включается совместное использование папки на диске NTFS, с ней связаны разрешения общего доступа и разрешения NTFS. Важно понимать, каким образом эти разрешения взаимодействуют друг с другом, чтобы пользователь мог получить подходящее разрешение.

Контрольный вопрос. Мария состоит в группах `G_HR` и `G_HRManagers`. Для папки `Policies` на сервере создан общий ресурс по имени `Policies` со следующими разрешениями:

- разрешения NTFS: Read для `G_HR`, Full Control для `G_HR_Managers`;
- разрешения общего доступа: Read для `G_HR`, Change для `G_HR`.

Какое разрешение получит Мария при доступе к этому общему ресурсу? Какое разрешение ей будет предоставлено при доступе к этой папке непосредственно на сервере?

Решение. Разрешением Марии при доступе к этому общему ресурсу является Change (Изменение). Определить результат комбинирования разрешений NTFS и разрешений на общем ресурсе можно за три шага.

- *Определение совокупных разрешений NTFS.* У Марии есть разрешения Read (Чтение) и Full Control (Полный доступ), поэтому совокупным разрешением NTFS является Full Control.
- *Определение совокупных разрешений на общем ресурсе.* У Марии есть разрешения Read и Change, поэтому ее совокупным разрешением на общем ресурсе является Change.
- *Определение, какое из двух совокупных разрешений обеспечивает минимальный доступ (или является наиболее ограничивающим).* Разрешение Change является более ограничивающим, чем Full Control.

Если к папке производится доступ напрямую, то разрешения на общем ресурсе не применяются. Таким образом, Мария будет иметь разрешение Full Control.

Внедрите BitLocker Drive Encryption. Средство BitLocker Drive Encryption (Шифрование диска BitLocker) позволяет шифровать целый диск. Если кто-то, кто не должен иметь доступа к данным, получит этот диск, шифрование предотвратит доступ к данным.

Контрольный вопрос. Каковы требования к оборудованию для средства BitLocker Drive Encryption, и что должно быть сделано, чтобы операционная система использовала BitLocker?

Решение. Для BitLocker требуется криптопроцессор Trusted Platform Module 1.2, который является аппаратным компонентом и обычно находится на материнской плате. Средство BitLocker можно использовать без TPM, применяя либо пароль, либо смарт-карту и PIN-код. Прежде чем можно будет пользоваться средством BitLocker, его необходимо добавить как компонент в диспетчере серверов.

Глава 14. Создание и управление общими папками

Добавьте роль File and Storage Services к своему серверу. Прежде чем вы сможете создавать и пользоваться DFS или NFS, открывать общий доступ к файлам и папкам или выполнять другие функции, связанные с файлами, внутри домена Windows Server 2012, вы должны установить дополнительные роли File and Storage Services.

Контрольный вопрос. Запустите диспетчер серверов и добавьте серверные роли DFS и NFS.

Решение. Выполните следующие шаги.

1. Откройте диспетчер серверов и выберите пункт меню Tools⇨Add Roles and Features (Сервис⇨Добавить роли и компоненты).
2. В мастере добавления ролей и компонентов (Add Roles and Features Wizard) доберитесь до экрана с ролями и компонентами, которые вы хотите установить, и щелкните на кнопке Install (Установить).
3. После завершения работы мастера возвратитесь в окно диспетчера серверов и щелкните в меню Manage (Управление); вы должны увидеть дополнительные установленные роли и компоненты.

Если вы сделали все корректно, то сервер покажет, что роли DFS и NFS установлены.

Добавьте общую папку NFS. После того, как роли File and Storage Services успешно добавлены, вы можете открывать общий доступ к папкам, как это делалось для папки `APPS` в этой главе.

Контрольный вопрос. Создайте общую папку по имени `APPS` на своем сервере Windows Server 2012 R2; по завершении мастер должен отобразить успешно созданный общий ресурс.

Решение. После настройки разрешений для общего ресурса щелкните на кнопке Next (Далее), чтобы перейти на финальный экран мастера создания общей папки (Create A Shared Folder Wizard), на котором отображаются результаты и предоставляется возможность запустить этот мастер снова для создания еще одной общей папки.

1. Запустите консоль Computer Management (Управление компьютером) из программной группы Administrative Tools (Администрирование) и выберите в меню Actions (Действия) пункт New Share (Новый общий ресурс).
2. Следуйте указаниям мастера и перейдите к папке, для которой вы хотите открыть общий доступ. Щелкните на кнопке Next (Далее) и установите разрешения, необходимые для этой общей папки. Щелкните на кнопке Finish (Готово).

Добавьте корень DFS. Если ваша организация располагает большим количеством файловых серверов, созданных на протяжении длительного времени, у вас могут быть пользователи, которые не знают, где находятся те или иные файлы. Вы можете упростить процесс поиска и работы с множеством файловых серверов, создав корень DFS и объединив существующие файловые серверы в общие пространства имен.

Контрольный вопрос. Создайте новое пространство имен под названием `MYFIRSTNS` на своем сервере Windows Server 2012 R2; по завершении мастер должен отобразить успешно созданное пространство имен `MYFIRSTNS`.

Решение. В меню Action (Действие) внутри окна DFS Management (Управление DFS) выберите пункт New Namespace (Создать пространство имен). Запустится мастер создания пространства имен (New Namespace Wizard). Далее выполните следующие шаги.

1. В окне диспетчера серверов выберите пункт меню Tools⇨DFS Management (Сервис⇨Управление DFS).
2. В области Actions (Действия) окна DFS Management щелкните на пункте New Replication Group (Создать группу репликации).
3. На первом экране мастера создания группы репликации (New Replication Group Wizard) выберите тип группы. Введите имя группы репликации (`MYFIRSTNS`), любое ее описание и щелкните на кнопке Next (Далее).
4. Добавьте серверы и щелкните на кнопке Next.
5. Выберите топологию и щелкните на кнопке Next.
6. Добавьте членов сервера концентратора и щелкните на кнопке Next.
7. Выберите расписание группы репликации и щелкните на кнопке Next.
8. Укажите, какой сервер является главным членом, и щелкните на кнопке Next.
9. Добавьте папки для репликации и щелкните на кнопке Next.
10. Просмотрите все настройки и щелкните на кнопке Finish (Готово).

Глава 15. Динамическое управление доступом: общие файлы

Защищайте свои данные, используя условия. Изучите способы защиты своих данных, не прибегая к членству в сотнях групп. Имея эти знания, вы сможете понять строительные блоки динамического управления доступом.

Контрольный вопрос. Воспользовавшись примерами, рассмотренными в начале этой главы, создайте в испытательной среде новый общий ресурс по имени `Projects` и защитите его так, чтобы доступ к нему имел только персонал из отделов `Engineering` и `IT`. Протестируйте результат. Помните, как это делать?

Решение. Используя диалоговое окно Advanced Security Settings (Расширенные настройки безопасности) для этого общего ресурса, добавьте условие для участника безопасности Authenticated Users (Аутентифицированные пользователи), которое выбирает группу `IT` или `Engineering`. Поля, которые понадобится изменить, показаны на рис. 15.5.

Создайте новый тип утверждения и свойство ресурса. По мере того, как вы отойдете от применения групп и раздутых билетов Kerberos, вам необходимо понять, как обеспечить возможность доступа к своим данным только соответствующим людям. Использование типов утверждений и свойств ресурсов позволяет защищать данные с помощью новых элементов.

Контрольный вопрос. Как обеспечить возможность доступа к данным, находящимся на ваших общих ресурсах, только сотрудникам из Ирландии? Что нужно сделать для того, чтобы можно было применять название страны в качестве маркера авторизации?

Решение. С помощью инструментов конфигурирования динамического управления доступом в окне Active Directory Administrative Center (Административный центр Active Directory) создайте новый тип утверждения, основанный на атрибуте Country в Active Directory, и добавьте разные значения, включая Ирландию. После этого создайте новое ссылочное свойство ресурса, которое должно быть основано на только что сконфигурированном типе утверждения.

Защищайте сотни серверов. Динамическое управление доступом (Dynamic Access Control) — это мощный инструмент для защиты данных, и когда серверов очень много, необходимо сделать внедрение этой технологии внутри организации простым и обеспечивающим максимальные преимущества.

Контрольный вопрос. Вам требуется защитить все данные на всех файловых серверах. Как изначально защитить данные так, чтобы полный доступ ко всем общим ресурсам был лишь у сотрудников IT-отдела, а персонал из бухгалтерского и конструкторского отделов имел доступ только для чтения?

Решение. Прежде всего, понадобится создать центральные правила доступа, которые будут содержать разрешения для защиты ваших данных. Затем необходимо добавить аутентифицированных пользователей и установить разрешения в Read (Чтение) и Read & Execute (Чтение и выполнение). Далее нужно модифицировать условие для пользователей из бухгалтерского (`Accounts`) и конструкторского (`Engineering`) отделов. Наконец, снова добавьте аутенти-

фицированных пользователей, а также установите разрешения в Full Control (Полный доступ) и добавьте условие для пользователей из отдела IT.

Создайте центральную политику доступа и добавьте в нее центральное правило доступа. По завершении создайте новый объект GPO и добавьте к нему новую центральную политику доступа. Примените этот объект GPO к подходящей организационной единице, чтобы обеспечить ее применение к требуемым файловым серверам.

При необходимости запустите команду `gpupdate /force` на соответствующих файловых серверах, а затем на общем ресурсе, к которому требуется применить центральную политику доступа.

Классифицируйте и защищайте данные, не зная, чем в действительности они являются. Представьте себе огромный массив файловых серверов с миллионами файлов. Вам известно, что в организации не практиковалось классифицировать документы должным образом при их создании. Знание того, как подойти к решению этой проблемы и правильно классифицировать и защищать такие данные, является первостепенным для любой организации.

Контрольный вопрос. На ваших файловых серверах находятся документы, которые содержат конфиденциальную информацию, в том числе номера кредитных карт и данные платежных ведомостей. Как автоматически защитить эти данные и обеспечить возможность доступа к ним только сотрудникам из бухгалтерии и отдела кадров?

Решение. Первым делом, создайте правила классификации; правила кредитных карт должны использовать регулярные выражения для обнаружения шаблонов номеров кредитных карт. Следующий набор правил должен обнаруживать строки, имеющие отношение к платежной ведомости (например, месячная заработная плата). Сконфигурируйте параметры в диспетчере ресурсов файлового сервера (File Server Resource Manager) на запуск по расписанию, чтобы они задним числом применились ко всему серверу. Наконец, создайте новое правило доступа и политику, которые будут нацелены на ресурсы, классифицированные по отделам, и защитите их с использованием условного доступа к отделам бухгалтерии (`Accounts`) и кадров (`HR`).

Глава 16. Общий доступ к принтерам в сетях Windows Server 2012 R2

Добавьте роль Print and Document Services. Серверы Windows Server 2012 R2 могут быть сконфигурированы, чтобы функционировать в качестве серверов печати. Одним из первых шагов, которые вы должны предпринять, является добавление роли Print and Document Services (Службы печати и документов). Шаги по добавлению этой роли в полную версию Windows Server 2012 R2 и версию Server Core отличаются.

Контрольный вопрос. Каким инструментом вы будете пользоваться для добавления роли Print and Document Services на сервер с установленной полной версией Windows Server 2012 R2? Какой инструмент вы будете применять, чтобы добавить роль Print and Document Services на сервер с установленной версией Server Core?

Решение. Используйте диспетчер серверов для добавления роли Print and Document Services к полной установке Windows Server 2012 R2. Применяйте утилиту командной строки PowerShell для добавления роли Print and Document Services к установке Server Core сервера Windows Server 2012 R2. Действительная команда выглядит следующим образом:

```
add-WindowsFeature Print-Service
```

Управляйте принтерами с помощью консоли Print Management. После добавления на сервер роли Print and Documents Services вы можете использовать консоль Print Management (Управление печатью) для управления другими серверами печати, принтерами и драйверами печати.

Контрольный вопрос. Ваша компания приобрела новое устройство печати, и вы хотите, чтобы оно было размещено на сервере, сконфигурированном как сервер печати. Как вы будете добавлять принтер к серверу печати?

Решение. Добавлять принтеры можно посредством консоли Print Management. Щелкните правой кнопкой мыши на узле принтера внутри желаемого сервера и выберите в контекстном меню пункт Add Printer (Добавить принтер), чтобы запустить мастер установки сетевого принтера (Network Printer Installation Wizard).

Управляйте свойствами сервера печати. Папка спулера может иногда занимать значительный объем пространства на диске `C:`, приводя в результате к нехватке свободного пространства и соперничеству за ввод-вывод с операционной системой. По этой причине папку спулера часто переносят на другой физический диск.

Контрольный вопрос. Вы хотите перенести папку спулера в другое место. Как это можно сделать?

Решение. Откройте консоль Print Management и перейдите к нужному серверу. Щелкните правой кнопкой мыши на имени сервера и выберите в контекстном меню пункт Properties (Свойства). На вкладке Advanced (Дополнительно) открывшегося диалогового окна измените местоположение папки спулера. Любые документы, которые содержались в папке спулера, будут утеряны, поэтому вы должны позаботиться о том, чтобы при выполнении операции никто из пользователей не запускал печать на принтерах, размещенных на данном сервере.

Управляйте свойствами принтера. Принтеры могут быть добавлены в Active Directory, чтобы их было легко находить с помощью поиска в Active Directory. Сначала к принтерам должен быть открыт общий доступ, но при этом по умолчанию они не публикуются в Active Directory.

Контрольный вопрос. Вы хотите, чтобы пользователи имели возможность легко находить общий принтер. Что вы должны предпринять для того, чтобы общий принтер мог быть найден посредством поиска в Active Directory?

Решение. Откройте консоль Print Management и перейдите к нужному принтеру. Щелкните правой кнопкой мыши на этом принтере и выберите в контекстном меню пункт List in Directory (Перечислить в каталоге) или перейдите на вкладку Sharing (Общий доступ) в диалоговом окне свойств данного принтера и отметьте флажок List in the directory (Перечислить в каталоге).

Глава 17. Дистанционное администрирование сервера

Сконфигурируйте серверы Windows Server 2012 R2 для дистанционного администрирования. Прежде чем администраторы смогут подключаться дистанционно, серверы должны быть сконфигурированы таким образом, чтобы обеспечить возможность дистанционного администрирования.

Контрольный вопрос. Сконфигурируйте сервер так, чтобы могли дистанционно подключаться клиенты, у которых выполняется RDC версии 6.0 или выше.

Решение. Щелкните на кнопке Start (Пуск), щелкните правой кнопкой мыши на значке Computer (Компьютера) и выберите в контекстном меню пункт Properties (Свойства). Щелкните на Remote Settings (Удаленные параметры). Отметьте флажок Allow connections only from computers running Remote Desktop with Network Level Authentication (Recommended) (Разрешить подключения только от компьютеров с удаленными рабочими столами с аутентификацией сетевого уровня (рекомендуется)). Щелкните на кнопке OK.

Дистанционно подключайтесь к серверам Windows Server 2012 R2 с помощью Remote Desktop Connection. Вы можете дистанционно подключаться к серверам для выполнения практически любой административной работы. Серверы зачастую находятся в надежно защищенном серверном помещении, которое охлаждается для обеспечения бесперебойной работы электронного оборудования. Таким помещением может быть специальная комната; это помещение может находиться в другом здании или даже в отдаленном географическом пункте. Однако в любом случае серверы можно дистанционно администрировать с помощью либо RDC, либо Remote Desktops.

Контрольный вопрос. Подключитесь к какому-то серверу с помощью RDC. Позаботьтесь о том, чтобы при подключении к удаленному серверу обеспечивался доступ к вашим локальным дискам.

Решение. Запустите RDC, выбрав в меню Start (Пуск) пункт All Programs⇨Accessories⇨Remote Desktop Connection (Все программы⇨Стандартные⇨Подключение к удаленному рабочему столу). В качестве альтернативы можете ввести `mstsc` в командной строке или в поле Run (Выполнить). В текстовом поле Computer (Компьютер) введите имя удаленного сервера. Щелкните на кнопке Options (Опции). Перейдите на вкладку Local Resources (Локальные ресурсы). Щелкните на кнопке More (Дополнительно) и отметьте флажок Drives (Диски).

Дистанционно подключайтесь к серверам Windows Server 2012 R2 с помощью файла Remote Desktop Protocol. Если вы регулярно подключаетесь к удаленному серверу с помощью RDC, то можете сконфигурировать файл RDP, который можно заранее настроить с учетом потребностей в отношении этого сервера. В файле RDP будут храниться все настройки, которые вы сконфигурировали для этого подключения.

Контрольный вопрос. Создайте файл RDP, который можно применять для подключения к серверу по имени `Server1`. Сконфигурируйте этот файл так, чтобы при подключении автоматически запускался диспетчер серверов.

Решение. Запустите RDC, выбрав в меню Start (Пуск) пункт All Programs⇨Accessories⇨Remote Desktop Connection (Все программы⇨Стандартные⇨Подключение к удаленному рабочему столу). Щелкните на кнопке Options (Опции) и перейдите на вкладку Programs (Программы). Отметьте флажок Start the Following Program on Connection () и введите в расположенном ниже текстовом поле `ServerManager.msc`. Перейдите на вкладку General (Общие) и введите `Server1` в текстовом поле Computer (Компьютер). Щелкните на кнопке Save As (Сохранить как) и сохраните файл.

Сконфигурируйте сервер для получения удаленной помощи. Если в состав вашей среды входят удаленные площадки, где младшим администраторам время от времени требуется помощь, вы можете использовать Remote Assistance для получения доступа к их сеансу и демонстрации соответствующих процедур.

Контрольный вопрос. Сконфигурируйте сервер для Remote Assistance.

Решение. Откройте диспетчер серверов, на вкладке Dashboard (Управляющая панель) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты) и добавьте компонент Remote Assistance (Дистанционный помощник). После завершения работы мастера удостоверьтесь, что дистанционный помощник включен. Щелкните на кнопке Start (Пуск), щелкните правой кнопкой мыши на значке Computer (Компьютер), выберите в контекстном меню пункт Properties (Свойства) и щелкните на кнопке Remote Settings (Удаленные параметры). Проверьте, отмечен ли флажок Remote Assistance (Дистанционный помощник).

Установите инструменты дистанционного администрирования сервера. Инструменты Remote Server Administration Tools (RSAT) включают оснастки и инструменты командной строки, применяемые для управления серверами Windows Server 2003, Windows Server 2008 и Windows Server 2012 из настольных компьютеров, которые функционируют под управлением Windows Vista, Windows 7 или Windows 8.

Контрольный вопрос. Получите и установите RSAT в системе Windows Vista, Windows 7 или Windows 8.

Решение. Получите RSAT, перейдя на сайт загрузок Microsoft по ссылке `www.Microsoft.com/downloads` и введя `RSAT`. Установите RSAT, дважды щелкнув на имени загруженного файла и следуя указаниям мастера установки. Включите инструменты RSAT, добавив компонент Remote Server Administration Tools в окне Turn Windows Features On or Off (Включение или отключение компонентов Windows), которое доступно через панель управления.

Глава 18. Подключение клиентов Windows и Mac

Проверьте конфигурацию своей сети. Протокол DHCP предоставляет централизованные конфигурации IP-адресов, и все клиенты Windows понимают DHCP, не требуя установки дополнительных компонентов.

Контрольный вопрос. Вам нужно проверить, что клиентская машина получила правильную конфигурацию IP-адресов через DHCP для сети, в которой вы работаете. Какая из перечисленных ниже команд возвратит нужные результаты?

- `ipconfig /all`
- `ipconfig /refresh`
- `msconfig /show`
- `msconfig`

Решение. Команда `ipconfig /all` возвращает информацию о конфигурации подключения по локальной сети, в том числе:

- IP-адрес;
- IP-адреса DNS-серверов;
- IP-адрес DHCP-сервера;
- суффикс домена.

Присоедините клиентский компьютер к домену. Присоединение к домену Active Directory является одной из важнейших задач для рабочих станций, поскольку это обеспечивает централизованное управление из группы `Domain Admins` внутри домена. Групповая политика является централизованной, можно обеспечить защиту, и даже программным обеспечением можно управлять централизованным образом.

Контрольный вопрос. Является ли следующее утверждение правильным? Присоединить компьютер к домену Active Directory можно лишь в случае, если выполняющий это действие пользователь является администратором данного домена.

Решение. Это неправильное утверждение. Пользователи домена также могут добавлять компьютеры в домен, но не более 10 раз. Кроме того, пользователям может быть делегировано право добавления компьютеров в домен.

Измените пароли пользователей. По умолчанию Windows Active Directory обеспечивает 42-дневный максимальный возраст пароля. За 14 дней до истечения этого срока начинают ежедневно поступать напоминания о необходимости изменения пароля. Этот 42-дневный максимум предусмотрен с целью обеспечения определенного уровня безопасности для производственной среды, не позволяющий паролям устаревать.

Контрольный вопрос. Кого-то из пользователей одолела паранойя, поэтому он желает изменить пароль своей учетной записи прямо сейчас. Он не знает, как это сделать, и обращается в службу технической поддержки. Компьютер пользователя функционирует под управлением Windows 7. Что вы посоветуете данному пользователю?

Решение. Посоветуйте этому пользователю нажать комбинацию клавиш <Ctrl+Alt+Del> и щелкнуть на ссылке Change a password (Сменить пароль). Ему понадобится ввести старый пароль и новый пароль, после чего щелкнуть на кнопке с изображением стрелки вправо.

Подключитесь к сетевым ресурсам. Вот типичный сценарий: пользователь желает подключиться к такому принтеру в домене, который выполняет двустороннюю печать, а также сшивает документы. Но пользователю не известно, где в компании установлены такие принтеры. Пользователь обращается в службу технической поддержки.

Контрольный вопрос. Какой из перечисленных ниже способов является наиболее эффективным для пользователя, желающего отыскать принтеры, которые соответствуют этому описанию?

а. Предложите пользователю пройтись по офисному зданию и проверить каждый принтер, чтобы выяснить, обладает ли он нужными характеристиками.

б. Предложите пользователю воспользоваться командой `net view`, чтобы проверить общие принтеры, подключенные к каждому компьютеру.

в. Предложите пользователю запустить мастер добавления принтера (Add Printer Wizard) и выбрать в нем опцию Search Active Directory (Искать в Active Directory).

Решение. в. Пользователь должен выполнить поиск в Active Directory с помощью мастера Add Printer Wizard. В нем можно указать критерии поиска принтера со специфичными функциями и увидеть все принтеры, которые опубликованы в Active Directory и обладают характеристиками, требуемыми пользователю.

Подготовьте Active Directory для клиентов Mac OS X. Несмотря на то что операционная система Mac OS X позволяет присоединяться к доменам Active Directory, вы должны предпринять ряд подготовительных действий, чтобы обеспечить возможность коммуникации клиентов Mac OS X с Windows Server 2012.

Контрольный вопрос. Вы хотите, чтобы ваши пользователи Active Directory, имеющие дело с клиентами Mac, могли подключаться к серверам Windows Server 2008 R2 с помощью единственного входа в Active Directory. Какой компонент сетевой безопасности Windows необходимо изменить, чтобы разрешить клиентам Mac взаимодействовать с доменом Windows Server 2012?

Решение. Вы должны изменить локальную политику для контроллеров домена так, чтобы подписание пакетов SMB требовалось не всегда.

Подключите компьютер Mac к домену. Mac OS X может подключаться к Active Directory и присоединяться к доменам. Поддержка протокола SMB обеспечивается встроенной версией Samba, что позволяет подключать OS X к Windows для получения доступа к общим файловым ресурсам и общим принтерам.

Контрольный вопрос. Вы хотите добавить клиент Mac OS X к домену Active Directory. Какую утилиту OS X вы должны применять?

Решение. Воспользуйтесь утилитой Directory Access из папки `Utilities`, чтобы сконфигурировать и подключиться к Active Directory, а также создать в домене учетную запись компьютера.

Подключите компьютер Mac к общим файловым ресурсам и общим принтерам. OS X подключается к общим файлам и принтерам Windows с использованием поддержки SMB, предоставляемой Samba. Поскольку поддержка является интегрированной, для прямого подключения к Windows-ресурсам можно применять инструмент Finder, не устанавливая дополнительное программное обеспечение.

Контрольный вопрос. Вы пытаетесь получить доступ к сетевой папке, которая является общей на компьютере Windows Server 2012, из клиента Mac, присоединенного к домену. Как использовать Finder для такого подключения?

Решение. Внутри инструмента Finder щелкните на меню Go (Перейти) и затем на кнопке Connect to Server (Подключиться к серверу), после чего введите путь в формате `smb://имя_сервера/имя_общего_ресурса`.

Используйте Remote Desktop из клиента Mac. В Microsoft разработали Remote Desktop Connection для Mac, чтобы обеспечить клиентам Mac возможность подключения к Remote Desktop. Применяя RDC, можно получать доступ к функциональности компьютера Windows непосредственно из клиентов Mac.

Контрольный вопрос. Вы используете RDC для подключения к серверу Windows Server 2012 и хотите сохранить свои учетные данные для доступа в сеть, чтобы не приходилось вводить их при каждом подключении. Что вы можете предпринять?

Решение. Введите свои учетные данные Active Directory на экране Preferences (Предпочтения) в средстве RDC и выберите вариант их сохранения в вашей связке ключей (Keychain).

Глава 19. Управление веб-сервером с помощью IIS

Запланируйте использование IIS 8.5 и установите эту службу. Относительно экономный по умолчанию, сервер IIS 8.5 должен быть тщательно спланирован, чтобы не устанавливать большее количество модулей, чем в действительности необходимо. Даже если не принимать во внимание вопрос экономии ресурсов, устранение неиспользуемых служб ролей из сервера является также методом защиты веб-сайтов. Как всегда у Microsoft, существует несколько способов установки IIS 8.5, начиная с графического пользовательского интерфейса и заканчивая PowerShell.

Контрольный вопрос. Вы собираетесь установить IIS 8.5 в системе Windows Server 2012 R2, из которой удален графический пользовательский интерфейс. Вы хотите установить только стандартные роли, а также роль ASP.NET и все, что она требует. Какая команда PowerShell нужна для этого?

Решение. Такой командой PowerShell является `Install-WindowsFeature -Name Web-Server,Web-ASP-Net45`.

Управляйте стандартными глобальными параметрами IIS 8. Модули IIS 8 — это лишь одно из свидетельств блочной структуры продукта. Веб-приложения и индивидуальные параметры конфигурации для каждого сайта также могут управляться независимым образом. Иерархическая структура глобальных параметров, веб-параметров, параметров приложений и параметров страниц допускает возможность детализированного администрирования несколькими специалистами.

Контрольный вопрос. Что такое делегирование компонентов?

Решение. Делегирование компонентов — это искусство разрешения администраторам сайтов конфигурировать у себя на сайтах определенный компонент IIS, а не принимать его поведение, предписываемое глобальными настройками на сервере. Делегирование включается путем разблокирования специфичных разделов файлов `web.config` на одном и более сайтах.

Создавайте и защищайте веб-сайты в IIS 8. Проектирование и генерацию новых веб-сайтов в IIS 8 можно выполнять посредством графического пользовательского интерфейса или командной строки, что позволяет автоматизировать рутинную процедуру создания сайтов. Чтобы упростить выдачу разрешений, структуру разрешений можно копировать с одного сайта на другой или управлять ею на более высоких уровнях иерархии параметров. Задача генерации сайтов в IIS 8 облегчена за счет возможности пакетирования веб-сайта.

Контрольный вопрос. Вам необходимо создать новый веб-сайт, который обладает всеми характеристиками Default Web Site, но должен также поддерживать страницы ASP.NET. Вы не хотите добавлять к Default Web Site поддержку ASP.NET, поскольку опасаетесь увеличить уязвимость существующего веб-содержимого. Как вы поступите на практике?

Решение. Создайте новый веб-сайт и добавьте к нему модуль ASP.NET. Используйте специальный номер порта TCP/IP или заголовок хоста, чтобы отличать новый сайт от существующих сайтов. Подумайте о конфигурировании для этого сайта уникального удостоверения пула приложений, чтобы изолировать действия ASP.NET во время диагностики проблем.

Управляйте IIS 8 с помощью расширенных приемов администрирования. Повседневное обслуживание сайтов и отправка содержимого могут отнимать основное время при администрировании IIS 8. Однако именно дополнительное высокоуровневое управление обеспечивает согласованное и бесперебойное обслуживание ваших веб-страниц. Важные задачи конфигурирования, в числе которых восстановление после сбоев, мониторинг производительности, настройка безопасности доступа кода и определение шифрования, могут выполняться либо локально, либо дистанционно.

Контрольный вопрос. Из-за ограниченного пространства в хранилище вы пересматриваете план аварийного восстановления системы. Вы обдумываете возможность запаздывания резервного копирования файла `applicationhost.config` вплоть до месяца. Тем не менее, вас беспокоит, что небольшие изменения глобальной конфигурации, вносимые на протяжении месяца, могут быть утеряны, если сбой случится до момента создания ежемесячной резервной копии. Как бы вы восстанавливали изменение, сделанное в середине месяца?

Решение. В IIS 8 поддерживается хронология конфигурации `applicationhost.config` в соответствии со стандартным расписанием, которое находится в файле `iis_schema.xml`. Предыдущие версии этого файла можно восстановить с помощью командлета PowerShell под названием `Restore-WebConfiguration`. По умолчанию IIS 8 сохраняет автоматически генерируемые хронологические версии файла `applicationhost.config` в подкаталоге хронологии внутри `%systemdrive%\inetpub`.

Глава 20. Расширенный протокол IP: маршрутизация в Windows

Документируйте время жизни IP-пакета, маршрутизируемого по вашей сети. Понимание того, как компоненты маршрутизации действуют внутри хостов и мар-

шрутизаторов, позволит вам предвидеть, по каким маршрутам сети будет проходить сетевой трафик. Такое понимание способствует обнаружению и устранению неполадок, временами возникающих в сети.

Контрольный вопрос. Обратившись к сети Нью-Йорк/Лондон на рис. 20.1, воспользуйтесь своим пониманием маршрута, совершаемого IP-пакетом из хоста A на нью-йоркском сайте к хосту C на лондонском сайте, чтобы определить, какие адреса вы должны пропинговать для выявления проблем с маршрутизацией, которые препятствуют прохождению пакетов из пункта A в пункт C.

Решение. При использовании инструмента `ping` для отслеживания трафика от одного хоста к другому важно понимать, что вы отслеживаете возвращаемый трафик. Если маршрут нарушен, проблема вполне может быть связана с возвращением информации. С учетом сказанного, при отладке проблем с маршрутизатором на пути от системы A (Нью-Йорк) до системы C (Лондон) вы должны пропинговать по порядку следующие IP-адреса:

- A — 192.168.0.1 — чтобы убедиться в том, что протокол IP сконфигурирован на хосте A (Нью-Йорк);
- D — 192.168.0.100 — чтобы убедиться в том, что данный маршрутизатор находится в этой сети;
- D — 192.169.0.100 — чтобы убедиться в том, что данный маршрутизатор маршрутизирует трафик;
- B — 192.169.0.3 — чтобы убедиться в том, что хост B (Лондон) принимает трафик и отвечает на него.

Объясняйте точки зрения на IP-маршрутизацию с учетом классов и без учета классов. При обсуждении маршрутизации со специалистами по сетям важно понимать старую терминологию, основанную на классах. Это существенно облегчит как обсуждение подобных вопросов, так и знакомство с документацией, в которой может использоваться старая терминология. Понимание работы IP-маршрутизации без учета классов позволит избежать неэффективности, являющейся результатом чрезмерно строгого соблюдения границ классов при адресации сети.

Контрольный вопрос. Адрес 172.24.255.255 находится внутри класса B, для которого стандартной маской сети является 255.255.0.0. Он также относится к диапазону частных сетей 172.16/20 (RFC 1918), стандартная маска сети для которого выглядит как 255.255.240.0. С учетом этой информации укажите, чем является адрес 172.24.255.255 — адресом хоста или широковещательным адресом подсети?

Решение. Приведенной информации недостаточно, чтобы определить, является 172.24.255.255 адресом хоста или же широковещательным адресом подсети. Стандартная маска сети не играет роли; важна лишь маска сети, которая фактически используется. Если эта сеть построена проектировщиком, который не думал о создании суперсети или CIDR (Classless Inter-Domain Routing — междоменная маршрутизация без учета классов), то указанный адрес вполне можно трактовать как широковещательный адрес подсети. Однако с учетом того, что в документе RFC 1918 говорится о суперсети с таким диапазоном адресов, более вероятно, что он является простым адресом хоста.

Применяйте устройства NAT для маршрутизации трафика TCP. До тех пор, пока все мы не перейдем на использование протокола IPv6, нам придется применять устройства NAT для маршрутизации трафика TCP, который передается от множества хостов сети во внешний мир, используя для этого только несколько IP-адресов из сокращающегося резерва открытых IP-адресов. Понимание того, как устройства NAT изменяют адреса отправителя и получателя IP-пакетов, позволит отслеживать маршруты пакетов в сети и определять, какие системы следует рассматривать в качестве получателей данных.

Контрольный вопрос. Пользователь жалуется, что когда он подключается к FTP-сайту, подключение поначалу устанавливается, но при первой же попытке получения списка файлов оно разрывается, а сервер сообщает, что не может подключиться к 192.168.0.10.

Каковы вероятные причины возникновения этой проблемы и как ее можно решить?

Решение. Подобно SIP и ряду других протоколов, FTP часто включает в коммуникации IP-адрес хоста.

Когда адрес RFC 1918 вроде 192.168.*.* виден как часть ошибки, первое, о чем вы должны подумать — что может существовать проблема с маршрутизатором NAT между двумя хостами. В случае FTP есть несколько возможных причин и способов их устранения.

- Шлюз ALG для FTP в NAT должен изменять IP-адрес и порт в канале управления; обычной причиной, по которой это не происходит, является функционирование FTP-сервера на порте, отличном от стандартного порта 21. Возвращение сервера обратно на порт 21, если это возможно, позволит шлюзу ALG работать корректно.
- Если FTP-сервер функционирует на порте 21, то возможно, что в канале управления применяется шифрование с использованием FTP через SSL или FTP через GSSAPI. В этом случае шлюз ALG не может видеть или модифицировать трафик.
- Многие FTP-клиенты разрешают пользователю выбирать для передачи данных коммуникации в “пассивном режиме”; в этом случае через NAT должен передаваться IP-адрес сервера, и это может обеспечить пересылку данных между клиентом и сервером.
- Если это невозможно, то для обеспечения корректной работы подключений и передачи данных может оказаться необходимой прокси-служба FTP.

Глава 21. Дистанционный доступ в офис: виртуальные частные сети

Добавьте роль Network Policy and Access Services. Первым шагом при создании VPN-сервера является добавление роли Network Policy and Access Services. После этого можно предпринимать дополнительные действия по конфигурированию VPN-сервера.

Контрольный вопрос. Чтобы создать VPN-сервер, вам необходимо добавить роль Network Policy and Access Services. Как вы решите эту задачу?

Решение. Откройте диспетчер серверов и при выбранном пункте меню Local Server (Локальный сервер) выберите в меню Manage (Управление) пункт Add roles and features (Добавить роли и компоненты). С помощью мастера добавьте роль Network Policy and Access Services.

Освойте роль Remote Access. Роль Remote Access предусматривает гораздо больше, чем просто возможность создания традиционного VPN-сервера.

Контрольный вопрос. Назовите отдельные службы внутри этой роли (выберите три):

а. Remote Access Service

б. VPN Service

в. Routing

г. IPSec

д. DirectAccess

Решение. а, в, д. Тремя отдельными службами, образующими роль Remote Access, являются Remote Access Service, Routing и DirectAccess.

Сконфигурируйте VPN-сервер. Вы уже добавили роль Remote Access и теперь хотите сконфигурировать VPN-сервер, чтобы он мог принимать запросы на подключения от клиентов.

Контрольный вопрос. Что вы должны сделать для конфигурирования VPN-сервера?

Решение. Откройте оснастку Routing and Remote Access (Маршрутизация и удаленный доступ), выбрав в окне диспетчера серверов пункт меню Tools⇨Routing and Remote Access (Сервис⇨Маршрутизация и удаленный доступ). Щелкните правой кнопкой мыши на имени своего сервера и выберите в контекстном меню пункт Configure and Enable Routing and Remote Access (Конфигурировать и включить службу Routing and Remote Access). Воспользуйтесь мастером, чтобы выполнить конфигурирование.

Исследуйте DirectAccess. Технология DirectAccess позволяет удаленным пользователям безопасно подключаться к корпоративной среде без необходимости в использовании традиционного VPN-клиента.

Контрольный вопрос. Какие клиентские операционные системы поддерживаются для DirectAccess в Windows Server 2012 R2?

Решение. Для DirectAccess поддерживаются только клиентские операционные системы Windows 7 Enterprise, Windows 7 Ultimate и Windows 8 Enterprise.

Глава 22. Добавление дополнительных размещений: сайты в Active Directory

Создайте сайт. Объекты сайтов добавляются в Active Directory для представления физических площадок с высокоскоростными подключениями, на которых будут размещаться контроллеры домена. После принятия решения о размещении контроллера домена на физической площадке вы должны добавить сайт.

Контрольный вопрос. Создайте сайт для представления новой площадки в Вирджиния-Бич.

Решение. Откройте оснастку Active Directory Sites and Services. Щелкните правой кнопкой мыши на папке Sites (Сайты) и выберите в контекстном меню пункт New Site (Создать сайт). Назовите этот сайт `VB`, выберите существующую связь сайта и щелкните на кнопке OK.

Добавьте подсети к сайтам. Подсети клиентов в Active Directory используются для определения, на каком сайте они находятся. Чтобы это работало, необходимо создать объекты подсетей и ассоциировать их с сайтами.

Контрольный вопрос. Создайте объект подсети для представления подсети 10.15.0.0/16, которая существует на площадке Вирджиния-Бич. Ассоциируйте этот объект подсети с сайтом `VB` (Вирджиния-Бич).

Решение. Откройте оснастку Active Directory Sites and Services. Щелкните правой кнопкой мыши на папке Subnets (Подсети) и выберите в контекстном меню пункт New Subnet (Создать подсеть). Введите `10.15.0.0/16` в качестве префикса и выберите сайт `VB`. Щелкните на кнопке OK.

Сконфигурируйте связь сайта для выполнения репликации только в определенные периоды времени. Часто желательно ограничить время выполнения репликации между сайтами. Если используются стандартные параметры, то репликация будет происходить каждые 180 минут. Если в определенные периоды канал WAN интенсивное используется, вы можете сконфигурировать расписание так, чтобы репликация проводилась только в определенные периоды времени.

Контрольный вопрос. Сконфигурируйте сайт `Default-First-Site-Name` (или другой сайт) для выполнения репликации только в промежутке между полуночью и 5 часами утра.

Решение. Откройте оснастку Active Directory Sites and Services. Щелкните правой кнопкой мыши на связи сайта `DefaultIPSiteLink` и выберите в контекстном меню пункт Properties (Свойства). Щелкните на кнопке Change Schedule (Изменить расписание). Выберите переключатель Replication Not Available (Репликация не доступна) для изменения периода времени, когда выполнение репликации не планируется. С помощью курсора мыши выберите часы с 5:00 до полуночи для всех семи дней недели. Выберите переключатель Replication Available (Репликация доступна) и щелкните на кнопке OK.

Сконфигурируйте групповую политику для использования средства ближайшего соседнего сайта. Если на сайте клиента контроллер домена оказывается недостижимым, то клиент будет искать любой контроллер домена безотносительно того, насколько близко он находится. Это может отрицательно сказаться на времени открытия сеанса для предприятий с несколькими площадками, соединенными между собой каналами WAN с разными скоростями. Вы можете сконфигурировать клиентов Windows Vista (и более новых) так, чтобы они находили и входили в систему контроллера домена на ближайшем соседнем сайте, если контроллер домена на их сайте не доступен. Это можно сделать с помощью групповой политики или редактора реестра.

Контрольный вопрос. Какой из перечисленных ниже параметров групповой политики должен быть изменен, чтобы включить средство ближайшего соседнего сайта?

1. Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Logon⇨DC Locator DNS Records (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Вход⇨Записи DNS средства обнаружения контроллеров домена).
2. Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Вход в сеть⇨Записи DNS средства обнаружения контроллеров домена).
3. User Configuration⇨Policies⇨Administrative Templates⇨System⇨Logon⇨DC Locator DNS Records (Конфигурация пользователя⇨Политики⇨Административные шаблоны⇨Система⇨Вход⇨Записи DNS средства обнаружения контроллеров домена).
4. User Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records (Конфигурация пользователя⇨Политики⇨Административные шаблоны⇨Система⇨Вход в сеть⇨Записи DNS средства обнаружения контроллеров домена).

Решение. Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Net Logon⇨DC Locator DNS Records. Этот параметр применяется к компьютерам, а не пользователям. Вдобавок он влияет на то, как служба `netlogon` (не процесс входа) обнаруживает контроллеры домена.

Глава 23. Третий контроллер домена: контроллеры домена только для чтения

Подготовьте лес и домен для контроллеров RODC. В Windows Server 2012 R2 контроллеры RODC являются великолепным инфраструктурным активом, и их невозможно добавить до тех пор, пока не будут подготовлены лес и домен. Эта подготовка модифицирует используемую схему и разрешения.

Контрольный вопрос. Укажите команду, которую нужно выполнить, чтобы подготовить лес к поддержке контроллеров RODC.

Решение. В командной строке понадобится выполнить команду `adprep`. Подготовка леса производится следующим образом: `adprep /forestprep`.

Подготовьте домен. Прежде чем можно будет добавлять контроллеры RODC, в дополнение к подготовке леса вы должны также подготовить домен.

Контрольный вопрос. Укажите две команды, которые необходимо выполнить, чтобы подготовить домен к поддержке контроллеров RODC.

Решение. В командной строке понадобится выполнить команду `adprep`. После `adprep /forestprep` должны быть запущены следующие две команды:

- `adprep /domainprep`
- `adprep /rodcprep`

Если лес создается с использованием в качестве контроллеров домена серверов, которые функционируют под управлением Windows Server 2008 или более поздних версий, то выполнять `adprep /forestprep` и `adprep /domainprep` не обязательно, но команда `adprep /rodcprep` по-прежнему должна быть выполнена.

Разрешите кеширование паролей на любом RODC. Контроллер RODC может кешировать пароли для пользователей на основе того, каким образом он сконфигурирован. Когда пароль пользователя кешируется на RODC, процессу аутентификации нет необходимости обращаться к каналу WAN, поэтому он протекает быстрее. Тем не менее, кешированные пароли могут быть похищены злоумышленниками, поэтому привилегированные учетные записи не должны кешироваться на контроллере RODC.

Контрольный вопрос. Что понадобится модифицировать, чтобы разрешить кеширование паролей для пользователей на любом RODC в домене?

- группу `Allowed RODC Password Replication`;
- группу `Denied RODC Password Replication`;
- политику репликации паролей.

Решение. Вы должны модифицировать группу `Allowed RODC Password Replication`. Пароли членов этой группы могут реплицироваться или кешироваться на любом контроллере RODC в домене.

Разрешите кеширование паролей на отдельно взятом RODC. Среду можно сконфигурировать так, чтобы пароли членов определенной группы реплицировались и кешировались на любом RODC в соответствующем домене. Среду также можно сконфигурировать для репликации или кеширования этих паролей только на одиночном RODC.

Контрольный вопрос. Что понадобится модифицировать, чтобы разрешить кеширование паролей для пользователей на отдельном RODC в домене?

- группу `Allowed RODC Password Replication`;
- группу `Denied RODC Password Replication`;
- политику репликации паролей.

Решение. Вы должны модифицировать политику репликации паролей. С каждым контроллером RODC связано диалоговое окно, имеющее вкладку Password Replication Policy (Политика репликации паролей), в настройки которой можно внести изменения так, чтобы пользователям было разрешено кешировать или реплицировать свои пароли на данном контроллере RODC.

Глава 24. Создание более крупных сред Active Directory: за пределами одного домена

Четко сформулируйте фундаментальные концепции Active Directory. Лес и деревья возвращают среду Active Directory "обратно к природе". Лес — это коллекция доменов, построенных относительно друг друга посредством AD DS. Деревья — это домены внутри иерархического пространства имен DNS с одинаковой последней частью имени. Ключом к отношениям между доменами являются автоматические и не поддающиеся конфигурированию двунаправленные транзитивные доверительные отношения.

Контрольный вопрос. Когда создается первый контроллер домена для первого домена, в базе данных Active Directory формируются три раздела. Как называются эти три раздела, что в них содержится и какие из них реплицируются на другие контроллеры домена в лесе?

Решение. Этими тремя разделами являются раздел домена, раздел схемы и раздел конфигурации. Раздел домена содержит объекты, относящиеся к домену, такие как учетные записи компьютеров и пользователей, и реплицируется на контроллеры домена в домене. В разделе схемы определены объекты Active Directory и значения данных для каждого объекта. Раздел конфигурации содержит данные, касающиеся репликации Active Directory, и другие конфигурации, касающиеся леса. Разделы схемы и конфигурации реплицируются по всему лесу.

Выберите между использованием в структуре Active Directory одного домена, нескольких доменов или нескольких лесов. При выборе структуры Active Directory вы можете решить, что требуется несколько доменов, а не один домен с несколькими организационными единицами внутри. Ограничения репликации, юридические требования и политические факторы — вот главные причины, которые могут обусловить выбор структуры с множеством доменов.

Контрольный вопрос. Какие средства Windows Server 2012 R2 устраняют две причины применения структуры с несколькими доменами, которые связаны с безопасностью?

Решение. Двумя причинами использования структуры с несколькими доменами, которые связаны с безопасностью, были политики паролей и недостаточный уровень защиты в офисах филиалов. Средство детализированных политик паролей, которые могут применяться к пользователям посредством объектов GPO, устранило необходимость в создании отдельных доменов для использования отличающихся политик паролей. Контроллер домена только для чтения с кешированием паролей снижает риск извлечения паролей из базы данных Active Directory в результате похищения контроллера домена. Кроме того, снижается риск репликации разрушительных изменений на остальные контроллеры домена.

Добавьте домены в среду Active Directory. При построении нового домена или контроллера домена с репликой в лесе Active Directory вы будете использовать мастер конфигурирования служб домена Active Directory (Active Directory Domain Services Configuration Wizard). В предыдущих версиях Windows Server структура DNS должна была быть на месте еще до установки. В Windows Server 2012 R2 все необходимое выполняется автоматически.

Контрольный вопрос. Поскольку все необходимые действия, связанные с DNS, теперь обрабатываются Windows Server 2012 R2, полезно знать, правильно ли они выполнены. Какие четыре изменения вы должны увидеть после добавления нового дочернего домена?

Решение. Вы должны увидеть следующие изменения.

- В конфигурациях IP контроллер домена отображается как DNS-сервер с использованием адресов обратной связи для IPv4 и IPv6.

- Зона DNS для нового дочернего домена поддерживается на контроллере домена как зона, интегрированная с Active Directory.
- Дочерний контроллер домена отображается как DNS-сервер пересылки.
- Имя DNS дочернего домена делегируется новому контроллеру домена в дочерней зоне DNS.

Управляйте функциональными уровнями, доверительными отношениями, ролями FSMO и глобальным каталогом. Мы обсудили несколько конфигураций, связанных с лесом, которые будут управляться администраторами предприятия. Функциональные уровни для леса и доменов обеспечивают доступность возможностей, предусмотренных в самой последней версии Windows Server. Чтобы получить в свое распоряжение эти возможности, все контроллеры домена должны быть модернизированы до этого уровня. Функциональные уровни можно поднимать, но не опускать. Пять ролей FSMO представляют собой особые роли, назначаемые контроллерам домена внутри доменов, а также лесу. Ролями, связанными с доменом, являются PDC Emulator, RID Master и Infrastructure Master. К ролям, связанным с лесом, относятся Domain Naming Master и Schema Master. Чтобы домены, не являющиеся частями одного и того же леса, могли совместно пользоваться определенными ресурсами, необходимо создавать доверительные отношения. Исключением являются установленные напрямую доверительные отношения, которые позволяют сократить путь доверия между двумя доменами внутри того самого леса.

Контрольный вопрос. Размещение роли FSMO диктуется доменом, которому она назначена, и ролью Global Catalog. В каких двух ролях предусмотрены правила, связанные с размещением, в том, что касается глобального каталога?

Решение. Роль Domain Naming Master, которая находится в корневом домене леса, должна размещаться на контроллере домена с ролью Global Catalog. Роль Infrastructure Master, которая присутствует в каждом домене, не может располагаться на контроллере домена с ролью Global Catalog. Тем не менее, это не относится к среде Active Directory с одним доменом.

Глава 25. Миграция, слияние и модификация Active Directory

Внедрите в сеть новые версии Active Directory. Модернизация до новой версии Windows Server означает также необходимость в модернизации существующих контроллеров домена. Добавить в организацию новую версию Active Directory можно с помощью двух базовых методов — модернизации контроллера домена и модернизации домена за счет добавления нового контроллера домена.

Контрольный вопрос. Обе операции требуют модификации базы данных Active Directory с использованием утилиты `adprep.exe`. С какими тремя параметрами ее нужно запускать? С каким еще параметром ее можно запускать?

Решение. Параметр `/forestprep` модифицирует схему леса Active Directory для поддержки Active Directory версии Windows Server 2008 R2.

Параметр `/domainprep` выполняет подготовку домена для контроллера домена Windows Server 2008 R2.

Параметр `/gpprep` изменяет разрешения в объектах GPO для репликации на контроллеры домена Windows Server 2008 R2.

Параметр `/rodcprep` производит подготовку леса к развертыванию контроллеров домена только для чтения. Это действие является необязательным и может быть выполнено в любой другой момент времени.

Проведите миграцию доменных учетных записей из одного домена в другой. Требование перемещения пользователей и групп из существующего домена в чистый изначальный домен часто возникает при слиянии или разделении компаний. Кроме того, это может потребоваться, когда оправдана реструктуризация леса. Для выполнения миграций доменов Microsoft предлагает утилиту ADMT.

Контрольный вопрос. Что обеспечивает пользователю доступ к ресурсам, находящимся внутри исходного домена, после того как учетная запись пользователя перенесена в новый домен?

Решение. Ресурсам в исходном домене назначены разрешения, позволяющие получать к ним доступ таким перечисленным участникам безопасности, как учетные записи пользователей. В этих разрешениях, которые также называются ACE, указан идентификатор SID пользователя. После переноса учетной записи пользователя его идентификатор SID изменяется. Однако исходный идентификатор SID сохраняется в хронологии SID. Когда пользователь проходит аутентификацию в другом домене, хронология SID будет идентифицировать разрешения для данного ресурса.

Это действие предотвращается фильтрацией SID, которая по умолчанию включена в доверительных отношениях между доменами. Вы должны вручную отключить фильтрацию SID.

Глава 26. Расширенное управление пользовательскими учетными записями и поддержка пользователей

Разверните домашние каталоги для множества пользователей. Домашние каталоги позволяют пользователю иметь персональное хранилище информации на файловом сервере. Это делает данные доступными пользователю независимо от того, где он входит в сеть.

Контрольный вопрос. Перед вами поставлена задача создать домашние каталоги для многих пользователей в организационной единице, которой вы управляете. Вы хотите решить эту задачу как можно быстрее. Ваше приложение резервного копирования использует учетную запись администратора, поэтому вам нужно позаботиться о том, чтобы у приложения был доступ к домашним каталогам пользователей на файловом сервере. Как вы поступите?

Решение. Выполните следующие действия.

1. Создайте на файловом сервере общий файловый ресурс, предназначенный для ваших домашних каталогов, и соответствующим образом установите разрешения.

2. Сконфигурируйте объект групповой политики (GPO) для организационной единицы. Включите политику Add the Administrators security group to roaming user profiles (Добавить группу доступа `Administrators` в перемещаемые профили пользователя), которая расположена в папке Computer Configuration \ Administrative Templates \ System \ User Profiles (Конфигурация компьютера \ Административные шаблоны \ Система \ Профили пользователей).
3. В окне оснастки Active Directory Users and Computers перейдите к этой организационной единице. Выделите все объекты пользователей, щелкните правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства). Введите путь к общему файловому ресурсу с домашними каталогами и добавьте в конце `\%username`.

Домашние каталоги будут созданы автоматически, и администраторы на файловом сервере будут иметь к ним доступ.

Настройте обязательные перемещаемые профили. Обязательные перемещаемые профили можно применять для предоставления пользователям предварительно сконфигурированной рабочей среды и предотвращения сохранения в ней изменений.

Контрольный вопрос. Ваш руководитель попросил вас настроить обязательный перемещаемый профиль для пользователей Windows 8. Вас также попросили выяснить, нельзя ли каким-то образом предотвратить вход пользователей в систему, если обязательный перемещаемый профиль не удалось загрузить.

Решение. Вам необходимо сконфигурировать принудительный перемещаемый профиль.

1. Войдите в систему ПК как обычный пользователь. Надлежащим образом сконфигурируйте рабочую среду.
2. Войдите в систему того же ПК как администратор и скопируйте профиль обычного пользователя в какое-то сетевое расположение. С помощью `regedit.exe` вы должны сделать так, чтобы требуемая группа доступа Active Directory имела разрешение Full Control (Полный доступ) для куста реестра в профиле.
3. Переименуйте файл `NTUSER.DAT` внутри профиля в **`NTUSER.MAN`**. Это приведет к тому, что профиль станет обязательным.
4. Переименуйте этот профиль, например, в `Mandatory.V2`, зная, что `.V2` требуется для пользователей Windows 8.
5. Чтобы сделать этот обязательный перемещаемый профиль принудительным, можете переименовать папку профиля в **`Mandatory.MAN.V2`**.

Создайте сценарии входа для автоматизации администрирования. Администраторы могут использовать сценарии входа, чтобы запускать последовательность команд для предварительного конфигурирования рабочей среды пользователям при их входе в систему. Для этих целей администраторы могут применять команды командной строки, VBScript или PowerShell.

Контрольный вопрос. Вы проектируете среду Active Directory для крупной организации, включающей множество сайтов. Вам требуется возможность настройки сценариев входа для разных ситуаций:

- имеются глобальные команды, которые должны выполняться для каждого пользователя;
- любой пользователь в организационной единице `Accounts` должен иметь доступ к определенным ресурсам;
- любой пользователь, в том числе посетители, который входит на сайт Dublin Active Directory, должен подключаться к локальному общему диску.

У вас спрашивают, какой окажется последовательность запуска для любого пользователя, который будет выполнять все эти сценарии входа.

Решение. Подготовьте эти три сценария входа и сохраните их в папке `NETLOGON` на контроллере домена. Создайте три объекта GPO. Свяжите первый объект GPO с доменом и отредактируйте его так, чтобы данный сценарий входа выполнялся для каждого пользователя. Свяжите второй объект GPO с организационной единицей `Accounts` и отредактируйте его так, чтобы сценарий входа выполнялся для организационной единицы `Accounts`. Свяжите третий объект GPO с сайтом Dublin Active Directory и отредактируйте его так, чтобы выполнялся сценарий входа для этого сайта.

Порядок применения объектов GPO таков: сайт, домен, организационная единица, дочерняя организационная единица. Порядок выполнения сценариев входа для пользователя, наследующего все эти политики, выглядит следующим образом:

- сайт Dublin Active Directory;
- домен;
- организационная единица `Accounts`.

Глава 27. Виртуализация серверов с помощью Hyper-V

Уясните, что собой представляет виртуализация сервера. Вы закупаете новые серверы, главной ролью которых будет запуск Hyper-V. Однако вас заботит вопрос, способны ли новые серверы обеспечить работу Hyper-V, т.е. удовлетворяют ли они минимальным требованиям, предъявляемым Hyper-V.

Контрольный вопрос. Каковы базовые требования к ЦП и BIOS для запуска Hyper-V?

Решение. Вам потребуется 64-разрядный ЦП и система BIOS, которая поддерживает виртуализацию, выполняемую с помощью ЦП, и функцию предотвращения выполнения данных (Data Execution Prevention — DEP). Распространенная проблема состоит в том, что хотя эти возможности предлагаются системой, обычно в системе BIOS на более старом серверном оборудовании они не включены. Позаботьтесь о включении данных функций. Если нужно изменить настройки DEP или виртуализации, помните о том, что для этого необходима холодная начальная загрузка: компьютер должен быть полностью выключен. Сброса или программной перезагрузки будет недостаточно.

Исследуйте нововведения Hyper-V в Windows Server 2012 R2. Специалисты Microsoft разработали большой набор новых возможностей и внесли множество усовершенствований в Hyper-V версии Windows Server 2012 R2, которые должны значительно облегчить IT-специалистам, администраторам и консультантам работу по убеждению своих клиентов и руководителей в необходимости использования Hyper-V в своих производственных средах.

Контрольный вопрос. В ранних версиях Hyper-V сложное копирование и вставка в виртуальные машины могло быть обеспечено только с применением подключения Remote Desktop и вообще не работало при отсутствии подключения к сети. Как называется новое средство, которое делает возможными копирование и вставку в виртуальную машину безо всякого сетевого подключения за счет использования VMBus?

Решение. Режим расширенного сеанса позволяет без труда выполнять копирование и вставку напрямую в и из виртуальной машины, даже без сконфигурированного сетевого подключения. На практике это выглядит точно так же, как подключение к удаленному рабочему столу, но без необходимости беспокоиться о сетевом подключении. Для этого в режиме расширенного сеанса применяется VMBus через компоненты интеграции Hyper-V.

Уясните архитектуру Hyper-V. Когда вы разворачиваете роль Hyper-V на своем компьютере, то тем самым создаете архитектуру гипервизора. *Гипервизор* — это программный уровень, который располагается между оборудованием и операционными системами, функционирующими на хосте. Такой подход называется "голым железом", т.е. виртуализация реализуется на самом низком из возможных уровней. Главная цель гипервизора заключается в создании изолированных сред выполнения (разделов) для всех операционных систем. В полном соответствии с этой функцией гипервизор отвечает за арбитраж доступа к оборудованию.

Контрольный вопрос. Во время развертывания роли Hyper-V хост пару раз перезапускается, чтобы обеспечить размещение Hyper-V поверх оборудования. На уровне какого кольца оно находится?

а. Кольцо 3

б. Кольцо 0

в. Кольцо -1

г. Кольцо 2

Решение. в. Размещение Hyper-V поверх оборудования обеспечивается на уровне кольца -1.

Установите и сконфигурируйте хост Hyper-V. Едва ли не единственным решением, которое понадобится принять перед установкой роли Hyper-V, является выбор сетевой интерфейсной платы, предназначенной для управления хостом Hyper-V. Идея в том, чтобы на хосте было, по меньшей мере, две сетевых интерфейсных платы, хотя можно обойтись и одной, если так сложились обстоятельства. В таком случае не рассчитывайте на высокую производительность. При наличии двух сетевых интерфейсных плат, выделите одну из них для управления хостом, а другую — для сетевого трафика виртуальной машины.

Контрольный вопрос. Если вы располагаете в своей среде Hyper-V двумя или большим количеством сетевых интерфейсных плат, то какой параметр, включенный по умолчанию, вы должны отключить на виртуальном сетевом адаптере?

Решение. После завершения работы мастера установки Hyper-V рекомендуется снять отметку с флажка Allow management operating system to share this network adapter (Разрешить управляющей операционной системе совместное использование этого сетевого адаптера) для виртуальной сетевой интерфейсной платы. Оставляя этот флажок отмеченным, вы обеспечиваете хосту доступ к данному коммутатору, а это означает возможность разделения трафика между виртуальными машинами и операционной системой их хоста. В испытательной или непроизводственной среде, где в вашем распоряжении может оказаться только одна сетевая интерфейсная плата, отметки этого флажка должно быть вполне достаточно. Но при наличии нескольких сетевых интерфейсных плат или в случае работы в производственной среде Hyper-V рекомендуется снять отметку с этого флажка и щелкнуть на кнопке Apply (Применить).

Сконфигурируйте и установите операционную систему на виртуальной машине. Концептуально создание виртуальной машины с нуля выполняется в два этапа. Сначала вы конфигурируете виртуальное оборудование виртуальной машины, затем загружаете виртуальную машину и приступаете к установке на ней операционной системы. Когда эти два этапа будут завершены, вы можете с помощью диспетчера Hyper-V или PowerShell управлять виртуальной машиной.

Контрольный вопрос. При управлении виртуальной машиной с применением графического пользовательского интерфейса консоль может "захватывать" клавиатуру и мышь. Для этого нужно щелкнуть на виртуальном экране. После захвата весь ввод с клавиатуры и мыши отправляется виртуальной машине. В начальной стадии нельзя освободить виртуальную машину от управления клавиатурой и мышью, просто переместив курсор мыши. Какая клавиатурная комбинация сконфигурирована по умолчанию для возврата управления клавиатурой и мышью обратно операционной системе хоста?

Решение. Чтобы освободить управление, понадобится нажать сочетание клавиш <Ctrl+Alt+стрелка влево>. В полноценно функционирующей виртуальной машине с установленными компонентами интеграции (Integration Components) все намного проще: перемещение курсора мыши с виртуального экрана на рабочий стол приводит к тому, что хост возобновляет управление клавиатурой и мышью. Существует один особый случай: последовательность <Ctrl+Alt+Del>. Даже когда управление принадлежит виртуальной машине, эту последовательность обрабатывает хост. Чтобы отправить последовательность <Ctrl+Alt+Del> виртуальной машине, можно либо нажать <Ctrl+Alt+End>, либо воспользоваться соответствующим действием в меню консоли.

Глава 28. Управление виртуальными машинами

Виртуализируйте контроллеры домена. В Windows Server 2012 предлагается новый метод очень быстрого развертывания любого количества виртуальных контроллеров домена посредством *клонирования виртуальных контроллеров домена*. Он позволяет администраторам оперативно вводить в действие копии

контроллеров домена, используя в качестве эталона существующий шаблонный контроллер домена. Клонирование виртуальных контроллеров домена может быть выгодно организациям, которым необходимо быстро развернуть много контроллеров в новых доменах. Эта функция также полезна в частных облачных средах при удовлетворении требований масштабируемости.

Контрольный вопрос. Какова минимальная поддерживаемая версия Active Directory, которую можно использовать с клонированием виртуальных контроллеров домена?

Решение. Для клонирования виртуальных контроллеров домена требуется виртуальный контроллер домена, работающий под управлением Windows Server 2012 или последующей версии, который является членом того же домена, что и эмулятор PDC, также функционирующий под управлением Windows Server 2012 или выше.

Уясните, как перемещать виртуальные машины. Средство Hyper-V в Windows Server 2012 позволяет относительно просто *экспортировать* и *импортировать* виртуальные машины между хостами. Это стало возможным за счет того, что все хосты Hyper-V предоставляют своим виртуальным машинам практически идентичное оборудование посредством компонентов интеграции и синтетических драйверов. Если требовалось перемещать установленные копии ОС в мире физических серверов, то нужно было, как минимум, переносить физические диски, что работало только в случае достаточного сходства оборудования, но при этом далеко не всегда гарантировало успех.

Контрольный вопрос. Какие три параметра необходимо перенести при перемещении виртуальной машины на другой хост Hyper-V?

Решение. Тремя параметрами виртуальной машины, которые необходимо перенести на другой хост при перемещении виртуальной машины, являются конфигурация, текущее состояние и данные.

Управляйте виртуальными машинами. Хотя виртуализация привносит множество новых средств и добавляет гибкости, вам по-прежнему приходится выполнять более традиционные задачи по обслуживанию виртуальных машин, такие как резервное копирование, управление защитой от вредоносного программного обеспечения и своевременное применение обновлений и исправлений.

Контрольный вопрос. Какую технологию вы использовали бы для применения исправлений к производственным виртуальным машинам, если вы располагаете кластером с обходом отказа Hyper-V, который функционирует под управлением Windows Server 2012 R2?

Решение. Если у вас имеется среда кластера Hyper-V с обходом отказа, функционирующая под управлением Windows Server 2012 или последующей версии, вы можете задействовать средство обновления, осведомленное о кластерах (Cluster-Aware Updating — CAU), которое позволит применять исправления к серверам с минимальным временем простоя в процессе развертывания обновлений.

Средство CAU интегрируется со встроенным агентом обновления Windows (Windows Update Agent) и службами обновления сервера Windows (Windows Server Update Services — WSUS) для загрузки и установки обновлений. Когда

необходимо применить исправления к кластерному узлу Hyper-V с работающим Windows Server 2012 R2, понадобится всего лишь остановить хост, после чего активизируется новая функция Virtual Machine Drain on Shutdown, которая выполнит миграцию всех виртуальных машин на любой другой доступный хост.

Уясните, как выполняется восстановление в аварийных ситуациях с помощью Hyper-V. Средство Hyper-V Replica (HVR) доступно в Windows Server 2012 и последующих версиях. Оно делает возможной репликацию виртуальных машин на основе хоста, не требуя создания общих кластерных компонентов для поддержки сценариев восстановления в аварийных ситуациях.

Контрольный вопрос. На какое количество сайтов, находящихся за пределами производственного сайта, можно реплицировать виртуальные машины, имея функционирующее средство Hyper-V Replica в Windows Server 2012 R2?

Решение. С помощью Hyper-V Replica можно взять виртуальную машину, работающую внутри хоста Hyper-V на одном сайте, и легко реплицировать ее на другой сайт с возможностью использования до двух дополнительных сайтов.

Глава 29. Установка, использование и администрирование служб удаленного рабочего стола

Ограничьте максимальное количество соединений. Вы можете изменить режим лицензирования сервера, чтобы гарантировать соответствие лицензионному соглашению и существующим назначениям.

Контрольный вопрос. Вы хотите знать, в каком режиме лицензирования находится сервер. Что вы предпримете?

Решение. Выполните следующие действия.

1. Откройте диспетчер серверов.
2. Щелкните на элементе Remote Desktop Services (Службы удаленного рабочего стола).
3. Щелкните на кнопке Tasks (Задачи) рядом с разделом Deployment Overview (Обзор развертывания) и выберите пункт Edit Deployment Properties (Редактировать свойства развертывания).
4. Щелкните на значке “плюс” рядом с элементом RD Licensing (Лицензирование RD).

Добавьте приложения к серверу RD Session Host. После добавления роли RDS и конфигурирования сервера RD Session Host можно приступить к добавлению приложений, чтобы сделать их доступными этому серверу.

Контрольный вопрос. Ваша компания приобрела приложение, которое поддерживает многопользовательский доступ. Вы хотите установить его на сервере RD Session Host. Что потребуется сделать?

Решение. Установите это приложение с применением файла `.msi` (Windows Installer) или функции установки и удаления программ панели управления.

Если приложение может быть установлено с помощью одного из этих методов, то не придется пользоваться командой `Change User`, которая требовалась в старых версиях Terminal Services. Если же установить приложение посредством файла `.msi` или функции установки и удаления программ панели управления невозможно, вы должны ввести команду `Change User /install` перед установкой и `Change User /execute` после установки.

Добавьте приложения RemoteApp для доступа через веб. Приложения RemoteApp могут быть сконфигурированы так, чтобы пользователи могли получать доступ к ним из веб-браузера. Пользователям просто необходимо обратиться к подходящей странице и выбрать приложение для запуска.

Контрольный вопрос. Предположим, что вы уже сконфигурировали среду для поддержки приложений RemoteApp. Теперь вы хотите добавить приложение RemoteApp. Что потребуется сделать?

Решение. Выполните следующие действия.

1. Откройте диспетчер серверов.
2. Щелкните на элементе Remote Desktop Services (Службы удаленного рабочего стола).
3. Щелкните на элементе Collections (Коллекции).
4. Выберите свою коллекцию.
5. Щелкните на кнопке Tasks (Задачи) рядом с разделом RemoteApp Programs (Программы RemoteApp) в диспетчере серверов и выберите пункт Publish RemoteApp Programs (Опубликовать программы RemoteApp).
6. Выберите свое приложение из списка или перейдите к нужному исполняемому файлу.
7. Щелкните на кнопке Publish (Опубликовать).
8. Щелкните на кнопке Close (Закрыть).

Глава 30. Мониторинг Windows Server 2012 R2

Используйте диспетчер серверов для мониторинга множества серверов. Новая консоль диспетчера серверов в Windows Server 2012 R2 обеспечивает мониторинг и проверку работоспособности инфраструктуры локальных и удаленных серверов. Ее можно применять для мониторинга нескольких серверов и ролей, за которые они отвечают, причем все это из одной центральной консоли.

Контрольный вопрос. Вам необходимо знать комплексное состояние работоспособности для коллективных ролей на множестве серверов; кроме того, вы хотите управлять ими посредством диспетчера серверов. Что вам понадобится развернуть?

а. Группы доступа

б. Группы серверов

в. Группы рассылки

г. Административные группы

- *Решение.* б. Серверные группы используются, когда необходимо знать комплексное состояние работоспособности для коллективных ролей на нескольких серверах, а также для управления ими с помощью диспетчера серверов.

Научитесь пользоваться средством Event Viewer. Средство Event Viewer в Windows Server 2012 R2 является одним из важнейших инструментов, используемых для мониторинга системы. Часто он оказывается одним из первых мест, куда вы будете заглядывать, когда обнаружите, что в сервере имеется проблема, однако Event Viewer можно также применять и для упреждающего мониторинга серверов. Средство Event Viewer может помочь в быстрой идентификации источника проблемы или, по крайней мере, в получении достаточного объема информации, чтобы знать, куда двигаться дальше.

Контрольный вопрос. Вы только что развернули роль Hyper-V на своем компьютере Windows Server 2012 R2. Где вы будете искать журнал событий, связанный с этой ролью?

Решение. Папка `Applications and Services Logs` включает журналы для определенных приложений или компонентов; именно в ней вы найдете журнал событий, связанный с ролью Hyper-V.

Исследуйте монитор производительности. Группы сборщиков данных можно использовать для измерения и мониторинга производительности сервера. Монитор производительности включает встроенные группы сборщиков данных, которые могут запускаться по запросу; кроме того, можно создавать собственные группы сборщиков данных.

Контрольный вопрос. Запустите группу сборщиков данных System Performance и просмотрите результирующий отчет.

Решение. Запустите комплект монитора производительности, выбрав пункт меню Tools⇨Performance Monitor (Сервис⇨Монитор производительности) в диспетчере серверов. Щелкните правой кнопкой мыши на группе сборщиков данных System Performance (Производительность системы) и выберите в контекстном меню пункт Start (Запустить). Когда работа будет завершена, щелкните правой кнопкой мыши на этой группе сборщиков данных и выберите в контекстном меню пункт Latest Report (Самый последний отчет).

Исследуйте инструменты PAL и PerfView. Инструменты Performance Analysis of Logs (PAL) и PerfView являются двумя дополнительными внешними средствами, которые помогают упростить сбор и анализ данных о производительности, а также создать всеобъемлющие базовые уровни производительности для приложений, функционирующих под управлением Windows Server 2012 R2.

Контрольный вопрос. Инструмент PAL может быть очень полезным, когда применяется в сочетании с журналами счетчиков монитора производительности. Какое расширение используется для файлов этих журналов счетчиков?

а. `.chk`

б. `.perf`

в. `.blg`

г. `.evnt`

Решение. в. Расширение `.blg` используется для файлов с журналами счетчиков монитора производительности.

Изучите диспетчер операций, входящий в состав System Center 2012 R2. Диспетчер операций (Operations Manager, также известный как OpsMgr или SCOM) представляет собой решение сквозного мониторинга, которое охватывает среду Microsoft и 19 других межплатформенных сред. Диспетчер операций позволяет централизованно проводить мониторинг серверов, приложений, оборудования и операций для многих компьютеров из центральной консоли. Его можно использовать для отображения всех компонентов индивидуальных IT-служб и последующей их организации в единое и легкое в управлении представление для мониторинга.

Контрольный вопрос. Когда вы впервые развертываете Operations Manager и решаете поместить агент на сервер, он будет видеть этот сервер как сущность, которая либо функционирует, либо нет. Как заставить Operations Manager видеть разные роли и приложения на серверах?

Решение. Диспетчеру операций известно, что он должен выполнять мониторинг на каждом агенте через специальные пакеты управления, которые были разработаны и сделаны доступными либо поставщиком приложения/продукта, либо сообществом System Center. Эти пакеты управления проливают свет на инфраструктуру Operations Manager и позволяют агентам воспринимать компоненты, которые необходимо взять под контроль мониторинга.

Глава 31. Управление исправлениями

Используйте Windows Automatic Updates для проверки наличия новых обновлений на компьютере, работающем под управлением Windows 8. Компонент Windows Automatic Updates входит в состав панели управления и применяется для проверки наличия на сайте Microsoft Update любых обновлений для вашего компьютера.

Контрольный вопрос. Воспользуйтесь Windows Automatic Updates на компьютере Windows 8, чтобы проверить наличие для него доступных обновлений.

Решение. Чтобы проверить доступность обновлений, выполните следующие действия.

1. Щелкните на кнопке Start (Пуск) и введите `Control Panel`.
2. Щелкните на значке Windows Update (Центр обновления Windows).
3. Щелкните на Check for updates (Поиск обновлений).

Если для вашего компьютера имеются обновления, их будет предложено установить.

Применяйте Windows Update Standalone Installer для молчаливой установки обновлений безопасности. Инструмент Windows Update Standalone Installer применяется для установки обновлений безопасности во всех операционных системах Windows, начиная с Windows Vista и Windows Server 2008.

Контрольный вопрос. Установите в молчаливом режиме обновление безопасности и отложите требуемую перезагрузку с использованием Windows Update Standalone Installer.

Решение. В окне командной строки с повышенными разрешениями введите команду *исполняемый_файл* /quiet /norestart, где *исполняемый_файл* — это имя файла обновления безопасности.

Идентифицируйте четыре фазы управления исправлениями. Согласно рекомендациям Microsoft, существуют четыре фазы при планировании стратегии управления исправлениями.

Контрольный вопрос. Какое из перечисленных ниже действий не имеет отношения к четырем фазам управления исправлениями?

1. Идентификация
2. Поиск и устранение проблем
3. Оценка и планирование
4. Оценка
5. Развертывание

Решение. Поиск и устранение проблем не является одной из четырех фаз управления исправлениями. Эти четыре фазы в порядке их следования указаны далее.

1. Идентификация
2. Оценка и планирование
3. Оценка
4. Развертывание

Следование стандартизованному и документированному процессу помогает привнести порядок в хаос, присущий управлению исправлениями.

Глава 32. Резервное копирование и обслуживание Windows Server 2012 R2 и Active Directory

Используйте Windows Server Backup для резервного копирования и восстановления компьютера Windows Server 2012 R2. Инструмент Windows Server Backup устанавливается в виде компонента Windows Server 2012 R2 и может применяться для создания разнообразных типов резервных копий с целью защиты серверного компьютера. Полные резервные копии сервера содержат операционную систему, критически важные тома и все данные на сервере, тогда как резервные копии критически важных томов защищают все тома, от которых зависит операционная система, но не обязательно дополнительные данные, хранящиеся на сервере.

Контрольный вопрос. Ваш сервер содержит два жестких диска: на первом находится операционная система, а на втором — пользовательские данные. Как с помощью Windows Server Backup можно защитить операционную систему и пользовательские данные?

Решение. Выполните полное резервное копирование сервера, которое по умолчанию создает резервные копии обоих томов.

Выполните автономную дефрагментацию AD DS. Версия Windows Server 2012 R2 предлагает возможность выполнения автономной дефрагментации и проверки целостности базы данных AD DS без необходимости в перезапуске компьютера и входе в режим DSRM. Вместо этого вы можете остановить AD DS и затем воспользоваться `Ntdsutil.exe` в окне командной строки с повышенными разрешениями для запуска автономной дефрагментации и проверки целостности.

Контрольный вопрос. Вы хотите дефрагментировать базу данных AD DS, но не желаете прекращать работу сервера и перезапускать его в режиме DSRM. Как вы поступите?

Решение. Остановите AD DS и запустите утилиту `Ntdsutil.exe` в окне командной строки с повышенными разрешениями, чтобы дефрагментировать базу данных `Ntds.dit`.

Установите корзину Active Directory. Недостаток версии корзины в Windows Server 2008 R2 для части пользователей заключался в том, что ей приходилось управлять полностью с помощью PowerShell. В Windows Server 2012 R2 появилась возможность управления корзиной посредством графического пользовательского интерфейса.

Контрольный вопрос. Вы хотите установить корзину Active Directory, не используя PowerShell. Как это можно сделать?

Решение. В окне центра администрирования Active Directory щелкните на своем (локальном) домене в панели навигации слева и в панели Tasks (Задачи) справа щелкните на элементе Enable Recycle Bin (Включить корзину).

Создайте и восстановите резервную копию состояния системы для Active Directory. Поскольку контроллеры домена содержат всю информацию базы данных для Active Directory, восстановление вышедшего из строя сервера контроллера домена является чрезвычайно важной задачей. При использовании инструмента Windows Server Backup или утилиты командной строки `Wbadmin.exe` создавайте резервные копии, содержащие, как минимум, состояние системы, чтобы предохранить Active Directory.

Контрольный вопрос. Вы хотите защитить данные Active Directory от возможного полного отказа оборудования серверного компьютера. Какие типы резервного копирования предоставят такую защиту?

Решение. Используйте как минимум резервную копию состояния системы. Резервные копии критически важных томов и полная резервная копия сервера также включают всю информацию, необходимую для восстановления Active Directory.

Предметный указатель

U

V

W

A

Б

B

К

Л

М

О

П

P

C

Т

У

Ф

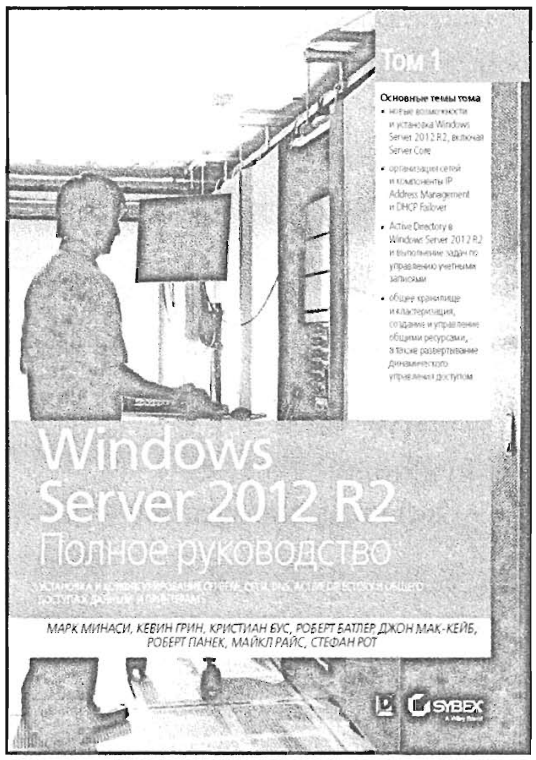
Х

Ш

WINDOWS SERVER 2012 R2 ПОЛНОЕ РУКОВОДСТВО. ТОМ 1

УСТАНОВКА И КОНФИГУРИРОВАНИЕ СЕРВЕРА, СЕТИ, DNS, ACTIVE DIRECTORY И ОБЩЕГО ДОСТУПА К ДАННЫМ И ПРИНТЕРАМ

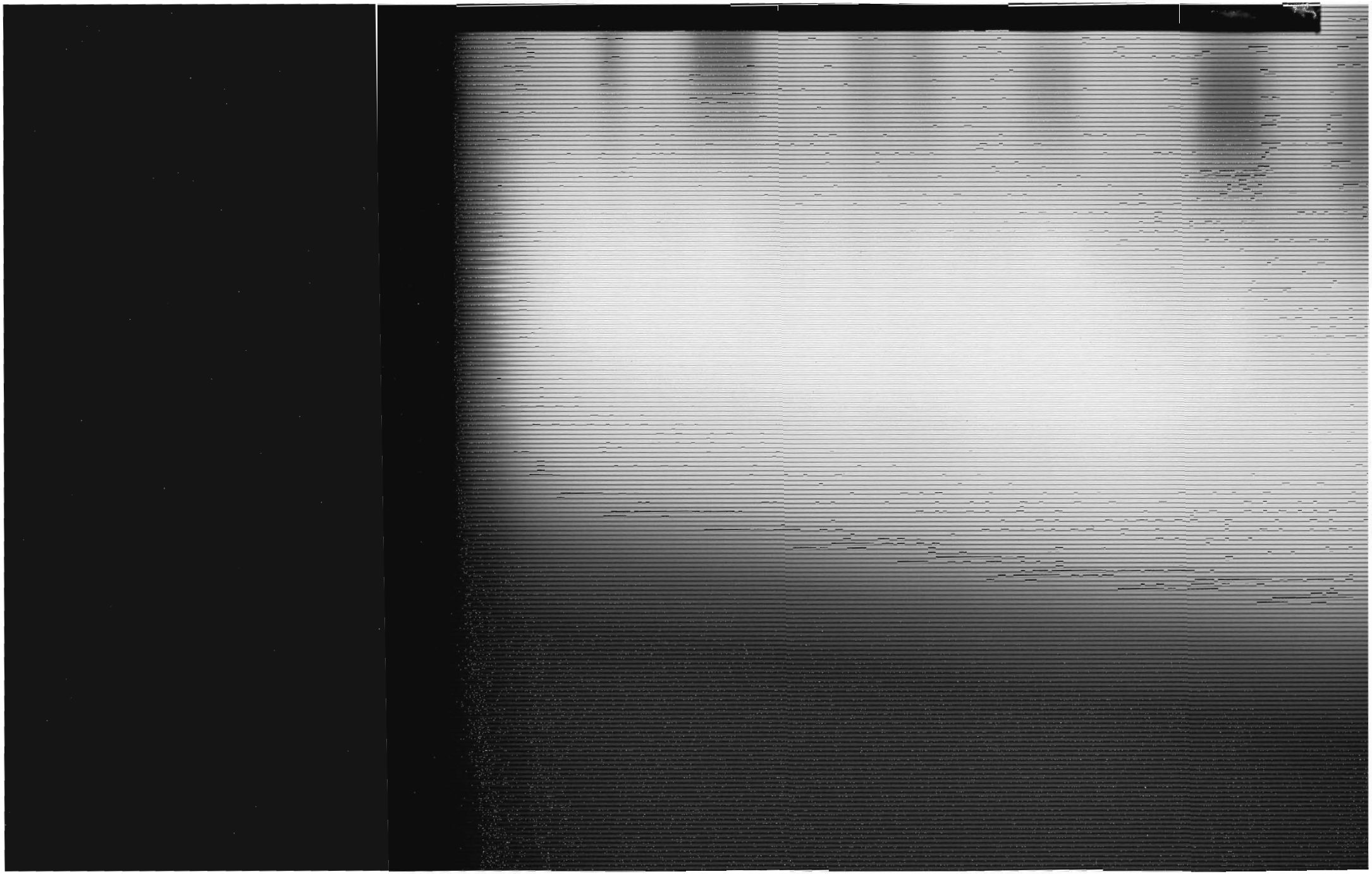
Марк Минаси и др.



www.dialektika.com

Попробуйте новый гипервизор Hyper-V, найдите новые и более простые способы дистанционного подключения к офису, а также изучите Storage Spaces — это всего лишь несколько компонентов Windows Server 2012 R2, которые подробно рассматриваются в данном обновленном издании книги признанного авторитета в области Windows Марка Минаси и команды экспертов по Windows Server, возглавляемой Кевином Грином. Основные темы книги: установка или модернизация и последующее управление сервером с Windows Server 2012 R2; настройка объединения сетевых интерфейсных плат Microsoft NIC Teaming 2012 и работа с PowerShell; установка операционной системы через графический пользовательский интерфейс или обновленную версию Server Core 2012; миграция, слияние и модификация Active Directory; управление адресным пространством с помощью IPAM; новые общие хранилища, пространства хранения и улучшенные инструменты для работы с ними; управление доступом к общим файлам — новый и усовершенствованный подход; использование и администрирование Remote Desktop, Virtual Desktop и Hyper-V.

ISBN 978-5-8459-1935-9 **в продаже**



Универсальное руководство по Windows Server 2012 R2

Попробуйте новый гипервизор Hyper-V, найдите новые и более простые способы дистанционного подключения к офису, а также изучите Storage Spaces — это всего лишь несколько компонентов Windows Server 2012 R2, которые подробно рассматриваются в данном обновленном издании от признанного авторитета в области Windows Марка Минаси и команды экспертов по Windows Server, возглавляемой Кевином Грином. Настоящая книга поможет быстро освоить все новые средства и функции Windows Server, а также включает реальные сценарии развертывания. Если вы — системный администратор, которому необходимо перейти к Windows Server 2012 R2 и управлять им или же модернизировать его, то в этом полном пособии вы найдете все, что нужно.

Вы изучите следующие темы

- Установка или модернизация и последующее управление сервером Windows Server 2012 R2
- Настройка объединения сетевых интерфейсных плат Microsoft NIC Teaming 2012 и работа с PowerShell
- Установка операционной системы через графический пользовательский интерфейс или обновленную версию Server Core 2012
- Миграция, слияние и модификация Active Directory
- Управление адресным пространством с помощью IPAM
- Новые общие хранилища, пространства хранения и улучшенные инструменты для работы с ними
- Управление доступом к общим файлам — новый и усовершенствованный подход
- Использование и администрирование Remote Desktop, Virtual Desktop и Hyper-V

С помощью этой книги вы

- научитесь планировать установку и управлять сервером Windows Server 2012 R2
- ознакомитесь с советами и пошаговыми руководствами от гуру по Windows Марка Минаси и его команды экспертов
- узнаете, что появилось нового в Active Directory и PowerShell
- освоите виртуализацию с помощью усовершенствованных возможностей Hyper-V и VDI
- переведете управление хранилищем на новый качественный уровень
- закрепите свой уровень знаний на реальных примерах

Марк Минаси (MCSE) — один из гуру по Windows во всем мире. Он преподает в 15 странах и очень популярен как лектор на конференциях и итоговых отраслевых обзорах. Фирма Марка Минаси, MR&D, обучила десятки тысяч людей проектированию и запуску в производство сетей Windows. Марк выступал автором и соавтором многочисленных книг, включая популярные издания *Mastering Microsoft Windows Server 2008 R2* и *The Complete PC Upgrade and Maintenance Guide*.

В томе 1 были описаны новые возможности сервера, установка Windows Server 2012 R2, организация сетей и компоненты IP Address Management и DHCP Failover, Active Directory в Windows Server 2012 R2, общее хранилище, кластеризация и динамическое управление доступом.

Категория: серверные решения Microsoft
Предмет рассмотрения: Windows Server 2012 R2
Уровень: для пользователей средней и высокой квалификации

ISBN 978-5-8459-1936-6

9 785845 919366 15015

ДИАЛЕКТИКА
www.dialektika.com

SYBEX
A Wiley Brand
sybex.com