Том 1

Основные темы тома

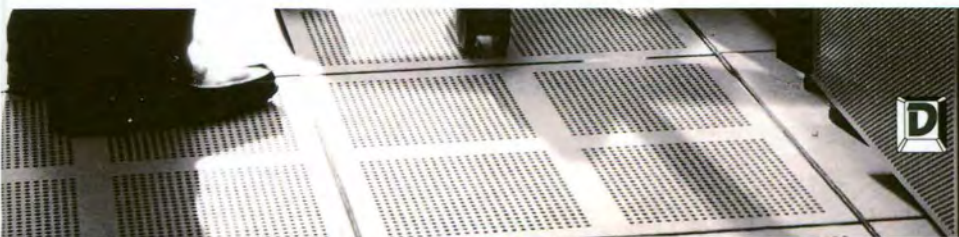
- новые возможности и установка Windows Server 2012 R2, включая Server Core
- организация сетей и компоненты IP Address Management и DHCP Failover
- Active Directory в Windows Server 2012 R2 и выполнение задач по управлению учетными записями
- общее хранилище и кластеризация, создание и управление общими ресурсами, а также развертывание динамического управления доступом

Windows Server 2012 R2

Полное руководство

УСТАНОВКА И КОНФИГУРИРОВАНИЕ СЕРВЕРА, СЕТИ, DNS, ACTIVE DIRECTORY И ОБЩЕГО ДОСТУПА К ДАННЫМ И ПРИНТЕРАМ

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 1
УСТАНОВКА И КОНФИГУРИРОВАНИЕ СЕРВЕРА, СЕТИ, DNS, ACTIVE DIRECTORY И ОБЩЕГО ДОСТУПА К ДАННЫМ И ПРИНТЕРАМ

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

Диалектика

Москва • Санкт-Петербург • Киев
2015

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

Windows Server 2012 R2. Полное руководство. Том 1: установка и конфигурирование сервера, сети, DNS, Active Directory и общего доступа к данным и принтерам. : Пер. с англ. — М. : ООО "И.Д. Вильямс", 2015. — 960 с. : ил. — Парал. тит. англ.

Научно-популярное издание

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

Windows Server 2012 R2. Полное руководство. Том 1:
установка и конфигурирование сервера, сети, DNS,
Active Directory и общего доступа к данным и принтерам

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

Подписано в печать 15.12.2014. Формат 70×100/16.
Гарнитура Times.
Усл. печ. л. 60,0. Уч.-изд. л. 65,75.
Тираж 500 экз. Заказ № 7071.

Отпечатано способом ролевой струйной печати
в ОАО «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 978-5-8459-1935-9 (рус., том 1)
ISBN 978-5-8459-1934-2 (рус., многотом.)
ISBN 978-1-1182-8942-6 (англ.)

Оглавление

Содержание

Благодарности

Коллектив авторов хотел бы поблагодарить Гевина Мак-Шира за его обширную помощь и конструктивную критику как научного редактора (блог Гевина доступен по адресу `mcshera.com`), а также литературному редактору Тому Сиртину, которому довелось возиться с нашими широко варьирующимися черновиками, приводя их в печатную форму. Мы выражаем благодарность производственному отделу в Wiley: менеджеру редакторов Питу Гогену, редактору по сбору данных Мариэнн Барсоло, производственному редактору Ребекке Андерсон, литературному редактору Линде Ректенуолд и корректору Саре Кейкини.

Авторы

Выражаю особую благодарность моей прекрасной жене Лоре за ее терпение и поддержку на протяжении тех многих часов, пока я писал свои главы для этой книги! Конечно, большое спасибо двум моим сыновьям, Мэттью и Дилану, кто обеспечивал мне раннее пробуждение на выходных, чтобы продолжать написание!

Благодарю Мариэнн Барсоло и Пита Гогена за то, что привлекли меня к работе над этой книгой и предоставили возможность взаимодействовать с фантастическими техническими умами на протяжении всего процесса. Я обнаружил, что работа с другими авторами, участниками и редакторами в этом проекте очень вдохновляла, даже несмотря на то, что нам пришлось переписать половину книги для учета выпуска R2!

Еще одну благодарность хочу выразить моим коллегам в Ergo, давшим мне возможность поработать над проектами производственного уровня, которые помогли получить опыт, необходимый для написания книги вроде этой.

Наконец, я хотел бы посвятить работу над этой книгой своему тестю Сесилу Андерсону, который был мне как отец на протяжении многих лет. Его сила и смелость служат источником вдохновения для всех нас.

Кевин Грин

Я хотел бы поблагодарить свою семью за поддержку. Казалось, на эту книгу потрачена целая вечность, и многие выходные приходилось проводить за клавиатурой, занимаясь написанием глав. Я очень благодарен за ваше терпение. Люблю вас всех! За мужество!

Кристиан Бус

Я хотел бы выразить благодарность моей жене Николь и нашим двум сыновьям Алексу и Майлзу. Ваша любовь и поддержка помогают мне во всем, что бы я ни делал.

Роберт Батлер

Хочу поблагодарить мою жену Шерон и наших троих детей, Софи, Адама и Сэма, за их терпение на протяжении последнего года. Ох, как непросто найти баланс между беспокойной рабочей нагрузкой и семейной жизнью!

Джон Мак-Кейб

Прежде всего, я выражаю благодарность Кевину Грину за то, что он предоставил мне возможность работать над этой книгой и направлял меня на первых порах. Также особо благодарю мою жену Симону за ее терпение и принятие того факта, что многие часы я тратил на книгу, а не на нее!

Наконец, я благодарю свою семью за, друзей и мою компанию, itnetx, за поддержку меня во многих отношениях, чтобы я мог шагать в ногу с проектом.

Стефан Рот

Об авторах

Марк Минаси — автор множества бестселлеров, популярный обозреватель технологий, комментатор, ведущий докладчик и IT-консультант. Впервые он получил шанс поработать с компьютером в университетской группе в 1973 году. В то время он узнал две вещи.

- Во-первых, компьютеры искусны. (Люди до сих пор говорят "искусны", прямо как в 1973 году. Эй, это же было в XX веке.)
- Во-вторых, многие технические специалисты — очень хорошие люди, но они способны мгновенно вогнать вас в сон, объясняя технические понятия.

Марк воплотил эти две вещи в своей карьере, делая компьютеры и организацию сетей проще и интереснее для понимания. Он добивался этого путем написания тысяч обзоров, нескольких десятков технических книг, ставших бестселлерами, а также объяснением планирования, установки, обслуживания и восстановления операционных систем и сетей для людей числом от двух до двух тысяч. Согласно независимому мнению, провозглашенному издателем CertCities об "излюбленном техническом авторе" четыре раза из четырех, Марк обладает необыкновенной возможностью взять даже самую технически сложную тему, отфильтровать назойливую рекламу и объяснить ее на обычном языке. Вероятно, именно по этой причине, когда компания TechTarget наняла его для ведения веб-трансляций по настройке ПК, он привлек в три раза больше слушателей, чем любые предыдущие веб-трансляции, катастрофически перегрузив серверы Yahoo. По тем же соображениям Марка приглашали выступать с основными докладами на сотнях конференций, организованных для технических специалистов по всему миру.

Наибольшую известность Марку принесли его книги *Mastering Windows Server* и *Complete PC Upgrade and Maintenance Guide*, которые претерпели свыше 12 изданий и были проданы числом более 1 миллиона экземпляров.

Юмористичный, провокационный и содержательный стиль Марка делает его любимцем зрителей по всему миру. При содействии своей фирмы, MR&D (`www.minasi.com`), Марк предлагает технические семинары, учебные курсы и лекции, а также технический форум. Вы также можете подписаться на получение информационного бюллетеня.

Кевин Грин, являющийся лидирующим автором этой книги, имеет звание Microsoft MVP для управления облаком и центром данных посредством системного центра и работает в индустрии IT с 1999 года. Он нанят в качестве эксперта предметной области в системном центре Ergo в Дублине (Ирландия). В этой роли он взаимодействует с клиентами, строя решения производственного уровня с помощью Windows Server и системного центра. В прошлом Кевин работал IT-администратором, IT-инженером, главой технической бригады и старшим консультантом. Он проходил программы сертификации Microsoft еще со времен Windows NT 4.0 и обладает квалификацией, включающей MCSE, MCSA, MCITP, MCP и MCTS. Кевин — активный участник сообщества Windows Server and System Center (WSSC) посредством своего блога по адресу `http://kevingreeneitblog.blogspot.com`, и его также можно найти в Твиттере как `@kgreeneit`.

Он регулярно поставляет презентации и участвует в подкастах по Windows Server и системному центру, а также является соавтором книги *Mastering System Center 2012 Operations Manager* (Sybex, 2012 г.).

Кевин живет в Саллинсе (графство Килдэр, Ирландия) со своей женой Лорой и двумя сыновьями, Мэттью и Диланом. Когда он не работает за ноутбуком, он уделяет свободное время семье и болеет за Манчестер Юнайтед. Кевин также является обладателем черного пояса второй ступени в кикбоксинге свободного стиля, и хотя уже не так увлечен спортом, как когда-то, он по-прежнему является заядлым последователем боевых искусств.

Кристиан Бус ранее имел звание Microsoft MVP по дисциплине System Center: Cloud and Datacenter Management (Системный центр: управление облаком и центром данных), и недавно ушел работать с полной занятостью в Microsoft на должность старшего программного менеджера в бригаде, занимающейся системным центром, и сосредоточился на программе Cloud and Datacenter Management MVP.

На протяжении прошедших 17 лет Кристиан работал руководителем отдела, ведущим техническим архитектором и инженером по решениям в округе Сиэтла. Его опыт и внимание было всегда ориентировано на платформу Microsoft со специализацией на системном центре, Windows Server и виртуализации.

Кристиан привлекался в качестве эксперта предметной области, писателя экзаменационных материалов, разработчика учебных курсов и технического рецензента во многих официальных учебных программах Microsoft (Microsoft Official Curriculum — MOC). Дополнительную информацию о Кристиане можно почерпнуть по адресу `http://about.me/chbooth`.

Роберт Батлер в течение последних 17 лет был IT-профессионалом. Он работает в компании Affirma Consulting, где специализируется на интеграции разнообразных частей стека системного центра Microsoft в существующие среды.

Он являлся обладателем звания Microsoft Certified Professional на протяжении прошедших 16 лет, а в настоящее время имеет множество других сертификатов Microsoft, в числе которых MCSE PC, MCSA 2012, MCITP EA и MCTS для SCCM 2012. Роберт живет в Сиэтле (штат Вашингтон) со своей женой Николь и двумя детьми, Алексом и Майлзом. Дополнительные сведения о нем можно узнать в его блоге по адресу `http://rbutler.me` или отслеживать его в Твиттере как `@robert_butler`.

Джон Мак-Кейб работает в Microsoft главным инженером по эксплуатации. Благодаря своей роли, он взаимодействует с рядом крупнейших мировых компаний, которые поддерживают разнообразные технологии, охватывая широкий спектр от унифицированных коммуникаций до частного облака и все, что посередине. До присоединения к Microsoft он обладал сертификатом MVP по унифицированным коммуникациям.

Джон живет в Ирландии со своей женой Шерон и тремя детьми, Софи, Адамом и Сэмюелем. В свободное от работы время он обучается боевым искусствам, а именно — Будзинкан будо тай-дзюцу, а когда позволяет время, увлекается виниловыми проигрывателями.

Роберт Панек — независимый консультант, сделавший успешную карьеру в индустрии IT и разработке программного обеспечения. Начиная с 1995 года, Роберт работал в таких компаниях, как AIG, L-3, Radianse и IPOSyndicate, а в 2000 году его работа была удостоена премии "Best of the Web" ("Лучшая в веб"), учрежденной журналом *Forbes Magazine*, на протяжении четырех кварталов подряд. Из-за своих огромных достижений в IPOSyndicate, он был выдвинут на должность руководителя технического отдела.

На протяжении 19 лет работы в сфере IT Роберт достиг квалификации MCP, MCSA, MCSE, MCSD — веб-приложения и MCDBA, а его опыт наряду с наставничеством начинающих IT-профессионалов привели его в издательство Sybex с целью дальнейшего обучения и сертификации учащихся.

В настоящее время Роберт живет в Нью-Гемпшире со своей женой Дженни.

Майкл Райс продолжает преуспевать как талантливый и успешный администратор центра данных в компании-подрядчике министерства обороны Intelligent Software Solutions Inc.

Он специализируется на лидирующих методах для корпоративных структур в областях виртуализации, хранения и администрирования систем. На протяжении последних 8 лет, будучи IT-профессионалом, Майкл получил множество сертификатов в сфере IT, таких как MCP, MCTS, MCSA, MCSE, VCP 5 и Net +, а также был обладателем многочисленных наград за выдающуюся производительность и стремление к совершенству.

Майкл живет в штате Колорадо со своей женой Джессикой и двумя замечательными детьми, Кристен и Энтони. Он планирует однажды стать сертифицированным инструктором и в дальнейшем приспосабливать свою карьеру под обучение технологиям других IT-профессионалов по всему миру.

Стефан Рот работает архитектором частного облака в itnetx gmbh, консультационной и инженерной компании, находящейся в Швейцарии, которой корпорацией Microsoft было присуждено звание "Partner of the Year — Datacenter" ("Партнер года — центр данных") в 2011, 2012 и 2013 годах. Он появляется на технических мероприятиях и тесно взаимодействует со своими заказчиками и Microsoft, пропагандируя технологии облака и центров данных.

Работая в отрасли IT последние 13 лет, Стефан ранее трудился инженером систем и консультантом в национальных и интернациональных компаниях, где получил огромный опыт в управлении центрами данных. Основными объектами его внимания являются Active Directory, System Center Operations Manager и System Center Orchestrator, и он имеет сертификаты от Microsoft по дисциплинам MCITP: Enterprise Administrator (MCITP: администратор предприятия) и MCSE: Private Cloud (MCSE: частное облако).

Дополнительная информация о Стефане доступна в его блоге по адресу `http://blog.scomfaq.ch` или в Твиттере как `@scomfaq`.

Введение

Добро пожаловать в книгу, посвященную Windows Server 2012 R2. Все усовершенствования и новые средства, которые предлагает эта флагманская операционная система производственного уровня от Microsoft, определенно поднимают планку будущих версий Windows Server. Чтобы уловить, насколько много возможностей вы получаете с Windows Server 2012 R2, вам нужно только взглянуть на первоначальный выпуск Windows Server 2012, который достиг общей готовности в сентябре 2012 года. Вскоре после поступления данной версии в продажу издательство Sybex собрало группу авторов для написания книги по этой версии, но как только мы подошли к этапу финального редактирования глав, в Microsoft анонсировали выход версии Windows Server 2012 R2 в октябре 2013 года — всего лишь спустя 12 месяцев после выпуска Windows Server 2012. За этот короткий период в версии Windows Server 2012 R2 появился настолько большой объем новой функциональности, что нам пришлось буквально переписать около половины первоначальной книги, посвященной предыдущей версии Windows Server 2012!

Коллектив авторов, работающих над этой книгой, обладал обильным опытом проектирования, развертывания, управления и устранения неполадок Windows Server в крупномасштабных производственных средах, и они с радостью расскажут вам все о данной версии продукта.

Если вы являетесь новичком в Windows Server, эта книга предоставит вам багаж знаний, требуемых для того, чтобы немедленно приступить к самостоятельной работе. Если вы — опытный администратор или консультант и уже знакомы с этой операционной системой, волноваться не стоит; вы определенно найдете здесь массу новой информации, чтобы уверенно держаться во главе стаи.

Кто должен читать эту книгу?

Подобно любой другой книге из серии *Mastering Windows Server*, мы ориентировали эту книгу на тех, кто стремится узнать, как устанавливать, конфигурировать, обслуживать и устранять неполадки в среде Windows Server. Мы предполагаем, что у вас есть, по крайней мере, базовое понимание построения стандартных сетей TCP/IP и базовый опыт работы с предшествующими версиями графического пользовательского интерфейса Windows, в частности, консоли управления Microsoft (Microsoft Management Console — MMC).

Из-за возрастающей сложности программных продуктов никто не способен быть экспертом по всем ним. Если вы похожи на большинство администраторов, то располагаете временем на изучение только тех сведений о продукте, которых достаточно для того, чтобы им можно было эффективно управлять. Тем не менее, с любым продуктом, как правило, можно делать много чего еще. Эта книга позволит вам быстро продвигаться в обучении и поможет разобраться в некоторых наиболее загадочных вопросах.

Не каждый администратор имеет дело с одним и тем же типом рабочей инфраструктуры. То, что работает хорошо в крупной корпорации, не всегда работает в небольших компаниях. С другой стороны, то, что хорошо подходит для небольших компаний, может не очень удачно масштабироваться в крупных организациях. В Microsoft попытались сгладить отличия между компаниями и предложили продукт,

который может быть быстро внедрен в небольшой компании, и в то же самое время хорошо масштабироваться для крупных организаций. Независимо от того, какой сценарий вам больше подходит, вы заинтересованы в изучении, как этот продукт будет работать для вашего блага.

Что внутри?

В связи с типографскими особенностями книга разбита на два тома. В первый том вошли главы 1–16, а во второй том – главы 17–32 и приложение.

Глава 1 начинается с обзора новых возможностей операционной системы Windows Server 2012 R2, а в главе 2 показано, как ее устанавливать на серверах и начать интеграцию с существующей сетью при ее наличии.

Ветераны сетей Windows будут ожидать, что ОС Windows Server 2012 R2 окажется похожей на другие версии Windows, с рабочим столом, меню Start (Пуск) и семейством графических инструментов, но, как вы вскоре увидите, появился совершенно новый графический пользовательский интерфейс. В главе 3 приводится введение в Server Core, и мы рекомендуем уделить время на изучение материалов этой главы. В главе 4 рассматриваются усовершенствования организации сетей в Windows Server 2012 R2, а в главе 5 дается введение в новую функциональность IPAM и DHCP Failover. В главе 6 рассказывается в системе DNS, отвечая на вопрос: "Как построить инфраструктуру DNS, которая является безопасной и настроенной на наилучшее обслуживание Active Directory?"

В главе 7 начинается описание Active Directory — важнейшей технологии Windows Server, с объяснением метода построения наиболее распространенного и простого типа среды Active Directory, содержащей всего один домен и единственную площадку. Даже если вы собираетесь строить огромные, охватывающие весь земной шар среды AD, здесь приводятся необходимые основы, поэтому ни в коем случае не пропускайте эту главу. После настройки среды AD вам понадобится создавать и управлять учетными записями пользователей, чему посвящена глава 8. После построения работающей среды AD возникает необходимость уделить определенное внимание работе всего проектного решения и настройки, и для этого предусмотрен инструмент Group Policy (Групповая политика). Хорошая новость заключается в том, что Group Policy предоставляет великолепный способ централизованного управления как десятью, так и десятью тысячами машин с учетными записями пользователей; плохая же новость — инструмент Group Policy может быть довольно сложным, но материал в главе 9 поможет справиться с этим. Еще одна глава, касающаяся AD, — глава 10 — посвящена службам федерации Active Directory (Active Directory Federation Services), которые позволяют предоставить доступ с единым входом к ресурсам через организационные границы.

В главах 11 и 12 будет дано введение в общее хранилище и кластеризацию, которые являются опорными компонентами по обеспечению IT-инфраструктуры с высокой готовностью для бизнеса, а также введение в новые возможности по работе с SAN в Windows Server 2012 R2, применяя пространства хранения.

В главах 13–15 предлагается последовательность, состоящая из трех частей, по открытию совместного использования для файлов и папок в Windows Server, которая начинается с основ открытых папок и файлов и применения средств безопасности Windows для управления доступом к конкретным файлам. Затем рассматривается динамическое управление доступом (Dynamic Access Control), которое представляет

собой новый способ управления и аудита доступа к открытым файловым ресурсам. Многие серверы обслуживают не только файлы, но также и общие принтеры, поэтому в главе 16 показано, как достичь этого в Windows Server 2012 R2.

В главе 17 рассказывается о том, как обслуживать и управлять серверами дистанционным образом, используя несколько встроенных технологий, в числе которых Remote Desktop. К этому времени у вас уже будут работающие серверы (что хорошо), но не будет клиентов, которые бы пользовались их службами (что делает эти серверы несколько бессмысленными). Именно поэтому в главе 18 рассматриваются вопросы связывания разнообразных машин Windows, созданных за прошедшее десятилетие, в сеть Windows Server 2012 R2. Что вы говорите? У вас есть Mac? Нет проблем, вы узнаете, как подключить также и его.

В главе 19 описана настройка и запуск одного из наиболее сложных серверных дополнений Windows — служб Microsoft Internet Information Services (IIS), которые лучше известны как веб-сервер. Будет показано, как запустить IIS, настроить простой веб-сайт и работать с инструментами управления IIS, встроенными в Windows Server 2012 R2.

В главе 20 обсуждаются вопросы содействия системы Windows Server 2012 R2 задаче маршрутизации IP. Это может показаться странной темой, но только до тех пор, пока вы не примете во внимание, что должны немного понимать маршрутизацию IP в Windows Server, прежде чем вы сможете освоить материал главы 21, в которой показано, как с применением системы Windows Server 2012 R2 настроить виртуальную частную сеть. В главе 21 вы также освоите действительно замечательную функциональность DirectAccess, которая в готовом виде доступна сразу после установки Windows Server 2012 R2.

Далее наступает время возвратиться к Active Directory и ознакомиться с рядом более сложных тем, на что выделены четыре следующих главы. Глава 22 посвящена добавлению в AD сведений о множестве местоположений с рассмотрением сайтов, связей сайтов и подсетей в стиле AD. И если вы располагаете несколькими сайтами, то на некоторых сайтах установка контроллера домена может оказаться рискованной — именно по этой причине предусмотрены контроллеры домена только для чтения (RODC); вы узнаете о них в главе 23. Затем в главе 24 рассказывается об усложнении инфраструктуры AD за счет добавления одного, двух или ста дополнительных доменов. Слияния, поглощения или просто набившие оскомину реорганизации могут потребовать придания AD новой формы в манере, которая будет отнюдь не простой, если только вы не изучите миграции доменов, хронологии SID и доверительные отношения — обо всем этом пойдет речь в главе 25. Продолжая тему Active Directory, глава 26 предоставит более подробные сведения о расширенном управлении и поддержке учетных записей пользователей.

Возможно, вы уже читали о том, что технология Hyper-V является значительным компонентом в Windows Server 2012 R2, поэтому данная книга не могла бы претендовать на полноту без пары глав по этой теме — таковыми являются главы 27 и 28. Даже если вы не планируете внедрять виртуализацию, загляните в эти главы, поскольку материал в них поможет понять саму технологию и проблемы в виртуализации серверов, что представляет собой область, знать которую обязательно.

В главе 29 мы пройдем через процесс установки, использования и администрирования служб Remote Desktop Services, что поможет в проектировании и обеспечении оптимального решения по удаленному доступу и публикации приложений внутри организации.

К этому моменту вы потратили немало времени на настройку и приведение сервера в рабочее состояние, так что вы готовы к изучению финальных глав этой книги, 30–32, которые посвящены мониторингу производительности, применению исправлений и резервному копированию системы.

Заключительные комментарии

Удостоверьтесь, что располагаете достаточным временем на освоение операционной системы Windows Server 2012 R2. Чем лучше вы ее будете знать, тем больше сможете с ее помощью делать. В самом конце каждой главы вы найдете контрольные вопросы, которые помогают закрепить материал, изложенный в главе. Предусмотрены инструкции по созданию небольшой экспериментальной среды. Построение экспериментальной среды пригодится при проработке новой темы или устранении проблемы. Прежде всего, старайтесь получать удовольствие от процесса изучения материалов, представленных в этой книге. Как только вы обнаружите, насколько большую мощь предлагает вам этот продукт, вы будете приятно поражены теми вещами, которые он позволяет делать.

От издательства

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш веб-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас. Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

E-mail: info@dialektika.com

WWW: http://www.dialektika.com

Информация для писем из:

России: 127055, г. Москва, ул. Лесная, д. 43, стр. 1

Украины: 03150, Киев, а/я 152

Глава 1

Новые возможности Windows Server 2012 R2

Операционная система (ОС) Windows Server 2012 R2 имеет свыше 300 новых функциональных возможностей, и это первая серверная ОС от Microsoft, которая обладает средством подключения к облаку. Объяснение всех этих возможностей потребовало бы гораздо больше одной главы (что и стало причиной написания настоящей книги), но давайте воспользуемся несколькими страницами в начале, чтобы обрисовать положение вещей. Мы осознаем, что некоторые читатели всего лишь начитают свое знакомство с Windows Server, и для них новым является *абсолютно все*. Однако многим другим уже известна масса информации об организации сетей на основе Windows, и они хотели бы просто получить сводку о новых возможностях Windows Server — в настоящей главе приведены сведения о том, что и где можно найти в данной книге.

К этому времени мы наблюдали буквально несметное количество презентаций от Microsoft, посвященных Windows Server, и все они начинались одинаково, так что, по всей видимости, мы обязаны по закону (или, по крайней мере, по обычаю) представить следующий список в качестве первой рубрики в предлагаемом обзоре.

В этой главе рассматриваются следующие темы:

- существенные изменения в пользовательском интерфейсе;
- новые возможности Active Directory, улучшающие развертывание и обслуживание;
- усовершенствования PowerShell;
- новая технология, добавленная в Hyper-V;
- усовершенствования в организации сетей на основе Windows, делающие сети более быстрыми и защищенными;
- новые инструменты управления;
- важные возможности IIS 8.0.

Введение в Windows Server 2012 R2

Из слогана "Built from the cloud up" ("Построена из облака") несложно выяснить, для чего была задумана ОС Windows Server 2012 R2. Так что же собой представляет облачная технология? Коротко говоря, это практика использования для хранения, управления и обработки данных сети удаленных серверов, а не локального сервера. ОС Windows Server 2012 R2 распространяет такие технологии на корпорации, чтобы они могли обеспечить их применение своими сотрудниками.

Все корпоративные данные, использующие либо виртуальные машины, либо отдельные рабочие станции, могут быть сохранены непосредственно в облаке либо на сайте, либо за его пределами. Облачные технологии являются движущей силой современного стиля ведения бизнеса и останутся таковой в ближайшем будущем.

Начиная с небольших компаний и заканчивая крупнейшими центрами данных, ОС Windows Server 2012 R2 стала хитом сезона. Предлагая буквально сотни новых средств для виртуализации, организации сетей, хранения, удобства в эксплуатации и многого другого, ОС Windows Server 2012 R2 вас не разочарует. Чем дольше мы ею пользуемся, тем больше она нам нравится, и мы думаем, что вы не станете исключением!

В последующих разделах предлагается краткий обзор материалов, приведенных в настоящей книге. Поскольку это вводная глава, все упомянутые в ней темы будут подробно рассматриваться в других местах книги.

Редакции Windows Server

Когда была выпущена ОС Windows Server 2012, существовал выбор между редакциями Standard и Datacenter в обеих версиях, Server Core и GUI (с графическим пользовательским интерфейсом). С выходом Windows Server 2012 R2 на выбор стали доступны две дополнительных редакции: Foundation и Essentials. Каждая версия обладает разными возможностями, что отражено в цене лицензии на нее. Давайте обсудим отличительные особенности всех редакций.

Редакция Standard

Это облачный сервер производственного класса, который является флагманской ОС. В настоящей главе будут детально раскрыты изменения, внесенные в редакцию Standard, поскольку она представляет собой наиболее популярный выбор. Такой сервер обладает развитой функциональностью, и он будет поддерживать практически все общие потребности в организации сетей. Сервер редакции Standard может применяться для многоцелевых или индивидуальных ролей. Он может быть усечен вплоть до одного своего ядра для получения еще более зашищенной и высокопроизводительной рабочей лошадки.

Редакция Datacenter

Это сверхмощная версия сервера виртуализации от Microsoft. Данную редакцию лучше всего использовать в высоко виртуализированных средах, т.к. она предлагает неограниченные права виртуальных экземпляров. Именно так: неограниченные! В действительности это единственное отличие редакции Datacenter от Standard и, разумеется, оно сказывается на цене; редакция Datacenter стоит примерно в четыре раза дороже редакции Standard.

Редакция Foundation

Редакция Foundation содержит большинство ключевых средств из других редакций, но прежде чем ее развертывать, следует уяснить ряд важных ограничений. Роли службы сертификатов Active Directory ограничены только центрами сертификации. Ниже перечислены другие ограничения.

- Максимальное количество пользователей составляет 15.
- Максимальное количество подключений Server Message Block (SMB) равно 30.
- Максимальное количество подключений Routing and Remote Access (RRAS) составляет 50.
- Максимальное количество подключений Internet Authentication Service (IAS) равно 10.
- Максимальное количество подключений Remote Desktop Services (RDS) Gateway составляет 50.
- Разрешено только одно гнездо центрального процессора (ЦП).
- Не допускается хостинг виртуальных машин и не разрешено использование этой редакции в качестве гостевой виртуальной машины.

Редакция Essentials

Данный сервер предназначен для очень мелких компаний, насчитывающих не более 25 пользователей и 50 устройств. Это достаточно эффективный по цене способ организации небольших бизнес-сетей. Ниже перечислены некоторые (но не все) новые возможности редакции Essentials ОС Windows Server 2012 R2.

- Усовершенствованное развертывание клиентов.
- Возможность установки в качестве виртуальной машины или в виде сервера.
- Управление группами пользователей.
- Улучшенная хронология файлов.
- Доступность средства BranchCache.
- Возможность использования управляющей панели для управления мобильными устройствами.
- Доступность средства System Restore.

Изменения в рабочем столе

В Windows Server 2012 разработчики из Microsoft удалили кнопку Start (Пуск), которая располагалась в левом нижнем углу. В версии R2 кнопка Start была возвращена на свое место, так что можно снова получать доступ к меню приложений. Для доступа к этому меню можно по-прежнему нажимать клавишу <Windows>, если вы уже привыкли поступать так. На тот случай, если вы не знакомы с этой клавишей: на стандартной клавиатуре она находится слева от левой клавиши <Alt>. Существует также горячая точка в правом нижнем углу, которая вызывает отображение вертикальной панели меню. Это динамическое меню содержит следующие кнопки: меню Start, параметры настройки рабочего стола и поиск посредством Explorer.

Привыкание к новому внешнему виду и поведению может потребовать некоторого времени, но мы думаем, что вам понравятся изменения в пользовательском интерфейсе. Диспетчер серверов (Server Manager) был подвергнут крупной реконструкции, и он привлечет ваше внимание своими красочными предупреждающими сообщениями в управляющей панели, отображаемыми при возникновении проблем.

Одним из востребованных пользователями средств, отсутствующих в Windows Server, была возможность переключения между версией GUI и Server Core. Требования часто изменяются, что может вызвать необходимость в переходе на Server Core. Ранее для этого приходилось выполнять полную повторную установку Server Core. Теперь администратор имеет возможность преобразования версии GUI в Server Core и наоборот.

Дополнительные сведения по этому поводу будут встречаться повсюду в книге, начиная с главы 2.

Изменения в Active Directory

Как вам может быть известно, службы Active Directory (AD) во многих отношениях являются краеугольным камнем организации сетей Windows; другими словами, они формируют центральную базу данных для аутентификации пользователей и машин. Версия AD в Windows Server 2012 R2 включает множество удобных новых возможностей для службы сертификатов Active Directory (Active Directory Certificate Services), службы управления правами Active Directory (Active Directory Rights Management Services) и службы доменов Active Directory (Active Directory Domain Services). Все вместе новые возможности ориентированы на развертывание и обслуживание. План состоит в том, чтобы сделать развертывание служб Active Directory быстрым и простым, и получить более гибкий доступ к файлам одновременно с лучшей их защитой. Средства администрирования также усовершенствованы, обеспечивая администрированию с помощью графического пользовательского интерфейса и посредством сценариев большую согласованность и дружественность к пользователю. Дополнительные сведения об этом можно найти в главе 7.

Изменения в Active Directory Domain Services

В Microsoft всегда стремились делать Active Directory Domain Services (AD DS) более надежной службой структуры каталогов. В последующих разделах объясняются улучшенные возможности, относящиеся к Active Directory Domain Services.

Клонирование контроллеров доменов

ОС Windows Server 2012 R2 снабжает вас возможностью клонирования существующего контроллера домена для ускорения развертывания. Используя интерфейс контроллеров доменов в диспетчере серверов, можно поднять одиночный виртуальный контроллер домена. Затем внутри того же домена можно развернуть дополнительные виртуальные контроллеры доменов.

Клонирование сократит количество повторяющихся шагов в процессе развертывания. Оно также позволит развертывать дополнительные контроллеры доменов, сконфигурированные и авторизованные посредством Active Directory. Это достигается путем создания копии виртуального контроллера домена с последующей авто-

ризацией исходного контроллера и запуском соответствующих командлетов Windows PowerShell. Командлеты Windows PowerShell создадут конфигурационный файл с инструкциями повышения. Этот файл будет содержать информацию Domain Name Server (DNS), имя, IP-адрес и другие сведения, относящиеся к делу.

За дополнительной информацией обращайтесь в главу 7.

Улучшения в детализированной политике для паролей

Служба Active Directory выполняет множество задач помимо хранения списка имен и паролей пользовательских учетных записей, но если бы нам пришлось выбирать наиболее важную задачу, то мы бы по справедливости отметили защиту и поддержание паролей.

До выхода Windows Server 2008 проблема, с которой все мы сталкивались, заключалась в том, что все в домене должно было следовать одним и тем же правилам для паролей. Таким образом, административный персонал должен был следовать таким же правилам для паролей, как, например, персонал, занимающийся продажами. Администраторы должны знать, каким способом защитить свои пароли, лучше продавцов. В противном случае лучше поискать новых администраторов!

В версии Windows Server 2008 были представлены детализированные политики паролей. Это позволяет назначать отдельным группам разные политики паролей. Итак, теперь администраторы могут иметь свои политики, а персонал, отвечающий за продажи — свои.

В Windows Server 2012 R2 детализированные политики паролей были улучшены, так что теперь появилась возможность создавать и администрировать свои объекты параметров паролей (password-settings object — PSO), используя административный центр Active Directory (Active Directory Administrative Center). Эта новая возможность помогает упростить управление объектами PSO. До появления версии Windows Server 2012 R2 все объекты PSO должны были создаваться с применением инструмента ADSI Edit (Редактор Active Directory Schema Interface (Интерфейс схемы Active Directory)). Дополнительные сведения об этом также приведены в главе 7.

Корзина Active Directory

Мы считаем, что объяснить функциональность корзины Active Directory (Active Directory Recycle Bin) лучше всего на реальном примере, показав, как эта технология может спасти положение.

Джон — младший администратор в Wiley Books. Ему понадобилось несколько часов, чтобы добавить 20 новых авторов в Active Directory. Позже, когда работа была завершена, он случайно удалил одну из организационных единиц (Organizational Unit — OU) компании.

Резервное копирование данных в Wiley проводится каждую ночь с использованием утилиты Microsoft Windows Backup. Из-за этого восстановление Active Directory осуществляется по принципу "все или ничего". Утилита Microsoft Windows Backup не предоставляет возможности восстановления только OU. Таким образом, поскольку необходимо восстановить Active Directory, Джон потерял бы результаты нескольких часов своей работы, т.к. восстановилась бы версия Active Directory из предыдущей ночной резервной копии на ленте. Именно здесь на помощь приходит корзина Active Directory. Благодаря корзине Active Directory, Джон смог просто восстановить OU, не возвращаясь к другой точке во времени из-за применения резервной копии.

Посредством использования нового графического пользовательского интерфейса корзины администраторы теперь могут легко отменять удаление объектов Active Directory, не проходя через утомительный процесс, который приходилось бы делать в Windows Server 2008. На рис. 1.1 показана корзина Active Directory в действии.

За дополнительной информацией о корзине Active Directory обращайтесь в главу 7.

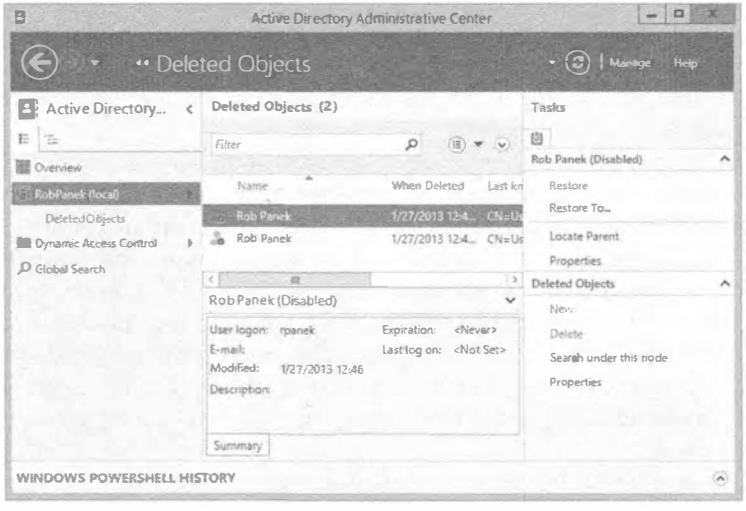


Рис. 1.1. Графический пользовательский интерфейс корзины Active Directory

PowerShell и административный центр Active Directory

С наступлением эпохи Windows компания Microsoft поставляла операционные системы, административные инструменты которых имели главным образом инструменты, основанные на графических интерфейсах; в действительности многие администраторы в Windows могут неделями не открывать окно командной строки. Положительный момент в том, что освоение администрирования в Windows новичками будет проще, чем это было бы при попытке изучить администрирование в Unix/Linux, поскольку эта группа ОС в большей степени зависит от административных инструментов командной строки, нежели от таких инструментов, основанных на графическом пользовательском интерфейсе.

Однако ориентация на командную строку в мире Unix/Linux означает то, что автоматизировать выполнение административных задач в Unix/Linux проще, чем делать это для аналогичных задач в Windows. (Инструкции командной строки можно поместить в пакетный файл, который затем позволит автоматизировать выполнение любой необходимой задачи. Понятно, что щелчки кнопками мыши зафиксировать в пакетном файле не получится.) Таким образом, в Microsoft пытаются предоставить отсутствующую в Windows "возможность автоматизации", присущую Unix и Linux, предлагая командную оболочку под названием PowerShell. Он предназначен для простой автоматизации выполнения утомительных и повторяющихся задач. До настоящего момента кривая обучения работе с PowerShell была довольно крутой.

В Windows Server 2012 R2 появился браузер хронологии PowerShell, который позволяет администраторам применять административный центр Active Directory для просмотра выполненных команд Windows PowerShell.

Ниже перечислены усовершенствования, внесенные в PowerShell 3.0:

- рабочий поток Windows PowerShell;
- веб-доступ Windows PowerShell;
- новые возможности интегрированной среды сценариев (Integrated Scripting Environment — ISE) в Windows PowerShell;
- поддержка для Microsoft .NET Framework 4.0;
- поддержка для заранее установленных сред Windows;
- отключенные сеансы;
- надежная подключаемость сеансов;
- обновляемая справочная система;
- расширенная онлайновая справочная система;
- интеграция с общей информационной моделью (Common Information Model — CIM);
- файлы конфигурации сеансов;
- запланированные задачи и интеграция с планировщиком задач (Task Scheduler);
- языковые расширения Windows PowerShell;
- новые базовые командлеты;
- усовершенствования сушествующих основных командлетов и поставщиков;
- удаленный импорт и обнаружение модулей;
- расширенное завершение по нажатию клавиши <Tab>;
- автозагрузка модулей;
- улучшения в использовании модулей;
- упрошенное обнаружение команд;
- усовершенствованная регистрация в журналах, диагностика и поддержка групповой политики (Group Policy);
- улучшения в форматировании и выводе;
- расширенный хостинг консоли;
- новые командлеты и API-интерфейсы хостинга;
- улучшения производительности;
- поддержка возможности Run As (Запуск от имени) и разделяемого хостинга;
- усовершенствованная обработка специальных символов.

Как можно понять по длинному списку улучшений, в Microsoft намерены сделать PowerShell (рис. 1.2) такой же важной платформой для администрирования, как и сушествующие на сегодняшний день инструменты с графическим пользовательским интерфейсом.

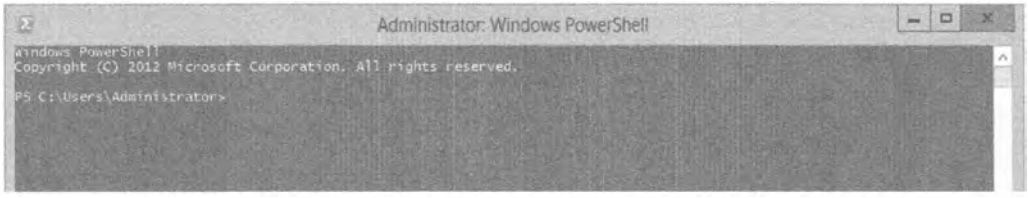


Рис. 1.2. Использование PowerShell для установки серверной роли

Средство PowerShell еще будет неоднократно упоминаться в этой книге, начиная с главы 2, где оно применяется для добавления ролей и функций.

Служба Active Directory Rights Management Services

Передача зашищенных документов и файлов внутри компании жизненно важна для целостности информации компании. Например, финансовый директор компании может составить отчет со списком сотрудников и получаемых ими зарплат. Финансовый директор желает, чтобы доступ к этому файлу имели только другие руководители компании. Именно здесь для защиты файла будет вызвана служба управления правами Active Directory (Active Directory Rights Management Services — AD RMS). С помощью AD RMS финансовый директор может зашифровать файл или применить к нему аутентификацию.

До выхода Windows Server 2012 R2 устанавливать службу AD RMS разрешалось только пользователю с привилегиями локального администратора на компьютере, на котором размещена база данных SQL Server. Причина заключалась в том, что во время установки службе AD RMS необходимо было читать настройки SQL Server из реестра. Во взаимодействие с AD RMS и способ доступа к SQL Server были внесены следующие изменения.

- Служба AD RMS теперь требует наличия у установщика полномочий системного администратора в установленной копии SQL Server.
- С целью обнаружения всех доступных экземпляров SQL Server должна быть запущена служба просмотра SQL Server.
- Любые порты, используемые установкой AD RMS на компьютере с SQL Server, должны иметь разрешенные исключения брандмауэра. Потребуется разрешить TCP-порт (стандартный порт 1433) для экземпляра SQL Server и UDP-порт (стандартный порт 1434) для службы просмотра SQL Server (SQL Server Browser Service).

Другая часть процесса установки AD RMS была модернизирована. В предыдущих версиях Windows Server развертывание приходилось выполнять из компьютера, где была установлена служба AD RMS. В Windows Server 2012 R2 разрешено удаленное развертывание на целевые серверные компьютеры. Дополнительные сведения о службе AD RMS будут предоставлены, начиная с главы 7.

Служба Active Directory Certificate Services

Идентичность служб, устройств и людей можно привязать к секретному ключу, используя службу сертификатов Active Directory (Active Directory Certificate Services — AD CS). Это расширенное средство зашиты разрешает доступ только участвующим приложениям, которые поддерживают AD CS.

Ниже перечислены некоторые изменения, внесенные в Windows Server 2012 R2.

- Интеграция с диспетчером серверов.
- Развертывание и управление с использованием Windows PowerShell.
- Службы ролей AD CS могут быть запущены в редакции Server Core на компьютере с любой версией Windows Server 2012 R2.
- Автоматическое обновление сертификатов теперь поддерживается для соединенных компьютеров, не находящихся в домене.
- Принудительное применение обновления сертификатов с одним и тем же ключом.
- Поддержка международных имен доменов.
- Служба ролей CA имеет усиленную защиту по умолчанию.

Дополнительные сведения о службе AD CS будут предоставлены, начиная с главы 7.

Виртуализация

Виртуализация позволяет размещать несколько операционных систем на одной физической машине. В прошлом необходимо было использовать четыре сервера для контроллера домена, Exchange Server, сервер DNS и сервер DHCP. Теперь можно иметь один физический системный блок и четыре виртуальных сервера. Это сохраняет денежные ресурсы (на оборудовании) и пространство (четыре сервера ранее и один сервер сейчас). Виртуализация в Windows Server 2012 R2 продолжает совершенствоваться.

Hyper-V

Виртуализация сервера — разбиение одного физического сервера на группу *виртуальных машин* — входит в число наиболее значительных изменений в управлении серверами за последние 10 лет. Формулировка "управление серверами" (а не "управление Windows Server") применяется потому, что виртуализация касается не только Windows Server, а также разнообразных видов Linux, Unix, Sun Solaris и т.д. Наличие возможности приобретения одного большого, мощного, надежного комплекта оборудования и затем представление его так, как если бы взамен было 10 или 20 небольших аппаратных фрагментов, с последующей установкой отдельных серверных ОС на этом "виртуальном серверном оборудовании" значительно упрощает управление серверами для крупных и мелких операций. Более того, она решает проблему управления серверами, которая годами мучила планировщиков по использованию пространства в помещениях: недогруженное оборудование. Инструмент, который заставляет думать о компьютере так, как если бы он был группой отдельных компьютеров, в общем случае называется *диспетчером виртуальных машин* (virtual machine manager — VMM).

Можно заметить, что с момента начала серверных вычислений большинство организаций предпочитают помещать каждую серверную функцию — электронную почту, контроллер домена AD, файловый сервер, веб-сервер, сервер баз данных — на собственный отдельный физический сервер. Таким образом, если требуется контроллер домена, веб-сервер и сервер электронной почты, обычно пришлось бы приобрести три серверных компьютера, установить на каждом из них ОС Windows Server

и сделать один контроллером домена, другой — веб-сервером (включив на сервере службу Internet Information Services, представляющую собой программное обеспечение встроенного в Windows Server 2012 R2 веб-сервера), а третий — Exchange Server.

Недостаток такого подхода связан с тем, что каждый из трех серверов, скорее всего, будет функционировать с довольно низким уровнем загрузки: не должен вызывать удивление тот факт, что контроллер домена отнимает около 5% максимальной мощности ЦП, веб-сервер — немного больше, а сервер электронной почты — еше чуть больше. Функционирование такого количества физических серверов с недогруженными возможностями означает напрасную трату электроэнергии, и дело тут не только в энергосбережении. В противоположность этому, приобретение одного большого физического сервера и применение VMM для его разделения на (к примеру) три виртуальных сервера, вероятно, привело бы к получению физического сервера, который работает на полную мощность, экономит электроэнергию и удовлетворяет всем нуждам организации.

Прежде всего, давайте рассмотрим новую технологию, добавленную в этой версии. Поскольку усовершенствований внесено в Hyper-V очень много, мы лишь кратко коснемся каждой из них.

- Клиент Hyper-V предлагает настольную технологию Windows Hyper-V без необходимости в установке серверной ОС.
- Модуль Hyper-V для Windows PowerShell предоставляет более 160 командлетов, предназначенных для управления Hyper-V.
- Инструмент Hyper-V Replica позволяет реплицировать виртуальные машины между системами хранения, кластерами и центрами данных на двух сайтах. Это помогает обеспечивать непрерывность бизнеса и восстановление после аварий.
- Измерение ресурсов помогает отслеживать и собирать данные об использовании сети и ресурсов на определенных виртуальных машинах.
- Упрощенная аутентификация группирует администраторов в локальную группу доступа. За счет этого для доступа к Hyper-V понадобится создавать меньшее число пользователей.
- Виртуализация ввода-вывода с единым корнем (single-root I/O virtualization — SR-IOV) — это новая возможность, которая позволяет назначать сетевой адаптер непосредственно виртуальной машине.
- Миграция хранилищ позволяет перемещать виртуальные жесткие диски по разным физическим хранилищам во время функционирования виртуальной машины.
- Совместное использование файлов SMB 3.0 — это новая возможность, которая предоставляет виртуальным машинам совместно используемые хранилища без применения сети хранения данных (storage area network — SAN).
- Виртуальный оптоволоконный канал (Fibre Channel) позволяет виртуализировать рабочую нагрузку и приложения, которые требуют прямого доступа к хранилищу, основанному на оптоволоконном канале. Также появляется возможность конфигурирования кластеризации непосредственно внутри гостевой ОС (иногда это называют гостевой кластеризацией).

- Виртуальная архитектура неоднородной памяти (Non-Uniform Memory Architecture — NUMA) позволяет некоторым высокопроизводительным приложениям, выполняемым на виртуальной машине, использовать топологию NUMA для оптимизации производительности.

А теперь кратко взглянем на ряд улучшений, внесенных в существующую технологию Hyper-V, которые многие администраторы сочтут удобными.

- Динамическая память позволяет конфигурировать интеллектуальный страничный обмен (Smart Paging), что предоставляет виртуальным машинам возможность более эффективного перезапуска. Если виртуальная машина имеет меньше начальной памяти, для ее поддержки можно сконфигурировать динамическую память.
- Отрегулировано импортирование виртуальных машин с целью улучшения обработки проблем с конфигурацией, которые обычно предотвращают импорт. До сих пор процесс включал копирование виртуальной машины, но никогда не предусматривал проверку проблем, связанных с конфигурацией.
- Живые переносы делают возможным завершение переноса в некластеризованной среде. Это улучшение упростит перемещение активной виртуальной машины.
- Данная версия предлагает более объемные ресурсы хранения, увеличенную масштабируемость и улучшенную обработку аппаратных ошибок. Все это предназначено для того, чтобы помочь в конфигурировании крупных высокопроизводительных виртуальных машин с возможностью масштабирования.
- Формат виртуальных жестких дисков (Virtual Hard Disk Format — VHDX) увеличивает максимальный размер хранилища каждого виртуального жесткого диска. Новый формат поддерживает объем хранилища до 64 Тбайт. Он также поступает со встроенной аппаратной защитой от сбоев электропитания. Вдобавок этот формат предотвращает ухудшение производительности на физических дисках с большими секторами.
- Больше нет необходимости в завершении работы активной виртуальной машины с целью восстановления удаленного пространства из хранилища. Виртуальные машины теперь освобождают пространство потребляемого снимка после того, как он удален.

Дополнительные сведения ищите в главе 27.

Удаленные или устаревшие элементы в Windows Server 2012 R2

Механизм VM Chimney, также называемый TCP Offload, был удален и больше не доступен гостевым ОС. Пространство имен WMI-интерфейса `root\virtualization` изменилось на `root\virtualization\v2` и, в конце концов, будет полностью устранено из будущих версий Windows Server. Диспетчер авторизации (Authorization Manager — AzMan) объявлен в этой версии устаревшим и будет постепенно исчезать из будущих выпусков. Новым стандартом станут новые инструменты управления для виртуальных машин.

Инфраструктура виртуальных рабочих столов

В Windows Server 2012 R2 разработчики из Microsoft внесли огромное количество усовершенствований в инфраструктуру виртуальных рабочих столов (virtual desktop infrastructure — VDI), упростив администрирование, увеличив значимость и в целом улучшив удобство работы пользователей.

В условиях современного рынка поддержка мобильных устройств является обязательной. Инфраструктура виртуальных рабочих столов помогает заполнить брешь в совместимости между устройствами путем виртуализации ресурсов. Инфраструктура VDI предоставляет более строгую защиту и высокую эффективность, что улучшает продуктивность работы с пользовательским интерфейсом, который хорошо знаком потребителю. ОС Windows Server 2012 R2 и VDI делают простым развертывание виртуальных ресурсов на устройствах.

При функционировании в центре данных инфраструктура VDI в Windows Server 2012 R2 разрешает доступ мобильным устройствам с использованием Hyper-V и службы удаленных рабочих столов (Remote Desktop Services). В одном решении от Microsoft предлагаются три разных типа развертывания: рабочие столы из пула, персональные рабочие столы и сеансы удаленных рабочих столов.

Дополнительная информация о VDI приведена в главе 27.

Изменения в организации сетей

От серверов было бы мало пользы, если бы отсутствовала возможность их взаимодействия друг с другом, но — что естественно — возможности взаимодействия с другими системами присущ и недостаток: *инфицированные* системы могут попытаться распространить вредоносное программное обеспечение. ("Хотите защитить свой сервер? Легко... Отключите кабель Ethernet!") ОС Windows Server 2012 R2 предлагает несколько изменений в организации сетей, которые делают работу сети Windows немного быстрее и безопаснее.

EAP-TTLS

В Windows Server 2012 R2 появился эксклюзивный протокол типа EAP (Extensible Authentication Protocol — расширяемый протокол аутентификации) под названием TTLS (Tunneled Transport Layer Security — туннелированная защита транспортного уровня). Данный протокол используется с аутентифицированным проводным и беспроводным доступом по стандарту 802.1X. Этот новый основанный на стандарте протокол предоставляет зашищенный туннель для аутентификации клиентов. Стандарт 802.1X обеспечивает щит безопасности, который предотвращает неавторизованный доступ в интрасеть.

DNS

Хотя система DNS существовала всегда, процесс, согласно которому она транслировала имена, с каждой версией заметно улучшался. Изменения в Windows Server 2012 R2 оказывают влияние и на DNS Server (Сервер DNS), и на DNS Client (Клиент DNS). Давайте кратко рассмотрим изменения, внесенные в Windows Server 2012 R2.

В PowerShell появились некоторые улучшения в плане управления DNS. Например, роль DNS Server получила ряд усовершенствований по ее установке и

удалению с применением PowerShell. Другие разработки в PowerShell включают пользовательский интерфейс, клиентский запрос и конфигурацию сервера в старых ОС. Тайм-аут запроса LLMNR составлял 300 миллисекунд, что было недостаточно для компьютеров, находящихся в режиме сохранения электропитания. Благодаря новым усовершенствованиям DNS Client, тайм-аут был увеличен до 820 миллисекунд.

Инфраструктура IP Address Management

Инфраструктура IPAM (IP Address Management — управление IP-адресами) — это новый набор технологий для управления, мониторинга и аудита пространства IP-адресов. За счет мониторинга DHCP и DNS инфраструктура IPAM может находить серверы IP-адресов внутри сети и дать возможность управлять ими из единого центрального пользовательского интерфейса.

Технология NIC Teaming

Технология NIC Teaming (Объединение сетевых интерфейсных плат) в Windows Server 2012 R2 может взять несколько сетевых интерфейсных плат (NIC) и объединить их вместе, чтобы взаимодействовать с ними как с одной платой. Это помогает в ситуации сбоя, когда одно из устройств становится неработоспособным. При объединении сетевых интерфейсных плат также улучшается балансировка нагрузки, потому что полосы пропускания индивидуальных NIC комбинируются в единую более широкую полосу пропускания.

Дополнительные сведения по этим темам и новым средствам можно найти в главах 4 и 5.

Инструменты управления

Любая качественная сетевая ОС должна предлагать способы упрощения работы по поддержанию одного или тысячи серверов в работоспособном состоянии. Кроме того, сервер должен функционировать с минимально возможными усилиями со стороны со стороны персонала, занимающегося его администрированием. За администрирование отвечает не только одна операционная система, но версия Windows Server 2012 R2 в этом отношении стала немного лучше за счет появления ряда удобных новых инструментов.

Диспетчер серверов

До выхода Windows Server 2008 для конфигурирования и обслуживания сервера администратор вынужден был пользоваться *множеством* разных инструментов. В версии Windows Server 2008 положение дел изменилось благодаря вводу диспетчера серверов — многоцелевого средства, предоставляющего доступ ко всем инструментам конфигурирования и управления в одном месте.

В версии Windows Server 2012 R2 разработчики из Microsoft расширили эту функциональность даже больше (рис. 1.3). Диспетчер серверов теперь позволяет администраторам управлять несколькими серверами (виртуальными или физическими, локальными или удаленными) при условии, что на них установлена версия ОС не старее Windows Server 2003.

Добавление ролей и средств к диспетчеру серверов стало еще интеллектуальнее. По мере выбора вами опций мастер добавления ролей и компонентов (Add Roles and Features Wizard) динамически изменяется. Этот мастер помогает принять решение о том, какое подмножество инструментов и средств необходимо для затребованной роли.

Диспетчер серверов имеет новую управляющую панель, которая может сообщать о наличии проблем с использованием квадратов с цветовым кодированием.

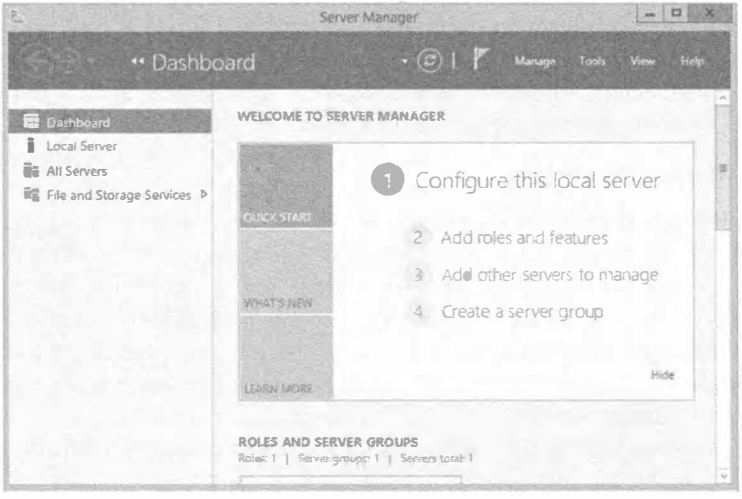


Рис. 1.3. Окно диспетчера серверов

Например, если произошла ошибка, зафиксированная в журнале событий DNS, то квадрат DNS в управляющей панели отобразится красным цветом. Это великолепный инструмент для поиска и устранения неисправностей на сервере, и поскольку управляющая панель является первым окном, которое вы видите при входе на сервер, ей непременно следует уделить внимание.

Раз уж речь зашла о поиске и устранении неисправностей, то диспетчер серверов для этого имеет массу новых инструментов, которые будут рассматриваться более подробно в главе 2. Все эти инструменты находятся внутри роли в диспетчере серверов, так что вам не придется открывать множество инструментов вроде Event Viewer (Просмотр событий) или Performance Analyzer (Анализ производительности), чтобы увидеть результат — все они в одном месте!

Диспетчер серверов более подробно описан в главе 2.

Дистанционные инструменты: WinRM и WinRS

Часто новые ОС включают действительно важные и удобные средства, которые оказываются в основном незамеченными. ОС Windows Server 2012 R2 содержит одно из таких ловких, но в значительной степени неизвестных средств в новом сетевом протоколе, которое называется удаленным управлением Windows (Windows Remote Management — WinRM). Чтобы понять, почему WinRM является отличным средством, следует принять во внимание, для замены чего оно предназначено — протокола, известного как вызов удаленных процедур (Remote Procedure Call — RPC).

Даже если вы никогда ранее не слышали о протоколе RPC, скорее всего, вы пользовались им на протяжении многих лет. Работа RPC заключается в том, чтобы позволить одной программе взаимодействовать с другой, даже когда эти программы выполняются на разных компьютерах. Например, если вы когда-либо запускали Outlook для чтения электронной почты из экземпляра Exchange Server, то применяли протокол RPC: именно так Outlook может хлопнуть Exchange по плечу и спросить "Могу ли я получить свою электронную почту?". Вы также использовали протокол RPC, когда применяли такие оснастки консоли MMC, как DNS, DHCP или Computer Management (Управление компьютером), для дистанционного управления этими функциями на удаленном компьютере со своего рабочего стола.

Протокол RPC на протяжении многих лет предоставлялся большим числом службами, но ему была присуща одна крупная проблема: его трудно было защитить. Специалисты в Microsoft изобрели протокол RPC в дни, когда не было Интернета, и подавляющее большинство локальных сетей распространялось не далее, чем в пределах от первого до последнего этажа офисного здания, поэтому безопасность вообще не считалась существенной проблемой. Спустя годы, когда безопасность стала крупной проблемой, в Microsoft попытались внедрить защиту в протокол RPC за счет внесения ряда необязательных изменений, отточенных в Windows XP SP2. Однако к тому моменту, как говорится, джин был уже выпущен из бутылки, и требование безопасности RPC просто привело бы к нарушению работы сотен, а то и тысяч приложений, зависящих от RPC.

Очевидно, наступило время для изменения способа взаимодействия Windows-программ друг с другом, так что в Microsoft решили принять протокол, который делает то же, что и RPC, но с несколькими изменениями.

- Он не является патентованным, но основан на стандартах и не зависит от платформы — существуют похожие реализации в Linux и Mac OS.
- Он представляет собой модифицированную форму протокола HTTPS.
- Коммуникации с его участием зашифрованы.
- Он требует для своего использования аутентификацию.

Компоненты Windows Server 2012 R2, использующие WinRM, включают коллекцию журналов событий, возможность применения новой оснастки для диспетчера серверов на удаленных серверах, а также защищенную удаленную командную оболочку под названием Windows Remote Shell, или `winrs`. Если вам нужен защищенный инструмент с низкой полосой пропускания, обратите внимание на `winrs`. За более детальными сведениями относительно WinRM обращайтесь в главу 17.

Служба Remote Desktop Services

В Windows Server 2012 R2 разработчики из Microsoft предприняли крупные шаги в плане улучшения пользовательского интерфейса и интерфейса управления. Разработчики из Microsoft намеревались усовершенствовать пользовательский интерфейс вне зависимости от вида устройства, используемого для подключения. Они желали обеспечить, чтобы подключения через региональную или локальную сеть (к виртуальным рабочим столам, программам RemoteApp или рабочим столам, основанным на сеансах) предоставляли пользователям полноценный интерфейс. Разработчики из Microsoft также хотели улучшить управление удаленными рабочими

столами. Мы согласны с тем, что они достигли своих целей за счет добавления централизованной консоли, поэтому администраторы могут управлять службой удаленных рабочих столов (Remote Desktop Services) из единственного местоположения.

Дополнительные сведения о службе Remote Desktop Services приведены в главе 17.

Усовершенствования объектов групповых политик

Что стало лучше? Многое. Благодаря консоли управления групповой политикой (Group Policy Management Console) управление объектами групповых политик (Group Policy Object — GPO) упростилось. В предыдущих версиях Windows у администраторов была проблема с обновлением GPO вручную. Несмотря на то что объекты GPO автоматически обновлялись каждые 90 минут, возникали ситуации, когда нужно было обеспечить эффект от объекта GPO незамедлительно. Администраторам приходилось перемещать этот объект на нужный компьютер и запускать утилиту `gpupdate.exe` в командной строке для ручного обновления GPO.

Теперь, чтобы вручную обновить GPO, администратор может воспользоваться контекстным меню для организационной единицы (OU) в консоли управления групповой политикой и запланировать запуск `gpupdate.exe` на множестве компьютеров одновременно. Кроме того, указанное действие можно осуществить с применением командлета `Invoke-GPUpdate` в PowerShell.

Ниже описаны дополнительные изменения, касающиеся групповой политики, в Windows Server 2012 R2.

- При мониторинге проблем с репликацией на уровне домена больше не требуется загружать и запускать отдельные инструменты.
- Для устройств, функционирующих под управлением Windows RT, теперь можно конфигурировать локальную групповую политику. По умолчанию она отключена, а служба должна быть запущена и настроена на автоматический запуск.
- Групповая политика была модернизирована для поддержки Internet Explorer 10.

Дополнительные сведения о групповой политике будут даны в главе 9.

Совместное использование файлов и принтеров

До того как мы запускали веб-службы или службы электронной почты на серверах Windows, мы применяли Windows Server только для разделения двух вещей: жестких дисков большого объема и дорогостоящих принтеров. Файлы и принтеры — это старейшие службы, предлагаемые сетями Microsoft, но очевидно не настолько старые, чтобы не изучить несколько новых приемов.

BranchCache

Технология BranchCache предназначена для оптимизации полосы пропускания региональной сети за счет копирования содержимого либо из главного местоположения, либо из облачного сервера в офис филиала. После того, как содержимое скопировано в филиал, пользователи могут получать к нему доступ локально, а не через региональную сеть. Наличие возможности кеширования файлов сберегает полосу пропускания и улучшает защиту. Технология BranchCache может поддерживать офис любого размера и не ограничивается их количеством. Развернуть BranchCache мож-

но с единственным объектом групповой политики (GPO). Эта технология использует файловый сервер Windows для деления файлов на небольшие зашифрованные порции. Преимущество деления файлов на небольшие порции связано с тем, что клиентские компьютеры могут загружать только те порции, которые изменились. Вдобавок BranchCache выполняет проверку на предмет дублирования содержимого и загружает только один экземпляр содержимого, сохраняя дисковое пространство.

Усовершенствования технологии BranchCache в Windows Server 2012 R2 включают автоматическое конфигурирование клиентских компьютеров, а также существенное увеличение производительности и масштабируемости. Клиентские компьютеры могут быть сконфигурированы с применением объекта групповой политики. Если GPO не был настроен для BranchCache, то BranchCache проверит сервер размещенного кеша, и по умолчанию будет использовать его настройки.

Одним из новых преимуществ BranchCache является возможность предварительной загрузки специфичного содержимого, подобного медиа-носителю или DVD, на сервер размещенного кеша и обеспечения дальнейшей его отправки клиентскому кешу.

Еще одним преимуществом следует считать усовершенствования, внесенные с целью улучшения производительности баз данных. Для этого в BranchCache используется расширяемый механизм хранения (Extensible Storage Engine — ESE). Это та же самая технология баз данных, которая применяется в Microsoft Exchange Server. Она позволяет масштабировать единственный сервер размещенного кеша для обработки увеличивающегося числа запросов от большего количества пользователей без наращивания оборудования.

Серверы размещенного кеша больше не нуждаются в сертификате сервера, выданном центром сертификации (certificate authority — CA). Это значительно сокращает денежные затраты, связанные с развертыванием открытого ключа с множеством CA.

SMB 3.0

Служба файлового сервера Windows имеет официальное название SMB, означающее Server Message Block (Блок сообщений сервера). (Вина за такое неудачное название лежит на IBM, а не на Microsoft, поскольку эта служба первоначально была спроектирована в IBM.) За почти 25 лет своего существования служба SMB изменялась мало. Самые крупные изменения касались поддержки блоков больших размеров для использования сетей быстрее 100 Мбит/с (в 2000 г.), возможности обработки множества маршрутов и добавления цифровых подписей, чтобы защититься от атак типа "человек посередине" (в 2001 г.).

В Windows Server 2012 R2 присутствует несколько переделанная версия SMB, которая лучше работает с медленными сетями, более интеллектуально поддерживает шифрование, ловко использует полосу пропускания при передаче файлов и поддерживает PowerShell.

Диспетчер ресурсов файлового сервера

Для управления данными, хранящимися на файловом сервере, предназначены инструменты, которые доступны в диспетчере ресурсов файлового сервера (File Server Resource Manager). Некоторые из этих инструментов помогают автоматизировать классификацию, а также формирование отчетов и управление файлами и квотами.

Благодаря инфраструктуре классификации файлов (File Classification Infrastructure), как части динамического управления доступом (Dynamic Access Control), можно управлять и проводить аудит доступа к файлам на файловом сервере. Теперь обеспечивается более высокий контроль над способом классификации файлов на файловых серверах. С помощью расширенных средств классификацию файлов можно проводить вручную или автоматически.

Дополнительную информацию по этой теме можно найти далее в книге, начиная с главы 13.

Службы, основанные на веб

Наконец, имеется подмножество средств Интернета, которые стали более важными, чем все остальное взятое вместе в Сети: веб и связанные с ним службы. Они важны для Windows, и в версии Windows Server 2012 R2 они претерпели ряд крупных изменений.

Веб-сервер IIS

Файловые службы Windows могли и не изменяться на протяжении многих лет, но это не касается *веб-сервера* Windows. Одним из ключей к зашите любого серверного продукта является сведение к минимуму объема кода, который виден из Интернета. Например, если веб-сервер поддерживает средство под названием FastCGI, но вебсайт в нем *не нуждается*, то зачем запускать FastCGI на сервере, открытом для Интернета, и идти на риск того, что злоумышленник отыщет способ применения FastCGI из IIS для взлома сервера? Очевидно, что подобное не имеет смысла, и было бы неплохо исключить из программного обеспечения веб-сервера те компоненты, которыми вы не собираетесь пользоваться. (Специалисты в области безопасности называют это "минимизацией поверхности атаки". Иногда нам кажется, что они слишком часто играют в Halo.)

Идеальный веб-сервер тогда бы состоял из десятков небольших модулей, каждый из которых по мере необходимости можно было бы добавлять или удалять, что позволило бы веб-администратору строить сервер, в точности соответствующий существующим потребностям, но не больше. Эта цель была путеводной звездой для IIS 7.0 в Windows Server 2008 — полностью переделанной версии IIS, включающей набор последних технологий защиты, в том числе WinRM. (Именно этот протокол, а не RPC используется при выполнении удаленного администрирования машины с IIS 7.)

Взлом IIS 7.0

Насколько нам известно, пока еще никто не взломал IIS 7, равно как и версию IIS 7.5, которая представляет собой обновление, поставляемое в составе Windows Server 2008 R2. Веб-администраторам также нравится ясный и ориентированный на задачи интерфейс инструментов администрирования IIS 7.x.

Зная, сколько компаний на современном рынке буквально дышат Интернетом, мы ожидали от Microsoft не меньшего, чем вращение их технологии вокруг веб-сервера. С выпуском Windows Server 2012 R2 поступает новейшая версия веб-сервера, IIS 8.0 (рис. 1.4).

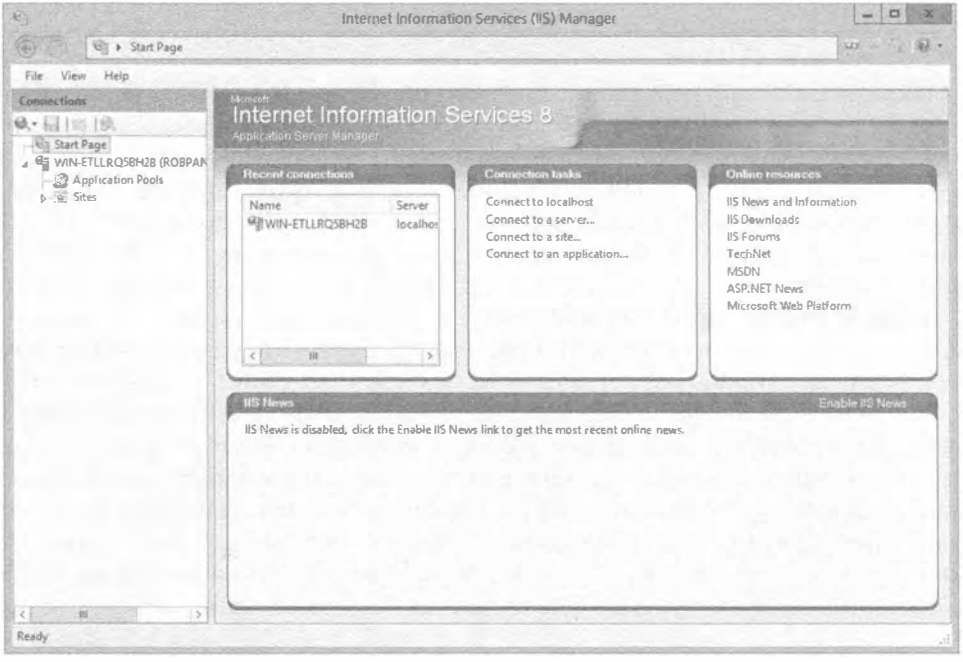


Рис. 1.4. Новый инструмент управления IIS

В IIS 8.0 было добавлено множество новых средств, предназначенных для администрирования и защиты веб-сайтов. Ниже перечислены некоторые важные изменения, внесенные в IIS 8.0:

- инициализация приложений;
- ограничения динамических IP-адресов;
- централизованная поддержка сертификатов SSL;
- плавная регулировка ЦП;
- ограничения на попытки входа через FTP;
- поддержка индикации имен серверов (Server Name Indication — SNI);
- улучшенный протокол SSL и масштабируемость конфигурации;
- поддержка многоядерного масштабирования на оборудовании NUMA.

Даже если вы по профессии — создатель веб-страниц, никогда не помешает разобраться в работе текущего веб-сервера Windows, поэтому не пропустите главу 19.

Консоль управления Microsoft канула в лету!

В Windows Server 2012 R2 оснастка консоли управления Microsoft (Microsoft Management Console — MMC) для диспетчера Internet Information Services (IIS) Manager 6.0 объявлена устаревшей. В будущих выпусках Windows Server она будет удалена.

Сервер FTP

Разработчики из Microsoft делают что-то правильно, а что-то неправильно. В редких случаях вещи делаются в высшей степени неправильно, как это было со встроенным программным обеспечением сервера FTP (File Transfer Protocol — протокол передачи файлов), который поставлялся с ОС Windows в течение последних 15 лет или около того. Он был весьма неуклюж, труден в конфигурировании и предлагал очень мало полезных журналов. Отсутствовала возможность настройки параметров, которые должны быть по определению простыми в конфигурировании (вроде домашних каталогов пользователей). Все эти факторы приводили тому, что любой, кому требовался FTP-сервер на основе Windows, вынужден был приобретать программное обеспечение для FTP-сервера у независимых разработчиков. Тем не менее, начиная с Windows Server 2008 и Windows Server 2008 R2, положение дел кардинально изменилось. Насколько мы можем видеть, в Microsoft отбросили весь старый код FTP-сервера и построили его с нуля. В Windows Server 2012 R2 также была добавлена возможность ограничения количества неудачных попыток входа, которые можно делать для учетной записи FTP на протяжении определенного периода времени. Таким образом, если необходим FTP-сервер, основанный на Windows, ознакомьтесь с материалом в главе 19, где описаны возможности нового сервера FTP.

Дополнительные сведения об управлении веб-сервером приведены в главе 19.

Глава 2

Установка и модернизация до версии Windows Server 2012 R2

Опытные администраторы и консультанты по Windows Server могут испытывать желание пропустить эту главу. Вы можете посчитать, что снова проходить данный материал нет необходимости. Мы призываем вас дважды подумать, прежде чем принимать такое решение. В главе раскрываются основы, но также даются детали, которые вы, возможно, еще не знаете и найдете их полезными.

Вашим первым опытом работы с Windows Server, скорее всего, была ручная установка этой ОС на экспериментальной или виртуальной машине. В зависимости от сложности среды и ваших планов по модернизации, вы можете решить продолжить установку вручную или автоматизировать ее. Независимо от того, какой вариант был выбран, имеет смысл прочитать эту главу, чтобы ознакомиться с типичными шагами по установке.

В настоящей главе будет рассмотрена чистая ручная установка и ручная модернизация Windows Server. После этого мы углубимся в стратегии установки и модернизации для Active Directory. Если вам приходится выполнять многочисленные установки Windows Server, то вам понравится материал, который будет представлен следующим. Мы обсудим способы сохранения времени и нажатий клавиш на клавиатуре за счет автоматизации процесса установки Windows Server 2012 R2 с использованием файла ответов для автономной (не требующей вмешательства) установки, который создается с применением диспетчера образов системы Windows (Windows System Image Manager).

В этой главе вы узнаете, как решать следующие задачи:

- модернизация старых серверов;
- конфигурирование сервера;
- построение небольшой фермы серверов.

Что изменилось?

Мы уверены, что вы найдете процесс установки Windows Server 2012 R2 намного более простым, чем во всех предшествующих версиях Windows Server. Если вы уже устанавливали ОС Windows 8 или Windows Server 2008, то должны хорошо представлять себе, чего можно ожидать от установки Windows Server 2012 R2. Процедура установки в действительности была сокращена, чтобы запрашивать только базовые сведения и предоставить защищенную установку, которую можно затем настроить.

Давайте взглянем на последнее предложение. Это то, что вы могли слышать ранее, но не придали ему должного значения. Вы увидите такой подход непосредственно в Windows Server 2012 R2. Что он означает? Означает он то, что устанавливается намного меньший объем функциональности. При этом никаких предположений относительно того, что должно входить в данный сервер, не делается. Чистая стандартная установка Windows Server 2012 R2 в действительности мало что умеет. В ней отсутствует полезная функциональность. Вы сами должны решить, что этот сервер будет делать в сети, и какая *функциональность* должна быть установлена. В результате сервер имеет намного меньшую поверхность атаки. А это что значит? Дело в том, что чем больший объем функциональности устанавливается на компьютере, тем больше целей представляется атакующим. Задача состоит в том, чтобы устанавливать только требуемую функциональность, другими словами, сокращать количество целей или минимизировать поверхность атаки. Более того, с точки зрения безопасности операционная система блокируется по умолчанию. Первое, что происходит при первоначальной загрузке — запрос нового пароля администратора. Вы также обнаружите, что брандмауэр Windows (Windows Firewall) по умолчанию включен. Эта ОС очень сильно изолирует себя от сети до тех пор, пока не будет сконфигурирована. Вам предоставляется полный контроль над тем, каким образом новый сервер взаимодействует с сетью и/или с Интернетом.

Звучит ли это как то, что для сборки и запуска сервера придется выполнить немало работы? Может быть, но на самом деле разработчики из Microsoft сделали все довольно простым. Если вы проводите небольшое число ручных установок и модернизаций, то можете быстро сконфигурировать свои серверы с применением групповой политики (Group Policy) и диспетчера серверов (Server Manager). Речь о диспетчере серверов пойдет далее в главе. Если вы развертываете множество серверов, то должны рассмотреть варианты автоматизированных решений, такие как служба развертывания Windows (Windows Deployment Services) или предпочитаемое решение от третьей стороны. Опять-таки, для развертывания политик можно использовать групповую политику и версию диспетчера серверов с командной строкой, называемую PowerShell, в виде сценариев с целью настройки ролей и возможностей сервера.

Как насчет Server Core?

Установка Server Core операционной системы Windows Server чуть более подробно рассматривается в главе 3. Для конфигурирования функциональности, установленной на сервере, в установке Server Core применяется ряд отличающихся инструментов.

Каким образом вы собираетесь развертывать Windows Server 2012 R2? Здесь существуют некоторые сложности. ОС Windows Server 2012 R2 доступна только для 64-разрядных архитектур. В Microsoft решили сделать все свои серверные продукты только 64-разрядными. Это означает невозможность модернизации 32-разрядных установок Windows Server 2008. В таких случаях придется делать чистую установку на новом оборудовании и переносить любые службы или данные. При наличии 64-разрядных развертываний серверов модернизацию можно выполнять на месте. Это может сэкономить время, но обычно поступать так не рекомендуется. В Microsoft настоятельно призывают каждый раз проводить чистую установку. Тем не менее, если на вашем сервере функционируют только компоненты, роли и приложения производства Microsoft (и все они 64-разрядные), то модернизация на месте возможна. Мы делали это и впоследствии получали надежные серверы.

Требования к установке

В предшествующих версиях Windows Server могли существовать разные требования для каждой редакции ОС, выбранной для установки, т.е. Enterprise или Standard. В Windows Server 2012 R2 редакция Enterprise больше не доступна, а требования были сведены в один набор для всех редакций.

По обыкновению вместе с операционной системой получается набор минимальных и рекомендуемых требований. Учтите, что *минимальные* требования означают именно минимальные; ОС будет функционировать, но не обязательно эффективно. Должны приниматься во внимание и приложения, которые будут установлены, а также планируемая нагрузка на сервер.

Условия могут широко варьироваться в зависимости от приложений и организаций, поэтому не существует жестких правил относительно того, какими должны быть спецификации сервера. Лучшее, что можно сделать для получения точных спецификаций — это разработать экспериментальную среду и сгенерировать нагрузку на серверах "подтверждения концепции", одновременно выполняя мониторинг производительности и способности к реагированию серверов и приложений. Однако если ваш сервер по плану будет иметь умеренную нагрузку в небольшой среде, то, скорее всего, подойдут и рекомендуемые спецификации. В табл. 2.1 описаны требования для Windows Server 2012 R2, сформулированные Microsoft.

Аудит текущей инфраструктуры

Когда планируется крупное изменение, такое как развертывание серверной ОС, критически важно аккуратно провести аудит существующей инфраструктуры. Компания Microsoft предоставляет бесплатный комплект инструментов Microsoft Assessment and Planning Toolkit for Windows Server 2012 (`http://tinyurl.com/ycpuk3l`). Этот простой в использовании набор инструментов позволяет выполнять аудит серверов, а также проверять совместимость оборудования и драйверов. На основе этих сведений можно создавать отчеты для планирования любых изменений.

Поддержка 64-разрядного оборудования

ОС Windows Server 2012 R2 доступна только в виде 64-разрядного продукта. Еще раз: *версий x86 или 32-разрядных версий Windows Server 2012 R2 не существует.*

Таблица 2.1. Требования для Windows Server 2012 R2

Компонент	Минимальное требование	Рекомендуемое требование	Максимальное требование
ЦП	1,4 ГГц для x64	2 ГГц	64-ядерный процессор
ОЗУ	512 Мбайт	2 Гбайт или более	32 Гбайт для редакции Standard, 4 Тбайт для редакции Datacenter
Диск	32 Гбайт	40 Гбайт плюс дополнительное пространство для приложений или данных, 10 Гбайт для установки Server Core	
DVD-ROM	Требуется для доступа к носителю с копией устанавливаемой ОС; CD-ROM больше не поддерживается		
Дисплей	Super-VGA (800×600) или с более высоким разрешением		
Устройства ввода	Клавиатура и совместимое устройство указания, такое как мышь		
Доступ в Интернет	Требуется		

Ниже приведены некоторые замечания по развертыванию серверов x64.

- Аппаратная поддержка для x64 вряд ли является крупной проблемой: основные производители продают процессоры x64 в течение многих лет. Можно провести быстрый аудит серверного оборудования и проверить его на предмет 64-разрядной поддержки.
- Многие 32-разрядные приложения должны иметь возможность выполняться под управлением 64-разрядной ОС Windows Server 2012 R2: этому способствует эмулятор 32-разрядной среды, предоставляемый подсистемой Windows-on-Windows (WOW32). Не рассчитывайте только на нее; проконсультируйтесь с поставщиком приложения и проведите тестирование в экспериментальной среде, прежде чем формировать план модернизации серверов с Windows Server 2008 до Windows Server 2012 R2.
- Модернизация с x86 до x64 невозможна: это препятствует модернизации установки x86 версии Windows Server 2003 или Windows Server 2008 до Windows Server 2012 R2. Переход серверов с x86 на x64 потребует плана миграции с одного физического сервера на другой.
- 64-разрядные сборки Windows требуют драйверов режима ядра с цифровой подписью: конечно, ОС позволит установить другие драйверы, выдав соответствующее предупреждение, но в действительности они никогда не будут загружаться. Удостоверьтесь, что производитель оборудования предоставляет подходящим образом подписанные драйверы x64 для Windows Server 2012 R2. Очень часто пользователи жалуются в Microsoft на проблемы с драйверами, но на самом деле за драйверы отвечает производитель оборудования. Например, драйверы принтеров делают много такого, за чем следует следить.

Как в любом проекте, подготовка является ключом к успеху. Прежде чем переходить к развертыванию Windows Server 2012 R2, пересмотрите требования к оборудованию, а также проверьте совместимость приложений и служб.

Пример из практики

Итак, что вы собираетесь развертывать?

Многим, кому приходилось развертывать Windows Server 2008, известно, что поддержка оборудования x86 от Microsoft в центрах данных закончилась. Где только было возможно, развертывались сборки x64, и то же самое делалось для заказчиков. Ключевые программные продукты наподобие SQL Server 2008 имели собственные редакции x64. При развертывании Windows Server 2008 все равно разрабатывался проект по развертыванию ОС, поэтому многие посчитали это подходящим моментом для перехода на 64-разрядные решения. Конечно, иногда приходилось придерживаться сборок x86, т.к. это регламентировалось условиями поддержки приложений от независимых поставщиков. Это означало, что миграция будет проведена в более позднее время.

Проверьте оборудование, драйверы, возможность поддержки со стороны поставщиков приложений и принтеры. Протестируйте все в экспериментальной среде. Если все в порядке, разверните на сервере ОС Windows Server 2012 R2 в зависимости от имеющейся лицензии и проектных целей.

В экспериментальной среде может возникнуть желание взглянуть на решение для виртуализации от Microsoft — Hyper-V. Гипервизор Hyper-V включен как часть Windows Server 2012 R2; он позволяет запускать виртуальные машины с операционными системами x64 или x86, даже ОС Linux, поддерживающую гипервизор Xen. Кроме того, Hyper-V требует выполняемой с помощью ЦП виртуализации и включения в BIOS функции предотвращения выполнения данных (Data Execution Prevention — DEP). Мы рекомендуем воспользоваться этой технологией (или даже одним из конкурирующих вариантов, если вы отдаете ему предпочтение). Дополнительные сведения о Hyper-V буду приведены далее в этой книге.

Установка операционной системы

Первая установка Windows Server 2012 R2 в производственной или экспериментальной среде, вероятно, будет либо чистой установкой, либо модернизацией. Существует ряд других, более сложных способов установки Windows, которые перечислены ниже.

- Автономная установка: о ней речь пойдет позже в этой главе.
- Клонированная установка с применением средства ImageX из пакета автоматической установки Windows (Windows Automated Installation Kit).
- Одно из решений для развертывания от Microsoft, такое как служба развертывания Windows (Windows Deployment Services — WDS): это расширенная установка, выполняемая по сети с использованием функциональности, которая включена в Windows Server 2012 R2.
- Независимые решения: программное обеспечение (ПО) Ghost является классическим примером независимого решения для клонирования, которое работает в сочетании с инструментом `sysprep` от Microsoft.

Мы собираемся взглянуть на процессы чистой установки и модернизации. Ранее уже упоминалось, что процесс установки довольно прост.

Процесс чистой установки Windows Server 2012 R2 очень прост. По большому счету, будет предложено выполнить следующие действия.

1. Выберите язык, формат для представления времени и валюты, а также клавиатуру или метод ввода.
2. Выберите редакцию и сборку Windows Server.
3. Прочитайте и примите условия лицензионного соглашения.
4. Выберите ручную установку или модернизацию.
5. Сконфигурируйте диск.
6. Укажите пароль для администратора.
7. Войдите в систему.

Во время этого потока существуют некоторые опции:

- установка драйвера, когда в нем есть необходимость;
- исправление существующей установки ОС на компьютере.

В следующем разделе будет рассмотрено завершение данного потока для чистой установки и модернизации. Затем будут раскрыты опции, возникающие во время установки, и показано, как настроить установленную копию ОС.

Выполнение чистой установки

Под *чистой* понимается установка ОС на компьютере, на котором отсутствует текущая установленная копия или такая, которую требовалось бы сохранить. В настоящем примере мы имеем дело с компьютером, не имеющим предыдущей установленной копии. Мы предполагаем, что ранее вы подобных действий не делали, поэтому начнем с основ. У более опытных читателей может возникнуть желание пропустить данный раздел, но мы рекомендуем хотя бы бегло просмотреть его, чтобы ознакомиться с изменениями.

ОС Windows Server 2012 R2 поставляется на DVD. Это довольно большая установка. Обеспечьте наличие на сервере устройства DVD-ROM и вставьте в него носитель DVD. В качестве альтернативы, если вы используете виртуальную машину, то можете перенаправить виртуальный CD/DVD на ISO-образ Windows Server DVD, который можно загрузить из веб-сайта Microsoft или создать из исходного носителя.

> **Что делать, если нет устройства DVD?**
>
> Вы можете иметь дело с сервером, у которого отсутствует устройство DVD. Если это так, обратитесь к одному из упомянутых ранее более сложных методов установки. Однако установить Windows Server 2012 R2 можно также и с внешнего диска USB. Соответствующие инструкции приведены в записи блога одного из сотрудников Microsoft по ссылке `http://tinyurl.com/ktz5fq`.

После загрузки носителя необходимо включить сервер и обеспечить загрузку с устройства DVD. Обычно компьютер с пустым жестким диском по умолчанию будет

производить загрузку с устройства DVD. Если же загрузка из DVD не происходит, причин тому несколько. На жестком диске, с которого по умолчанию производится загрузка, может находиться допустимая ОС. На компьютере может быть доступно меню загрузки, которое появляется на короткий период времени в течение или после самопроверки при включении (Power-On Self Test — POST). Или же из-за конфигурации загрузки сервер может не предоставлять вариант загрузки с устройства DVD. Чтобы решить проблему, войдите в настройки BIOS и внесите соответствующее изменение. Эти две опции будут варьироваться в зависимости от оборудования, так что вы должны проконсультироваться с документацией по оборудованию или обратиться в службу поддержки производителя. В большинстве случаев это будет выглядеть подобно "Boot Order" ("Последовательность загрузки"). Мы также сталкивались с ситуациями, когда DVD-диск прожигался из ISO-файла, но была выбрана слишком большая скорость записи, чтобы обеспечить качественный прожиг. В последующих примерах будет показано, как установить Windows Server 2012 R2.

На рис. 2.1 приведен первый экран, который вы увидите. Он позволяет указать язык установки, формат времени и валюты, а также параметры клавиатуры сервера. Здесь понадобится изменить те параметры, стандартные значения которых не соответствуют вашему языку, региону и клавиатуре. Например, если вы находитесь в Ирландии и пользуетесь клавиатурой с ирландским языком, то стандартные параметры совершенно не подойдут! Часовой пояс не будет соответствовать, символ валюты окажется некорректным, а клавиатурная раскладка абсолютно не совпадает. К примеру, вы с трудом найдете клавишу с обратной косой чертой (<\>), которая настолько важна в мире Windows.

Содержимое списка Language to install (Язык установки) будет меняться в зависимости от языков, поддерживаемых носителем DVD. Большинство читателей этой книги могут иметь дело с англоязычным носителем, даже если английский не является для них родным. Но на выбор доступны испанский, французский, немецкий, китайский и другие языки, что зависит от вашего местонахождения и стандартов, принятых в компании.

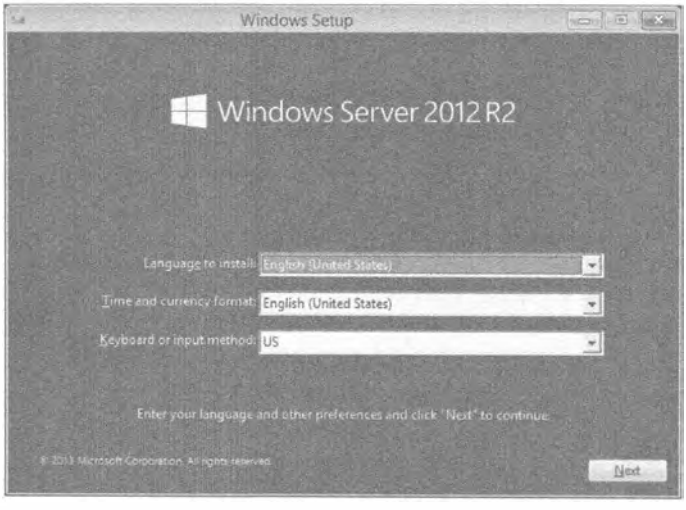


Рис. 2.1. Настройка среды для установки Windows

Параметр в списке Time and currency format (Формат времени и валюты) влияет на то, как Windows представляет и форматирует данные специфичным от региона образом. Практически всегда выбранное значение должно соответствовать месту, где находится сервер.

Параметр в списке Keyboard or input method (Клавиатура или метод ввода) должен отражать клавиатуру, которая физически подключена к компьютеру. В разных странах часто применяются разные клавиатуры, поэтому удостоверьтесь, что выбран подходящий вариант. Не переживайте; это не повлияет на возможность управления сервером с использованием удаленного рабочего стола (Remote Desktop). Сеанс RDP будет применять параметры клавиатуры клиентского компьютера, подключаемого к серверу. Экран, показанный на рис. 2.2, позволяет выполнить пару действий:

- запустить процесс установки;
- запустить поиск неполадок и исправить существующую установленную копию Windows Server 2012 R2.

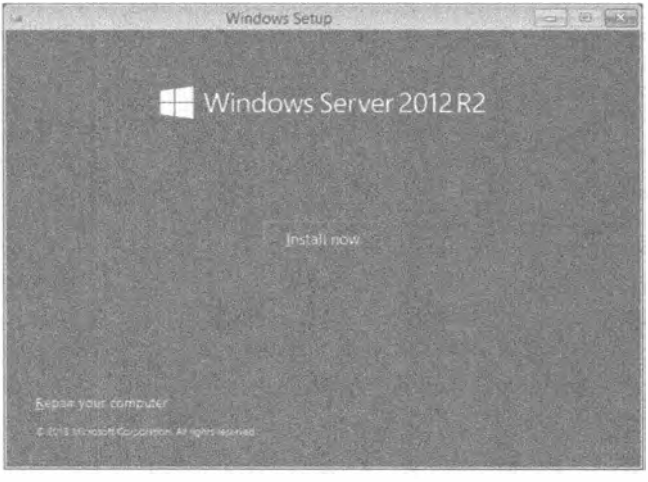


Рис. 2.2. Установка Windows Server 2012 R2

В данном примере будет устанавливаться Windows Server 2012 R2, поэтому щелкните на кнопке Install Now (Установить сейчас).

Установка GUI или установка Server Core

Вы также заметите, что имеется выбор между типами установки. Это было введено в версии Windows Server 2008. Установка GUI имеет развитый графический пользовательский интерфейс Windows. В случае установки Server Core графический пользовательский интерфейс отбрасывается и предполагается, что вам удобно иметь дело с командной строкой и приемами дистанционного администрирования.

Более подробно установка Server Core рассматривается в главе 3.

В настоящем примере будет демонстрироваться способ настройки экспериментальной среды, поэтому нам понадобится большая часть функциональности, доступной в Windows Server 2012 R2. Выберите вариант Windows Server 2012 R2 Standard

Evaluation (Server with a GUI) (Оценочная версия Windows Server 2012 R2 Standard (сервер с GUI)), как показано на рис. 2.3.

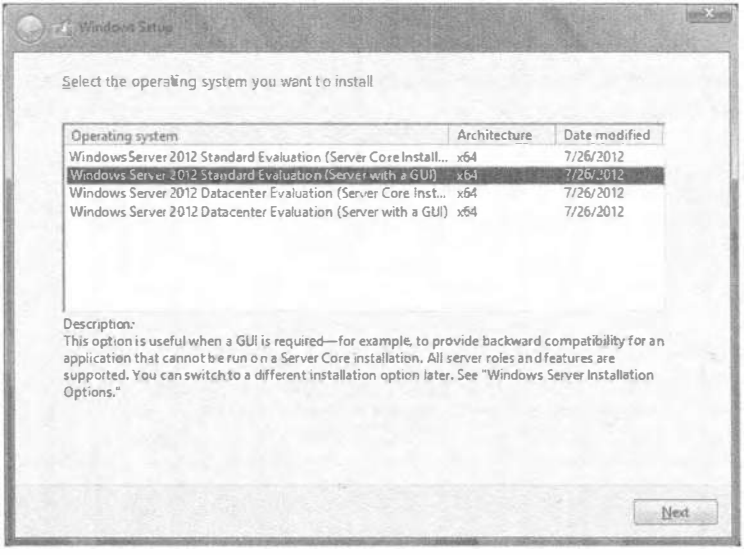


Рис. 2.3. Выбор редакции и типа установки

Теперь вы получили возможность прочитать легендарное лицензионное соглашение с конечным пользователем от Microsoft (end user license agreement — EULA), что иллюстрируется на рис. 2.4. Большинство раздраженных пользователей просто отмечают флажок I accept the license terms (Я принимаю условия лицензии) и щелкают на кнопке Next (Далее), даже не читая текст соглашения.

Рис. 2.4. Принятие условий соглашения EULA

Экран, показанный на рис. 2.5, позволяет выбрать новую или специальную установку Windows Server 2012 R2 либо модернизацию на месте. Выбрать модернизацию можно только при наличии предыдущей версии Windows Server 2008 R2. Не забывайте, что провести модернизацию с версии x86 до x64 невозможно. Также не получится модернизировать установленную копию Server Core до полной установки или наоборот. В данном примере выполняется чистая или новая установка, поэтому выберите вариант Custom (Специальная). Для продолжения щелкните на кнопке Next.

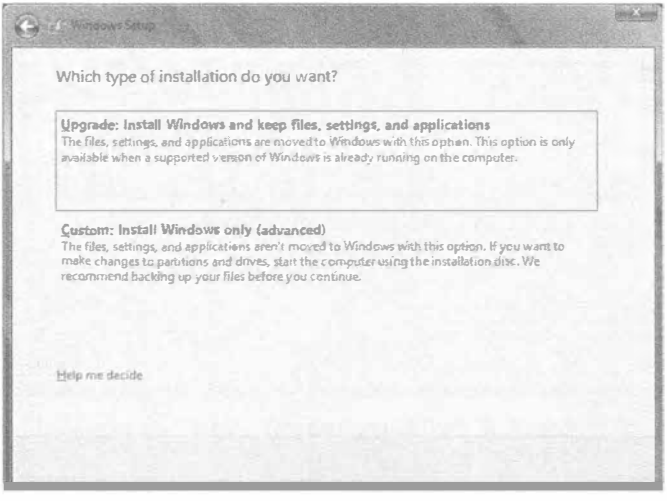


Рис. 2.5. Выбор между модернизацией и чистой установкой

На рис. 2.6 отражено несколько разных действий. Возможно, вы щелкнете на кнопке Next, если устанавливается простой сервер, когда нужно сделать все пространство первого диска устройством C. Щелчок на кнопке Next приведет к тому, что будет создан том по имени C, который задействует полностью весь первый диск на сервере.

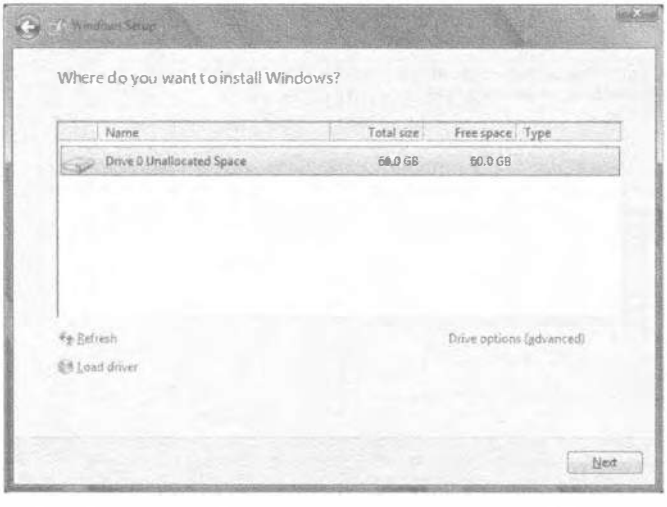


Рис. 2.6. Настройка устройства для установки Windows

Но как поступить, если необходимо разделить диск на несколько томов? Например, может потребоваться создать том, чтобы отделить веб-содержимое от ОС в целях безопасности. Для этого следует щелкнуть на ссылке Drive options (advanced) (Параметры устройства (дополнительные)). Откроется экран, показанный на рис. 2.7.

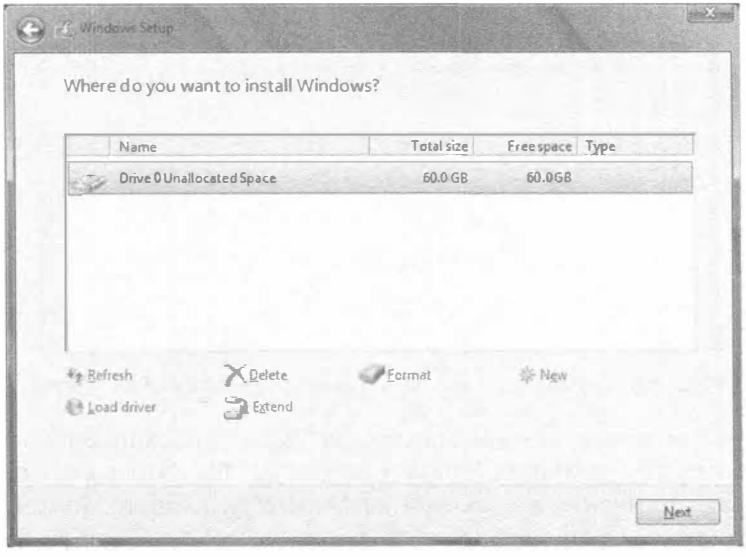


Рис. 2.7. Параметры устройства

На этом экране можно удалять, создавать и форматировать тома по мере необходимости. Вы окажетесь на данном экране, если не хотите принять предлагаемый по умолчанию выбор целиком первого диска (Disk 0) для устройства C. Если вы решили добавить новый раздел, просто щелкните на ссылке New (Новый), укажите необходимый размер раздела и щелкните на кнопке Apply (Применить).

Но что, если программа установки вообще не смогла найти какие-либо диски? Вы несколько раз проверили оборудование и не обнаружили ничего подозрительного. Кабели в порядке, BIOS видит все диски. Дело в том, что программа установки, скорее всего, не имеет драйвера, требуемого для доступа к дисковому контроллеру. С течением времени такая ситуация становится все более распространенной по мере того, как на рынке появляются новейшие контроллеры. Добавить драйвер можно, щелкнув на ссылке Load Driver (Загрузить драйвер). Откроется диалоговое окно, представленное на рис. 2.8.

Ранее считалось обычным, что драйвер дискового контроллера находится на флоппи-диске. С учетом того, что теперь серверы, как правило, не имеют устройства для флоппи-дисков, это стало бы проблемой, и в Microsoft действительно хотят избавиться от необходимости в применении таких дисков. Это диалоговое окно позволяет работать с флоппи-диском, CD, DVD и даже флэш-накопителем USB, где может храниться требуемый драйвер контроллера. Вставьте носитель с драйвером, подождите немного и перейдите на соответствующее устройство для его поиска.

Возвратитесь на экран Where do you want to install Windows? (Где необходимо установить Windows?) и сконфигурируйте диск до того, как продолжить.

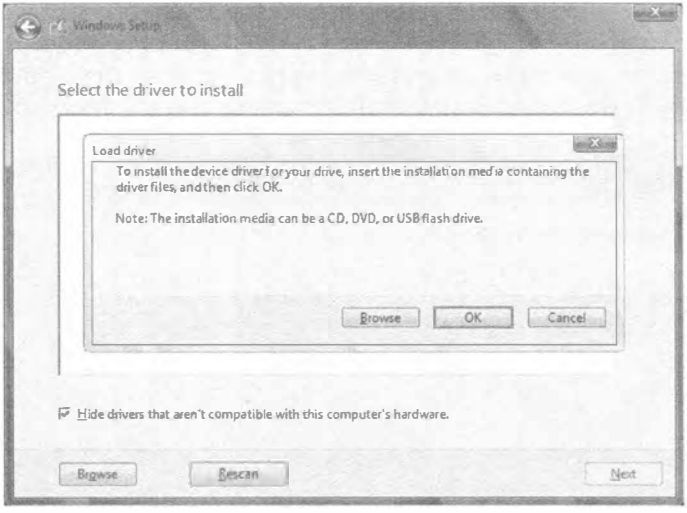


Рис. 2.8. Добавление драйвера контроллера массовой памяти

Процесс близок к завершению. Диалоговое окно, показанное на рис. 2.9, отражает выполняющуюся установку Windows Server 2012 R2. Это займет определенное время, зависящее от носителя установки и целевого устройства. Можете отвлечься и выпить чашку кофе или ответить на письма, которые нескончаемо поступают в ваш почтовый ящик.

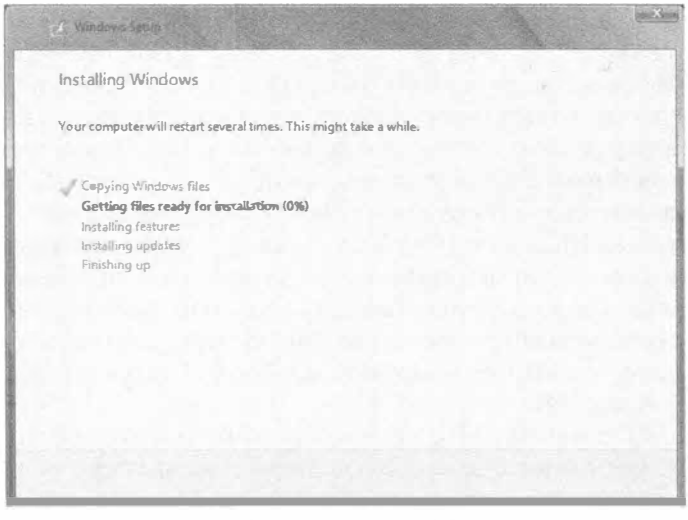


Рис. 2.9. Ход установки Windows

На рис. 2.10 приведен экран, который вы увидите после завершения установки. Прежде чем можно будет войти в систему, Windows Server 2012 R2 предлагает указать пароль для учетной записи локального администратора. Требуется сформировать сложный пароль, имеющий длину не менее восьми символов и содержащий смесь цифр и букв верхнего и нижнего регистров.

Рис. 2.10. Установка пароля для администратора

Выбирайте надежный пароль. На самом деле лучше использовать идентификационную фразу. Дополнительные сведения можно найти в статье "The Great Debates: Pass Phrases vs. Passwords" ("Крупные дебаты: идентификационные фразы или пароли") по адресу `http://tinyurl.com/3hrbg`. После указания нового пароля вы войдете в систему как локальный администратор.

Итак, в конце концов, вы вошли в систему. Обратите внимание на рис. 2.11: кнопка Start (Пуск) возвращена обратно на свое место в нижнем левом углу. Это было сделано по многочисленным запросам пользователей. Кроме кнопки Start можно заметить управляющую панель диспетчера серверов (Server Manager), которая позволяет настраивать сервер. Позже в этой главе мы сконфигурируем сервер с применением диспетчера серверов и его альтернативы для командной строки, PowerShell.

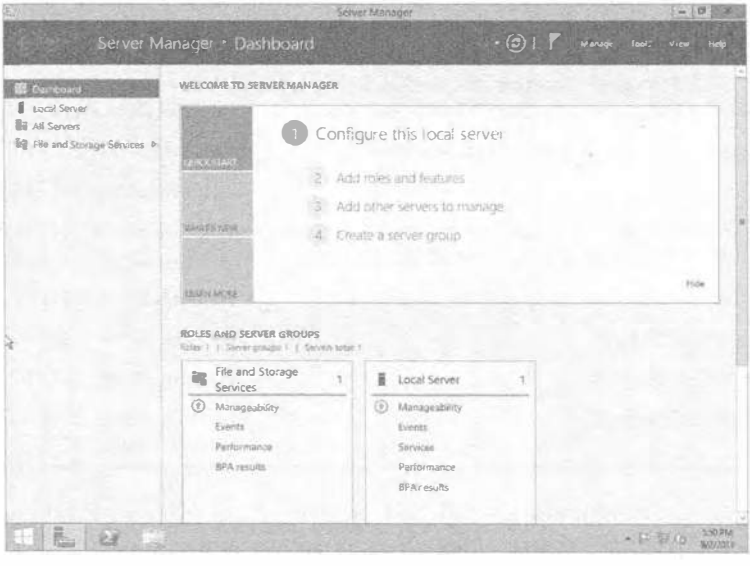


Рис. 2.11. Вход в систему с учетной записью администратора

Ваша первая машина Windows Server 2012 R2 готова и функционирует. Поздравляем! Хотя она предлагает не так много функций, это уже небольшая победа. Далее мы рассмотрим процесс модернизации существующей установленной копии Windows Server до Windows Server 2012 R2.

Выполнение модернизации

У большинства организаций имеются производственные серверы, и они хотят знать, каким образом развернуть Windows Server 2012 R2 в сетях без необходимости в перестройке существующих серверов или миграции приложений на новое оборудование.

Хотя в Microsoft утверждают, что вы должны по возможности избегать проведения модернизации на месте, в определенных сценариях это имеет смысл.

- Небольшая организация, которая недавно инвестировала в серверы, не располагает бюджетом для приобретения нового сервера, чтобы сделать своего рода последовательную модернизацию. Ей желательно задействовать существуюшие установленные копии.
- Крупная организация, которая не желает проводить миграцию на всех серверах из-за большой стоимости этого процесса.
- Миграция сложных производственных сред может оказаться затратной в плане усилий и времени простоя.

Мы считаем вполне реалистичным ожидать, что процесс перехода на Windows Server 2012 R2 будет включать смесь чистых установок и модернизаций. Хорошая новость в том, что модернизация поддерживается и нормально работает. Необходимо тщательно выбирать производственные серверы, чтобы они полностью поддерживали новую ОС. В табл. 2.2 описаны поддерживаемые сценарии модернизации. Обратите внимание, что это схематичные сценарии. Любая планируемая модернизация должна быть предварительно протестирована и согласована с поставщиками.

Таблица 2.2. Поддерживаемые сценарии модернизации Windows Server 2012 R2

Существующая ОС	Поддерживаемая модернизация
Windows Server 2008 Standard с пакетом обновлений SP2 или Windows Server 2008 Enterprise с пакетом обновлений SP2	Windows 2012 R2 Standard или Windows 2012 R2 Datacenter
Windows Server 2008 Datacenter с пакетом обновлений SP2	Windows Server 2012 R2 Datacenter
Windows Web Server 2008	Windows Server 2012 R2 Standard
Windows Server 2008 R2 Standard с пакетом обновлений SP1 или Windows Server 2008 R2 Enterprise с пакетом обновлений SP1	Windows Server 2012 R2 Standard или Windows 2012 R2 Datacenter
Windows Server 2008 R2 Datacenter с пакетом обновлений SP1	Windows Server 2012 R2 Datacenter
Windows Web Server 2008 R2	Windows Server 2012 R2 Standard
Windows Server 2012 Datacenter	Windows Server 2012 R2 Datacenter
Windows Server 2012 Standard	Windows Server 2012 R2 Standard или Windows Server 2012 R2 Datacenter

Если подумать о комбинациях x86, x64, Server Core и полной установки, то получится множество разнообразных сценариев модернизации.

Ниже перечислены аспекты, которые следует принимать во внимание.

- Провести модернизацию с x86 до x64 или наоборот невозможно.
- Модернизация напрямую с Windows Server 2003 не допускается. Сначала придется провести модернизацию до версии Windows Server 2008 и только затем переходить на Windows Server 2012 R2.
- Модернизация с Windows Server 2003 до редакций Windows Server 2012 R2 Server Core невозможна.
- Хотя можно модернизировать до более высокой редакции, например, с Windows Server 2008 R2 Standard до Windows Server 2012 R2 Datacenter, необходимо удостовериться в наличии допустимой лицензии Windows.
- Прежде чем можно будет выполнить модернизацию с Windows Server 2008, нужно лицензировать новую ОС, такую как Windows Server 2012 R2. Это означает либо наличие гарантии Software Assurance, либо приобретение обязательной лицензии Windows Server 2012 R2 для каждого модернизируемого сервера и обязательных лицензий клиентского доступа (client access license — CAL) для доступа конечных пользователей.
- Модернизация ОС с одного языка на другой не допускается.

Переход от серверов x86 на серверы x64 требует миграции определенного вида. Вероятный процесс будет предусматривать введение нового оборудования. Это может делаться как часть утилизации всего оборудования, которое больше не поддерживается производителем. Также это могло быть частью миграции на виртуализированный центр данных. Или же это может быть циклический процесс, который уже делался ранее, поскольку он позволял минимизировать затраты на оборудование. Ниже приведен пример.

1. Сервер A, сервер B и т.д. функционируют под управлением Windows Server 2008 для x86 в машинном зале.
2. Сервер X приобретается для модернизации сети.
3. Сервер X собирается с Windows Server 2012 R2 для близкого соответствия серверу A.
4. Службы переносятся из сервера A на сервер X.
5. Сервер A пересобирается с Windows Server 2012 R2 для близкого соответствия серверу B.
6. Службы переносятся из сервера B на сервер A.
7. Процесс повторяется со всеми оставшимися машинами с Windows Server 2008.

По-прежнему можно встретить множество машин с Windows 2000 Server. Как вы собираетесь поступить с ними? Для модернизации до Windows Server 2012 R2 сначала придется провести их модернизацию до Windows Server 2003, а затем до Windows Server 2008 R2. Вполне возможно, что в большинстве ситуаций это не произойдет. ОС Windows 2000 Server не имеет выпуска для процессоров x64 производства Intel и AMD. Существовал выпуск для процессора Itanium, но это не то же самое, что x64. Это значит, что способа модернизации на месте с Windows 2000 Server до Windows Server 2012 R2 не предусмотрено.

Прежде чем даже рассматривать вопрос модернизации, потребуется проделать ряд рутинных работ.

- Вам придется дважды удостовериться, что все ПО и драйверы, установленные на модернизируемом компьютере, будут поддерживаться версией Windows Server 2012 R2. Программные продукты могут функционировать, но всегда возникает вопрос поддержки со стороны их поставщиков. Высока вероятность того, что поначалу такая поддержка будет ненадежной, но со временем положение дел улучшится.
- Самым важным драйвером, который должен быть в наличии, является драйвер контроллера массовой памяти. Вы уже видели в процессе чистой установки, что этот драйвер может понадобиться предоставить на съемном носителе, если в Windows Server не обнаружится подходящего встроенного драйвера.
- Проверьте работоспособность серверного оборудования. Обычно поставщик предлагает для этого какое-то бесплатное ПО. В Microsoft рекомендуют также воспользоваться их инструментом диагностики памяти.
- Если вы модернизируете производственный или другой важный сервер, то должны провести его резервное копирование, прежде чем переходить к дальнейшим действиям. По возможности проверьте полученную резервную копию. В случае использования виртуальной машины все намного упрощается. Можно создать снимок и в ситуации, когда модернизация не прошла, откатиться к этой точке во времени. Но сначала проконсультируйтесь со своим поставщиком относительно поддержки снимков в производственной среде.
- На модернизируемом сервере потребуется либо отключить, либо удалить антивирусное ПО. Скорее всего, его придется удалить, т.к. высока вероятность того, что оно будет мешать процессу или даже нарушит работу модернизированного сервера. По завершении модернизации необходимо удостовериться в том, что существующая версия антивирусного ПО пригодна для развертывания в среде Windows Server 2012 R2.
- Если функционирует какое-либо решение мониторинга, подобное диспетчеру операций системного центра (System Center Operations Manager), понадобится либо отключить мониторинг на несколько часов, либо даже удалить этот агент. Проконсультируйтесь со своим поставщиком относительно поддерживаемых сценариев.
- Наконец, подготовьте брандмауэр Windows. Он может блокировать трафик приложений, предназначенный для модернизированных серверов. Заблаговременно узнайте, какие порты необходимо сконфигурировать. Это может потребовать консультаций с поставщиком приложения либо использования инструмента вроде бесплатного монитора сети Microsoft (Microsoft Network Monitor).

Мы рекомендуем сначала испытать процесс модернизации в виртуальной экспериментальной среде. Это можно сделать с довольно небольшими затратами, воспользовавшись TechNet или демонстрационными лицензиями и одним из многочисленных бесплатных решений для виртуализации. Если вы тестируете Windows Server 2012 R2, то можете применять следующие средства:

- бесплатный программный продукт Hyper-V Server 2012 производства Microsoft;
- программный продукт VMware Server, который будет запускаться на хосте Windows Server;
- программный продукт VMware Workstation 9.0;
- программный продукт Citrix XenServer — еще один гипервизор, который относительно близок продукту Hyper-V от Microsoft.

Обратите внимание, что при тестировании Windows Server 2012 R2 должна использоваться технология виртуализации, подобная перечисленным выше, которая поддерживать 64-разрядные виртуальные машины или гостей.

Использование Hyper-V

Вы изучаете ОС Windows Server 2012 R2, поэтому вполне логично применять Hyper-V. Настоятельно рекомендуем прочитать главы 27 и 28 (том 2), в которых рассказывается о том, как развертывать среду виртуализации для целей экспериментальной среды.

Все формальности закончились, так что давайте взглянем на модернизацию в действии. Вы не сможете провести модернизацию на месте, когда сервер был загружен с устройства DVD или USB. Этот метод позволяет делать только чистую установку. Если необходимо выполнить модернизацию, придется загрузить установленную копию Windows Server и вставить носитель DVD или USB. В случае виртуальной машины понадобится смонтировать ISO-образ носителя Windows Server 2012 R2. Это позволит программе модернизации загрузить обновления из веб-сайта Microsoft и должным образом просканировать сервер, прежде чем будут внесены любые изменения.

На рис. 2.12 показана копия экрана, полученная на существующей машине с установленной версией Windows Server 2008 R2 x64, которую планируется модернизировать до Windows Server 2012 R2.

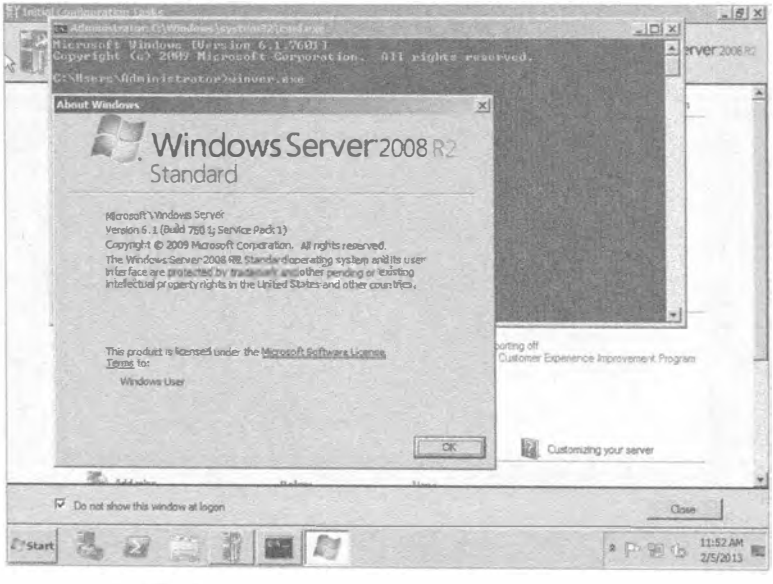


Рис. 2.12. На сервере установлена версия Windows 2008 R2

Рис. 2.13. Начальный экран `setup.exe`

Для проверки версии и сборки ОС была запущена утилита `winver.exe`. Наличие папки `C:\Program Files (x86)` означает, что установленная ОС является 64-разрядной. Процесс похож на модернизацию Windows Server 2003 x86 до Windows Server 2008 x86. Для продолжения войдите в систему на сервере, который нужно модернизировать, и вставьте или смонтируйте носитель с версией Windows Server 2012 R2.

Диалоговое окно, приведенное на рис. 2.13, откроется автоматически, если для DVD-привода включена функция автозапуска (AutoPlay). Если указанное окно не открылось, запустите программу `setup.exe` из корневой папки носителя с Windows Server 2012 R2.

Вы заметите, что процесс модернизации в основном идентичен процессу чистой установки. Действия, которые придется проделать с применением клавиатуры и мыши, довольно просты.

Щелкните на пункте Go online to install updates now (Перейти в онлайн для установки обновлений), чтобы продолжить модернизацию (рис. 2.14).

Процесс установки начнется с копирования временных файлов; это может занять несколько минут в рамках подготовки к установке Windows Server 2012 R2.

Экран, показанный на рис. 2.14, позволяет загрузить обновления из веб-сайта Microsoft, чтобы улучшить процесс установки.

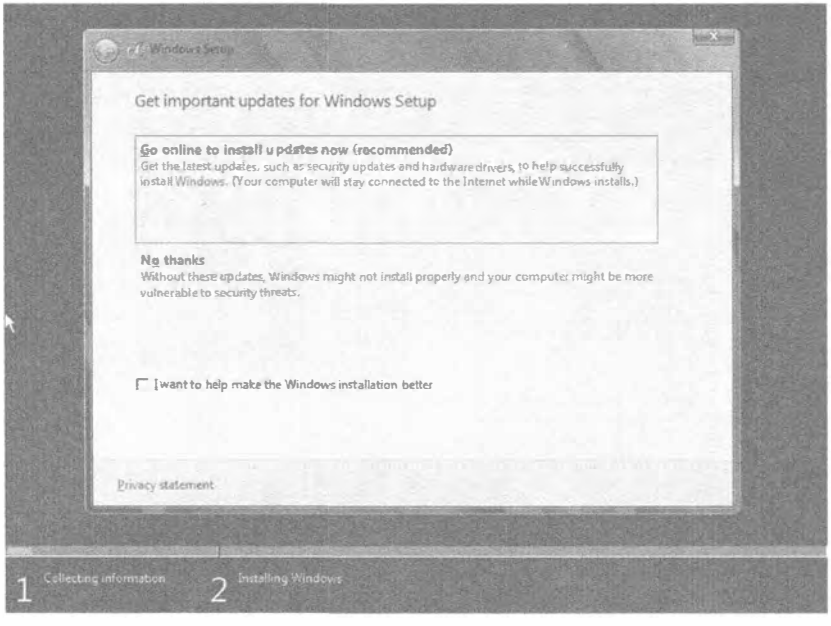


Рис. 2.14. Получение обновлений для установки

В этом процессе предполагается, что учетная запись, под которой был совершен вход на сервер, имеет доступ в Интернет. В Microsoft указывают четыре причины для загрузки обновлений установки.

- Загружаются обновления для процесса установки. Это позволяет решить проблемы, обнаруживаемые с течением времени.
- Доступны обновления драйверов, улучшающие автоматическое конфигурирование устройств во время установки.
- Загружаются обновления Windows, которые вносят исправления в ОС.
- Загружаются обновления для инструмента удаления вредоносного ПО (Microsoft Windows Malicious Software Removal Tool), что помогает защищать новый сервер.

Мы советуем загружать обновления установки, если вы считаете модернизируемый сервер важным. Если же вы просто проводите эксперимент, то вопрос о том, что установка завершится неудачно, а обновление могло бы решить проблему, может не беспокоить. На рис. 2.15 видно, что мы решили загрузить обновления, так что программа установки подключается к веб-сайту Microsoft с целью загрузки доступных обновлений. Мы уже обсуждали возможные опции; они будут такими же, как в процессе чистой установки. Вы должны выбрать требуемую установку и подтвердить наличие для нее лицензии. Давайте займемся этим.

Но подождите! Почему мы видим экран, показанный на рис. 2.16? Разве мы выполняем не модернизацию? Пока еще вы ничего не сообщили программе установки о том, что следует делать. В этой точке можно было бы установить новую ОС.

Удостоверьтесь, что выбираете нужную редакцию для модернизации. В табл. 2.2 были описаны допустимые пути модернизации до версии Windows Server 2012 R2.

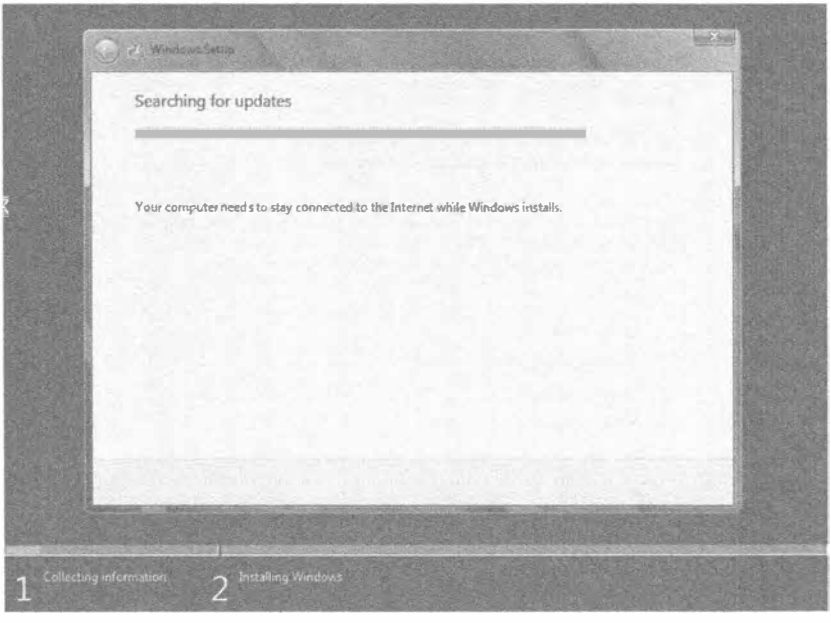


Рис. 2.15. Загрузка доступных обновлений

Естественно, вам понадобится пройти через лицензию EULA и хорошо ознакомиться с ее условиями, прежде чем принимать их (рис. 2.17). Вполне ответственно заявляем, что вы не сможете установить Windows Server 2012 R2, если не согласитесь с условиями, предъявляемыми Microsoft.

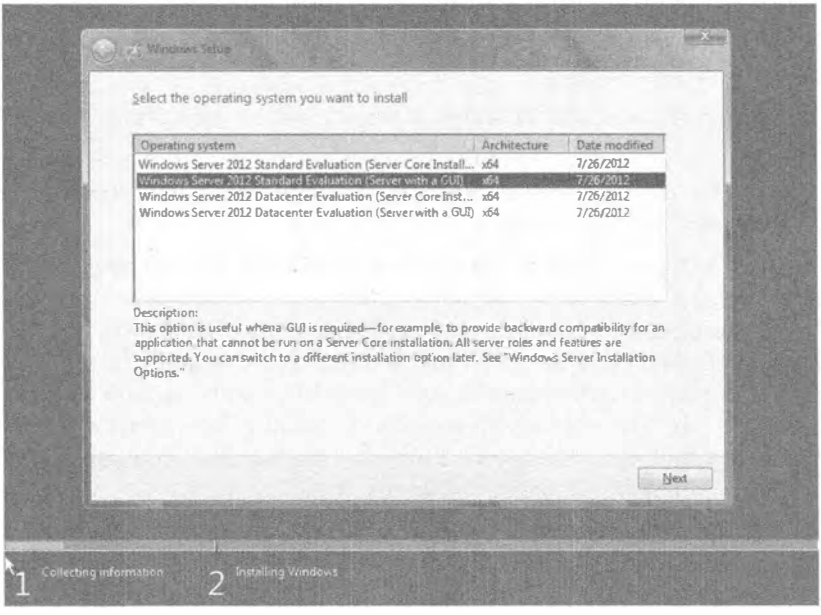


Рис. 2.16. Выбор редакции и типа установки

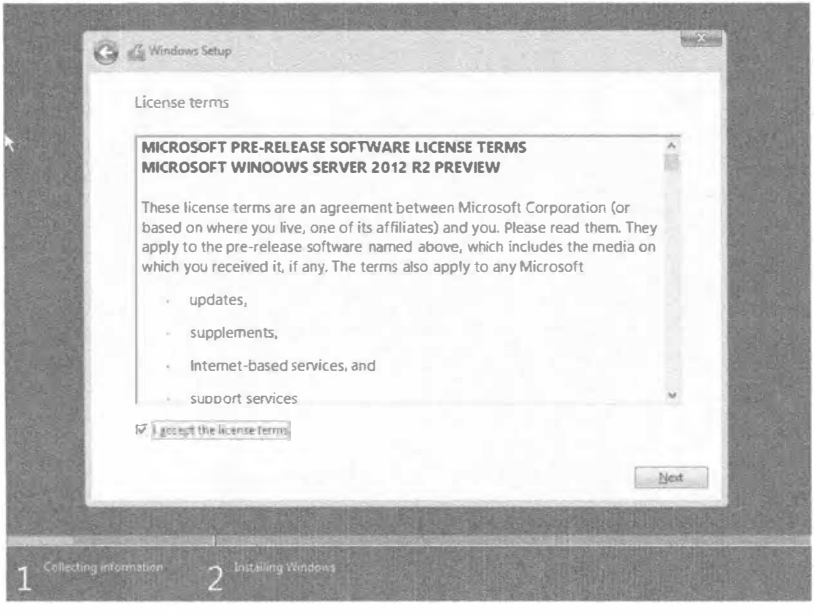


Рис. 2.17. Принятие условий лицензии EULA

Диалоговое окно, представленное на рис. 2.18, предлагает возможность либо провести модернизацию, либо выполнить специальную или чистую установку Windows Server 2012 R2. Если до сих пор вы точно следовали инструкциям, то будут доступны обе опции. Однако в случае выбора для установки некорректной редакции Windows Server 2012 R2 опция модернизации будет отсутствовать.

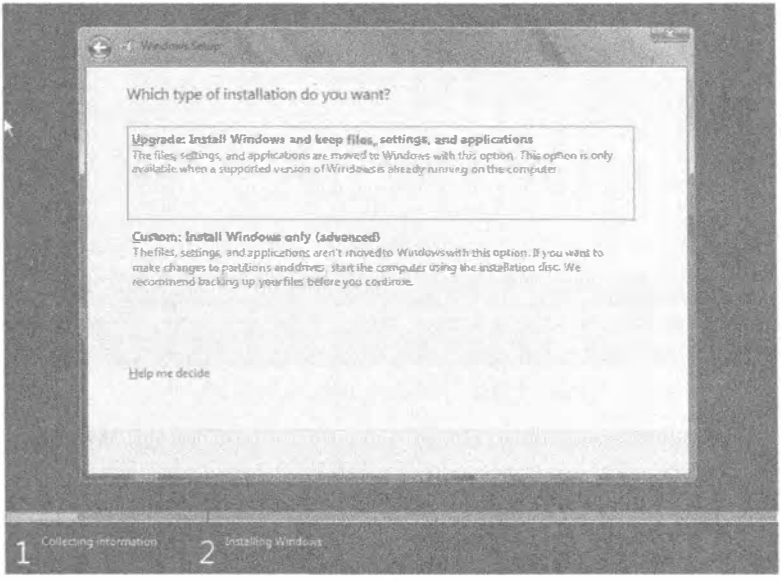


Рис. 2.18. Выбор проведения модернизации

В этом примере мы выполняем модернизацию редакции Windows Server 2008 R2 Standard до редакции Windows Server 2012 R2 Standard с графическим пользовательским интерфейсом, поэтому щелкните на варианте Upgrade: Install Windows and keep files, settings, and applications (Модернизация: установить Windows и сохранить файлы, параметры и приложения).

Программа установки просканирует существующую установленную копию на предмет наличия несовместимостей с Windows Server 2012 R2.

Программа установки проверит, совместим ли существующий сервер. Если он не совместим, в отчете по совместимости будет указана причина, такая как попытка проведения модернизации оценочной версии Windows Server 2008 R2 (рис. 2.19). Процесс модернизации может быть начат после устранения всех проблем.

В данный момент вы находитесь на последнем этапе, когда еще есть возможность внести изменения. Программа установки позволит подтвердить, что все оборудование, ПО и драйверы в существующей установке сервера будут функционировать после завершения модернизации. После щелчка на кнопке Next возвратиться назад не удастся! Здесь будут перечислены все обнаруженные несовместимости с Windows Server.

В случае выдачи предупреждения о том, что один из драйверов может не работать после модернизации, проблему можно исправить после ее завершения.

И снова можно сделать перерыв. Программа установки теперь обладает достаточной информацией, чтобы продолжить процесс. Она выполнит модернизацию и при необходимости перезагрузит систему.

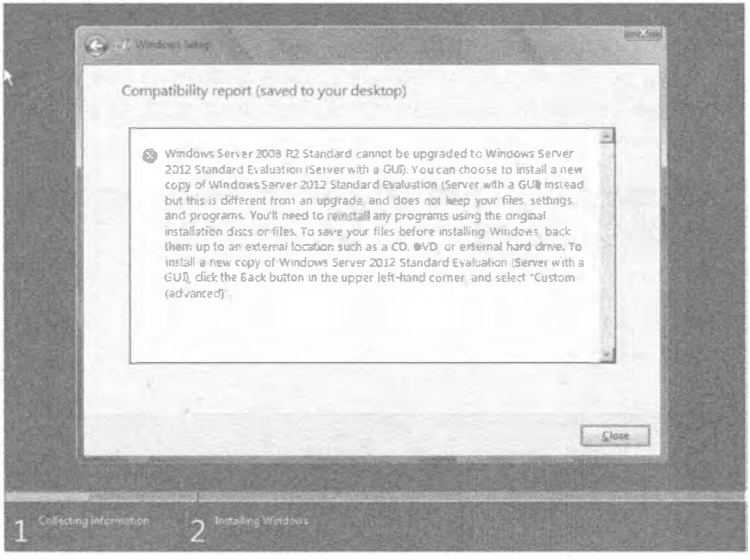


Рис. 2.19. Отчет по совместимости

Вашим следующим действием будет вход на новый сервер Windows Server 2012 R2, предполагая, что все прошло по плану. Необходимо удостовериться в том, что все функционирует корректно, и внести требуемые изменения в конфигурацию.

Сервер будет перезагружаться несколько раз; в конце концов, он перезагрузится в Windows Server 2012 R2 и станет ожидать вашего входа (рис. 2.20). Сколько времени это займет, зависит от оборудования. Серверное оборудование может быть быстрым или медленным; например, компьютер с недорогой и медленной памятью, очевидно, потребует больше времени на модернизацию. Вот почему вас предупреждают о том, что модернизация *может* занять несколько часов.

Рис. 2.20. Модернизация завершена

На рис. 2.20 вы могли заметить значок в форме "глаза" внутри поля для ввода пароля. Это средство позволяет видеть набираемый пароль, что довольно удобно при вводе некорректного пароля. Войдите в систему и посмотрите, как выглядит модернизированный сервер.

После входа вместо окна утилиты Initial Configuration Tasks (Задачи начального конфигурирования) вы видите окно Server Manager (Диспетчер серверов), как показано на рис. 2.21. Пока что диспетчер серверов не должен особо заботить; он будет подробно рассматриваться немного позже. Это первое отличие между чистой установкой и модернизацией. Прокрутив панель подробных сведений в середине окна, вы отметите, что состояние брандмауэра Windows унаследовано из предыдущей установленной копии системы.

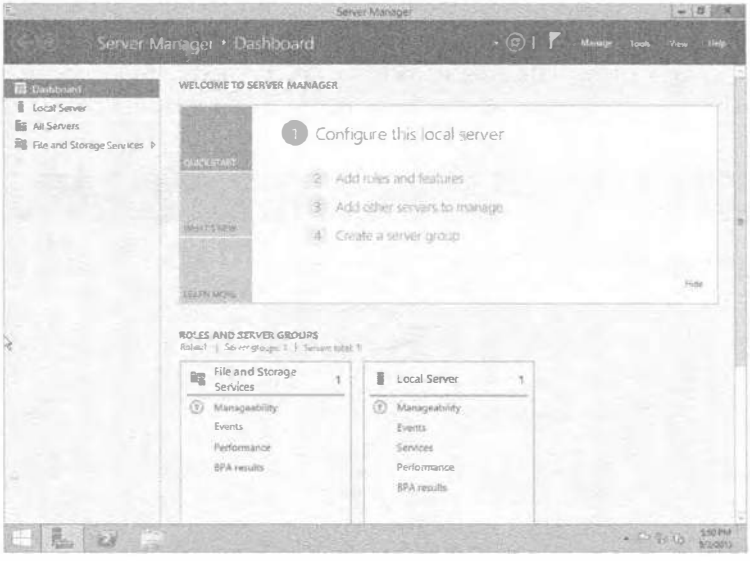


Рис. 2.21. Диспетчер серверов

Вы также увидите, что были установлены некоторые *роли* и *компоненты*. Как утверждалось ранее, установка Windows Server 2012 R2 по умолчанию ничего не содержит. И это правда. Но в данном примере мы провели модернизацию сервера. На только что модернизированном сервере дополнительные компоненты не устанавливались. Но ОС Windows Server 2012 R2 трактует это совершенно по-другому. ОС считает, что важная функциональность должна быть сохранена в случае, если она уже использовалась. Позже вы узнаете, каким образом применять диспетчер серверов или PowerShell для добавления либо удаления ролей и компонентов.

В этот момент имеет смысл убедиться в том, что все успешно завершено.

- Проверьте журналы в программе Event Viewer (Просмотр событий), чтобы выяснить, не возникали ли проблемы, которые должны быть устранены.
- При необходимости присоединитесь к домену и удостоверьтесь в том, что все требуемые политики были применены.
- Установите все доступные обновления, связанные с безопасностью.

- Установите все защитное ПО, такое как антивирусная программа, и примените все обязательные ручные обновления.
- Может понадобиться установить, сконфигурировать или протестировать ПО от независимых разработчиков.

На этом модернизация завершена. Все было не так уж и страшно. Теперь можно приступать к настройке сервера.

Управляющая панель диспетчера серверов

Управляющая панель диспетчера серверов является стандартным экраном, который вы будете видеть первым после входа в систему (см. рис. 2.21). При проведении чистой установки или модернизации сервера данный инструмент позволит быстро выполнить ряд важных задач.

Прежде чем раскрывать детали, необходимо резюмировать темы, которые будут рассмотрены далее в главе. Щелчок на ссылке Local Server (Локальный сервер) приводит к открытию окна настройки свойств, представленного на рис. 2.22.

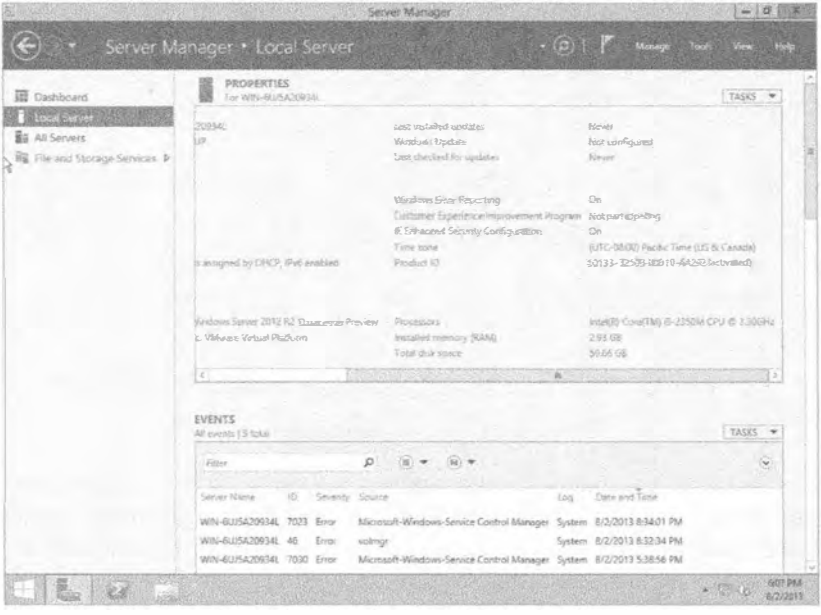


Рис. 2.22. Окно настройки свойств локального сервера

Компьютер будет настраиваться в следующем разделе, в котором раскрываются перечисленные ниже темы.

- **Активация Windows.** Каждая копия Windows Server 2012 R2 нуждается в активации либо через Интернет, либо посредством телефонного звонка в Microsoft. Пока не будет проведена активация, сервер функционировать не будет.
- **Установка часового пояса.** Прямо над ссылкой Product ID (Идентификатор продукта) находится ссылка Time zone (Часовой пояс), позволяющая установить часовой пояс. После щелчка на ней можно указать часовой пояс и установить время.

- **Конфигурирование сети.** Ссылка Ethernet позволяет сконфигурировать подключение сервера к сети.
- **Предоставление имени компьютера и домена.** Воспользовавшись ссылкой Computer name (Имя компьютера), можно установить имя компьютера и сконфигурировать для сервера членство в домене.
- **Включение автоматических обновлений и обратной связи.** Это должно делаться либо вручную, либо через групповую политику. Автоматические обновления позволят загружать важные обновления, в том числен и безопасности, от Microsoft, обычно на ежемесячной основе.
- **Загрузка и установка обновлений.** Загрузить и применить обновление можно и вручную, чтобы немедленно защитить сервер. Мы настоятельно рекомендуем поступать так.
- **Добавление ролей.** Роли и компоненты более подробно рассматриваются в следующем разделе.
- **Добавление компонентов.** Подобно предыдущему пункту, это позволяет добавлять функциональность к серверу.
- **Включение удаленного рабочего стола.** Скорее всего, вы будете управлять своим сервером с применением удаленного рабочего стола через сеть. Это средство позволит решить данную задачу.
- **Конфигурирование брандмауэра Windows.** Брандмауэр Windows на сервере по умолчанию должен быть включен. Его можно сконфигурировать автоматически с помощью групповой политики Active Directory или же вручную. Конфигурирование необходимо для того, чтобы разрешить удаленный доступ к сетевым службам, размещенным на сервере.

По умолчанию окно диспетчера серверов продолжит появляться после каждого входа в систему на серверах, где была выполнена чистая установка.

Теперь вы имеете представление об инструментах, с помощью которых можно управлять сервером.

Использование диспетчера серверов для конфигурирования серверов

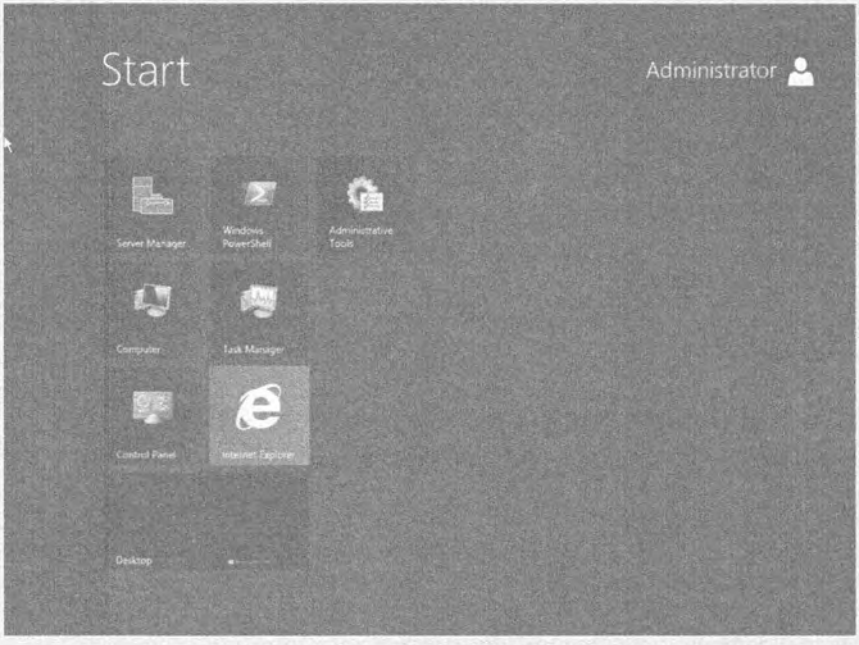
Многие годы в Microsoft пытались заставить пользователей применять единственный инструмент для управления конфигурацией серверов. В прошлом при входе в ОС Windows Server самой новой версии нас приветствовало окно какого-то инструмента, обещающего решить довольно много задач. После беглого взгляда мы находили флажок, выглядящий примерно как Do not display this again at logon (Не отображать это снова при входе), отмечали его и затем закрывали окно инструмента, чтобы больше никогда не видеть его. Единственный раз, когда мы слышали об этом инструменте — во время изучения материалов для сертификационного экзамена Microsoft. Зачем использовать этот инструмент, если достичь желаемого можно гораздо быстрее с помошью значка Add/Remove Programs (Установка и удаление программ) в панели управления?

Вероятно, вы уже заметили, что ОС Windows Server 2012 R2 действительно отличается от своих предшественников. До выхода версии Windows Server 2012 стандартным инструментом была утилита Initial Configuration Tasks (Задачи начального конфигурирования). Теперь при каждом входе в систему вас приветствует управляющая панель диспетчера серверов (см. рис. 2.21).

Итак, добро пожаловать в диспетчер серверов. В ОС Windows Server 2012 R2 он находится в *суперпанели* (или в панели задач). Вдобавок получить доступ к диспетчеру серверов можно путем его выбора в меню Administrative Tools (Администрирование), запуска `compmgmtlauncher.exe` или применения значка Programs and Features (Программы и компоненты) панели управления.

Возвращение кнопки Start

В версии Windows Server 2012 для получения показанного ниже списка программ нужно было нажать клавишу <Windows>, которая расположена левее левой клавиши <Alt> на стандартной клавиатуре. В версии Windows Server 2012 R2 кнопка Start была возвращена в свою первоначальную позицию — в нижний левый угол панели задач. Она снова позволяет быстро получать доступ к главным программам, установленным вместе с Windows Server. По мере добавления программ и ролей вы будете видеть здесь новые кнопки.



Диспетчер серверов — это инструмент, который вы будете использовать для управления конфигурацией своих машин Windows Server 2012 R2. С его помощью можно добавлять и удалять встроенные функциональные средства, управлять этими средствами и диагностировать проблемы. Для управления встроенной функциональностью, установленной в Windows Server 2012 R2, можно также применять альтернативу в виде командной строки PowerShell.

Совет по диспетчеру серверов

Диспетчер серверов имеет привычку появляться каждый раз, когда вы входите в систему. Очень скоро это может надоесть. Для управления открытием диспетчера серверов при входе можно изменить значение типа `REG_DWORD` по имени `DoNotOpenServerManagerAtLogon` ключа `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Server Manager` в реестре. Стандартным его значением является `0`, что приводит к появлению диспетчера серверов после входа в систему. Установка значения `1` отключает это. Другой способ отключения предполагает выбор пункта Server Manager Properties (Свойства диспетчера серверов) в раскрывающемся меню Manage (Управление), которое расположено в правом верхнем углу окна диспетчера серверов. Откроется небольшое окно, в котором понадобится отметить флажок Do not show me this console at logon (Не показывать эту консоль при входе).

Изменения в диспетчере серверов

Между диспетчерами серверов в версиях Windows Server 2008 и Windows Server 2012 R2 имеется ряд отличий.

- Как было указано ранее в этой главе, утилита Initial Configuration Tasks больше не является стандартным инструментом, открывающимся сразу после входа в систему; таким инструментом стал диспетчер серверов. Диспетчер серверов открывается с выбранной вкладкой Local Server (Локальный сервер), отображающей все свойства локального сервера, которые можно использовать для управления сервером.
- Вы быстро заметите, что графический пользовательский интерфейс диспетчера серверов отличается от его предыдущей версии. Привыкание к новым прямоугольникам в стиле Metro может занять некоторое время, но в долгосрочной перспективе вы оцените их по достоинству.
- В диспетчере серверов теперь имеется поддержка многосерверного дистанционного управления. Инструмент позволяет легко добавить серверы к сети. Добавленным средством является групповое управление, которое позволяет отправлять команды всем серверам внутри группы.
- Теперь в диспетчере серверов можно получать доступ к журналам событий и службам как на локальном, так и на удаленных серверах.
- Мастер добавления ролей (Add Roles Wizard) имеет ряд новых экранов с несколькими новыми опциями добавления до перехода к выбору ролей. Первый новый экран называется Installation Type (Тип установки), а второй новый экран — Server Selection (Выбор сервера). Мы обсудим эти новые экраны и работу с ними далее в главе.
- Утилита `servermanagercmd.exe` была объявлена устаревшей. Теперь в качестве инструмента командной строки следует применять PowerShell.
- Функция добавления компонента посредством графического пользовательского интерфейса теперь является частью мастера добавления ролей, а не отдельным инструментом.

На основе приведенного списка может показаться, что отличий очень много, однако диспетчеры серверов в версиях Windows Server 2008 и Windows Server 2012 R2 в большей степени похожи, чем различны.

Общие задачи конфигурирования

При установке нового сервера необходимо пройти через ряд общих задач конфигурирования, чтобы подключить сервер к сети. Далее мы рассмотрим некоторые примеры с применением диспетчера серверов.

В левой части управляющей панели имеется ссылка под названием Local Server (Локальный сервер). Щелчок на ней приводит к открытию большого окна Properties (Свойства) со списком всех свойств сервера (см. рис. 2.22).

Как видите, рядом с каждым элементом списка находится текстовая ссылка, в результате щелчка на которой открывается окно свойств для этого элемента. Давайте приступим к конфигурированию нового сервера.

Активация Windows

Если вы используете лицензию OEM, то она должна быть указана на стикере, приклеенном к корпусу компьютера. Эта лицензия и ключ продукта привязаны к данному компьютеру и могут применяться только на нем. Если вы приобрели розничную или индивидуальную копию лицензии, то ключ, скорее всего, находится на контейнере DVD. При наличии корпоративной лицензии (volume license) от Microsoft вы можете получить единый многократно используемый лицензионный ключ либо на веб-сайте лицензирования Microsoft, либо через канал поставщика или партнера, авторизованного на продажу соглашений (large account reseller — LAR).

В зависимости от лицензионного соглашения, вы можете активировать каждую установленную копию напрямую через Microsoft либо посредством локально размещенной службы активации продукта. Корпоративное лицензирование и активация являются довольно сложными темами, которые с течением времени изменяются. Лучше всего обращаться напрямую к последним материалам от Microsoft. В настоящее время актуальна статья "Обзор активации корпоративных лицензий" по адресу `http://technet.microsoft.com/ru-ru/library/hh831612.aspx`.

Рядом с элементом Product ID (Идентификатор продукта) находится ссылка на экран, на котором можно ввести идентификатор продукта. Щелкните на этой ссылке, чтобы открыть экран Windows Activation (Активация Windows). Для завершения процесса активации просто введите свой ключ в текстовом поле Product key (Ключ продукта) и щелкните на кнопке Activate (Активировать), как показано на рис. 2.23.

Изменение свойств сети

Одним из первых действий, которые обычно будут выполняться с сервером, является обеспечение для него статической конфигурации сети IPv4. В сети IPv4 это требуется для того, чтобы сервер мог видеть другие сетевые устройства и службы.

Как было указано ранее, рядом с каждым элементом списка свойств расположена ссылка, позволяющая изменить настройку. В данном случае необходимо щелкнуть на ссылке рядом с элементом Ethernet. Здесь можно видеть все сетевые интерфейсные платы (network interface card — NIC), установленные на сервере. Наш текущий сервер очень прост. Он содержит только один сетевой интерфейс, предназначенный для конфигурирования (рис. 2.24).

Ваш сервер может иметь две сетевых интерфейсных платы. Их можно связать в один отказоустойчивый и/или балансирующий нагрузку виртуальный интерфейс. Вполне вероятно, что для этого у поставщика оборудования предусмотрено соответствующее ПО.

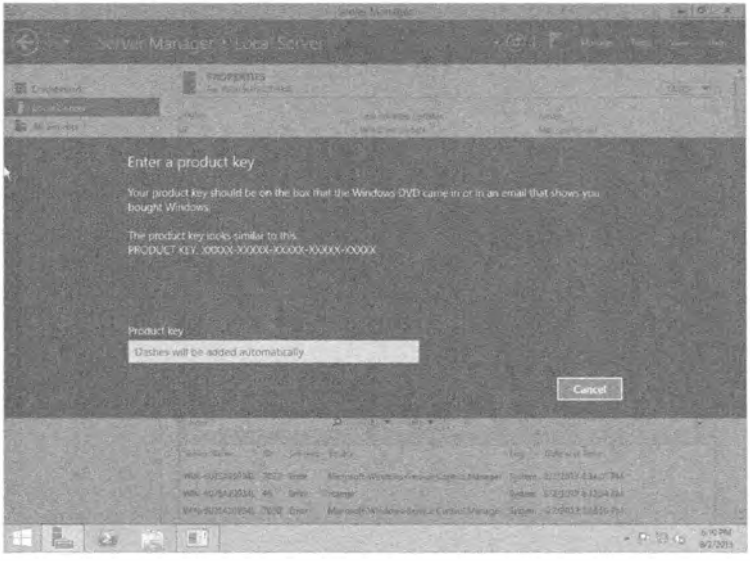


Рис. 2.23. Экран Windows Activation

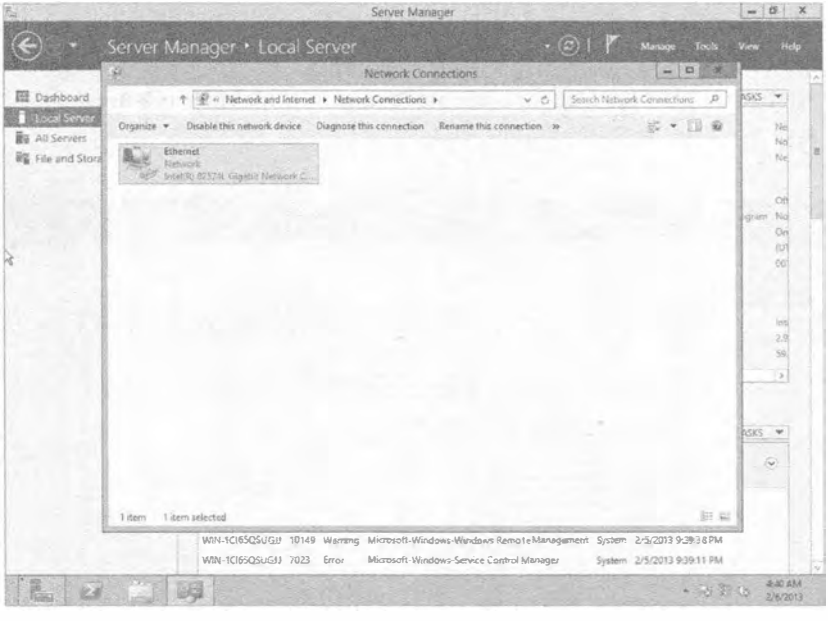


Рис. 2.24. Сетевые подключения

Существует один удобный прием: вы можете запустить утилиту `ncpa.cpl` в PowerShell, чтобы быстро открыть таблицу свойств Network Connections (Сетевые подключения).

Для конфигурирования сетевой интерфейсной платы сервера щелкните правой кнопкой мыши на ее изображении и выберите в контекстном меню пункт Properties (Свойства). Откроется диалоговое окно, приведенное на рис. 2.25.

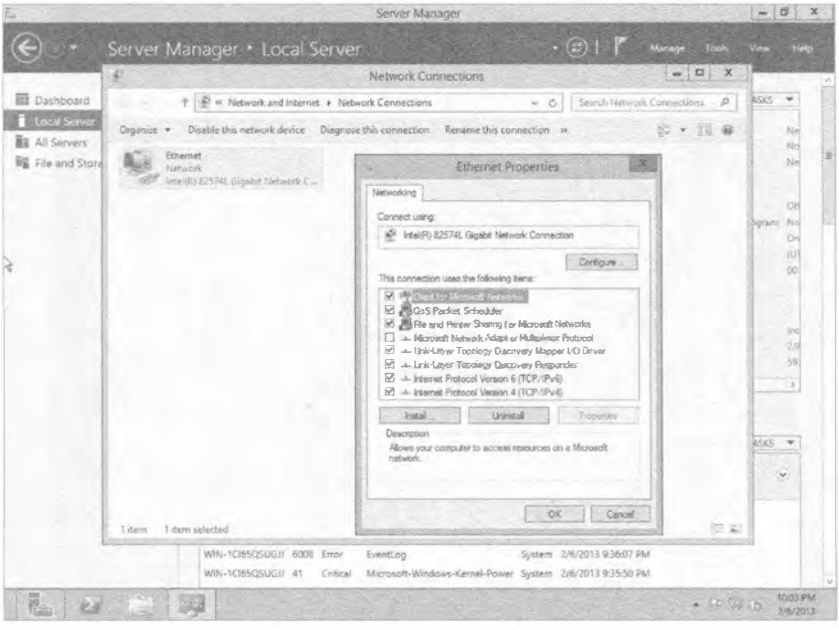


Рис. 2.25. Свойства подключения к локальной сети

Далее выберите элемент Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)) и щелкните на кнопке Properties (Свойства). Откроется диалоговое окно, показанное на рис. 2.26.

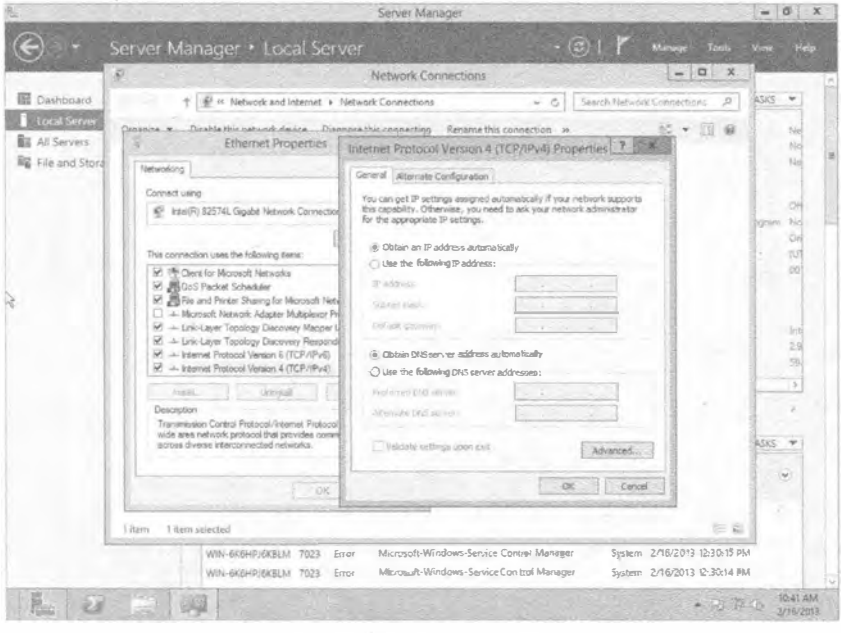


Рис. 2.26. Свойства IPv4

По умолчанию новый сервер Windows Server 2012 R2 не имеет сконфигурированного IP-адреса. Он будет пытаться получить конфигурацию TCP/IPv4 от DHCP-сервера. Для производственного сервера это обычно нежелательно, так что измените конфигурацию на статическую (рис. 2.27).

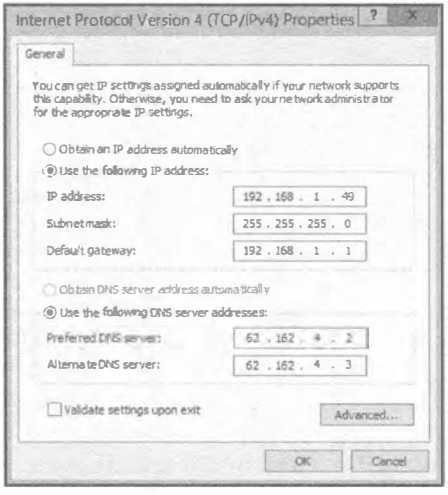


Рис. 2.27. Конфигурирование свойств IPv4

Узнайте у администраторов сети конфигурацию для нового сервера и введите сведения примерно так, как показано на рис. 2.27. Щелкните на кнопке OK, чтобы сохранить настройки, и закройте все оставшиеся диалоговые окна.

То же самое можно проделать в командной строке с помощью команды `netsh`. Позже понадобится проверить имя сетевого интерфейса; для его получения можно воспользоваться командой `ipconfig`.

```
C:\>netsh interface ip set address name="Local Area Connection"
  static 192.168.1.49 255.255.255.0 192.168.1.1
```

Синтаксис команды `netsh` выглядит следующим образом:

```
C:\>netsh interface ip set address name="<Имя сетевого интерфейса>"
  static <Желаемый IP-адрес> <Желаемая маска подсети>
  <Желаемый стандартный шлюз>
```

Конфигурация адресов сервера сохраняется. Необходимо также установить адреса DNS-серверов. Следующая команда `netsh` установит адрес первичного DNS-сервера:

```
C:\>netsh interface ip set dns "Local Area Connection" static 192.168.1.21
C:\>
```

Синтаксис ее такой:

```
netsh interface ip set dns "<Имя сетевого интерфейса>"
  static <IP-адрес первичного DNS-сервера>
```

При наличии вторичного DNS-сервера придется выполнить еще одну команду `netsh`, которая немного отличается:

```
C:\>netsh interface ip add dns "Local Area Connection" 192.168.1.22
C:\>
```

Теперь новая конфигурация IPv4 должна быть применена. Чтобы проверить проделанную работу, следует запустить команду ipconfig:

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5819:d35b:1b24:de7f%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.49
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
Tunnel adapter Local Area Connection* 8:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Tunnel adapter Local Area Connection* 9:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e50:1817:3f21:3f57:fc97
   Link-local IPv6 Address . . . . . : fe80::1817:3f21:3f57:fc97%12
   Default Gateway . . . . . . . . . : ::
C:\>
```

В выводе легко заметить, что адаптер с именем Local Area Connection теперь имеет новую конфигурацию IPv4. Обратите внимание, что в случае запуска команды ipconfig /all вы получите намного больше информации.

Следующее действие заключается в тестировании подключения. Это можно сделать с помощью команды ping, которая посылает тестовый пакет сетевому устройству или серверу:

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=13ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
C:\>
```

В этом примере тестирование производится с использованием стандартного шлюза, который был определен в конфигурации сети IPv4. Обычно это хороший первый шаг. Как видите, для каждого отправленного тестового пакета получен ответ. Если ответы не получены, значит, имеется проблема с оборудованием, драйверами, конфигурацией сети, кабелями или, возможно, даже с самой сетью. Если есть устройства за локальным шлюзом, то вы должны попробовать пропинговать одно из них при условии, что администраторы сети разрешили трафик ICMP. Такой тест подтвердит возможность маршрутизации сервера на удаленные узлы сети.

Переименование сервера

Каждый компьютер Windows должен иметь уникальное имя, чтобы уникальным образом идентифицироваться в рамках сети. Любая организация устанавливает свою

практику назначения имен. В одних организациях применяют хорошо структурированные имена, которые описывают местоположение и функцию, в других используют неописательные имена с увеличивающимися числами, а в третьих — имена персонажей из любимых телевизионных шоу или игроков из команд, за которые они болеют.

Щелкните на ссылке рядом с элементом Computer Name (Имя компьютера), который находится в панели свойств диспетчера серверов (рис. 2.28), для управления именем этого сервера и его членством в домене или рабочей группе. Серверу должно быть назначено имя, соответствующее стандартам именования, принятым в организации. Для этого щелкните на кнопке Change (Изменить), как показано на рис. 2.29.

Рис. 2.28. Элемент Computer Name в свойствах локального сервера

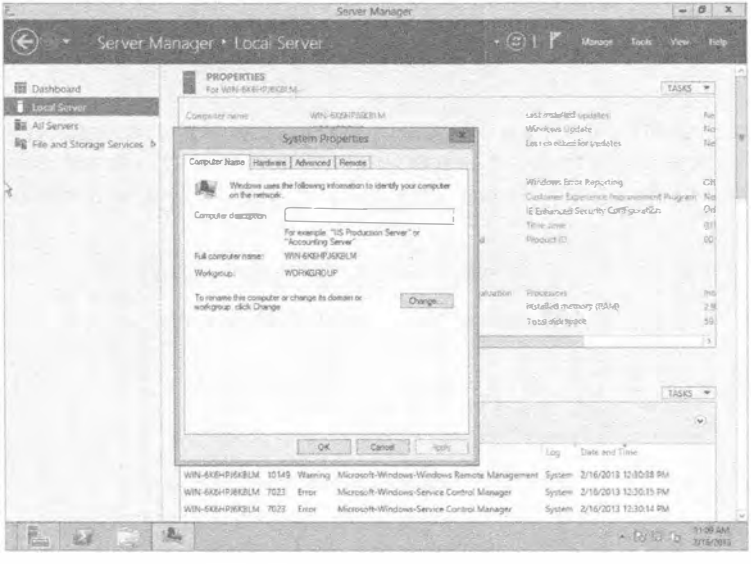


Рис. 2.29. Изменение имени компьютера

Вы выполняли чистую установку Windows Server. Вы можете вспомнить, что процедура установки не запрашивала имя компьютера. Вместо этого сервер получил случайно сгенерированное имя. Некоторым экспертам по безопасности такой принцип нравится, но мы предпочитаем иметь возможность отслеживания своих серверов, поэтому стараемся назначать им структурированные имена.

Измените имя в поле Computer name (Имя компьютера) и щелкните на кнопке OK (рис. 2.30). Удостоверьтесь в том, что имя является уникальным внутри сети, иначе будут возникать проблемы.

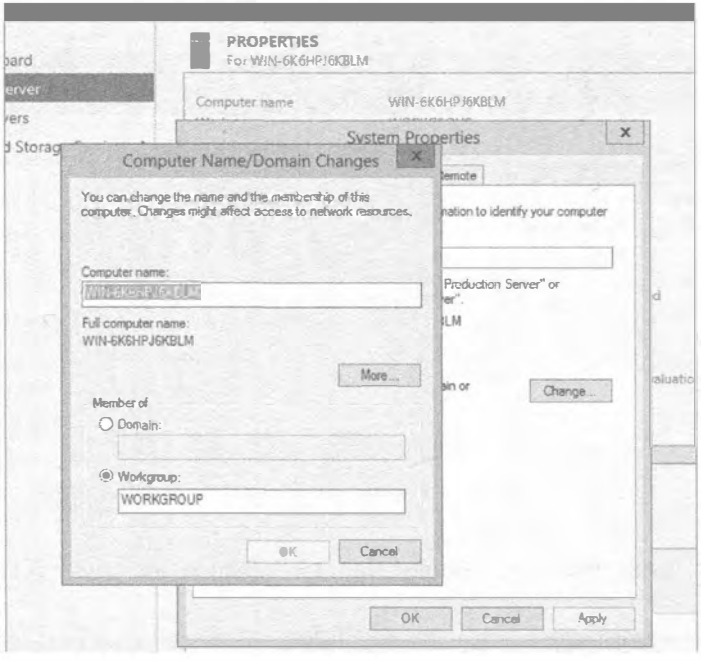


Рис. 2.30. Установка имени компьютера

Откроется диалоговое окно с сообщением о необходимости перезагрузки компьютера, чтобы изменения вступили в силу (рис. 2.31). Закройте оставшиеся диалоговые окна и перезагрузите сервер. После перезагрузки сервер получит новое имя.

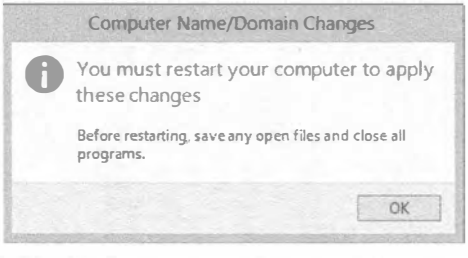


Рис. 2.31. Сообщение о необходимости перезагрузки после изменения имени компьютера

В качестве альтернативы провести аналогичную процедуру переименования можно в командной строке с помощью команды netdom:

```
C:\>netdom /renamecomputer WIN-DCL9MRNLVOH /newname:BIGFIRMAPPSVR1
This operation will rename the computer WIN-DCL9MRNLVOH
to BIGFIRMAPPSVR1.

Certain services, such as the Certificate Authority, rely on a fixed
machine name. If any services of this type are running on
WIN-DCL9MRNLVOH, then a computer name change would have an adverse impact.

Do you want to proceed (Y or N)?
y
The computer needs to be restarted in order to complete the operation.

The command completed successfully.
Эта операция переименует компьютер WIN-DCL9MRNLVOH
на BIGFIRMAPPSVR1.

Определенные службы, такие как центр сертификации, полагаются на
фиксированное имя машины. Если на WIN-DCL9MRNLVOH функционируют
любые службы такого типа, то изменение имени компьютера может иметь
неблагоприятное влияние.

Желаете ли вы продолжить (Y или N)?
y
Для завершения операции компьютер необходимо перезапустить.

Команда успешно завершена.
C:\>
```

Ниже приведен синтаксис команды netdom:

```
netdom /renamecomputer <Текущее имя компьютера>
       /newname:<Желаемое имя компьютера>
```

После выполнения команды netdom понадобится вручную перезагрузить сервер.

После перезагрузки снова войдите в систему и запустите диспетчер серверов. Вы увидите в панели свойств новое имя компьютера.

Присоединение к домену

Скорее всего, вам потребуется присоединить сервер к домену, чтобы получить возможность использования разделяемых ресурсов и централизованного управления. Перейдите в диалоговое окно Computer Name/Domain Changes (Имя компьютера/Изменение домена).

Мы присоединим этот сервер к домену, который имеет DNS-имя BigFirm.com (рис. 2.32). После ввода указанного имени щелкните на кнопке OK. Затем будет предложено ввести имя и пароль пользователя, имеющего права для добавления этого сервера в домен. Им может быть bigfirm\administrator или bigfirm\jbloggs, если пользователю jbloggs были делегированы права в Active Directory. Закройте все диалоговые окна и перезагрузите сервер, после чего вы будете иметь сервер, который является членом домена, и получить в свое распоряжение преимущества групповой политики, пользовательских учетных записей Active Directory и групп доступа, централизованного администрирования и т.д.

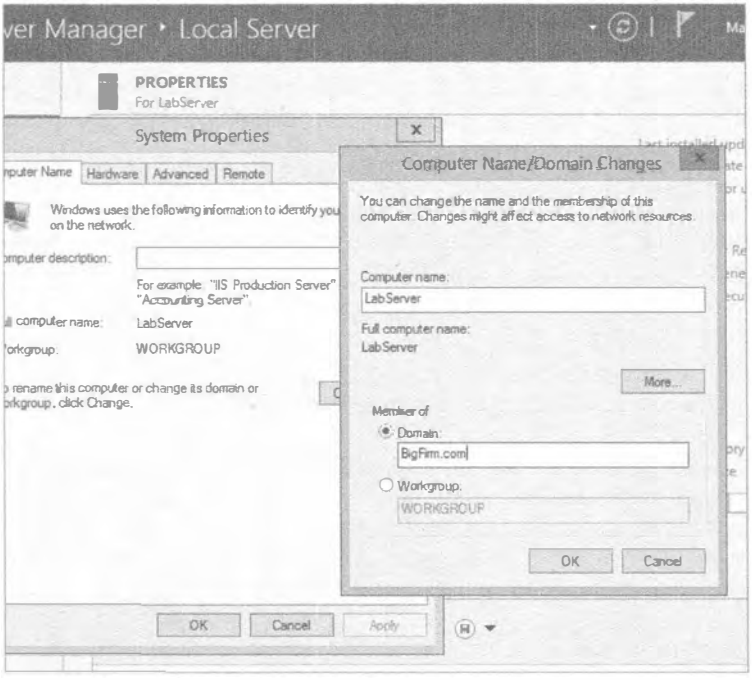


Рис. 2.32. Изменение членства в домене

В качестве альтернативы предыдущую процедуру можно выполнить в командной строке:

```
C:\>netdom join bigfirmappsvrl /Domain: bigfirm.com /UserD:bigfirm\
administrator /PasswordD:*
Type the password associated with the domain user:
Введите пароль, ассоциированный с пользователем домена:
The command completed successfully.
Команда выполнена успешно.
C:\>
```

Для завершения операции компьютер должен быть перезагружен:

Синтаксис `netdom` выглядит следующим образом:

```
netdom join <Имя компьютера, присоединяемого к домену>
    /Domain:<Домен для присоединения>
    /UserD:<Имя пользователя домена с правами для присоединения к домену>
    /PasswordD:*
```

После запуска этой команды будет предложено ввести пароль пользовательской учетной записи. По завершении команды `join` будет указано на необходимость перезагрузки сервера. Можно инициировать автоматическую перезагрузку, добавив флаг `/REBoot`, как показано ниже. Возможно, вы предпочитаете максимально контролировать моменты перезагрузки, тогда проводите ее вручную.

```
netdom join bigfirmappsvr1
    /Domain: bigfirm.com
    /UserD:bigfirm\administrator
    /PasswordD:* /REBoot
```

Почему именно командная строка?

Вас могло заинтересовать, по какой причине мы демонстрируем эти альтернативные подходы с командной строкой. Командная строка пригодится в перечисленных ниже ситуациях.

- Работа проводится в среде Windows Server 2012 R2 Server Core, где альтернатива вообще отсутствует. ОС Windows Server 2012 R2 включает удобный инструмент под названием `sconfig`.
- Процедура запуска таких команд может быть быстрее, чем навигация в рамках графического пользовательского интерфейса.
- При построении множества серверов вручную или с применением какого-нибудь решения для клонирования везде, где только возможно, используются сценарии.

Включение дистанционного администрирования

Большинству администраторов Windows необходима возможность управления своими серверами из рабочих столов. Кому охота бегать в машинный зал каждый раз, когда требуется внести какое-то изменение в систему сервера? Для этого на сервере следует включить удаленный рабочий стол (Remote Desktop). Затем на своем ПК или ноутбуке можно использовать инструмент Remote Desktop для подключения к серверу через TCP-порт 3389, другими словами, по протоколу RDP (Remote Desktop Protocol — протокол удаленного рабочего стола). Возможность включения дистанционного администрирования регламентируется политиками безопасности в организации. Чтобы включить доступ через RDP, в панели свойств локального сервера (Local Server) щелкните на ссылке рядом с элементом Remote Desktop (Удаленный рабочий стол), которая в текущий момент помечена как Disabled (Отключен). На рис. 2.33 видно, что протокол RDP по умолчанию отключен.

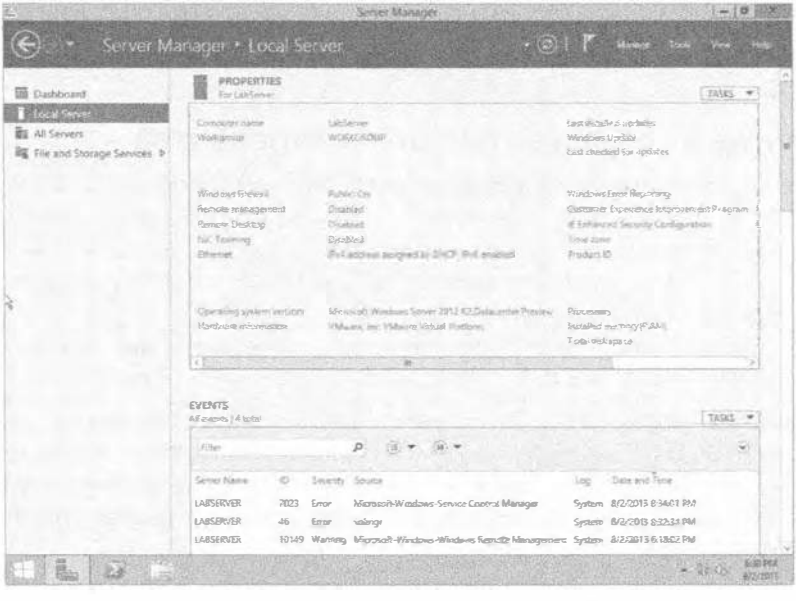


Рис. 2.33. Конфигурирование удаленного рабочего стола

Существуют две других опции.

- Allow Connections from Computers Running Any Version of Remote Desktop (Less Secure) (Разрешить подключения с компьютеров, выполняющих любую версию Remote Desktop (менее безопасно)). Это позволяет подключаться к новому серверу инструменту Remote Desktop версий, предшествующих версии 6. Версия 8 содержит новую функциональность защиты, поэтому в Microsoft рекомендуют применять именно ее. Обратите внимание, что Remote Desktop версии 8 входит в состав Windows Server 2012 R2. Более старые ОС, такие как Windows XP и Windows Server 2003, требуют бесплатного обновления, которое можно получить посредством Windows Update либо из веб-сайта Microsoft.
- Allow Connections Only from Computers Running Remote Desktop with Network Level Authentication (More Secure) (Разрешить подключения только с компьютеров, выполняющих Remote Desktop с аутентификацией сетевого уровня (более безопасно)). Это то, что в Microsoft рекомендуют выбирать, если вы включаете доступ через RDP. Обратите внимание, что для использования данной опции на всех возможных административных компьютерах должен быть установлен инструмент Remote Desktop версии не ниже 6.

По умолчанию доступ к серверу через RDP будут иметь только члены локальной группы администраторов (Administrators). Это подходит в большинстве сценариев. Тем не менее, вы можете принять решение делегировать выполнение определенных низкоуровневых функций персоналу, не входящему в состав администраторов. Для этого понадобится щелкнуть на кнопке Select Users (Выбрать пользователей) и добавить имена пользовательских учетных записей или, что предпочтительнее, имена групп доступа, которым выданы права на подключение посредством протокола RDP.

В данный момент сервер находится в сети, добавлен в домен и на нем включен удаленный рабочий стол, так что с ним можно взаимодействовать дистанционно. Самое время добавить на машину с Windows Server 2012 R2 некоторую функциональность.

Добавление и удаление ролей и компонентов

До настоящего времени вы установили ОС Windows Server 2012 R2 и сконфигурировали ее так, что машина находится в сети и ее можно дистанционно администрировать. Оставшиеся конфигурационные задачи можно выполнять относительно комфортно, тем более, если вспомнить еще и о небольшом мониторе в шумном и прохладном серверном помещении.

Прежде чем открывать диспетчер серверов, необходимо определить ряд терминов, которые уже несколько ряд встречались в этой главе.

- **Роли.** Роль (role) — это обобщенная функция, размещенная на сервере. Роль может быть DNS-сервером или веб-сервером. Каждая роль поступает с набором функциональных средств, которые могут быть установлены на сервере, чтобы позволить компьютеру выполнять нужные задачи. Они называются службами ролей.
- **Компоненты.** Компонент (feature) — это отдельная порция ПО, которая добавляет очень гранулированный фрагмент функциональности на сервер.

Важно упомянуть о том, что компоненты теперь являются частью мастера добавления ролей и компонентов (Add Roles and Features Wizard). В Windows Server 2008 R2 этот мастер является отдельным инструментом, содержащим расширяемый набор ролей и компонентов. Это значит, что со временем в Microsoft могут сделать доступными дополнительные роли и компоненты.

Унаследованные роли и компоненты

В чистой установке Windows Server 2012 R2 какие-либо компоненты или роли отсутствуют. В Microsoft решили не делать предположения за вас. Это позволяет создавать настроенные серверы с минимальным риском в плане безопасности. Однако модернизированный сервер будет включать роли и компоненты, которые программа установки Windows Server 2012 R2 смогла обнаружить на существующем сервере Windows Server 2008. Например, если сервер Windows Server 2008 был DNS-сервером, то модернизированный до Windows Server 2012 R2 сервер будет иметь установленную роль DNS-сервера. При желании можете удалить некоторые из таких унаследованных ролей или компонентов, поскольку они не подходят для нового сервера Windows Server 2012 R2.

Добавление роли

Роль может быть описана как важная функция, которую сервер может играть в сети. Установка роли приводит к установке набора компонентов, обеспечивающих нужную функциональность. Для каждой роли предусмотрен стандартный набор компонентов, который можно настраивать.

Далее будет показано, как добавить роль с применением диспетчера серверов и PowerShell. Прежде всего, запустите диспетчер серверов. В левой части окна диспетчера серверов расположены пункты меню Dashboard (Управляющая панель), Local Server (Локальный сервер), All Servers (Все серверы) и File and Storage Services (Службы файлов и хранилища). Но какие-либо роли или компоненты отсутствуют. Ниже надписи Welcome To Server Manager (Добро пожаловать в диспетчер серверов) находится ссылка Add roles and features (Добавить роли и компоненты), которую можно видеть на рис. 2.34. Щелчок на этой ссылке приводит к запуску мастера добавления ролей и компонентов (Add Roles and Features Wizard).

Мастер добавления ролей и компонентов

Новый мастер добавления ролей и компонентов предлагает огромные по масштабу и динамике возможности выбора. О функциональности и опциях этого мастера можно было бы написать отдельную книгу, но мы собираемся представить здесь только наиболее распространенные случаи его использования.

Многие новые мастера имеют экран приветствия, на котором описана роль того или иного мастера (рис. 2.35). Дальнейшее отображение такого экрана можно отключить, отметив флажок Skip this page by default (По умолчанию пропускать эту страницу).

На следующем экране мастера (рис. 2.36) можно сделать выбор между переключателями Role-based or feature-based installation (Установка на основе ролей или на основе компонентов) и Remote Desktop Services installation (Установка служб удаленного рабочего стола); все это является нововведениями Windows Server 2012 R2.

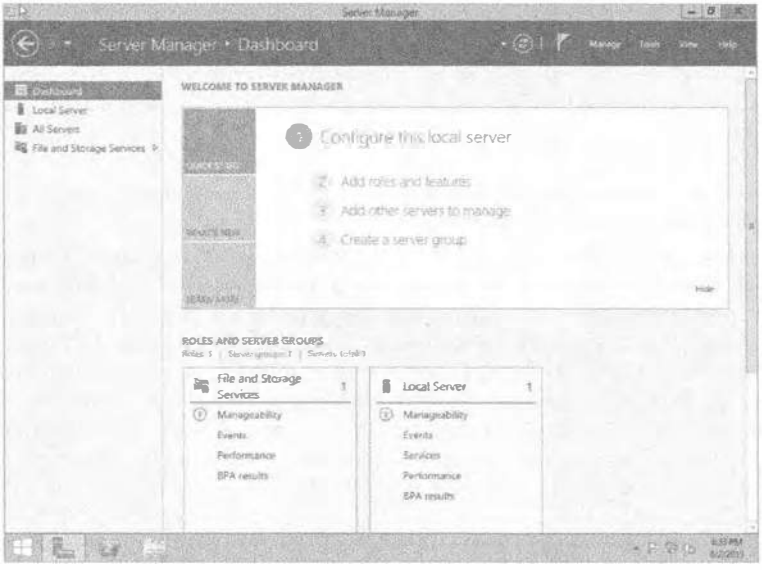


Рис. 2.34. Роли в диспетчере серверов

Рис. 2.35. Экран Before you begin (Прежде чем начать)

На экране Select installation type на выбор предлагаются два варианта. Установка на основе ролей может понадобиться, если необходимо установить роли (все части) или компоненты на одиночный сервер. Переключатель Remote Desktop Services installation выбирается в случае установки либо рабочего стола на основе виртуальной машины, либо рабочего стола на основе сеанса для Remote Desktop Services. Выбор Remote Desktop Services installation приводит к распространению (только логических частей) роли Remote Desktop Services по различным серверам. Мы собираемся применять установку на основе ролей для единственного сервера.

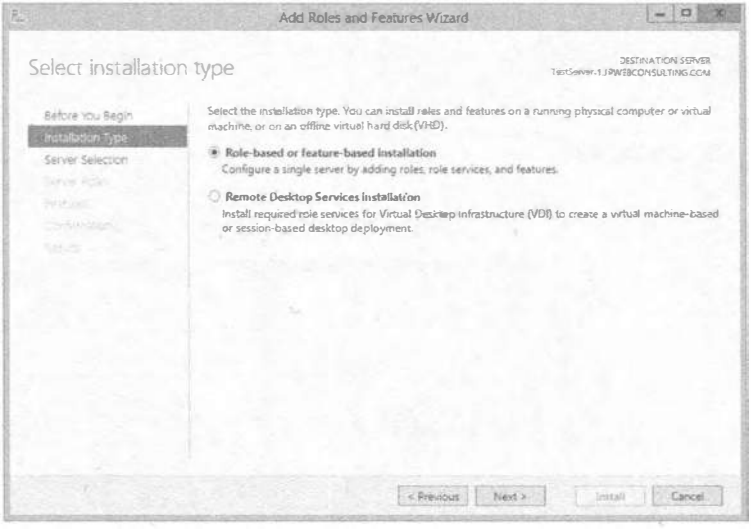


Рис. 2.36. Экран Select installation type (Выбор типа установки)

После выбора переключателя Role-based or feature-based installation появляется экран Select destination server (Выбор сервера назначения), показанный на рис. 2.37. Это тоже новый экран мастера в Windows Server 2012 R2.

- Select a server from the server pool (Выбрать сервер из пула серверов). Выбирайте этот переключатель для установки на сервере из пула серверов.
- Select a virtual hard disk (Выбрать виртуальный жесткий диск). Второй вариант несколько более сложен и налагает ряд требований, которые должны быть удовлетворены, чтобы можно было добавить файл виртуального жесткого диска (virtual hard disk — VHD). Требования перечислены ниже.
- Диски VHD должны функционировать под управлением Windows Server 2012 R2.
- Диски VHD не могут содержать более одного системного тома или раздела.
- Для папки совместного доступа из сети, в которой хранится файл VHD, должны быть выданы следующие права доступа учетной записи компьютера сервера, выбранного с целью монтирования этого файла VHD:
  - права доступа Read (Чтение) / Write (Запись) в диалоговом окне File Sharing (Общий доступ к файлам);
  - права доступа Full Control (Полный доступ) на вкладке Security (Безопасность) диалогового окна File or Folder Properties (Свойства файлов или папок).

Совет по доступу

Для установки роли на диске VHD доступа только пользовательской учетной записи недостаточно. Чтобы разрешить доступ к диску VHD, для папки совместного доступа можно выдать права Read и Write группе Everyone (Все), но по соображениям безопасности это не рекомендуется.

Теперь выберите переключатель Select a server from the server pool. Затем выделите желаемый сервер из списка серверов и щелкните на кнопке Next.

Рис. 2.37. Выбор сервера

Вы увидите перечень всех доступных ролей, которые можно установить (рис. 2.38). При щелчке на каждой из них справа отображается краткое описание роли. Новый настраиваемый сервер должен быть веб-сервером, поэтому отметьте флажок для роли Web Server (IIS) (Веб-сервер (IIS)). После выбора роли Web Server (IIS) откроется диалоговое окно, информирующее о том, что вместе с этой ролью должны быть установлены дополнительные инструменты управления (рис. 2.39). Щелкните на кнопке Add Features (Добавить компоненты), затем щелкните на кнопке Next на экране Select server roles (Выбор серверных ролей). Как видите, мастер динамически корректирует произведенный выбор. Это действительно удобно, т.к. отслеживаются дополнительные компоненты, которые необходимы серверу для того, чтобы делать свою работу в заданной роли.

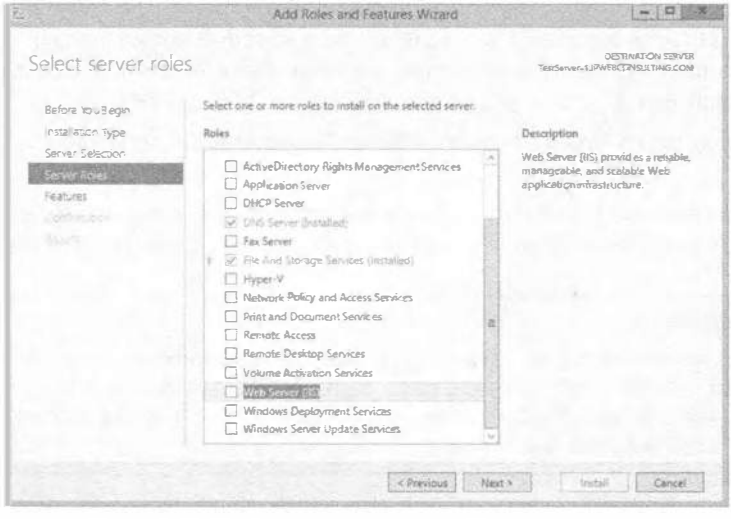


Рис. 2.38. Выбор серверных ролей для установки

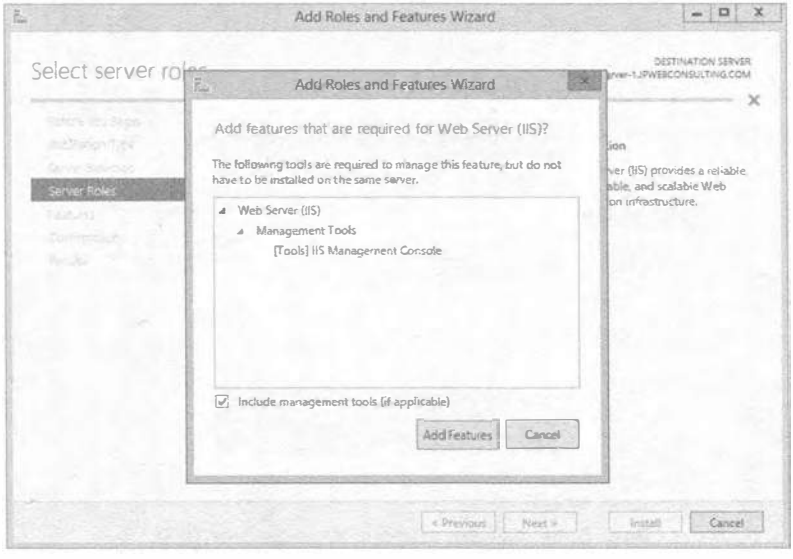


Рис. 2.39. Для веб-сервера IIS требуется установка дополнительных инструментов

На рис. 2.40 показан экран Select features (Выбор компонентов) со списком компонентов, которые можно установить. Подобно ролям, щелчок на каждом компоненте приводит к отображению в правой части экрана краткого его описания. Щелкните на кнопке Next, чтобы продолжить взаимодействие с мастером.

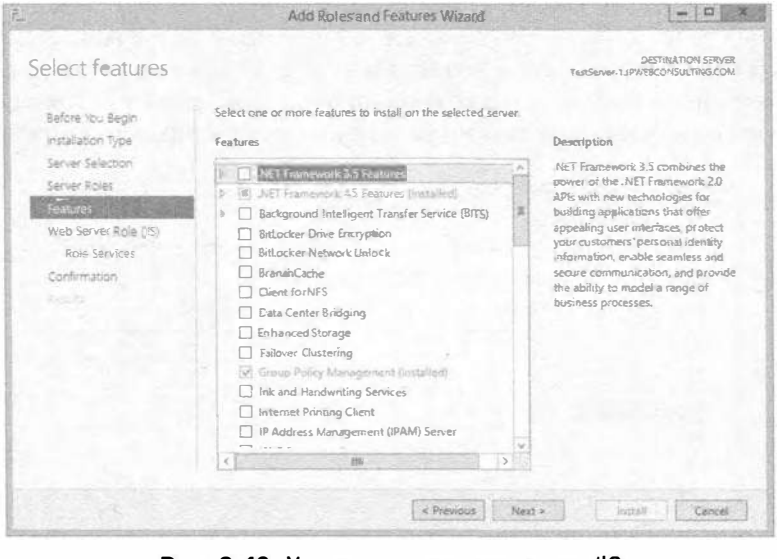


Рис. 2.40. Установка компонентов для IIS

Появляется экран Web Server Role (IIS) (Роль Web Server (IIS)) со сводкой по роли, выбранной для установки, которой в рассматриваемом случае является Web Server (IIS), как можно видеть на рис. 2.41.

Рис. 2.41. Сводка по роли Web Server (IIS)

Роли и компоненты имеют смысл

Обратите внимание, что вам было сообщено о необходимости установки дополнительных компонентов для IIS. Это первый намек на интеллектуальное поведение, положенное в основу всей функциональности ролей и компонентов в Windows Server 2012 R2. По мере продвижения вперед мастер продолжит добавлять новые экраны и опции.

Служба роли является компонентом роли. Она представляет собой либо основной компонент роли, либо необязательный компонент. Каждая роль имеет одну или целый набор стандартных служб ролей. На рис. 2.42 показано, что для роли Web Server по умолчанию отмечено несколько дополнительных ролей. Кроме того, имеется ряд служб ролей, которые можно установить, если в них есть потребность.

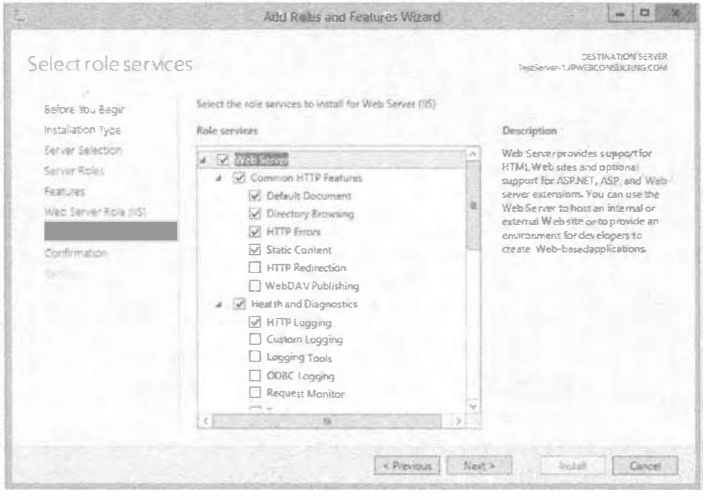


Рис. 2.42. Службы ролей

Разработчики из Microsoft создали все доступные роли, службы ролей и компоненты. Продуманы все отношения, зависимости и конфликты. То же самое касается и диспетчера серверов. Например, если роль требует определенной службы роли, то удаление этой службы роли в результате приводит к удалению самой роли. Это устраняет необходимость в выдвижении предположений администраторами, что, безусловно, хорошо.

Открывается экран подтверждения, на котором можно проверить новую конфигурацию до того, как что-либо будет установлено (рис. 2.43). Щелкните на кнопке Install (Установить), чтобы запустить установку.

Установка некоторых ролей и служб ролей занимает определенное время. Для этого отображается экран с индикатором хода работ, позволяющий отслеживать продвижение процесса установки.

В конечном счете, установка роли успешно завершится. Поскольку автоматические обновления и загрузка исправлений для сервера пока еще не были сконфигурированы, в зависимости от установленной роли может быть выдано предупреждение.

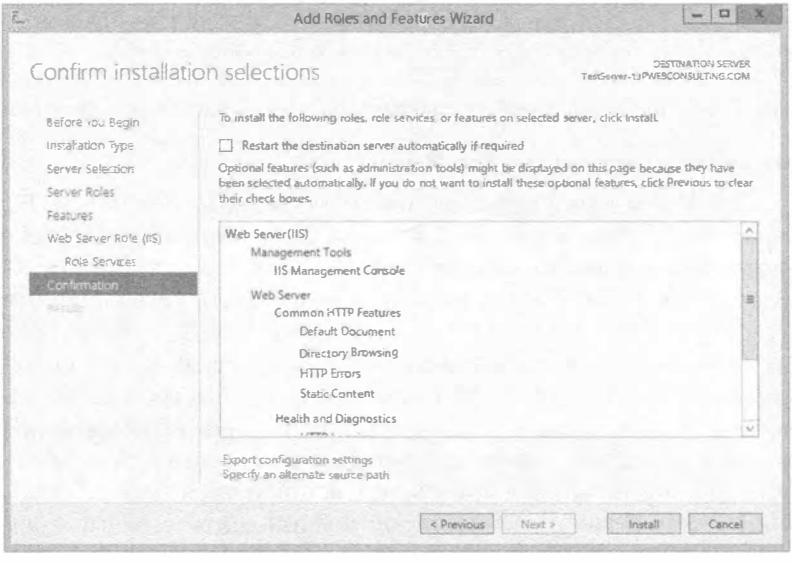


Рис. 2.43. Подтверждение установки

При отработке данного процесса в экспериментальной среде такое предупреждение можно благополучно проигнорировать. Тем не менее, это важное предупреждение. Обновления потребуется сконфигурировать либо на выполнение вручную, либо через групповую политику и затем развернуть их как можно быстрее.

Теперь меню в левой части окна диспетчера серверов содержит только что установленную роль Web Server (IIS), что иллюстрируется на рис. 2.44.

Итак, выше было показано, каким образом добавлять роль и службы ролей с использованием графического пользовательского интерфейса. Это можно также делать с применением командной строки в PowerShell. Именно здесь многие администраторы Windows начинают пропускать страницы. Не поступайте так! Поверьте, вы должны знать данный материал.

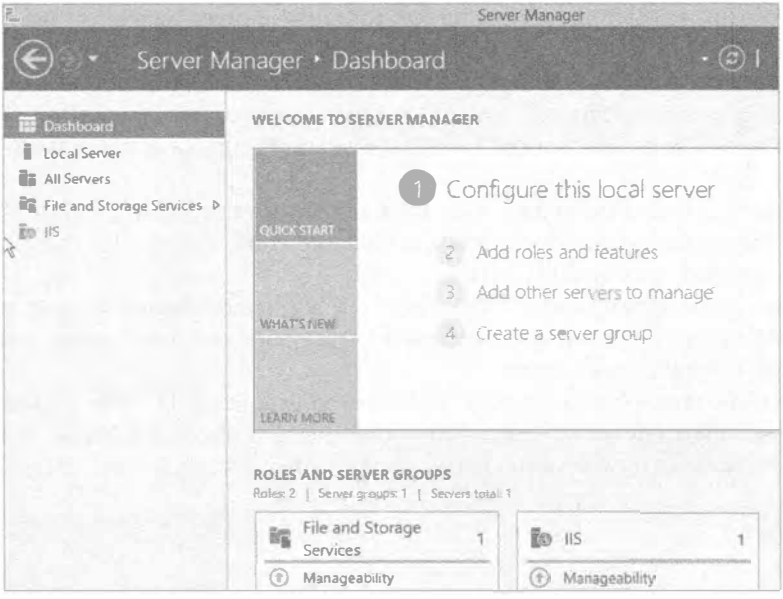


Рис. 2.44. Просмотр ролей в управляющей панели диспетчера серверов

Установка ролей с использованием PowerShell

Роли и компоненты можно устанавливать с помощью PowerShell. Если вы управляете сервером Windows Server 2012 R2, то будете применять PowerShell — сценарный и командный язык от Microsoft. Тема, связанная с PowerShell, довольно обширна. В этой главе будут описаны только командлеты, имеющие отношение к диспетчеру серверов.

Поначалу PowerShell может выглядеть несколько неуклюжим в использовании. Но вскоре вы обнаружите, что он обеспечивает более быстрое получение нужных результатов, чем графический пользовательский интерфейс. Вдобавок PowerShell можно также применять для настройки серверов с помощью сценариев. Это очень удобно, когда для установки Windows Server используется клонирующий или автоматический механизм либо даже при построении множества серверов вручную. Необходимо просто развернуть один образ и запустить подходящий сценарий или файл автоматических ответов для настройки этого общего образа, чтобы он превратился в требуемый сервер.

Запустить PowerShell можно из суперпанели либо щелкнуть на кнопке Start (Пуск) и затем щелкнуть правой кнопкой мыши на большой квадратной кнопке PowerShell. В нижней части экрана появится новая панель меню. Удостоверьтесь, что PowerShell запущен с правами администратора. Модули PowerShell, имеющие отношение к диспетчеру серверов, по умолчанию не загружены. Выполните следующую команду, чтобы загрузить их:

```
PS C:\Users\Administrator> import-module Servermanager
```

Запустив командлет `Get-WindowsFeature`, можно получить отчет по установленным ролям, службам ролей и компонентам:

```
PS C:\Users\Administrator>Get-WindowsFeature
```

Сгенерированный отчет довольно большой, поэтому полностью он здесь не приводится. На рис. 2.45 представлен только фрагмент результатов запроса.

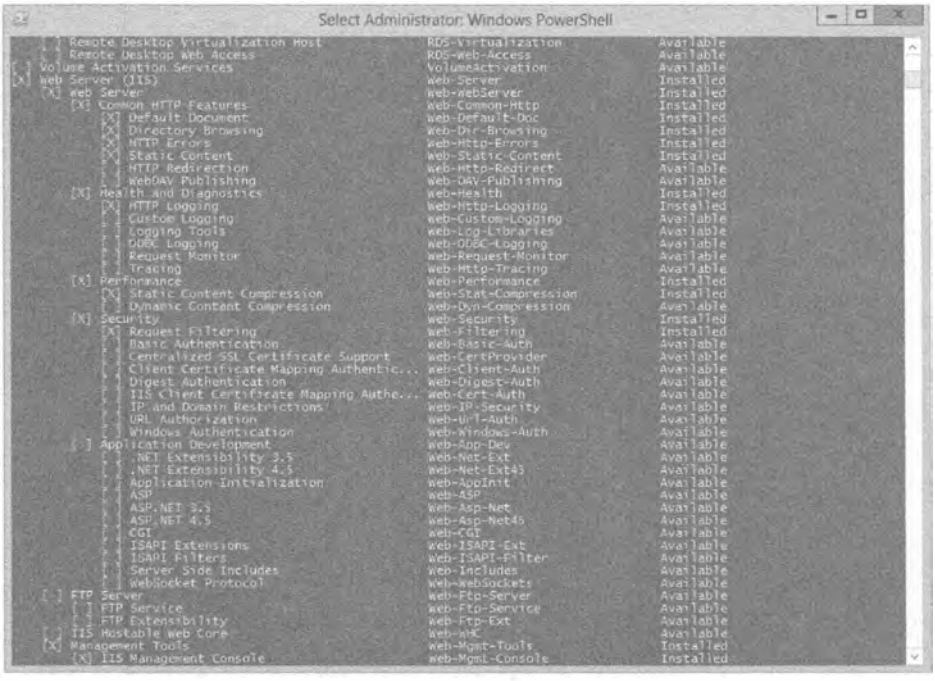


Рис. 2.45. Результат работы командлета `Get-WindowsFeature`

Наличие символа `X` означает, что роль, служба роли или компонент установлен, как это видно для добавленной роли Web Server (IIS). Следовательно, мы работаем с практически пустым сервером.

В рассматриваемом примере мы хотим установить FTP-сервер, который, как показано в нижней части рис. 2.45, все еще доступна для установки (что обозначено словом `Available` (Доступна) в последнем столбце). Обратите внимание на наличие столбца `Name` (Имя), расположенного посередине. Роль FTP Server имеет имя `Web-Ftp-Server`, которое и указывается в командлете `Install-WindowsFeature`:

```
PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Ftp-Server -Restart

Success     RestartNeeded    Exit Code   Feature Result
--------    -------------    ---------   --------------
True        No               Success     {Web-Ftp-Server, Web-Ftp-Service}

PS C:\Users\Administrator>
```

Довольно просто, не так ли? К тому же результат был получен намного быстрее, чем если бы пришлось применять мастер с графическим пользовательским интерфейсом. Поскольку мы знаем, чего хотим, то, насколько быстро это можно сделать, по сути, сводится к скорости набора на клавиатуре.

Некоторые роли, службы ролей или компоненты при своем добавлении требуют перезагрузки. Это можно сделать автоматически, указав при запуске командлета флаг `-restart`.

Давайте проверим установку. Снова запустите PowerShell и выполните командлет `Get-WindowsFeature`; результаты показаны на рис. 2.46:

```
PS C:\Users\Administrator> Get-WindowsFeature
```

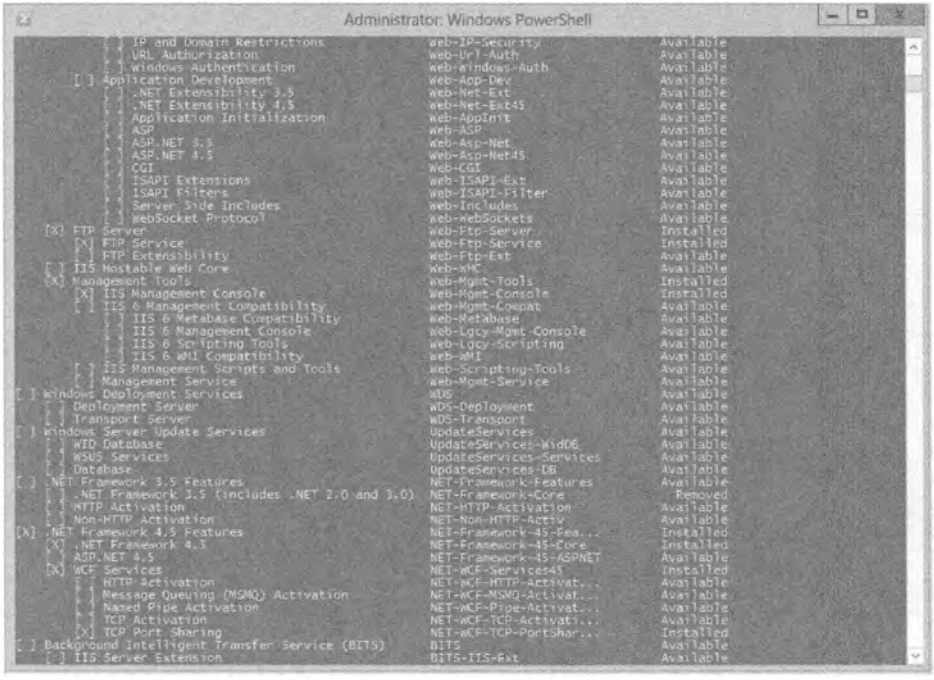


Рис. 2.46. Проверка установленной роли

Запрашиваемые роли и службы ролей помечены символом `X`, а это означает, что они установлены. Вы также заметите, что были установлены и обязательные компоненты для роли FTP Server. Как видите, результаты идентичны тем, что получились бы с использованием графического пользовательского интерфейса, предлагаемого диспетчером серверов.

Теперь у любого, кого немного пугало администрирование из командной строки, должен появиться хотя бы минимальный интерес.

Если необходим текстовый отчет по конфигурации сервера, можете запустить приведенный ниже командлет; отчет будет помещен в файл по имени `c:\InstalledFeatures.txt`:

```
PS C:\Users\Administrator> get-windowsfeature > C:\InstalledFeatures.txt
```

Имеется удобная возможность проверить, что бы произошло в результате запуска команды без ее действительного выполнения. Это делается путем добавления к команде флага `-whatif`:

```
Add-WindowsFeature Name -whatif
```

Например, если вы собираетесь добавить роль `File-Services` и службу роли `FS-Resource-Manager`, то выяснить, что в итоге произойдет, можно с помощью следующей команды:

```
PS C:\Users\Administrator> add-windowsfeature File-Services,
  FS-Resource-Manager -whatif
What if: Checking if running in 'WhatIf' Mode.
Что, если: проверка выполнения в режиме WhatIf.
What if: Performing operation "Add-WindowsFeature"
  on Target "[File Services] File Server Resource Manager".
Что, если: выполнение операции Add-WindowsFeature
  для цели [File Services] File Server Resource Manager.
What if: Performing operation "Add-WindowsFeature"
  on Target "[File Services] File Server".
Что, если: выполнение операции Add-WindowsFeature
для цели [File Services] File Server.
What if: This server may need to be restarted after the
installation completes.
Что, если: этот сервер может нуждаться в перезагрузке после
завершения установки.
Success  Restart Needed   Exit Code   Feature Result
-------  --------------   ---------   --------------
True     Maybe            Success     {}
```

Благодаря флагу `-whatif`, никаких изменений на сервере не произошло. Обратили внимание, что могла бы потребоваться перезагрузка? Знание о том, что после завершения команды необходима перезагрузка, очень важна. Это позволит запланировать перезагрузку и предупредить пользователей различных служб, размещаемых на данной машине.

Установка ролей на нескольких серверах с использованием сценариев в PowerShell

Представьте себе, что вы установили еще большее число ролей, служб ролей и компонентов. Вы могли бы упаковать все это в один сценарий и запускать его по мере необходимости. Благодаря такой возможности командной строки PowerShell, можно было бы автоматически переконфигурировать сотни или даже тысячи серверов, применяя инструмент вроде диспетчера конфигурации системного центра Microsoft (Microsoft System Center Configuration Manager). Теперь вы понимаете мощь PowerShell. Этот инструмент позволяет сберечь часы работы при развертывании или конфигурировании серверов.

До того как слишком глубоко погружаться в настройку установки посредством сценариев, необходимо проверить, разрешено ли вообще запускать сценарии. Откройте PowerShell и запустите следующий командлет:

```
PS C:\Users\Administrator> get-executionpolicy
Restricted
Ограничено
```

Результат выполнения этого командлета указывает на то, что запуск сценариев на сервере запрещен. Это стандартная установка в PowerShell. Чтобы разрешить запуск сценариев на сервере, когда они завершены, понадобится запустить на сервере следующий командлет:

```
PS C:\Users\Administrator> set-executionpolicy unrestricted

Execution Policy Change
```

```
The execution policy helps protect you from scripts that you do not
trust. Changing the execution policy might expose you to the security
risks described in the about_Execution_Policies help topic.
Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Изменение политики выполнения
Политика выполнения помогает защитить от сценариев, которым вы не доверяете. Изменение политики выполнения может привести к рискам в плане безопасности, описанным в теме about_Execution_Policies справочной системы.
Желаете ли вы изменить политику выполнения?
[Y] Да [N] Нет [S] Отложить [?] Справка (по умолчанию Y): Y

Проверить, что изменение вступило в силу, можно с помощью повторного запуска командлета `Get-ExecutionPolicy`:

```
PS C:\Users\Administrator> get-executionpolicy
Unrestricted
```

Не ограничено

Теперь на сервере разрешен запуск сценариев. По причинам, связанным с безопасностью, рекомендуется по завершении выполнения сценариев возвратить политику выполнения снова в состояние `Restricted` (Ограничено).

Давайте посмотрим, как используется сценарий в PowerShell. Вы найдете такой подход удобным, когда требуется добавить роли, службы ролей или компоненты на множество серверов. При этом необходим конфигурационный файл. В целях демонстрации мы воспользуемся мастером добавления ролей и компонентов для экспорта информации по установке роли в XML-файл.

Согласно тому, как было показано ранее, добавьте роль службы удаленного рабочего стола (Remote Desktop Services), но остановитесь на экране подтверждения добавления роли (последнем экране мастера). В нижней части этого экрана имеется ссылка Export configuration settings (Экспортировать параметры конфигурации), которая позволяет экспортировать конфигурацию в файл (рис. 2.47).

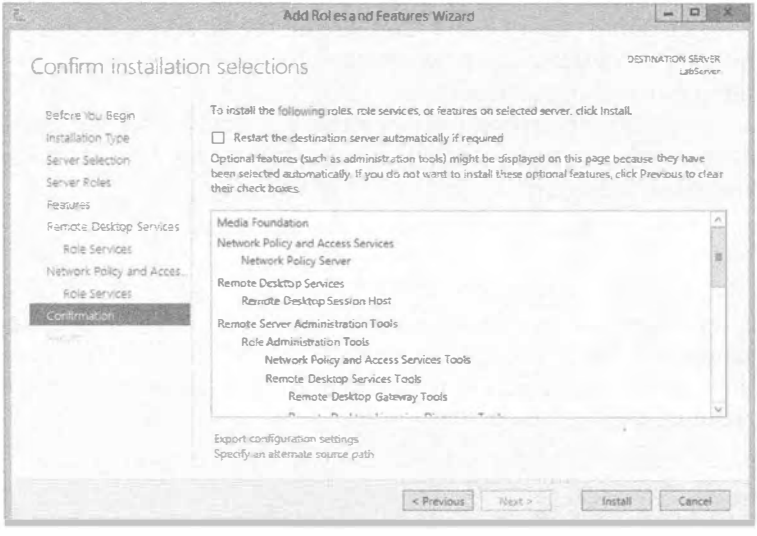


Рис. 2.47. Экспортирование конфигурации роли в XML-файл

Сохраните конфигурацию в файл `RemoteDesktopConfig.xml` в корневой папке на диске C или в другом удобном месте. Если хотите, можете открыть его в браузере Internet Explorer. На рис. 2.48 приведена часть этого файла. Теперь, когда файл сохранен, можно прервать работу мастера. Не щелкайте на кнопке Install (Установить)!

Рис. 2.48. XML-файл с конфигурационной информацией

Итак, все готово к установке роли Remote Desktop Services на множество компьютеров с применением файла сценария. Откройте окно PowerShell, щелкнув правой кнопкой мыши на значке PowerShell в панели задач, и выберите в контекстном меню пункт Run as Administrator (Запуск от имени администратора).

Внутри PowerShell добавьте следующую функцию:

```
function Invoke-WindowsFeatureBatchDeployment {
   param (
      [parameter(mandatory)]
      [string[]] $ComputerNames,
      [parameter(mandatory)]
      [string] $ConfigurationFilePath
   )
   # Развернуть компоненты одновременно на множестве компьютеров.
   $jobs = @()
   foreach($ComputerName in $ComputerNames) {
      $jobs += Start-Job -Command {
         Install-WindowsFeature -ConfigurationFilePath
$using:ConfigurationFilePath -ComputerName $using:ComputerName -Restart
      }
   }
   Receive-Job -Job $jobs -Wait | Select-Object Success,
        RestartNeeded, ExitCode, FeatureResult
```

Эта функция принимает несколько параметров — список имен компьютеров, на которые будет добавлена роль Remote Desktop Services, и путь к файлу со сценарием. Вызовите созданную функцию, передав ей необходимые параметры, с помощью показанного ниже фрагмента кода:

```
# Пример вызова
$ServerNames = 'TestServer_01', 'LabServer_02'
Invoke-WindowsFeatureBatchDeployment -ComputerNames
  $ServerNames -ConfigurationFilePath C:\RemoteDesktopConfig.xml
```

В следующей строке из фрагмента кода указаны имена серверов, которые вы должны привести в соответствие с используемыми у вас именами. В примере заданы имена серверов `TestServer_01` и `LabServer_02`, разделенные запятой. Можно указывать столько серверов, сколько необходимо, например:

```
$ServerNames = 'TestServer_01', ' LabServer_02', ' LabServer_03',
  ' LabServer_04'
```

В следующей строке из фрагмента кода необходимо указать реальный путь к сохраненному ранее XML-файлу:

```
-ConfigurationFilePath C:\RemoteDesktopConfig.xml
```

После ввода последней строки нажмите <Enter> и процесс установки начнется. Он может занять некоторое время.

Проверить установку можно с помощью такой команды:

```
PS C:\Users\Administrator> Get-WindowsFeature
```

И снова любые установленные роли, службы ролей или компоненты помечаются символом `X`. Обратите внимание на столбец `Name` (Имя). Информация в нем будет использоваться в будущих командах. Если вы уже знаете, какую роль или компонент заинтересованы изучить, то попробуйте запустить такую команду:

```
PS C:\Users\Administrator> get-windowsfeature RSAT-RDS-Tools

Display Name                          Name            Install State
------------                          ------          -------------
[X] Remote Desktop Services Tools     RSAT-RDS-Tools  Installed
```

Удаление роли

Удаление ролей, служб ролей и компонентов с помощью PowerShell выполняется так же просто, как и их установка. Командлет `Remove-WindowsFeature` похож на командлет `Install-WindowsFeature`:

```
Remove-WindowsFeature <Role>,<RoleService>,<Feature> -restart -whatif
```

Ниже описано, как его применять.

- Введите роль, службу роли или компонент, который требуется удалить. Их можно указывать несколько, разделяя запятыми.
- Используйте флаг `-restart` для инициирования автоматической перезагрузки, если она необходима.
- Используйте флаг `-whatif` для эмуляции выполнения команды.

Приведенная ниже команда эмулирует удаление ранее установленной роли FTP-сервера:

```
PS C:\Users\Administrator> remove-windowsfeature Web-Ftp-Server -whatif
What if: Continue with removal?
Что, если: Продолжить удаление?
What if: Performing uninstallation for "[Web Server (IIS)] FTP Server".
Что, если: выполнить удаление для [Web Server (IIS)] FTP Server.
What if: Performing uninstallation for "[Web Server (IIS)] FTP Service".
Что, если: выполнить удаление для [Web Server (IIS)] FTP Service.
What if: The target server may need to be restarted after the removal
completes.
Что, если: по завершении удаления целевой сервер может потребовать
перезапуска.

Success    Restart Needed    Exit Code      Feature Result
-------    --------------    ---------      --------------
True       Maybe             Success        {FTP Server, FTP Service}
```

Если такое поведение команды устраивает, можете устранить флаг -whatif:

```
PS C:\Users\Administrator> remove-windowsfeature Web-Ftp-Server

Success    Restart Needed    Exit Code      Feature Result
-------    --------------    ---------      --------------
True       Yes               SuccessRest... {FTP Server, FTP Service}
WARNING: You must restart this server to finish the removal process.
ПРЕДУПРЕЖДЕНИЕ: для завершения процесса удаления вы должны перезапустить
этот сервер.
```

Сервер понадобится перезагрузить. Перезагрузку можно выполнить автоматически, воспользовавшись следующей командой:

```
PS C:\Users\Administrator> remove-windowsfeature Web-Ftp-Server -restart
```

Удаление роли завершено. Чтобы установить только компоненты, повторите процесс установки роли. Добравшись до экрана **Select server roles** (Выбор серверных ролей), щелкните на кнопке **Next**, чтобы пропустить добавление ролей. На открывшемся далее экране выберите любые нужные компоненты, после чего завершите процесс, как это делалось при добавлении роли.

Диагностика ролей и компонентов

Одной из работ, выполняемых администратором IT, является поддержание серверов в работоспособном состоянии. Это включает мониторинг всех ролей и компонентов сети с целью обеспечения их работоспособности при пиковых нагрузках.

Помощь в такой работе оказывает диспетчер серверов. Прежде всего, в управляющей панели диспетчера серверов теперь применяется цветовое кодирование. В случае возникновения проблемы предупреждение отображается красным цветом. На рис. 2.49 видно, что с компонентом **BPA results** (Результаты анализатора передового опыта (Best Practices Analyzer — BPA)) в DNS связаны три проблемы. Мы должны приступить к исследованию этих проблем. Необходимо шелкнуть на элементе **DNS** в меню слева, чтобы получить доступ ко всем инструментам анализа производительности, помогающим найти проблему.

Внутри каждой роли можно просматривать следующую информацию.

- **Servers (Серверы).** Здесь перечислены серверы с установленными ролями (рис. 2.50). Внутри этого окна есть несколько средств для получения дополнительных сведений. Щелкнув правой кнопкой мыши на заголовке (рис. 2.51), можно добавить столбцы с другой информацией. Мы добавляем столбец с версией ОС, чтобы видеть, какая версия ОС функционирует на том или ином сервере. В случае одного сервера это может быть не так уж важно, но при наличии пула серверов или веб-фермы данный столбец может быть удобен.
- **Events (События).** Это очень полезный инструмент, помогающий диагностировать проблемы. Подобно программе просмотра событий в предыдущих версиях ОС, здесь предоставляется важная для поиска неполадок информация. У нас имеется предупреждение, связанное с ролью DNS. При этом отображается краткая форма предупреждения или ошибки. Щелчок на сообщении приводит к выводу детального описания проблемы (рис. 2.52).
- **Services (Службы).** Это удобный инструмент, который показывает только службы, ассоциированные с конкретной ролью. Щелкнув на элементе Local Server (Локальный сервер), вы увидите все службы, выполняющиеся на локальной машине. Из этого окна можно также запускать, останавливать и приостанавливать службы (рис. 2.53).
- **Best Practices Analyzer (Анализатор передового опыта).** Этот инструмент сканирует роли и измеряет их соответствие передовому опыту в восьми разных категориях:
  - Security (Безопасность)
  - Performance (Производительность)
  - Configuration (Конфигурация)
  - Policy (Политика)
  - Operation (Операция)
  - Pre-Deployment (Предразвертывание)
  - Post-Deployment (Постразвертывание)
  - Prerequisites (Предварительные условия)

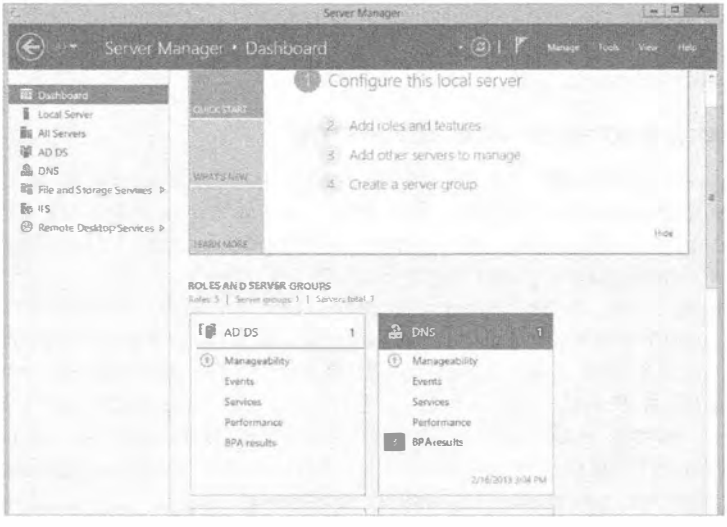


Рис. 2.49. Цветовое кодирование предупреждений в диспетчере серверов

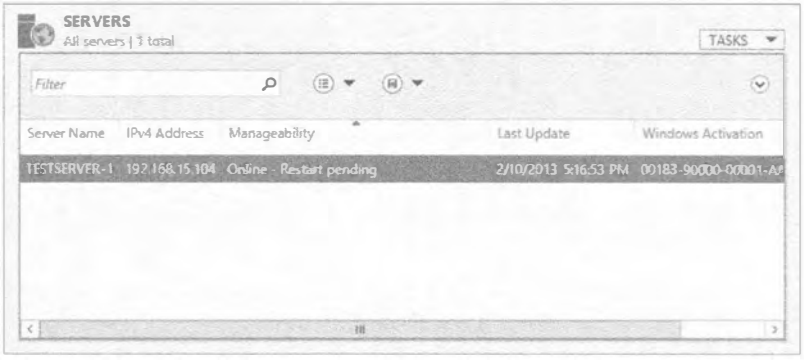


Рис. 2.50. Окно Servers

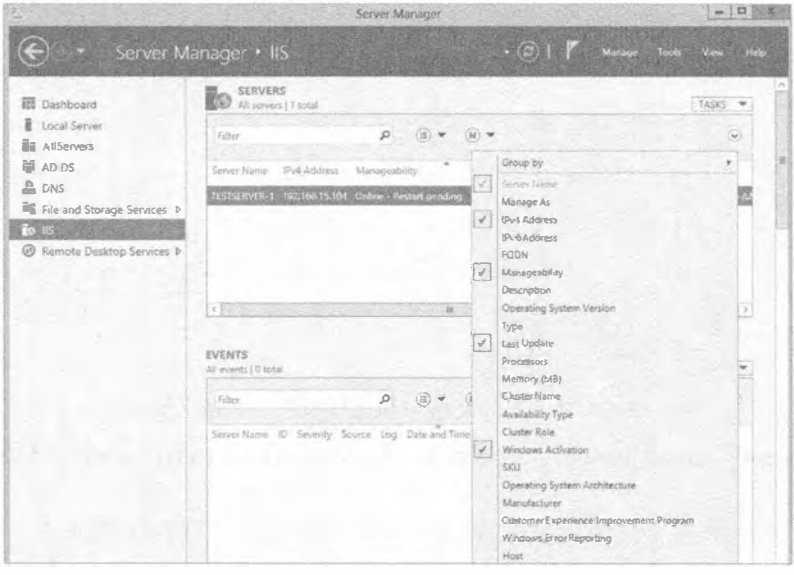


Рис. 2.51. Добавление столбцов с информацией

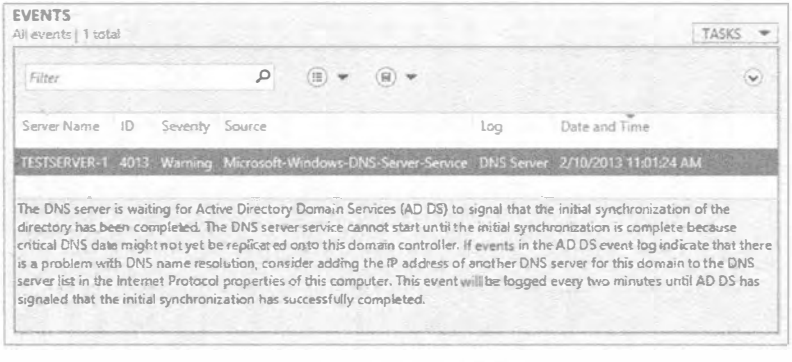


Рис. 2.52. Окно Events

Рис. 2.53. Окно Services

Запустить сканирование легко. Просто щелкните на кнопке Tasks (Задачи) в окне Best Practices Analyzer для роли, как показано на рис. 2.54.

Рис. 2.54. Запуск инструмента Best Practices Analyzer

Теперь необходимо выбрать сервер, для которого будет выполнено сканирование (рис. 2.55).

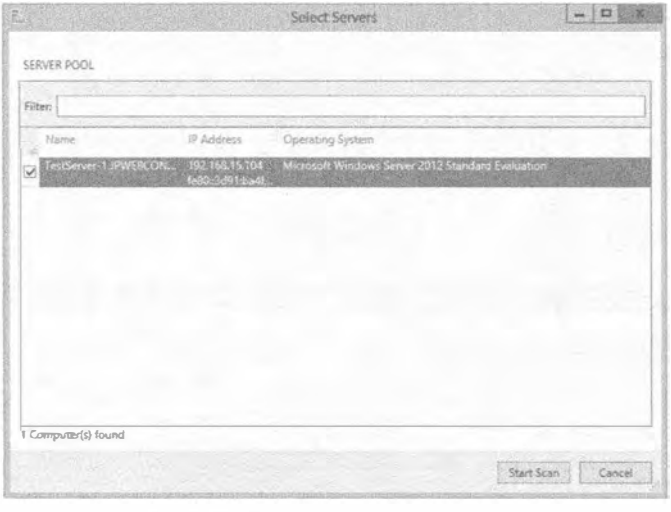


Рис. 2.55. Выбор сервера для сканирования

Сканирование займет несколько минут. Как и в окне Events, вы получите список ошибок и предупреждений (рис. 2.56).

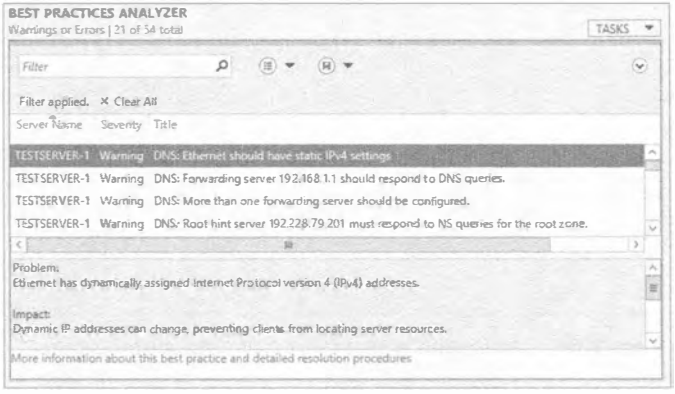


Рис. 2.56. Результаты запуска инструмента Best Practices Analyzer

Щелчок на предупреждении или ошибке позволяет получить подробное описание проблемы. Ниже описания предлагается ссылка для получения дополнительной информации о проблеме.

- Performance (Производительность). В этом окне отображаются данные о производительности отдельной роли (рис. 2.57). По умолчанию счетчик производительности отключен. Щелкните правой кнопкой мыши на сервере в списке и запустите счетчик производительности.

  В диалоговом окне Configure Performance Alerts (Конфигурирование предупреждений производительности) можно настроить параметры использования ЦП, памяти и количества дней для построения графика (рис. 2.58).

- Roles And Features (Роли и компоненты). В этом окне отображаются дополнительные компоненты, ассоциированные с ролью. На рис. 2.59 показано окно Roles And Features для роли Web Server (IIS), в котором перечислены все роли и компоненты, относящиеся к IIS.

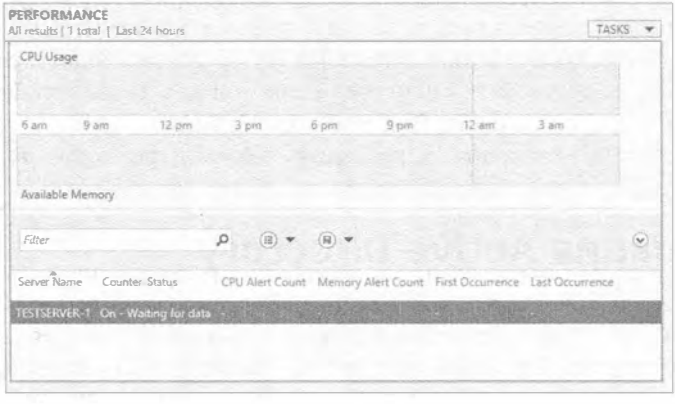


Рис. 2.57. Окно Performance

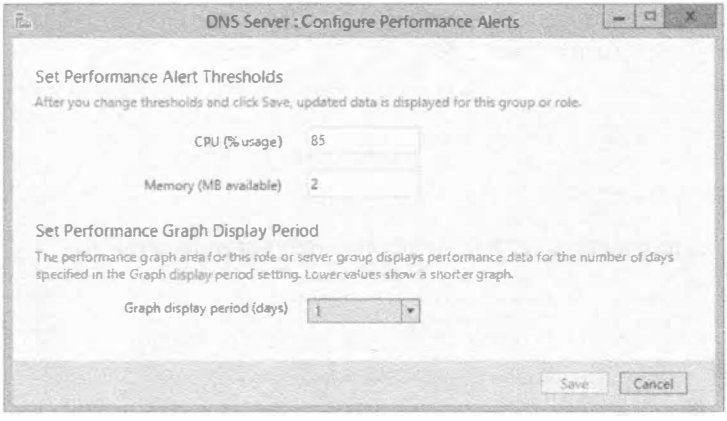


Рис. 2.58. Параметры, связанные с производительностью

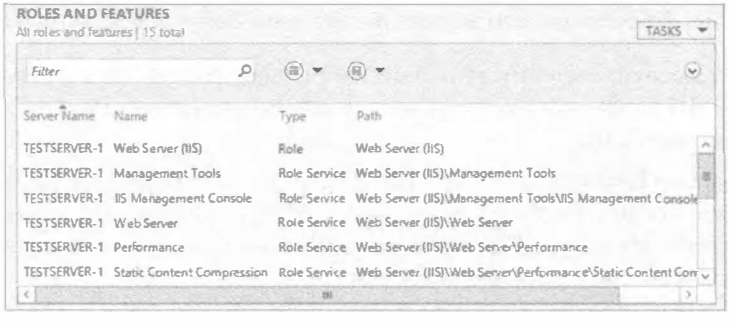


Рис. 2.59. Окно Roles And Features

Описанные выше инструменты помогают управлять и устранять неполадки в установленных ролях и компонентах без необходимости в запуске пяти разных программ, как это было на унаследованных серверах.

Заключительное слово о диспетчере серверов

Вы узнали, что утилита `servermanagercmd` была объявлена устаревшей в Microsoft, а также научились устанавливать и удалять роли и компоненты с применением PowerShell и графического пользовательского интерфейса диспетчера серверов. Вы также видели, как использовать диспетчер серверов для диагностики ролей и компонентов, в том числе инструмент Best Practices Analyzer.

Итак, самое время переходить к рассмотрению контроллеров доменов и Active Directory.

Модернизация Active Directory

Хорошая новость для читателей: мы не собираемся раскрывать здесь эту тему полностью. Она будет рассматриваться в главе 7, а в данной главе мы лишь кратко упомянем о ней для тех, кто работал с Active Directory (AD) в прошлом. Если вам не приходилось иметь дело с AD, не переживайте — просто пропустите следующие несколько страниц; вы узнаете об AD в главе 7.

Обзор Active Directory: новая функциональность в Windows Server 2012 R2

Как обычно, с появлением новой версии ОС Windows Server необходимо ознакомиться с новой функциональностью и проектными возможностями в Active Directory. Многие аспекты новой функциональности должны понравиться, т.к. они были введены в ответ на пожелания пользователей. Некоторые из новых опций определенно ответят на ряд вопросов, часто задаваемых на форумах поддержки в Интернете.

Что нового в службах доменов Active Directory

Службы доменов Active Directory (Active Directory Domain Services — AD DS) позволяют развертывать контроллеры доменов либо локально, либо в облаке. При развертывании контроллеров доменов имеется семейство задач администрирования, которые могут быть легко выполнены с использованием AD DS. Ниже рассматриваются новые функциональные возможности, которые вы можете счесть полезными.

Корзина Active Directory

Слышите ли вы крик администраторов Active Directory со всего мира? Худшим кошмаром любого администратора домена было удаление объектов. После того как в Windows Server 2008 R2 был добавлен компонент корзины Active Directory, появилась возможность восстанавливать объекты, если они были удалены недавно, минуя неприятные процедуры восстановления из резервной копии. Корзина Active Directory (Active Directory Recycle Bin) позволяла быстро восстановить случайно удаленные объекты с помощью нового более простого процесса. Единственная проблема заключалась в том, что корзина не обладала дружественным к пользователю интерфейсом. В версии Windows Server 2012 R2 указанная проблема была решена — корзина Active Directory снабжена развитым пользовательским интерфейсом, который упрощает восстановление объектов. Время восстановления сокращается, т.к. появилось согласованное представление удаленных объектов.

Детализированные политики паролей

Один из наиболее распространенных вопросов, задаваемых с момента начального выпуска Active Directory, звучал следующим образом: "Как можно иметь более одной политики паролей?". Официальный ответ от Microsoft был таким: для этого необходимо располагать более чем одним доменом. Конечно, это противоречит базовой проектной цели, заключающееся в сокращении количества доменов в сетях. Это также вносит путаницу, когда о домене больше не приходится думать как о границе безопасности — домен является границей политики, а границей безопасности становится лес.

Решение, при котором не задействовались продукты третьих сторон, возможно, не поддерживаемые Microsoft, предусматривало создание домена для каждой необходимой политики паролей (что приводило к появлению множества дочерних доменов) или переход на какой-нибудь программный продукт третьей стороны, позволяющий иметь в одном домене сразу несколько политик паролей.

Цель детализированных политик паролей — связать с важными пользовательскими учетными записями более строгие политики; другими словами, с теми пользователями, которые имеют обширный доступ к системам или ценным данным. Однако

в конечном итоге определенные вручную настройки политик не вели себя ожидаемым образом и становились весьма требовательными в плане затрат времени. ОС Windows Server 2012 R2 теперь позволяет управлять политиками с применением центра администрирования Active Directory (Active Directory Administrative Center), который упрощает управление объектами настройки паролей.

Быстрое развертывание посредством клонирования

Клонирование по определению означает "создание идентичной копии чего-либо". Каким же образом клонирование используется с AD DS? Выражаясь кратко, теперь создавать точную реплику или клонировать существующий виртуальный контроллер домена можно в AD DS.

Поднять одиночный виртуальный контроллер домена можно с применением интерфейса для поднятия контроллеров доменов в диспетчере серверов и затем быстро развернуть дополнительные виртуальные контроллеры доменов внутри того же самого домена посредством клонирования. Первым делом, создайте копию существующего виртуального контроллера домена и авторизуйте исходный контроллер домена для клонирования в AD DS. Используя командлеты PowerShell, можно создать конфигурационный файл с детальными инструкциями по поднятию, такими как имя, IP-адрес и DNS-серверы. Путем клонирования удастся сохранить время, устраняя повторяющиеся задачи развертывания.

Упрощенное управление

Для упрощения интерфейса управления AD DS были усовершенствованы перечисленные ниже области:

- динамическое управление доступом (Dynamic Access Control);
- отключенное присоединение к домену с помощью (DirectAccess Offline Domain Join);
- служба федерации Active Directory (Active Directory Federation Services — AD FS);
- средство просмотра хронологии Windows PowerShell (Windows PowerShell History Viewer);
- пользовательский интерфейс корзины Active Directory;
- репликация и топология Active Directory (Active Directory Replication and Topology);
- командлеты Windows PowerShell;
- активация на базе Active Directory (Active Directory Based Activation — AD BA);
- групповые управляемые учетные записи служб (Group Managed Service Account — gMSA).

Средство просмотра хронологии Windows PowerShell

Если вы внимательно читали данную главу, то должны быть практически экспертом в PowerShell. Инструмент PowerShell в настоящем и будущих выпусках Windows Server воплощает усилия многих разработчиков, поскольку все большее и большее число администраторов изучают и применяют PowerShell.

В какой-то момент вы поймете, что производительность, безопасность и скорость развертывания обеспечивают более эффективный способ управления, не-

жели симпатичный графический пользовательский интерфейс (и связанные с его использованием накладные расходы). Помните DOS? Так вот, считайте PowerShell своего рода усовершенствованной системой DOS. Как только вы начнете пользоваться PowerShell, вы оцените все его преимущества. Средство просмотра хронологии Windows PowerShell поможет одолеть кривую изучения PowerShell и привлечет интерес со стороны даже большего числа администраторов.

Например, вы применяете Active Directory Administration Center для добавления пользователя. В пользовательском интерфейсе отображается эквивалент Windows PowerShell для команды Active Directory. Администратор может скопировать синтаксис для последующего использования его в сценариях.

Что нового в AD CS

Давайте обсудим новые и расширенные возможности, которые стали доступны в этой версии службы сертификатов Active Directory (Active Directory Certificate Services — AD CS). Первым делом, кратко посмотрим, что собой представляют службы AD CS. Этот очень важный инструмент безопасности предоставляет службы для управления и распределения сертификатов открытых ключей. Они главным образом применяются программными системами защиты, которые используют технологии открытых ключей. Эти службы допускают настройку для усиления безопасности путем привязки идентичности устройства, человека или службы к секретному ключу.

Интеграция с диспетчером серверов

Устанавливать AD CS вместе с шестью связанными ролями теперь можно с помощью диспетчера серверов. Подобно тому, как было описано в разделе "Добавление роли" ранее в главе, службы ролей AD CS можно добавить с использованием мастера добавления ролей и компонентов. После этого они будут отображаться в управляющей панели диспетчера серверов, как и любая другая роль. И подобно любой другой роли ими можно управлять на множестве серверов из одного местоположения.

Развертывание и управление с помощью Windows PowerShell

Службы ролей AD CS могут быть развернуты с применением командлетов PowerShell, как было показано ранее в этой главе во время демонстрации использования PowerShell для добавления роли. Ниже перечислены новые командлеты, предназначенные для установки и удаления AD CS и связанных ролей.

- `Install-AdcsCertificationAuthority`. Устанавливает службу роли Certification Authority (Центр сертификации).
- `Install-AdcsEnrollmentPolicyWebService`. Устанавливает службу роли Certificate Enrollment Policy Web Service (Веб-служба политик развертывания сертификатов).
- `Install-AdcsEnrollmentWebService`. Устанавливает службу роли Certificate Enrollment Web Service (Веб-служба развертывания сертификатов).
- `Install-AdcsNetworkDeviceEnrollmentService`. Устанавливает службу роли Network Device Enrollment (Развертывание сетевых устройств).
- `Install-AdcsOnlineResponder`. Устанавливает службу роли Online Responder (Онлайновый автоответчик).

- `Install-AdcsWebEnrollment`. Устанавливает службу роли Certification Authority Web Enrollment (Веб-развертывание центра сертификации).
- `Uninstall-AdcsCertificationAuthority`. Удаляет службу роли Certification Authority.
- `Uninstall-AdcsEnrollmentPolicyWebService`. Удаляет службу роли Certificate Enrollment Policy Web Service.
- `Uninstall-AdcsEnrollmentWebService`. Удаляет службу роли Certificate Enrollment Web Service.
- `Uninstall-AdcsNetworkDeviceEnrollmentService`. Удаляет службу роли Network Device Enrollment.
- `Uninstall-AdcsOnlineResponder`. Удаляет службу роли Online Responder.
- `Uninstall-AdcsWebEnrollment`. Удаляет службу роли Certification Authority Web Enrollment.

Что нового в роли Active Directory Rights Management Services

Роль AD RMS (Active Directory Rights Management Services — службы управления правами Active Directory) предназначена для оказания помощи в разработке и сопровождении решений защиты. С помощью роли AD RMS можно поддерживать аутентификацию, шифрование и сертификаты. Давайте посмотрим, что в ней нового.

Изменения в AD RMS, влияющие на SQL Server

В предыдущих выпусках Windows Server для установки AD RMS на любой машине SQL Server, где планировалось хранить данные AD RMS, требовались полномочия локального администратора. Причина в том, что для проведения установки необходима была возможность чтения конфигурационных параметров SQL Server из реестра. Требования для конфигурирования SQL Server с AD RMS изменились. Учетная запись, используемая для установки AD RMS, должна иметь полномочия системного администратора в установленной копии the SQL Server.

Необходимо также иметь функционирующий браузер SQL Server, чтобы службы AD RMS могли видеть экземпляр SQL Server.

Изменения в развертывании AD RMS для диспетчера серверов и Windows PowerShell

Еще один дефект AD RMS в предыдущих выпусках Windows Server заключался в том, что роль AD RMS можно было развертывать только на том же сервере, на котором она устанавливалась. Благодаря обширным усовершенствованиям, внесенным в диспетчер серверов и его интеграции с AD RMS, диспетчер серверов теперь поддерживает дистанционное развертывание на целевых серверных компьютерах.

Использование Windows PowerShell для развертывания AD RMS

Как было описано ранее в разделе, посвященном применению командлетов Windows PowerShell для установки ролей, теперь аналогичным образом можно устанавливать и AD RMS. В следующем списке приведены новые командлеты, предназначенные для этого.

- `Add-WindowsFeature ADRMS -IncludeAllSubFeature -IncludeManagementTools`. Этот командлет добавляет все службы ролей и инструменты AD RMS. Он загружает все поддерживающие файлы, необходимые для работы с AD RMS.
- `Add-WindowsFeature ADRMS-Server`. Этот командлет добавляет только роль AD RMS Server. Он также загружает все файлы, необходимые для поддержки установки сервера AD RMS.
- `Add-WindowsFeature ADRMS-Identity`. Этот командлет добавляет поддержку федерации идентичностей для AD RMS. Он также загружает все файлы, необходимые для поддержки работы AD RMS с AD FS.

Стратегии модернизации Active Directory

Для модернизации Active Directory существует несколько отличающихся сценариев. Провести прямую модернизацию Active Directory из 32-разрядной ОС Windows Server 2008 до Active Directory в Windows Server 2012 R2 невозможно, но можно выполнить модернизацию на месте с версии Windows Server 2008 R2 до Windows Server 2012 R2, т.к. они обе являются 64-разрядными.

Ниже описаны некоторые сценарии модернизации Active Directory из Windows Server 2008.

- Когда необходимо вывести в резерв все старые контроллеры домена.
  1. Подготовьте лес.
  2. Подготовьте домен.
  3. Установите серверы членов Windows Server 2012 R2 и повысьте их до контроллеров домена.
  4. Выведите в резерв старые контроллеры домена.
- Когда все старые контроллеры домена являются 64-разрядными.
  1. Подготовьте лес.
  2. Подготовьте домен.
  3. Модернизируйте 64-разрядные контроллеры домена до Windows Server 2012 R2.
- Когда имеется смесь старого и нового оборудования, а также смесь 32- и 64-разрядных контроллеров домена.
  1. Подготовьте лес.
  2. Подготовьте домен.
  3. Модернизируйте новые контроллеры домена до Windows Server 2012 R2.
  4. Установите новые серверы членов Windows Server 2012 R2 и повысьте их до контроллеров домена. Они заменят собой старые контроллеры домена Windows.
  5. Выведите в резерв старые контроллеры домена.

Все приведенные стратегии обладают парой общих шагов. Для модернизации схемы леса или, другими словами, для подготовки леса применяется инструмент под названием `adprep`. Это делается один раз пользователем, являющимся членом групп Schema Admins (Администраторы схемы), Enterprise Admins (Администраторы

предприятия) и Domain Admins (Администраторы домена) в домене, который содержит роль FSMO (Flexible Single Master Operations — гибкие операции с одним хозяином) уровня леса по имени Schema Master (Хозяин схемы). Тот же самый инструмент также используется для подготовки любого домена, который будет содержать контроллеры домена Windows Server 2008. Это будет делаться пользователем, который является администратором домена.

Подход бок о бок с модернизацией от Windows Server 2008 до Windows Server 2012 R2 требует одного дополнительного шага. Он необходим для применения полномочий к объектам групповой политики, чтобы ими можно было управлять в консоли управления групповой политикой (Group Policy Management console).

Последний способ модернизации Active Directory до версии Windows Server 2012 R2 довольно радикален. Вы можете обнаружить, что сеть не находится в работоспособном либо известном состоянии. Иногда ситуацию лучше не усугублять и начать с создания заново всей структуры Active Directory, которая будет хорошо спланированной, документированной, управляемой и обслуживаемой. Вы можете построить новый лес/домен, после чего перенести пользователей, данные и службы в новую среду Active Directory. Мы поступали так в прошлом, когда присоединяли новую компанию, которая прошла через последовательность слияний. Приложенные усилия окупились получением намного более прочной и управляемой рабочей среды.

Весь приведенный здесь материал по Active Directory имеет высокоуровневый характер, что и должно быть. Он позволяет получить представление о том, чего следует ожидать в главе 7.

Автономная установка

Возможно, вы чувствуете, что приближаетесь к концу этой главы. Ведь больше не осталось тем, связанных с установкой Windows Server 2012 R2, которые можно было бы обсудить, не так ли? Хорошо, подумайте еще раз.

Небольшие организации будут вполне благополучно пользоваться ручным подходом к установке и модернизации Windows Server 2012 R2, который был описан ранее в главе. Однако может понадобиться уделить внимание альтернативным подходам. Можно применять решение с клонированием, такое как Windows Deployment Services, которое доступно в ОС Windows Server, начиная с пакета обновлений Service Pack 2 для Windows Server 2003, или бесплатный комплект инструментов для развертывания Microsoft Deployment Toolkit 2012. Возможно, вы уже используете какое-нибудь решение от третьей стороны. Вы можете быть заинтересованы в другом способе, который не требует сервера для управления процессом.

Автономная установка Windows расширяет носитель установки за счет его настройки. Часть процесса заключается в ответе на вопросы, отвечать на которые постоянно довольно утомительно. Идея в том, что установку можно начать и двигаться через нее, не отвечая при этом на любые вопросы. Новый сервер будет установлен совершенно самостоятельно согласно заранее определенным ответам. Новая процедура установки для Windows 8 и Windows Server 2012 R2 довольно мала, но при наличии большого количества машин вы очень скоро устанете вводить ключи продуктов, выбирать редакции ОС и т.п. Другая, более мощная часть процесса — возможность подстройки установки способами, которые скрыты в процессе ручной установки. Каким образом вы могли бы установить компоненты ОС, которые не отражены в

графическом пользовательском интерфейсе? Это позволило бы упростить постустановочную настройку и рационализировать развертывания.

Все это возможно благодаря применению файла ответов, который предоставляется процедуре установки. Такой подход может быть знаком инженерам, которым приходилось развертывать старые версии Windows. В прошлом вы могли пользоваться инструментом под названием Setup Manager (Диспетчер установки) для создания простого текстового файла ответов, который затем должен был настраиваться в Notepad.

С выходом Windows Vista все изменилось. В составе Windows Vista был предложен выпуск пакета автоматической установки Windows (Windows Automated Installation Kit — WAIK), который претерпел ряд обновлений, включая поддержку для Windows Server 2008, Windows 7 и Windows Server 2008 R2. С выходом Windows Server 2012 R2 имя пакета изменилось на Windows Assessment and Deployment Kit (Пакет оценки и развертывания Windows), или Windows ADK. Пакет ADK представляет собой мощный набор инструментов, в числе которых средство для создания загрузочного DVD-диска. Загрузка производится с использованием Windows PE, усеченной версии Windows, которую можно применять для выполнения многих задач, включая развертывание ОС и устранение неполадок. Что более важно для целей данной главы, пакет содержит диспетчер образов систем Windows (Windows System Image Manager — WSIM), который является заменой инструмента Setup Manager и используется для создания файлов ответов для Windows 8 и Windows Server 2012 R2.

Еще одно крупное изменение касается формата файлов ответов, которые будут применяться. Ранее было привычным редактирование текстовых файлов. Инструмент Setup Manager в действительности делал немногим более чем настройку скелета файла ответов. Вам по большей части приходилось проделывать немалую работу по редактированию этого файла в Notepad. Однако диспетчер WSIM создает XML-файлы. Эх! Снова эта аббревиатура: XML! Не впадайте в отчаяние. Поначалу формат XML пугает многих администраторов, поскольку они далеки от программирования. Но интерфейс WSIM делает почти все, что вам будет нужно. Вы можете по-прежнему вручную редактировать этот файл в Notepad или в любом редакторе XML-файлов. Единственный случай, когда это действительно понадобится — изменение ключа продукта.

Далее будет показано, каким образом развертывать ОС Windows Server 2012 R2 в автономной манере. Вы увидите, как установить ADK, с помощью WSIM создать файл ответов и затем использовать этот файл для молчаливого процесса установки.

Обратите внимание, что многие материалы (если только не все), рассмотренные в данном разделе, также применимы при развертывании Windows 8.

Установка Windows Assessment and Deployment Kit

Упражнение, через которое вы пройдете, продемонстрирует процедуру развертывания редакции Windows Server 2012 R2 с очень небольшим вмешательством со стороны человека. Предположим, что вам необходимо развернуть несколько серверов с редакцией Windows Server 2012 R2 Standard. Работу имеет смысл автоматизировать. Это делается с использованием файла ответов для ответа на вопросы, задаваемые во время ручной установки Windows Server 2012 R2. Мы покажем, как создать такой файл ответов с помощью Windows System Image Manager и затем пройдем через процесс развертывания Windows Server автономным образом.

ADK представляет собой бесплатный набор инструментов, которые можно загрузить из веб-сайта Microsoft. Указать точный URL для загрузки затруднительно, т.к. с момента начального выпуска разработчики из Microsoft несколько раз обновляли комплекты развертывания. Лучше всего зайти на `www.microsoft.com/downloads` и выполнить поиск по строке *Windows ADK*. Это позволит гарантированно получить последнюю версию ADK.

Программа установки запросит, нужно ли проводить установку на текущем компьютере либо загрузить эту программу на другую машину. Выбор установки на компьютере, который используется для загрузки ADK, приводит одновременно к его загрузке и установке. По этой причине мы советуем выбрать загрузку для установки на другом компьютере, что предполагает только загрузку, но не установку ПО. В результате вы получите полную копию ПО, которая пригодится на случай повторной его установки.

Новая версия ADK, выпущенная для Windows 8

Размер загружаемого файла очень большой — около 5,1 Гбайт на время написания этой главы. Вы можете располагать ранее загруженным комплектом ADK, который был доступен до выхода Windows Server 2012 R2. Тем не менее, одновременно с выпуском Windows 8 в Microsoft предложили новую версию ADK, поддерживающую новые серверные ОС, поэтому вам понадобится загрузить более свежую копию этого комплекта.

Следующее, что необходимо иметь — административную рабочую станцию, представляющую собой ПК, который будет применяться для подготовки будущих сборок. Это может быть ваш ПК, но поступать так не очень осмотрительно, поскольку можно нанести вред самому административному ПК из-за неаккуратного использования ADK и WSIM, нарушив работу машины, на которой выполняются повседневные задачи.

Удостоверьтесь, что на жестком диске имеется достаточно свободного пространства. Вскоре вы увидите, по какой причине. Мы предпочитаем делать это либо на отдельной машине, либо, что даже лучше, на виртуальной машине. Последнему случаю присущи экономические преимущества, а также наличие возможности сохранения и восстановления состояния. С помощью виртуальных машин можно также монтировать файлы ISO, что приносит огромную пользу, т.к. не приходится тратить время на возню с утилитами и пустыми дисками. Виртуальные машины великолепны для тестирования новых файлов ответов, поэтому нам так нравится использовать их в качестве административных рабочих станций.

Необходимо, чтобы функционировала ОС версии Windows Vista или более поздней. Единственным предварительным условием является наличие платформы .NET Framework 4.0 (она устанавливается вместе с ОС).

В проводнике Windows перейдите в каталог, в котором находится загруженное ПО ADK, и запустите файл `adksetup.exe`.

Появится первый экран с запросом местоположения для установки (рис. 2.60). После ввода местоположения или принятия предложенного стандартного местоположения щелкните на кнопке Next (Далее), чтобы продолжить процесс.

На следующем экране отображается приглашение принять участие в программе по улучшению работы пользователей Microsoft (Microsoft Customer Experience Improvement Program — CEIP), как показано на рис. 2.61.

На следующем экране выводится текст лицензионного соглашения. Щелкните на кнопке Accept (Принять), чтобы согласиться с условиями лицензии, регламентирующими использование ADK компанией Microsoft (рис. 2.62).

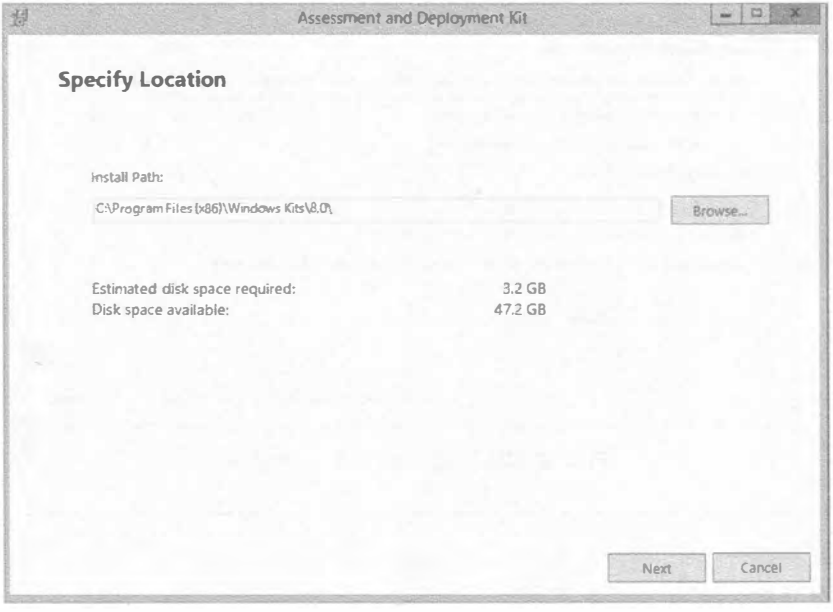


Рис. 2.60. Начальный экран программы установки ADK

Рис. 2.61. Участие в программе по улучшению работы пользователей ADK

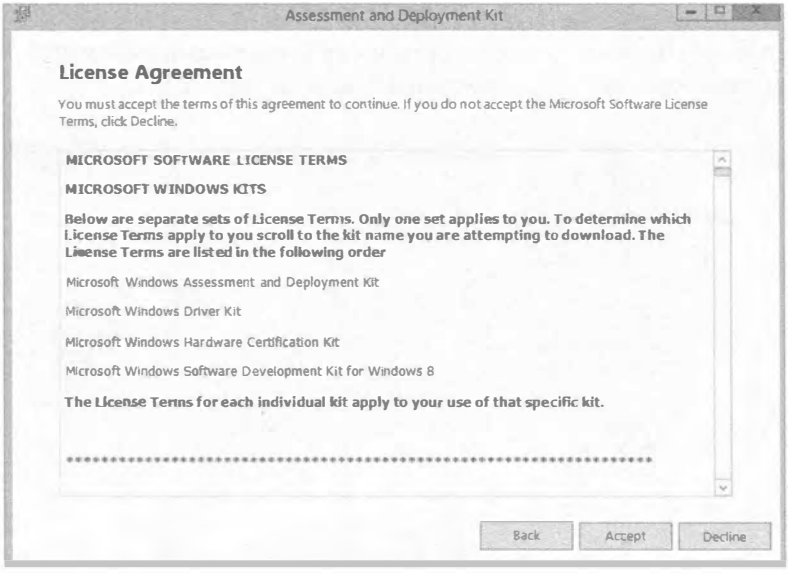


Рис. 2.62. Лицензия EULA для ADK

Пример из практики

Лучшее местоположение

Ронда Лэйфилд, коллега и гуру по развертыванию, дает важный совет по установке ADK. На первом экране программы установки запрашивается местоположение, куда необходимо установить ADK. Обычно в качестве стандартного предлагается местоположение `C:\Program Files(x86)\Windows Kits\8.0\`. Однако поскольку вы начинаете интенсивно применять ADK, подумайте, сколько лишних символов придется вводить в командной строке. Установка ПО в место с настолько глубоким путем определенно не является дружественным к командной строке. Ронда советует устанавливать ADK в каталог `C:\ADK`. Это обеспечит существенную экономию клавиатурного ввода.

Вы добрались до экрана, позволяющего выбрать компоненты ADK для установки. Давайте уделим некоторое время их обсуждению. В списке на рис. 2.63 не присутствует SQL Server Express. Причина в том, что на данном компьютере ПО SQL Server было установлено ранее. Если это не так, то в списке будет находиться флажок для ПО SQL Server Express, которое является обязательным для комплекта инструментов совместимости приложений (Application Compatibility Toolkit — ACT).

- Application Compatibility Toolkit (ACT) (Комплект инструментов совместимости (ACT)). Этот комплект инструментов проверяет совместимость компьютеров, на которых планируется проведение автономной установки.
- Deployment Tools (Инструменты развертывания). Инструменты развертывания требуются для выполнения автономной установки потому, что именно они выполняют такую автоматизированную установку. Фактически это под-

множество инструментов для ADK. Оно содержит несколько поддерживающих программ, таких как инструмент обслуживания и управления образами (Deployment Image Servicing and Management — DISM), инструмент активации OEM (OEM Activation) и диспетчер образов систем Windows (Windows System Image Manager), а также другие средства.

- **Windows Preinstallation Environment (Windows PE)** (Среда предустановки Windows (Windows PE)). Это элементарная ОС, которая помещается на целевую машину. Она необходима для подготовки процесса установки на целевом компьютере.
- **User State Migration Tool (USMT)** (Инструмент миграции состояния пользователей (USMT)). Инструмент USMT переносит данные пользовательских учетных записей и настройки приложений на целевую машину. Это экономит время администратора, но не воссоздает систему в первоначальном состоянии.
- **Volume Activation Management Tool (VAMT)** (Инструмент управления активацией томов (VAMT)). Инструмент VAMT поддерживает активации ПО операционной системы.
- **Windows Performance Toolkit** (Комплект инструментов производительности Windows). Это еще одно подмножество инструментов, применяемых для отслеживания процесса установки и фиксации событий, происходящих на протяжении установки. Такие действия возможны благодаря тому, что данный комплект является встроенным в инфраструктуру трассировки сообщений для Windows (Event Tracing for Windows — ETW).
- **SQL Server Express** (Продукт SQL Server Express). Программный продукт SQL Server Express — это переносимая версия SQL Server, которая требуется для комплекта ACT, поскольку позволяет хранить данные, используемые во время процесса установки.

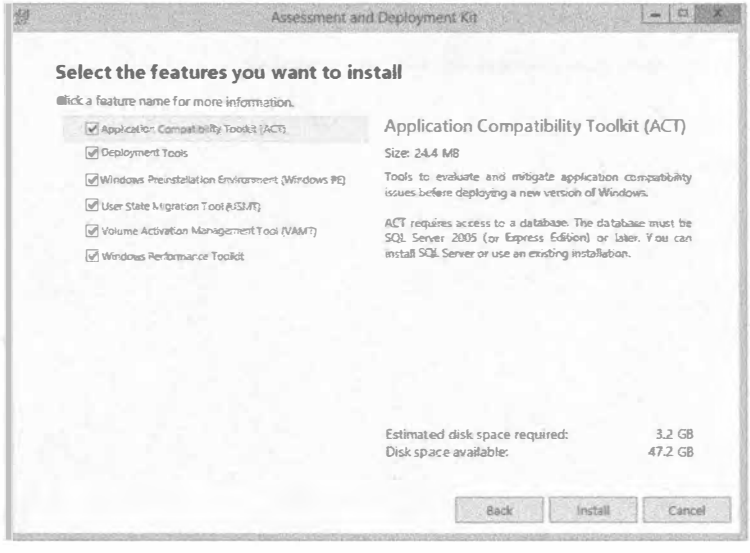


Рис. 2.63. Компоненты ADK

Щелкните на кнопке Install (Установить), если готовы к установке ADK. Сама установка может занять несколько минут (рис. 2.64). В это время можете ответить на накопившиеся сообщения электронной почты.

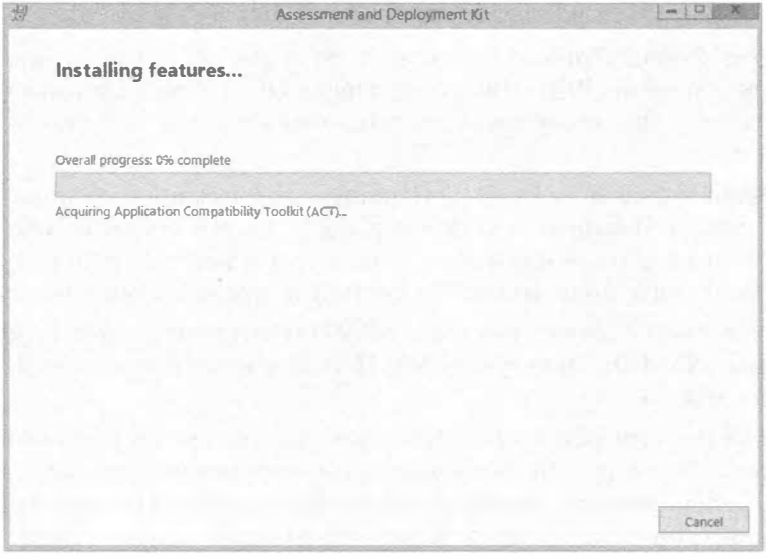


Рис. 2.64. Ход работ по установке ADK

В конечном счете, ADK установится (рис. 2.65). Вы увидите экран с флажком Launch the Getting Started Guide (Запустить руководство по началу работы). Это великолепное руководство по всем инструментам ADK. Рекомендуем ознакомиться с ним.

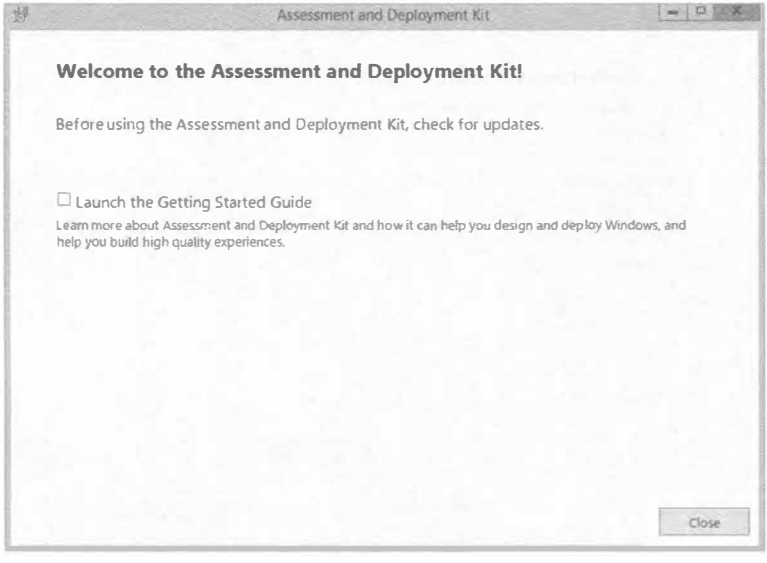


Рис. 2.65. Завершение установки ADK

Вы обнаружите установленные инструменты, щелкнув на кнопке Start (Пуск), как показано на рис. 2.66.

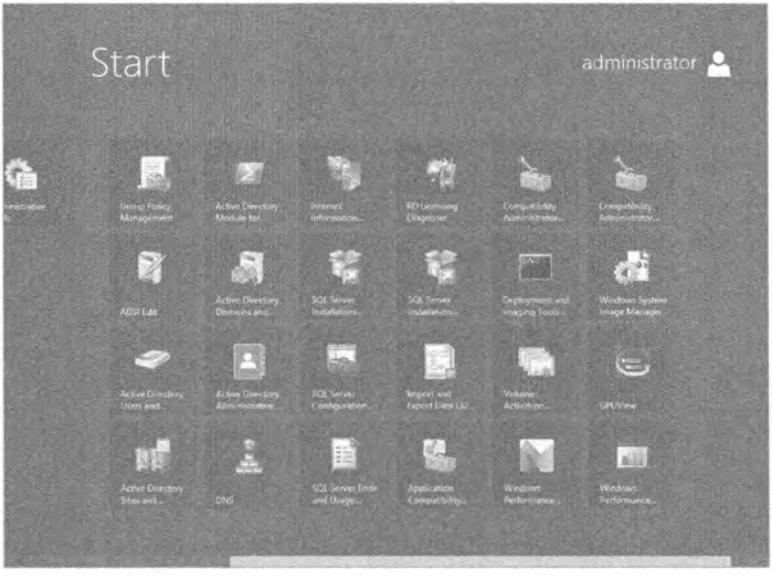


Рис. 2.66. ADK в меню Start

Создание файла ответов

Прежде чем заняться созданием файла ответов, необходимо понять, что он собой представляет и что происходит "за кулисами".

Что собой в точности представляет файл ответов? Это XML-файл, который содержит ответы на вопросы, задаваемые во время процесса установки. Если вы когда-либо устанавливали ОС, то должны знать, что в какой-то момент понадобится указать, к примеру, часовой пояс. Вместо установки часового пояса вручную его можно указать в файле ответов, и он обеспечит автоматический ответ на этот вопрос. Это не принесет особых выгод при установке ОС на одном или двух компьютерах, но в случае множества компьютеров экономится немало усилий.

Во время установки Windows 8 или Windows Server 2012 R2 процедура установки выполняет некоторые или все последовательности конфигурационных операций, описанные в табл. 2.3. Каждая из этих последовательностей отвечает за выполнение определенных задач. Можете думать о них как о фазах. Некоторые задачи могут выполняться на протяжении более чем одной последовательности. Обычно для установки Windows необходимо выполнить только три из указанных последовательностей.

Вы увидите некоторые из описанных последовательностей при создании файла ответов в диспетчере WSIM. Как только вы начнете работать с WSIM, все станет значительно яснее.

Для примера, рассматриваемого в этом разделе, понадобится установочный DVD-диск Windows Server 2012 R2. В папке `\sources` носителя установки имеется WIM-файл по имени `install.wim`. Этот файл содержит все, что нужно для установки новых копий ОС, причем для всех редакций, доступных на носителе.

Таблица 2.3. Последовательности конфигурационных операций

Последовательность	Описание
windowsPE	Загружает среду установки Windows PE, устанавливает ключ продукта и конфигурирует установочный диск
offlineServicing	Применяет обновления к образу Windows, включая пакеты, исправления и языки
Specialize	Конфигурирует настройки, которые могут быть уникальными для системы, такие как параметры сети, региона и домена
Generalize	Удаляет информацию, специфичную для системы. Выполняется только в случае запуска sysprep /generalize
auditSystem	Обрабатывает шаги автономной установки перед входом пользователя в систему. Эта последовательность выполняется только в случае загрузки в режиме аудита
auditUser	Обрабатывает шаги автономной установки после входа пользователя в систему. Эта последовательность выполняется только в случае загрузки в режиме аудита
oobeSystem	Применяет настройки до появления начального экрана Windows, т.е. до входа пользователя в систему

Например, на DVD-диске Windows Server 2012 R2 находятся редакции Standard Full, Datacenter Full, Standard Core и Datacenter Core. Дело в том, что в отношении этого WIM-файла используется концепция единственного хранилища.

Диспетчеру WSIM необходима копия данного файла на административном ПК. Этот *установочный образ* применяется WSIM для выяснения того, какие задачи могут выполняться для версии и редакции ОС Windows, с которой планируется работа. Они будут варьироваться в зависимости от используемой системы: Windows 8, Windows Server 2012 R2 Standard, Windows Server 2012 R2 Datacenter и т.д. Почему упомянутый WIM-файл помещается на жесткий диск, а не применяется его копия на DVD-диске? Диспетчеру WSIM необходимо создать каталожный файл для содержимого файла образа, при этом папка, в которой находится образ, используется в качестве рабочей, а поскольку DVD-диск допускает только чтение, сделать это не удастся.

В рассматриваемом примере мы имеем дело с DVD-диском для установки Windows Server 2012 R2. Скопируйте файл `\sources\install.wim` в `C:\W2012\install.wim` на административном ПК.

Теперь запустите диспетчер WSIM и выберите пункт меню File⇨Select Windows Image (Файл⇨Выбрать образ Windows).

Перейдите к установочному образу (рис. 2.67), который хранится в `C:\W2012\install.wim`, и откройте его.

Вы увидите в действии некоторую магию, связанную с WIM-файлом. Установочный образ содержит внутри себя несколько версий Windows. Выберите ту версию Windows, которую необходимо установить в автономной манере. На рис. 2.68 показан выбор редакции Standard версии Windows Server 2012 R2.

Отобразится диалоговое окно с предупреждением о невозможности открытия каталожного файла для этого образа, т.к. он не существует (рис. 2.69). Вы можете либо создать каталожный файл, либо отменить процесс. Щелкните на кнопке Yes (Да), чтобы создать такой файл. Обратите внимание, что для этого необходимо быть локальным администратором на административном ПК.

В зависимости от настроек безопасности административной рабочей станции может быть выдан запрос от системы контроля пользовательских учетных записей (User Account Control — UAC). Процесс создание каталожного файла занимает некоторое время (рис. 2.70). Развертывание ОС иногда сводится к наблюдению за индикатором хода работ.

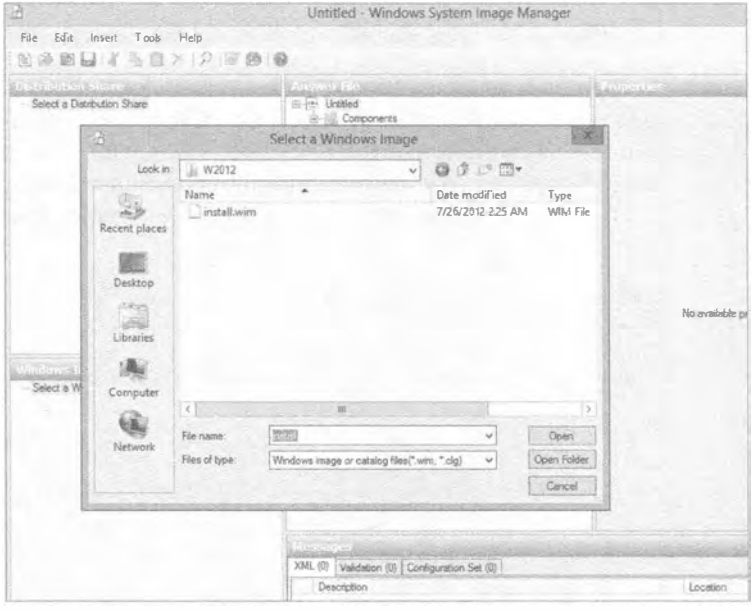


Рис. 2.67. Добавление образа Windows в WSIM

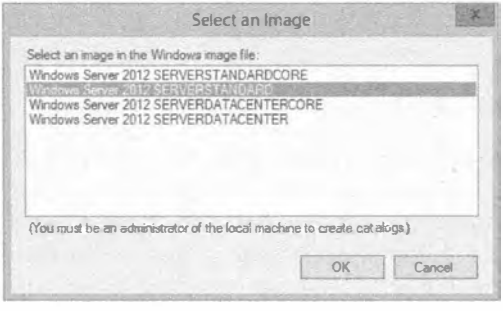


Рис. 2.68. Выбор нужного образа Windows

Рис. 2.69. Создание каталожного файла

Рис. 2.70. Генерация каталожного файла

В конце концов, наряду с файлом образа в `C:\W2012` создается каталожный файл. Вы увидите, что в панели Windows Image (Образ Windows) окна WSIM появились ветви Components (Компоненты) и Packages (Пакеты), как показано на рис. 2.71. Мы не собираемся работать с панелью Distribution Share (Дистрибутивный общий ресурс), поэтому можете расширить панель Windows Image, предоставив ей больше места.

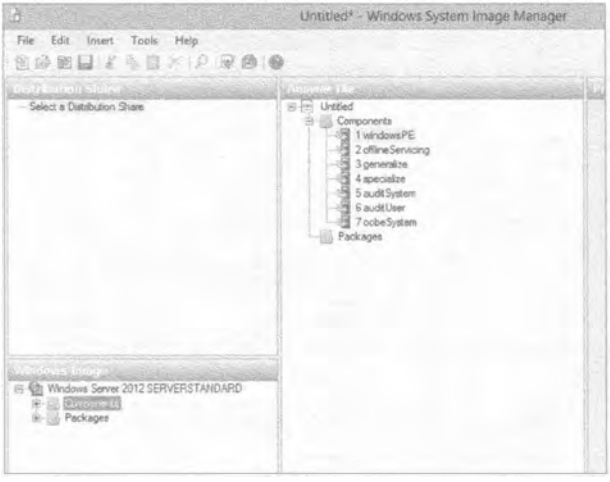


Рис. 2.71. Результат добавления образа Windows

Нас интересует работа с ветвью Components, так что разверните ее (рис. 2.72). *Компонент* — это набор связанных настроек, которые используются в качестве строительных блоков для конструирования файла ответов. Каждый компонент отвечает на какой-то вопрос или набор вопросов во время установки. Компоненты можно выбирать с целью получения желаемой автономной установки. Во время ручной установки необходимо было ответить только на несколько вопросов. Как ни странно, при автономной установке для получения аналогичного результата требуется ответить на большее число вопросов. Если вы пройдетесь по компонентам, то заметите, что доступных опций довольно много. Настоятельно рекомендуем прочитать документацию, установленную вместе с ADK. В справочнике по автономной установке Windows (Unattended Windows Setup Reference) приведены подробные сведения по каждому компоненту.

Следующий шаг заключается в создании нового файла ответов в среде WSIM. Выберите пункт меню File⇨New Answer File (Файл⇨Создать файл ответов). Когда будет предложено сохранить этот файл, сохраните его в том же каталоге `C:\W2012`.

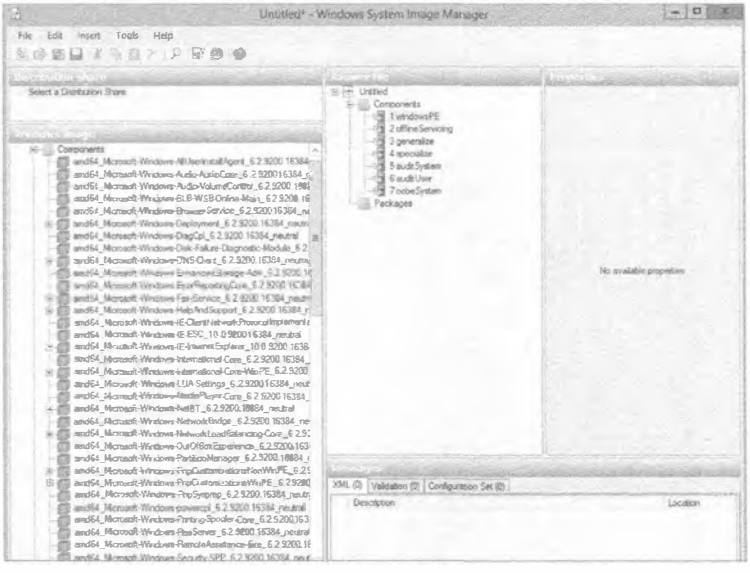


Рис. 2.72. Просмотр компонентов образа Windows

Взгляните на панель Answer File (Файл ответов), представленную на рис. 2.73. Ее содержимое должно выглядеть знакомым. Это доступные последовательности конфигурационных операций, которые применялись для установки Windows. Теперь для построения файла ответов мы будем добавлять компоненты к необходимым последовательностям.

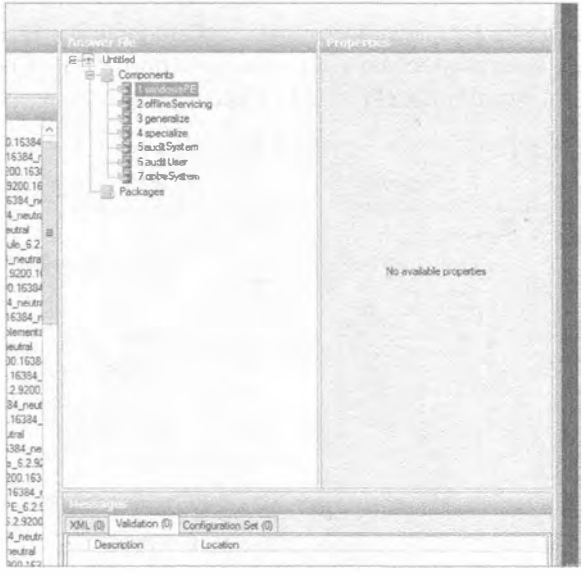


Рис. 2.73. Создание нового файла ответов

В ветви Components внутри панели Windows Image найдите компонент `amd64_Microsoft-Windows-International-Core-WinPE` (рис. 2.74).

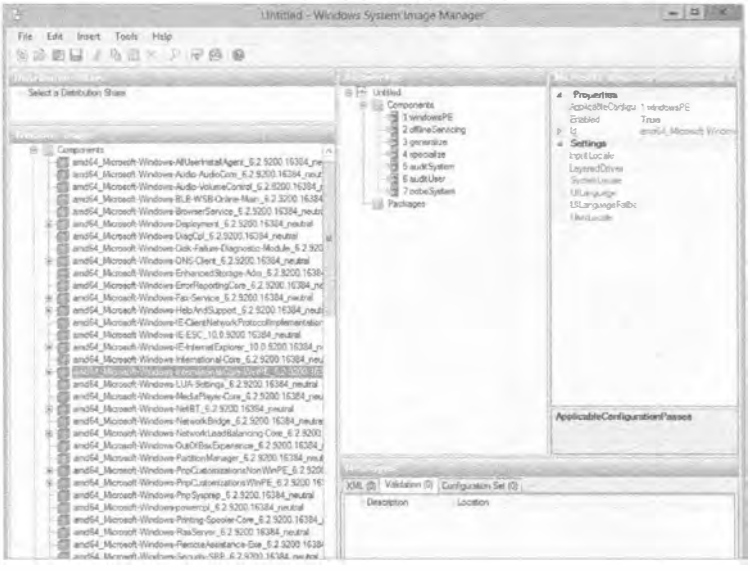


Рис. 2.74. Выбор компонента для добавления в файл ответов

Этот компонент отвечает за конфигурирование настроек среды установки Windows. В начале главы было указано, что при ручной чистой установке требуется сконфигурировать языковые настройки. Данный компонент автоматизирует этот шаг. Щелкните правой кнопкой мыши на компоненте и выберите в контекстном меню пункт Add Setting to Pass1 windowsPE (Добавить настройку в последовательность `1 windowsPE`).

Вы увидите, что данный компонент был добавлен в файл ответов, в панели Answer File под последовательностью `1 windowsPE` (рис. 2.75). Кроме того, в правой верхней панели теперь доступны для редактирования свойства компонента.

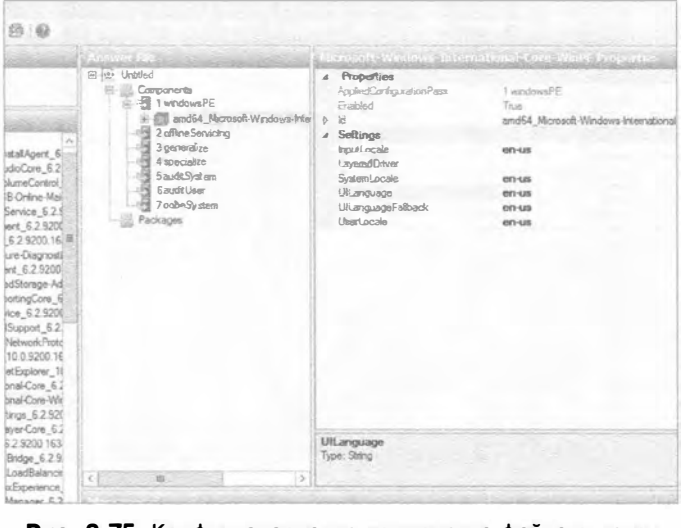


Рис. 2.75. Конфигурирование компонента файла ответов

Обратите внимание, что компонент можно развернуть, чтобы отобразить его дочерний компонент, который тоже может иметь свойства, предназначенные для редактирования. Для получения справки по свойству необходимо выбрать поле со значением свойства и нажать клавишу <F1>. Теперь можно отредактировать свойства компонента. Добавьте следующие значения:

Последовательность	Компонент	Свойство	Значение
1	amd64_Microsoft-Windows-International-Core\SetupUILanguage	InputLocale	en-us
		UserLocale	en-us
		UILanguage	en-us
		SystemLocale	en-us
		UILanguage	en-us

Все настройки сконфигурированы для языка US English (см. рис. 2.75). По нажатию <F1> для одного из свойств можно получить сведения о других региональных кодах. Кроме того, понадобится также отредактировать свойство UILanguage дочернего компонента SetupUILanguage. Далее будут добавлены другие компоненты и отредактированы их свойства. (Удостоверьтесь, что добавляете компоненты в последовательность, номер которой указан в первом столбце.)

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\DiskConfiguration\Disk	DiskID	0
		WillWipeDisk	True

Подкомпонент Disk, добавленный к файлу ответов в последовательность 1, сообщает программе установки о необходимости управления диском Disk 0 на сервере. Вспомните, что в Microsoft называют Disk 0 первый диск компьютера. Кроме того, программе установки указывается на то, что этот диск должен быть очищен.

Разверните подкомпонент Disk в панели Answer File. Вы увидите два подкомпонента, которые называются CreatePartitions и ModifyPartitions. Щелкните на каждом из них правой кнопкой мыши и выберите в контекстном меню пункт Insert New (Вставить новый). Это позволит создать том на очищенном диске Disk 0 и затем сформатировать его с использованием следующих настроек свойств подкомпонента:

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	Extend	True
		Order	1
		Type	Primary

Здесь программа установки Windows Installer инструктируется на предмет создания раздела и его расширения, так что новый том займет целиком весь диск Disk 0. Свойство Order указывает программе установки о необходимости пометки тома как 1, поскольку вскоре потребуется ссылаться на эту метку.

Если заполнять весь диск Disk 0 одним разделом нежелательно, то вместо установки свойства Extend в True понадобится указать в свойстве Size нужный размер раздела 1 в мегабайтах, например, 40960 для тома в 40 Гбайт. Указывать значение для свойства Size *и* устанавливать свойство Extend в True не допускается, т.к. это приводит к конфликту.

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\ModifyPartition	Active	True
		Format	NTFS
		Label	Windows
		Letter	C
		Order	1
		PartitionsID	1

Здесь снова применяется свойство Order. Это инструктирует программу установки о том, чтобы она сформатировала ранее созданный том. Он настраивается как раздел 1 с использованием свойства PartitionsID. В терминах Microsoft раздел 1 является первым разделом; раздела 0 не предусмотрено. За счет установки свойства Active в True том делается активным, чтобы была возможность выполнения загрузки с него. Путем установки свойства Format в NTFS том форматируется с файловой системой NTFS, посредством свойства Label он помечается как Windows, а с помощью свойства Letter тому назначается буква C.

Следующая часть работы несколько сложнее. Мы уже отмечали, что заглядывать в документацию полезно, и она дает практически любые сведения. Но вы также увидите, что необходим еще один инструмент из ADK.

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\InstallImage\OSImage\InstallFrom\Metadata	Key	/IMAGE/NAME
		Value	Windows Server 2012 SERVERSTANDARD

Когда мы первоначально пытались устанавливать Windows Server 2012 R2 с применением автономного подхода, процедура установки всегда останавливалась и предлагала сделать выбор между доступными редакциями ОС Windows на DVD-диске. Вполне очевидно, что это не то, что нам требовалось; нам была нужна авто-

номная установка. В справочном файле ADK было указано, что этот подкомпонент мог бы помочь выбрать подходящую редакцию. К сожалению, не были предоставлены сведения о необходимых значениях свойств. Но было сказано, что искомые значения содержатся внутри установочного образа `install.wim`.

Итак, мы запустили инструмент Deployment and Imaging Tools Environment (command prompt) (Среда инструментов для развертывания и работы с образами (командная строка)), который является частью ADK и доступен через кнопку Start панели задач. После это мы выполнили следующую команду:

```
IMAGEX /info C:\W2012\INSTALL.WIM
```

Команда `IMAGEX` — это утилита ADK, позволяющая управлять WIM-файлами. Ниже показан ее синтаксис:

```
IMAGEX.EXE /info <Путь к желаемому WIM-файлу>
```

Утилита генерирует отчет по содержимому установочного образа Windows Server 2012 R2 x64 (рис. 2.76).

Рис. 2.76. Фрагмент отчета с именем сервера

Вот необходимый фрагмент из отчета, показанного на рис. 2.76:

```
<NAME>Windows Server 2012 SERVERSTANDARD</NAME>
<DESCRIPTION>Windows Server 2012 SERVERSTANDARD</DESCRIPTION>
```

Подкомпонент `Metadata` позволяет указать ключ для поиска этих результатов (`Key`) и значение для соответствия (`Value`). В предыдущем фрагменте видно, что имеется ключ `NAME`. Он находится внутри пути `/IMAGE/PATH`. Ключ `NAME` используется для уникальной идентификации каждой доступной редакции ОС Windows, содержащейся внутри установочного образа. Желаемая в этом примере редакция обнаруживается внутри элемента `IMAGE INDEX="2"`.

Ключ NAME здесь установлен в Windows Server 2012 SERVERSTANDARD. Следовательно, подкомпонент Metadata необходимо настроить для поиска ключа /IMAGE/NAME со значением Windows Server 2012 SERVERSTANDARD. Именно этот образ программа установки должна установить на сервере. Уф! Мы обещаем, что это самое трудное действие из всего процесса.

Далее программе установки ОС нужно сообщить о том, что выбранный образ следует установить на ранее указанный диск в только что созданный и сформатированный том, т.е. в первый раздел первого диска.

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\ ImageInstall\OSImage\InstallTo	DiskID	0
		PartitionID	1

С помощью подкомпонента UserData вводится лицензионная информация для установки Windows. Условия лицензии Microsoft принимаются путем установки свойства AcceptEula в True. В свойствах FullName и Organization указывается наименование компании, что является обычной практикой обозначения права собственника лицензии. В свойстве Key подкомпонента ProductKey задан наш ключ продукта, приведенный здесь только для демонстрационных целей.

Последовательность	Компонент	Свойство	Значение
1	AMD64_Microsoft-Windows-Setup\ UserData	AcceptEula	True
		FullName	Bigfirm
		Organization	Bigfirm
	AMD64_Microsoft-Windows-Setup\ UserData\ProductKey	Key	HFG76-34GFT-O6ID9-MNBW4-IYUSD

Добавьте показанный ниже компонент в последовательность 4 specialize. Свойство ComputerName применяется для установки имени компьютера. Никакой мистики здесь нет. Установка этого свойства в * приводит к тому, что программа установки ОС сгенерирует случайное имя. При желании можно было бы ввести какое-то имя. Свойство TimeZone предназначено для конфигурирования системных часов. В данном примере указан часовой пояс USA Eastern Standard. Список доступных часовых поясов можно получить по нажатию <F1> при редактировании TimeZone.

Последовательность	Компонент	Свойство	Значение
4	AMD64_Microsoft-Windows-Shell-Setup	ComputerName	*
		TimeZone	Eastern Standard Time

Добавьте показанный ниже подкомпонент `OOBE` в последовательность `7 oobeSystem`. Сконфигурируйте брандмауэр Windows посредством свойства `NetworkLocation`. Установка этого свойства в `Work` приводит к включению брандмауэра, но к более слабым его настройкам, подходящим для типичной корпоративной сети. Свойство `ProtectYourPC` включает автоматические обновления и конфигурирует их на автоматическую установку.

Данный подкомпонент демонстрирует возможность добавления дополнительных настроек процесса установки, которые при ручной установке попросту недоступны.

Последовательность	Компонент	Свойство	Значение
7	AMD64_Microsoft-Windows-Shell-Setup\OOBE	HideEULAPage	True
		NetworkLocation	Work
		ProtectYourPC	1

Последний настраиваемый компонент полезно иметь в виду для экспериментальных сред, где может использоваться лицензирование MSDN или TechNet. Такие подписки предоставляют ограниченное количество активаций для каждого лицензионного ключа. Обычно экспериментальная машина обладает очень коротким периодом существования, поэтому бессмысленно растрачивать на нее ценные активации.

Этот компонент позволяет отключить стандартный процесс автоматической активации установленной копии.

Последовательность	Компонент	Свойство	Значение
7	AMD64_Microsoft-Windows-Security-Licensing-SPP-UX	SkipAutoActivation	False

Вот и все компоненты, которые требовалось добавить. Следующим действием будет проверка правильности файла ответов. Выберите пункт меню Tools⇨Validate Answer File (Сервис⇨Проверить файл ответов). Будет выполнен проход по свойствам и введенным для них значениям.

Все обнаруженные некорректные данные приведут к появлению сообщений об ошибках в панели Messages (Сообщения). Если вы добавляли компоненты и вводили значения для свойств так, как было показано до сих пор, то все должно быть в порядке (рис. 2.77).

Готовый файл ответов теперь можно сохранить. Выберите пункт меню File⇨Save Answer File As (Файл⇨Сохранить файл ответов как).

Сохраните файл `autounattend.xml` в желаемом месте, таком как `C:\Answer\autounattend.xml` (рис. 2.78).

Скорее всего, вы захотите посмотреть, на что похоже содержимое созданного XML-файла. Откройте файл ответов в редакторе Notepad. Вы должны увидеть примерно такой код:

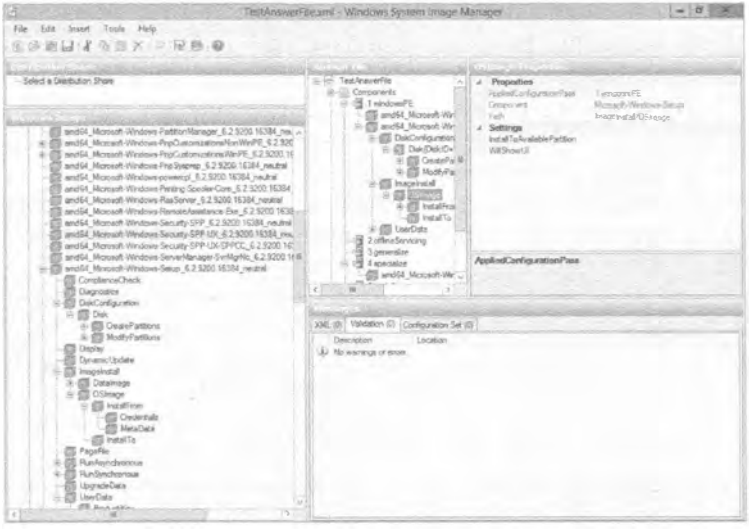


Рис. 2.77. Результаты проверки файла ответов

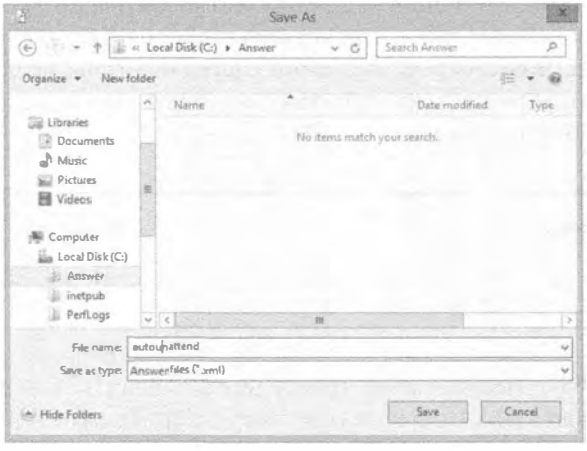


Рис. 2.78. Сохранение файла ответов

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
   <settings pass="windowsPE">
      <component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <InputLocale>en-us</InputLocale>
         <UserLocale>en-us</UserLocale>
         <UILanguage>en-us</UILanguage>
         <SystemLocale>en-us</SystemLocale>
         <UILanguageFallback>en-us</UILanguageFallback>
      </component>
```

```
      <component name="Microsoft-Windows-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <DiskConfiguration>
            <Disk wcm:action="add">
               <CreatePartitions>
                  <CreatePartition wcm:action="add">
                     <Extend>true</Extend>
                     <Order>1</Order>
                     <Type>Primary</Type>
                  </CreatePartition>
               </CreatePartitions>
               <ModifyPartitions>
                  <ModifyPartition wcm:action="add">
                     <Active>true</Active>
                     <Format>NTFS</Format>
                     <Label>Windows</Label>
                     <Letter>C</Letter>
                     <Order>1</Order>
                     <PartitionID>1</PartitionID>
                  </ModifyPartition>
               </ModifyPartitions>
               <DiskID>0</DiskID>
               <WillWipeDisk>true</WillWipeDisk>
            </Disk>
         </DiskConfiguration>
         <ImageInstall>
            <OSImage>
               <InstallFrom>
                  <MetaData wcm:action="add">
                     <Key>/IMAGE/NAME</Key>
                     <Value>Windows Server 2012 SERVERSTANDARD</Value>
                  </MetaData>
               </InstallFrom>
               <InstallTo>
                  <DiskID>0</DiskID>
                  <PartitionID>1</PartitionID>
               </InstallTo>
            </OSImage>
         </ImageInstall>
         <UserData>
            <ProductKey>
               <Key>HFG76-34GFT-O6ID9-MNBW4-IYUSD</Key>
            </ProductKey>
            <AcceptEula>true</AcceptEula>
            <FullName>BigFirm</FullName>
            <Organization>BigFirm</Organization>
         </UserData>
      </component>
   </settings>
   <settings pass="specialize">
      <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
```

```
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <ComputerName>*</ComputerName>
         <TimeZone>Eastern Standard Time</TimeZone>
      </component>
   </settings>
   <settings pass="oobeSystem">
      <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <OOBE>
            <HideEULAPage>true</HideEULAPage>
            <NetworkLocation>Work</NetworkLocation>
            <ProtectYourPC>1</ProtectYourPC>
         </OOBE>
      </component>
   </settings>
   <cpi:offlineImage cpi:source="wim:c:/w2012/install.wim#Windows
Server 2012 SERVERSTANDARD" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

Итак, у вас теперь имеется файл ответов, способный отвечать на все вопросы, которые задаются во время установки Windows. Осталось только предоставить этот файл программе установки ОС.

Использование файла ответов

Процесс довольно прост. Вы должны сохранить файл `autounattend.xml` в корневом каталоге на каком-нибудь сменном носителе. После этого перезагрузите новый сервер с применением корректной редакции Windows Server 2012 R2.

> **Краткое предостережение**
>
> Не делайте этого на машине, имеющей высокую ценность. Проведите сначала тестирование в лабораторной среде. Данный процесс является деструктивным, т.к. он предполагает очистку жесткого диска компьютера.

В рассматриваемом примере будет применяться DVD-диск с Windows Server 2012 R2. Как только сервер начнет загрузку с DVD-диска, вы должны вставить сменный носитель, содержащий файл ответов. Ниже перечислены поддерживаемые виды сменных носителей.

- **CD- или DVD-диск.** Это требует наличия на сервере двух устройств: устройства DVD для загрузки и установки ОС Windows Server 2012 R2 и еще одного устройства для чтения файла ответов с CD- или DVD-диска.
- **Флоппи-диск.** Часто ли на современных серверах присутствует устройство для флоппи-дисков? Это возможно лишь в лабораторной среде или на более старых машинах.
- **Флэш-память USB.** Это наиболее вероятный случай из всех возможных.

Выберите носитель, подходящий для сервера, который вы собираетесь строить, и скопируйте файл ответов в корневой каталог на этом носителе.

Если вы используете виртуальную машину, то имеется один ловкий трюк. Добавьте второе виртуальное устройство для чтения CD- или DVD-дисков к виртуальной машине, на которой планируется установка Windows Server 2012 R2. Удостоверьтесь в том, что для загрузочного DVD-диска смонтирован корректный ISO-файл для установки Windows. Создайте ISO-файл, который содержит только файл `autounattend.xml`. Не располагаете подходящим инструментом для этого? Ничего страшного, поскольку такой инструмент имеется в ADK. Попробуйте запустить следующую команду в Deployment and Imaging Tools Environment (command prompt):

```
oscdimg -n C:\Answer C:\answer.iso
```

В `C:\` будет создан ISO-файл по имени `answer.iso` с применением содержимого папки `C:\Answer`. Обязательно удостоверьтесь, что не поместили файл `autounattend.xml` в `C:\` и попытайтесь создать ISO-файл для полного жесткого диска! В такую ловушку очень легко попасть. Ниже показан синтаксис предыдущей команды:

```
oscdimg -n <Папка для использования в качестве исходной >
          <Местоположение и имя нового ISO-файла>
```

Что же, приступим. Вставьте DVD-диск с Windows Server 2012 R2 в DVD-привод на сервере.

Как только сервер начнет загрузку с DVD-диска, вы должны вставить в устройство носитель, содержащий файл ответов. Первые несколько раз потребуется следить за тем, что происходит, удостоверяясь в аккуратном ходе работ. Должна пройти молчаливая установка Windows Server 2012 R2, перезагрузка и ожидание установки пароля для администратора, что позволит войти в систему. Если в файле ответов присутствует ошибка, то произойдет что-то из перечисленного ниже:

- откроется диалоговое окно с вопросом, ожидающее реакции со стороны человека;
- отобразится диалоговое окно с сообщением об ошибке;
- произойдет критический отказ с последующей перезагрузкой.

В таком случае понадобится пересмотреть файл ответов в диспетчере WSIM.

Если все прошло успешно, то вы имеете файл ответов, полностью автоматизирующий процесс установки Windows Server 2012 R2. Вдобавок вы узнали некоторые шаги, требуемые при автоматической установке.

Установка сети серверов для примеров, рассматриваемых в этой книге

Для проработки примеров, рассматриваемых в этой книге, необходима экспериментальная или тестовая сеть.

Чтобы следовать примерам, постройте два сервера с использованием процесса чистой или автономной установки. При создании этой экспериментальной сети рекомендуется задействовать оба метода. Метод автономной установки впоследствии ускорит построение всех будущих серверов.

Настройте оба сервера согласно показанным ниже параметрам.

Сервер 1

Элемент	Конфигурация
Полное имя компьютера	bf1.bigfirm.com
Адрес IPv4	192.168.1.51
Маска подсети	255.255.255.0
Стандартный шлюз	192.168.1.1
Первичный DNS-сервер	<пусто>
Вторичный DNS-сервер	<пусто>

Сервер 2

Элемент	Конфигурация
Полное имя компьютера	bf2.bigfirm.com
Адрес IPv4	192.168.1.52
Маска подсети	255.255.255.0
Стандартный шлюз	192.168.1.1
Первичный DNS-сервер	<пусто>
Вторичный DNS-сервер	<пусто>

Теперь вы располагаете тестовой сетью серверов Windows Server 2012 R2.

Резюме

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?

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?

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?

Глава 3

Введение в Server Core

Специалисты из компании Microsoft проектируют и разрабатывают очередные версии своих продуктов на основе рыночного спроса. Вдобавок они противостоят конкуренции путем объединения достоинств и компонентов, на что другим приходится как-то реагировать. Так, продуктом Server Core, который появился в Windows Server 2008 и был улучшен в Windows Server 2012 R2, разработчики из Microsoft расширили линейку своих ОС Windows для борьбы с конкурентами и в ответ на запросы системных администраторов, желавших работать в командной строке. В этой главе мы посмотрим, что нового в Server Core версии Windows Server 2012 R2, и покажем, как управлять этой ОС с использованием PowerShell.

В этой главе вы научитесь:

- пользоваться новой функциональностью в Server Core;
- устанавливать и конфигурировать Server Core;
- настраивать Server Core для развертывания внутри филиала;
- дистанционно управлять ОС.

Что нового в Server Core

Вы уже устанавливали Windows Server 2012 R2 и видели, что на паре экранов отображались варианты установки. Обязаны ли вы применять версию с графическим пользовательским интерфейсом (GUI)? Вам нравятся преимущества Server Core в отношении безопасности и сокращения накладных расходов, но вам также нравится пользовательский интерфейс в стиле "указать и щелкнуть", предлагаемый версией GUI. Для вас есть хорошие новости: в версии Windows Server 2008 R2 после установки Server Core возвратиться назад было невозможно, но в Windows Server 2012 R2 теперь можно переключаться туда и обратно между версиями Server Core и GUI. Стандартным выбором является Server Core, но если вы решите выбрать установку с использованием GUI, то все равно будете иметь доступный инструмент PowerShell. Настроив сервер и подготовив его к функционированию в производственной среде, можете просто переключить его на версию Server Core.

При чтении этой главы имейте в виду, что несмотря на возможность переключения на версию GUI с целью решения тех же задач, мы будем применять для этого Server Core. Например, мы покажем, каким образом проверить копию Windows с использованием Server Core. Вы можете счесть выполнение этих задач более простым, переключившись на версию GUI, и будете полностью правы. Большинство примеров в данной главе рассматривались также в главе 2, где они прорабатывались в версии GUI. В настоящее время PowerShell 3.0 предлагает дополнительные командлеты для администрирования сервера Server Core. Синтаксис командлетов теперь проще для понимания. Ко многим существовавшим ранее командлетам были добавлены параметры, позволяющие расширить их функциональность. В разделе "Руководство по безотказной работе Server Core" далее в этой главе будет приведен полный список новых командлетов, добавленных в Windows Server 2012 R2.

Что такое Server Core?

Server Core — это ОС Windows Server с минимально необходимыми требованиями, позволяющими функционировать в качестве операционной системы. В состав этой ОС не входит графический пользовательский интерфейс, проводник Windows, браузер Internet Explorer и другие зависимые компоненты. Устранение этих дополнений означает, что мы должны обходиться без многих удобных инструментов администрирования, в частности оснасток, встроенных в консоль управления Microsoft (Microsoft Management Console). В итоге главным интерфейсом для управления системой остается командная строка PowerShell.

Что же это означает для администратора?

- **Сокращение затрат на обслуживание.** Меньший объем функциональности снижает объем необходимых обновлений.
- **Уменьшение площади атаки.** Отсутствие дополнительных средств приводит к снижению числа потенциальных целей для атаки. Роли и компоненты можно устанавливать по мере необходимости, а ограниченное количество служб сократит площадь атаки.
- **Сокращение требований к производительности.** Редакция Server Core меньше загружает ЦП и занимает меньше пространства на диске, поэтому требования к оборудованию снижаются.

Установка Server Core

Перед установкой Server Core примите во внимание тот факт, что благодаря возможности переключения между версиями Server Core и GUI, совершенно не имеет значения, какая версия была установлена первой. Это дает возможность установить сервер версии GUI, как объяснялось в главе 2, а затем переключить его на Server Core.

Процесс установки Windows Server 2012 R2 Server Core так же прямолинеен, как и в случае других редакций этой ОС. Вы загружаете сервер из установочного DVD-диска и дальше следуете инструкциям. Можете использовать файл `.xml` автономной установки, чтобы сконфигурировать все вплоть до устанавливаемых компонентов. Этот файл генерируется с помощью комплекта Windows Automated Installation Kit, что в данной главе не рассматривается.

Программа установки позволяет выбрать ОС для установки, как показано на рис. 3.1.

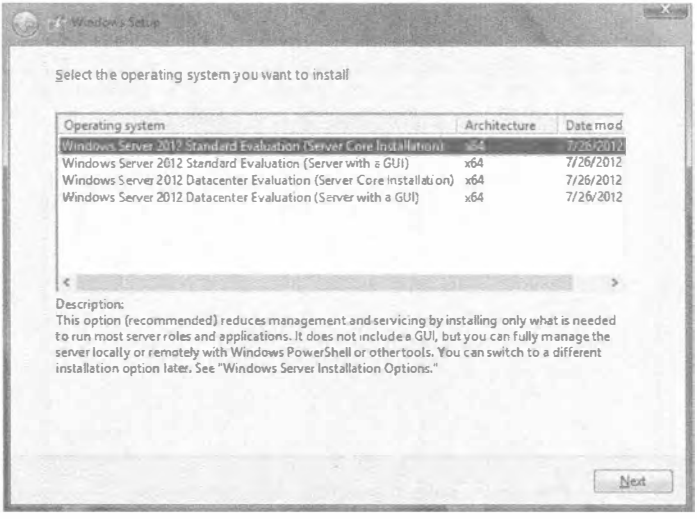


Рис. 3.1. Выбор редакции Server Core при установке Windows Server 2012 R2

1. Выберите желаемую редакцию Server Core — Standard или Datacenter — и щелкните на кнопке Next (Далее).
2. Ознакомьтесь и примите условия лицензионного соглашения и щелкните на кнопке Next. На следующем экране запрашивается необходимый тип установки.
3. Поскольку выполняется чистая установка, выберите переключатель Custom (Специальная). На следующем экране запрашивается местоположение для установки (рис. 3.2).

   Мы предпочитаем делить жесткий диск на два раздела: 50 Гбайт для ОС и оставшийся объем для данных и приложений. Это уменьшает размер резервной копии системного диска. Меньший размер раздела может не позволить дальнейшую установку дополнительных приложений, пакетов обновлений, обновлений безопасности и исправлений, что приведет к нестабильной работе и потенциальной перестройке ОС.
4. Щелкните на ссылке New (Новый) в нижней части экрана, чтобы создать раздел с объемом 50 Гбайт.

   Программу установки Windows также создает системный раздел размером 350 Мбайт, в котором хранится консоль восстановления ОС. Удалить этот раздел не удастся. Не переживайте по поводу этого недоступного пространства; в настоящее время даже флэш-накопители обладают большей емкостью.
5. После успешной установки войдите в систему с применением учетной записи администратора (`Administrator`), как это делалось бы при полной установке.
6. Пароль пока не назначен, поэтому введите новый пароль.

Как только процесс установки завершит построение профиля администратора, появится рабочий стол, показанный на рис. 3.3, который имеет совершенно спартанский вид. Нет ни диспетчера серверов, ни панели задач, ни системного лотка. Имеется только открытое окно командной строки.

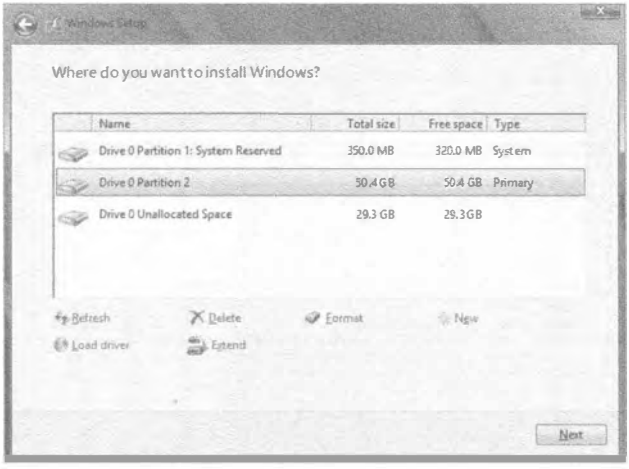


Рис. 3.2. Выбор раздела для установки

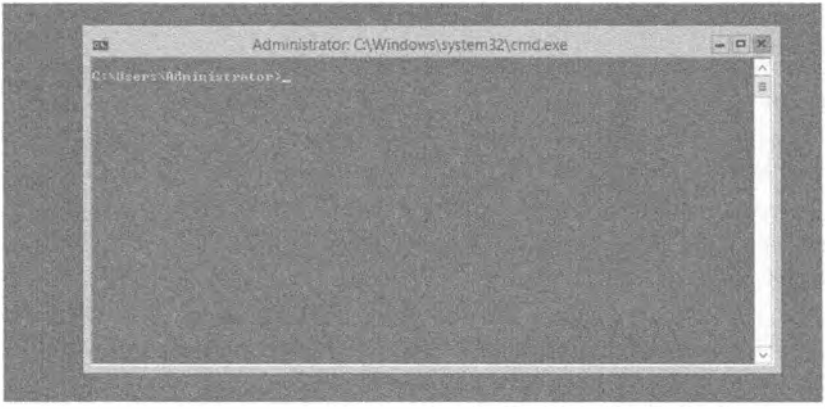


Рис. 3.3. Пустой пользовательский интерфейс Server Core

Для целей этой книги мы изменили стандартные настройки окна командной строки PowerShell, улучшив читабельность экранных снимков. По умолчанию команды будут отображаться белыми символами на черном фоне. Чтобы внести аналогичные изменения, щелкните правой кнопкой мыши на левом верхнем углу экрана и выберите в контекстном меню пункт Properties (Свойства). На вкладке Colors (Цвета) измените цвет шрифта и фона, как показано на рис. 3.4.

Руководство по безотказной работе Server Core

Перед погружением в детали вы должны ознакомиться с несколькими советами по обеспечению безотказной работы этой ОС. Мы обсудим доступ к диспетчеру задач для управления процессами, запуска задач и просмотра показателей производительности. Затем мы рассмотрим базовые команды, которые обычно упускаются из виду, когда доступен графический пользовательский интерфейс, предлагаемый версией GUI. Они позволят выполнять рутинные задачи администрирования и обеспечат доступ в сеть.

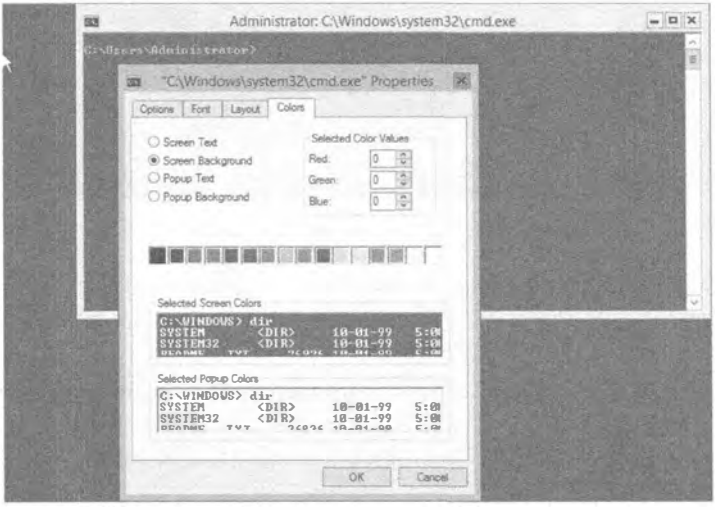


Рис. 3.4. Изменение цветовых настроек окна командной строки

Переключение между версиями Server Core и GUI

Этот прием будет описан первым в руководстве по безотказной работе, поскольку возможность переключения между версиями Server Core и GUI может оказаться очень удобной. Многие администраторы завершают начальную настройку, используя версию GUI, и переключаются на версию Server Core в производственной среде.

Вам понадобится загрузить сценарий, находящийся по адресу:

```
http://gallery.technet.microsoft.com/scriptcenter/
  Switch-between-Windows-9680265d/file/107247/1/SwitchGUIServerCORE.zip
```

Данный сценарий применяется вне зависимости от того, какие версии переключаются. Прежде чем запускать сценарий, необходимо разрешить выполнение сценариев на сервере; по умолчанию это запрещено. Для этого запустите следующий командлет:

```
PS C:\>Set-ExecutionPolicy AllSigned
```

Теперь можно запустить сценарий из местоположения, куда был загружен файл, используя PowerShell (рис. 3.5).

После выдачи запроса введите одно из перечисленных ниже целых значений:

- `1` — для переключения на версию Server Core;
- `2` — для переключения на версию GUI;
- `3` — для установки версии GUI из онлайнового ресурса.

Потерпите некоторое время; весь процесс может занять несколько минут. По завершении будет запрошена перезагрузка сервера, по прошествии которой вы должны увидеть нужную версию ОС.

Доступ к диспетчеру задач

Версия Server Core предоставляет совсем немного компонентов графического пользовательского интерфейса. Наиболее важным является диспетчер задач (Task Manager).

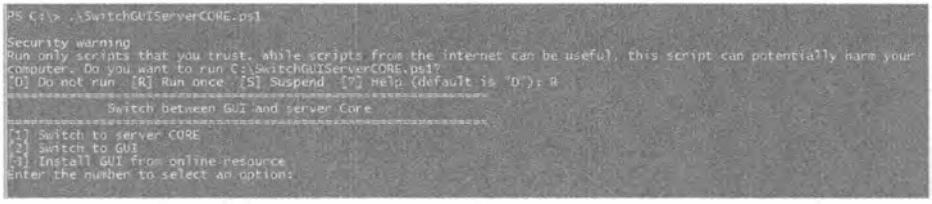


Рис. 3.5. Запуск сценария PowerShell

Это тот самый диспетчер задач, который вы хорошо знаете и любите по другим версиям Windows. Существует два главных способа открыть диспетчер задач, которые описаны ниже.

- <Ctrl+Alt+Del>. Вы можете открыть проверенное временем диалоговое окно Security (Безопасность), нажав комбинацию клавиш <Ctrl+Alt+Del>. В этом диалоговом окне можно по выбору блокировать рабочую станцию, выйти из системы или запустить диспетчер задач.
- <Ctrl+Shift+Esc>. Для запуска диспетчера задач вы можете также воспользоваться методом "секретного рукопожатия MSCE", нажав комбинацию клавиш <Ctrl+Shift+Esc>. Теперь, когда вы об этом знаете, считайте себя членом элитного клуба. Данный метод был одной из недокументированных возможностей.

Закрытие окна командной строки

Вы, как хороший системный администратор, всегда закрываете приложения после завершения работы с ними, чтобы они не потребляли ценные ресурсы, подобные памяти и ЦП, верно? Значит, вы наверняка пожелаете закрыть окно командной строки после завершения задачи во время нахождения в системе Server Core.

Поняв, что вы только что закрыли единственный интерфейс с ОС, для возвращения окна командной строки можете выполнить перечисленные ниже шаги.

1. Откройте диспетчер задач, как объяснялось ранее.
2. Выберите пункт меню File⇨New Task (Run) (Файл⇨Новая задача (Выполнить)). Откроется окно Create new task (Создать новую задачу), подобное окну Run (Выполнить), которое доступно через меню Start (Пуск).
3. Введите **cmd** и щелкните на кнопке OK, как показано на рис. 3.6.
4. Введите **PowerShell** в окне командной строки, что приведет к переключению на командную строку PowerShell.

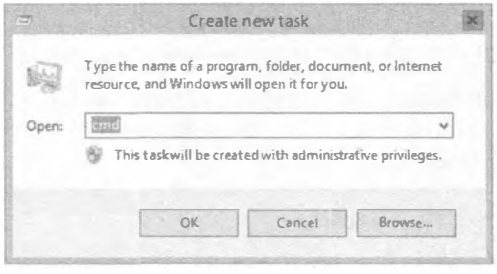


Рис. 3.6. Окно Create new task

Изменение пароля администратора

Инструмент PowerShell будет применяться для выполнения большинства задач администрирования, но все равно есть несколько инструментов командной строки, которые проще в использовании, поэтому они включены в рассматриваемые здесь примеры. После входа в систему Server Core в первый раз вас может интересовать, как можно изменить пароль администратора в будущем.

Это делается с помощью команды `net user`:

```
PS C:\Users\Administrator>net user administrator *
Type a password for the user:
Введите пароль для пользователя:
Retype the password to confirm:
Повторите ввод пароля для подтверждения:
The command completed successfully.
Команда выполнена успешно.
```

Символ звездочки обеспечивает запрос нового пароля.

Команда `net` действительно стара. Она относится к временам, когда ОС Windows NT считалось новой технологией (NT — new technology).

Один из новейших способов изменения пароля предусматривает применение командлета PowerShell под названием `Set-ADAccountPassword`. Ниже приведен синтаксис этого командлета:

```
Set-ADAccountPassword [-Identity] <Учетная запись AD>
[-AuthType {Negotiate | Basic}] [-Credential <Учетные данные PowerShell>]
[-NewPassword <Надежная строка>] [-OldPassword <Надежная строка>]
[-Partition <Строка>] [-PassThru <Переключатель>] [-Reset <Переключатель>]
[-Server <Строка>] [-Confirm] [-WhatIf] [<Общие параметры>]
```

Доступ к общим файлам

С учетом того, что Windows Server является сетевой ОС, вам понадобится получать доступ к общим ресурсам в сети. Если в своей работе вы опирались на проводник Windows, то могли никогда не сталкиваться с необходимостью подключения к общей папке из командной строки. Для отображения общих ресурсов на сервере предназначена команда `net view`:

```
PS C:\Users\Administrator>net view \\bf1
Shared resources at \\bf1
Share name  Type   Used as  Comment
-------------------------------------------------------------------------------
isos        Disk
netlogon    Disk
Public      Disk
SYSVOL      Disk
temp        Disk
The command completed successfully.
```

Для доступа к тому служит команда `net use`, которая отображает общий ресурс на букву устройства:

```
PS C:\Users\Administrator>net use Z: \\bf1\temp
The command completed successfully
```

В командной строке можно переходить на такое устройство, вводя его букву, например, **Z:**. Затем вводятся нужные команды MS-DOS для работы с папками.

Для удаления отображенного устройства используйте следующую команду:

```
PS C:\Users\Administrator>net use Z: /del
Z: was deleted successfully
```

Можно также применять командлет PowerShell под названием `get-psdrive` для получения информации об устройстве и командлет `New-PSDrive` для отображения на новое устройство. Ниже в целях справки показан синтаксис командлета `New-PSDrive`:

```
New-PSDrive [-Name] <Строка> [-PSProvider] <Строка> [-Root] <Строка>
[-Credential <Учетные данные PowerShell>] [-Description <Строка>]
[-Persist] [-Scope <Строка>] [-Confirm] [-WhatIf] [-UseTransaction]
[<Общие параметры>]
```

Поиск команд от A до Z

Справочники по командам очень удобны. В Windows Server 2012 R2 имеется такой справочник для оказания помощи при полной установке; тем не менее, он содержит гиперссылки на объяснения всех этих команд. Лучшим местом для нахождения списка доступных команд является справочник по командам (`http://technet.microsoft.com/en-us/library/cc754340.aspx`), который предлагает меню от A до Z. При поиске команды, которая выполнит работу, это первое место, где следует начинать.

Большинство командлетов PowerShell можно найти через страницу `http://technet.microsoft.com/en-us/library/hh801904.aspx`. На ней вы увидите все категории администрирования со ссылками на сотни командлетов.

Чтение текстовых файлов с помощью Notepad

В полной установке для редактирования текстовых файлов вы используете утилиту Notepad. Она также доступна в Server Core. Эта утилита относится к "старой школе" и представлена в виде очень ранней версии. Хотя она и не настолько древняя, как VI, но существует с тех дней, когда была актуальна ОС Windows NT.

Невероятно, но проектировщики Core на самом деле думали о том, чтобы исключить эту удобную утилиту, пока специалисты из отдела маркетинга не получили обратную связь от пользователей. Удаление этой утилиты стало бы крупной ошибкой. Утилита Notepad является важнейшим инструментом для Server Core.

У нас есть пример текстового файла по имени `ipconfigCommand.txt`. Для его открытия служит следующая команда:

```
C:\Users\Administrator>notepad documents\ipconfigCommand.txt
```

Нам нравится применять Notepad для построения сложных команд. В конце справочного текстового файла, подобного `ipconfigCommand.txt`, приводятся примеры, которые можно вырезать, копировать, вставлять и редактировать необходимым образом. Затем результирующую команду можно вставить в окно командной строки. Вывод этой команды легко скопировать из командной строки, используя пункт Mark (Пометить) контекстного меню, которое доступно по щелчку правой кнопкой мыши. После этого вывод можно вставить обратно в файл, открытый в Notepad.

Редактирование реестра

Сценарий `SCRegedit.wsf` создан командой разработчиков Server Core и предназначен для выполнения общих задач, связанных с редактированием реестра. Список общих задач в Server Core можно получить с помощью параметра `/cli`. Не все задачи придется выполнять, но список включает "секретное рукопожатие MSCE", позволяющее открыть диспетчер задач. Поскольку `scregedit.wsf` является сценарием Visual Basic (VB), его придется запускать через интерпретатор, который находится в папке `System32`, поэтому перейдите в нее:

```
C:\Windows\System32>cscript scregedit.wsf /cli
```

Завершение работы и перезагрузка

Имеется также команда PowerShell, предназначенная для завершения работы и перезагрузки сервера. Можно даже ввести причину перезагрузки или завершения работы в качестве примечания. Для перезагрузки сервера введите следующую команду:

```
PS C:\> Restart-Computer
```

Чтобы перезагрузить удаленные компьютеры, можно ввести показанную ниже команду, которая завершит работу двух удаленных (`Server01` и `Server02`) и локального компьютера (`localhost`):

```
PS C:\> Restart-Computer -ComputerName Server01, Server02, localhost
```

Начальная конфигурация Server Core

Как было указано ранее в этой главе, можно переключиться на версию GUI и сконфигурировать сервер из диспетчера серверов (рис. 3.7), после чего переключиться обратно в режим командной строки.

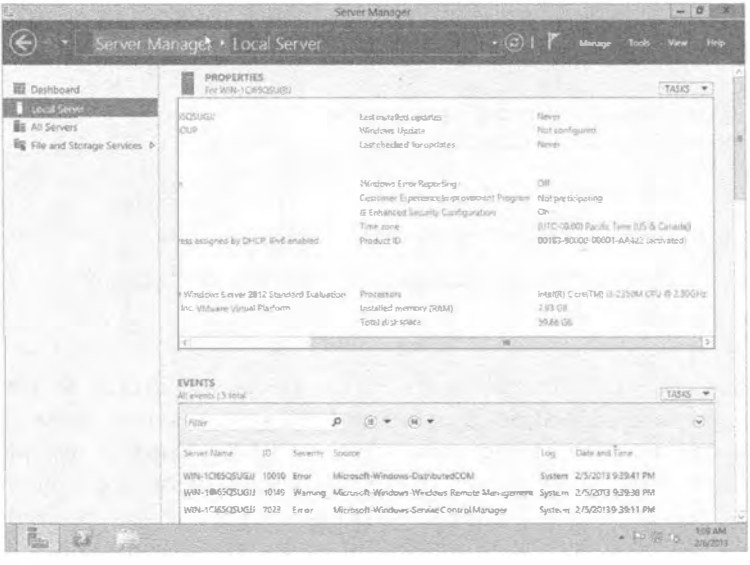


Рис. 3.7. Окно свойств локального сервера в диспетчере задач, доступное после стандартной установки Windows

Мы хотим показать, каким образом конфигурировать сервер с Server Core без установки версии GUI, поэтому мы рассмотрим способы получения работоспособного сервера с применением командной строки.

Предоставление информации о компьютере

Первым делом мы исследуем четыре наиболее базовых задачи конфигурирования, которые обычно выполняются в диспетчере серверов после чистой установки версии GUI системы Windows Server. Все они также могут быть выполнены в командной строке:

- добавление ключа продукта и активация сервера;
- установка часового пояса;
- конфигурирование сети;
- установка имени компьютера и домена.

Ввод ключа продукта и активация сервера

Если вы еще не заметили, в течение процесса установки Windows Server 2012 R2 ввод ключа продукта не является обязательным. Со временем ОС затребует его; без активации Windows Server 2012 R2 может функционировать 60 дней. Когда период льготного пользования установленной полной копии истекает, система переходит в режим сокращенной функциональности (reduced functionality mode — RFM). В результате вы получаете черный рабочий стол и постоянные уведомления, а инструмент Windows Update будет загружать и применять только критические исправления безопасности.

Сценарий `slmgr.vbs` позволяет предоставить ключ продукта и провести активацию сервера. Традиционный процесс предусматривает ввод ключа с последующей онлайновой активацией сервера. В приведенных ниже и далее примерах команд обратите внимание на то, что `rem` — это комментарий, который не обрабатывается командной строкой или пакетными файлами:

```
rem Ввод ключа продукта
cscript c:\windows\system32\slmgr.vbs
-ipk q7y83-w4fvq-6mc6c-6qqtd-tpm88
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Installed product key q7y83-w4fvq-6mc6c-6qqtd-tpm88 successfully.
```

Онлайновая активация осуществляется тем же самым сценарием:

```
rem Онлайновая активация
cscript c:\windows\system32\slmgr.vbs -ato
```

В крупных средах преобладающим методом получения ПО от Microsoft является корпоративное лицензирование. Этот процесс может включать применение службы управления ключами (Key Management Service — KMS), которая централизует активацию на каком-нибудь сервере внутри организации. Такой сценарий будет обсуждаться для развертывания в филиале, поэтому мы рассмотрим настройку KMS на центральном сервере в разделе "Управление лицензиями с помощью службы KMS" далее в главе.

Настройка часового пояса

Версия Server Core не полностью лишена графического пользовательского интерфейса панели управления: в ней остается окно Time and Date (Время и дата), которое открывается с помощью следующей команды:

```
control timedate.cpl
```

После указания времени и даты можно проверить изменения с использованием такой команды:

```
PS C:\Users\Administrator>w32tm /tz
Time zone: Current:TIME_ZONE_ID_DAYLIGHT Bias: 300min
(UTC=LocalTime+Bias)
  [Standard Name:"Eastern Standard Time" Bias:0min Date:(M:10 D:5 DoW:0)]
  [Daylight Name:"Eastern Daylight Time" Bias:-60min Date:(M:4 D:1 DoW:0)]
```

Конфигурирование настроек сети

Главным элементом, который необходимо изменить для сети, является статический IP-адрес.

Для получения ряда базовых конфигурационных настроек сети можно применить утилиту ipconfig или командлет PowerShell:

```
PS C:\Users\Administrator> get-netipconfiguration

InterfaceAlias       : Ethernet
InterfaceIndex       : 12
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection
NetProfile.Name      : Network
IPv4Address          : 192.168.1.20
IPv6DefaultGateway   :
IPv4DefaultGateway   : 192.168.1.1
DNSServer            : 192.168.1.1
```

По умолчанию используется подключение к локальной сети. Для его изменения предназначен командлет PowerShell под названием New-NetIPAddress. Ниже приведен его синтаксис:

```
New-NetIPAddress [-IPAddress] <Строка> -InterfaceAlias <Строка>
[-AddressFamily <Семейство адресов>] [-AsJob] [-CimSession <Массив
CimSession[]>] [-DefaultGateway <Строка>] [-PolicyStore <Строка>]
[-PreferredLifetime <Объект TimeSpan>] [-PrefixLength <Байт>]
[-SkipAsSource <Булевское значение>] [-ThrottleLimit <Значение Int32>]
[-Type <Тип>] [-ValidLifetime <Объект TimeSpan>] [-Confirm] [-WhatIf]
[<Общие параметры>]
```

Предоставление имени компьютера и домена

Какой командлет PowerShell предназначен для добавления компьютера в домен? Все очень просто — командлет Add-Computer:

```
PS c:\Users\Administrator>Add-Computer
```

Командлетам PowerShell не обязательно передавать многочисленные ключи и параметры. Многие командлеты запрашивают параметры, намного упрощая кривую обучения, т.к. требуется запомнить только название командлета, а не все его параметры. С учетом сказанного вы увидите запрос учетных данных для входа (рис. 3.8).

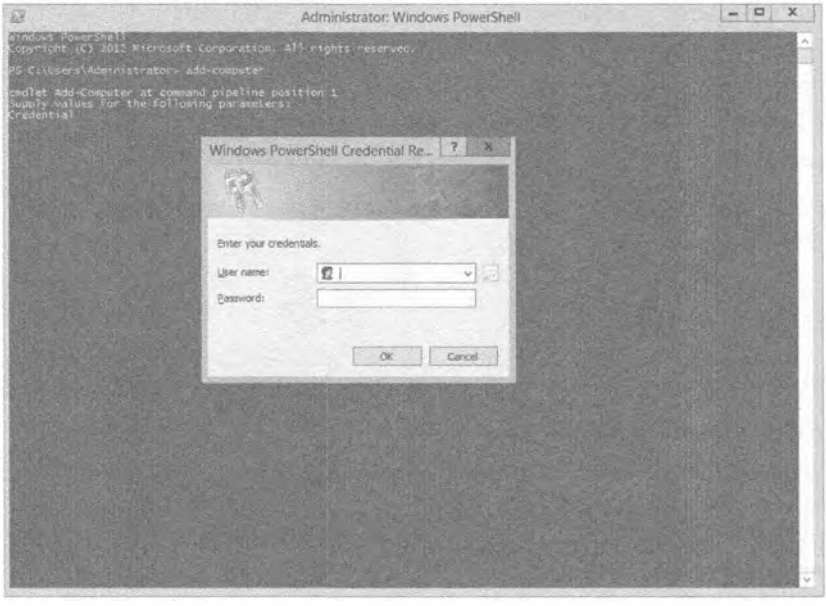


Рис. 3.8. Введите учетные данные для входа

После входа будет запрошено имя домена:

```
cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
DomainName: BigFirm.com
```

По умолчанию программа установки Windows назначает компьютеру довольно оригинальное имя, которое можно просмотреть с применением команды `hostname`:

```
PS c:\Users\Administrator>hostname
WIN-AG6PVO7DM2A
```

Поскольку это имя не особо дружественное к пользователю, мы изменим его на **`Bfsc1`**. (Это не крупное улучшение, но такое имя хотя бы проще для ввода с клавиатуры.) Следующий командлет PowerShell выполняет переименование компьютера:

```
PS c:\Users\Administrator>Rename-Computer
```

После этого PowerShell запросит новое имя компьютера:

```
cmdlet Rename-Computer at command pipeline position 1
Supply values for the following parameters:
NewName:bfsc1
```

Обновление сервера

Следующее действие заключается в выполнении типичных рутинных работ для обновления сервера последними исправлениями, в том числе и связанными с безопасностью. Работы состоят из двух шагов.

1. Включение автоматического обновления и обратной связи.
2. Загрузка и установка обновлений.

Включение автоматического обновления

Поведение автоматического обновления можно модифицировать с помощью нескольких команд, используя SCONFIG. Введите в командной строке **SCONFIG**. В окне командной строки отобразится меню. Выберите вариант 5, Windows Update Settings (Параметры обновления Windows), введя **5**. Это приведет к сообщению текущей настройки, которой по умолчанию является Manual (Ручное). Чтобы изменить его на Automatic (Автоматическое), просто введите букву **A**. На рис. 3.9 показано меню Server Configuration (Конфигурация сервера) и окно с сообщением о том, что автоматическое обновление было включено.

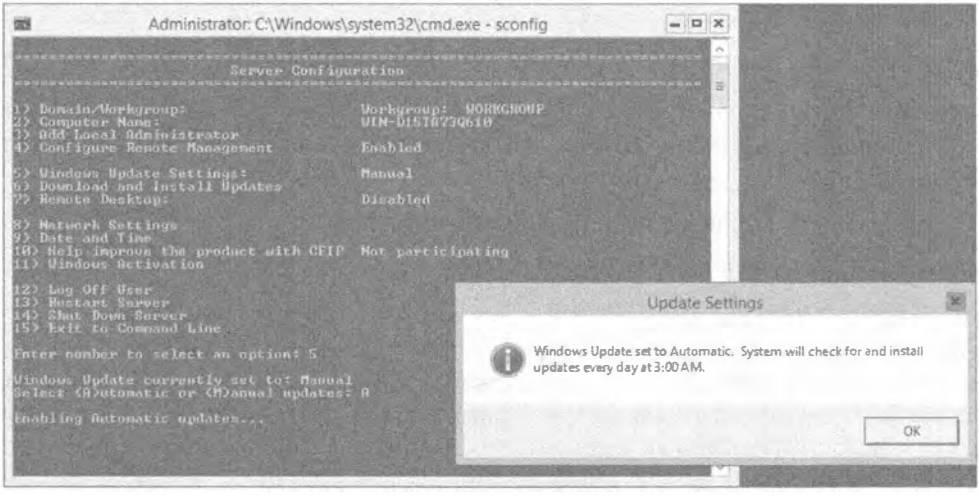


Рис. 3.9. Включение автоматического обновления посредством SCONFIG

На рис. 3.9 также видны все задачи, для выполнения которых можно применять SCONFIG. Мы объясним, как решать некоторые из этих задач с использованием различных инструментов, подобных PowerShell, но это просто другой способ достижения той же самой цели.

Загрузка и установка обновлений

При полной установке мы предпочитаем выполнять этот шаг путем открытия окна свойств системы и перехода в нем на вкладку Automatic Updates (Автоматические обновления). Щелчок на гиперссылке Windows Update Web Site (Веб-сайт Windows Update) инициирует загрузку и установку исправлений. Однако в этом участвует браузер Internet Explorer, который в версии Server Core не устанавливается. Взглянув снова на рис. 3.9, вы заметите, что об этом позаботится вариант 6, Download and Install Updates (Загрузить и установить обновления).

После ввода **6** в командной строке утилита SCONFIG запросит о том, искать все или только рекомендуемые обновления. Сделайте выбор и получите нужные результаты. Затем можете установить все обновления, ни одного или отдельные из них.

Отказ от ответственности за последствия использования примера сценария

Не забывайте, что сценарии, которые вы обнаружите на веб-сайтах, являются примерами, а это значит, что вы должны применять их под собственную ответственность. Компания Microsoft стоит только за объектной моделью, с применением которой они разрабатывались, но не за самими сценариями. У вас имеется возможность модифицировать сценарий; таким образом, есть реальный шанс нарушить работу установленной копии ОС. Вы должны давать себе отчет, что ваши сценарии могут содержать промахи и ошибки. Только от вас зависит написание безошибочного сценария, который делает именно то, что от него требуется. Поскольку эта глава посвящена изложению Server Core, вопросы написания сценариев на VB и детальные обсуждения любых примеров выходят за рамки целей, на которые глава ориентирована.

Настройка сервера

На этом этапе вы приступаете к применению инфраструктурных ролей и включению дистанционного администрирования. Ниже перечислены соответствующие шаги.

1. Добавление ролей и компонентов.
2. Включение дистанционного администрирования.
3. Конфигурирование брандмауэра Windows.

Добавление ролей и компонентов

Консоль диспетчера серверов, появившаяся в полной версии Windows Server 2012, сделала установку ролей и компонентов прямолинейной. По существу вы отмечаете флажок — и роль устанавливается. Если в дополнение к желаемой роли должны быть установлены связанные роли и/или компоненты, мастер добавления ролей и компонентов (Add Roles and Features Wizard) уведомит об этом. Затем по мере продвижения по экранам мастера они будут установлены. В Server Core процесс аналогичен. В результате выполнения команды будет выдано уведомление обо всех связанные ролях и/или компонентах, но без их установки. После этого вам придется выдать множество команд для добавления заранее требуемых компонентов и ролей.

Добавляемыми ролями являются контроллер домена (Active Directory Domain Services), DNS, DHCP и Print and Document Services. Базовые файловые службы уже установлены и поддерживаются службой ролей File Server. Кроме того, добавлена пара компонентов, в том числе Windows Server Backup (Резервное копирование Windows Server) для обеспечения возможности резервного копирования. Следующий командлет PowerShell выдает список доступных ролей и компонентов:

```
rem Вывод списка доступных (включенных и отключенных) ролей
PS C:\Users\administrator>Get-WindowsFeature
```

Теперь, имея этот список, вы можете видеть имена ролей, чтобы добавить их с помощью следующего командлета. В приведенном ниже списке показана роль DHCP Server. В качестве параметра командлета должно указываться имя из столбца `Name` (Имя).

```
Display Name                                Name                 Install State
[ ]DHCP Server                              DHCP                   available
[ ]Active Directory Domain Services         AD-Domain-Services     available
[ ]DNS Server                               DNS                    available
[ ]Print and Document Services              Print-Services         available
PS C:\Users\administrator>Add-WindowsFeature DHCP
```

Установка каждой роли может занять несколько минут. При возникновении проблем с установкой инструмент PowerShell уведомит об этом. Он также сообщит о заранее требуемых компонентах. После добавления роли можете запустить командлет `Get-WindowsFeature` снова, чтобы удостовериться в том, что состояние изменилось на `Installed` (Установлена). Давайте установим оставшиеся компоненты:

```
PS C:\Users\administrator>Add-WindowsFeature AD-Domain-Services
PS C:\Users\administrator>Add-WindowsFeature DNS
PS C:\Users\administrator>Add-WindowsFeature Print-Services
```

Включение удаленного рабочего стола

И снова на помощь приходит утилита `SCONFIG`. Обратившись к рис. 3.9, вы увидите вариант `7, Remote Desktop` (Удаленный рабочий стол). После ввода **7** в командной строке будет выдан запрос о том, что необходимо сделать — включить или отключить удаленный рабочий стол. Выберите `Enable` (Включить), введя букву **E**. Будет задан вопрос о том, нужно ли разрешить клиенты, выполняющие любую версию Remote Desktop, или только клиенты, выполняющие Remote Desktop с Network Level Authentication.

Введите выбранный вариант. Отобразится всплывающее окно с подтверждением, и на этом работа завершена.

Конфигурирование брандмауэра

Понадобится внести некоторые изменения в конфигурацию брандмауэра. Брандмауэр должен пропускать протоколы дистанционного администрирования (Remote Administration). Это включает конфигурирование портов для разрешения коммуникаций, требуемых оснастками консоли управления Microsoft (Microsoft Management Console). Следующая команда разрешает протоколы, ассоциированные с группой Remote Administration:

```
netsh advfirewall firewall set rule group="Remote Administration"
      new enable=yes
```

Указанная группа включает все порты MMC, которые могут быть доступны на сервере. Поскольку существуют подмножества протоколов, вы можете точно настроить политики брандмауэра для дистанционного управления конкретными операциями MMC, такими как Event Viewer (Просмотр событий), Disk Management (Управление дисками), File and Print Services (Службы фалов и печати) и Task Scheduler (Диспетчер задач).

Удивительно, но эта группа не содержит операции Remote Desktop. Они являются частью собственной группы с таким же именем. Группа Remote Desktop должна быть разрешена с помощью приведенной ниже команды, которая, кстати говоря, представляет собой пример из встроенной справочной системы `netsh advfirewall firewall set rule`. Никакой магии здесь нет. (Параметр `new` указывает на добавление новой настройки к правилу.)

```
netsh advfirewall firewall set rule group="Remote Desktop"
      new enable=yes
```

Если вы хотите администрировать брандмауэр из консоли MMC, то должны также выполнить следующую команду:

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

Хотя брандмауэр должен всегда оставаться включенным, бывают ситуации вроде тестирования нового приложения, когда может понадобиться его отключить. Ниже показана команда для включения и отключения брандмауэра:

```
netsh advfirewall set allprofiles state on
netsh advfirewall set allprofiles state off
```

В случае если в конфигурации допущена ошибка, брандмауэр можно сбросить с помощью следующей команды:

```
netsh advfirewall reset
```

Последней из рассматриваемых команд для брандмауэра вы, скорее всего, будете пользоваться наиболее часто; она позволяет разрешать или запрещать порт. Ниже приведен пример добавления и удаления порта 1433 для SQL Server:

```
netsh advfirewall firewall add rule name="Open SQL Server Port 1433"
      dir=in action=allow protocol=TCP localport=1433
netsh advfirewall firewall delete rule name="Open SQL Server Port 1433"
      protocol=tcp localport=1433
```

Мы должны продемонстрировать также командлет PowerShell, который можно применять для конфигурирования брандмауэра. С его помощью можно устанавливать правила, модифицировать их и управлять поведением, изменяя свойства:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

Для удаления правила брандмауэра используйте следующий командлет:

```
Remove-NetFirewallRule -Action Block
```

Дистанционное администрирование Server Core

Прежде чем приступать к конфигурированию ролей, установленных на сервере, необходимо ознакомиться с опциями дистанционного администрирования. Ниже мы кратко опишем их, но вы будете встречаться с ними при конфигурировании ролей в последующих разделах.

Удаленный рабочий стол (Remote Desktop) — это очень надежный и безопасный метод дистанционного администрирования стандартных установленных копий ОС, и он также доступен в версии Server Core. Консоль управления Microsoft (Microsoft Management Console) и ее оснастки превосходны для администрирования Server Core, пока сеть поддерживает это. Новой возможностью является удаленная командная оболочка Windows (Windows Remote Shell), которая предоставляет возможность подключения к удаленному серверу в режиме командной строки.

Управление серверами с помощью удаленного рабочего стола

Терминальные службы (Terminal Services) в административном режиме появились в версии Windows 2000. Они были желанным дополнением, т.к. предоставляли среду виртуального рабочего стола подключаемого компьютера. В Windows Server 2003 они стали устанавливаться по умолчанию. Это важный метод для выполнения дистанционной работы на серверах. С применением данного метода мы обычно устанавливали и конфигурировали приложения на серверах Windows, находящимся на другом конце континента. Это надежный вариант для Server Core.

В Windows Server 2012 Server Core вы должны понимать, что рабочий стол содержит всего лишь командную строку и несколько инструментов с графическим поль-

зовательским интерфейсом, т.е. все то же самое, как если бы вы вошли в систему локально. Существуют методы для публикации на вашем рабочем столе только командной строки Server Core в виде приложения RemoteApp, но мы не рекомендуем поступать так. Вам по-прежнему нужны инструменты с графическим пользовательским интерфейсом, такие как диспетчер задач, Notepad и редактор реестра, входящие в состав ядра Server Core. Не забывайте, что удаленный рабочий стол и его политика брандмауэра должны быть разрешены, чтобы быть доступными. Мы делали это ранее в разделе "Начальная конфигурация Server Core".

Дистанционное управление с помощью оснасток консоли MMC

Администраторы нашли консоль управления Microsoft (Microsoft Management Console — MMC) универсальным методом для управления удаленными компьютерами. Ее сила заключается в использовании протокола RPC и интегрированной аутентификации Windows, что обеспечивает быстрое и эффективное управление компьютерами из домена внутри локальной сети.

Проблему с изменением учетных данных аутентификации можно обойти. Введите следующую команду, чтобы зарегистрировать свои учетные данные:

```
cmdkey /add:bfscl /user:Administrator /pass:P@ssw0rd
```

Вы можете предпочесть не указывать параметр `/pass`, чтобы ввод пароля запрашивался интерактивно. После регистрации своих учетных данных к серверу можно подключаться через оснастку.

Для получения в свое распоряжение оснасток, управляющих всеми службами Windows, в предшествующих версиях Windows Server необходимо было устанавливать пакет `adminpak.msi`. В версии Windows Server 2012 пакет `adminpak.msi` был заменен компонентом Remote Server Administration Tools (Инструменты дистанционного администрирования северов). Его установка стала проще и лучше в настройке. На рис. 3.10 показано, что компонент Remote Server Administration Tools был включен в мастере добавления ролей и компонентов.

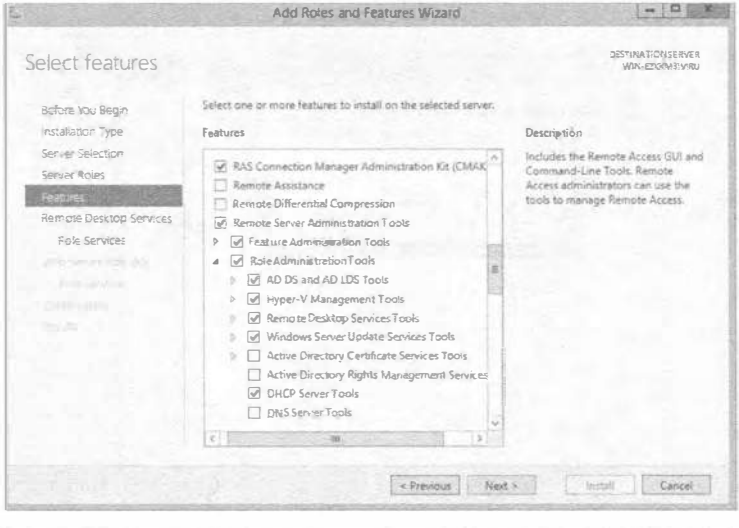


Рис. 3.10. Установка компонента Remote Server Administration Tools

Добавив оснастку к новой консоли MMC, при желании можете подключиться к другому компьютеру. Некоторые оснастки позволяют объединять множество серверов в одно дерево с целью проведения консолидированного администрирования. Ниже описаны шаги по созданию консоли MMC для управления службой в установленной копии Windows Server 2012 Server Core. Обратите внимание, что эти шаги могут быть выполнены только после того, как служба DHCP будет запущена и авторизована. Все это обсуждается в разделе "Конфигурирование службы DHCP" далее в главе.

1. После установки компонента Remote Server Administration Tools в полной установленной копии ОС введите **mmc** в окне Run (Выполнить).
2. Выберите в меню File (Файл) пункт Add/Remove Snap-in (Добавить или удалить оснастку).
3. Откроется диалоговое окно Add/Remove Snap-in (Добавление или удаление оснасток) со списком доступных оснасток, которые можно добавить в этот экземпляр консоли.
4. Выберите оснастку DHCP и щелкните на кнопке Add (Добавить). Затем щелкните на кнопке OK.
5. В окне консоли MMC щелкните правой кнопкой мыши на значке DHCP и выберите в контекстном меню пункт Add Server (Добавить сервер).
6. Откроется диалоговое окно Add Server (Добавление сервера), в нижней части которого находится список авторизованных серверов DHCP (рис. 3.11). Выберите нужный экземпляр Server Core.
7. Щелкните на кнопке OK, и отобразятся детали выбранного сервера DHCP, по которым можно осуществлять навигацию, как показано на рис. 3.12.

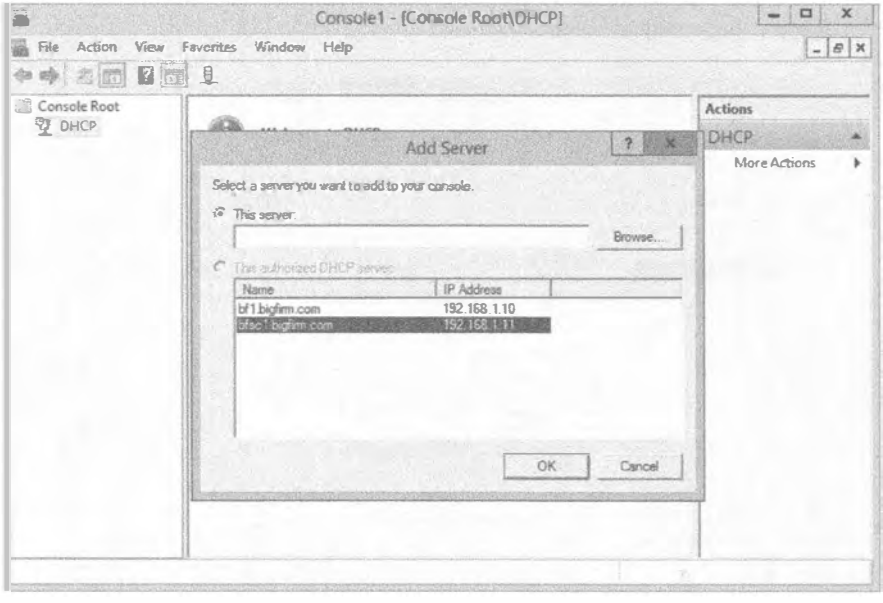


Рис. 3.11. Добавление сервера DHCP в консоль MMC

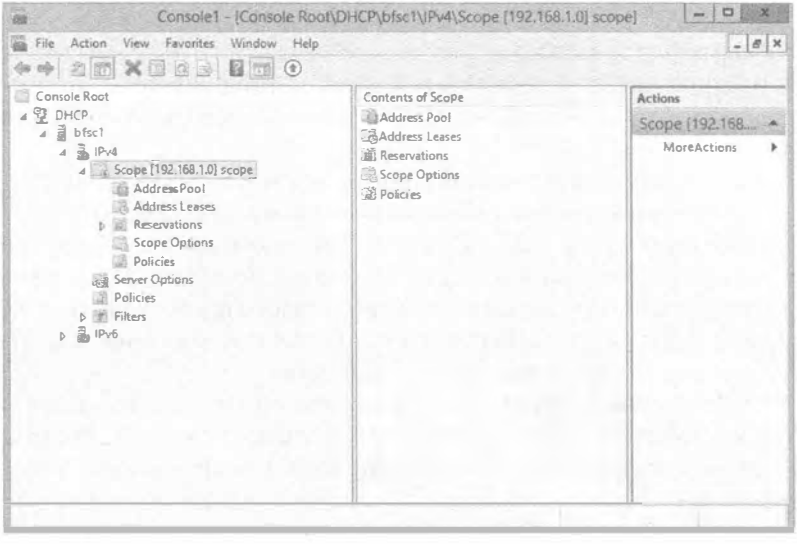


Рис. 3.12. Консоль DHCP с выбранным экземпляром Server Core

Отправка команд дистанционным образом: Windows Remote Shell

Инструмент Windows Remote Shell (Удаленная командная оболочка Windows) позволяет отправлять команды серверу. Аналогично Telnet, он дает возможность подключиться к серверу и запустить команду из удаленной командной строки. Однако он не поддерживает постоянное подключение, как это присуще Telnet. Инструмент Windows Remote Shell отправляет команду, получает результаты ее выполнения и закрывает подключение.

Это облегченное клиент-серверное приложение, построенное на основе технологии SOAP (Simple Object Access Protocol — простой протокол доступа к объектам). Относительно протокола SOAP нужно знать только то, что для отправки команды серверу клиент использует текст в формате XML, и тот же самый формат имеет вывод, посылаемый обратно клиенту по протоколу HTTP. Коммуникации, основанные на тексте, легко читать с помощью текстовых редакторов наподобие Notepad, а протокол HTTP легко отслеживать посредством анализатора протоколов. Таким образом, не считайте Windows Remote Shell безопасным методом управления сервером. Вы должны заблокировать его.

В Microsoft предлагают возможность испытания Windows Remote Shell через команду `winrm quickconfig`. Тем не менее, она устроена так, что работает с HTTP и портом TCP под номером 5985. Согласно рекомендациям, такая настройка не предназначена для производственных сред. Чтобы пользоваться этим инструментом, вы должны обеспечить шифрование коммуникаций и аутентификацию сервера. Такой уровень защиты предоставляется протоколом IPsec, но он может оказаться недоступным. Вы можете настроить Windows Remote Shell для коммуникаций по протоколу HTTPS (SSL), который применяет серверный сертификат для аутентификации сервера и шифрования подключения.

Ниже рассматриваются необходимые основные шаги.

Получение сертификата

Получить сертификат можно двумя способами: купить его в известном центре сертификации или настроить собственный центр сертификации и запросить сертификат у него. Второй способ гораздо менее затратный, особенно при использовании Windows Server.

Собственный центр сертификации также несложен в настройке; однако вы должны иметь полностью готовый план относительно того, как это будет достигнуто в производственной среде Active Directory. Вы должны обдумать решения, которые оказывают продолжительное влияние на всю организацию. И это влияние будет требовать ручного администрирования, если понадобится устранить его. В данном разделе не будем вдаваться в особые детали. Мы собираемся показать, как это сделать "быстро и начерно" в экспериментальной среде.

В контроллере домена с полностью установленной ОС Windows Server 2012 установлена служба сертификатов Active Directory (Active Directory Certificate Services). Обычно эта служба роли включает компонент Certification Authority Web Enrollment (Веб-развертывание центра сертификации). В свою очередь, он может потребовать компонент Internet Information Services (IIS). Мы не будем его устанавливать, а выберем только службу Certificate Authority (Центр сертификации). Она позволит создавать и администрировать сертификаты. В дополнение эта служба предоставит компьютерам домена возможность запрашивать сертификаты, применяя протокол RPC и аутентификацию Kerberos. Мы установим *доверенный корневой центр сертификации предприятия*. Корневой выбран потому, что это первый и единственный домен в организации. Уровень предприятия выбран из-за того, что для выяснения, заслуживают ли доверия серверы и пользователи, центр сертификации использует Active Directory. Поскольку он взаимодействует с Active Directory, центр сертификации автоматически выдает проверенных пользователей и компьютеры. Учитывая, что `Bfsc1` является контроллером домена, он автоматически запрашивает сертификат. Словом, быстро и начерно.

Нам необходимо просмотреть сертификат в Server Core. (Мы сначала пробовали использовать консоль MMC дистанционным образом, но по причинам, связанным с безопасностью, это не вариант.) Доступны два метода просмотра сертификатов в Server Core — команда `certutil` или и команда PowerShell по имени `dir`:

```
rem Использование certutil
PS C:\Users\Administrator.BIGFIRM\Documents>certutil -viewstore my
my
```

Строка `my` ссылается на собственные сертификаты из хранилища локальной машины. После запуска `certutil` открывается окно со списком установленных сертификатов (рис. 3.13). Обратите внимание на ссылку Click here to view certificate properties (Щелкните здесь, чтобы просмотреть свойства сертификата) ниже единственного установленного сертификата. Щелчок на ней приведет к открытию окна с информацией о сертификате.

Инструмент PowerShell предлагает еще один способ получения сертификатов через их поставщиков. Обычно поставщик представляет собой группу объектов, по которым PowerShell может проходить. Примером поставщика является файловая система, поэтому вы можете выполнять операции над объектами файлов и папок внутри нее. Другой поставщик — хранилище сертификатов. По хранилищу сертификатов можно проходить для просмотра и управления сертификатами.

Рис. 3.13. Сертификаты, отображаемые `certutil`

Команда `dir` — это псевдоним, созданный разработчиками PowerShell для командлета `get-items`. Подобным образом вы можете применять стандартную командную строку MS-DOS для навигации по файловой системе. Следующая команда выводит список тех же самых местоположений, что и выполненная ранее команда `certutil`:

```
rem Запуск PowerShell
C:\Users\Administrator.BIGFIRM >powershell

PS C:\Users\administrator.BIGFIRM> dir cert:\localmachine\my | FL

Subject          : CN=BFSC1.bigfirm.com
Issuer           : CN=bigfirm-BF1-CA, DC=bigfirm, DC=com
Thumbprint       : 03ADB670C63E8D1CDB764CD7AA589C51D854307C
FriendlyName     :
NotBefore        : 7/23/2009 6:55:41 PM
NotAfter         : 7/23/2010 6:55:41 PM
Extensions       : {System.Security.Cryptography.Oid, System.Security.
Cryptography
                   .Oid, System.Security.Cryptography.Oid,
                        System.Security.Cryptography.Oid...}
```

Параметр `| FL` в действительности является сокращением другой команды. Он форматирует вывод команды `dir` в список строк. Нам нравится подобный формат, потому что значения не усекаются, как обычно происходит в табличном формате. В данном случае табличный формат (который не показан) не усекает самое важное значение — отпечаток (`Thumbprint`).

Создание прослушивателя

Прослушиватель сообщает службе Windows Remote Shell порт и IP-адрес для прослушивания и ответа на клиентские запросы. По умолчанию порт HTTP имеет номер 5985, а порт HTTPS — 5986. Ниже приведена команда, с помощью которой можно просмотреть стандартные настройки. Атрибуты `<cfg:HTTP>` и `<cfg:HTTPS>` в выводе этой команды отражают настройки портов. Независимо от того, что вы можете думать о языке XML, параметром команды является `format:pretty`. Вывод выглядит избыточным. Тем не менее, верхняя половина, начиная с `<cfg:Client>`, представляет настройки клиента, который будет отправлять запросы другим серверам. Нижняя половина, начинающаяся с `<cfg:Service>`, описывает настройки службы, которая будет получать эти запросы для их выполнения на данном сервере.

```
PS C:\Users\administrator.BIGFIRM>winrm get winrm/config -format:pretty
<cfg:Config xml:lang="en-US" xmlns:cfg="http://schemas.microsoft.com/wbem/wsman/
1/config">
   <cfg:MaxEnvelopeSizekb>150</cfg:MaxEnvelopeSizekb>
   <cfg:MaxTimeoutms>60000</cfg:MaxTimeoutms>
   <cfg:MaxBatchItems>32000</cfg:MaxBatchItems>
   <cfg:MaxProviderRequests>4294967295</cfg:MaxProviderRequests>
   <cfg:Client>
      <cfg:NetworkDelayms>5000</cfg:NetworkDelayms>
      <cfg:URLPrefix>wsman</cfg:URLPrefix>
      <cfg:AllowUnencrypted>false</cfg:AllowUnencrypted>
      <cfg:Auth>
         <cfg:Basic>true</cfg:Basic>
         <cfg:Digest>true</cfg:Digest>
         <cfg:Kerberos>true</cfg:Kerberos>
         <cfg:Negotiate>true</cfg:Negotiate>
         <cfg:Certificate>true</cfg:Certificate>
         <cfg:CredSSP>false</cfg:CredSSP>
      </cfg:Auth>
      <cfg:DefaultPorts>
         <cfg:HTTP>5985</cfg:HTTP>
         <cfg:HTTPS>5986</cfg:HTTPS>
      </cfg:DefaultPorts>
      <cfg:TrustedHosts></cfg:TrustedHosts>
   </cfg:Client>
   <cfg:Service>
    <cfg:RootSDDL>O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
    </cfg:RootSDDL>
    <cfg:MaxConcurrentOperations>4294967295</cfg:MaxConcurrentOperations>
    <cfg:MaxConcurrentOperationsPerUser>15</cfg:MaxConcurrentOperationsPerUser>
    <cfg:EnumerationTimeoutms>60000</cfg:EnumerationTimeoutms>
    <cfg:MaxConnections>25</cfg:MaxConnections>
    <cfg:MaxPacketRetrievalTimeSeconds>120</cfg:MaxPacketRetrievalTimeSeconds>
    <cfg:AllowUnencrypted>false</cfg:AllowUnencrypted>
    <cfg:Auth>
         <cfg:Basic>false</cfg:Basic>
         <cfg:Kerberos>true</cfg:Kerberos>
         <cfg:Negotiate>true</cfg:Negotiate>
         <cfg:Certificate>false</cfg:Certificate>
         <cfg:CredSSP>false</cfg:CredSSP>
         <cfg:CbtHardeningLevel>Relaxed</cfg:CbtHardeningLevel>
    </cfg:Auth>
    <cfg:DefaultPorts>
         <cfg:HTTP>5985</cfg:HTTP>
         <cfg:HTTPS>5986</cfg:HTTPS>
    </cfg:DefaultPorts>
    <cfg:IPv4Filter>*</cfg:IPv4Filter>
    <cfg:IPv6Filter>*</cfg:IPv6Filter>
    <cfg:EnableCompatibilityHttpListener>false</cfg:EnableCompatibilityHttpListener>
    <cfg:EnableCompatibilityHttpsListener>false
    </cfg:EnableCompatibilityHttpsListener>
    <cfg:CertificateThumbprint></cfg:CertificateThumbprint>
   </cfg:Service>
```

```
    <cfg:Winrs>
      <cfg:AllowRemoteShellAccess>true</cfg:AllowRemoteShellAccess>
      <cfg:IdleTimeout>180000</cfg:IdleTimeout>
      <cfg:MaxConcurrentUsers>5</cfg:MaxConcurrentUsers>
      <cfg:MaxShellRunTime>2147483647</cfg:MaxShellRunTime>
      <cfg:MaxProcessesPerShell>15</cfg:MaxProcessesPerShell>
      <cfg:MaxMemoryPerShellMB>150</cfg:MaxMemoryPerShellMB>
      <cfg:MaxShellsPerUser>5</cfg:MaxShellsPerUser>
    </cfg:Winrs>
</cfg:Config>
```

Прослушиватель также позволяет сопоставлять сертификат с портом и IP-адресом. Таким образом, используя надежный прием, который приведен в примере внутри встроенной документации по команде `winrm /?`, мы подготовили следующую команду, предназначенную для создания прослушивателя:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @
{Hostname="bfsc1.bigfirm.com";
  CertificateThumbprint="03ADB670C63E8D1CDB764CD7AA589C51D854307C"}
```

Параметры команды объясняются ниже.

`Address=*`	Служба будет прослушивать все доступные IP-адреса.
`Transport=HTTPS`	Существуют только два варианта: HTTP и HTTPS. Указанные протоколы работают со стандартными портами 5985 и 5986.
`Hostname=`	Это должно соответствовать имени хоста в сертификате.
`CertificateThumbprint=`	Это отпечаток, полученный с помощью команды `certutil`.

Создание входящего правила брандмауэра

Следующее требование связано с включением входящего правила брандмауэра с целью получения клиентских запросов. Для незащищенного порта HTTP такое правило уже доступно, и его можно настроить с применением опции `/quickconfig`, но необходимо построить правило для порта HTTPS.

Если вы — дотошный системный администратор, то можете быть склонны к использованию команды `netsh advfirewall firewall` с многочисленными параметрами. С другой стороны, оснастка MMC предназначена для спокойных, попивающих кофе непрофессиональных системных администраторов. Материал этой книги ориентирован как на первый, так и на второй типаж.

Мы начнем с непрофессионального стиля, который позволит увидеть важнейшие параметры при конструировании правила. Мастера наподобие New Inbound Rule Wizard (Мастер нового входящего правила) удобны, поскольку они обеспечивают проход по всем шагам процесса конфигурирования, не пропуская ни одного важного из них. Они будут оказывать помощь в формировании строки команды, позволяющей создать то же самое правило. Точно так же как в разделе "Руководство по безотказной работе Server Core", мы рекомендуем создавать правила сначала посредством мастера в случае стандартной установки и затем пробовать делать это в командной строке. Другой вариант предполагает принятие более простого подхода, при котором строка команды создается в среде стандартной установки и преобразуется в Server Core, как объяснялось в разделе "Руководство по безотказной работе Server Core".

Используя брандмауэр Windows в режиме повышенной безопасности (Windows Firewall with Advanced Security), сфокусированный на установку Server Core, мы проведем вас через мастер нового входящего правила.

На первой странице мастера (рис. 3.14) выберите переключатель Port (Для порта), чтобы создать правило для порта.

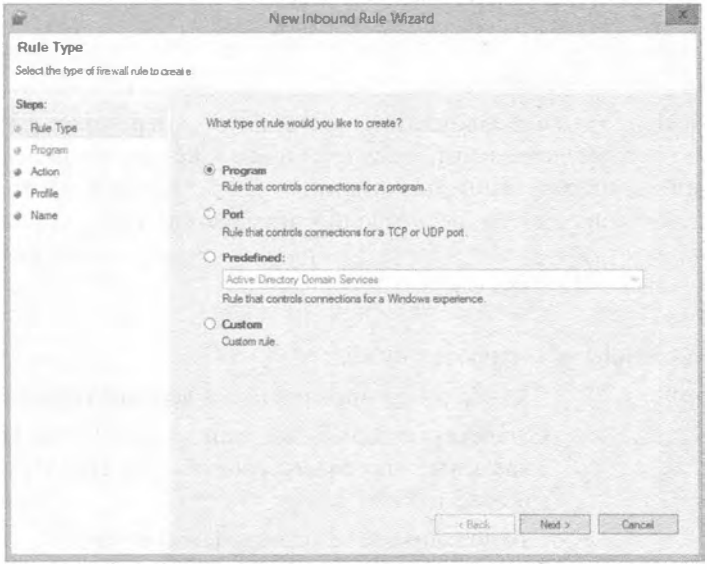


Рис. 3.14. Выбор типа входящего правила

На странице Protocol and Ports (Протокол и порты) выберите переключатель TCP и введите **5986** в качестве номера порта (рис. 3.15).

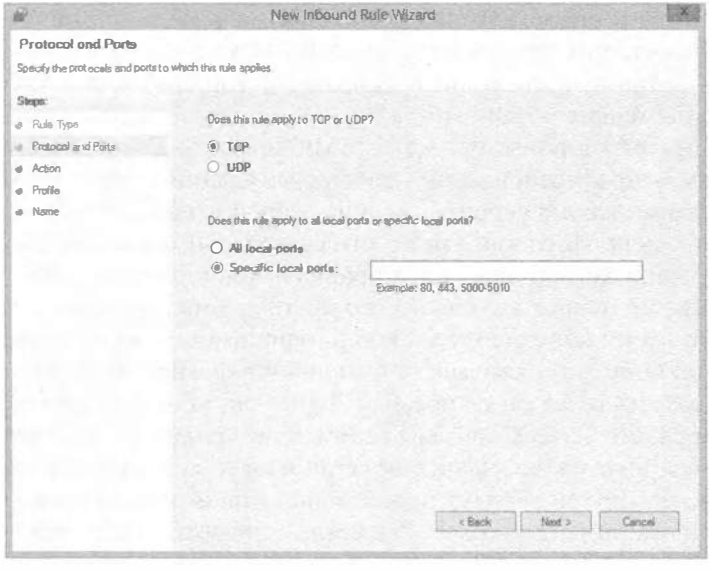


Рис. 3.15. Выбор протокола и порта для входящего правила

На странице Action (Действие), показанной на рис. 3.16, предлагаются три опции, которые описаны ниже.

- Allow the connection (Разрешить подключение). Это то, что нужно в рассматриваемом примере.
- Allow the connection if it is secure (Разрешить безопасное подключение). Для организации подключения требуются коммуникации IPSec. Для установки политик IPSec можно воспользоваться компонентом Network Access Protection (Защита доступа в сеть) внутри сети.
- Block the connection (Блокировать подключение). Это приводит к блокированию подключения.

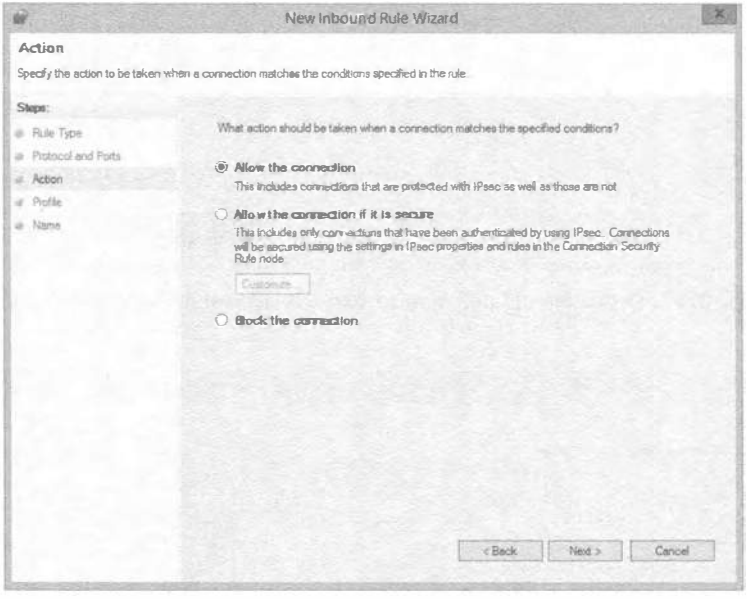


Рис. 3.16. Выбор действия для входящего правила

Страница Profile (Профиль) позволяет выбрать профили, для которых применяется создаваемое правило (рис. 3.17). Публичный и частный профили предназначены для компьютеров, являющихся мобильными, так что вы можете работать дома или в беспроводных точках доступа. Поскольку текущий сервер выступает в качестве контроллера домена, понятия "публичный" и "частный" к нему неприменимы. В целях защиты оставьте отмеченным только флажок Domain (Доменный).

На странице Name (Имя) можно ввести имя и необязательное описание нового правила (рис. 3.18).

Теперь, когда вы знаете параметры, требуемые для создания входящего правила, давайте взглянем на метод, ориентированный на опытных системных администраторов. Ниже приведен синтаксис для создания правила брандмауэра, взятый из встроенной справочной системы. Обратите внимание, что команда должна выполняться в интерактивной оболочке `netsh`.

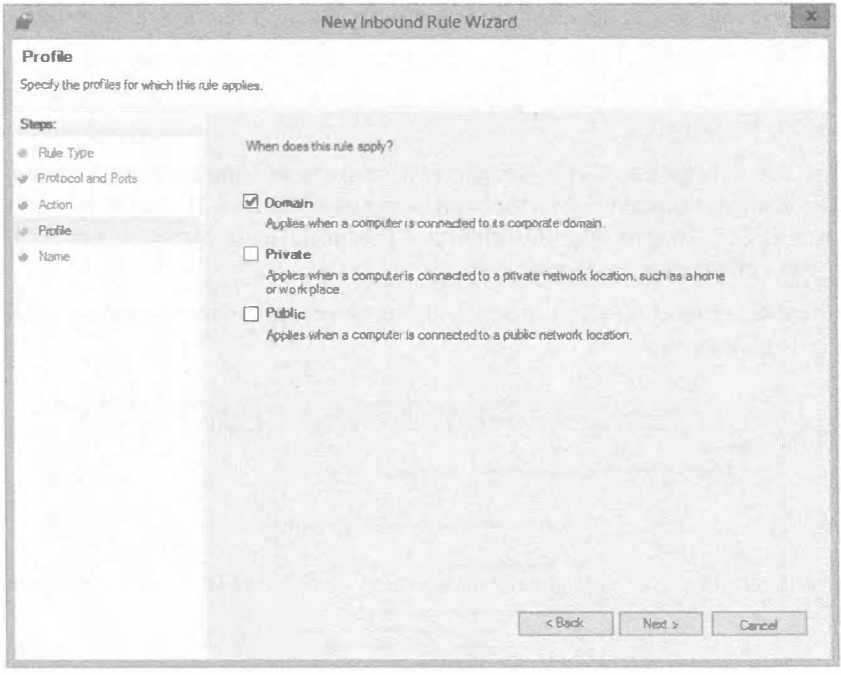


Рис. 3.17. Ограничение правила только коммуникациями внутри домена

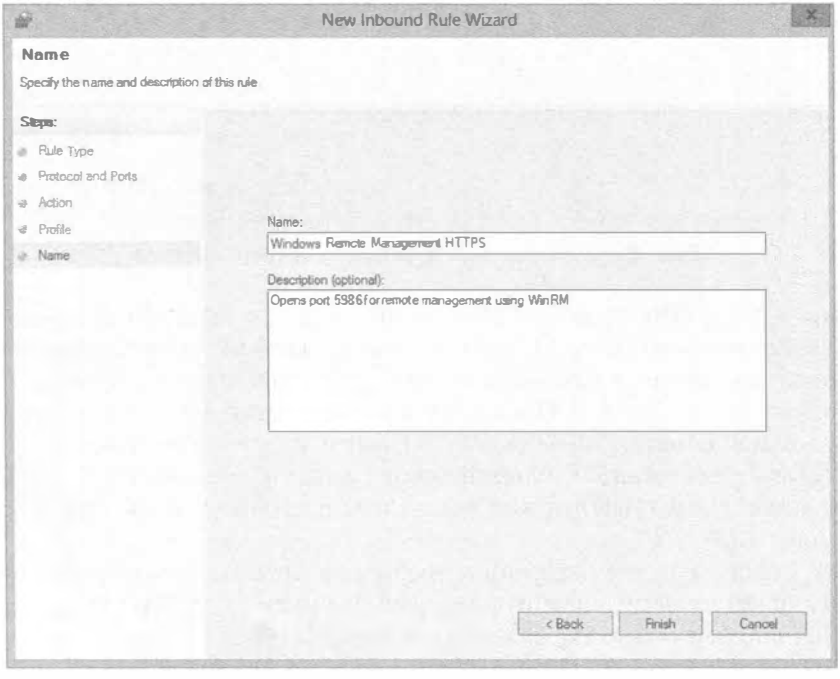


Рис. 3.18. Предоставление описательного имени для правила

Данная работа также может быть сделана в виде одной командной строки:

```
netsh advfirewall firewall>add rule ?

Использование: add rule name=<строка>
  dir=in|out
  action=allow|block|bypass
  [program=<путь к программе>]
  [service=<короткое имя службы>|any]
  [description=<строка>]
  [enable=yes|no (по умолчанию=yes)]
  [profile=public|private|domain|any[,...]]
  [localip=any|<адрес IPv4>|<адрес IPv6>|<подсеть>|<диапазон>|<список>]
  [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|
      <адрес IPv4>|<адрес IPv6>|<подсеть>|<диапазон>|<список>]
  [localport=0-65535|<диапазон портов>[,...]|RPC|RPC-EPMap|IPHTTPS|any
(по умолчанию=any)]
  [remoteport=0-65535|<port range>[,...]|any (по умолчанию=any)]
  [protocol=0-255|icmpv4|icmpv6|icmpv4:тип,код|icmpv6:тип,код|
      tcp|udp|any (по умолчанию=any)]
  [interfacetype=wireless|lan|ras|any]
  [rmtcomputergrp=<строка SDDL>]
  [rmtusrgrp=<строка SDDL>]
  [edge=yes|deferapp|deferuser|no (по умолчанию=no)]
  [security=authenticate|authenc|authdynenc|authnoencap|notrequired
      (по умолчанию=notrequired)]
```

Список параметров является длинным и пугающим. Однако в разделе "Руководство по безотказной работе Server Core" было указано, что вы можете ознакомиться с примерами, приведенными в конце встроенной справки. Их можно вырезать и редактировать в Notepad, чтобы добиться необходимого эффекта. Следует отметить, что командная строка не обладает особо большими возможностями по обучению:

```
PS C:\Users\administrator.BIGFIRM> netsh advfirewall firewall add rule
name="Windows Remote Management HTTPS"
description="Открывает порт 5986 для дистанционного управления с
использованием WinRM" protocol=TCP dir=in localport=5986
profile=domain action=allow
Ok
```

Ниже приведено описание параметров и их соответствие ранее показанным страницам мастера.

- `add rule`. В оснастке мы должны щелкнуть на объекте Inbound Rules (Входящие правила) правой кнопкой мыши и выбрать в контекстном меню пункт New (Новое).
- `name=` и `description=`. Это информация, добавленная на последнем экране мастера (см. рис. 3.18).
- `protocol=` и `localport=`. Эта информация была добавлена так, как показано на рис. 3.15.
- `dir=`. Это отражает входящую характеристику правила. Направление было установлено выбором мастера нового входящего правила (New Inbound Rule Wizard).

- `profile=`. Установка профиля иллюстрировалась на рис. 3.17. Опции в командной строке имеют те же самые значения: `[profile=public|private|domain|any[,...]]`.
- `action=`. Установка профиля была произведена так, как показано на рис. 3.16. Опции в командной строке имеют в основном такие же значения: `action=allow|block|bypass`. Однако `bypass` — это эквивалент выбора переключателя Allow the connection if it is secure.

На рис. 3.15 обратите внимание на то, что тип правила является следствием выбора локального порта. Правило, которое основано на программе или службе, обладает собственной структурой, которая имеет примеры, приведенные во встроенной справке.

Тестирование с помощью WinRS

Текущим клиентом, доступным для Windows Remote Shell, является `winrs.exe`. Он функционирует в средах Windows 7, Windows 8 и Windows Server 2012. Для тестирования службы мы воспользовались справочной информацией по `winrs.exe`:

```
rem Тестирование winrs с включенным брандмауэром.
PS C:\Users\Administrator.BIGFIRM>winrs -r:https://bfsc1.bigfirm.
com:5896 ipconfig

Windows IP Configuration


Ethernet adapter Internal:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b5a1:157f:7220:4f4c%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

Конфигурирование ролей и компонентов

Теперь все готово для помещения этой скромной инфраструктурной машины в производственную среду. Данный экземпляр Server Core планируется настроить в качестве инфраструктурного сервера филиала. Он будет предоставлять службы аутентификации, файлов и печати, а также общую сетевую поддержку для небольшой группы компьютеров в корпоративной сети, имеющей связи с глобальной сетью.

Во время выполнения начальных задач на компьютере были установлены роли Active Directory Domain Services, DNS, DHCP и Print and Document Services. Каждая из упомянутых ролей нуждается в конфигурировании. Мы покажем, как выполнять начальные задачи для каждой службы с применением командной строки и инструментов с графическим пользовательским интерфейсом.

На сервере уже установлены две дополнительные роли — служба роли File Server (Файловый сервер) и служба Key Management Service (Служба управления ключами). Служба роли File Server будет конфигурироваться для предоставления сетевого доступа к локальным папкам. Служба Key Management Service будет управлять активацией ОС с корпоративными лицензиями внутри сети. Сервер филиала может оказаться наилучшей площадкой для получения информации об активации, предназначенной филиалу, от серверов лицензий Microsoft.

Поскольку сервер филиала изолирован от корпоративного центра данных, он должен выполнять операции резервного копирования данных, хранящихся в общих папках. В первоначальной конфигурации устанавливается компонент Windows Server Backup (Резервное копирование Windows Server), и далее мы продемонстрируем команды, позволяющие соответствующим образом скопировать нужные данные.

Детали конфигурирования Server Core для того или иного компонента будут встречаться в этой книге повсеместно.

Создание контроллера домена и управление DNS

В предшествующих версиях Windows Server для создания и продвижения контроллеров доменов необходимо было использовать утилиту командной строки `DCPromo`. В Windows Server 2012 утилита `DCPromo` была объявлена устаревшей и допускала применение только с файлом ответов. По этой причине мы собираемся продемонстрировать новый способ создания контроллера домена с применением PowerShell. Так как роль Active Directory Domain Services (AD DS) была установлена ранее в главе, большая часть работы уже сделана.

Вы должны провести проверку предварительных условий, которая является нововведением Windows Server 2012. Такая проверка поможет выяснить, подходит ли сервер для установки контроллера домена.

Командлет `Test-ADDSDomainControllerInstallation` выполняет проверку предварительных условий для установки контроллера домена, как если бы осуществлялась реальная установка. Он запрашивает учетные данные для входа в домен, как показано на рис. 3.19.

Рис. 3.19. Выполнение `Test-ADDSDomainControllerInstallation`

Все готово для установки контроллера домена. Командлет `Install-ADDS DomainController` одновременно установит и DNS. Если никакие параметры не указаны, то будут использоваться следующие стандартные настройки:

- Контроллер домена, допускающий только чтение: нет
- Глобальный каталог: да
- DNS-сервер: да
- Папка базы данных: `C:\Windows\NTDS`
- Папка журнальных файлов: `C:\Windows\NTDS`
- Папка SYSVOL: `C:\Windows\SYSVOL`

Существует множество сценариев, которые можно загрузить и применять для конфигурирования всех параметров. Ниже приведен полный список параметров на тот случай, если вам необходимо изменить конфигурацию:

```
Install-ADDSDomainController -DomainName <Строка> [-ADPrepCredential
<Учетные данные PowerShell>] [-AllowDomainControllerReinstall]
[-ApplicationPartitionsToReplicate <Строковый массив>]
[-CreateDnsDelegation] [-Credential <Учетные данные PowerShell>]
[-CriticalReplicationOnly] [-DatabasePath <Строка>]
[-DnsDelegationCredential <Учетные данные PowerShell>] [-Force]
[-InstallationMediaPath <Строка>] [-InstallDns] [-LogPath <Строка>]
[-MoveInfrastructureOperationMasterRoleIfNecessary] [-NoDnsOnNetwork]
[-NoGlobalCatalog] [-NoRebootOnCompletion] [-ReplicationSourceDC
<Строка>] [-SafeModeAdministratorPassword <Безопасная строка>]
[-SiteName <Строка>] [-SkipAutoConfigureDns] [-SkipPreChecks]
[-SystemKey <Безопасная строка>] [-SysvolPath <Строка>] [-Confirm]
[-WhatIf] [<Общие параметры>]
```

Теперь запустите командлет:

```
PS C:\Users\administrator> Install-ADDSDomainController
```

Будет выдан следующий запрос:

```
The target server will be configured as a domain controller and restarted
when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):Y
```

Целевой сервер будет сконфигурирован как контроллер домена и перезапущен после завершения этой операции.
Хотите ли вы продолжить данную операцию?
[Y] Да [A] Да для всех [N] Нет [L] Нет для всех [S] Приостановить [?] Справка (по умолчанию "Y"):Y

После выбора варианта `Yes` начнется процесс установки (рис. 3.20), который может занять несколько минут.

Рис. 3.20. Установка контроллера домена

Конфигурирование службы DHCP

После выхода ОС Windows Server 2003 разработчики из Microsoft начали кое в чем имитировать системы Linux. Они увеличили набор команд, чтобы снабдить поклонников систем Linux инструментами для конфигурирования максимально возможного числа аспектов. Именно тогда вошло в моду пользоваться командой `netsh`.

Упомянутая команда приходит на ум, когда речь идет об управлении службой DHCP. Документация по `netsh dhcp` доступна в TechNet. С ее помощью можно подготовить однострочные команды или воспользоваться интерактивной оболочкой, что и делается в рассматриваемом примере.

Офис филиала требует базовой реализации DHCP, с единственной областью видимости и стандартными опциями областей видимости шлюза, DNS-серверов и доменного имени DNS. Перед настройкой понадобится авторизовать службу в

Active Directory с применением опции add server. В следующем коде для ввода команд используется интерактивный режим:

```
netsh> dhcp
netsh dhcp>add server bfscl.bigfirm.com 192.168.1.11

Adding server bfscl.bigfirm.com, 192.168.1.11

Command completed successfully.
netsh dhcp>show server

1 Servers were found in the directory service:
В службе каталогов найден 1 сервер:

      Server [bfscl.bigfirm.com] Address [192.168.1.11] Ds location: c
n=bfscl.bigfirm.com


Command completed successfully.
```

Для добавления области видимости понадобится переключиться на командную строку netsh dhcp server и применить команду add scope. Обязательными параметрами являются подсеть и маска подсети, которые представляют эту область видимости, имя области видимости и любые комментарии:

```
netsh dhcp>server
netsh dhcp server>add scope 192.168.1.0 255.255.255.0 "Branch Office 1"
 "Sample DHCP scope"


Command completed successfully.
netsh dhcp server>show scope

 Scope Address - Subnet Mask    - State  - Scope Name     -  Comment

 192.168.1.0   - 255.255.255.0 -Active  -Branch Office 1 -Sample DHCP scope

 Total No. of Scopes = 1
Command completed successfully.
```

Для области видимости необходимо указать диапазон IP-адресов, чтобы она могла обслуживать клиентов DHCP, и стандартные опции области видимости. Опции области видимости задаются с помощью кодов опций в форме трехзначных идентификаторов. Такие идентификаторы можно видеть в консоли управления DHCP (DHCP Management Console). Опции имеют значения в форматах байта, слова, двойного слова, строки или IP-адреса. В нашем примере мы применяем следующие опции, идентификаторы и значения:

- Диапазон IP-адресов: 192.168.1.50 - 100
- Стандартный шлюз: 003, 192.168.1.254
- DNS-сервер: 006, 192.168.1.11
- Доменное имя DNS: 015, bigfirm.com

```
netsh dhcp server>scope 192.168.1.0

Changed the current scope context to 192.168.1.0 scope.
netsh dhcp server scope>add iprange 192.168.1.50 192.168.1.100
```

```
Command completed successfully.
netsh dhcp server scope>set optionvalue 003 IPADDRESS 192.168.1.254

Command completed successfully.
netsh dhcp server scope>set optionvalue 006 IPADDRESS 192.168.1.11

Command completed successfully.
netsh dhcp server scope>set optionvalue 015 STRING bigfirm.com

Command completed successfully.
netsh dhcp server scope>show optionvalue

Options for Scope 192.168.1.0:

      DHCP Standard Options :
      General Option Values:
      OptionId : 51
      Option Value:
            Number of Option Elements = 1
            Option Element Type = DWORD
            Option Element Value = 691200
      OptionId : 3
      Option Value:
            Number of Option Elements = 1
            Option Element Type = IPADDRESS
            Option Element Value = 192.168.1.254
      OptionId : 6
      Option Value:
            Number of Option Elements = 1
            Option Element Type = IPADDRESS
            Option Element Value = 192.168.1.11
      OptionId : 15
      Option Value:
            Number of Option Elements = 1
            Option Element Type = STRING
            Option Element Value = bigfirm.com
Command completed successfully.
```

После выполнения показанных выше команд на машине с Server Core можно также подключиться к службе из удаленного сервера и проверить конфигурацию через инструмент с графическим пользовательским интерфейсом.

Настройка файлового сервера

Служба роли файлового сервера, File Server, предоставляет базовые возможности совместного использования файлов. Для ее поддержки никаких специальных ролей или компонентов устанавливать не придется. Подобно многим другим ролям, процедуры по открытию совместного использования папок в полных установках обычно выполняются с помощью консоли MMC или других приложений с графическим пользовательским интерфейсом, таких как проводник Windows. Далее мы продемонстрируем альтернативный способ проведения этих процедур с применением командной строки.

Создание основного раздела

Первая задача заключается в предоставлении раздела данных. В следующем примере мы решили установить его размер в 10 Гбайт.

Для выполнения этой операции подходит команда DiskPart. Она реализует всю функциональность консоли управления дисками (Disk Management Console) в формате командной строки или интерактивной оболочки. Первый набор команд отображает сведения о дисках и томах на компьютере. Обратите внимание, что перечисленные тома включают тома на других дисках. Раздел данных пока еще не размещен, поэтому в списке томов он отсутствует. Для создания раздела данных понадобится выбрать диск, который обозначается значением в столбце Disk ### вывода команды list disk.

```
PS C:\Windows\system32>diskpart
Microsoft DiskPart version 6.1.7000
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: BFSC1
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online         75 GB    55 GB

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   GBlSXFRE_EN  UDF    CD-ROM      2850 MB  Healthy
  Volume 1                      NTFS   Partition    200 MB  Healthy    System
  Volume 2     C                NTFS   Partition     19 GB  Healthy    Boot
DISKPART> select disk 0
Disk 0 is now the selected disk.
```

Теперь мы создадим основной раздел. Для начала следует отобразить справочную информацию. Размеры разделов в выводе указываются в мегабайтах, и можно пользоваться примерной оценкой вида 10 Гбайт = 10 000 Мбайт. После того как основной раздел создан, его необходимо выбрать. Это позволит назначить ему букву диска:

```
DISKPART> help create partition primary
.....
Example:

   CREATE PARTITION PRIMARY SIZE=1000
rem size is in MB so 55 gb is 55000
DISKPART> create partition primary size=10000

DiskPart succeeded in creating the specified partition.

DISKPART> list partition

  Partition ###      Type              Size     Offset
  -------------      ----------------  -------  -------
  Partition 1        Primary           200 MB   1024 KB
  Partition 2        Primary            19 GB    201 MB
* Partition 3        Primary            10 GB     20 GB

DISKPART> select partition 3

Partition 3 is now the selected partition.

DISKPART> assign letter=e

DiskPart successfully assigned the drive letter or mount point.
```

Созданный раздел можно видеть как доступный том. Его нужно выбрать и сформатировать с файловой системой NTFS:

```
DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   GB1SXFRE_EN  UDF    CD-ROM      2850 MB  Healthy
  Volume 1                      NTFS   Partition    200 MB  Healthy    System
  Volume 2     C                NTFS   Partition     19 GB  Healthy    Boot
* Volume 3     E                RAW    Partition     10 GB  Healthy

DISKPART> select volume 3
Volume 3 is the selected volume.

DISKPART> format fs=ntfs label="Data volume" quick
  100 percent completed

DiskPart successfully formatted the volume.
```

Создание папок и редактирование разрешений

В этом примере будет создана папка `sales`. Для создания папки используется командлет PowerShell под названием `New-Item`: `NEW-ITEM E:\sales -type directory`. Затем необходимо привести в порядок настройки безопасности для папки `sales` — назначить группе `Administrators` (Администраторы) разрешение `Full Control` (Полный доступ).

Когда через свойства пользователя в консоли Active Directory Users and Computers (Пользователи и компьютеры Active Directory) выделяется домашняя папка, то она создается автоматически и пользователь получает для нее разрешение `Full Control`. К папке применимы унаследованные разрешения, поэтому стандартная группа `Users` (Пользователи) получает для нее разрешение `Read` (Чтение). Разрешения для группы `Users` при доступе к папке `sales` понадобится удалить.

Важность правильного написания

Для автоматического применения имен пользователей к путям домашних папок вы должны использовать системную переменную `%username%`. Таким образом, в консоли Active Directory Users and Computers путь домашней папки внутри свойств пользователя может выглядеть следующим образом: `\\bfsc1.bigfirm.com\users\%username%`. Внимательно относитесь к правильному написанию. Если ввести имя этой переменной некорректно, к домашней папке пользователя будет применена литеральная строка. Нередко нам приходилось встречать домашние папки с именами вроде `%usrename%` или `%usernam%`.

Как удостовериться в правильности написания? С помощью команды `echo`. Переменная `%username%` подобна другим системным переменным в том, что она действует также и в строке с приглашением на ввод команды. Команда `echo` выведет значение переменной, как показано ниже:

```
rem Имя записано правильно
C:\>echo %username%
Administrator

rem Имя записано неправильно
C:\>echo %uesername%
%uesername%
```

Получив подтверждение правильности написания, можете скопировать имя переменной в буфер обмена и впоследствии вставлять его в консоли Active Directory Users and Computers или внутри сценария.

Далее демонстрируется применение командлетов PowerShell, позволяющих модифицировать разрешения для папки sales. Первый командлет, Get-Acl, извлекает разрешения для папки. Свойство Format-List обеспечивает форматирование результатов в читабельном виде. Второй командлет, Set-Acl, используется для установки разрешений для папки.

```
rem Отображение разрешений для папки sales
Get-Acl E:\sales | Format-List
 Path : Microsoft.PowerShell.Core\FileSystem::C:\sales
Owner : BUILTIN\Administrators
Group : BFSC1\None
Access: NT AUTHORITY\SYSTEM Allow  FullControl
        BUILTIN\Administrators Allow  FullControl
        BUILTIN\Users Allow  ReadAndExecute, Synchronize
        BUILTIN\Users Allow  AppendData
        BUILTIN\Users Allow  CreateFiles
        CREATOR OWNER Allow  268435456
Audit :
Sddl  : O:BAG:S-1-5-21-4204471083-1189308523-3240350476-513D:
        AI(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIID;0x1200a9;
        ;;BU)(A;CIID;LC;;;BU)(A;CIID;DC;;;BU)(A;OICIIOID;GA;;;CO)
```

Ниже приведен удобный небольшой сценарий, который позволяет модифицировать групповые разрешения для папки. Он изменяет разрешения для папки sales так, чтобы только группа Administrators имела доступ Full Control:

```
$acl = Get-Acl "E:\Sales"
$Group1 = "Administrators"
$rule1 = New-Object System.Security.AccessControl.FileSystemAccessRule
-ArgumentList @($Group1,"FullControl","ContainerInherit,
ObjectInherit", "None","Allow")
$acl.SetAccessRule($rule1)
$acl |Set-Acl
$acl.SetAccessRuleProtection($true,$false)
$acl |Set-Acl
```

Далее показаны результаты выполнения этого сценария для папки sales. Как видите, теперь разрешение Full Control есть только у группы Administrators:

```
Path   : Microsoft.PowerShell.Core\FileSystem::E:\sales
Owner  : BUILTIN\Administrators
Group  : BFSC1\None
Access : BUILTIN\ Administrators Allow  FullControl
Audit  :
Sddl   : O:BAG:S-1-5-21-4204471083-1189308523-3240350476-513D:
         PAI(A;OICI;FA;;;BU)
```

Совместное использование папки

Совместное использование папок организуется исключительно просто с помощью команды net share. Действительно, это почтенная команда, появившаяся еще во времена LAN Manager. Приведенная ниже команда создает общий ресурс. Имя общего ресурса эквивалентно пути, за которым следуют разрешения.

Параметр /Unlimited задает количество подключений, разрешенных к этому общему ресурсу.

```
rem Создание общих ресурсов
E:\>net share SALES=e:\sales /grant:bigfirm\sales,FULL /Unlimited
Sales was shared successfully.
```

Разумеется, мы должны проверить общий ресурс. Возвратитесь к клиенту и введите путь UNC в окне Run (Выполнить); на рис. 3.21 показаны результаты.

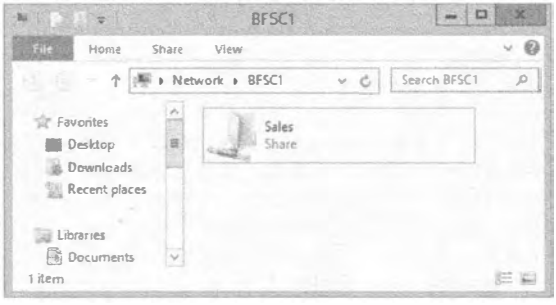


Рис. 3.21. Проверка общих ресурсов в Server Core

Настройка сервера печати

Службы e-Print требуют компонентов установленной роли Print and Document Services. Кроме того, как и другие роли, эту роль понадобится сконфигурировать. В предшествующих версиях Windows процесс добавления принтера управлялся мастером, при этом все компоненты были сведены в одну процедуру. В число таких компонентов входил выбор драйвера и порта, с возможностью создания конфигураций порта TCP и принтера. Функциональность существенно не изменилась, а лишь внешний вид, поэтому мы не будем особенно задерживаться на деталях.

Можно было бы предусмотреть команды для выполнения каждой процедуры в командной строке, но это стало бы своего рода пятым колесом в телеге. В среде Windows Server 2012 управление конфигурациями принтера производится в консоли Print Management (Управление печатью), которая является еще одной оснасткой MMC. Мы кратко рассмотрим этот подход, а затем предложим другой способ.

Администратор, ответственный за принтеры, должен установить консоль Print Management путем установки либо роли Print and Document Services (Службы печати и документов), либо только компонента Print and Document Services в Remote Server Administration Tools (Инструменты дистанционного администрирования серверов) на совместимой рабочей станции.

После установки консоли Print Management ее можно открыть и добавить экземпляр Server Core, как показано на рис. 3.22. Каждый компонент попадает в собственную объектную категорию, так что теперь вы располагаете мастером для каждой из них.

Для добавления драйвера необходимо щелкнуть правой кнопкой мыши на элементе Drivers (Драйверы) и выбрать в контекстном меню соответствующий пункт. Открывшийся мастер выглядит похожим на мастера из предыдущих версий ОС Windows.

Формы довольно стандартны, поэтому нет нужды возиться с ними, однако порты очень важны. Обычно офисные принтеры не подсоединены локально к серверу, а подключены к сети. Следовательно, придется создавать стандартный порт TCP. Опять-таки, это выглядит очень знакомо (рис. 3.23).

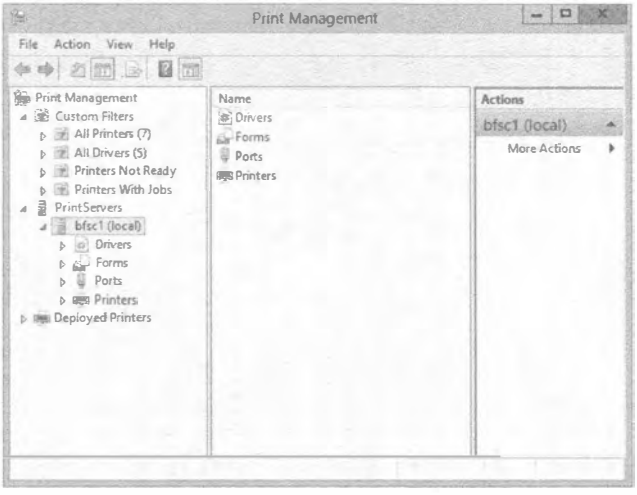


Рис. 3.22. Консоль Print Management, предназначенная для конфигурирования службы печати

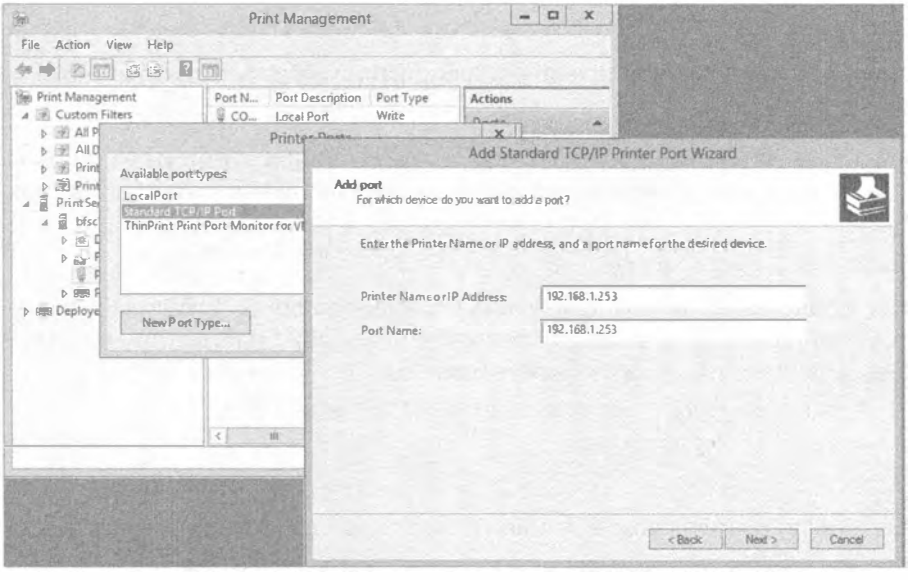


Рис. 3.23. Добавление порта TCP

Затем можно создать принтер со специфическим драйвером, портом, именем, общим именем, разрешениями и другими конфигурационными настройками, воспользовавшись мастером установки сетевого принтера (рис. 3.24).

Теперь давайте посмотрим, как конфигурировать принтер с применением командлетов PowerShell вместо старых методов сценариев в Server Core. При желании можно по-прежнему пользоваться сценариями `.vbs`, но, как упоминалось ранее, в Microsoft прикладывают большие усилия, чтобы сделать PowerShell основной средой администрирования в командной строке.

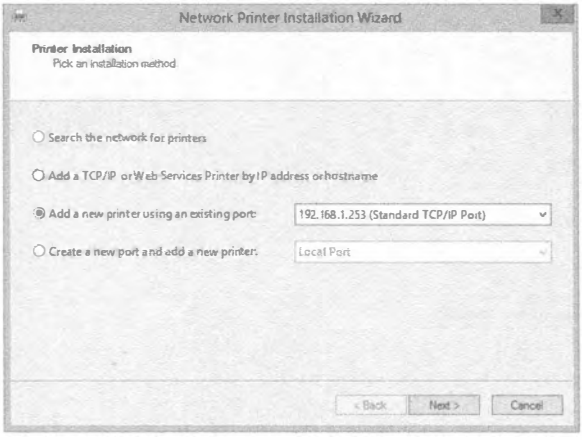


Рис. 3.24. Мастер установки сетевого принтера

Для добавления принтера предназначен командлет `Add-Printer`, который позволяет добавить как локальный, так и сетевой принтер. Ниже рассмотрены оба случая. Сначала добавим локальный принтер HP 5150 для отдела продаж (`Sales`):

```
PS C:\> Add-Printer -Name "Sales Printer" -DriverName "HP 5150"
```

А теперь добавим сетевой принтер к настроенному ранее серверу печати:

```
PS C:\> Add-Printer -ConnectionName \\bfsc1\192.168.1.253
```

Временами на сервере может отсутствовать драйвер принтера. Добавление драйвера принтера на сервер осуществляется с помощью следующего командлета PowerShell:

```
PS C:\> Add-PrinterDriver -Name "HP 5150"
```

После установки принтера необходимо сконфигурировать свойства печати, такие как цвет. Для начала имеет смысл просмотреть текущие настройки свойств, чтобы выяснить, какие из них должны быть изменены:

```
PS C:\> Get-PrintConfiguration -PrinterName " HP 5150"
PrinterName     ComputerName    Collate    Color      DuplexingMode
-----------     ------------    -------    -----      -------------
HP 5150                          True       True       OneSided
```

Имея конфигурацию, можно изменить значение свойства `Color` на `false`:

```
PS C:\> Set-PrintConfiguration -PrinterName "HP 5150" -Color $false
```

Управление лицензиями с помощью службы KMS

Компания Microsoft предложила в версиях Windows 8 и Windows Server 2012 новый процесс корпоративной активации Volume Activation 3.0. Он отличается от привычной онлайновой активации. Установленные копии, регулируемые корпоративной лицензией, подключаются к центральному серверу службы управления ключами (Key Management Service — KMS) внутри локальной сети, который будет регистрировать "лицензию" активации для клиента в Microsoft через Интернет. Это позволяет Microsoft контролировать количество активаций с одним и тем же корпоративным ключом продукта.

По умолчанию серверы Windows 8 и Windows Server 2012 сконфигурированы на подключение к серверу KMS, прежде чем предпринимать попытки онлайновой активации. Если сервер не может обнаружить в сети сервер KMS, но выполняет онлайновую активацию, то он действует в качестве сервера KMS. Данным процессом можно управлять.

При рассмотрении развертывания сервера KMS в рамках офиса филиала понадобится принять во внимание два ключевых аспекта. Первый — обеспечение возможности защищенного подключения по TCP/IP. Этот процесс всерьез облегчен, так что не требует медленных подключений к WAN; тем не менее, по-прежнему необходимо централизовать активации на одной площадке. Другой аспект касается того, что сервер KMS не начнет взаимодействовать с Microsoft до тех пор, пока не наберется 25 подходящих лицензий для активации. Это означает, что должно быть 25 установок Windows 8. Лицензия Windows Server 2012 учитывается как 5 установок Windows 8. Таким образом, одного сервера Windows Server 2012 и двадцати рабочих станций будет достаточно для запуска взаимодействия с Microsoft.

До запуска взаимодействия ОС на компьютерах работает на протяжении льготного периода, который без активации в конечном итоге завершится переходом в так называемый "режим сокращенной функциональности".

В офисе филиала, в котором имеется более 25 лицензий, но нет защищенного подключения по TCP/IP к головному офису, практическим вариантом является настройка сервера KMS. Если порог в 25 лицензий не удовлетворяет, то в Microsoft предлагают множественный ключ активации корпоративной лицензии (Volume License Multiple Activation Key — MAK), который работает подобно онлайновой активации ключей продуктов.

В последующих разделах описаны шаги по настройке сервера KMS на базе установки Server Core в офисе филиала.

Отключение публикации SRV в DNS

Записи SRV находятся в DNS и публикуют факт существования служб в сети. Более подробно они будут обсуждаться в главе 5. По умолчанию сервер KMS публикует службу посредством записи SRV в первичном домене DNS. В рассматриваемом примере Windows Server 2012 Server Core таким доменом является BigFirm.com.

В домене DNS по имени `BigFirm.com` вы увидите запись SRV для `_VLMCS._TCP.Bigfirm.com`. Она будет иметь следующие свойства:

- Имя: `_vlmcs._TCP`
- Тип: `SRV`
- Приоритет: `0`
- Вес: `0`
- Порт: `1688`
- Имя хоста: `Bfsc1.bigfirm.com`

Если вы хотите, чтобы это произошло, то должны добавить разрешения для зоны DNS, чтобы позволить обновления серверам KMS. Мы рекомендуем использовать в качестве сервера KMS контроллер домена, поскольку он уже обладает разрешениями для регистрации записей SRV в DNS.

Однако с помощью записей SRV отсутствует контроль над тем, на какой сервер KMS попадут клиенты, если они находятся в офисе филиала. Клиенты могут запросить DNS и получить ответ для сервера, который расположен где-то в другом месте. Для сохранения коммуникаций локальными сервер KMS должен быть зарегистрирован на стороне клиента. Кроме того, для сервера в офисе филиала публикация SRV в DNS должна быть отключена. Это делается путем создания параметра типа `dword` по имени `DisableDNSPublishing` со значением `1` внутри ключа `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL` реестра.

Включение брандмауэра

В конфигурации брандмауэра Windows уже присутствует одно входящее правило, которое является частью группы ролей Key Management Service. Его необходимо включить с помощью следующей команды:

```
netsh advfirewall firewall set rule group="Key Management Service"
      new enable=yes
```

Активация установки

Точно так же, как активировался экземпляр Server Core, сервер KMS офиса филиала должен быть активирован посредством опций `slmgr.vbs /ipk` и `/ato`.

Указание клиентам на сервер KMS

По умолчанию клиенты Volume Activation 3.0 (Windows 8 и Windows Server 2012) пытаются подключиться к серверу KMS автоматически с применением записей SRV. Поскольку этот процесс не учитывает площадку, может быть задействован любой предоставленный сервер KMS. С помощью следующей команды можно вручную назначить сервер KMS каждому клиенту внутри филиала:

```
cscript c:\windows\system32\slmgr.vbs /skms bfsc1.bigfirm.com:1688
```

Для распространения этого по всей площадке можно было бы воспользоваться объектом групповой политики.

Защита данных с помощью утилиты Windows Server Backup

Это один из компонентов, добавляемых к установке Server Core. Резервное копирование данных — всегда хорошая идея. В вашей среде могут пренебрегать использованием встроенных инструментов резервного копирования, отдавая предпочтение независимым решениям по резервному копированию уровня предприятия. Мы не порицаем такой подход. Тем не менее, между установкой и полноценным производством всегда существует момент, когда решение по резервному копированию уровня предприятия еще не установлено или не сконфигурировано. Мы обнаружили, что утилита NTBackup Utility великолепно подходит для резервного копирования жизненно важных данных.

Разработчики из Microsoft модернизировали встроенную утилиту резервного копирования и назвали ее Windows Server Backup (Резервное копирование Windows Server). Она взаимодействует со службой теневого копирования томов (Volume Shadow Copy Service) с целью фиксации состояния данных, предназначенных для резервной копии. Изначально эта утилита была спроектирована для предоставления только дистанционных копий на наборе переносимых жестких дисков. Копии на лентах были

устранены, так что съемные жесткие диски являлись единственным вариантом резервного копирования. К счастью, к моменту выпуска разработчики из Microsoft расширили приложение для включения путей UNC к общим папкам и локально подключаемым жестким дискам.

В этом обсуждении мы исследуем командлеты PowerShell, управляющие утилитой Windows Server Backup. Прежде всего, понадобится установить компонент Windows Server Backup. Ниже приведено его точное имя, а просмотреть полный список имен можно посредством командлета `Get-WindowsFeature`. Можно также получить список всех командлетов, ассоциированных с Windows Server Backup, запустив команду `get-command *wb* -commandtype cmdlet`.

```
PS  c:\Users\Administrator>Install-WindowsFeature Windows-Server-Backup
```

В случае успешной установки компонента вы увидите в PowerShell следующий вывод:

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Windows Server Backup}
```

Теперь необходимо создать новую политику резервного копирования. Политика резервного копирования представляет собой набор инструкций для автоматизации этого процесса. Сразу после создания политика по умолчанию пуста и должна вручную быть заполнена инструкциями. Такие инструкции включают планирование графика резервного копирования, а также установку целевого местоположения, файлов и ряда других параметров. Для установки политики применяется командлет `New-WBPolicy`:

```
PS  c:\Users\Administrator> New-WBPolicy

Schedule              :
BackupTargets         :
VolumesToBackup       :
FilesSpecsToBackup    :
FilesSpecsToExclude   :
ComponentsToBackup    :
BMR                   : False
SystemState           : False
OverwriteOldFormatVhd : False
VssBackupOptions      : VssCopyBackup
```

Просмотрев свойства `New-WBPolicy`, с помощью показанного ниже сценария их можно установить. Этот сценарий установит политику для выполнения резервного копирования содержимого папки `Sales` каждый день в 9:00.

```
PS C:\Users\Administrator> $policy = New-WBPolicy

$fileSpec = New-WBFileSpec -FileSpec C:\Sales
Add-WBFileSpec -Policy $policy -FileSpec $filespec

Add-WBBareMetalRecovery $policy

$disks = Get-WBDisk
$backupLocation = New-WBBackupTarget -Disk $disks[2]
Add-WBBackupTarget -Policy $policy -Target $backupLocation

Set-WBSchedule -Policy $policy 09:00

Set-WBPolicy -Policy $policy
```

Итак, вы узнали, как использовать PowerShell для работы с утилитой Windows Server Backup. Полный список командлетов для взаимодействия с Windows Server Backup приведен по адресу `http://technet.microsoft.com/en-us/library/ee706683.aspx`.

Резюме

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?

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 обших задач, которые модифицируют реестр. Как называется этот сценарий? Какой параметр может предоставить список дополнительных команд для выполнения многих общих задач конфигурирования?

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?

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?

Глава 4

Улучшения организации сетей в Windows Server 2012 R2

Когда компания Microsoft впервые выпустила Windows Server 2012, новые возможности организации сетей были, вероятно, наиболее рекламируемыми и с нетерпением ожидаемыми средствами этой ОС. С выходом Windows Server 2012 R2 в организацию сетей были внесены дальнейшие улучшения. В этой главе мы объясним, каким образом IPv6 и Windows PowerShell улучшают организацию сетей на базе Windows Server 2012 R2, и обсудим такую функциональность, как Network Interface Card (NIC) Teaming (Объединение сетевых интерфейсных плат) и расширенное качество обслуживания (Quality of Service — QoS). Некоторые знакомые средства организации сетей наподобие BranchCache и доступ, аутентифицированный с помощью протокола 802.1X, также были обновлены. Ближе к концу главы мы углубимся в исследования производительности сетей и управление ими для обеспечения максимальной эффективности сетевых развертываний.

В этой главе вы изучите следующие темы:

- протокол IPv6;
- использование PowerShell для лучшей управляемости сетями;
- реализация NIC Teaming;
- новые средства QoS;
- управление производительностью сетей.

Краткий экскурс в IPv6

Поскольку организация сетей в Windows Server 2012 построена на протоколе Интернета версии 6 (Internet Protocol version 6 — IPv6), полезно немного возвратиться назад в историческом смысле, чтобы исследовать разработку протокола управления

передачей (Transmission Control Protocol — TCP) и его доводку до современного состояния. Когда TCP был скомбинирован с первой публично доступной версией протокола Интернета (Internet Protocol — IPv4), мы получили протокол TCP/IP, который является основой всех современных сетей компьютеров. Свой первый стек протоколов TCP в Microsoft разработали в 1990-х годах. Он развивался вместе с выходом различных версий ОС от Microsoft, но в своей основе стек оставался по большей части неизменным вплоть до версии Windows Server 2003. В тот момент стало очевидным, что старый стек протоколов TCP/IP (версии 4) больше не мог развиваться и начал превращаться в узкое место. Разработчики в Microsoft увидели потребность в новом стеке, чтобы иметь возможность воспользоваться преимуществами новых технологий и перспективами, которые появились перед клиентами и партнерами. В результате они приступили к работе над новой версией TCP/IP, которая должна была включать комплект протоколов и стандартов, заново спроектированный инженерной группой по развитию Интернета (Internet Engineering Task Force — IETF) и называемый IPv6.

Переход на IPv6 начался в 1998 году, когда в Microsoft разработали ОС Windows 2000, а впервые мы столкнулись со стеком протоколов TCP/IP следующего поколения (интегрированный стек IPv4/IPv6 в многоуровневой архитектуре двойного IP) в версии Windows Vista. С тех пор все клиентские и серверные ОС производства Microsoft содержат в основе организации сетей тот же самый стек протоколов TCP следующего поколения и, естественно, ОС Windows Server 2012 не является исключением.

Преимущества IPv6

Переход на сети IPv6 сопровождается рядом преимуществ, если сравнивать с сетями IPv4, наиболее существенные из которых перечислены ниже.

- **Большой диапазон адресов.** С ростом потребления мобильных устройств, подключенных к Интернету, протокол IPv4 перестал справляться с потребностью во все большем объеме IP-адресов. Решение заключалось в создании протокола, который бы поддерживал триллионы IP-адресов, и вот именно тогда в игру вступил IPv6. Адреса IPv6 имеют длину 128 битов, что намного больше длины адресов IPv4, составляющей всего 32 бита. В IPv6 получить открытое адресное пространство очень легко, и внутри локальной сети закрытое адресное пространство, которое использует префиксы ULA (Unique Local Address — уникальный локальный адрес), может применяться к каждому сайту организации. Комбинация открытого адресного пространства и префиксов ULA позволяет масштабировать интрасети до гигантских размеров.
- **Эффективная подключаемость к Интернету.** Протокол IPv6 в Windows Server 2012 обнаруживает потенциальные проблемы маршрутизации между сетями IPv4 и IPv6 и может предотвращать начальную проблематичную попытку подключения. Эта характеристика, наряду с другими преимуществами, такими как заголовки IP-пакетов фиксированной длины и собранное вместе выделение адресов, с самого начала обеспечивает более эффективную подключаемость к Интернету.
- **Усиленная безопасность.** В IPv6 поддержка IPSec является требованием протокола; в IPv4 она была необязательной. Это требование предоставляет основанное на стандартах решение для нужд сетевой безопасности, способствует взаимодействию между различными реализациями IPv6 и применимо к устройствам, приложениям и службам.

- **Интегрированное качество обслуживания** (Quality of Service — QoS). Средство QoS позволяет измерять и регулировать уровни полосы пропускания, доступной сетевым интерфейсным платам (NIC). Оно присутствовало в операционных системах производства Microsoft на протяжении многих лет, но не применялось широко администраторами и профессионалами в области IT из-за наличия на рынке более удобных аппаратных решений. Средство QoS полностью интегрировано в Windows Server 2012 и работает за счет использования 20-битного поля Flow Label (Метка потока) и 8-битного поля Traffic Class (Класс трафика) в заголовке IPv6 для определения, с каким трафиком приходится иметь дело.

Технологии перехода на IPv6

Безусловно, переход с IPv4 на IPv6 не мог произойти в течение короткого периода времени, и проектировщикам IPv6 с самого начала было ясно, что оба протокола будут сосуществовать и работать вместе в рамках одной и той же инфраструктуры. Тем не менее, имелось одна проблема: протоколы IPv4 и IPv6 не могли естественным образом взаимодействовать друг с другом, поэтому на переходный период должно было быть разработано решение по преодолению коммуникационных барьеров между этими двумя протоколами. Был создан набор технологий перехода, так что узлы IPv6 могли взаимодействовать с любыми другими узлами в среде со смешанными протоколами, даже если они разделены инфраструктурой с одним лишь протоколом IPv4.

Первоначальные проектировщики IPv6 создали документ RFC (Request for Comment — Предлагается к обсуждению) 2893, "Transition Mechanisms for IPv6 Hosts and Routers" ("Механизмы перехода для хостов и маршрутизаторов IPv6"). В этом документе RFC определены различные типы узлов IPv4 и IPv6 в Интернете, объяснение которых дано в табл. 4.1.

Таблица 4.1. Определения типов узлов в RFC 2893

Тип узла	Описание
Узел только IPv4	Реализует только IPv4 (имеет только адреса IPv4) и не поддерживает IPv6. Этот тип узла весьма распространен в наши дни, и хорошими примерами могут служить Windows Server 2003 и Windows XP
Узел только IPv6	Реализует только IPv6 (имеет только адреса IPv6) и не поддерживает IPv4. Этот узел способен взаимодействовать только с узлами и приложениями IPv6. Такой тип узла встречается редко, поскольку он поддерживает только IPv6, но с обретением зрелости устройств с IPv6 он станет превалирующим
Узел IPv6/IPv4	Реализует как IPv6, так и IPv4 и в наши дни является самым распространенным типом узла в Интернете. Примерами могут быть Windows Server 2012, Windows Server 2008, Windows 8 и Windows 7
Узел IPv4	Узел, который реализует IPv4, но может быть также узлом только IPv4 или узлом IPv6/IPv4
Узел IPv6	Узел, который реализует IPv6, но может быть также узлом только IPv6 или узлом IPv6/IPv4

Организации могут переходить на IPv6, по-прежнему сохраняя функционирование бок о бок существующей инфраструктуры IPv4.

В документе RFC 2893 в общих чертах описаны разные сценарии, которые позволяют туннелировать трафик между инфраструктурами IPv6 и IPv4:

- маршрутизатор-маршрутизатор;
- хост-маршрутизатор или маршрутизатор-хост;
- хост-хост.

Протокол IPv6 для Windows Server 2012 поддерживает технологии автоматического туннелирования, которые перечислены ниже.

- **Туннелирование ISATAP (ISATAP Tunnelling).** Протокол автоматической внутрисайтовой адресации туннелей (Intra-Site Automatic Tunnel Addressing Protocol — ISATAP) предоставляет возможность подключения для хостов IPv6 по интрасети IPv4 с использованием упомянутых ранее сценариев хост-хост, хост-маршрутизатор и маршрутизатор-хост. Двумя главными компонентами для сети ISATAP являются маршрутизатор ISATAP и хосты ISATAP. В сети должна быть сконфигурирована запись DNS для маршрутизатора ISATAP, чтобы разрешить обнаружение этого маршрутизатора хостом ISATAP. После обнаружения маршрутизатор способствует взаимодействию IPv6 и IPv4, пересылая пакеты между сетями с двумя разными типами протокола.
- **Туннелирование 6to4 (6to4 Tunnelling).** Механизм 6to4 предоставляет назначение адресов и технологию автоматического туннелирования типа маршрутизатор-маршрутизатор, хост-маршрутизатор и маршрутизатор-хост. Для доставки пакетов IPv6 через инфраструктуру IPv4 он не нуждается в явных туннелях. Располагая 6to4, нет необходимости в запрашивании внешнего адреса IPv6 у поставщика Интернет-услуг, поскольку можно просто назначать внешние (глобальные) адреса IPv6 внутри сети, которые позволят взаимодействовать с местоположениями во внешнем Интернете с IPv6.
- **Туннелирование Teredo (Teredo Tunneling).** С помощью Teredo можно выполнять назначение адресов и автоматическое туннелирование типа хост-хост даже через устройства NAT (network address translation — преобразование сетевых адресов), таких как домашние маршрутизаторы. Устройства подобного рода не имеют встроенной возможности прямого подключения к сети IPv6. Протокол Teredo был спроектирован как последнее средство перехода на подключаемость IPv6. Он не будет применяться при наличии подключаемости IPv6, ISATAP или 6to4 между взаимодействующими узлами. По мере того, как поддержка 6to4 становится более преобладающей среди пограничных устройств IPv4, а подключаемость IPv6 превращается в норму, Teredo будет использоваться все реже и реже, а потом и вовсе исчезнет.

Дополнительные сведения об архитектуре IPv6 приведены в руководстве по безотказной работе IPv6:

```
http://social.technet.microsoft.com/wiki/contents/articles/
  1728.ipv6-survival-guide.aspx
```

При желании можете также почитать исходный документ RFC 2893:

```
http://www.ietf.org/rfc/rfc2893.txt
```

Улучшенная управляемость сетями с помощью PowerShell

Инструмент Windows PowerShell первоначально был представлен как встроенный компонент ОС в Windows Server 2008. Он применялся многими приложениями Microsoft, такими как Exchange Server, SQL Server, SharePoint и System Center, для открытия доступа к их интерфейсам управления и переноса администрирования и автоматизации задач на новый качественный уровень. В ОС Windows Server 2012 R2 встроена версия инструмента PowerShell 4.0, сопровождаемая обширным набором команд Windows PowerShell, обычно называемых командлетами, которые предназначены для конфигурирования настроек IPv6 и других связанных с сетью параметров в командной строке и на основе сценариев.

Исторически сложилось так, что для управления IPv6 использовалась утилита командной строки `Netsh.exe` (Network Shell), но хотя команды `Netsh.exe` для конфигурирования IPv6 по-прежнему поддерживаются, в настоящее время при управлении конфигурациями сетей Windows Server 2012 R2 рекомендуется применять Windows PowerShell. В этом разделе будет показано, как задействовать PowerShell, чтобы получить максимальную отдачу от функциональности сети.

Командлеты и модули для работы с сетью

В то время как в Windows Server 2008 было приблизительно 200 командлетов PowerShell, в Windows Server 2012 R2 их доступно почти 2 500! Из этого громадного пула новых командлетов буквально сотни можно использовать для просмотра, конфигурирования и мониторинга всех сетевых компонентов и служб, предлагаемых Windows Server 2012. С помощью этих командлетов можно выполнять широкий диапазон задач, начиная с простой настройки IP-адресов и заканчивая более специализированными функциями вроде конфигурирования параметров качества обслуживания (Quality of Service) и виртуализации сетей. Изучение PowerShell является ключом к управлению и автоматизации серверов в центре данных, а также к упрощению организации сетей на основе Windows Server 2012.

Командлеты PowerShell сгруппированы в наборы связанных функций, которые называются модулями. Из-за большого количества командлетов, доступных для работы с сетями Windows Server 2012, и невозможности раскрытия их всех в одной главе в табл. 4.2 описаны важные модули PowerShell, имеющие отношение к организации сетей, и предоставлены ссылки на справочники по содержащимся в этих модулях командлетам.

Таблица 4.2. Модули для работы с сетями

Модуль	Описание модуля	Ссылка на справочник по командлетам
`BrancheCache`	Средство BranchCache	`http://tinyurl.com/branchecache`
`NetAdapter`	Сетевой адаптер	`http://tinyurl.com/ws2012netadapter`
`NetConnection`	Состояние подключаемости к сети	`http://tinyurl.com/ws2012netconnectivity`
`NetLBFO`	Объединение сетевых интерфейсных плат (NIC Teaming)	`http://tinyurl.com/ws2012nicteaming`

Окончание табл. 4.2

Модуль	Описание модуля	Ссылка на справочник по командлетам
NetQos	QoS	http://tinyurl.com/ws2012qos
NetSecurity	Безопасность сети	http://tinyurl.com/ws2012netsecurity
NetSwitchTeam	Объединение сетевых коммутаторов (Network Switch Team)	http://tinyurl.com/ws2012netswitchteam
NetTCPIP	TCP/IP	http://tinyurl.com/ws2012nettcpip
NetworkTransition	Сетевой переход (Network Transition)	http://tinyurl.com/ws2012nettransition
NetWNV	Виртуализация сетей Windows (Windows Network Virtualization)	http://tinyurl.com/ws2012netwnv

Новая утилита пингования?

Еще один действительно замечательный и, безусловно, полезный командлет, доступный в Windows Server 2012 R2, называется `Test-NetConnection`. Этот командлет является серьезным претендентом на замену старой, но очень широко применяемой команды `ping`. Если командлет `Test-NetConnection` запустить без параметров, он попытается автоматически распознать внешний адрес Microsoft (`internetbeacon.msedge.net`) и возвратит такую информацию, как удаленный IP-адрес, Интернет-псевдоним и PingReplyDetails (Round Trip Time (RTT) — время между отправкой запроса и получением ответа в миллисекундах). Это может сэкономить время, когда нужно проверить возможность подключения к Интернету того или иного сервера, например.

Запуск данного командлета с параметром `-ComputerName` позволяет указать имя определенного компьютера, который требуется проверить:

```
Test-NetConnection - ComputerName Host2
```

В результате получается следующий вывод:

```
PS C:\Windows\system32> test-netconnection -computername Host2
ComputerName : Host2
RemoteAddress : 192.168.0.200
InterfaceAlias : Ethernet
SourceAddress : 192.168.0.100
PingSucceeded : True
PingReplyDetails (RTT) : 0 ms
```

Microsoft NIC Teaming

Назначение NIC Teaming заключается в объединении двух и более сетевых адаптеров для создания одного логического адаптера с целью обеспечения отказоустойчивости или агрегирования полосы пропускания для сетевых подключений. Каждый адаптер, являющийся членом объединения NIC, поддерживает собственное отдельное физическое существование и подключен к отдельному сетевому кабелю.

В ранних выпусках Windows Server возможность NIC Teaming была доступна только через программные решения третьих сторон, таких как HP, Intel и Dell, а также требовала специальных сетевых адаптеров. При наличии проблем с подключением к сети на сервере, на котором сконфигурировано средство NIC Teaming, и обращении в службу поддержки Microsoft за консультацией по устранению проблемы вам бы посоветовали связаться непосредственно с третьей стороной, поскольку средство NIC Teaming находиться вне зоны ответственности Microsoft. Однако в Windows Server 2012 R2 возможность NIC Teaming является встроенной в ОС и не зависит от поставщика, оборудования и скорости линии. В этом разделе будут продемонстрированы преимущества NIC Teaming в Windows Server 2012 R2 и показано, насколько легко создать и управлять объединением NIC в вашей среде.

Преимущества NIC Teaming в Windows Server 2012 R2

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, известного также под названием балансировка нагрузки и обход отказов (load balancing and failover — LBFO). Это сводит на нет необходимость в приобретении какого-либо дополнительного (и потенциально дорогого) оборудования или программного обеспечения. Благодаря NIC Teaming, множество сетевых адаптеров работают вместе как единое логическое подключение, гарантируя обеспечение подключаемости даже в случае отказа одного сетевого адаптера. Это средство предлагает сценарий, при котором сервер может допускать отказ сетевого адаптера и порта до первого сегмента коммутатора.

Средство NIC Teaming можно также применять для агрегирования полосы пропускания из множества сетевых адаптеров, чтобы добиться лучшей и более быстрой пропускной способности. Например, если на вашем сервере установлены три адаптера 1 Гбит/с, и вы решили создать объединение NIC, включающее их все, то получите в итоге агрегат с пропускной способностью 3 Гбит/с.

Другие преимущества средства NIC Teaming заключаются в том, что оно предлагает общий набор инструментов управления для всех типов сетевых адаптеров, устраняет потенциальные проблемы, возникающие из-за патентованных решений, и, разумеется, полностью поддерживается Microsoft.

Конфигурации объединений NIC

При развертывании NIC Teaming в Windows Server 2012 R2 можно делать выбор из трех базовых режимов объединения.

- **Статическое объединение (Static).** Известный также как зависящий от коммутатора, этот тип конфигурации требует, чтобы коммутатор был о нем осведомлен и принимал участие в NIC Teaming. Поскольку объединение NIC зависит от коммутатора, понадобится обеспечить, чтобы все члены объединения NIC были подключены к одному и тому же физическому коммутатору, а не распределялись по множеству разных коммутаторов (рис. 4.1).

- **Объединение, не зависящее от коммутатора (Switch Independent).** Конфигурация объединения, не зависящего от коммутатора, не требует участия коммутатора в объединении. Здесь коммутатору ничего не известно о том, что сетевой адаптер является частью объединения на хосте, поэтому адаптеры могут быть подключены к разным коммутаторам, чтобы обеспечивать базовую отказоустойчивость также и на уровне коммутатора. Эта конфигурация объединения будет работать с любыми коммутаторами, включая неинтеллектуальные и не осведомленные об объединении, т.к. все логические возможности, требуемые для поддержки NIC Teaming, поддерживаются внутри Windows Server 2012. Пример объединения, не зависящего от коммутатора, приведен на рис. 4.2.
- **LACP.** Подобно статическому объединению, режим LACP (Link Aggregation Control Protocol — протокол управления агрегированием каналов) требует предварительного конфигурирования коммутаторов с целью включения LACP. После включения данный режим можно использовать для автоматического объединения множества NIC в один логический канал в любое время, когда коммутатор реконфигурирован. Это устраняет накладные расходы, связанные с администрированием, и упрощает работу администратора сети.

Рис. 4.1. Объединение, зависящее от коммутатора

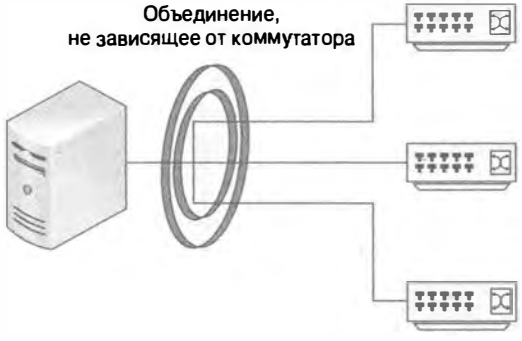


Рис. 4.2. Объединение, не зависящее от коммутатора

После выбора режима объединения необходимо определиться с балансировкой нагрузки, чтобы указать, каким образом трафик обрабатывается после того, как он проходит через объединение NIC. В Windows Server 2012 R2 можно работать со следующими тремя режимами балансировки нагрузки.

- **Хеширование адресов (Address Hash).** Когда пакеты получаются объединением в этом режиме, они сначала инспектируются, после чего алгоритм хеширования обрабатывает целевую информацию — обычно номер порта, IP-адрес и MAC-адрес. По результатам работы алгоритма объединение NIC затем определяет, какой физический сетевой адаптер будет применяться для отправки пакета.
- **Порт Hyper-V (Hyper-V Port).** Данный режим можно развертывать при конфигурировании объединения NIC для использования с ролью Hyper-V (отсюда и название). Это не является предварительным условием для конфигурирования виртуальных сетей, но когда применяется Hyper-V, такой режим обладает рядом преимуществ по сравнению с хешированием адресов. Например, он может быть более предсказуемым при отправке пакетов через NIC, которые используются для Hyper-V, особенно если объединение подключено к внешнему виртуальному коммутатору.
- **Динамический (Dynamic).** Это новый режим балансировки нагрузки, который появился в версии Windows Server 2012 R2. Он лучше двух других режимов. Входящий и исходяший трафик может быть равномерно распределен по членам объединения NIC посредством концепции под названием *флоулеты* (flowlet), которые по существу разбивают крупный поток на небольшие порции для обеспечения оптимальной передачи данных.

В зависимости от того, планируете вы создавать объединение NIC на физическом или же на виртуальном сервере, необходимо принять во внимание несколько требований и ограничений.

- **Объединение NIC на физическом сервере.** ОС Windows Server 2012 R2 поддерживает до 32 сетевых адаптеров в объединении, которое было создано на физическом сервере. Для создания объединения должен быть в наличии, по крайне мере, один сетевой адаптер: объединение с одним NIC могло бы применяться для разделения трафика VLAN, но для обеспечения отказоустойчивости рекомендуется использовать минимум два NIC.
- **Объединение NIC внутри виртуальной машины.** Если вы решили развернуть NIC Teaming внутри виртуальной машины, то при формировании объединения будете ограничены применением только двух членов NIC. Причина сводится к возможности поддержки со стороны Microsoft и не обязательно означает, что вы не сможете создавать более крупные объединения NIC для демонстрационных или тестовых целей.
- **Поддерживаемые типы NIC.** Для объединения NIC может использоваться практически любой сетевой адаптер Ethernet при условии прохождения им циклического теста пригодности оборудования для ОС Windows (Windows Hardware Qualification Loop test). Однако перечисленные ниже типы NIC *не* поддерживаются:
  - WLAN
  - Bluetooth
  - WWAN
  - Infiniband

- **Смешивание NIC с разными скоростями.** Если вы создаете объединение NIC в целях балансировки нагрузки и улучшения пропускной способности (как противоположность целям обхода отказов), то должны гарантировать, что все сетевые адаптеры в объединении NIC обладают одинаковой скоростью подключения (например, все имеют скорость 1 Гбит/с). Смешивание NIC с разными скоростями, когда одни имеют скорость, скажем, 1 Гбит/с, а другие — 100 Мбит/с, в объединении не поддерживается и приводит к нежелательным результатам, если вы все же решите развернуть объединение подобным образом.

Онлайновые ресурсы по NIC Teaming

При желании изучить средство NIC Teaming в Windows Server 2012 более глубоко выделите время на чтение следующей великолепной серии статей в блоге Эйдена Финна, обладателя звания MVP по Hyper-V из Ирландии:

```
http://www.aidanfinn.com/?p=13984
```

Полезно также просмотреть видеозапись заседания "What's New in Windows Server 2012 R2 Networking" ("Что нового в организации сетей Windows Server 2012 R2"), которая проходило на конференции TechEd North America 2013, организованной Microsoft:

```
http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/MDC-B216
```

Конфигурирование объединения NIC

Создание и управление объединением NIC в Windows Server 2012 R2 осуществляется действительно просто. Создать объединение можно либо путем нескольких щелчков кнопками мыши прямо в графическом пользовательском интерфейсе, либо для достижения той же цели воспользоваться командлетами PowerShell. В этом разделе будут рассмотрены оба сценария. Для конфигурирования объединения NIC с применением графического пользовательского интерфейса выполните описанные ниже шаги.

1. Войдите на свою машину Windows Server 2012 с помощью учетной записи, имеющей полномочия администратора, и откройте диспетчер серверов (Server Manager).
2. Щелкните на элементе Local Server (Локальный сервер) слева и отобразится панель свойств, где видно, что средство NIC Teaming в текущий момент отключено (Disabled), как показано на рис. 4.3.

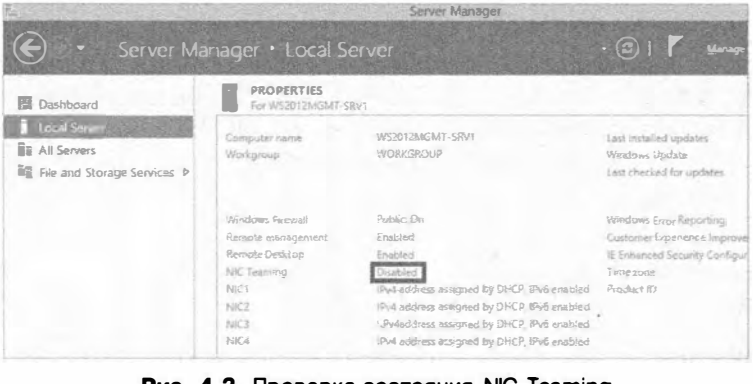


Рис. 4.3. Проверка состояния NIC Teaming

3. Щелкните на ссылке Disabled (Отключено) рядом с NIC Teaming, чтобы открыть диалоговое окно NIC Teaming (рис. 4.4).

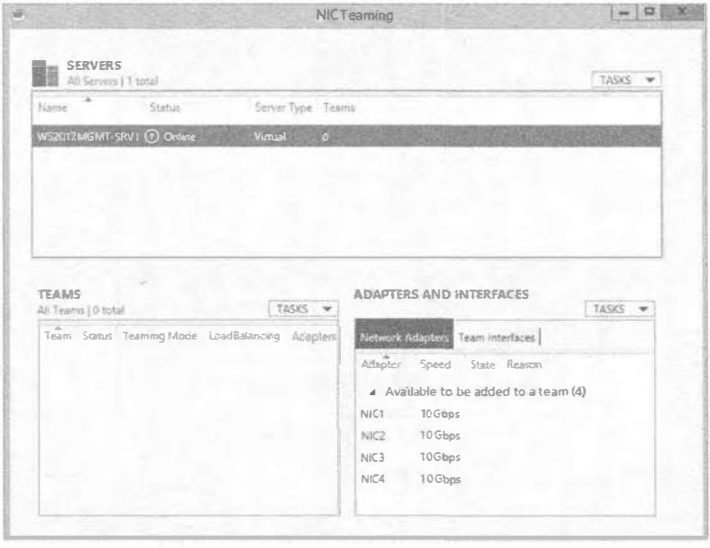


Рис. 4.4. Диалоговое окно NIC Teaming

4. В разделе Adapters and Interfaces (Адаптеры и интерфейсы) диалогового окна NIC Teaming, щелкните на адаптерах, для которых необходимо создать объединение, удерживая нажатой клавишу <Ctrl>.
5. Щелкните правой кнопкой мыши на выделенных адаптерах и выберите в контекстном меню пункт Add to New Team (Добавить в новое объединение), как показано на рис. 4.5.

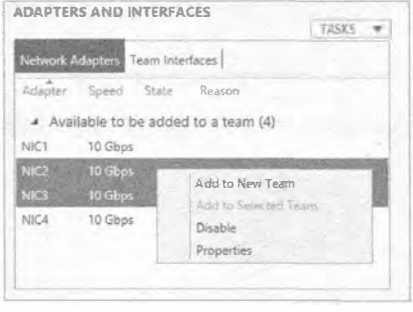


Рис. 4.5. Добавление адаптеров в объединение

6. Когда откроется диалоговое окно New Team (Новое объединение), введите в поле Team Name (Имя объединения) имя нового объединения и удостоверьтесь, что все сетевые адаптеры, которые нужно добавить, выбраны в разделе Member Adapters (Адаптеры-члены).

   На рис. 4.6 видно, что путем развертывания опции Additional Properties (Дополнительные свойства) можно сконфигурировать режимы объединения и балансировки нагрузки (в списках Teaming mode и Load balancing mode соответственно).

Рис. 4.6. Диалоговое окно New Team

7. Выберите адаптер, который будет сконфигурирован в качестве резервного (если применимо), и выберите основной интерфейс объединения с членством VLAN (если применимо).
8. Щелкните на кнопке OK, чтобы создать новое объединение NIC.

   По прошествии нескольких секунд вы увидите, что объединение было создано и добавлено в раздел Teams (Объединения) диалогового окна NIC Teaming (рис. 4.7).

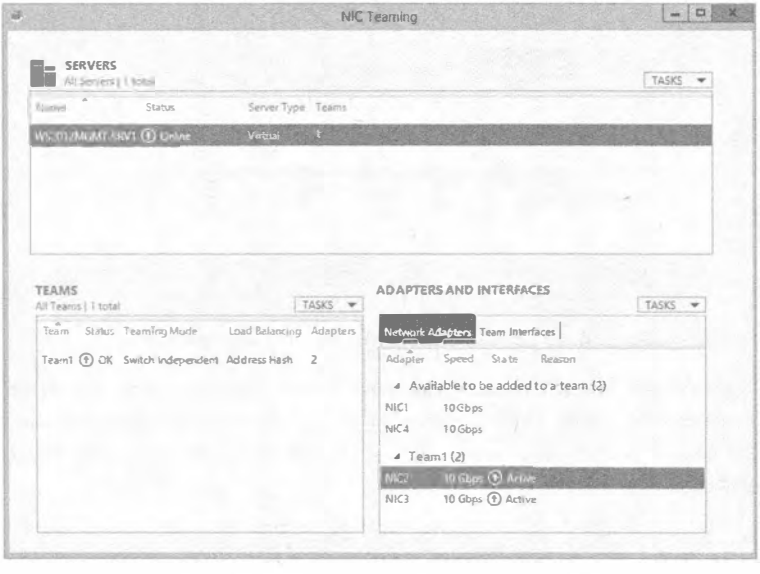


Рис. 4.7. Созданное объединение NIC

Если вы откроете элемент Network Connections (Сетевые подключения) панели управления, то увидите, что был создан новый объект объединения NIC, а при проверке его состояния заметите, что он скомпоновал скорость всех сетевых адаптеров, входящих в объединение. В примере на рис. 4.8 видна скорость 20 Гбит/с, т.к. в объединение было добавлено два виртуальных сетевых адаптера.

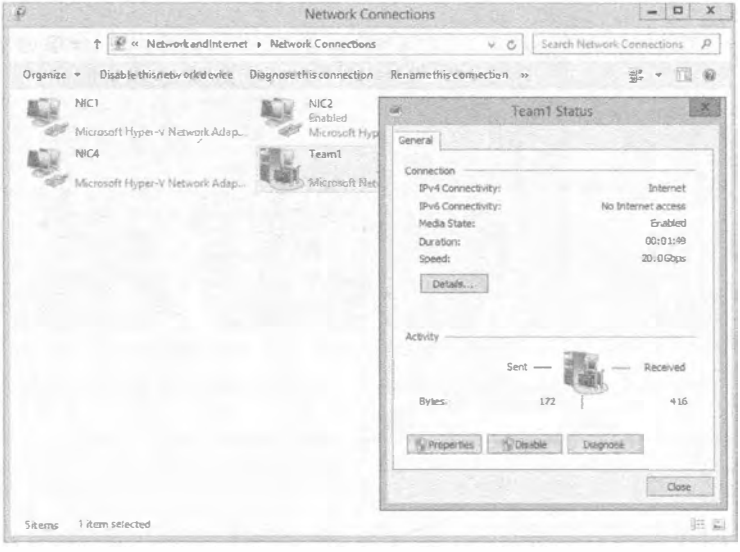


Рис. 4.8. Состояние объединения NIC

Объединение NIC на виртуальных машинах

Если вы решили развернуть NIC Teaming внутри виртуальных машин Hyper-V, то знайте, что, во-первых, в качестве членов объединения NIC можно использовать только синтетические NIC, но не унаследованные. Синтетические NIC являются стандартной конфигурацией для виртуальной машины в Hyper-V. Во-вторых, обработка отказа в объединении NIC внутри виртуальной машины может привести к отправке трафика по неправильному MAC-адресу, и это может радикально повлиять на балансировку нагрузки. Чтобы смягчить данную проблему, вы должны убедиться, что каждый порт коммутатора Hyper-V в хосте Hyper-V, который ассоциирован с виртуальной машиной, использующей NIC Teaming, сконфигурирован на разрешение объединения. Для этого запустите на каждом хосте следующую команду PowerShell, предварительно войдя в систему с полномочиями администратора:

```
Set-VMNetworkAdapter -VMName <Имя виртуальной машины> -AllowTeaming On
```

Если необходима возможность создавать объединение NIC с применением PowerShell, выполните перечисленные ниже шаги (объединение NIC конфигурируется таким же образом, как это делалось ранее с использованием графического пользовательского интерфейса).

1. Откройте окно PowerShell с учетной записью, имеющей административные полномочия, и введите следующую команду (имена объединения и сетевых адаптеров должны соответствовать применяемым в вашей среде):

```
New-NetLbfoTeam Team1 NIC3,NIC4
```

2. Введите Y для согласия и нажмите <Enter>, чтобы подтвердить выполнение действия.

На рис. 4.9 видно, что с помощью PowerShell было создано новое объединение NIC.

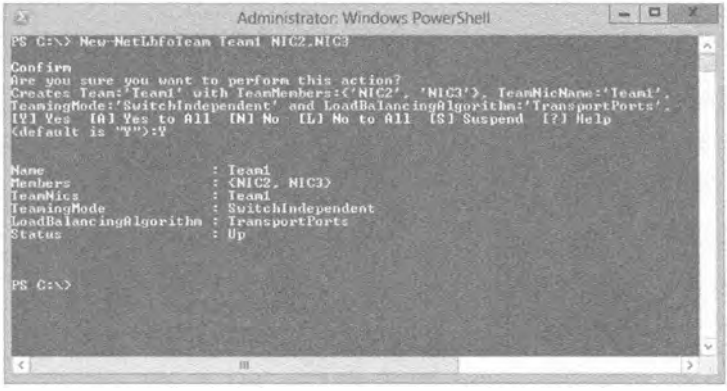


Рис. 4.9. Создание объединения NIC посредством PowerShell

Пример из практики

Не смешивайте разные решения по объединению

Дилан был администратором Windows Server 2012, работающим в группе внутренней поддержки в многопользовательском центре данных с общим хостингом. Он отвечал за поддержку сетевой подключаемости и безотказной работы кластерной среды Windows Server 2012, используемой потребителями.

Когда Дилан создавал первоначальный кластер, он сконфигурировал функцию NIC Teaming, встроенную в Windows Server 2012, и ему очень нравилась обеспечиваемая ею производительность и агрегирование каналов. Однако пока Дилан был в отпуске, один из его коллег из группы поддержки решил применить исправления и провести общее обслуживание во внерабочее время. К сожалению, коллега не был хорошо знаком с новым средством NIC Teaming в Windows Server 2012 и не понял, что оно уже сконфигурировано в кластере. В результате он развернул решение NIC Teaming от третьей стороны поверх существующей функции и сделал один из сетевых адаптеров, являющихся членами Microsoft NIC Teaming, частью объединения NIC третьей стороны. В итоге, вернувшись из отпуска, Дилан обнаружил в кластере два решения NIC Teaming, совместно использующие те же самые сетевые адаптеры.

По прошествии нескольких дней кластер начал постоянно терять подключаемость к сети, и его работа становилась неустойчивой. Когда Дилан приступил к выяснению источника проблемы, он быстро понял, что в кластере оказалось два разных решения NIC Teaming. Во время исследований он нашел на сайте поддержки Microsoft Windows Server 2012 TechNet статью со следующей рекомендацией.

"Системным администраторам настоятельно рекомендуется никогда не запускать два решения по объединению одновременно на одном сервере. Решениям по объединению ничего не известно о существовании друг друга, и это в результате приводит к возникновению серьезных проблем.

В случае если администратор нарушил данные руководящие принципы и попал в ситуацию, описанную выше, проблему можно решить с помощью перечисленных ниже шагов.

1. Перезагрузите сервер. При необходимости принудительно отключите питание, чтобы заставить сервер перезагрузиться.
2. После перезагрузки запустите следующий командлет Windows PowerShell:

```
Get-NetLbfoTeam | Remove-NetLbfoTeam
```

3. Воспользуйтесь инструментами администрирования из решения по объединению от третьей стороны и удалите все экземпляры ранее созданных объединений.
4. Снова перезагрузите сервер.

Компания Microsoft продолжает свою многолетнюю политику по не поддержанию решений объединения от третьих сторон. Если пользователь решил запустить какое-то решение объединения от третьей стороны, а затем обнаружил проблемы с сетью, он должен обратиться за поддержкой к поставщику решения. Если проблема повторяется уже без решения от третьей стороны, пользователь должен сообщить о ней в Microsoft".

После того как Дилан выполнил шаги, приведенные в этой статье TechNet, удалив решение NIC Teaming от третьей стороны и воссоздав объединение NIC из Windows Server 2012, кластер снова стал функционировать нормально.

Расширенное качество обслуживания

Качество обслуживания (Quality of Service — QoS) было компонентом операционных систем Microsoft на протяжении многих лет, и оно позволяло администраторам конфигурировать и развертывать политики, которые заранее определяли, какие приложения или службы должны иметь приоритет при выделении полосы пропускания. Другими словами, трафик для одних сетевых приложений будет передаваться до или после трафика для других приложений. 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.

Даже притом, что QoS доставляется через ОС Windows, сетевые устройства (такие как адаптеры, коммутаторы, маршрутизаторы и шлюзы), которые ответственны за коммуникации между хостами, также должны быть осведомлены о QoS. Любые устройства, не осведомленные о QoS, которые обрабатывают трафик, назначенный QoS, будут иметь дело с трафиком на базе в лучшем случае "первый пришел, первый обслужен", в той же самой манере, что и стандартные сетевые коммуникации.

QoS внутри виртуальных машин

Включать QoS в ОС Windows Server 2012, когда она функционирует как гостевая виртуальная машина внутри виртуализированной среды, не рекомендуется. Средство QoS предназначено для управления трафиком в физических, а не виртуальных сетях, и должно конфигурироваться в управляющей ОС на физическом хост-сервере с развернутой ролью Hyper-V.

Средство Minimum Bandwidth

В ранних операционных системах QoS можно было использовать только для соблюдения максимума по потреблению полосы пропускания, что также известно как ограничение скорости, и не было возможности указать минимальную полосу пропускания. Вместо системы резервирования полосы пропускания это было больше похоже на решение по регулировке полосы пропускания. При попытке достичь правильной политики управления полосой пропускания QoS в средах виртуальных центров данных такое решение становилось крупной проблемой, в результате чего оно не подходило хорошо для предприятий, которые быстро выбирали решения облачного хостинга.

Для решения описанной проблемы к QoS в Windows Server 2012 было добавлено 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.

Если вы хотите изучить передовой опыт Microsoft по развертыванию QoS Minimum Bandwidth, то по следующей ссылке доступно соответствующее руководство: `http://tinyurl.com/ws2012qosmb`.

> **Рекомендуемые скорости адаптеров для Minimum Bandwidth**
>
> В Microsoft определили, что средство Minimum Bandwidth лучше всего работает с сетевыми адаптерами Ethernet со скоростью либо 1 Гбит/с, либо 10 Гбит/с. Адаптеры с меньшими скоростями для QoS не подходят.

Средство Data Center Bridging

Мостовое соединение центров данных (Data Center Bridging — DCB) — это поддерживаемое средство в Windows Server 2012, которое предоставляет гарантированную полосу пропускания различным типам сетевого трафика в конвергированной сетевой инфраструктуре или конвергированной фабрике. Конвергированный трафик имеет разные смешанные классы, такие как высокоскоростная сеть SAN, VoIP и традиционная локальная сеть (LAN) — обычно желательно всех их удерживать изолированными друг от друга. Средство DCB освобождает центральный процессор (ЦП) от вычислений и соблюдения политики QoS и переносит их в сетевой адаптер. По этой причине, если вы хотите применять в своей среде средство DCB, удостоверьтесь, что установленные сетевые адаптеры и коммутаторы поддерживают функциональность DCB.

В качестве примера можно рассмотреть преимущества с точки зрения поставщика облачного хостинга. В случае реализации DCB это особенно помогло бы сократить сложность за счет разрешения всему трафику проходить по той же самой аппаратной инфраструктуре как по конвергированной единственной подсети с изолированными сегментами, тем самым устраняя требование по наличию специального изолированного оборудования, которое обычно необходимо для разделения трафика хранилища и трафика локальной сети.

Управление DCB

Управление DCB должно осуществляться через WMI (Windows Management Instrumentation — инструментарий управления Windows) и PowerShell после того, как средство Data Center Bridging было включено на серверах Windows Server 2012. Ниже описана процедура включения DCB из графического пользовательского интерфейса.

1. Войдите на машину с Windows Server 2012, используя учетную запись с полномочиями администратора, и откройте диспетчер серверов.
2. В диалоговом окне Configure This Local Server (Конфигурировать этот локальный сервер) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты) и затем щелкните на кнопке Next (Далее) на экране Before You Begin (Прежде чем начать) мастера добавления ролей и компонентов (Add Roles and Features Wizard).
3. Выберите 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) мастера выберите переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов).
5. Удостоверьтесь, что ваш сервер выбран в разделе Server Pool (Пул серверов) и для продолжения щелкните на кнопке Next.
6. На экране Select Server Roles (Выбор серверных ролей) мастера просто щелкните на кнопке Next, чтобы продолжить.
7. На экране Select features (Выбор компонентов) мастера отметьте флажок рядом с Data Center Bridging (Мостовое соединение центров данных), как показано на рис. 4.10, и щелкните на кнопке Next.

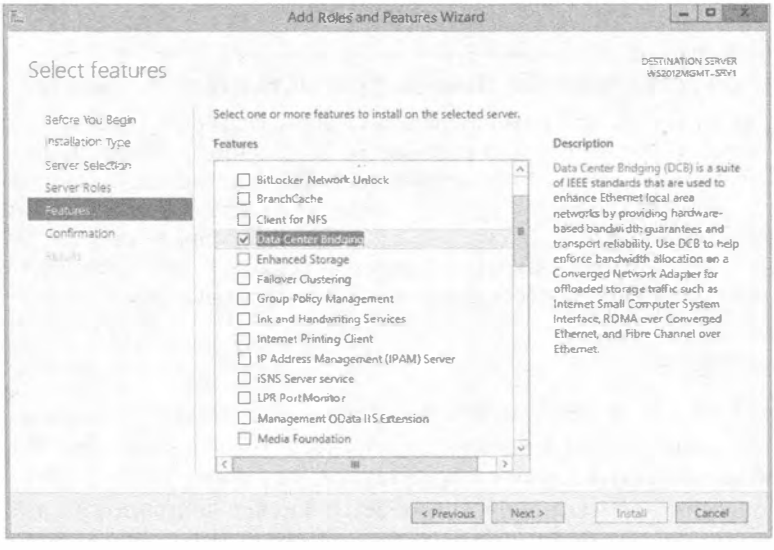


Рис. 4.10. Включение средства Data Center Bridging

8. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) мастера щелкните на кнопке Install (Установить), чтобы установить и включить DCB.

После того, как средство DCB включено, им можно управлять с помощью командлетов PowerShell, перечисленных в табл. 4.3.

Таблица 4.3. Командлеты PowerShell для управления DCB

Командлет	Описание
`Get-NetQosFlowControl`	Получает параметры управления потоком на основе приоритетов (priority-based flow control — PFC)
`Set-NetQosFlowControl`	Устанавливает параметры управления потоком
`Enable-NetQosFlowControl`	Включает управление потоком уровня канала на основе приоритета IEEE 802.1p
`Disable-NetQosFlowControl`	Отключает управление потоком уровня канала на основе приоритета IEEE 802.1p
`Get-NetQosDcbxSetting`	Получает параметры обмена мостового соединения центров данных (data center bridging exchange — DCBX)
`Set-NetQosDcbxSetting`	Устанавливает параметры DCBX
`Get-NetQosTrafficClass`	Получает параметры класса трафика
`New-NetQosTrafficClass`	Создает новый класс трафика
`Set-NetQosTrafficClass`	Устанавливает параметры класса трафика
`Remove-NetQosTrafficClass`	Удаляет класс трафика

Для дальнейшего изучения темы, связанной с управлением DCB посредством PowerShell, обратитесь к руководству пользователя по написанию сценариев на Windows PowerShell для DCB ("DCB Windows PowerShell User Scripting Guide"): `http://tinyurl.com/ws2012dcb`.

Могут ли средства Minimum Bandwidth и DCB работать вместе?

Несмотря на то что средства Minimum Bandwidth и DCB обладают одинаковой функциональностью, обеспечивая справедливое выделение рабочей нагрузке полосы пропускания, когда случается перегруженность сети, он не предназначены для совместной работы. Важно отметить, что вы никогда не должны включать одновременно Minimum Bandwidth и DCB для рабочих нагрузок, которые совместно используют один и тот же сетевой стек или сетевой адаптер, поскольку это приведет к серьезным проблемам с пропускной способностью и производительностью в сети.

Hyper-V QoS

Средство QoS для Hyper-V может быть исключительно полезным для организаций, предлагающих услуги многопользовательского облачного хостинга, которые обязаны соблюдать соглашения по уровню обслуживания (service-level agreement — SLA) в отношении полосы пропускания сети. За счет использования Hyper-V QoS такие организации могут обеспечить гладкое проведение регулировки и сегментации сетевого трафика.

В Microsoft определяют следующие возможности для Hyper-V QoS.

- Принудительное применение минимальной и максимальной полосы пропускания для потока трафика, который идентифицируется номером порта виртуального коммутатора Hyper-V.
- Конфигурирование минимальной и максимальной полосы пропускания для каждого порта виртуального коммутатора Hyper-V с использованием либо командлетов PowerShell, либо Windows Management Instrumentation.
- Настройка множества виртуальных сетевых адаптеров в Hyper-V и указание QoS для каждого из них на индивидуальной основе.

Средство Hyper-V QoS может получить преимущество от оборудования, поддерживающего DCB, чтобы свести множество типов рабочих нагрузок сетевого трафика Hyper-V (таких как живой перенос, общий кластерный том и трафик хранилища) в единственный сетевой адаптер с соглашением SLA по гарантированной полосе пропускания, назначенным каждому типу. В результате станет возможным более эффективное использование дорогих высокоскоростных сетевых адаптеров, подобных Ethernet в 10 Гбит/с.

QoS на основе политики

С помощью групповой политики (Group Policy) можно определить QoS приложения с применением следующих настроек:

- отправляющее приложение и путь к каталогу;
- целевой и исходный IP-адреса и порты;
- протокол — либо TCP, либо UDP;
- пользователи и группы Active Directory.

Все вместе эти настройки будут определять значение DSCP (Differentiated Services Code Point — точка кода дифференцированных услуг). Протокол TCP использует это для внедрения значения от 0 до 63 в поле TOS (Type of Service — тип службы) внутри пакета TCP IPv4. Обратите внимание, что он также внедряет значение в поле Traffic Class (Класс трафика) внутри пакета IPv6. Маршрутизаторы в сети затем будут использовать значение DSCP для определения, какие пакеты имеют приоритет. Чем более высокое значение DSCP, назначенное администратором через групповую политику, тем большее число маршрутизаторов будут отдавать предпочтение связанным с этим значением пакетам.

Средство QoS на основе политик можно настраивать либо посредством групповой политики, либо с помощью конфигураций групповой политики домена Active Directory, и политика QoS может быть создана на уровне компьютера, на уровне пользователей или на обоих уровнях, если это необходимо. Однако в общем случае рекомендуется применять политику QoS на уровне компьютера, поскольку это гарантирует, что независимо от того, какие пользователи входят на устройство, все они получат ту же самую конфигурацию QoS. На рис. 4.11 показан контейнер Policy-based QoS (QoS на основе политики) внутри представления Computer Configuration (Конфигурация компьютера) в Local Computer Policy (Политика локального компьютера).

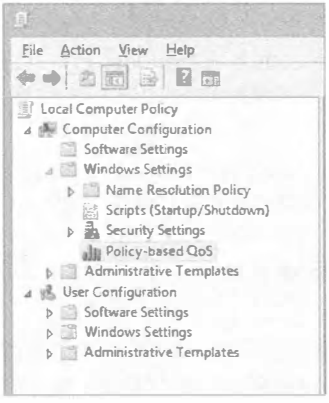


Рис. 4.11. Контейнер Policy-based QoS в редакторе групповой политики

Давайте рассмотрим пример. Администратору необходимо назначить приоритет приложению LOB, когда с ним работает персонал, занимающийся продажами, и начальники отделов. Известно, что приложение функционирует на TCP-порте 3299, а в Active Directory имеются группы пользователей для отдела продаж и начальников отделов. Вы можете построить групповую политику, нацеленную на TCP-порт 3299 и на упомянутые выше группы пользователей, тем временем назначив приложению значение DSCP выше нормального, составляющего 60. Это значение будет внедряться во все пакеты на TCP-порту 3299, которые ассоциированы с указанными пользователями и группами пользователей. Затем сетевые маршрутизаторы запросят это значение из пакетов IPv4 или IPv6 и отдадут им предпочтение, как и было проинструктировано.

Ниже перечислены предварительные условия для QoS на основе политики.

- На управляемых компьютерах должна функционировать ОС Windows Server 2012, Windows Server 2008 R2/R1, Windows 8, Windows 7 или Windows Vista.
- Они должны быть членами домена Active Directory, поэтому политики можно развертывать с использованием Group Policy.
- Маршрутизаторы, которые располагаются между клиентами и серверами, должны быть способны конфигурироваться для DSCP (см. документ RFC 2474 по ссылке `http://tinyurl.com/nb852k`).

Обязательно проверьте удовлетворение каждого предварительного условия, прежде чем начинать развертывание QoS. Вы же не хотите считать, что имеете контроль над всем, используя только QoS, а потом обнаружить, что QoS на самом деле ничего не делает! Сетевые маршрутизаторы являются предварительным условием, которое может доставить наибольшие проблемы. Они могут потребовать значительных затрат и, возможно, вызвать определенные трудности, если вы поручили работу по развертыванию WAN независимому подрядчику. Развертывание QoS потребует тщательного планирования и исследований с вашей стороны. Каждая организация будет иметь отличающиеся нужды, и при проектировании своего решения вам понадобится тесно взаимодействовать с руководством и персоналом.

Доступ, аутентифицированный с помощью протокола 802.1X

Протокол аутентификации 802.1X определен ассоциацией стандартов института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers (IEEE) Standards Association) и предоставляет дополнительный уровень безопасности для устройств, которые необходимо подключать к средам проводных (LAN) и беспроводных (WLAN) локальных сетей. Он оперирует на уровне порта сетевого адаптера и может применяться для обеспечения того, чтобы запретить доступ в интрасеть любым нежелательным компьютерам, которые не смогли пройти аутентификацию.

Хотя протокол 802.1X существовал много лет и получал разные уровни поддержки от Microsoft, начиная с Windows 2000, в Windows Server 2012 появилась новая функциональность, которая не была доступна в ранних выпусках ОС. Шагом вперед стала туннелированная защита транспортного уровня в расширяемом протоколе аутентификации (Extensible Authentication Protocol (EAP) Tunneled Transport Layer Security (TTLS)), по-другому называемая EAP-TTLS.

EAP-TTLS — это по существу основанный на стандартах метод туннелирования, который поддерживает взаимную аутентификацию. Он включает безопасность аутентификации клиентов за счет предоставления защищенного туннеля с использованием комбинации методов EAP, унаследованных баз данных аутентификации и унаследованных механизмов паролей. Дополнительные сведения о проводной и беспроводной аутентификации 802.1X доступны по ссылкам `http://tinyurl.com/8021wired` и `http://tinyurl.com/8021wireless`.

Усовершенствованное средство BranchCache

Встроенное в Windows Server 2012 R2 средство BranchCache существует на протяжении некоторого времени и делает возможной оптимизацию WAN для организаций, имеющих удаленные офисы филиалов. Когда компьютеры в офисе филиала запрашивают содержимое из головного офиса или центра данных, BranchCache сохраняет это содержимое в локальной (запрашивающей) сети, либо на выделенном сервере, либо на назначенных клиентских рабочих станциях. В результате доступ к файлам и папкам становится быстрее и одновременно уменьшается потребление полосы пропускания. Так как дистанционное содержимое кешируется в локальной сети, при последующих его запросах другие клиенты будут получать к нему доступ непосредственно в локальной сети, а не через WAN.

Средство BranchCache может быть сконфигурировано в двух разных режимах.

- **Режим распределенного кеша (Distributed Cache).** Когда средство BranchCache настроено в этом режиме, нет необходимости иметь какие-либо серверные компьютеры в офисах филиалов. Вместо этого данные, запрошенные и загруженные из головного офиса клиентскими компьютерами, которые расположены в офисе филиала, кешируются на них локально. В следующий раз, когда другие клиентские компьютеры из этого офиса филиала запросят то же самое содержимое, они просто получат доступ к нему через кеш на исходных клиентских компьютерах.
- **Режим размещенного кеша (Hosted Cache).** В этом режиме серверные компьютеры должны быть расположены в офисах филиалов. Эти компьютеры действуют в качестве локальных серверов содержимого, и когда клиентские компьютеры офиса филиала запрашивают и загружают данных из головного офиса, такие серверы содержимого извлекают и кешируют данные до тех пор, пока в них нуждаются другие клиентские компьютеры в том же офисе филиала.

Хотя средство BranchCache было доступно в предшествующих версиях Windows Server, в Windows Server 2012 оно было значительно усовершенствовано.

- **Глубокая интеграция с файловым сервером Windows.** Используя новую функциональность дедупликации данных из Windows Server 2012 для индексации со-

держимого, BranchCache может гарантировать оптимальную экономию полосы пропускания. Средство дедупликации данных Windows Server 2012 более подробно обсуждается в главе 12.

- **Обработка дублированного содержимого.** При наличии дублированного содержимого внутри одиночного файла или даже среди нескольких файлов средство BranchCache будет сохранять только один экземпляр такого содержимого, обеспечивая большую экономию полосы пропускания и дискового пространства.
- **Отсутствие ограничений на размеры офисов и количество офисов филиалов.** Когда средство BranchCache развернуто в режиме Hosted Cache, нет никаких ограничений на количество офисов филиалов, которые можно иметь в качестве части своего решения BranchCache.
- **Упрощенное развертывание с помощью Active Directory.** Независимо от размера организации, внутри которой развертывается средство BranchCache, его конфигурация управляется через единственный объект групповой политики Active Directory (Active Directory Group Policy object (GPO)), что упрощает задачу управления для бригады, отвечающей за инфраструктуру.
- **Автоматическое конфигурирование клиентских компьютеров.** Объект Active Directory Group Policy может также применяться для конфигурирования клиентских компьютеров в качестве клиентов с режимом Distributed Cache по умолчанию. Если клиенты сконфигурированы подобным образом, и они обнаруживают наличие сервера размещенного кеша, то они автоматически сконфигурируют себя как клиенты с режимом Hosted Cache.
- **Более высокая производительность благодаря автономному созданию содержимого.** Если средство BranchCache было включено на серверах, то вычисления, необходимые для сбора информации содержимого, выполняются в автономном режиме до того, как любой из клиентских компьютеров в действительности запросит эти данные. В результате улучшается производительность и экономится полоса пропускания.
- **Зашифрованные данные кеша.** По умолчанию все кешированные данные теперь хранятся в зашифрованном виде, обеспечивая постоянную защиту и целостность данных.
- **Управление с помощью PowerShell и WMI.** При управлении средами серверов и клиентов BranchCache теперь можно использовать сценарии PowerShell и WMI.

Если вы решили развернуть BranchCache в режиме Hosted Cache с Windows Server 2012 R2, то сможете получить преимущества от следующих усовершенствований.

- **Более одного сервера размещенного кеша на местоположение.** Ранее можно было развертывать только один сервер размещенного кеша в каждом местоположении офиса в рамках организации. Благодаря Windows Server 2012 (или выше) в режиме Hosted Cache, появляется возможность развернуть в каждом местоположении сразу несколько серверов размещенного кеша, что способствует более высокой масштабируемости.

- **Улучшенная технология баз данных.** Теперь базы данных BranchCache обслуживаются технологией баз данных Extensible Storage Engine (ESE), что обеспечивает намного лучшую производительность и функциональность хранения, чем в предшествующих версиях. Это та же самая технология, которая является движущей силой Microsoft Exchange Server, и она представляет собой проверенное расширение уровня предприятия.

Управление производительностью сети

Понимание методов управления производительностью сетевой среды имеет первостепенное значение для обеспечения оптимального уровня продуктивности организации. В этом разделе обсуждается ряд средств и инструментов, которые могут помочь в достижении указанной цели. В главе 30 (том 2) более подробно рассматривается мониторинг производительности.

Когда мы говорим о том, что производительности сети хороша или плоха, то обычно в конечном результате присутствует, по крайней мере, одна из метрик, описанных в табл. 4.4.

Таблица 4.4. Метрики производительности

Метрика	Описание
Задержка	Время, требуемое на завершение операции. Чем меньше, тем лучше
Масштабируемость	Возможность приспосабливаться к растущим требованиям в системных ресурсах. Чем больше, тем лучше
Пропускная способность	Объем данных, передаваемых или обрабатываемых в заданный промежуток времени. Чем больше, тем лучше
Длина пути	Количество циклов ЦП, деленное на пропускную способность. Чем меньше, тем лучше
Вариабельность задержки	Колебания пропускной способности и/или задержки. Чем меньше, тем лучше

Если вы хотите добиться максимальной производительности своих сетей, управляя указанными метриками производительности, то должны понимать и уметь задействовать некоторые из перечисленных ниже средств Windows Server 2012 R2.

- **Объединение полученных сегментов.** Если ваши серверы постоянно получают высокую рабочую нагрузку, вы можете воспользоваться в своих интересах объединением полученных сегментов (Receive Segment Coalescing — RSC), чтобы убрать накладные расходы из сервера и перенести их в сетевые адаптеры, совместимые с RSC. Средство RSC работает путем комбинирования мелких пакетов из потоков данных в один крупный пакет с целью увеличения производительности.
- **Зарегистрированные расширения API ввода-вывода.** Зарегистрированные расширения API ввода-вывода (Registered I/O — RIO) ориентированы главным образом на разработчиков приложений, которые нуждаются в отправке и получении данных с микросекундной детализацией. Средство RIO делает возможным выполнение операций отправки и получения с применением заранее зарегистрированных буферов, использующих очереди для запросов и заверше-

ний. Низкая задержка достигается RIO за счет закрепления памяти приложения и, таким образом, сокращения расходов со стороны ЦП.

- **Масштабирование на стороне приема.** Масштабирование на стороне приема (Receive-Side Scaling — RSS) хорошо работает с веб-серверами и файловыми серверами, и может применяться для распределения принимаемого сетевого трафика по множеству процессоров, так что пакеты, принадлежащие одному подключению TCP, обрабатываются на том же самом логическом процессоре. Скорости сетевых адаптеров возросли (наиболее превалирует в наши дни скорость 10 Гбит/с), поэтому у ЦП будет достаточный объем для обработки. Если не реализовывать RSS для серверов с очень высокой рабочей нагрузкой из сети, возникает риск исчерпать возможности ЦП и в конечном итоге придется приобретать новое оборудование. Конечно, чтобы можно было использовать RSS, понадобится иметь на серверах сетевые адаптеры, поддерживающие RSS.

Анализ производительности и инструменты

Если вы хотите провести анализ производительности сети, то хорошей отправной точкой будет инструмент `Perfmon.exe`, который поставляется как часть ОС Windows Server 2012 R2, и позволяет исследовать данные, сгенерированные счетчиками производительности, которые имеют отношение к сети (табл. 4.5).

Таблица 4.5. Счетчики производительности, имеющие отношение к сети

Объект	Что анализирует	Счетчик
IPv4, IPv6	Потребление ресурсов	Datagrams Received/sec (Дейтаграмм получено/с) Datagrams Sent/sec (Дейтаграмм отправлено/с)
TCPv4, TCPv6	Потребление ресурсов	Segments Received/sec (Сегментов получено/с) Segments Sent/sec (Сегментов отправлено/с) Segments Retransmitted/sec (Сегментов передано/с)
Network Interface Network Adapter (Сетевой адаптер сетевого интерфейса)	Потребление ресурсов	Bytes Received/sec (Байтов получено/с) Bytes Sent/sec (Байтов отправлено/с) Packets Received/sec (Пакетов получено/с) Packets Sent/sec (Пакетов отправлено/с) Output Queue Length (Длина выходной очереди)
Processor Information (Информация о процессоре)	Потребление ресурсов	% Processor Time (% процессорного времени) Interrupts/sec (Прерываний/с) DPCs Queued/sec (Отложенных вызовов процедур поставлено в очередь/с)
Network Interface Network Adapter (Сетевой адаптер сетевого интерфейса)	Потенциальные проблемы с сетью	Packets Received Discarded (Отброшено полученных пакетов) Packets Received Errors (Ошибок в полученных пакетах) Packets Outbound Discarded (Отброшено исходящих пакетов) Packets Outbound Errors (Ошибок в исходящих пакетах)

Окончание табл. 4.5

Объект	Что анализирует	Счетчик
WFPv4, WFPv6	Потенциальные проблемы с сетью	Packets Discarded/sec (Отброшено пакетов/с)
UDPv4, UDPv6	Потенциальные проблемы с сетью	Datagrams Received Errors (Ошибок в полученных дейтаграммах)
TCPv4, TCPv6	Потенциальные проблемы с сетью	Connections Failures (Отказов при подключениях) Connections Reset (Сбросов подключений)
Network QoS Policy (Политика QoS сети)	Потенциальные проблемы с сетью	Packets Dropped (Отброшенных пакетов)
Per Processor Network Interface Card Activity (Активность сетевой интерфейсной платы на процессор)	Потенциальные проблемы с сетью	Low Resource Received Indications/sec (Индикаций нехватки ресурсов/с) Low Resource Received Packets/sec (Пакетов нехватки ресурсов/с)
Microsoft Winsock BSP	Потенциальные проблемы с сетью	Dropped Datagrams (Отброшенных дейтаграмм) Dropped Datagrams/sec (Отброшенных дейтаграмм/с) Rejected Connections (Отклоненных подключений) Rejected Connections/sec (Отклоненных подключений/с)
Network Adapter (Сетевой адаптер)	RSC performance	TCP Active RSC Connections (Активных подключений TCP RSC) TCP RSC Average Packet Size (Средний размер пакета TCP RSC) TCP RSC Coalesced Packets/sec (Объединенных пакетов TCP RSC/с) TCP RSC Exceptions/sec (Исключений TCP RSC/с)

Инструмент Server Performance Advisor

Если вы ищете что-то более глубокое, чем `Perfmon.exe`, то должны взглянуть на инструмент, который называется советником по производительности сервера от Microsoft (Microsoft Server Performance Advisor — SPA); его версия 3.0 доступна для загрузки по ссылке `http://tinyurl.com/ws2012spa` (вам понадобится Windows Live ID). Целью это инструмента является помощь системным администраторам в оценке и решении проблем с производительностью серверов.

Инструмент SPA предоставляет отчеты и рекомендации для системных администраторов о распространенных проблемах с конфигурацией и производительностью. Он собирает данные, связанные с производительностью, из различных источников на серверах, таких как счетчики производительности, ключи реестров, запросы WMI, конфигурационные файлы и трассировка событий для Windows (Event Tracing for Windows — ETW). На основе собранных данных по производительности сервера SPA может обеспечить глубокий взгляд на текущую ситуацию с производительностью и выдать рекомендации относительно ее улучшения.

Версия SPA 3.0 разработана для запуска на сервере с Windows Server 2012 и главным образом ориентирована на системных администраторов, управляющих не более чем 100 серверами с различными серверными ролями. Она также будет применяться инженерами по поддержке для сбора данных по производительности и для решения проблем с производительностью у пользователей.

Ограничение масштабирования SPA 3.0

Инструмент Server Performance Advisor 3.0 не очень хорошо масштабируется при попытке управлять производительностью для более чем 100 серверов. Если вы управляете средами больших размеров, то должны рассмотреть возможность использования в качестве инструмента для мониторинга и управления диспетчера операций системного центра (System Center 2012 R2 Operations Manager).

Установка SPA 3.0

Прежде чем приступить к установке инструмента SPA 3.0, проверьте, удовлетворены ли следующие предварительные условия:

- наличие .NET Framework 4
- наличие SQL Server 2008 R2 Express

После удовлетворения всех условий выполните описанные ниже шаги, чтобы развернуть, сконфигурировать и запустить генерацию отчетов в SPA 3.0 на сервере Windows Server 2012.

1. Загрузите файл `SPAPlus_amd64.cab` и извлеките его содержимое в подходящем месте на своем жестком диске.

   Для распаковки файла `.cab` советуем воспользоваться инструментом вроде WinRAR (`rarlab.com`) или WinZip (`winzip.com`). Согласно нашему опыту, применение встроенного проводника Windows для распаковки таких файлов не обеспечивает создание корректной структуры папок и препятствует нормальной работе SPA 3.0.

2. В том месте, где вы распаковали файлы, найдите файл приложения `SpaConsole.exe`, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Run as administrator (Запуск от имени администратора), как показано на рис. 4.12.

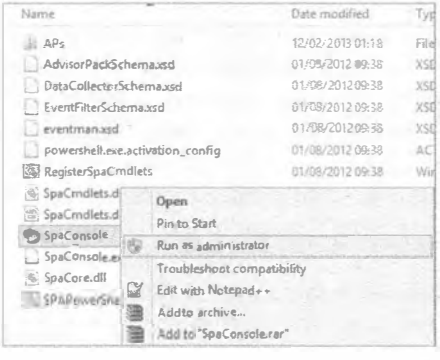


Рис. 4.12. Конфигурирование консоли SPA

3. Прочитайте и примите условия лицензионного соглашения на экране Server Performance Advisor License Agreement (Лицензионное соглашение по использованию SPA) мастера настройки и щелкните на кнопке Next (Далее).
4. В окне консоли Server Performance Advisor (Советник по производительности сервера) выберите в меню File (Файл) пункт New Project (Новый проект), как показано на рис. 4.13.

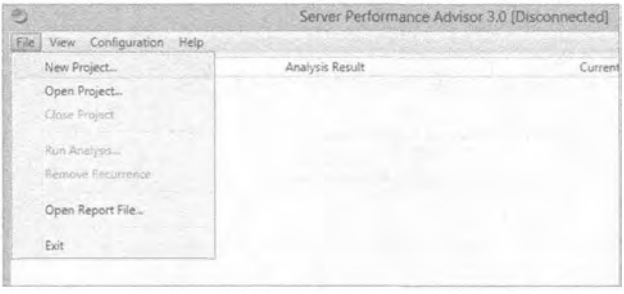


Рис. 4.13. Создание нового проекта

5. На начальном экране мастера нового проекта (New Project Wizard) щелкните на кнопке Next.
6. На экране Create Project Database (Создание базы данных проекта) введите имя экземпляра SQL Server и укажите имя базы данных SQL, которую нужно назначить проекту SPA. Щелкните на кнопке Next.
7. На экране Add Servers (Добавление серверов) введите имена серверов, которыми необходимо управлять с помощью SPA.
8. Укажите общий сетевой ресурс, который будет применяться для хранения отчетов, и щелкните на кнопке Finish (Готово), чтобы завершить настройку проекта (рис. 4.14).

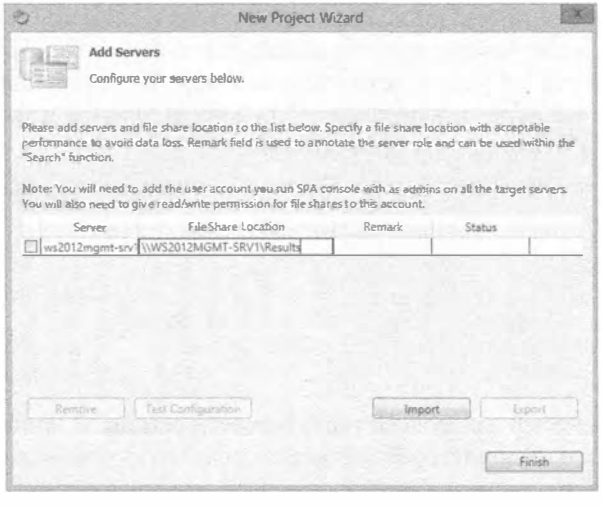


Рис. 4.14. Конфигурирование сервера и общего сетевого ресурса

9. В окне консоли Server Performance Advisor отметьте флажок рядом с именем сервера и выберите в меню File (Файл) пункт Run Analysis (Запустить анализ), чтобы запустить генерацию отчета.
10. Выберите пакеты советника, значимые для системы, для которой строился отчет, например, Core OS, Hyper-V или IIS, и щелкните на кнопке OK два раза подряд.
11. После завершения анализа можете просмотреть содержимое отчета с помощью инструмента Report Viewer (Просмотр отчетов), как показано на рис. 4.15.

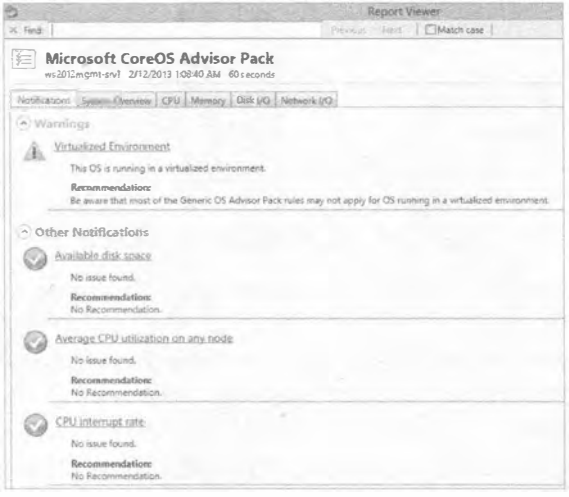


Рис. 4.15. Просмотр отчета

Резюме

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

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`?

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?

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?

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`

Глава 5

Компоненты IP Address Management и DHCP Failover

По мере усложнения сетевых сред и становления дополнительных сетевых протоколов, таких как IPv6, более привычными, возрастает важность наличия возможности централизованного управления и обеспечения высокой доступности конфигураций IP-адресов. Для удовлетворения этих требований в Windows Server 2012 предусмотрены дополнительные компоненты — IP Address Management (Управление IP-адресами), или IPAM, и DHCP Failover (Обработка отказа DHCP). Указанные компоненты работают с существующими развертываниями DNS и DHCP, помогая отслеживать и сокращать перебои в работе (и, в конечном счете, узкие места), которые связаны с проблемами при IP-адресации.

В этой главе вы изучите следующие темы:

- реализация IPAM;
- эффективное использование компонентов IPAM;
- интеграция IPAM с System Center 2012;
- управление делегированием IPAM;
- функционирование DHCP Failover.

IPAM

IP Address Management — это не просто новые модные слова, которые предписывают, каким образом должно проводиться управление IP-адресами. На самом деле это современный (и определенно необходимый) новый компонент ОС Windows Server 2012, который снижает сложность сети за счет своей интеграции с существующими корпоративными развертываниями DNS и DHCP.

В документации от Microsoft компонент IPAM описан следующим образом.

IPAM — это интегрированный комплект инструментов, которые делают возможным сквозное планирование, развертывание, управление и мониторинг инфраструктуры IP-адресов с помощью развитого пользовательского интерфейса. IPAM автоматически обнаруживает серверы инфраструктуры IP-адресов в сети и позволяет управлять ими через централизованный интерфейс.

Если после чтения данного определения у вас возник вопрос наподобие "Выглядит достаточно полезным компонентом, но какие проблемы он мог бы решить?", то ниже приведены описания ряда типичных примеров проблем, возникающих при управлении IP-адресами, которые вполне могут возникнуть и в вашей сети.

- Вы делаете все возможное, чтобы вручную вести несколько электронных таблиц и специальных баз данных, содержащих (как вы надеетесь) все IP-адреса в ваших сетевых средах.
- Вам нужно быстро идентифицировать свободный IP-адрес для нового сетевого компьютера или устройства и затем обеспечить его регистрацию в DNS.
- Одна из областей видимости DHCP достигла своего максимального предела, и вам необходимо как можно быстрее идентифицировать ее и расширить.
- У вас имеется требование отслеживать адреса, используемые во множестве разных мест и подсетей, в том числе в виртуальных адресных пространствах.
- Вы хотите внести изменение в настройку DHCP, которая распространяется по всем областям видимости DHCP, такое как удаление старых ссылок на сервер WINS либо изменение прокси-сервера для доступа в веб.
- Вас утомила необходимость в открытии несметного числа разных консолей DNS и DHCP каждый раз, когда требуется внести изменение, которое применимо ко всей сетевой среде.

Благодаря развертыванию IPAM, можно сократить временные затраты на обслуживание существующих и новых диапазонов адресов IPv4 и IPv6. Чем сложнее среда IP-адресов, тем больший смысл в использовании компонента IPAM. Кроме того, организации, которые имеют смесь физических и виртуальных сетей, теперь могут получить унифицированное решение по управлению IP-адресами в них.

Полезная возможность компонента IPAM заключается в том, что он будет автоматически искать в среде все серверы DNS, Domain Controller (контроллер домена) и DHCP и предложит поместить их под централизованный контроль или же нет. Если вы развернули роль NPS (Network Policy Server — сервер сетевой политики) на любых серверах в сети, то IPAM не найдет их автоматически, однако такие серверы можно легко добавить вручную, чтобы обеспечить над ними контроль со стороны IPAM. На рис. 5.1 приведен пример работы IPAM с серверами, помогающей централизовать решение по управлению адресами.

Требования для развертывания IPAM

Как и с любым типом конфигурирования или развертывания, устоявшаяся практика предусматривает проверку того, удовлетворены ли все существенные предварительные условия. Прежде чем развертывать IPAM в своей среде, удостоверьтесь в выполнении описанных ниже требований.

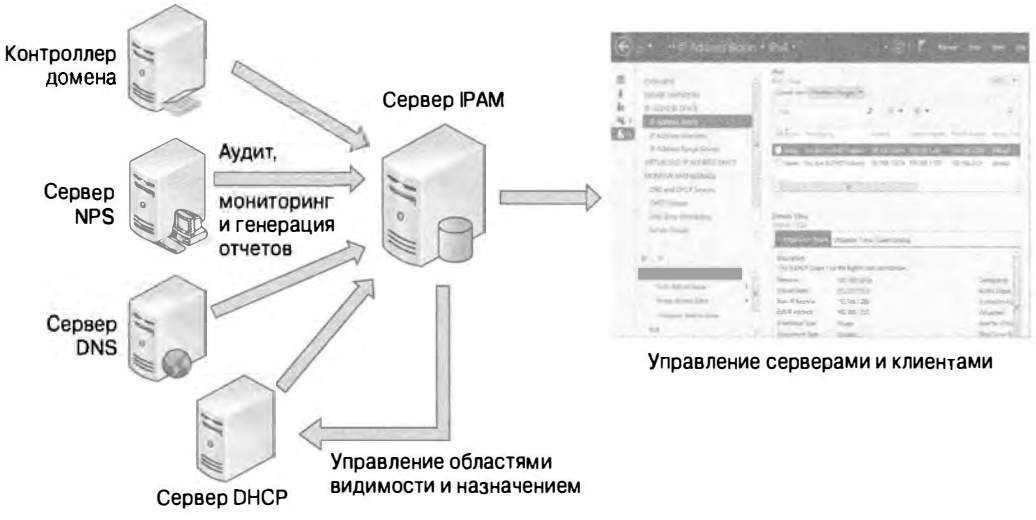


Рис. 5.1. Пример использования IPAM

Поддержка Windows Server

Поскольку средство IPAM было введено в Windows Server 2012, оно должно устанавливаться на компьютере, функционирующем под управлением ОС Windows Server 2012 (или выше) редакции Standard либо Datacenter. После установки IPAM получит возможность управлять только серверами DHCP, DNS и Domain Controller (DC) с ОС версии Windows Server 2008 или выше. Это означает, что если в сети есть ряд унаследованных компьютеров с Windows Server 2003 или Windows Server 2000, то ими придется управлять старым "децентрализованным" способом.

Поддержка Active Directory

Сервер IPAM должен быть членом домена Active Directory; серверы IPAM, не присоединенные к домену, не поддерживаются. Сервер IPAM может функционировать только в границах одного леса Active Directory, но внутри этого леса допускается иметь смесь доверенных и недоверенных доменов, которые все могут управляться данным сервером IPAM. К тому же, можно управлять только серверами, присоединенными к домену; любые серверы, не являющиеся членами домена Active Directory, средством IPAM не поддерживаются.

Можно ли установить IPAM на контроллере домена или на сервере DHCP?

Если кратко, то нельзя. Хотя вы и не получите сообщения об ошибке при первоначальной установке компонента IPAM, его развертывание на сервере, на котором уже установлена роль Active Directory Services Domain Controller, не поддерживается. Когда позже вы попытаетесь подготовить сервер IPAM после начального развертывания компонента, он доставит бесконечно много проблем, и в конечном итоге работать не будет. Аналогично, если вы развернете IPAM на компьютере с установленной серверной ролью DHCP, то обнаружение средством IPAM серверов DHCP в сети будет отключено.

Поддержка DHCP и DNS

К средам DHCP и DNS, управляемым IPAM, применимы следующие ограничения поддержки.

- Серверы DHCP и DNS должны быть членами домена Active Directory.
- Одиночный сервер IPAM может поддерживать до 150 серверов DHCP и до 6 000 областей видимости DHCP.
- Одиночный сервер IPAM может поддерживать до 500 серверов DNS и до 150 зон DNS.

Поддержка базы данных

Средству IPAM необходимо хранить конфигурацию и данные внутри базы данных. Ниже перечислены сведения, которые вы должны знать о поддержке баз данных IPAM.

- Информация, называемая в Microsoft "историческими данными", которая предназначена для целей аудита и отслеживания, хранится в базе данных IPAM на протяжении максимум трех лет.
- Эти данные образованы за счет комбинации аренд IP-адресов, MAC-адресов и деталей входа/выхода из системы для максимум 100 000 пользователей. Несмотря на большой объем данных для хранения, как ни странно, в Microsoft не предоставили политику очистки базы данных. Вы, как администратор IPAM, должны очищать базу данных вручную по мере необходимости.
- IPAM в Windows Server 2012 (не R2) поддерживает стандартный формат Windows Internal Database (Внутренняя база данных Windows). Никакие внешние базы данных не поддерживаются.
- Тем не менее, IPAM в Windows Server 2012 R2 предоставляет возможность использовать на выбор либо Windows Internal Database, либо базу данных SQL 2008 R2/SQL 2012. База данных SQL может располагаться на том же сервере, где функционирует IPAM, или же размещаться внешне на удаленном компьютере.

Поддержка сети

Совершенно очевидно предположить, что работоспособное развертывание IPAM зависит от полностью функциональной сетевой среды (IPv4/IPv6), но со стороны сети есть несколько дополнительных аспектов, которые должны быть приняты во внимание.

- Отсутствует поддержка для сетевых элементов, отличных от Microsoft (таких как NetBIOS Name Service (Служба имен NetBIOS), ретрансляторы DHCP или прокси-серверы).
- WINS является унаследованным решением Microsoft по преобразованию имен NetBIOS, но средством IPAM оно не поддерживается.
- Если вы хотите иметь доступ к данным о тренде потребления IP-адресов из IPAM, то должны будете работать только с отчетами для протокола IPv4, поскольку данные о тренде потребления адресов IPv6 пока еще не поддерживаются.
- Поддержка восстановления адресов IPv6 не доступна; имеется только поддержка для IPv4.

- IPAM не согласовывает свои IP-адреса с маршрутизаторами и коммутаторами, так что вы должны быть осведомлены о любых службах DHCP, функционирующих на этих устройствах.

Компоненты IPAM

Средство IPAM состоит из трех разных функциональных компонентов, которые интегрированы вместе для обеспечения комплексного управления инфраструктурой IP-адресов. Этими тремя компонентами являются Multi-Server Management and Monitoring (Многосерверное управление и мониторинг), Address Space Management (Управление адресным пространством) и Network Auditing (Аудит сети). В настоящем разделе детально обсуждаются все три компонента, чтобы вы полностью поняли, как работает комплект IPAM, и знали, каким образом каждый его фрагмент вписывается в решение по управлению сетями.

Компонент Multi-Server Management and Monitoring

Компонент Multi-Server Management and Monitoring из 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 компонента является возможность одновременного обновления всех серверов DHCP и DNS. Данный компонент также предоставляет функциональность мониторинга, с помощью которой можно проверять доступность областей видимости DHCP и зон DNS.

Компонент Address Space Management

Компонент Address Space Management (ASM) из IPAM обеспечивает полную прозрачность инфраструктуры IP-адресов из единой централизованной консоли. Он включает ясную функцию генерации отчетов, которая позволяет отслеживать тренды потребления адресов IPv4 и формировать данные в виде простых в анализе отчетов. Использование ASM для улучшения планирования, учета и контроля в сети может продемонстрировать реальное отличие между проактивным (исправление проблемы до ее возникновения) и реактивным (изучение проблемы после ее возникновения) подходами к решению проблем с IP-адресацией.

Компонент ASM из IPAM можно применять для обнаружения перекрывающихся диапазонов IP-адресов или областей видимости, которые были сконфигурированы по-разному среди серверов DHCP, а также для создания записей DNS и DHCP и нахождения свободных IP-адресов внутри диапазона. На рис. 5.2 показан график тренды потребления IP-адресов за месячный период.

Компонент Network Auditing

Компонент Network Auditing из IPAM исследует журналы событий Windows на серверах DHCP и дает полное представление обо всех изменениях в конфигурации DHCP, которые происходили в среде. Она сопоставляет данные из базы данных IPAM, журналов аренды серверов DHCP, а также журналов безопасности серверов DC и NPS, чтобы представить информацию по отслеживанию пользователей, устройств и IP-адресов. Имея готовые данные такого типа, к тому же допускающие

полноценный поиск в них, отчеты можно строить на лету, что помогает в идентификации любых проблем, присутствующих в конфигурации.

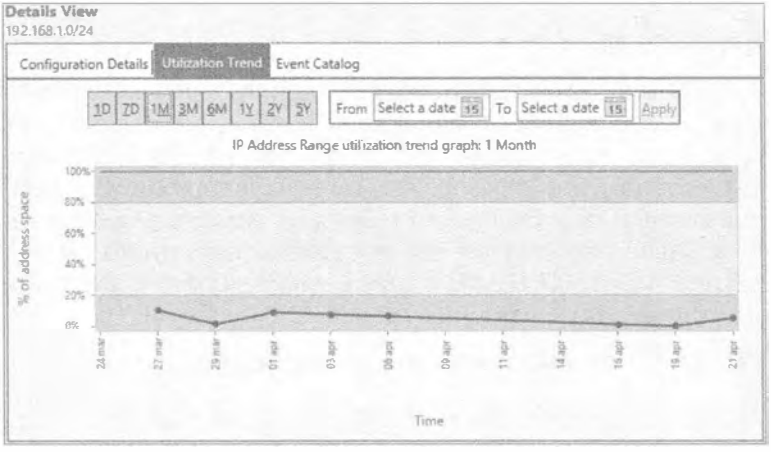


Рис. 5.2. График тренда ASM

Варианты развертывания топологии

При развертывании IPAM для управления инфраструктурой IP-адресов существуют три варианта проектов развертывания топологии, распространяющиеся на множество физических и логических сред. Эти типы конфигураций описаны в табл. 5.1.

Таблица 5.1. Топологии IPAM

Топология	Описание
Централизованная	Один сервер IPAM в центральном местоположении для управления всем
Распределенная	На каждом сайте предприятия разворачивается сервер IPAM. Информация каждого сервера IPAM будет изолирована внутри своего сайта безо всякой репликации или синхронизации данных между различными серверами IPAM в предприятии
Гибридная	В этом проекте топологии используется смесь централизованной и распределенной моделей и имеется развернутый центральный сервер IPAM наряду с несколькими распределенными серверами IPAM на разных сайтах

Установка IPAM

Теперь, когда вы понимаете, что собой представляет компонент IPAM, мы можем пройтись по процессу его установки. В описанных здесь шагах предполагается, что либо есть существующая производственная инфраструктура IP-адресов (DC, DNS, DHCP и т.п.), подлежащая управлению, либо, по крайней мере, вы следуете шагам, приведенным в этой книге, для построения и конфигурирования экспериментальной или тестовой сети (в качестве примера среды мы используем домен `Bigfirm.com`), где можно развернуть IPAM.

Ниже перечислены высокоуровневые шаги, требуемые для развертывания IPAM.

1. Установите компонент IPAM Server с помощью мастера добавления ролей и компонентов (Add Roles and Features Wizard).
2. Сконфигурируйте IPAM либо вручную, либо с применением групповой политики (Group Policy).
3. Сконфигурируйте обнаружение серверов DHCP и DNS внутри домена (доменов).
4. Запустите обнаружение серверов DHCP и DNS.
5. Выберите обнаруженные серверы для управления.
6. Извлеките данные из обнаруженных серверов DHCP и DNS.
7. Установите компонент IPAM Client на дополнительных компьютерах.

Установка компонента IPAM Server

В этом разделе мы рассмотрим процесс установки IPAM.

1. Первым делом войдите в систему Windows Server 2012 R2, присоединенную к домену, с использованием учетной записи, которая имеет разрешения администратора. 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) ничего не выбирайте, а просто щелкните на кнопке Next, чтобы продолжить.
6. Попав на экран Select Features (Выбор компонентов), прокручивайте вниз список Features (Компоненты), пока не найдете компонент IP Address Management (IPAM) Server (Сервер управления IP-адресами (IPAM)), и отметьте флажок рядом с ним (рис. 5.3). Откроется диалоговое окно с запросом на добавление нескольких обязательных компонентов, таких как консоль Group Policy Management (Управление групповой политикой) и Windows Internal Database (Внутренняя база данных Windows); просто щелкните в этом окне на кнопке Add Features (Добавить компоненты). Для продолжения щелкните на кнопке Next.
7. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) просмотрите выбранные варианты и щелкните на кнопке Install (Установить), чтобы запустить установку сервера IPAM.
8. После завершения установки щелкните на кнопке Close (Закрыть) для закрытия окна мастера.

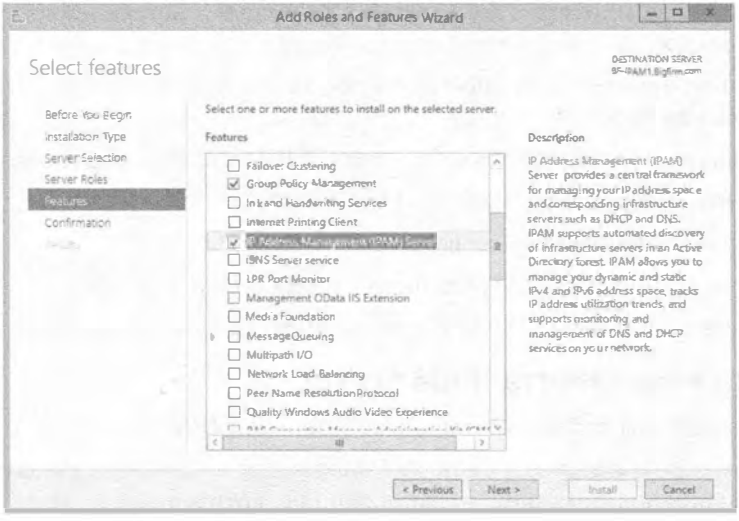


Рис. 5.3. Выбор компонента IPAM

Установка IPAM с помощью PowerShell

Установить сервер IPAM можно также с использованием PowerShell, выполнив перечисленные ниже шаги.

1. Откройте окно командной строки Windows PowerShell с повышенными разрешениями, щелкнув правой кнопкой мыши на соответствующем значке и выбрав в контекстном меню пункт Run As Administrator (Запуск от имени администратора). Затем предоставьте свои учетные данные администратора.
2. Введите следующую команду и нажмите <Enter>:

```
Install-WindowsFeature IPAM -IncludeManagementTools
```

Установка средства IPAM Client

Средство IPAM Client является по существу той же самой консолью IPAM, которую вы получаете при установке компонента IPAM Server, но только оно установлено не на сервере IPAM. Чтобы развернуть IPAM Client на сервере, отличном от первичного сервера IPAM, понадобится развернуть инструменты дистанционного администрирования серверов (Remote Server Administration Tools — RSAT). Ниже описаны шаги по развертыванию IPAM Client на компьютере с Windows Server 2012 или выше.

1. Войдите в систему Windows Server 2012, присоединенную к домену, с использованием учетной записи, которая имеет разрешения администратора. 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) ничего не выбирайте, а просто щелкните на кнопке Next, чтобы продолжить.
6. Попав на экран Select Features (Выбор компонентов), раскройте элемент Remote Server Administration Tools (Инструменты дистанционного администрирования серверов) и затем раскройте Feature Administration Tools (Инструменты администрирования компонентов).
7. Отметьте флажок возле компонента IP Address Management (IPAM) Client (Клиент управления IP-адресами (IPAM)) и щелкните на кнопке Next.
8. Если откроется диалоговое окно с запросом на добавление нескольких обязательных компонентов, таких как консоль Group Policy Management (Управление групповой политикой) и Windows Internal Database (Внутренняя база данных Windows), просто щелкните на кнопке Add Features (Добавить компоненты). Для продолжения щелкните на кнопке Next.
9. На экране Confirm Installation Selections (Подтверждение выбранных настроек для установки) просмотрите выбранные варианты и щелкните на кнопке Install (Установить), чтобы запустить установку клиента IPAM.
10. После завершения установки щелкните на кнопке Close (Закрыть) для закрытия окна мастера.

Конфигурирование предоставления IPAM

После развертывания компонента IPAM необходимо создать инфраструктуру IP-адресов для управления. Как упоминалось ранее, существуют два метода предоставления IPAM: вручную или путем применения групповой политики Active Directory (Active Directory Group Policy). Для простоты (и с точки зрения здравого смысла) мы сосредоточим здесь внимание на методе, предусматривающем использование групповой политики. По очевидным причинам, если вы хотите пройти через этот процесс, то должны располагать развернутой средой Active Directory. В случае если в экспериментальной среде службы Active Directory пока не настроены, выполните задачи, описанные в главе 7, после чего возвратитесь обратно.

1. На сервере, где развернут сервер IPAM, откройте диспетчер серверов. Обратите внимание на появление элемента IPAM в навигационной панели слева, как показано на рис. 5.4.

   Щелчок на ссылке IPAM внутри диспетчера серверов приводит к открытию консоли IPAM Overview (Обзор IPAM), которая будет центральным узлом для управления IPAM. На выбор доступны три опции: Quick Start (Быстрый старт), Actions (Действия) и Learn More (Продолжить обучение).

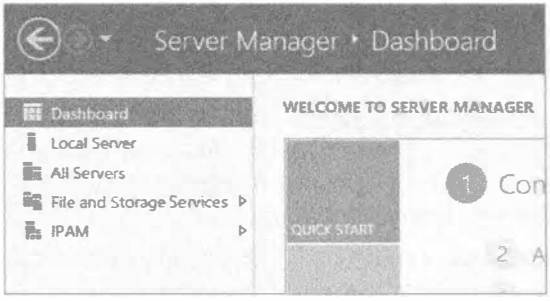


Рис. 5.4. IPAM в диспетчере серверов

2. Щелкните на Quick Start, чтобы увидеть, что консоль уже обнаружила и подключилась к локальному серверу IPAM, который был сконфигурирован ранее (рис. 5.5).

Рис. 5.5. Управление IPAM

3. Щелкните на ссылке Provision the IPAM server (Предоставление сервера IPAM) из меню Quick Start, чтобы открыть мастер предоставления IPAM (Provision IPAM Wizard).
4. Бегло прочитайте текст на экране Before you begin (Прежде чем начать) и щелкните на кнопке Next (Далее).

   Появится экран Configure Database (Конфигурирование базы данных), где можно выбрать тип базы данных для развертывания IPAM — либо Windows Internal Database, либо Microsoft SQL Server. В этом примере оставьте стандартный вариант Windows Internal Database и щелкните на кнопке Next.
5. На экране Select provisioning method (Выбор метода предоставления), показанном на рис. 5.6, понадобится выбрать один из переключателей Manual (Ручной) или Group Policy Based (Основанный на групповой политике). Второй переключатель выбран по умолчанию и является рекомендуемой опцией.

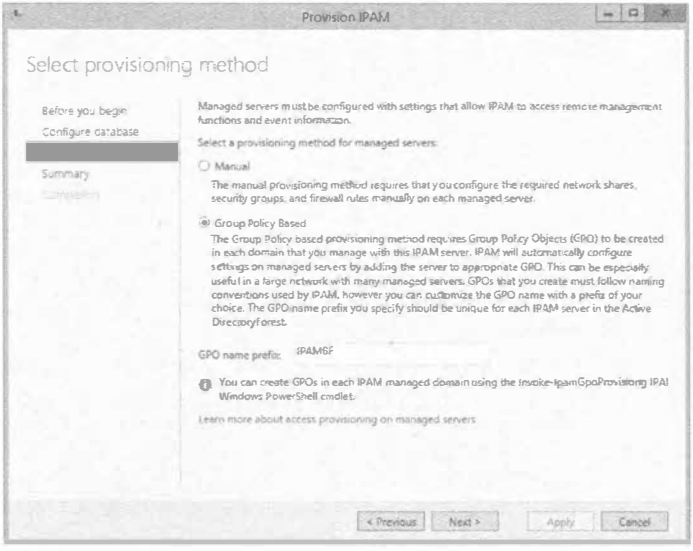


Рис. 5.6. Выбор метода предоставления

Введите префикс имени объекта GPO в пустом поле ниже и щелкните на кнопке Next.

6. На экране Summary (Сводка) приводятся все выбранные опции и в рассматриваемом примере перечисляются объекты GPO, которые будут развернуты для управляемых серверов DHCP, DNS и NPS. Внимательно все проверьте, прежде чем щелкать на кнопке Apply (Применить)! После щелчка на Apply изменить метод предоставления не получится, и если вы захотите перейти на другой метод, то придется полностью переустанавливать IPAM.

   Если выбранный метод предоставления устраивает, щелкните на кнопке Apply.

7. После успешного завершения настройки предоставления IPAM щелкните на кнопке Close (Закрыть), чтобы закрыть окно мастера.

Конфигурирование обнаружения серверов

В этот момент вы должны заметить, что консоль IPAM Overview начинает заполняться информацией, и с помощью выбранного метода предоставления вы можете переходить к обнаружению серверов DC, DNS и DHCP.

1. В консоли IPAM Overview щелкните на плитке Quick Start (Быстрый старт) и затем щелкните на ссылке Configure Server Discovery (Конфигурирование обнаружения серверов).

   В диалоговом окне Configure Server Discovery (Конфигурирование обнаружения серверов) вы должны увидеть свой корневой домен в раскрывающемся списке Select Domains to Discover (Выберите домены для обнаружения).

2. Щелкните на кнопке Add (Добавить), чтобы добавить этот домен в список местоположений для обнаружения серверов DC, DNS и DHCP (рис. 5.7).

3. Щелкните на кнопке OK, чтобы подтвердить выбор и возвратиться в консоль IPAM Overview.

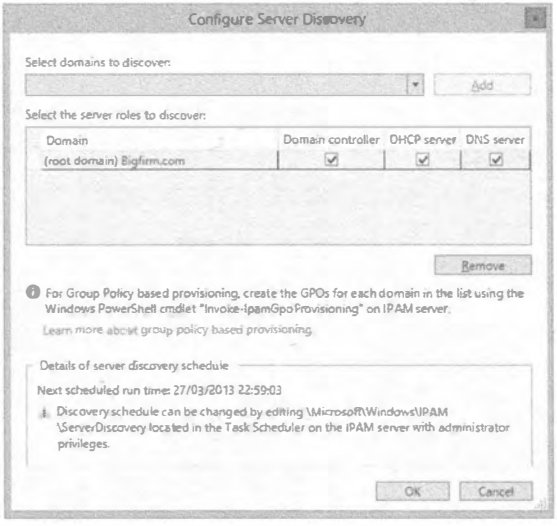


Рис. 5.7. Конфигурирование обнаружения серверов

Запуск обнаружения серверов

После конфигурирования домена, в котором будет выполняться управление серверами, наступает время сообщить IPAM о необходимости проведения их поиска. Все, что нужно для выполнения этой задачи — щелкнуть на ссылке Start Server Discovery (Начать обнаружение серверов) при выбранной плитке Quick Start внутри консоли IPAM Overview. Щелчок приведет к запуску задачи IPAM ServerDiscovery. Чтобы просмотреть детали выполнения этой задачи, можно щелкнуть на флаге Information (Информация) внутри диспетчера серверов; на рис. 5.8 показано результирующее окно Task Details (Детали задачи).

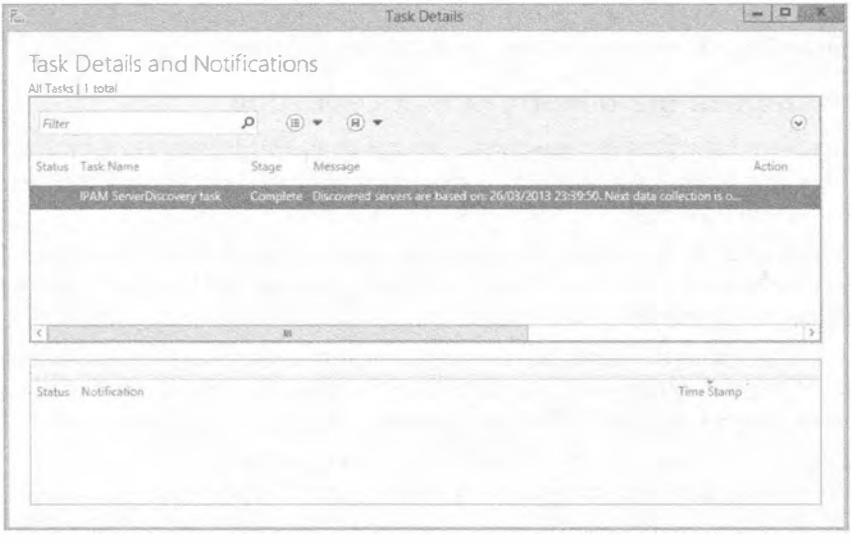


Рис. 5.8. Просмотр деталей задачи ServerDiscovery

Выбор серверов для управления

После выполнения задачи обнаружения можно выбрать из числа обнаруженных серверов те, которыми необходимо управлять посредством IPAM. Для этого сначала щелкните на ссылке Select or Add Servers to Manage and Verify IPAM Access (Выбрать или добавить серверы для управления и проверить доступ IPAM) при выбранной плитке Quick Start. Когда эта опция выбрана, в разделе IPv4 вы должны увидеть список обнаруженных серверов, но вы также заметите, что в столбце IPAM Access Status (Состояние доступа IPAM) они имеют состояние Blocked (Заблокирован), а в столбце Manageability Status (Состояние управляемости) — состояние Unspecified (Не определено), как показано на рис. 5.9.

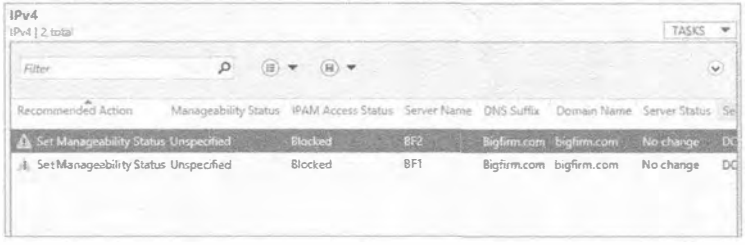


Рис. 5.9. Заблокированные серверы

Не переживайте; это ожидаемое стандартное поведение, и вам нужно лишь инициировать созданные ранее объекты GPO с использованием командлета `Invoke-IpamGpoProvisioning` в PowerShell. Для этого выполните следующие шаги.

1. Проверьте, что вы вошли на сервере IPAM под учетной записью с разрешениями администратора домена.
2. Откройте окно командной строки Windows PowerShell с применением пункта Run as Administrator (Запуск от имени администратора) контекстного меню, чтобы получить повышенные разрешения на локальном сервере.
3. Введите показанную ниже команду и нажмите <Enter> (приведите ее в соответствие со своей средой):

```
Invoke-IpamGpoProvisioning -Domain Bigfirm.com -GpoPrefixName IPAMBF
 -DelegatedGpouser administrator -IpamServerFqdn BF-IPAM1.bigfirm.com
```

4. Будет запрошено подтверждение, поэтому введите `Y` (рис. 5.10).

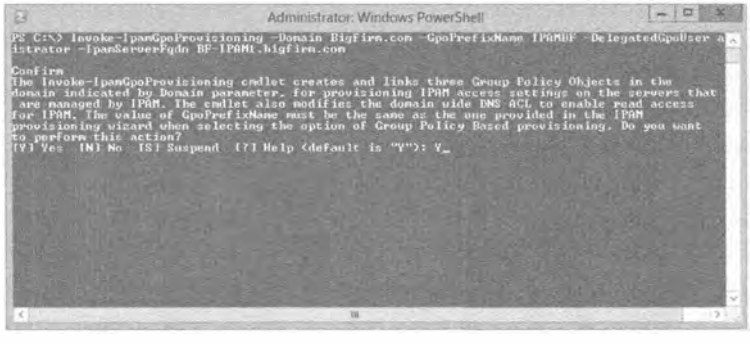


Рис. 5.10. Активизация объектов IPAM GPO

5. Процесс активизации проходит относительно быстро. По его завершении проверьте, что объекты GPO были развернуты, открыв оснастку Group Policy Management (Управление групповой политикой) через меню Tools (Сервис) диспетчера серверов (эта оснастка была развернута как часть установки сервера IPAM).

   Вы должны увидеть три объекта IPAM GPO в корне вашего домена (рис. 5.11).

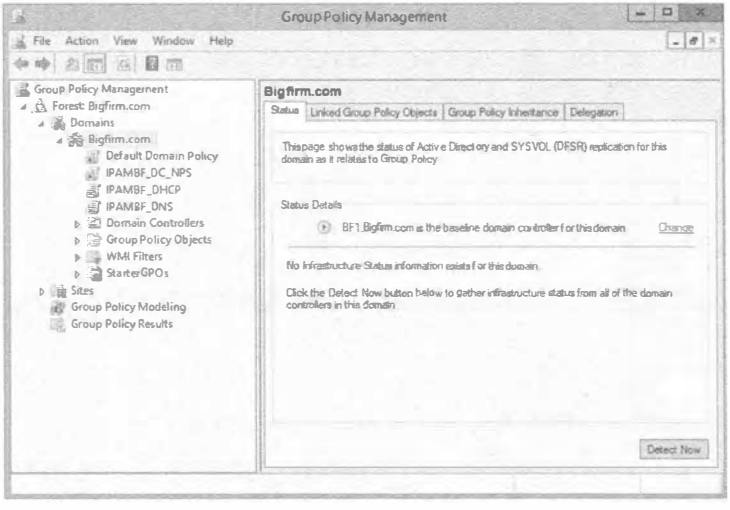


Рис. 5.11. Подтверждение активизации объектов IPAM GPO

Имея развернутые в домене объекты GPO, осталось только выбрать серверы, которыми необходимо управлять с помощью IPAM, и позволить Active Directory сделать все остальное.

6. Чтобы выбрать серверы, возвратитесь в консоль IPAM Overview и выберите элемент Server Inventory (Инвентаризационная запись о сервере) в навигационной панели слева.

   Это приведет к отображению представления, которое вы видели ранее на рис. 5.9 с серверами, имеющими состояние Unspecified.

7. Щелкните правой кнопкой мыши на каждом сервере, которым нужно управлять, и выберите в контекстном меню пункт Edit Server (Редактировать сервер).

8. В открывшемся диалоговом окне Add or Edit Server (Добавление или редактирование сервера) выберите в раскрывающемся списке Manageability Status (Состояние управляемости) элемент Managed (Управляемый), как показано на рис. 5.12; щелкните на кнопке OK.

9. Повторите шаги 6–8 для каждого сервера, которым необходимо управлять.

   После того как все нужные серверы сконфигурированы как Managed, вы можете либо подождать, пока Active Directory не обновит групповую политику в домене (это происходит обычно каждые 15 минут), либо запустить на каждом сервере команду `gpupdate /force` в командной строке или в окне PowerShell.

10. Как только объекты GPO помещены в домен, возвратитесь к представлению Server Inventory внутри консоли IPAM Overview на сервере IPAM.

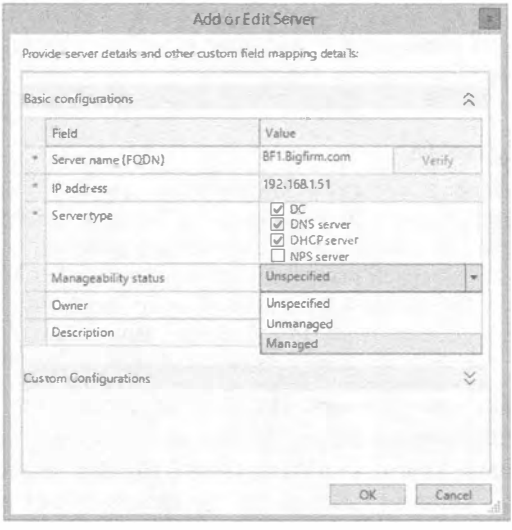


Рис. 5.12. Изменение состояния управляемости

11. Щелкните правой кнопкой мыши на любых серверах с состоянием Managed и выберите в контекстном меню пункт Refresh Server Access Status (Обновить состояние доступа к серверу).

    Это приведет к запуску быстрой проверки процесса обнаружения между сервером IPAM и управляемыми серверами на предмет корректности применения объектов GPO.

12. После того как обнаружение завершится, щелкните на значке Refresh IPv4 (Обновить IPv4) в верхней части консоли; состояние доступа IPAM для управляемых серверов изменится на Unblocked (Разблокирован), что можно видеть на рис. 5.13.

Рис. 5.13. Разблокированные серверы

Извлечение данных

Теперь серверы управляются и разблокированы и почти все готово к запуску. Последнее действие, которое необходимо предпринять — щелкнуть правой кнопкой

мыши на этих серверах и выбрать в контекстном меню пункт Retrieve All Server Data (Извлечь данные из всех серверов). Это приведет к заполнению консоли IPAM областями видимости DHCP и зонами DNS.

Обновление данных IPAM

Если вы корректно следовали всем указанным выше шагам, но консоль IPAM данными DHCP или DNS не заполняется, щелкните на значке Refresh (Обновить), расположенном слева от флага Notifications (Уведомления) консоли сервера IPAM. Однако мы обнаружили, что когда сервер поступает на управление IPAM в первый раз, иногда извлечение данных может занять несколько больше времени, чем ожидалось, поэтому не стоит создавать помехи этому процессу, вручную обновляя консоль.

Когда конфигурирование сервера IPAM завершено, вы можете просмотреть набор новых запланированных задач, установленных на запуск в разные промежутки времени, для чего понадобится открыть представление Task Scheduler (Local)⇨Task Scheduler Library⇨Microsoft⇨Windows⇨IPAM (Планировщик задач (локальный)⇨Библиотека планировщика задач⇨Microsoft⇨Windows⇨IPAM), показанное на рис. 5.14.

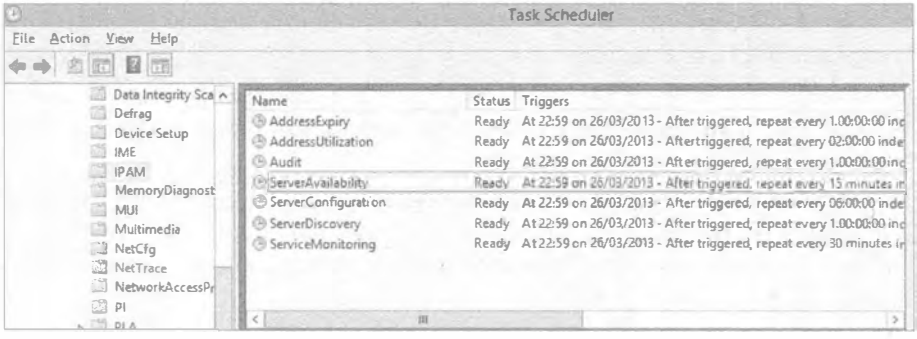


Рис. 5.14. Новые запланированные задачи IPAM

Использование IPAM

После того как вы развернули и сконфигурировали IPAM, вы захотите узнать, каким образом его применять для администрирования инфраструктуры IP-адресов. Навигационная панель консоли IPAM содержит набор различных ссылок, которые предоставляют опции для просмотра, управления, мониторинга и аудита пространств IP-адресов и управляемых серверов. Эти опции показаны на рис. 5.15. В настоящем разделе мы обсудим несколько разных сценариев управления и функциональные средства, которые IPAM может предложить через разнообразные представления в консоли.

Представления Overview и Server Inventory

Во время установки и конфигурирования IPAM вы хорошо ознакомились с представлениями Overview (Обзор) и Server Inventory (Инвентаризационная запись о сервере). Далее будут приведены дополнительные детали о них.

Представление Overview

В результате щелчка на ссылке Overview вы можете делать выбор среди трех задач сервера IPAM, которые представлены в форме плиток под названиями Quick Start (Быстрый старт), Actions (Действия) и Learn More (Продолжить обучение). Эти плитки по существу являются быстрыми ссылками, предназначенными для выполнения различных задач и действий в управляемой сети. Здесь вы также увидите графическую форму серверов IPAM и управляемых доменов в представлении Managed Network (Управляемая сеть) наряду с представлением Configuration Summary (Сводка по конфигурации) со всеми существующими конфигурационными настройками IPAM. В нижней части окна Overview находится представление Scheduled Tasks (Запланированные задачи), которое является альтернативным местом для просмотра списка запланированных задач IPAM, запускаемых на сервере.

Рис. 5.15. Опции навигации IPAM

Представление Server Inventory

В окне IPv4 вы получаете список всех управляемых и неуправляемых серверов. В этом списке присутствуют только те серверы, которые были автоматически и вручную обнаружены через консоль IPAM. В окне IPv4 можно щелкнуть на раскрывающееся меню Tasks (Задачи) и добавить новые серверы, извлечь данные из серверов или просто экспортировать данные в файл со значениями, разделенными запятыми (`.csv`). Представление Server Inventory также имеет удобную область Details (Детали), в которой отображается информация, специфичная для серверов (такая как имя хоста, описания IP-адресов, а также состояние IPAM, DHCP и DNS), каждый раз, когда производится щелчок на каком-либо сервере в окне IPv4.

Раздел IP Address Space

Раздел IP Address Space (Пространство IP-адресов) позволяет действительно увидеть, что IPAM может централизовать управление пространством IP-адресов. Он состоит из трех представлений, которые описаны ниже.

Представление IP Address Blocks

В IPAM блок IP-адресов является наивысшим организационным уровнем, который можно использовать для группирования адресных пространств. Блоки IP-адресов содержат диапазоны IP-адресов, которые могут быть классифицированы в логические порции (например, все частные адреса в одном блоке, а все публичные адреса в другом блоке), что помогает в управлении и обслуживании IP-среды. При конфигурировании блока IP-адресов в IPAM, если этот блок адресов заключает в себе адресные пространства как IPv4, так и IPv6, он будет автоматически классифицировать адреса IPv4 в публичные и частные адресные пространства, а любые адреса IPv6 — в одноадресатные глобальные адреса.

Чтобы создать *частный* блок адресов IPv4, выполните приведенную ниже процедуру.

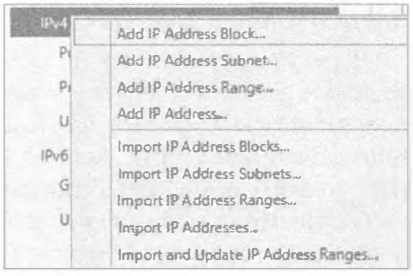


Рис. 5.16. Создание блока IP-адресов

1. Откройте консоль IPAM от имени учетной записи администратора и в навигационной панели щелкните на элементе IP Address Space⇨IP Address Blocks (Пространство IP-адресов⇨Блоки IP-адресов).
2. В нижней части навигационной панели щелкните правой кнопкой мыши на элементе IPv4 и выберите в контекстном меню пункт Add IP Address Block (Добавить блок IP-адресов), как показано на рис. 5.16.
3. В открывшемся диалоговом окне Add or Edit IPv4 Address Block (Добавление или удаление блока адресов IPv4) введите в полях Network ID (Идентификатор сети) и Prefix Length (Длина префикса) частный адрес IPv4 и длину префикса маски подсети (мы выбрали идентификатор сети 192.168.1.0 и длину префикса 24), после чего щелкните на кнопке OK.

   Полезно отметить, что в данный момент в зависимости от предоставленной информации об IP-адресе и подсети, IPAM автоматически добавит этот новый блок IP-адресов в пространство частных или публичных адресов.
4. Чтобы увидеть только что созданный блок IP-адресов, выберите представление IP Address Blocks (Блоки IP-адресов) из раскрывающегося меню Current View (Текущее представление).
5. Щелкните на новом блоке IP-адресов и на вкладке Configuration Details (Детали конфигурации) просмотрите все сведения, имеющие отношение к указанному критерию.

   Вкладки Utilization Trend (Тренд потребления) и Event Catalog (Каталог событий) начнут наполняться информацией после того, как блок IP-адресов приступит к обработке данных.

Процесс создания блока публичных IP-адресов похож на процесс создания блока частных IP-адресов, но предусматривает выполнение нескольких дополнительных шагов.

1. Откройте консоль IPAM от имени учетной записи администратора и в навигационной панели щелкните на элементе IP Address Space⇨IP Address Blocks (Пространство IP-адресов⇨Блоки IP-адресов).
2. В нижней части навигационной панели щелкните правой кнопкой мыши на элементе IPv4 и выберите в контекстном меню пункт Add IP Address Block (Добавить блок IP-адресов), как было показано на рис. 5.16.
3. В открывшемся диалоговом окне Add or Edit IPv4 Address Block (Добавление или удаление блока адресов IPv4) введите в полях Network ID (Идентификатор сети) и Prefix Length (Длина префикса) публичный адрес IPv4 и длину префикса маски подсети (мы выбрали идентификатор публичной сети Sybex.com 208.215.179.132 и длину префикса 30), после чего щелкните на кнопке OK.

4. Поскольку это блок публичных IP-адресов, выберите региональный реестр Интернета (Regional Internet Registry — RIR), который выдает IP-адреса (мы выбрали RIPE), и, если это применимо или возможно, также укажите значение Received Date from RIR (Дата получения от RIR), хотя оно не является обязательным.
5. Чтобы увидеть только что созданный блок IP-адресов, выберите представление IP Address Blocks (Блоки IP-адресов) из раскрывающегося меню Current View (Текущее представление) и в нижней навигационной панели щелкните на элементе Public Address Space (Пространство публичных адресов) под элементом IPv4.
6. Проверьте, что новый блок публичных адресов доступен, а также что можно просматривать информацию на вкладке Configuration Details (Детали конфигурации), как показано на рис. 5.17.

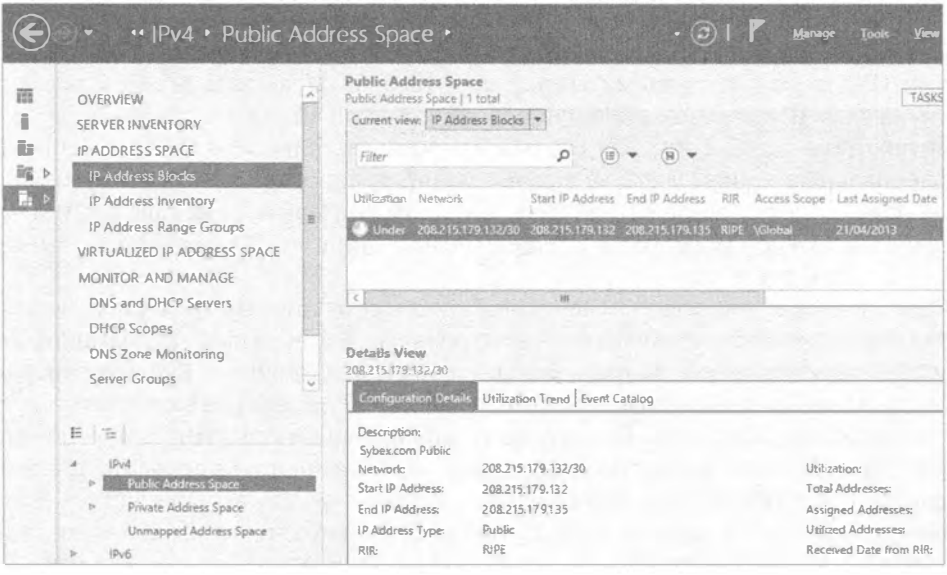


Рис. 5.17. Блок публичных IP-адресов

Если вы хотите разделить на категории все IP-адреса и диапазоны IP-адресов, которые формируют блоки IP-адресов, то можете легко переключаться между этими опциями, просто щелкая на раскрывающемся меню Current View и выбирая желаемый тип представления.

Назначения, выполняемые IPAM

Для лучшего понимания блоков IP-адресов запомните, что IPAM будет автоматически назначать IP-адреса диапазонам IP-адресов (подобно областям видимости DHCP), и затем эти диапазоны IP-адресов будут автоматически назначаться блокам IP-адресов примерно так: IP-адреса⇨диапазоны IP-адресов⇨блоки IP-адресов.

Представление IP Address Inventory

В представлении IP Address Inventory (Инвентаризационная запись об IP-адресах) можно видеть все IP-адреса, доступные средству IPAM, а также информацию о присоединенных к ним устройствам (например, имена хостов и типы устройств). Здесь имеются удобные опции фильтрации, которые позволяют обеспечивать видимость IP-адресов на детализированном уровне, основываясь на большом количестве параметров, в том числе на свойствах IP-адресов диспетчера виртуальных машин системного центра 2012 (System Center 2012 Virtual Machine Manager). В этом представлении можно также легко добавлять записи и резервирования в DNS и DHCP, просто щелкая правой кнопкой мыши на IP-адресе в списке и выбирая подходящий пункт в контекстном меню.

Представление IP Address Range Groups

Представление IP Address Range Groups (Группы диапазонов IP-адресов) из раздела IP Address Space (Пространство IP-адресов) позволяет создавать логические группы, помогающие лучше организовать диапазоны IP-адресов. С помощью раскрывающегося меню Current View можно переходить между IP-адресами, диапазонами IP-адресов и группами IP-адресов. Выбрав здесь вариант IP address ranges (Диапазоны IP-адресов), щелкнув правой кнопкой мыши на диапазоне и выбрав в контекстном меню пункт для его редактирования, в разделе Custom Configurations (Специальные конфигурации) можно сконфигурировать специальные поля, которые определяют диапазон IP-адресов по таким критериям, как сайт Active Directory, страна или регион (Country or Region), бизнес-единица (Business Unit), тип устройства (Device Type) и т.п.

Можно также указать указывать значение для некоторых критериев, чтобы обеспечить дальнейшую детализацию и контроль над логическими группами диапазонов адресов (примером может быть указание значения Reserved (Зарезервирован) для специального поля IP Address State (Состояние IP-адреса)). После того, как вы отредактировали диапазоны IP-адресов со специальными полями и значениями, вам будет представлено полностью прозрачное и знакомое группирование для всей инфраструктуры IP-адресов. Мы совершенно уверены, что вы согласитесь с тем, что такой подход к группированию и сортировке превосходит по эффективности подход с применением для этих же целей статической электронной таблицы Excel!

Раздел Virtualized IP Address Space

В первоначальном выпуске IPAM в Windows Server 2012 была очень ограниченная возможность управления пространствами виртуальных IP-адресов, которые создавались с использованием диспетчера виртуальных машин системного центра 2012 (System Center 2012 Virtual Machine Manager — VMM). Со всей ориентацией на управление центрами данных и облаком именно здесь в Microsoft инвестировали большинство средств 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.

Конфигурирование интеграции осуществляется относительно просто, но работать она будет только с версиями Windows Server 2012 R2 и System Center 2012 R2 Virtual Machine Manager. Предполагая, что вы уже развернули сервер VMM 2012 R2 в том же домене, где находится сервер IPAM, ниже перечислены шаги для их интеграции.

1. Используя учетную запись с разрешениями администратора, откройте консоль VMM 2012 R2 и щелкните на вкладке Fabric (Структура) в навигационной панели.
2. Щелкните на кнопке Add Resources (Добавить ресурсы) в ленте и выберите элемент Network Service (Сетевая служба), как показано на рис. 5.18.

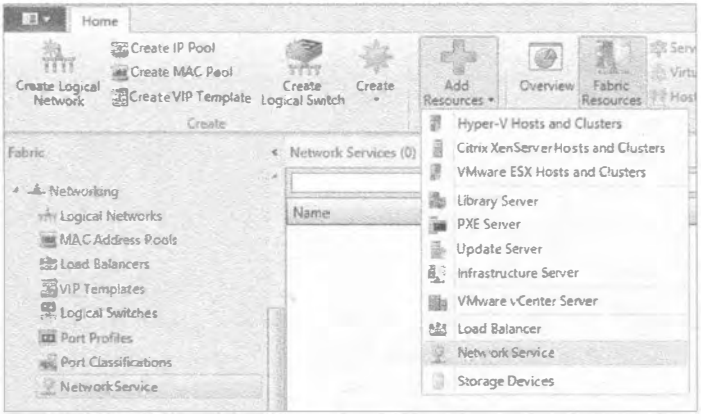


Рис. 5.18. Создание новой сетевой службы в VMM

3. На экране Name (Имя) мастера добавления сетевой службы (Add Network Service Wizard) введите имя (IPAM, например) и описание для службы, затем щелкните на кнопке Next (Далее).
4. На экране Manufacturer and Model (Изготовитель и модель) оставьте в качестве изготовителя Microsoft и выберите в списке Model (Модель) элемент Microsoft Windows Server IP Address Management (Управление IP-адресами Microsoft Windows Server), как показано на рис. 5.19; для продолжения щелкните на кнопке Next.
5. Укажите учетную запись, от имени которой будет выполняться создание службы интеграции; обычно это учетная запись с административными разрешениями на обоих серверах VMM и IPAM. Щелкните на кнопке Next.
6. На экране Connection String (Строка подключения) введите полное доменное имя (FQDN) сервера IPAM и щелкните на кнопке Next.

   Экран Provider (Поставщик), представленный на рис. 5.20, дает возможность протестировать подключение между серверами VMM и IPAM.
7. Здесь рекомендуется щелкнуть на кнопке Test (Протестировать), чтобы удостовериться в том, что все работает. Для продолжения щелкните на кнопке Next.
8. Выберите группу хостов VMM (VMM Host Group), к которой будет применяться служба IPAM. Щелкните на кнопке Next и затем на кнопке Finish (Готово), чтобы завершить процесс.

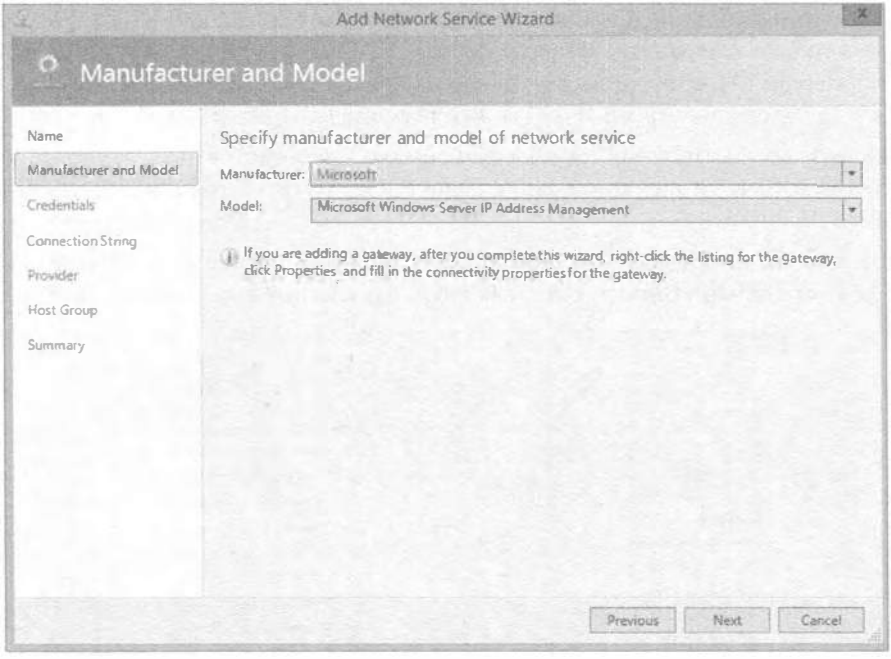


Рис. 5.19. Указание модели интеграции IPAM

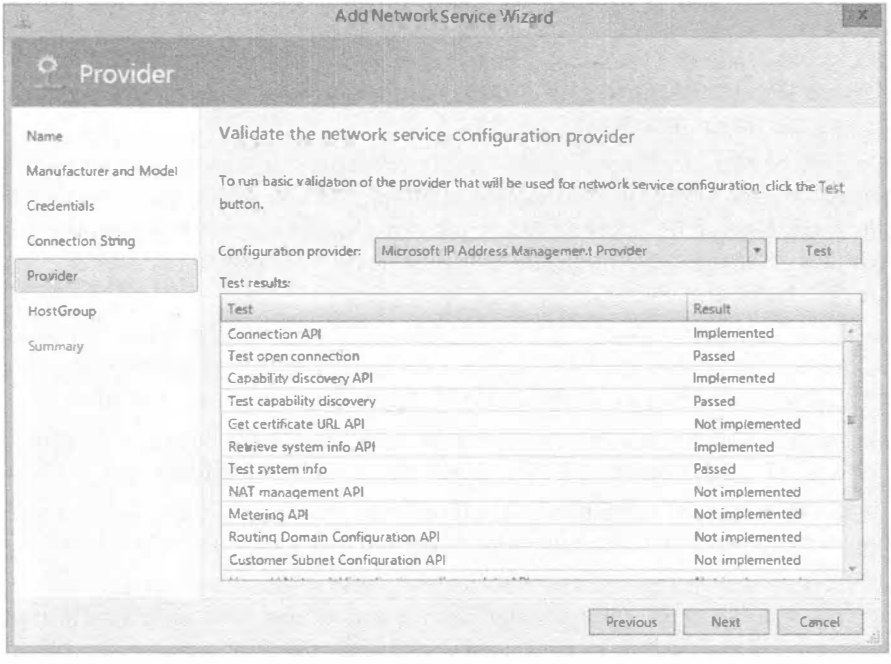


Рис. 5.20. Тестирование подключения

После конфигурирования интеграции между VMM и IPAM можно снова открыть консоль IPAM и заглянуть в раздел Virtualized IP Address Space, где теперь должны быть видны все пространства виртуальных IP-адресов (рис. 5.21).

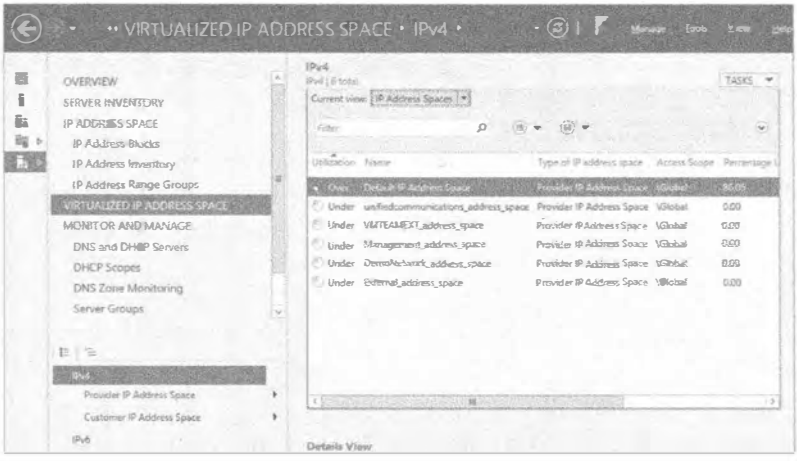


Рис. 5.21. Управление пространствами виртуальных IP-адресов с помощью IPAM

Раздел Monitor and Manage

Раздел Monitor and Manage (Мониторинг и управление) консоли IPAM позволяет отслеживать и управлять серверами DHCP и DNS, находящимися под контролем IPAM. Здесь вы найдете централизованное место, предоставляющее возможность выполнения множества стандартных задач, которые ранее должны были запускаться на каждом индивидуальном сервере — особенно задач, связанных с управлением DHCP. В данном разделе придется работать с четырьмя представлениями.

Представление DNS and DHCP Servers

Представление DNS and DHCP Servers (Серверы DNS и DHCP) отображает список серверов DHCP и DNS и предлагает раскрывающееся меню Server Type (Тип серверов), позволяющее устанавливать область действия представления в определенные серверы DHCP или DNS. Щелкнув правой кнопкой мыши на каком-нибудь сервере DHCP в списке, вы получите набор задач управления для этого конкретного сервера DHCP, которые позволят редактировать параметры сервера DHCP, создавать области видимости DHCP, конфигурировать классы пользователей и поставщиков и делать многое другое. На рис. 5.22 показано полное меню задач.

Можно также запустить оснастку MMC для DHCP и DNS, просто щелкнув правой кнопкой мыши на сервере и выбрав в контекстном меню пункт Launch MMC (Запустить MMC). Представление Details (Детали) предоставляет информацию по выбранному серверу, в том числе Server Properties (Свойства сервера), DHCP Options (Параметры DHCP) и DNS Zones (Зоны DNS).

Представление DHCP Scopes

В представлении DHCP Scopes (Области видимости DHCP) собраны вместе все области видимости DHCP, о которых осведомлено средство IPAM.

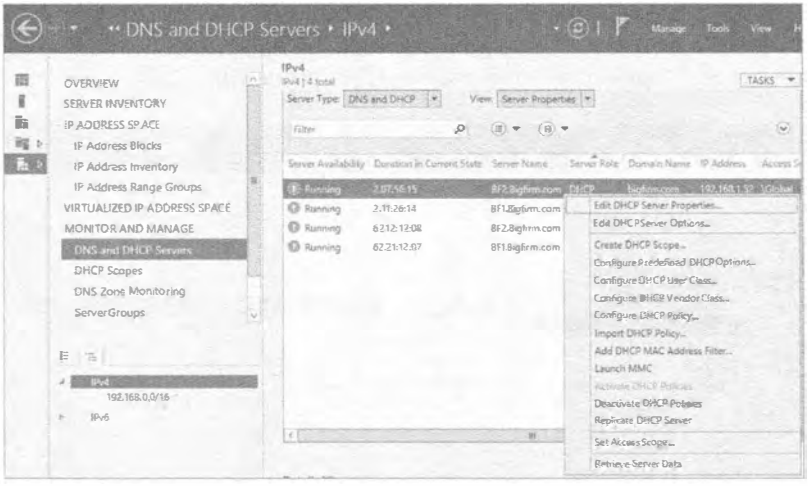


Рис. 5.22. Управление DHCP с помощью IPAM

Здесь можно видеть ключевую информацию о потреблении каждой области видимости и сконфигурированные параметры области видимости DHCP. Предусмотрены отдельные разделы для областей видимости IPv4 и IPv6, к тому же представления можно фильтровать по публичному, частному, глобальному и неназначенному пространству адресов.

Из этого представления можно выполнять множество управляющих действий, выделяя конкретную область видимости DHCP и щелкая на ней правой кнопкой мыши. Одни задачи могут запускаться применительно сразу к нескольким выбранным областям видимости, тогда как другие должны выполняться для одной области видимости за раз. Ниже перечислены некоторые доступные задачи:

- Edit DHCP Scope (Редактировать область видимости DHCP) (может выполняться на множестве областей видимости одновременно)
- Duplicate DHCP Scope (Дублировать область видимости DHCP) (должна выполняться на одной области видимости за раз)
- Activate DHCP Scope (Активировать область видимости DHCP) (может выполняться на множестве областей видимости одновременно)
- Replicate DHCP Scope (Реплицировать область видимости DHCP) (должна выполняться на одной области видимости за раз)
- Deactivate DHCP Scope (Деактивировать область видимости DHCP) (может выполняться на множестве областей видимости одновременно)
- Delete (Удалить) (может выполняться на множестве областей видимости одновременно)
- Create DHCP Reservation (Создать резервирование DHCP) (должна выполняться на одной области видимости за раз)
- Configure DHCP Failover (Конфигурировать DHCP Failover)
- Clear Config Sync Errors (Очистить ошибки синхронизации конфигураций)

Представление DNS Zone Monitoring

Представление DNS Zone Monitoring (Мониторинг зон DNS) является центральным для всех зон прямого и обратного просмотра DNS, которые управляются IPAM. Для каждой зоны можно просматривать состояние работоспособности (работоспособна, есть предупреждение или возникла ошибка), продолжительность нахождения в данном состоянии, информацию о сервере, на котором она выполняется, и тип этой зоны. Тем не менее, в плане более глубокого управления здесь, в отличие от DHCP, доступны только действия Launch MMC (Запустить MMC), Reset Zone Status (Сбросить состояние зоны) и Retrieve Server Data (Извлечь данные из сервера). После запуска оснастки MMC она подключится к выделенной вами зоне, и затем вы сможете администрировать эту зону, как если бы вы вошли локально на данный сервер DNS.

С помощью чего проводить мониторинг DNS — IPAM или System Center Operations Manager?

Вас может интересовать, является ли данный тип мониторинга DNS заменой для средства, подобного Microsoft System Center Operations Manager (Диспетчер операций системного центра Microsoft). Если Operations Manager у вас уже развернут, то мониторинг DNS посредством IPAM определенно не будет его заменой. Operations Manager — это флагманский инструмент мониторинга и управления от компании Microsoft, который предлагает модель служб IT на основе собственного передового опыта и рекомендаций. Диспетчер операций принимает во внимание намного больше аспектов, нежели только DNS, и располагает более широким диапазоном централизованных действий и информации, чем мониторинг зон DNS из IPAM. Продукт Operations Manager более подробно обсуждается в главе 30 (том 2). Однако если Operations Manager не развернут или затраты на развертывание System Center 2012 оказываются неприемлемыми, то мониторинг зон DNS из IPAM послужит хорошей отправной точкой для получения базового централизованного обзора работоспособности, которого в определенных средах оказывается более чем достаточно.

Представление Server Groups

Подобно ранее рассмотренным группам диапазонов IP-адресов, при добавлении или редактировании параметров новых серверов, предназначенных для управления посредством IPAM, вы можете также применять специальные поля. В этих специальных полях вы по существу можете помечать серверы с помощью таких критериев, как Region (Регион), Country (Страна), Building (Строение) или Floor Number (Номер комнаты). Сконфигурировав указанные критерии на серверах, в представлении Server Groups (Группы серверов) щелкните правой кнопкой мыши на ссылке IPv4 и выберите в контекстном меню пункт Add Server Group (Добавить группу серверов). После добавления специальной информации будет создана новая группа серверов, которую можно использовать для получения более специфичного для компании обзора среды серверных IP-адресов.

Раздел Event Catalog

Ранее мы упоминали, что средство IPAM предлагает функциональность для отслеживания IP-адреса и деятельности пользователя наряду с изменениями конфи-

гурации, внесенными в среды IPAM и DHCP. Эта информация собрана в разделе Event Catalog (Каталог событий). Данный раздел состоит из следующих трех представлений.

Представление IPAM Configuration Events

Внутри представления IPAM Configuration Events (События конфигурации IPAM) можно отслеживать любые события конфигурации, которые происходили в инфраструктуре IPAM. Это хорошая отправная точка, если у вас в компании работает множество администраторов IPAM и необходимо перепроверять процессы изменения управления. Вы можете получать информацию об учетной записи конкретного пользователя, который внес изменение в конфигурацию, и располагать возможностью применения определенного фильтра к событиям, чтобы быстро получить требуемые сведения. Для создания одного из таких фильтров щелкните на кнопке Add Criteria (Добавить критерий) и затем отметьте флажки возле каждого критерия, по которому должен быть отсортирован список событий.

Представление DHCP Configuration Events

Представление DHCP Configuration Events (События конфигурации DHCP) очень похоже на представление IPAM Configuration Events и отображает информацию о событиях конфигурации, специфичных для управляемых серверов DHCP. Как показано на рис. 5.23, щелчок на меню Tasks (Задачи) предоставит следующие варианты: Purge Event Catalog Data (Очистить данные каталога событий), Retrieve Event Catalog Data (Извлечь данные каталога событий) и Export (Экспортировать), который позволяет экспортировать события конфигурации в файл `.csv` для дальнейшего анализа.

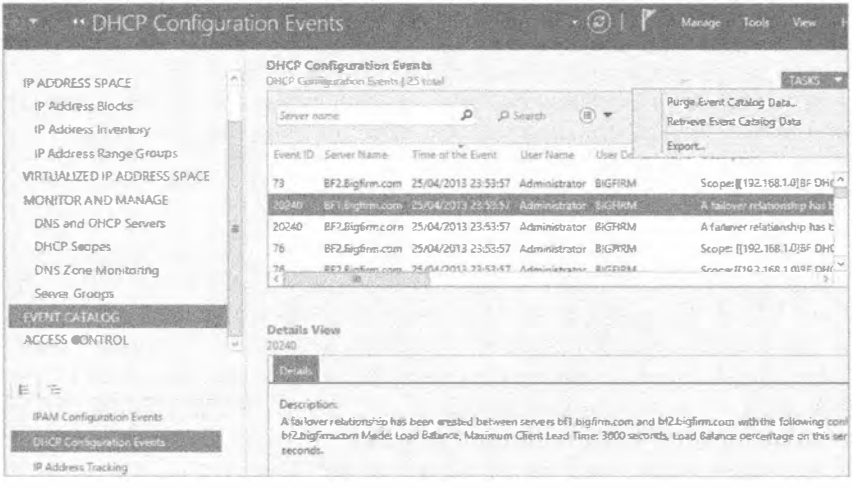


Рис. 5.23. Представление DHCP Configuration Events

Представление IP Address Tracking

Представлением IP Address Tracking (Отслеживание IP-адресов), скорее всего, вы будете пользоваться, когда возникнет необходимость в отслеживании информации об IP-адресах на основе определенных хостов или пользователей.

Здесь на выбор доступны четыре представления:

- By IP Address (По IP-адресу)
- By Client ID (По идентификатору клиента)
- By Hostname (По имени хоста)
- By User Name (По имени пользователя)

Путем выбора любого из этих представлений вы получаете возможность указать дату и время, когда нужен поиск, а также то, должен ли поиск включать или исключать дополнительные связанные данные событий, которые были сгенерированы управляемыми контроллерами доменов либо серверами Network Policy. Как и в представлении DHCP Configuration Events, щелчок на меню Tasks (Задачи) позволит выполнить очистку, извлечение или экспорт данных.

Делегирование 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.

На рис. 5.24 показаны эти группы на сервере IPAM, а далее описано, что предлагает каждая из них.

- **IPAM Administrators (Администраторы IPAM).** Наиболее вероятно, что вы решите сделать членом этой группы собственную учетную запись. Члены данной группы имеют разрешения для полного управления и администрирования IPAM и могут запускать все задачи и просматривать все представления.
- **IPAM IP Audit Administrators (Администраторы аудита IP-адресов IPAM).** Члены этой группы могут выполнять общие задачи управления IPAM и также имеют доступ к информации по отслеживанию IP-адресов, так что они могут проводить аудит IP-адресации, когда он требуется.
- **IPAM ASM Administrators (Администраторы IPAM ASM).** Любые пользовательские учетные записи, являющиеся членами этой группы, могут выполнять задачи, относящиеся к функциональности IPAM Address Space Management (ASM).
- **IPAM MSM Administrators (Администраторы IPAM MSM).** Любые пользовательские учетные записи, являющиеся членами этой группы, могут выполнять задачи на множестве серверов IPAM посредством функциональности IPAM Multi-Server Management and Monitoring.
- **IPAM Users (Пользователи IPAM).** Это самая базовая группа доступа для IPAM, и все пользователи, являющиеся членами данной группы, могут только просматривать информацию по обнаружению серверов, ASM и MSM. Они также могут видеть информацию о рабочих событиях, которые генерируют IPAM и DHCP, но не имеют доступа к любой информации аудита или отслеживания.

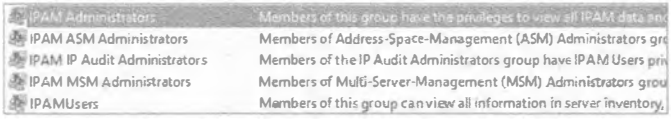


Рис. 5.24. Группы доступа IPAM RBAC

Поверх этих групп доступа располагается эксклюзивное для IPAM в Windows Server 2012 R2 новое представление Access Control (Контроль доступа), показанное на рис. 5.25.

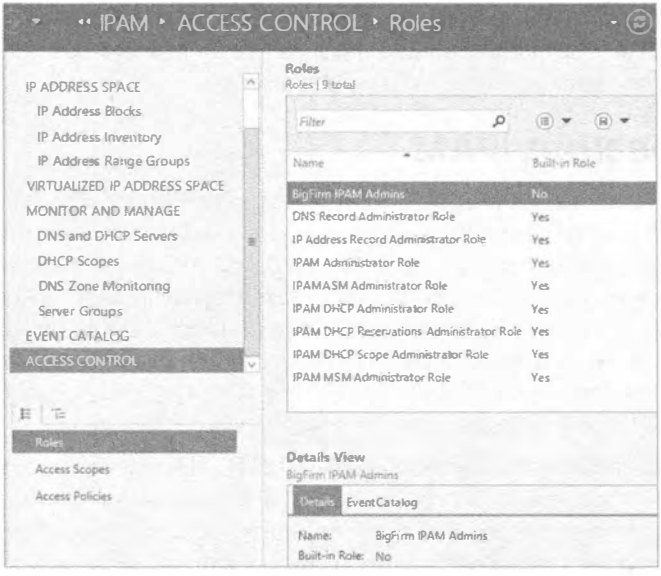


Рис. 5.25. Представление Access Control в IPAM

Вместе с представлением Access Control вы получаете восемь встроенных ролей, а также можете указывать специальные роли для администраторов IPAM и предоставлять им гранулярный доступ к различным компонентам и политикам в IPAM.

Ниже приведена пошаговая инструкция по конфигурированию новой роли, привязка ее к определенным границам IPAM и делегирование этой роли пользовательской учетной записи внутри организации.

1. Щелкните на представлении Access Control в консоли IPAM и удостоверьтесь, что выбрано подпредставление Roles (Роли).
2. В раскрывающемся меню Tasks (Задачи) выберите пункт Add User Role (Добавить пользовательскую роль). Откроется диалоговое окно Add or Edit Role (Добавление или редактирование роли), показанное на рис. 5.26.
3. Введите имя роли и щелкните на кнопке OK.
4. Оставаясь внутри представления Access Control, щелкните правой кнопкой мыши на подпредставлении Access Scopes (Области доступа) в навигационной панели слева и выберите в контекстном меню пункт Add Access Scope (Добавить область доступа).

Рис. 5.26. Создание специальной пользовательской роли

5. В открывшемся диалоговом окне Add Access Scope (Добавление области доступа) щелкните на кнопке New (Новая), укажите имя и описание для новой области доступа и щелкните на кнопке Add (Добавить) для связывания новой области доступа с областью доступа Global (Глобальная), как показано на рис. 5.27.

6. Щелкните на кнопке OK, чтобы продолжить.

Рис. 5.27. Конфигурирование области доступа

7. Далее необходимо щелкнуть правой кнопкой мыши на подпредставлении Access Policies (Политики доступа) внутри представления Access Control консоли, чтобы открыть диалоговое окно Add Access Policy (Добавить политику доступа).
8. В разделе User Settings (Настройки пользователя) укажите пользовательскую учетную запись, которую нужно ассоциировать с данной ролью, а затем в разделе Access Settings (Настройки доступа) выберите специальную роль и область доступа, которые были созданы ранее (рис. 5.28).

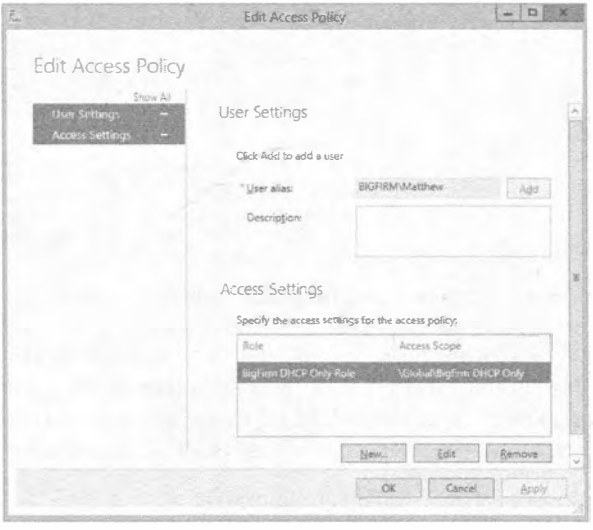


Рис. 5.28. Добавление политики доступа

9. Выберите конкретный раздел в IPAM, который хотите связать со специальной политикой доступа; мы выбрали представление DNS and DHCP Servers (Серверы DNS и DHCP).
10. Щелкните правой кнопкой мыши на сервере DHCP (или на другом управляемом объекте) и выберите в контекстном меню пункт Set Access Scope (Установить область доступа).
11. Выберите область доступа, которую необходимо назначить управляемому объекту, и щелкните на кнопке OK, чтобы завершить процесс.

Устранение неполадок в IPAM

При возникновении любых проблем с IPAM, прежде чем обращаться в службу поддержки Microsoft, ознакомьтесь с информацией и решениями, приведенными в данном разделе, которые могут помочь проникнуть в суть проблемы.

Использование программы Event Viewer

Как и в случае практически любого установленного приложения, роли и компонента от Microsoft, вы должны просмотреть определенные журналы событий в программе Windows Event Viewer (Просмотр событий Windows), что поможет в диагнос-

тике проблем с серверами IPAM. Журналы событий для IPAM находятся в Windows Event Viewer⇨Application and Services Logs⇨Microsoft⇨Windows⇨IPAM (Windows Event Viewer⇨Журналы приложений и служб⇨Microsoft⇨Windows⇨IPAM).

Ниже приведен список источников событий вместе с кратким их описанием.

- **Admin Channel (Административный канал).** Здесь зафиксированы любые неожиданные ошибки, которые возникли в результате какого-то действия пользователя или повторяющейся задачи.
- **Operational Channel (Операционный канал).** События, регистрируемые в этом канале, по умолчанию отключены, поскольку они носят информационный характер, основаны на операционном и работоспособном состоянии IPAM и в любой момент времени их может быть очень много. Просматривать эти оповещения может понадобиться только при устранении неполадок, поэтому такой тип регистрации событий изначально отключен.
- **Configuration Change Channel (Канал изменений в конфигурации).** В данном канале фиксируются любые изменения в конфигурации на сервере IPAM. Эти события можно использовать для аудита администраторов IPAM и идентификации тех, кто вносил изменения (или определения, кто что-то разрушил).
- **Analytic Channel (Аналитический канал).** Этот канал по умолчанию отключен и предназначен для содействия задачам отладки и трассировки.
- **Debug Channel (Отладочный канал).** Этот канал также по умолчанию отключен и предназначен для содействия задачам отладки и трассировки.

Общие проблемы

В табл. 5.2 описаны общие проблемы с подключаемостью, предоставлением, обнаружением и мониторингом, которые могут встретиться при работе с IPAM, и приведены советы, помогающие их решить.

Таблица 5.2. Общие проблемы, связанные с IPAM

Проблема	Предположительные решения
Не удается подключиться к серверу IPAM	Удостоверьтесь в том, что используемая учетная запись обладает подходящими разрешениями для доступа к консоли IPAM. Проверьте, запущена ли на сервере IPAM служба Windows Internal Database. Проверьте, запущена ли на сервере IPAM служба Windows Process Activation (Активация процессов Windows).
Невозможно извлечь данные из управляемого сервера	Удостоверьтесь в том, что для сервера значение IPAM Access Status (Состояние доступа к IPAM) установлено в Unblocked (Разблокирован) или значения DHCP RPC Access Status (Состояние доступа к DHCP RPC), DHCP Audit Share Access Status (Состояние доступа к общему аудиту DHCP), DNS RPC Access Status (Состояние доступа к DNS RPC) и Event Log Access Status (Состояние доступа к журналам событий) установлены в Not Applicable (Неприменимо). Удостоверьтесь в том, что брандмауэр не блокирует IPAM для любых серверов, которые перечислены с состоянием Blocked (Заблокирован). Следуйте инструкциям, приведенным в разделе "Конфигурирование предоставления IPAM" ранее в главе, чтобы выяснить, корректно ли сервер был подготовлен к работе.

Окончание табл. 5.2

Проблема	Предположительные решения
Не удается обнаружить серверы DNS или DHCP	Если ваш сервер DNS не расположен вместе с контроллером домена, проверьте, зарегистрировали ли вы этот сервер DNS в качестве сервера имен для зоны домена и также зарегистрировали ли суффикс DNS для домена. Кроме того, удостоверьтесь, что на сервере выполняется служба DNS Server. Если ваш сервер DHCP не удается обнаружить, проверьте, авторизован ли этот конкретный сервер DHCP для функционирования в домене, и удостоверьтесь, что на нем настроена и запущена служба DHCP Server.
Для управляемого сервера отображается состояние Not Reachable (Недостижимый)	Проверьте возможность взаимодействия с конкретным сервером и удостоверьтесь, что доступ к нему не блокируется брандмауэром или каким-то другим внешним фактором. Удостоверьтесь, что на сервере настроена и запущена служба DNS Server или DHCP Server. Проверьте корректность подготовки сервера к работе и при необходимости повторите шаги, описанные в разделе "Конфигурирование предоставления IPAM" ранее в главе.

DHCP Failover

Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol — DHCP) отвечает за автоматическое назначение IP-адресов из указанных адресных пулов (областей видимости) устройствам, подключенным к сети, которые нуждаются в идентификации. Он был неотъемлемой частью сетевых сред на протяжении многих лет, и без DHCP пришлось бы вручную поддерживать собственные списки выделенных IP-адресов. В любой среде умеренного размера это стало бы кошмаром при администрировании.

Однако особенностью традиционных реализаций DHCP в Windows Server было то, что обеспечение избыточности или высокой доступности (high availability — HA) для этой критически важной службы не всегда оказывалось простым, как должно быть.

Кластеризация или разделение областей

В Windows Server 2008 R2 для обеспечения HA необходимо было либо кластеризировать службу DHCP с применением роли Failover Clustering (Кластеризация с обходом отказа), либо развертывать два или более автономных серверов DHCP и затем разделять области адресов так, чтобы каждый сервер управлял только частью полного пула IP-адресов. Обоим вариантам были присущи проблемы. В случае роли Failover Clustering необходимо было иметь общее хранилище между всеми узлами кластера, и затраты на приобретение оборудования и конфигурирование данного варианта — особенно, если он предназначался только для службы DHCP — оказывались непомерно высокими.

При использовании метода разделения областей, обычно с двумя автономными серверами DHCP, области IP-адресов пришлось бы распределять в конфигурацию 70/30 или 50/50. Это означало, что в случае выхода из строя одного из серверов DHCP в сети оказался бы дефицит свободных IP-адресов, и отказавший сервер нужно было быстро возвращать в работоспособное состояние.

Что такое DHCP Failover?

В Windows Server 2012 при желании можно по-прежнему применять Failover Clustering или разделение областей, но в Microsoft предложили даже лучший метод обеспечения надежной работы среды DHCP — DHCP Failover.

Новая функциональность DHCP Failover позволяет настроить два сервера DHCP либо в конфигурации "активный/пассивный", известной как *горячее резервирование* (Hot standby), либо в конфигурации "активный/активный", называемой также *балансировкой нагрузки* (Load balance). 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.

DHCP Failover и IPv6

Если вы развернули IPv6 во всей сети, то знайте, что функциональность DHCP Failover в ОС Windows Server 2012 поддерживается только для адресации IPv4. Причина в том, что устройства, использующие IPv6, обычно определяют собственный адрес с применением не имеющей состояния автоконфигурации IP. Это означает, что сервер DHCP обслуживает только конфигурацию DHCP Option (Опция DHCP) и не управляет отдельными адресами IPv6. Все, что здесь понадобится сделать — это обеспечить наличие двух автономных серверов DHCP, на каждом из которых сконфигурирована в точности та же самая информация DHCP Option. В результате будет поддерживаться избыточность, которая нужна на случай, если один из серверов выйдет из строя.

Требования к развертыванию DHCP Failover

В последующих разделах кратко описаны предварительные условия, которые должны быть удовлетворены, чтобы в сети можно было развернуть DHCP Failover.

Поддержка Windows Server

Для развертывания DHCP Failover необходимо иметь два компьютера с функционирующей ОС версии Windows Server 2012 или выше. При наличии серверов DHCP, на которых установлена ОС версии Windows Server 2008 R2, Windows Server 2008 или Windows Server 2003, сначала понадобится перейти на Windows Server 2012. Для помощи в этом процессе компания Microsoft выпустила инструменты для миграции Windows Server (Windows Server Migration Tools), дополнительные сведения о которых можно получить по ссылке `http://tinyurl.com/ws2012migtools`. Кроме того, вам не удастся создать конфигурацию DHCP Failover с более чем двумя компьютерами, поскольку процесс репликации происходит только между двумя точками.

Поддержка членства в домене

Как и в случае с автономными серверами DHCP, компонент DHCP Failover можно развертывать либо на компьютерах, присоединенных к домену, либо на компью-

терах рабочей группы. В присоединенной к домену среде DHCP Failover можно устанавливать на серверы DHCP, функционирующие на серверах Domain Controller (Контроллер домена) или Domain Member (Член домена).

Установка DHCP Failover

Как только предварительные условия удовлетворены, все готово к началу установки DHCP Failover. В этом разделе мы предполагаем, что вы уже развернули серверную роль DHCP на двух компьютерах с Windows Server 2012 R2, а также сконфигурировали и активировали адресное пространство на одном из этих двух серверов DHCP.

Убедитесь, что на обоих серверах не сконфигурирована одна и та же область, поскольку если так поступить, то во время установки будет выдано сообщение об ошибке, гласящее, что для продолжения на втором сервере DHCP Failover эта область должна быть удалена.

Синхронизация часов на серверах

При установке DHCP Failover может возникнуть одно затруднение — часы на серверах должны быть синхронизированы с точностью до минуты. Если в процессе установки расхождение оказывается более одной минуты, выдается сообщение о критической ошибке, указывающее на необходимость синхронизации часов на серверах, прежде чем можно будет продолжить. Удостовериться, что с этим все в порядке, можно с помощью Active Directory или NTP (Network Time Protocol — протокол сетевого времени).

1. Войдите в систему первого компьютера Windows Server 2012 R2 (в этом примере он называется `BF1.Bigfirm.com`) с использованием учетной записи, имеющей разрешения администратора, и запустите консоль DHCP Manager (Диспетчер DHCP) оснастки MMC либо через меню DHCP диспетчера серверов, либо из консоли IPAM, как обсуждалось ранее.
2. Щелкните правой кнопкой мыши на области, для которой необходимо создать отношение DHCP Failover, и выберите в контекстном меню пункт Configure Failover (Конфигурировать обход отказа), как показано на рис. 5.29.

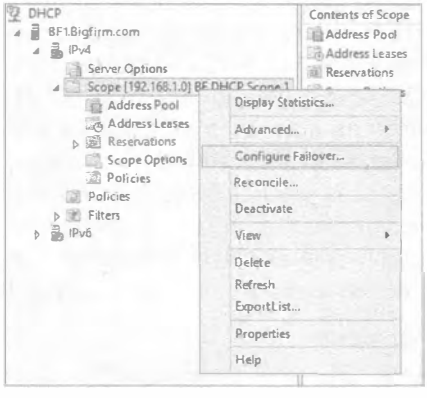


Рис. 5.29. Конфигурирование DHCP Failover

3. На экране Introduction to the DHCP Failover (Введение в DHCP Failover) мастера конфигурирования обхода отказа (Configure Failover Wizard) в разделе Available Scopes (Доступные области) удостоверьтесь в выборе нужной области и щелкните на кнопке Next (Далее).
4. На экране Specify The Partner Server To Use For Failover (Указание партнерского сервера для использования при обходе отказа) щелкните на кнопке Add Server (Добавить сервер) и выберите второй сервер (в примере он называется `BF2.Bigfirm.com`) из списка авторизованных серверов DHCP. Щелкните на кнопке OK, а затем на кнопке Next.
5. Сконфигурируйте новое отношение DHCP Failover, как показано на рис. 5.30, и шелкните на кнопке Next. Ниже описаны опции конфигурации.
   - Relationship Name (Имя отношения). Это дружественное имя для отношения DHCP Failover.
   - Maximum Client Lead Time (Максимальное время влияния на клиента). Эта настройка определяет максимальный период времени, на который один сервер может продлить аренду DHCP для клиента сверх времени, известного серверу обхода отказа. Стандартное значение составляет 1 час, и это время также определяет, сколько активный сервер ожидает, пока партнерский сервер неактивен, прежде чем брать под свой полный контроль область DHCP.
   - Mode (Режим). В этом раскрывающемся списке доступны на выбор варианты Load Balance (Балансировка нагрузки) для конфигурации "активный/активный" и Hot Standby (Горячее резервирование) для конфигурации "активный/пассивный".

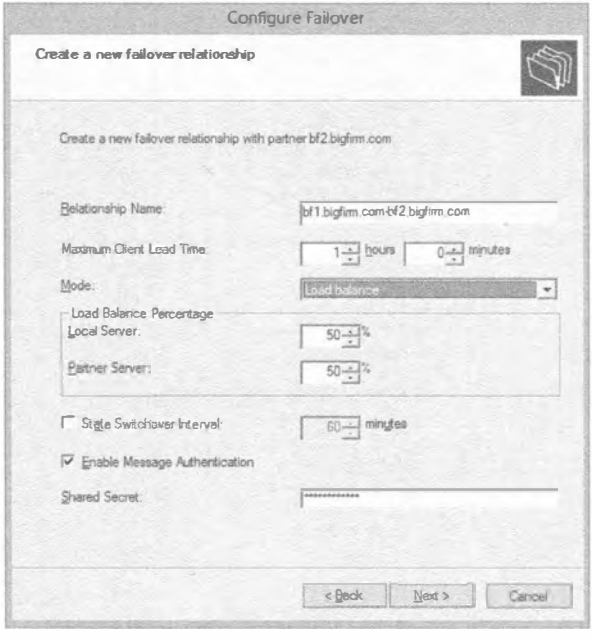


Рис. 5.30. Конфигурирование отношения DHCP Failover

- Load-balance Percentage (Процент балансировки нагрузки). Значения в этом разделе определяют процентное отношение диапазона IP-адресов, резервируемого каждым сервером в отношении. Стандартными значениями являются 50/50.
- State Switchover Interval (Интервал переключения состояния). По умолчанию этот флажок не отмечен, т.е. администратор должен вручную сообщить DHCP Failover, что сервер находится в состоянии отключенного партнерства. Если же флажок отмечен, то активный сервер DHCP будет автоматически переводить своего партнера в состояние отключенного партнерства, когда ему не удается взаимодействовать с ним на протяжении указанного периода времени.
- Enable Message Authentication (Включить аутентификацию сообщений). Этот флажок включает аутентификацию трафика репликации при обходе отказа между партнерами.
- Shared Secret (Общий пароль). Если флажок Enable Message Authentication отмечен, в этом поле понадобится указать пароль для аутентификации трафика.

6. Подтвердите корректность настроек и затем щелкните на кнопке Finish (Готово), чтобы завершить работу мастера.
7. Далее должно открыться диалоговое окно с индикатором хода работ и указанием на успешное выполнение конфигурирования. Щелкните в нем на кнопке Close (Закрыть), чтобы завершить процесс.
8. Для проверки работоспособности процесса просмотрите второй сервер DHCP. Вы должны теперь видеть в представлении IPv4 область, которая была выбрана для обхода отказа (рис. 5.31).

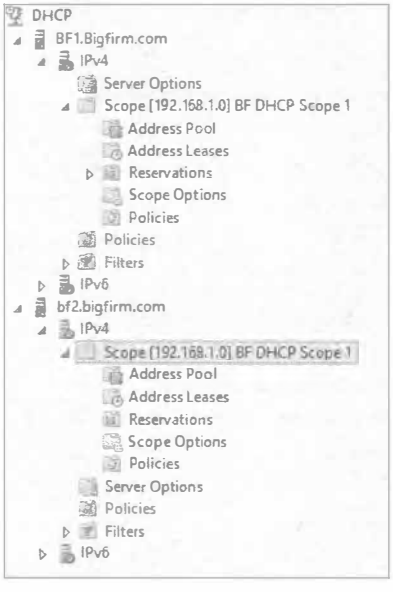


Рис. 5.31. Синхронизация области DHCP

DHCP Failover и PowerShell

Для работы с этим новым компонентом в Windows Server 2012 предусмотрены семь новых командлетов PowerShell:

```
Add-DhcpServerv4Failover
Add-DhcpServerv4FailoverScope
Get-DhcpServerv4Failover
Set-DhcpServerv4Failover
Remove-DhcpServerv4Failover
Remove-DhcpServerv4FailoverScope
Invoke-DhcpServerv4FailoverReplication
```

Перечисленные командлеты можно применять для быстрого развертывания, конфигурирования или даже удаления компонента DHCP Failover. За дополнительными сведениями и примерами синтаксиса обращайтесь в официальный блог разработчиков продукта Microsoft DHCP по следующей ссылке: `http://tinyurl.com/ws2012dhcpfailposh`.

Резюме

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?

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

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?

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)

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))

Глава 6

DNS и преобразование имен в Windows Server 2012 R2

Компьютеры взаимодействуют друг с другом с использованием IP-адресов, либо IPv4, либо IPv6. Тем не менее, большинству людей трудно запомнить IP-адрес излюбленного веб-сайта или файлового сервера. Людям нравится применять дружественные текстовые имена. Таким образом, для преобразования этих дружественных имен компьютеров в назначенные им IP-адреса реализуются системы имен. Система доменных имен (Domain Name System — DNS) — это система имен, используемая серверами Windows Server 2012 R2. Система DNS не только помогает пользователям легко идентифицировать устройства, она является обязательной для множества служб, таких как Active Directory, чтобы клиенты и серверы могли взаимодействовать с контроллерами доменов.

В этой главе вы изучите следующие темы:

- фундаментальные компоненты и процессы DNS;
- конфигурирование DNS для поддержки среды Active Directory;
- управление и устранение неполадок с преобразованием имен DNS для внутренних и внешних имен.

Понятие роли DNS Server

Система DNS существовала на протяжении десятилетий до того, как в Microsoft разработали свою первую редакцию DNS в Windows NT 4.0. Существует много разновидностей реализаций DNS, которые поддерживают компоненты и процессы, определяющие DNS. В этом разделе мы раскроем концепции системы доменных имен от Microsoft и покажем, как она применяется в операционных системах Windows.

Система DNS реализована внутри ОС Windows Server 2012 R2 для управления преобразованием имен в IP-адреса. После установки на сервере службе DNS понадобится взаимодействовать с другими серверами имен DNS, что достигается с

использованием множества разных методов, таких как переадресация, корневые подсказки и делегирование. Служба DNS будет также поддерживать базы данных, называемые *зонами*, для внутреннего домена Active Directory или других пространств имен. Компьютерам домена необходимо будет опрашивать эту службу DNS, поэтому вам придется сконфигурировать отдельные компьютеры, чтобы обеспечить эффективное и быстрое преобразование имен.

Windows Server 2012 R2 и предыдущие выпуски ОС Windows Server предлагают встроенную роль DNS Server (DNS-сервер). Система Windows Server 2012 R2 DNS совместима со старыми версиями DNS вплоть до Windows Server 2003; однако версии, более ранние, чем Windows Server 2008, не поддерживают IPv6 и функционируют только с адресами IPv4.

Ниже приведена краткая сводка по фундаментальным концепциям DNS, имеющим отношение к данной главе.

- **Имя хоста (hostname).** Это (дружественное) имя компьютера. Согласно стандартам DNS, оно может иметь длину до 255 символов. Имя хоста эквивалентно первому имени компьютера, например, `EC01`.
- **Пространство имен (namespace).** Это имя домена, хотя и не обязательно домена Active Directory. Пространство имен представляет собой логический набор хостов, обозначенных именем, которое управляется набором серверов имен. Это эквивалент второго имени компьютера; все они являются частью одного семейства. Например, `Bigfirm.com` — пространство имен для хостов в домене `Bigfirm.com`.
- **Полное имя домена (Fully Qualified Domain Name — FQDN).** Имя FQDN — это имя хоста, к которому добавлено пространство имен домена, такое как `EC01.Bigfirm.com`.
- **Файл HOSTS.** Это текстовый файл, в котором имена хостов статически отображаются на IP-адреса. Файл `HOSTS` расположен в `c:\windows\system32\drivers\etc` для стандартных установок Windows Server 2012 R2 и может применяться в качестве простейшей альтернативы DNS-серверу для преобразования имен в небольших средах. Тем не менее, не пытайтесь управлять крупными производственными средами с помощью записей в статическом файле `HOSTS`, поскольку это быстро превратится в кошмар администрирования!
- **Сервер имен (name server).** Это DNS-сервер, который будет преобразовывать имена FQDN в IP-адреса. Серверы имен также управляют пространствами имен для указанных доменов. Они будут обрабатывать запросы для этих пространств имен, поступающие от клиентов DNS через сеть.
- **Иерархическая структура имен (hierarchical naming structure).** Пространство имен создано, поэтому левой частью имени является подмножеством правой части имени, как можно видеть в FQDN. С учетом этого сервера имен могут начинать с правой части имени, а ответы от серверов имен направят его на корректный сервер имен для заданного пространства имен. Например, как показано на рис. 6.1, `Ec01.Ecoast.Bigfirm.com` является именем FQDN для сервера в домене `Ecoast.Bigfirm.com`. Данный домен в действительности представляет собой подмножество, или *поддомен*, находящееся под контролем домена

Bigfirm.com. То же самое можно сказать о Bigfirm.com в отношении имени домена верхнего уровня .com. Достоинство заключается в том, что вы можете запросить у сервера доменных имен .com, где находится сервер имен Bigfirm.com. То же самое можно делать для сервера Ecoast.Bigfirm.com и т.д. Имя FQDN направляет запрос правильному серверу имен посредством процесса, который называется *рекурсией*.

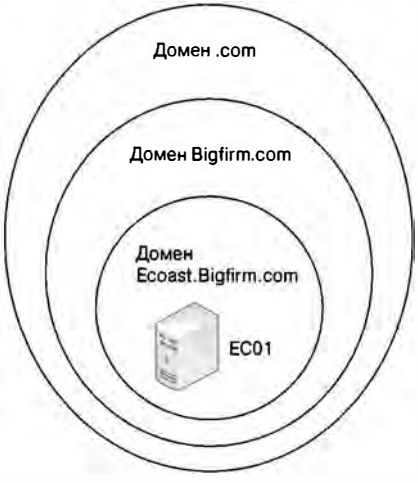


Рис. 6.1. Иерархическое именование DNS

- **Рекурсия (recursion).** Это управляемый сервером процесс преобразования имени FQDN. Если сервер не может распознать имя FQDN посредством собственной информации, он отправит запрос другим серверам имен. В процесс рекурсии вовлечены корневые серверы и серверы имен доменов. Корневые серверы находятся на верхушке иерархической структуры имен. Корневые серверы содержат списки серверов имен, которые управляют именами доменов верхнего уровня, такими как .com, .gov и .edu. Серверы доменов верхнего уровня управляют реестром поддоменов, расположенных в иерархии ниже доменов верхнего уровня. Например, серверы имен для поддомена Sybex.com зарегистрированы на серверах домена .com. Ниже описаны действия, которые происходят при поступлении запроса имени (рис. 6.2).

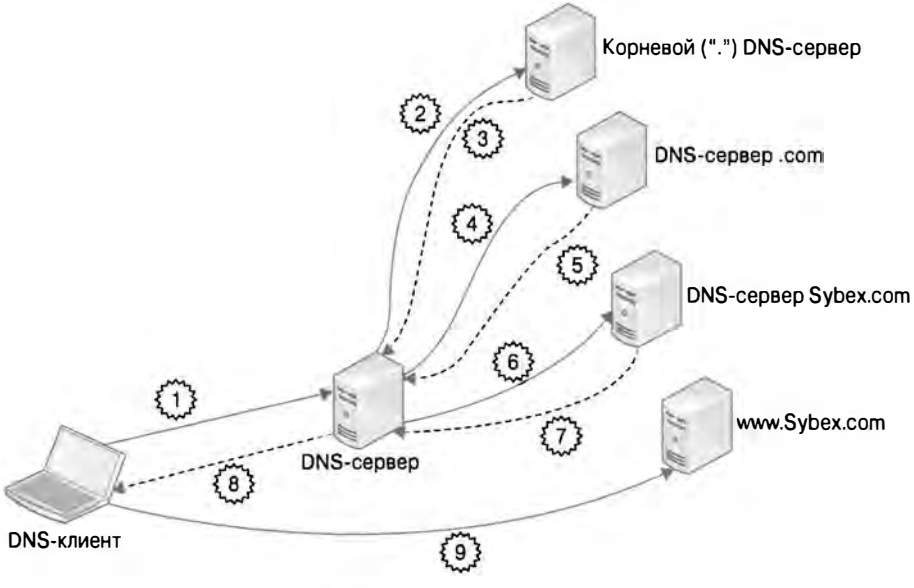


Рис. 6.2. Процесс рекурсии в DNS

1. Клиент DNS запрашивает у DNS-сервера имя, подобное `www.Sybex.com`.
2. Через процесс рекурсии DNS-сервер запрашивает у корневых серверов серверы имен домена `.com`.
3. Корневые серверы предоставляют список серверов имен для домена `.com`.
4. DNS-сервер запрашивает у серверов домена `.com` серверы имен для `Sybex.com`.
5. Он получает еще один список серверов имен для домена `Sybex.com`.
6. DNS-сервер запрашивает у предоставленных серверов имен FQDN-имя `www.Sybex.com`.
7. DNS-сервер `Sybex.com` выдает IP-адрес веб-сервера исходному DNS-серверу.
8. Исходный DNS-сервер передает IP-адрес клиенту.
9. Располагая этим IP-адресом, клиент подключается к веб-серверу `www.Sybex.com`.

- **Делегирование (delegation).** Это означает разрешение другому серверу имен управлять поддоменом заданного пространства имен. Например, серверы имен `Bigfirm.com` могут делегировать управление пространством имен `Ecoast.Bigfirm.com` другому серверу.
- **Переадресация (forwarding).** Это является альтернативой процессу рекурсии. Переадресация представляет собой ответвленный запрос к другому серверу имен внутри сети. Сервер, на который была произведена переадресация, получает ответ и ретранслирует его исходному серверу имен.
- **Итерация (iteration).** Это управляемый клиентом процесс преобразования имени FQDN. Если клиент получает отрицательный ответ от сервера имен, он будет запрашивать другой сервер имен.
- **Система имен NetBIOS (NetBIOS naming system).** Эта унаследованная система имен использовалась главным образом в старых сетях Microsoft NT 4.0. Тем не менее, ее процессы по-прежнему являются частью современных операционных систем Windows, особенно когда применяются компьютеры, входящие не в домен, а в рабочую группу.
- **Записи служб (service records).** Записи служб (SRV) представляют собой записи внутри пространства имен DNS, предназначенные для преобразования службы в имя хоста. Они являются неотъемлемой частью поддержки DNS для Active Directory.
- **Динамическое обновление DNS (dynamic DNS update).** Динамическое обновление DNS (Dynamic DNS — DDNS) — это процесс, который позволяет клиентам DNS регистрировать свои имена хостов в назначенном пространстве имен, таком как DHCP. Это сокращает необходимость ручного ввода записей администраторами в базы данных серверов имен. Динамическое обновление DNS является еще одной неотъемлемой частью поддержки DNS для Active Directory.

Установка DNS

Роль DNS для Windows Server 2012 R2 может быть развернута в нескольких отличающихся конфигурациях, зависящих от выбранного сценария. Можно установить автономный DNS-сервер на компьютере, не присоединенном к домену, или же можно развернуть его либо на серверах-членах домена, либо на серверах, являющихся контроллерами домена Active Directory. Какой бы сценарий не был выбран, установка роли DNS проста. Сначала мы покажем, что понадобится сделать для ручного развертывания DNS на компьютере, не присоединенном к домену, в автономной конфигурации. Затем мы объясним, как автоматически сконфигурировать DNS для интеграции с Active Directory, чтобы обеспечить гладкое выполнение преобразования имен внутри среды домена.

Конфигурирование автономного DNS-сервера

Самое важное: вы должны выделить серверу, на котором хотите установить роль DNS, статический IP-адрес, поскольку попадать в движущуюся цель клиенту DNS будет очень непросто! Если на рабочем столе вы нажмете комбинацию клавиш <Ctrl+R>, а затем введете **ncpa.cpl** и нажмете <Enter>, откроется окно Network Connections (Подключения к сети). В этом окне можно щелкнуть правой кнопкой на сетевом адаптере и выбрать в контекстном меню пункт Properties (Свойства), чтобы открыть окно конфигурирования. Если вы дважды щелкнете на элементе Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 ((TCP/IPv4))), откроется диалоговое окно Internet Protocol Version 4 (TCP/IPv4) Properties (Свойства протокола Интернета версии 4 (TCP/IPv4)). В нем можно назначить статический IP-адрес, как показано на рис. 6.3.

После назначения статического IP-адреса вы должны добавить первичный DNS-суффикс, такой как `Bigfirm.com`, в диалоговом окне Advanced TCP/IPv4 Settings (Расширенные настройки TCP/IPv4), как показано на рис. 6.4.

Рис. 6.3. Назначение статического IP-адреса

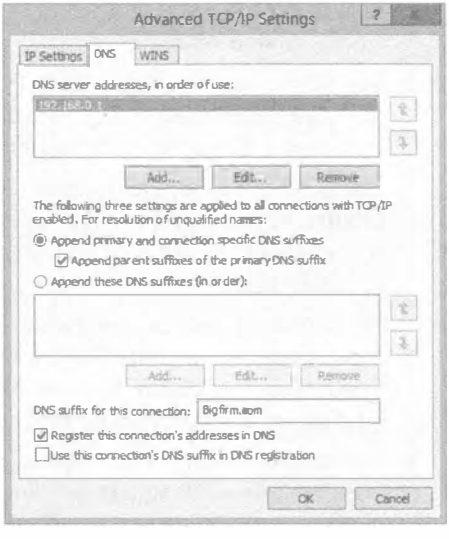


Рис. 6.4. Добавление DNS-суффикса

Добавление первичного DNS-суффикса требуется не всегда. Он модифицируется автоматически, когда компьютер присоединяется к домену. Если по плану сервер должен функционировать как часть рабочей группы (в рассматриваемом примере так и есть), первичный DNS-суффикс необходимо добавить, чтобы другие DNS-серверы могли находить этот сервер внутри структуры DNS, а служба DNS была корректно сконфигурирована во время установки.

После указания статического IP-адреса и DNS-суффикса на сервере, не присоединенном к домену, выполните перечисленные ниже шаги для установки роли DNS.

1. Откройте диспетчер серверов щелкните на элементе Dashboard (Управляющая панель) и затем щелкните на ссылке Add Roles and Features (Добавить роли и компоненты), как показано на рис. 6.5.

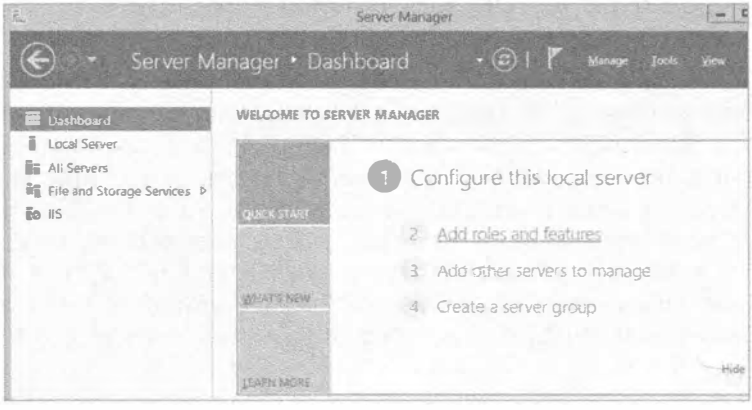


Рис. 6.5. Добавление роли DNS

2. На экране Before You Begin (Прежде чем начать) мастера добавления ролей и компонентов (Add Roles and Features Wizard) щелкните на кнопке Next (Далее), чтобы продолжить.
3. На экране Select Installation Type (Выбор типа установки) выберите 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) мастера выберите переключатель Select a Server from the Server Pool (Выбрать сервер из пула серверов) и удостоверьтесь в том, что ваш сервер отмечен; щелкните на кнопке Next.
5. На экране Select Server Roles (Выбор серверных ролей) мастера отметьте флажок возле роли DNS Server (DNS-сервер) и, если после выбора роли DNS Server откроется диалоговое окно, щелкните в нем на кнопке Add Features (Добавить компоненты), как показано на рис. 6.6.
6. На всех последующих экранах щелкайте на кнопке Next, пока не достигнете экрана Confirm Installation Selections (Подтверждение выбранных настроек для установки). Проверьте, все ли выбранные настройки корректны, и щелкните на кнопке Install (Установить), чтобы начать процесс установки.

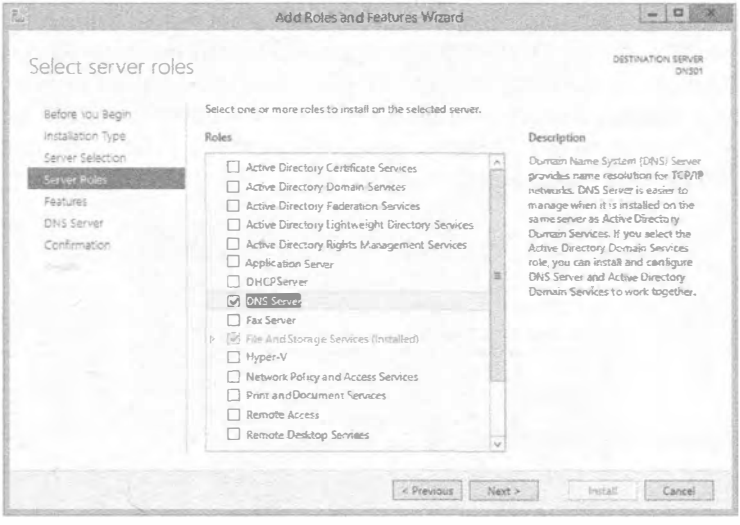


Рис. 6.6. Выбор роли DNS Server

7. После завершения установки роли DNS Server щелкните на кнопке Close (Закрыть) для закрытия окна мастера.

Установка роли подобным образом приводит к созданию изолированного сервера имен DNS, который взаимодействует только с корневыми серверами Интернета. Он может поддерживать среду локальной вычислительной сети для преобразования имен Интернета, но на этом и все. Система доменных имен использует другие серверы имен для преобразования имен по всей структуре DNS. По этой причине вы должны будете сконфигурировать сервер на взаимодействие с другими DNS-серверами, которые существуют во внутренней сети. Хотя настройка DNS-сервера в автономной конфигурации без присоединения к домену может иметь свои преимущества (вроде его развертывания в средах, где управление многочисленными статическими файлами `HOSTS` на серверах становится мучительным), действительная мощь системы Windows Server 2012 R2 DNS проявляется при ее применении с Active Directory.

Интеграция с другими DNS-серверами

В разделе "Понятие роли DNS Server" упоминалось, что существуют разные методы для преобразования имен DNS, такие как переадресация, рекурсия, делегирование и итерация. Эти методы относятся к интеграции с другими DNS-серверами. Прежде чем начать, вспомните, что итерация по существу управляется клиентом. Если DNS-сервер не имеет ответа, клиент перейдет на другой DNS-сервер. Сервер или клиент можно настроить только на итерацию, но это не делается по умолчанию и редко реализуется. Другие три приема — переадресация, рекурсия и делегирование — предусматривают взаимодействие запрашиваемого DNS-сервера с другими DNS-серверами.

Рекурсия — это главный процесс, происходящий в Интернете. Запрашиваемый DNS-сервер начинает с самого верха и проходит вниз по ссылкам, получаемым от каждого DNS-сервера, с которым он взаимодействует. На серверах Windows DNS

серверы верхнего уровня перечислены на вкладке Root Hints (Корневые подсказки) диалогового окна свойств DNS-сервера (рис. 6.7). Это окно можно отобразить в оснастке DNS Management (Управление DNS), щелкнув правой кнопкой мыши на значке сервера и выбрав в контекстном меню пункт Properties (Свойства). По умолчанию список Name servers (Серверы имен) на вкладке Root Hints заполнен "действующими" DNS-серверами из Интернета.

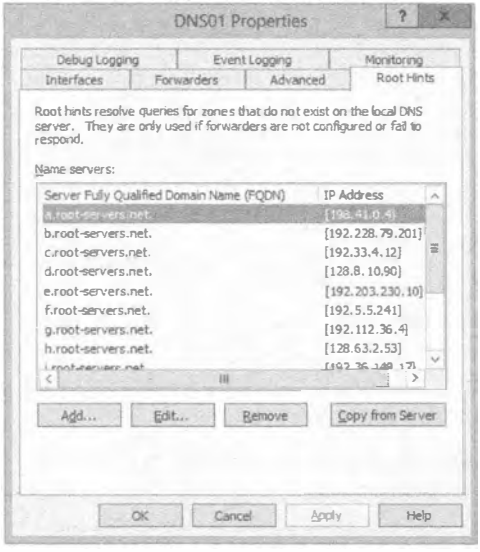


Рис. 6.7. Вкладка Root Hints

Этот список находится в текстовом файле по имени `cache.dns`, хранящемся в папке `c:\windows\system32\dns`, содержимое которого приведено на рис. 6.8.

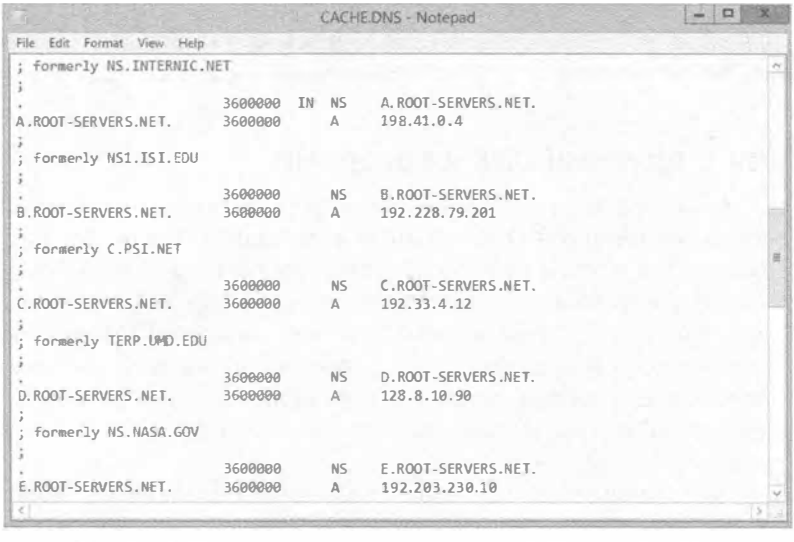


Рис. 6.8. Список корневых подсказок в файле `cache.dns`

В единственной среде домена Active Directory это можно оставить в том виде, как есть. DNS-серверы могут использовать эти ссылки для распознавания пространств имен, основанных на Интернете, таких как `Sybex.com`, когда клиент их запрашивает. В более крупных средах корневые подсказки на других серверах DNS можно удалить и полагаться на поддержку одного сервера в преобразовании имен DNS из внешней среды. В сущности это мог бы быть кеширующий DNS-сервер для внутренней структуры.

В то время как корневые подсказки управляют запросами, следующими вверх по иерархической структуре DNS, делегирование управляет запросами, проходящими вниз. В рассматриваемом примере DNS-серверам, которые управляют пространством имен `.com`, делегируется контроль над зарегистрированными поддоменами вроде `Sybex.com`. Делегирование представляет собой просто список этих серверов. Таким образом, сервер имен `.com` отправляет список серверов имен DNS-серверу, ищущему пространство имен `Sybex.com`.

В среде Windows делегирование можно увидеть в действии с множеством доменов Active Directory. При наличии домена Active Directory по имени `Bigfirm.com` вы имеете связанное с ним пространство имен DNS под названием `Bigfirm.com`. Вы могли бы создать домен Active Directory по имени `Ecoast.Bigfirm.com`. Вместо того чтобы хранить все пространства имен DNS на DNS-сервере `Bigfirm.com`, вы можете делегировать пространство имен DNS под названием `Ecoast.Bigfirm.com` другому DNS-серверу.

На рис. 6.9 такое делегирование демонстрируется в консоли управления DNS. В DNS-сервере по имени `DC01` поддерживается зона прямого просмотра `Bigfirm.com`. Поддомен `Ecoast`, представленный значком с папкой серого цвета с текстовым файлом поверх него, содержит только запись сервера имен для `EC1.Ecoast.Bigfirm.com` с его IP-адресом.

Сервер пересылки — это еще один DNS-сервер для обработки ответвленного запроса. Когда серверу не удается преобразовать имя DNS, он может переадресовать запрос другому DNS-серверу, а не проходить по корневым подсказкам.

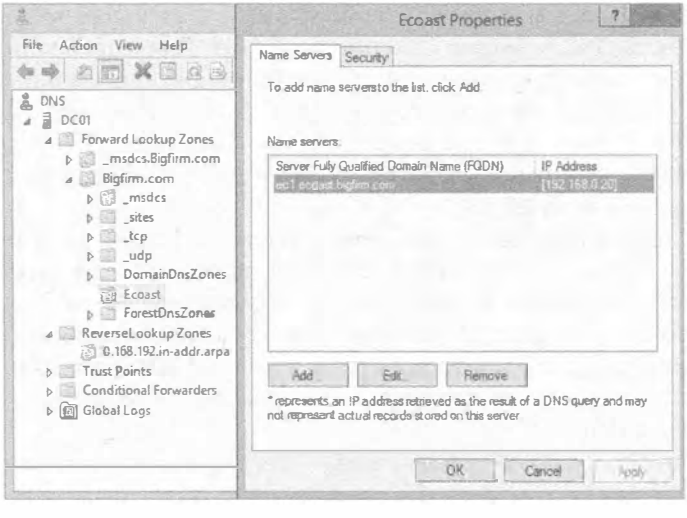


Рис. 6.9. Делегированный домен для `Ecoast.Bigfirm.com`

Во внутренней среде DNS серверы пересылки могут применяться для распознавания других пространств имен. Например, DNS-серверу `EC1.Ecoast.Bigfirm.com` необходимо распознавать серверы `Bigfirm.com` и другие пространства имен, поэтому на вкладке Forwarders (Серверы пересылки) окна его свойств указан сервер пересылки (рис. 6.10).

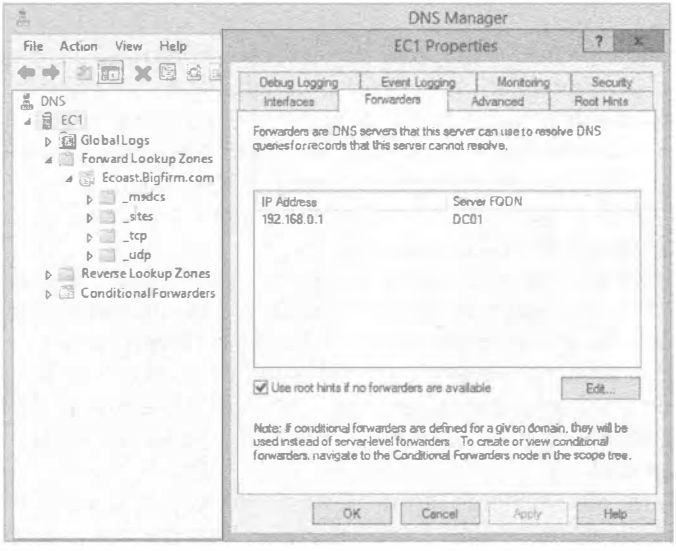


Рис. 6.10. Вкладка Forwarders

На рис. 6.10 обратите внимание на флажок Use root hints if no forwarders are available (Использовать корневые подсказки, если нет доступных серверов пересылки). В более крупной среде его можно не отмечать, если необходимо централизовать DNS-запросы, основанные на Интернете. Кроме того, взгляните на текст, касающийся серверов условной пересылки.

Серверы условной пересылки имеют собственный узел в дереве областей внутри левой панели окна DNS Manager (Диспетчер DNS). Для управления распознаванием конкретного пространства имен сервер условной пересылки может направлять запросы определенному серверу. На рис. 6.11 видно, что сервер условной пересылки был настроен для пространства имен `Otherdomain.local`. В результате любые запросы к этому пространству имен будут передаваться DNS-серверу `OS01.Otherdomain.local`.

Серверы условной пересылки создаются путем щелчка правой кнопкой мыши на папке Conditional Forwarder (Сервер условной пересылки) в консоли управления DNS и выбора в контекстном меню пункта New Conditional Forwarder (Новый сервер условной пересылки). Откроется диалоговое окно New Conditional Forwarder (Новый сервер условной пересылки), которое предоставит вариант репликации настройки другим контроллерам домена в домене или лесе с использованием разделов каталога приложений Active Directory.

Переадресация также может применяться для обработки запросов, основанных на Интернете, вместо использования корневых подсказок.

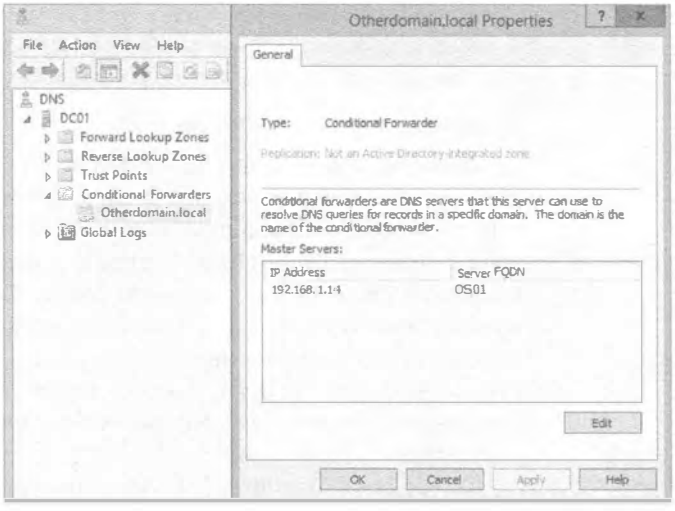


Рис. 6.11. Сервер условной пересылки

Мы предпочитаем поступать так в небольших средах, обслуживаемых поставщиком Интернет-услуг посредством кабеля или цифровой абонентской линии (Digital Subscriber Line — DSL). Эти поставщики Интернет-услуг имеют собственные DNS-серверы, которые находятся в конфигурации маршрутизатора. Таким образом, они указаны как серверы пересылки во внутренних серверах DNS. Хотя корневые подсказки и могут работать в такой среде, мы считаем прием с переадресацией более надежным. Вдобавок он ограничивает коммуникации внутреннего DNS-сервера заданным внешним источником.

Интеграция с другими DNS-серверами может завершить конфигурирование роли DNS. Один DNS-сервер может получать запросы и затем отправлять их другим DNS-серверам. После того, как DNS-сервер получит ответ, он может кешировать информацию в течение определенного периода времени, который в Windows Server 2012 R2 по умолчанию установлен равным одному часу. Такая конфигурация называется *сервером только для кеширования*. Если сервер предназначен для управления пространством имен, вы должны добавить зоны.

Реализация зон для управления пространствами имен

Зона — это база данных для пространства имен. В Интернете имеется DNS-сервер, который управляет пространством имен `Sybex.com`. Если вам необходим IP-адрес для `www.sybex.com`, то для нахождения ответа этот DNS-сервер будет просматривать свою зону (базу данных). Таким образом, для управления пространствами имен на серверах DNS можно создать зоны.

На серверах Windows DNS существуют зоны четырех типов:

- стандартная основная зона;
- стандартная дополнительная зона;
- зона, интегрированная с Active Directory;
- зона-заглушка.

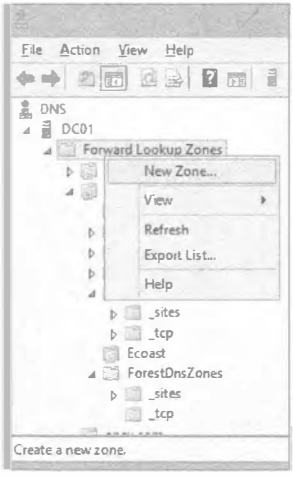


Рис. 6.12. Создание новой зоны

Зона-заглушка не управляет пространством имен и больше похожа на сервер условной пересылки. Все типы зон обсуждаются в последующих разделах.

Стандартная основная зона

Серверы имен были спроектированы для централизации преобразования имен в сети. Первоначально DNS-сервер отвечал на запросы, основываясь на своем текстовом файле `HOSTS`. По существу это то, что в Microsoft называют *стандартной основной зоной*. Стандартная основная зона представляет собой текстовый файл, в котором сервер поддерживает записи для заданного пространства имен. Это то, что характеризует реализацию Windows DNS как *стандартную*. Характеристика *основная* относится к репликации.

Во времена Windows NT существовал один ведущий контроллер домена, называемый *главным контроллером домена* (primary domain controller — PDC), который управлял всеми операциями записи в свою базу данных. Остальные операции управлялись *резервными контроллерами домена* (backup domain controller — BDC), которые представляли собой копии только для чтения. В терминах DNS основные зоны означают, что имеется только один хозяин, и им является данный сервер. Другие DNS-серверы могут содержать лишь копии этой зоны, предназначенные только для чтения; они являются дополнительными зонами.

Зона создается с помощью мастера новой зоны (New Zone Wizard), который можно запустить, щелкнув правой кнопкой мыши на папке Forward Lookup Zones (Зоны прямого просмотра) в диспетчере DNS и выбрав в контекстном меню пункт New Zone (Новая зона), как показано на рис. 6.12.

Мастер новой зоны запросит перечисленную ниже информацию.

- Пространство имен или имя домена, такое как `Primaryzone.local`.
- Имя текстового файла, который по умолчанию имеет расширение `.dns`.
- Возможность динамического обновления DNS. Мы обсудим это в разделе "Динамическое обновление DNS" далее в главе.

После создания зоны можно просмотреть содержимое текстового файла, который хранится в папке `c:\windows\system32\dns` (рис. 6.13). Созданные для примеров дополнительные записи CNAME и A находятся в конце файла.

Стандартная дополнительная зона

Стандартная дополнительная зона — это копия только для чтения стандартной основной зоны или зоны, интегрированной с Active Directory. Репликация выполняется посредством процесса переноса зоны, который конфигурируется через свойства зоны. На серверах Windows DNS стандартная настройка предусматривает разрешение переносов зоны только на зарегистрированные серверы имен этой зоны, что можно видеть на вкладке Zone Transfers (Переносы зоны), представленной на рис. 6.14.

Рис. 6.13. Файл стандартной основной зоны

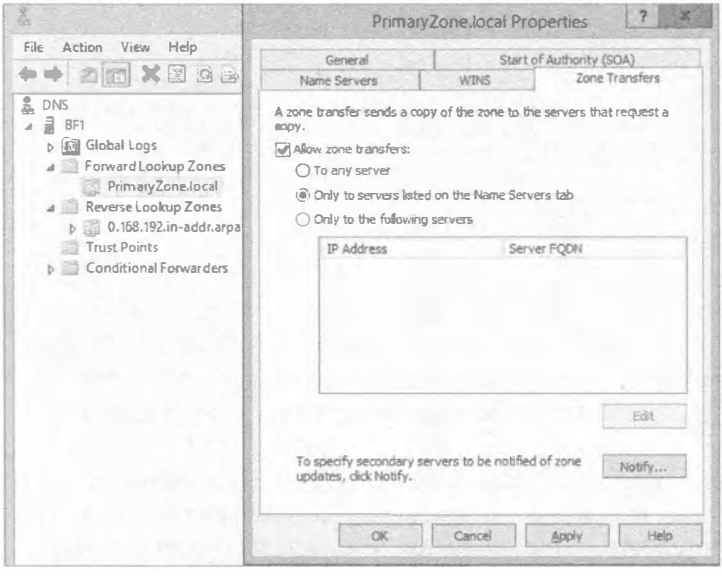


Рис. 6.14. Вкладка Zone Transfers для основной зоны

Чтобы разрешить репликацию на сервер имен `EC1.Ecoast.Bigfirm.com`, его необходимо добавить в список Name servers (Серверы имен) на вкладке Name Servers (Серверы имен), как показано на рис. 6.15.

Теперь можно запустить мастер New Zone Wizard для создания стандартной дополнительной зоны на сервере `EC1`. Это потребует указания IP-адреса сервера-хозяина, у которого может запрашиваться перенос зоны. Он не обязательно должен быть DNS-сервером со стандартной основной зоной. Результатом будет успешный перенос зоны на `EC1` (рис. 6.16).

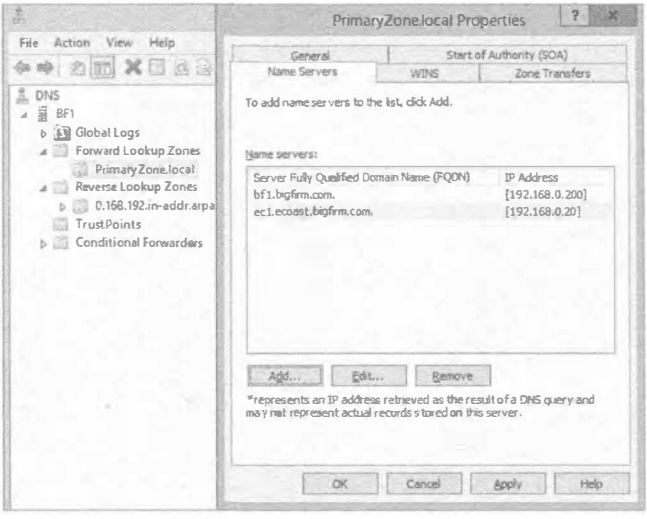


Рис. 6.15. Вкладка Name Servers для основной зоны

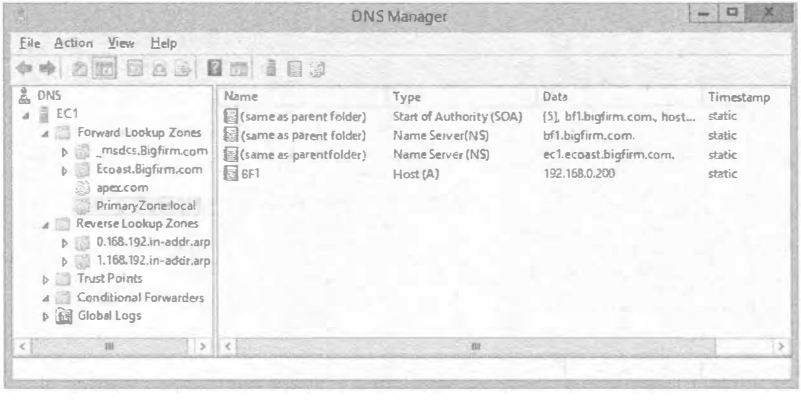


Рис. 6.16. Созданная стандартная дополнительная зона

Процесс переноса зоны не отличается особой сложностью. Сервер для основной зоны отслеживает вносимые им изменения, назначая каждому из них серийный номер. Когда сервер для дополнительной зоны контактирует с сервером для основной зоны, он проверяет этот серийный номер в записи Start of Authority (Начало зоны). Если серийный номер на сервере для дополнительной зоны не совпадает, значит, наступил момент для репликации изменений. Это просто текстовый способ заталкивания информации в базу данных. Ранние версии DNS поддерживали репликацию AXFR (все переносы зоны), которая означала, что на сервер для дополнительной зоны реплицировалась вся зона целиком. В результате по линии передавался намного больший объем трафика. В Windows DNS поддерживается репликация IXFR (инкрементные переносы зоны), при которой реплицируются только изменения. Кроме того, в DNS поддерживается уведомление серверов для дополнительных зон, что сокращает время ожидания для запуска репликации.

Зона, интегрированная с Active Directory

Зона, интегрированная с Active Directory, является преобладающей реализацией серверов Windows DNS. Присутствие в ее названии Active Directory говорит о многом.

- Во-первых, записи DNS хранятся в базе данных Active Directory, а не в текстовом файле.
- Во-вторых, зоны реплицируются всем другим контроллерам домена Active Directory в домене, а не посредством процесса переноса зоны.

Поскольку в базе данных Active Directory применяется репликация с несколькими хозяевами, изменения могут вноситься в зону DNS на любом контроллере домена, и они будут реплицироваться на другие контроллеры домена. Благодаря интеграции DNS с Active Directory, связка ролей DNS и контроллера домена становится нормой. За дополнительными сведениями о процессе репликации обращайтесь в главу 22.

Подобно стандартным зонам, зона, интегрированная с Active Directory, может быть создана с помощью мастера New Zone Wizard. На экране Zone Type (Тип зоны) мастера (рис. 6.17) отметьте флажок Store the zone in Active Directory (Хранить зону в Active Directory).

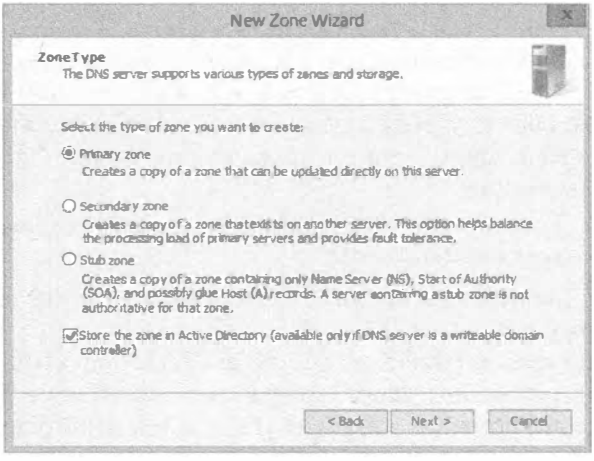


Рис. 6.17. Создание зоны, интегрированной с Active Directory

На экране Active Directory Zone Replication Scope (Область действия репликации зоны Active Directory) мастера (рис. 6.18) на выбор предусмотрены четыре опции: на уровне леса, на уровне домена, на уровне домена (совместимого с Windows 2000) и хранение базы данных зоны в указанном специальном разделе каталога приложений (последняя опция по умолчанию обычно недоступна, но в следующем абзаце мы объясним, как сделать ее доступной). Первые две опции приводят к размещению базы данных в автоматически созданном стандартном разделе каталога приложений: один для леса и один для домена, членом которого является контроллер домена. Местоположением, совместимым с Windows 2000, является раздел домена базы данных Active Directory, поэтому база данных зоны будет реплицироваться только контроллерам этого домена.

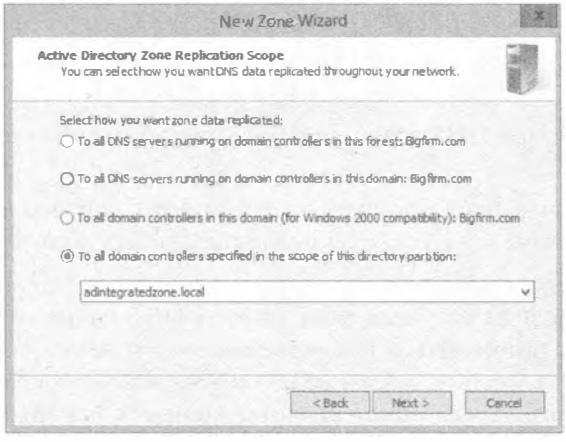


Рис. 6.18. Экран Active Directory Zone Replication Scope

Если вы хотите создать специальные разделы каталога приложений, такие как отображаемый в последней опции на рис. 6.18, то вам придется воспользоваться либо утилитой `DNSCmd`, либо командлетом `Add-DNSServerDirectoryPartition` в PowerShell. Оба средства встроены в Windows Server 2012 R2 и предоставляют возможность управления указанными типами специальных разделов. В сеансе PowerShell с разрешениями администратора введите показанную ниже команду, чтобы создать новый раздел каталога приложений для упомянутой ранее зоны, интегрированной с Active Directory. Имя раздела не обязательно должно совпадать с именем зоны; тем не менее, применение того же самого имени способствует лучшему пониманию конфигурации:

```
C:\Users\administrator.BIGFIRM>Add-DNSServerDirectoryPartition
  -Name "adintegratedzone.local"
```

После того, как новый раздел создан, ему можно назначить зону, интегрированную с Active Directory (см. рис. 6.18).

Затем также с помощью PowerShell можно сконфигурировать другие контроллеры домена для поддержки зоны. Давайте предположим, что на сервере `EC1`, который является контроллером домена `Ecoast.Bigfirm.com`, необходимо добавить следующие две зоны Active Directory:

- зону `adintegratedzone.local`, которая помещена в собственный раздел каталога приложений;
- зону обратного просмотра для подсети 192.168.0.0, которая помещена в общий раздел леса.

Для начала добавьте сервер в список на вкладке Name Servers окна свойств желаемых зон подобно тому, как было показано на рис. 6.15 ранее в главе.

Затем запустите следующий командлет для вывода доступных разделов на сервере `EC1`:

```
C:\Users\administrator.BIGFIRM>Get-DNSServerDirectoryPartition
```

В выводе можно заметить наличие четырех разделов каталога приложений. Первый из них — это специальный раздел, созданный недавно, который сервер вов-

лек в совместное использование. Второй является разделом каталога приложений домена, который совместно используется всеми контроллерами домена, отличными от Windows 2000, внутри домена `Bigfirm.com`. Третий раздел предназначен для домена `Ecoast.Bigfirm.com`. Четвертый раздел ориентирован на все контроллеры доменов в рамках леса доменов. Сервер `EC1` уже вовлечен в совместное использование этих двух разделов.

Использование зон-заглушек для интеграции с другими DNS-серверами

Зона-заглушка — это еще одно усовершенствование, впервые появившееся в Windows Server 2003. В версии Windows Server 2012 R2 концепции и функциональность зоны-заглушки не изменились, и по существу она представляет собой дополнительный метод для интеграции с другими DNS-серверами. В зоне-заглушке перечислены только серверы имен для заданного пространства имен. Она не имеет никакого контроля над зоной, так что она указывает только на то, какой сервер мог бы поддерживать преобразование имен для пространства имен. Подобно серверам условной пересылки, зона-заглушка предоставляет ответвленное взаимодействие с авторитетным DNS-сервером. Эти зоны также могут реплицироваться между контроллерами домена.

Мастер New Zone Wizard настраивает зону-заглушку со следующими параметрами:

- тип зоны Stub (Зона-заглушка);
- необязательное хранение в Active Directory с заданным разделом каталога приложений;
- пространство имен зоны, такое как `Apex.com`;
- DNS-сервер, который поддерживает это пространство имен.

После создания зоны-заглушки можно просмотреть ее содержимое (рис. 6.19). В нем присутствует запись Start of Authority для пространства имен, запись Name Server (Сервер имен) для пространства имен и запись Host (Хост) для сервера имен.

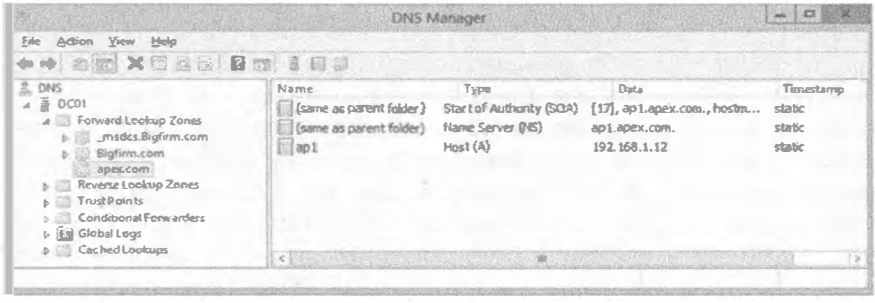


Рис. 6.19. Пример зоны-заглушки

Использование зон обратного просмотра для увеличения безопасности

Вы можете заметить, что созданные зоны находятся в папке Forward Lookup Zones (Зоны прямого просмотра) внутри консоли управления DNS. При прямом просмотре клиент предоставляет полное имя домена (FQDN), а DNS-сервер возвращает IP-адрес. При обратном просмотре делается противоположное: клиент предоставляет IP-адрес, а DNS-сервер возвращает имя FQDN.

Вас может интересовать, для чего это может потребоваться? Основные причины связаны с безопасностью. Представьте себе взломщика, который настроил вредоносную службу для прослушивания DNS-запросов к именам FQDN, начинающимся с `www.`, внутри сети. Когда эта служба получает запрос, она автоматически отправляет клиенту поддельный ответ с IP-адресом веб-сервера взломщика, который загрузит черви, вирусы, "троянские кони" еще до того, как пользователь узнает, что произошло. Если веб-браузер можно было бы сконфигурировать на выполнение обратного просмотра для предоставленного IP-адреса, то он мог бы сравнивать результат с запрошенным именем и в случае несовпадения не подключаться к веб-серверу.

В качестве реального примера работы такого обратного просмотра при преобразовании имен можно привести службу SMTP в Windows. Эта служба позволяет выполнять обратный просмотр для подключений к серверу. Серверы SMTP предоставляют при взаимодействии свои доменные имена, а при подключении указывается адрес TCP/IP. Затем может быть выполнен обратный просмотр для проверки, соответствуют ли имена адресам, как должно быть.

Команда `NsLookup` иллюстрирует использование обратного просмотра. Как показано ниже, эта команда запущена в интерактивном режиме для сервера, который не имеет записи указателя (PTR) в зоне обратного просмотра. Обратите внимание, что стандартный сервер обозначен как `UnKnown`. В этом случае запросы DNS могут быть ненадежными.

```
C:\Users\Administrator.BF1>Nslookup
Default Server:  UnKnown
Address:         192.168.0.10
```

Если в зоне обратного просмотра создана запись PTR, то вывод команды `NsLookup` выглядит гораздо лучше. Легко заметить, что в выводе присутствует имя сервера:

```
C:\Users\Administrator.BF1>Nslookup
Default Server:  BF1.bigfirm.com
Address:         192.168.0.10
```

Для корректного конфигурирования зон обратного просмотра внутри сети необходимо понимать, как работает обратное преобразование. Адрес IPv4 представляется в десятичной точечной нотации с помощью четырех октетов — x.y.w.z. Адрес IPv6 похож, но в нем применяются шестнадцатеричные числа, и их намного больше. В обоих случаях процесс обратного преобразования один и тот же. DNS-сервер, получающий запрос, изменяет порядок следования числе в IP-адресе. Таким образом, запрос имени FQDN для IP-адреса x.y.w.z становится z.w.y.x, а в конце добавляется `.in-addr.arpa`. Затем DNS-сервер пытается преобразовать FQDN-имя `z.w.y.x.in-addr.arpa` подобно обычному имени FQDN. Преобразование начинается с домена верхнего уровня `.arpa` и проходит вниз к серверам имен `in-addr.`, при этом каждое десятичное значение становится поддоменом пространства имен справа от него.

В небольших средах, которые включают только одну подсеть, эта подсеть может быть представлена единственной зоной. В рассматриваемом примере подсеть 192.168.0.0 является одной зоной (рис. 6.20). При создании зоны обратного просмотра мастер New Zone Wizard запрашивает имя подсети.

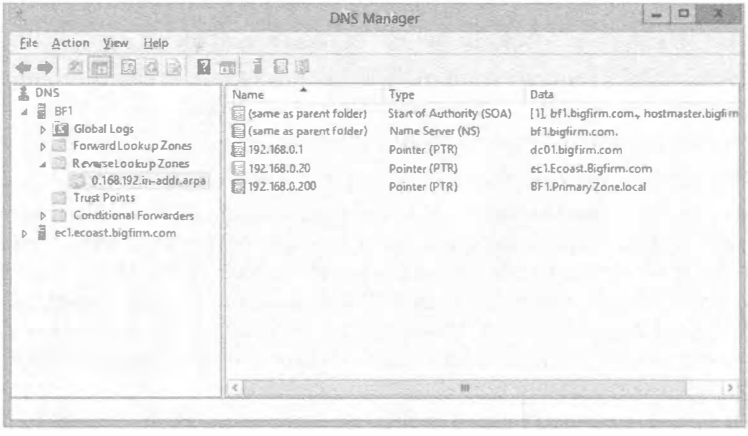


Рис. 6.20. Пример зоны обратного просмотра

В более крупных средах, имеющих несколько подсетей, потребуется создать зону для октета с наибольшим приоритетом, а октеты с меньшими приоритетами должны быть представлены как поддомены или делегированные поддомены. Например, если крупная организация использует схему частной IP-адресации 10.0.0.0, то в ней можно создать зону обратного просмотра для доменного имени `10.in-addr.arpa`.

Когда происходят динамические обновления, поддомены будут автоматически создаваться для следующего октета от 1 до 254, а записи PTR будут заполняться подпапками структуры. В определенный момент поддомены можно делегировать другому множеству DNS-серверов, вроде контроллеров домена, находящихся внутри сайта, который содержит эти подсети. Затем записи PTR можно зарегистрировать в соответствующей зоне, представляющей подсеть.

На рис. 6.21 видно, что на сервере `BF1` была создана зона `10.in-addr.arpa`. Если нужно, чтобы подсети 10.11.0.0 управлялись другим сервером, понадобится делегировать 11 поддоменов. Это было делегировано серверу `EC1`. Внутри него действительная подсеть 10.11.12.0 также представлена как делегированный поддомен.

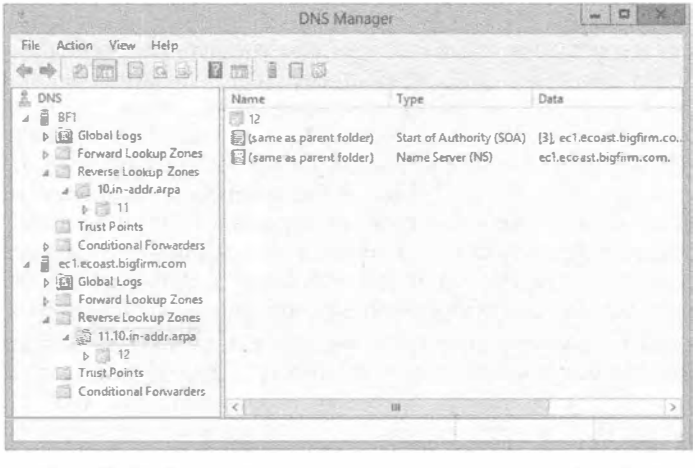


Рис. 6.21. Зона обратного просмотра для сети 10.0.0.0

Циклический перебор и упорядочение сетевых масок

На вкладке Advanced (Дополнительно) окна свойств DNS-сервера имеется несколько отмеченных флажком, два из которых приведены ниже:

- Enable round robin (Включить циклический перебор)
- Enable netmask ordering (Включить упорядочение сетевых масок)

Циклический перебор (round robin). Это прием балансировки сетевой нагрузки (network load balancing — NLB) "для бедняков". Если вы зарегистрировали несколько записей хостов с одним и тем же именем, но разными IP-адресами, то DNS-сервер будет отвечать последовательно с отличающимся IP-адресом для каждого запроса, начиная с самого меньшего IP-адреса. Хотя такой прием не распределяет клиентскую нагрузку равномерно или интеллектуально по доступным хостам, он все же предоставляет возможность некоторой балансировки между серверами.

Упорядочение сетевых масок (netmask ordering). Подобно циклическому перебору, при упорядочении сетевых масок используется множество записей хостов с одинаковым именем, но разными IP-адресами. Вместо выбора случайным образом выбирается запись, которая определена математически как более близкая. Это делается путем сравнения подсетей. Такой прием хорош при наличии географически разделенных хостов и клиенту необходимо взаимодействовать с хостом, находящимся в его сети. Таким образом, когда применяются географически разнесенные серверы, вы должны решить, какой метод лучше избрать. Упорядочение сетевых масок сохранит время отклика на минимальном уровне из-за более короткого маршрута. Циклический перебор более равномерно распределит нагрузку, если клиенты сконцентрированы в одном месте.

Однако эти процессы доступны в случае применения Windows Server 2012 R2 с Windows 7 или Windows 8. Стек TCP/IP для IPv6 и IPv4, "когда возможно", будет выполнять процесс похожий на упорядочение сетевых масок, который называется *стандартным выбором адресов*. Это значит, что он получает IP-адреса от DNS-сервера и самостоятельно решает, какой из них лучше использовать.

Подобно большинству конфигураций, это можно переопределить с помощью объекта групповой политики, указанного в следующем параметре реестра:

```
Hkey_Local_Machine\System\CurrentControlSet
\Services\Tcpip\Parameters\OverrideDefaultAddressSelection
```

Значение `1` отключает стандартный выбор и разрешает произвольный выбор циклических серверов NLB.

Увидеть эффект от всего этого можно при использовании циклического перебора географически разделенных серверов. Например, среда с сайтом для восстановления после аварий может предлагать два сервера, которые выполняют одну и ту же службу, но расположены на разных сайтах. В таком случае для загрузки данных доступны два сервера FTP. DNS-сервер сконфигурирован на предоставление двух IP-адресов для одного имени `ftp.Bigfirm.com`. Циклический перебор обеспечит последовательную обработку записей. Даже когда один из серверов FTP прекращает функционирование из-за аварийной ситуации, у клиентов по-прежнему сохранится подключаемость к `ftp.Bigfirm.com`. (Время от времени будет выбираться IP-адрес нерабочего сервера, но после повторного подключения поток данных возобновится.)

Тем не менее, если включено упорядочение сетевых масок или стандартный выбор адресов, то клиенты могут никогда не получить IP-адрес функционирующего сервера FTP. Выбор будет делать либо DNS-сервер, либо клиент. Таким образом, этот сценарий наталкивает на применение проверенного временем правила: "тестировать, тестировать, тестировать". Проверяйте, какие серверы используются в нормальном сценарии, и что происходит в аварийной ситуации.

Типы записей

Теперь, когда базы данных настроены для извлечения информации клиентами, необходимо добавить в них записи. Как упоминалось ранее, Dynamic DNS (DDNS) — это процесс, который позволяет DNS-клиентам регистрировать свои имена хостов в назначенном пространстве имен, таком как DHCP, и это приводит к добавлению записей для компьютеров Windows внутри среды. Тем не менее, некоторые записи по-прежнему придется добавлять вручную, равно как и проверять корректность записей, созданных динамически. Для зоны DNS доступно свыше 25 типов записей. В этом разделе мы рассмотрим наиболее распространенные типы записей в рамках реализации Windows DNS.

Записи хостов и указателей

Записи хостов (A) и указателей (PTR) наиболее распространены в зонах прямого просмотра и зонах обратного просмотра, соответственно. В записи A указывается имя хоста компьютера и возвращается IP-адрес. В записи PTR указывается IP-адрес и возвращается имя FQDN. Эти записи может потребоваться создать для компьютеров, не имеющих доступного протокола обновления DDNS.

Записи псевдонимов

Записи псевдонимов (CNAME) создаются для определения второго имени компьютера. В записи CNAME указывается имя и возвращается имя FQDN, назначенное компьютеру. Эти записи полезны в случае замены сервера с опубликованным именем, которое клиенты применяют для доступа к приложениям или службам. Без необходимости в переконфигурировании после замены клиенты по-прежнему будут иметь доступ через псевдоним.

Записи обмена почтой

Записи обмена почтой (mail exchanger — MX) предназначены для коммуникаций по протоколу SMTP. Почтовые серверы запрашивают записи MX для взаимодействия с получающим сервером SMTP в данном пространстве имен. Обычно записи MX настраиваются во внешней зоне DNS. Тем не менее, для специализированных приложений они могут потребоваться и внутренне. Записи MX нужно имя FQDN сервера SMTP и значение приоритета.

Приоритет помогает определить, с какой записью MX контактировать сначала, а с какой впоследствии, если записей несколько. Чем меньше значение, тем выше приоритет. Запомните это как "приоритет номер один".

Предположим, что у вас есть основной SMTP-сервер и SMTP-сервер типа смарт-хост (smart host), предназначенный для поддержки получения электронной почты, когда основной сервер недоступен. Вам необходимо создать записи MX для обоих серверов. Основной SMTP-сервер должен иметь меньшее значение приоритета, чем смарт-хост, например 10 и 20, соответственно. Когда основной SMTP-сервер недоступен, взаимодействие производится со смарт-хостом.

Записи служб

Записи служб (SRV) являются "знатным шаманом" для реализаций Windows DNS. Без записей SRV рабочие станции и серверы не смогли бы находить контроллеры доменов.

Сами по себе записи SRV имеют дело только с пятью значениями.

- **Имя службы.** Стандартное значение, обычно предваренное символом подчеркивания, такое как `_gc` или `_ladp`. Оно является эквивалентом имени хоста и будет присоединено к имени FQDN службы.
- **Имя FQDN сервера.** Сервер, который предоставляет службу.
- **Порт.** Порт TCP или UDP, на котором доступна служба. Протокол обозначается своим зарегистрированным именем, например, `_TCP`.
- **Приоритет.** Работает точно так же, как в записях MX — имеет "приоритет номер один".
- **Вес.** Используется для разрешения конфликтов с приоритетами. Оставьте его равным `0`, если вас это не заботит.

Вы обнаружите изобилие записей SRV в зоне Windows DNS, которая поддерживает Active Directory. Они находятся в папках поддоменов, поскольку именам служб назначаются разные имена FQDN. Запрашиваемая служба описывается с помощью имени FQDN наподобие `_gc._tcp.bigfirm.com`. Записи SRV можно видеть на рис. 6.22.

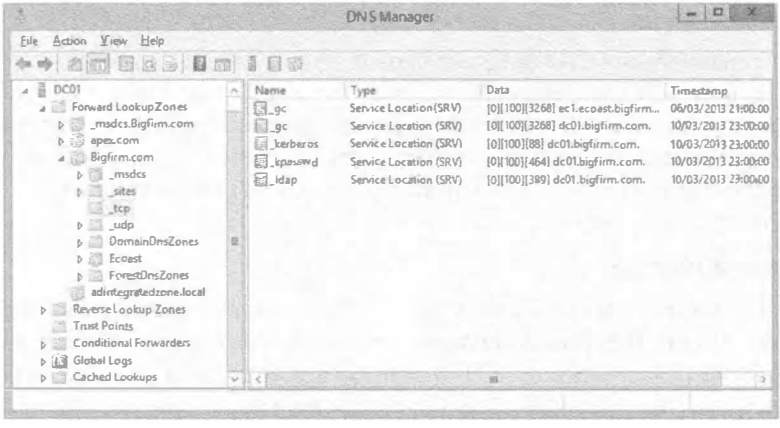


Рис. 6.22. Пример записей SRV

Записи начала зон

Запись начала зоны (Start of Authority — SOA) в единственном экземпляре присутствует в каждой зоне. Она определяет информацию о том, какой DNS-сервер управляет этой зоной, а также параметры, касающиеся того, каким образом трактовать распознанные записи. Запись SOA содержит несколько значений, которые не должны изменяться при редактировании записи. Редактирование производится на вкладке Start of Authority (SOA) (Запись начала зоны (SOA)) в окне свойств зоны (рис. 6.23).

Ниже описаны поля, находящиеся на вкладке Start of Authority (SOA).

- Serial Number (Серийный номер). Номер ревизии файла зоны. На самом деле он имеет значение для стандартных основных зон, т.к. репликация Active Directory поддерживает собственный серийный номер. Дополнительные зоны могут сравнивать с ним свои номера, чтобы выяснять, актуальна ли информация в них. Если информация не актуальна, необходим перенос зоны.

- Primary Server (Основной сервер). Сервер, на котором зона была изначально настроена. Если вы хотите изменить способ обновления зон в среде посредством репликации, можете переключать основной сервер на дополнительный сервер и наоборот.
- Responsible Person (Ответственное лицо). Предположительно это должен быть адрес электронной почты лица, администрирующего зону. Обратите внимание, что символ @ заменяется точкой (.). Если хотите кого-то по-настоящему свести с ума, можете указать здесь его электронный адрес.
- Refresh Interval (Интервал обновления). Период времени, в течение которого дополнительный сервер может ожидать до того, как начнет попытки проверить наличие изменений на основном сервере. В этот момент он сравнивает серийный номер из записи SOA со своим номером. По умолчанию интервал обновления составляет 15 минут. Внутри самой записи это значение указывается в секундах.
- Retry Interval (Интервал повтора). Период времени, в течение которого дополнительный сервер ожидает до того, как повторить попытку после отказавшего переноса зоны. По умолчанию интервал повтора составляет 10 минут и также внутри самой записи указывается в секундах.
- Expires After (Истекает после). Период времени, в течение которого дополнительный сервер может продолжать отвечать на запросы в этой зоне после того, как перенос зоны был выполнен. По умолчанию составляет один день. Внутри самой записи это значение также указывается в секундах и равно 86 400.
- Minimum (Default) TTL (Минимальное (стандартное) время TTL). Период времени, в течение которого запись должна находиться в кеше или, другими словами, значение времени существования (Time To Live — TTL). По умолчанию составляет один час, или 3 600 секунд.

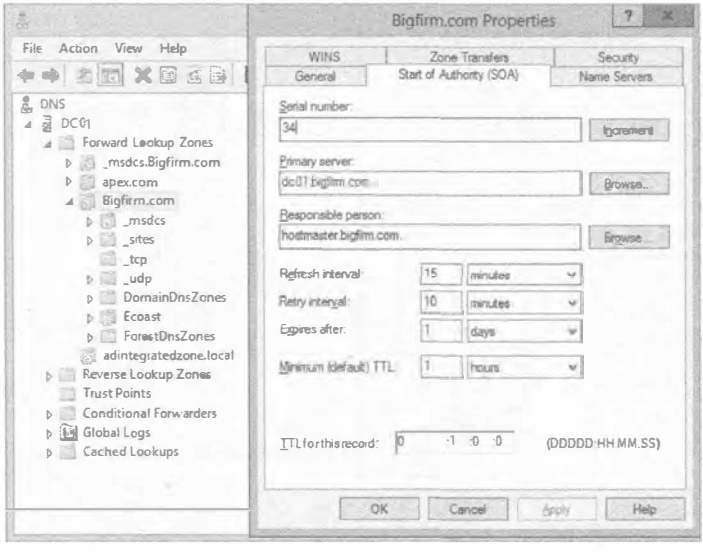


Рис. 6.23. Вкладка Start of Authority (SOA)

Записи серверов имен

Записи серверов имен (NS) перечисляют серверы, которые могут отвечать на запросы для этой зоны. В зоне должна присутствовать, по меньшей мере, одна такая запись. Подобно записи SOA, запись NS модифицируется на вкладке Name Servers (Серверы имен) окна свойств зоны, которая была показана ранее на рис. 6.15. Единственным обязательным значением в записи NS является имя FQDN сервера. В нижней части вкладке Name Servers вы заметите короткое примечание, указывающее на то, что IP-адрес представляет собой извлеченное значение.

Управление клиентами DNS и преобразованием имен

Вы можете прийти к выводу, что каждый компьютер является клиентом DNS. Служба DNS — это жизненно важный компонент сети, даже если Active Directory не входит в ее состав. Вдобавок он представляет собой единственный метод для перехода на ваши избранные веб-сайты в Интернете, такие как `www.Sybex.com`.

В операционных системах Windows есть две области, касающиеся клиентов DNS: преобразование имен хостов и регистрация имен хостов и IP-адресов через динамические обновления DNS.

Преобразование имен хостов

Процесс преобразования имен на компьютере Windows делится на две части. Данный процесс настолько важен, что мы будет называть его "жизненным циклом". Одной частью, которая близка к исчезновению, является NetBIOS, в другой — DNS. (Вы могли бы назвать ее процессом имени хоста, но большинство администраторов называют его DNS.) Этот цикл состоит из набора шагов, которые компьютер должен предпринять для преобразования заданного имени (рис. 6.24).

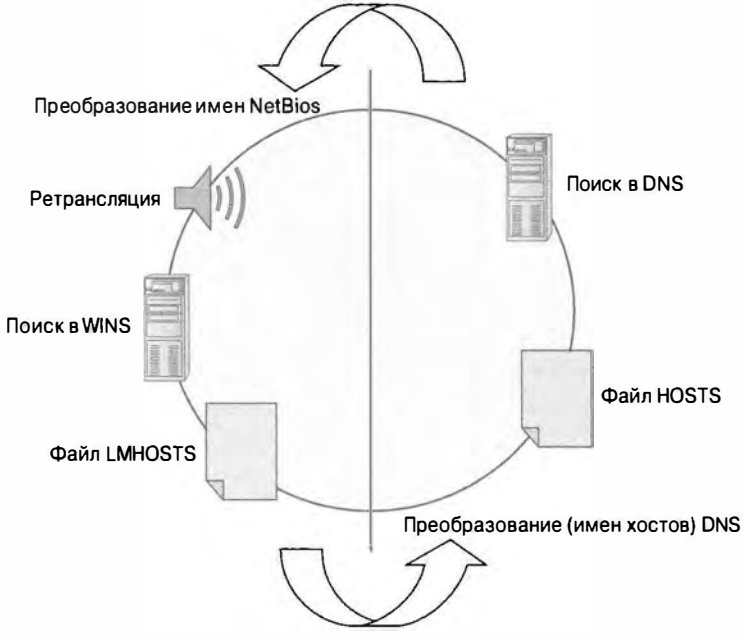


Рис. 6.24. Жизненный цикл

Процесс NetBIOS предусматривает выполнение следующих шагов.

1. Ретрансляция имени в сети и ожидание, ответит ли кто.
2. Поиск имени в WINS.
3. Поиск имени в файле LMHOSTS. Это еще один текстовый файл, аналогичный файлу HOSTS, который находится в том же самом месте: c:\windows\system32\drivers\etc. Вместо имен хостов в нем перечислены имена NetBIOS.

Порядок следования первых двух шагов можно изменять, особенно через сервер DHCP. Шаг с ретрансляцией или шаг с поиском в WINS может быть опущен. По умолчанию в Windows Server 2012 R2 сначала производится поиск имени посредством WINS, а затем с помощью ретрансляции. Однако поиск в файле LMHOSTS всегда выполняется последним.

Список шагов для процесса DNS короче.

1. Поиск имени в файле HOSTS.
2. Поиск имени в DNS.

Порядок следования шагов в процессе DNS настройке не поддается, но можно изменить поведение просмотра DNS. С тем, что поиск имени сначала производится в файле HOSTS, связаны как положительные, так и отрицательные моменты. Если получить доступ к DNS-серверу невозможно или требуется переадресовать преобразование имени в другое место, то редактирование файла HOSTS дает замечательные результаты. Если же файл HOSTS содержит устаревшие или вредоносные записи, то устранение неполадок DNS может оказаться затруднительным.

Процесс преобразования имен циркулирует по обеим частям до тех пор, пока не будет получен IP-адрес. Кроме того, имеется выбор с чего начинать — NetBIOS или DNS. В основном это зависит от приложения. Старые унаследованные приложения Windows рассматривают имя как относящееся к NetBIOS. Приложения, основанные на TCP/IP, считают его именем хоста. Это влияет на способ преобразования имен и является частью операционных систем Windows.

Примерами могут служить команды net view и ping.

Команда net view существует со времен LAN Manager, когда все полагалось целиком на NetBIOS. Если вы попытаетесь подключиться к серверу с применением указанной команды, то увидите, что имя сервера заносится в кеш имен NetBIOS. Содержимое этого кеша можно отобразить с помощью команды nbtstat -c. Для очистки кеша предназначена команда nbtstat -R.

```
rem Просмотр кеша имен NetBios
C:\Users\Administrator.BF1>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.0.10] Scope Id: []
    No names in cache

rem Доступ к общим ресурсам на сервере bfsc1
C:\Users\Administrator.BF1>net view \\bfsc1
Shared resources at \\bfsc1
```

```
Share name Type  Used as Comment
-------------------------------------------------------------------------------
NETLOGON   Disk          Logon server share
SALES      Disk
SYSVOL     Disk          Logon server share
Users      Disk
The command completed successfully.

rem Повторный просмотр кеша имен NetBios
C:\Users\Administrator.BF1>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.0.10] Scope Id: []
               NetBIOS Remote Cache Name Table
       Name          Type          Host Address     Life [sec]
       ------------------------------------------------------------
       BFSC1    <00>  UNIQUE        192.168.0.11     600
```

При пинговании сервера используется процесс DNS, т.к. команда `ping` является утилитой TCP/IP. Вы можете убедиться, что эта утилита распознает сервер через DNS, отобразив содержимое кеша DNS с применением команды `ipconfig /displaydns`. Кеш DNS очищается с помощью команды `ipconfig /flushdns`.

```
rem Очистка кеша DNS
C:\Users\Administrator.BF1>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator.BF1>ping BFSC1
Pinging BFSC1.bigfirm.com [192.168.0.11] with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Ping statistics for 192.168. 0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator.BF1>ipconfig /displaydns
Windows IP Configuration
    BFSC1
    ----------------------------------------
    Record Name . . . . . : BFSC1.bigfirm.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1185
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168. 0.11
```

Такие сведения помогают решить, каким образом поддерживать процесс преобразования имен DNS для клиентов и устранить либо поддерживать (при необходимости) имена NetBIOS. Процесс NetBIOS потребляет излишние циклы ЦП. В случае корректной конфигурации сервера и клиентов DNS поддержку преобразования имен NetBIOS можно отключить или, по крайней мере, свести к минимуму.

Конфигурирование клиентов

Конфигурации DNS и NetBIOS можно просмотреть в окне свойств протокола IP для сетевого подключения. Конфигурация NetBIOS находится на вкладке WINS. На рис. 6.25 показана вкладка WINS со стандартными настройками.

Рис. 6.25. Вкладка WINS

По умолчанию включен поиск в файле `LMHOSTS` и выбрано использование настроек NetBIOS из сервера DHCP. По умолчанию файл `LMHOSTS` пуст. Было бы неплохо отключить поиск в этом файле, поскольку вредоносное ПО могло в прошлом занести в него данные.

Настройки NetBIOS получаются от сервера DHCP. Области видимости сервера DHCP имеют опцию под названием NBT Node Type (046) (Тип узла NBT (046)). Эта настройка предписывает первые два шага процесса NetBIOS в жизненном цикле. Четыре опции задаются десятичным значением:

- только ретрансляция: “b-узел”, 1
- только обращение к WINS: “p-узел”, 2
- сначала ретрансляция, а затем обращение к WINS: “m-узел”, 4
- обращение к WINS, а затем ретрансляция: “h-узел”, 8

H-узел лучше всего подходит для сети, полагающейся на NetBIOS, т.к. он сокращает объем обмена в среде, поддерживающей WINS. При отсутствии доступных серверов WINS компьютер может, по крайней мере, получить какой-то ответ в подсети, например, дома или в рабочей группе. Если сервер DHCP не сконфигурирован с этим значением, применяется стандартная конфигурация, установленная в ОС. В Windows Server 2012 R2 по умолчанию используется h-узел, т.е. гибридный (hybrid) режим.

Для сред Active Directory лучше отключать NetBIOS, поскольку это сокращает объем дополнительного обмена и количество процессов. Кроме того, это помогает снизить

угрозы безопасности со стороны ботов, которые ищут в сетях компьютеры с целью атаки с применением данной системы имен. Однако прежде чем отключать NetBIOS, удостоверьтесь в отсутствии слабых мест в системе преобразования имен DNS.

Конфигурация клиента DNS находится на вкладке DNS окна свойств сети, показанной на рис. 6.26. Вполне очевидно, что обязательным является IP-адрес DNS-сервера. Подключение должно осуществляться к ближайшему серверу, как правило, на контроллере домена внутри локального сайта. Рекомендуется указать также дополнительный DNS-сервер.

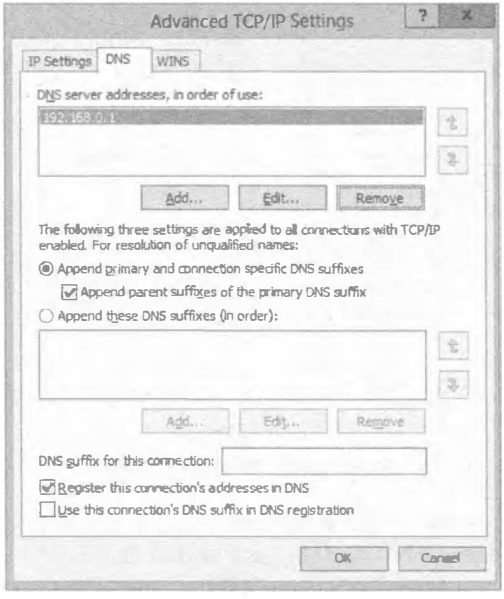


Рис. 6.26. Вкладка DNS

Средняя часть вкладки DNS имеет отношение к неполным именам. Это имя хоста без его "второго имени", суффикса DNS (такого как `BFSC1`, используемого ранее в примере команды `ping`). DNS-серверу необходимо имя FQDN, поэтому перед отправкой запроса клиент DNS добавляет суффиксы DNS, т.е. "второе имя". Основной суффикс DNS отображается на странице System (Система) панели управления, в области Computer Name (Имя компьютера). Он управляется автоматически ОС, когда компьютер присоединяется к домену, поэтому заботиться об этом суффиксе не придется. Дополнительные суффиксы могут понадобиться в крупных средах, но для сред с одним доменом стандартных настроек вполне достаточно. Добавлять суффикс DNS подключения нужно только в редких случаях.

Все это становится спорным в случае регулярного применения имен FQDN. Используйте имена FQDN серверов при конфигурировании приложений, папок или переадресации папок, равно как при написании сценариев, которые подключают сетевые диски. Уловили смысл? Вдобавок применение имен FQDN обходит процесс NetBIOS. Приложения могут определить разницу между именами NetBIOS и FQDN и прибегнуть к DNS, когда они распознают FQDN.

Динамическое обновление DNS

Чтобы сделать процесс преобразования имен DNS надежным, понадобится перечислить все компьютеры в зонах DNS. В прошлом система DNS требовала от системных администраторов работы в полную смену, т.к. нужно было вводить постоянно растущее количество записей для их сети. Для сокращения объема работы системных администраторов в Microsoft при создании ОС Windows NT нашли динамическое решение через WINS и затем перешли на DNS, когда стал доступным протокол обновлений Dynamic DNS (DDNS). Сам процесс довольно прост.

1. Клиент запрашивает запись SOA для пространства имен с основным суффиксом DNS. Это сообщит, может ли сервер принимать DDNS. То же самое делается для зоны обратного просмотра, с которой связан IP-адрес сервера.
2. Клиент отправляет запрос DDNS этому серверу.

В записях Start of Authority стандартных зон указан основной сервер. В зонах, интегрированных с Active Directory, контроллер домена, получающий запрос, модифицирует запись SOA с таким именем. Поскольку он может изменять содержимое базы данных Active Directory, нет нужды выискивать контроллер домена, находящийся где-то в другом месте. Если процесс обновления терпит неудачу, производится поиск других серверов имен для выполнения обновлений.

На вкладке DNS с протоколом обновлений DDNS связаны два флажка в самом низу (см. рис. 6.26). Имеется возможность зарегистрировать имя с основным суффиксом DNS или с суффиксом подключения. Второй флажок по умолчанию не отмечен.

Странно то, что служба клиента DNS не выполняет обновления DDNS. Это делает служба клиента DHCP. Это напоминает нам богатый событиями день, когда один из нас отключил службу клиента DHCP на контроллере домена. Он наивно полагал, что эта служба не нужна, т.к. имеется статический IP-адрес. Как уже упоминалось, процесс DDNS используется контроллерами домена с целью предоставления записей SRV для Active Directory. В конечном итоге клиенты не смогли найти контроллер домена, т.к. для него не было никаких записей SRV. К счастью, все это происходило в испытательной среде.

Существуют еше два места, где производится управление процессом DDNS: зона для пространства имен и сервер DHCP.

Зона DNS может быть включена для обновлений DDNS в мастере New Zone Wizard или же путем изменения свойств зоны. На рис. 6.27 показаны опции для обновлений DDNS — только безопасные, безопасные и небезопасные, а также полное отключение обновлений. Безопасные динамические обновления означают, что до их выполнения клиент DNS проходит аутентификацию на контроллере домена. Небезопасные динамические обновления означают, что они принимаются без аутентификации. Учитывая название, вы легко можете предположить, что злоумышленники способны воспользоваться этой опцией. В случае отключения никакие обновления DDNS поступать не будут.

Сервер DHCP также может участвовать в процессе DDNS. В самых ранних версиях Windows Server было много клиентов Windows, которые не обладали возможностями DDNS. Для решения этой проблемы сервер DHCP идентифицирует такие ОС и выполняет для них обновления. Кроме того, сервер DHCP может выполнять обновления по запросу. На рис. 6.28 приведена вкладка DNS окна свойств IPv4 для сервера DHCP.

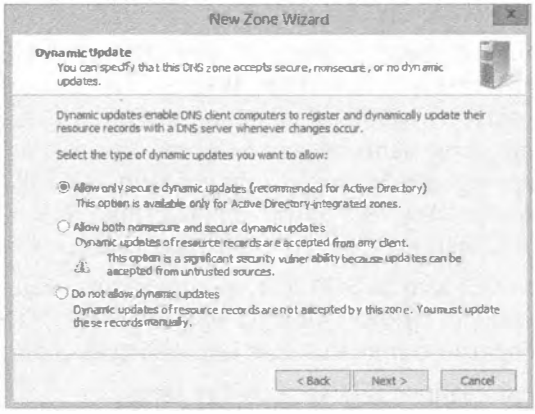


Рис. 6.27. Опции динамических обновлений DNS

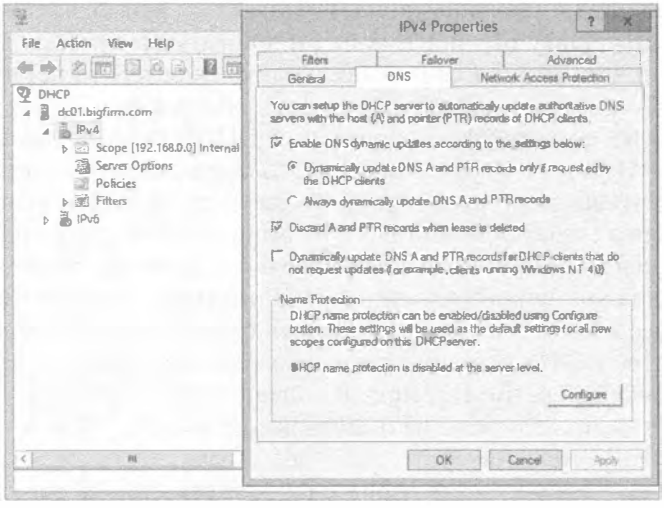


Рис. 6.28. Опции DDNS для сервера DHCP

Здесь показаны стандартные настройки, которые редко изменяются. В сущности, сервер DHCP не выполняет никаких обновлений, поскольку клиенты делают это самостоятельно. Сервер DHCP производит очистку, когда истекает срок аренды. Защита имен, включаемая за счет отметки флажка в окне, открывающемся по щелчку на кнопке Configure (Конфигурировать) в области Name Protection (Защита имен), предотвращает обновление сервером DHCP существуюшей записи DNS.

Система DNS в Active Directory

В Microsoft настолько тесно интегрировали DNS и Active Directory, что обсуждать их по отдельности довольно трудно. Во время создания среды Active Directory с Windows Server 2012 R2 процесс установки Active Directory автоматически конфигурирует DNS при добавлении роли. Это освобождает специалистов по IT от ручной настройки DNS.

В последующих разделах мы раскроем способ, которым Active Directory конфигурирует систему DNS и применяет ее для поддержки клиентов. За дополнительными сведениями о терминах и концепциях Active Directory обращайтесь в главу 7.

Автоматическое конфигурирование DNS

ОС Windows Server 2012 R2 предлагает два способа установки службы DNS: добавление роли DNS самой по себе (как было показано ранее для автономной конфигурации, не присоединенной к домену) или добавление роли Active Directory Domain Services (Службы домена Active Directory). В случае выбора второго способа вы должны запустить мастер установки служб домена Active Directory (Active Directory Domain Services Installation Wizard), который проведет ряд настроек для роли Active Directory Domain Services, включая автоматическое конфигурирование и интеграцию с ролью DNS. В главе 7 процесс установки Active Directory будет рассмотрен во всех деталях, а здесь мы лишь посмотрим, что произойдет с ролью DNS.

Первым делом вы должны понять предварительные условия, которые должны быть удовлетворены для проведения установки Active Directory. Будущему контроллеру домена необходима возможность подключения к существующей структуре Active Directory DNS. В противном случае нельзя будет подключиться к контроллерам домена и получить нужную информацию. Таким образом, в настройках IP-адресов должен быть указан DNS-сервер внутри среды Active Directory, желательно DNS-сервер корня леса или DNS-сервер в том же самом домене, к которому планируется присоединение. Единственным исключением является ситуация, когда создается самый первый контроллер домена в среде Active Directory. В этот момент нет никакой структуры Active Directory DNS, на которую можно было бы указывать.

Во время выполнения мастера Active Directory Domain Services конфигурируется новый контроллер домена. В зависимости от опций, выбранных в мастере, может быть создан новый контроллер домена. В любом случае служба DNS и соответствующие настройки конфигурируются автоматически. В среду вносятся описанные далее изменения.

Создание разделов каталога приложений

Разделы каталога приложений — это границы внутри базы данных Active Directory, которые создаются для совместного использования зон DNS разными доменами при создании нового домена или леса.

Раздел `DomainDNSZones.domain.name` создается для контроллеров домена внутри домена. Раздел `ForestDNSZones.domain.name` создается для совместного использования контроллерами домена в рамках леса Active Directory.

Если вы снова взглянете на рис. 6.9, то заметите, что поддомен `_msdcs.bigfirm.com` делегирован подобно `Ecoast`. Он делегирован на тот же самый контроллер домена, в рассматриваемом случае это `DC01.Bigfirm.com`.

Зона `_msdcs.Bigfirm.com` создается в разделе `ForestDNSZone.Bigfirm.com` каталога приложений. Это позволяет данной порции пространства имен реплицироваться на все домены внутри леса.

После создания дополнительных контроллеров доменов они автоматически появляются в этих разделах каталога приложений.

Добавление сервера пересылки

Сервер пересылки можно добавить, просмотреть и сконфигурировать на вкладке Forwarders (Серверы пересылки) окна свойств DNS-сервера. Обычно это будет IP-адрес исходного DNS-сервера, которым пользовался данный сервер.

Изменение IP-адреса

Новый контроллер домена, созданный мастером Active Directory Domain Services Wizard, также является новым DNS-сервером. Адрес основного DNS-сервера конфигурируется на IP-адреса обратной связи ::1 (для IPv6) и 127.0.0.1 (для IPv4).

Делегирование поддомена

Дочерний домен имеет имя, являющееся поддоменом внутри существующего пространства имен домена. Например, `Ecoast.Bigfirm.com` — это поддомен в пространстве имен `Bigfirm.com`. В результате работы мастера Active Directory Domain Services Wizard пространство имен нового домена будет поддерживаться в новом контроллере домена в виде делегированного поддомена.

В родительском домене поддомен вроде `Ecoast.Bigfirm.com` делегируется новому контроллеру домена. Делегирование свяжет родительский и дочерний домены для преобразования имен. Это иллюстрировалось ранее на рис. 6.9.

Дополнительные рекомендации по конфигурированию

После создания контроллера домена мы рекомендуем внести в настройки DNS перечисленные ниже изменения.

1. В свойствах TCP/IPv4 сетевого адаптера измените основной DNS-сервер на IP-адрес основного сетевого подключения. Например, если IP-адресом сервера является 192.168.0.1, его понадобится указать в качестве основного DNS-сервера.

   При поиске и устранении неполадок в DNS с помощью утилиты `NsLookup` адрес обратной связи (127.0.0.1) указывается как "неавторитетный". Мы находим результаты применения адреса обратной связи несколько ненадежными, поэтому лучше придерживаться основного IP-адреса.

2. Создайте зоны обратного просмотра в разделе `ForestDNSZones.domain.name` каталога приложений.

   Зону обратного просмотра для подсетей может потребоваться совместно использовать в контроллерах различных доменов.

3. Создайте зону-заглушку для новых деревьев доменов на корневом DNS-сервере.

   Дерево домена имеет имя, отличающееся от имени корневого DNS-сервера. Поскольку запись об исходном DNS-сервере указана как сервер пересылки, подобно поднятиям других контроллеров домена, этот DNS-сервер может взаимодействовать с остальной структурой Active Directory DNS. Тем не менее, для остальной структуры Active Directory DNS никакого автоматического конфигурирования для преобразования имен в новом пространстве имен не предусмотрено. Например, нам придется настроить сервер условной пересылки или зону-заглушку, чтобы нацелить DNS-серверы на новый контроллер домена для `Apex.com`. На рис. 6.19 демонстрируется применение зоны-заглушки для содействия преобразования имен FQDN домена `Apex.com`.

Записи SRV и клиенты

Глядя на зону DNS нового домена, вы заметите наличие в ней множества новых папок или поддоменов. Открывая эти папки, вы найдете множество записей расположения служб, как было показано ранее на рис. 6.22. Как уже упоминалось, записи SRV и динамические обновления DNS необходимы для обеспечения работы Active Directory. Они представляют собой результат совместного функционирования двух технологий.

Служба `netlogon` выполняет запросы DDNS для создания записей SRV внутри пространства имен Active Directory DNS. Единственная причина заключается в гарантировании того, что компьютеры смогут найти контроллеры домена.

Внутри процессов ОС Windows определенные службы находятся с использованием DNS. На рис. 6.22 присутствовало несколько служб:

- `_gc` (global catalog — глобальный каталог) — служба LDAP для поиска данных в глобальном каталоге;
- `_kerberos` — процесс аутентификации;
- `_kpassword` — еще одна часть процесса аутентификации;
- `_ldap` — служба LDAP для поиска данных в домене.

Каждая из перечисленных служб выполняется контроллерами домена внутри домена или леса. На рис. 6.22 было видно, что все эти роли выполнялись на `DC01.Bigfirm.com` и прослушивался порт TCP.

Таким образом, когда компьютеру Windows требуется какая-то служба контроллера домена, например, LDAP, он запросит запись SRV для `_ldap._tcp.Bigfirm.com`. После этого он получит все, что необходимо для взаимодействия с IP-адресом и портом.

Если компьютеру Windows нужно найти контроллер домена внутри собственного сайта, он может искать его в поддомене `_sites.Bigfirm.com`. В этом поддомене будут отображаться все созданные сайты в консоли Active Directory Sites and Services (Сайты и службы Active Directory).

Вероятность того, что администраторы могли бы поддерживать все это множество записей DNS вручную, довольно низка. Для одного контроллера домена можно ожидать регистрации, по меньшей мере, 16–20 разных записей SRV. Изучение их всех — задача, безусловно, не из простых. Именно здесь в игру вступают инструменты, подобные `DcDiag`. Инструкции по работе с этими утилитами приведены в разделе "Использование `NsLookup` и `DcDiag`" далее в главе.

Дополнительные компоненты Windows Server 2012 R2

К этому моменту мы обсудили существенные компоненты и способы обращения с ними, что уже позволяет вам достаточно квалифицированно управлять средой Windows Server 2012 R2 DNS. В настоящем разделе будут рассматриваться дополнительные компоненты DNS в Windows Server 2012 R2, которые развертываются не так часто, как основные компоненты, но о которых, тем не менее, полезно знать.

Глобальный список блокировки запросов

Существует несколько распространенных записей хостов, которые могут быть зарегистрированы в DNS другими службами. Одной из таких служб является протокол

автоматического обнаружения веб-прокси (Web Proxy Automatic Discovery Protocol — WPAD). Он помогает веб-браузерам автоматически загружать конфигурации прокси из сервера. Так как эта запись не относится к конкретному компьютеру, любой компьютер, включая потенциально скомпрометированный злоумышленниками, может попытаться зарегистрировать свое имя. Другой распространенной записью хоста является протокол автоматической внутрисайтовой адресации туннелей (Intra-Site Automatic Tunneling Addressing Protocol — ISATAP). Как объяснялось в главе 4, протокол ISATAP предназначен для выполнения маршрутизации из сети IPv4 в сеть IPv6.

В глобальном списке блокировки запросов (global query block list) указаны имена, для которых регистрация DDNS заблокирована. Таким образом, попытки компьютера злоумышленника зарегистрировать имена WPAD или ISATAP отклоняются.

Показанные ниже команды иллюстрируют способы администрирования этого списка. Для просмотра списка служит командлет `Get-DNSServerGlobalQueryBlocklist`. Обратите внимание, что по умолчанию в списке находятся `wpad` и `isatap`.

```
C:\Users\Administrator.BF1>Get-DNSServerGlobalQueryBlocklist
Enable:  True
List:    {wpad, isatap}
```

Чтобы добавить в этот список имя вроде `www`, можно воспользоваться командлетом `Set-DNSServerGlobalQueryBlocklist`. По умолчанию компонент глобального списка блокировки запросов включен. Он отключается и повторно включается с применением опции `-Enable` со значением `$True` или `$False`.

Преобразование глобальных имен и одиночных имен

Даже с учетом того, что использование WINS идет на убыль, возникает потребность в поддержке для некоторых приложений процесса преобразования имен NetBIOS. Компонент GlobalNames (глобальные имена) — это специальная зона, созданная для преобразования имен NetBIOS (15 символов безо всяких точек). Клиент DNS осуществляет запрос в зону GlobalName, когда поиски с основным и дополнительным суффиксом DNS завершились неудачей.

Конфигурирование компонента GlobalNames выполняется несложно.

1. Создайте новую зону по имени `GlobalNames`.

   Рекомендуется выбрать тип зоны, интегрированной с Active Directory, чтобы обеспечить репликацию в другие контроллеры домена.

2. Включите поддержку зоны `GlobalNames` с помощью командлета `Set-DNSServerGlobalNameZone`:

   ```
   C:\Users\Administrator.BF1>Set-DNSServerGlobalNameZone -Enable $True
   ```

3. Проведите репликацию зоны в другие контроллеры домена.

   Не забудьте добавить эти контроллеры домена в список серверов имен для зоны.

4. Добавьте в зону записи CNAME для переадресации на определенные хосты.

   В данном примере `www` переадресуется на `hostrecord.PrimaryZone.local` (рис. 6.29).

5. Добавьте запись местоположения службы, если необходимо, чтобы эту зону запрашивали другие леса Active Directory.

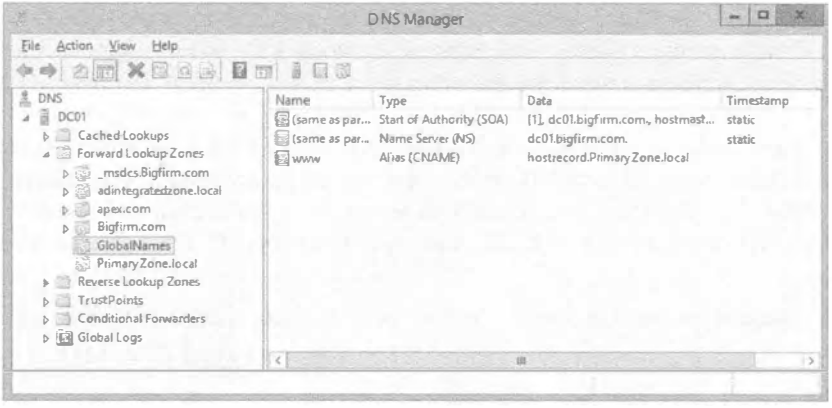


Рис. 6.29. Зона `GlobalNames`

Протестировать преобразование глобальных имен можно посредством утилиты `NsLookup`:

```
C:\Users\Administrator.DC1>Nslookup
Default Server:  DC01.bigfirm.com
Address:  192.168.0.1

> www
Server:    DC01.bigfirm.com
Address:   192.168.0.1

Name:      hostrecord.primaryzone.local
Address:   192.168.0.21
Aliases:   www.bigfirm.com
```

Как обсуждалось ранее, в большинстве сред, полагающихся на серверы Windows, потребность в преобразовании одиночных имен (NetBIOS) сведена к минимуму. Она также была минимизирована за счет подходящего развертывания приложений с применением имен FQDN и привлечения DNS.

Фоновая загрузка зон

Некоторые старые среды имеют настолько большие зоны DNS, что перезапуск службы DNS контроллерами доменов занимает более часа. Для решения этой проблемы предназначено средство фоновой загрузки зон. Чтобы такая проблема возникла, зона DNS должна содержать огромное количество записей.

Во время запуска службы DNS она начинает реагировать на запросы к зонам, которые уже загрузились. Запросы к пока еще не загруженным зонам будут отсылаться другим DNS-серверам.

DNSSEC

Подобно HTTP, система DNS является нешифрованной и неаутентифицируемой. Как упоминалось при рассмотрении зон обратного просмотра, злоумышленники могут подделывать ответы DNS. Чтобы противостоять этому, были разработаны стандарты DNSSEC (DNS Security Extensions — расширения безопасности DNS), которые позволяют DNS-серверу добавлять цифровую подпись к записям ресурсов.

ОС Windows Server 2012 R2 обеспечивает поддержку дополнительных зон как зон DNSSEC. Она реагирует только на запросы записей из зоны с цифровой подписью. ОС также будет предоставлять необходимые записи ресурсов для аутентификации подписи.

Такими записями являются KEY, SIG и NXT. Запись KEY — это открытый ключ подписи DNS-сервера. Запись SIG представляет цифровую подпись записи ресурса. В записи NXT перечислены все допустимые записи в пространстве имен.

В версии Windows Server 2012 R2 стандарты DNSSEC претерпели следующие улучшения:

- интеграция с Active Directory и поддержка динамических обновлений DNS;
- обновленная поддержка стандартов DNSSEC (NSEC3 и RSA/SHA-2);
- проверка достоверности записей с использованием обновленных стандартов DNSSEC;
- дополнительная поддержка DNSSEC в PowerShell.

Если вы хотите протестировать DNSSEC в испытательной среде, обратитесь к пошаговому руководству от Microsoft, доступному по ссылке `http://tinyurl.com/dnsseclab`.

Якори доверия

Якори доверия (trust anchors) — это открытые сертификаты серверов DNSSEC, которым DNS-сервер будет доверять при взаимодействии. Сертификаты якорей доверия будут применяться для проверки достоверности цифровых подписей ответов. Они добавляются в свойства DNS-сервера в форме открытых ключей.

В якори доверия Windows Server 2012 R2 внесены следующие усовершенствования:

- использование Active Directory для распространения якорей доверия;
- поддержка автоматического перебора;
- упрощенное извлечение корневого якоря доверия.

В Windows Server 2012 R2 якори доверия отображаются в консоли DNS Manager, внутри расположенной в левой части папки Trust Points (Точки доверия).

Поддержка преобразования имен DNS на основе Интернета

В рамках организации существует также потребность в управлении пространствами имен Интернета. Пользователям локальной сети понадобится доступ к веб-сайтам и другим основанным на Интернете службам. Внешним пользователям будет нужен доступ к веб-сайтам организации и, как минимум, постовым серверам. Таким образом, вы не должны упускать из виду и эти требования.

Чтобы разрешить внешним пользователям обращаться к веб-сайтам организации, должен существовать внешний домен DNS. Следовательно, вам придется обдумать вопрос о необходимости развертывания внешнего DNS-сервера. Внутренние компьютеры будут преобразовывать внешние имена с помощью внутренних DNS-серверов. По этой причине требуется интеграция со структурой DNS из Интернета.

Поддержка внешних доменов DNS

Большинство компаний для поддержки веб-сайта и электронной почты регистрируют какое-то пространство имен DNS. Мелкие и некоторые средние компании поручают управлять пространством имен на внешних DNS-серверах поставщикам Интернет-услуг. Преимущества такого подхода связаны с готовностью серверов и устранению потребности в обслуживании дополнительных серверов в подсети, открытой для Интернета. Эти серверы управляются посредством веб-интерфейса и позволяют работать только с небольшим набором типов записей, таких как A, CNAME и MX.

Допускается применение сервера Windows Server 2012 R2 для внешних операций DNS. Роль DNS можно установить на сервере, не являющемся членом домена (как обсуждалось в разделе "Конфигурирование автономного DNS-сервера" ранее в главе), и затем изменить запись сервера имен для зарегистрированного пространства имен DNS, указав публичный IP-адрес сервера. Конечно, открыть Интернету автономный DNS-сервер можно и таким способом, но в реальности существует несколько аргументов против такого подхода.

- ОС Windows Server 2012 R2 не является бесплатной, и ее использование в качестве внешнего решения DNS нельзя считать экономически оправданным подходом.
- Сервер Windows Server 2012 R2 нуждается в ограничении функциональных возможностей и зашите, когда он открыт внешне.
- Сервер должен обладать высокой доступностью, поэтому вам придется кластеризировать его или настроить несколько DNS-серверов.
- Если вы еще об этом не позаботились, вам также понадобится высокоскоростное подключение к Интернету.

Общая цена, которую придется заплатить, двигаясь в таком направлении, высока, поэтому многие компании предпочитают тратить свои деньги по-другому. Именно здесь преимущество следует отдать простой реализации DNS на базе Linux. Тем не менее, мы рекомендуем наиболее распространенный подход — поручить управление внешним пространством имен поставщику Интернет-услуг.

Разделение

Когда дело доходит до DNS, многие компании также внедряют сценарий с разделением (split-brain), хотя и неумышленно. Это означает, что они имеют внутреннее пространство имен, совпадающее с внешним пространством имен. Например, компания регистрирует внешнее пространство имен `Bigfirm.com` и затем решает строить среду Active Directory с тем же самым именем.

Управление данным сценарием на единственном сервере было бы идеальным. Реализация разделенной DNS — хорошая идея, предназначенная для решения проблемы. Можно было бы иметь один DNS-сервер, поддерживающий внутреннюю и внешнюю зону того же самого пространства имен. Тогда бы IP-адреса для внешней зоны предоставлялись бы внешним запросам, а внутренние IP-адреса — внутренним запросам.

Предостережения относительно применения разделенной DNS

Разные специалисты и различные технические документы по DNS могут утверждать о том, что использовать одно и то же доменное имя для внутреннего и внешнего пространства имен DNS компании не рекомендуется. Взамен предлагается выбрать другое имя, которое не встречается в Интернете, или зарегистрированное имя, которым вы не пользовались.

Когда компании не следуют этой рекомендации, они вскоре обнаруживают конфликт при распознавании внешних ресурсов, которыми владеют, таких как `www.Bigfirm.com`. Внутренний DNS-сервер не может найти это имя, и запрос терпит неудачу. Администраторы пытаются исправить это путем ручного добавления имени с внешним IP-адресом, но добавление внешнего IP-адреса вызывает проблемы с маршрутизацией. Кроме того, разработчики будут жаловаться на невозможность загрузки нового содержимого по внешнему IP-адресу. Им нужен внутренний IP-адрес. Такие дополнительные трудности администрирования становятся нормой при разделении DNS.

Идея неплоха, но Windows Server 2012 R2 это не поддерживает. В первую очередь не поддерживается организация, открывающая контроллер домена, на котором размещено внутреннее пространство имен DNS, даже на границе Интернета. Так сделано не только из соображений безопасности. База данных Active Directory слишком ценна, чтобы помещать ее в демилитаризованную зону (DMZ), где она станет лакомым кусочком для злоумышленников. Поэтому придется прибегнуть к альтернативе.

Цель заключается в том, чтобы обеспечить предоставление внешним запросам внешних IP-адресов, а внутренним запросам — внутренних IP-адресов. Для поддержки такого сценария вы должны будете администрировать (минимум) два DNS-сервера с помощью Microsoft DNS. Ниже перечислены базовые шаги.

1. Реализуйте внешний DNS-сервер для поддержки `Bigfirm.com`. Обычно это становится готовым после регистрации доменного имени с помощью поставщика Интернет-услуг.
2. Реализуйте внутреннюю структуру DNS. Это делается с применением мастера Active Directory Domain Services Installation Wizard.
3. Добавьте любые внешние записи во внутреннюю зону для `Bigfirm.com`.

   Помните, что DNS-серверы внутри сети будут авторитетными для домена `Bigfirm.com`. Если не удается найти сайт `www.Bigfirm.com`, то он не существует. Внешние записи должны быть продублированы во внутренней зоне, чтобы мог возвращаться положительный результат. Вам придется протестировать маршрутизацию, удостоверившись в доступности указанного IP-адреса. В случае возникновения проблем с маршрутизацией может понадобиться использовать внутренний адрес.
4. Сконфигурируйте преобразование внешних пространств имен с применением корневых подсказок или серверов пересылки. Данная тема раскрывается в следующем разделе.

Преобразование внешних пространств имен

Мы обсуждали, каким образом интегрировать DNS-сервер с другими. Основными методами преобразования имен DNS в Интернете являются корневые подсказки или серверы пересылки. Корневые подсказки содержат список DNS-серверов, находящихся наверху структуры DNS Интернета. DNS-сервер может взаимодействовать с такими серверами для выполнения рекурсивных запросов к внешним пространствам имен. Серверы пересылки производят ответвленные запросы к другому DNS-серверу, чтобы посмотреть, не распознает ли он имя. Ранее мы упоминали, что в небольших средах предпочитаем использовать серверы пересылки на внешний DNS-сервер, поддерживаемый поставщиком Интернет-услуг, но корневые подсказки в данном сценарии также работают.

Важно не смешивать эти два подхода. Не определяйте в корневых подсказках серверы как серверы пересылки. Запрос к корневой подсказке — это направленный запрос, который всегда возвращает сервер имен для домена. Он не отвечает записями хостов и не выполняет рекурсивную операцию, которую будет делать сервер пересылки. Кроме того, серверы пересылки имеют приоритет перед корневыми подсказками. На приведенном ранее рис. 6.10 вкладка Forwarders (Серверы пересылки) содержала флажок Use root hints if no forwarders are available (Использовать корневые подсказки, если нет доступных серверов пересылки). Вы можете сделать вывод, что если сервер пересылки указан, но получен отрицательный ответ, запрос завершится, а корневые подсказки вообще затрагиваться не будут.

В обширных внутренних средах DNS обдуманное применение серверов пересылки и корневых подсказок является обязательным. Внутренние серверы имен поддоменов должны распознавать запросы от корневого DNS-сервера. Они также должны распознавать запросы, основанные на Интернете. Получая преимущество возможности кеширования DNS, они могут полагаться на сервер в распознавании и сохранять распространенные запросы, чтобы сократить внешний трафик. В Microsoft рекомендуют, чтобы кеширующий сервер не был корневым, что позволит не перегружать корневой сервер дополнительной рабочей нагрузкой. Кроме того, в Microsoft предостерегают от прямого взаимодействия с Интернетом внутренних DNS-серверов, на которых размещены зоны, чтобы уменьшить их видимость в Интернете. На рис. 6.30 показано одно решение, которое могло бы работать с нашей вымышленной структурой DNS.

В этом примере серверы пересылки используются для отправки запросов корневому DNS-серверу в `Bigfirm.com`. Корневые подсказки можно было бы задействовать, удалив корневые подсказки Интернета и указав `BF1.Bigfirm.com` в качестве сервера корневых подсказок. Кеширующий сервер предотвращает отправку запросов в Интернет DNS-серверами, на которых размещены зоны, интегрированные с Active Directory. Он осуществляет преобразование имен посредством корневых подсказок. Для обработки запросов в домене `Apex.com` применяется зона-заглушка или сервер условной пересылки.

Возможны другие решения, обеспечивающие преимущества по разным причинам. Мы отдаем предпочтение простоте использования серверов пересылки для управления интеграцией серверов.

Рис. 6.30. Внутренняя структура DNS

Администрирование и устранение неполадок с помощью инструментов DNS

В этом разделе мы обсудим доступные инструменты и приемы устранения неполадок в преобразовании имен DNS. Учитывая важность DNS, вы должны хорошо знать инструменты, которые предоставляют ценную информацию, позволяющую выявить возможные проблемы с преобразованием имен. Вдобавок к конфигурированию стандартные инструменты администрирования, консоль управления DNS и PowerShell предлагают также и дополнительную информацию такого рода. Утилиты `NsLookup`, `DcDiag` и `DNSLint` предоставляют удобные начальные признаки наличия проблем, касающихся преобразования имен DNS.

Администрирование DNS-сервера с помощью консоли управления DNS и PowerShell

Для администрирования DNS-сервера придется иметь дело с двумя инструментами: консолью управления DNS, которая является оснасткой MMC, и PowerShell, представляющим собой инструмент командной строки. Подобно оснастке MMC, инструмент PowerShell предлагает возможность администрирования всего сервера, а также немного дополнительной функциональности. Например, как вы уже знаете, консоль управления DNS не позволяет изменять глобальный список блокировки запросов или создавать разделы каталога.

Повсюду в этой главе демонстрировалось применение консоли управления DNS для создания зон и редактирования свойств серверов и зон, что является обыденными задачами, с которыми приходится иметь дело.

Вы также можете воспользоваться внутри консоли несколькими диагностическими конфигурациями. Они настраиваются в свойствах DNS-сервера.

- **Вкладка Event Logging (Ведение журнала событий).** Для службы DNS создается отдельный журнал, который можно открыть в программе просмотра событий (Event Viewer). Он связан с консолью управления DNS. Вдобавок сервер по умолчанию собирает все события, что настраивается на вкладке Event Logging.
- **Вкладка Debug Logging (Ведение журнала отладки).** В целях анализа можно собрать в журнале более детальные сведения о действительных коммуникациях, возникающих на DNS-сервере. Ведение журнала отладки по умолчанию отключено, но может быть включено через свойства DNS-сервера; вкладка Debug Logging представлена на рис. 6.31. Эта возможность полезна при выявлении причин ненадежной работы DNS-сервера. Хотя большинство проблем с DNS решаются путем подходящей подключаемости IP, вы найдете данное средство полезным, когда подключаемость IP не имеет отношения к проблеме. В редких случаях мы должны проверять, попадают ли специфичные запросы на сервер, и это средство предоставляет нужную информацию.
- **Вкладка Monitoring (Мониторинг).** Эта вкладка также доступна из окна свойств DNS-сервера; она показана на рис. 6.32. Она позволяет проверить запросы DNS из этого сервера или предназначенные другому серверу — обратите внимание, не конкретному серверу, а любому произвольно выбранному серверу. Можно задать частоту запуска этого теста.

В выводе указывается только о том, прошел тест или нет. По существу, если на DNS-сервере имеются проблемы, тест не проходит. Нам не удалось обнаружить на этой вкладке сколько-нибудь полезные данные при решении проблем с DNS и, скорее всего, вы не найдете здесь ничего нового. Для мониторинга DNS-серверов рекомендуется применять инструменты вроде диспетчера операций системного центра 2012 R2 (Microsoft System Center 2012 R2 Operations Manager), и эта тема обсуждается в главе 30 (том 2).

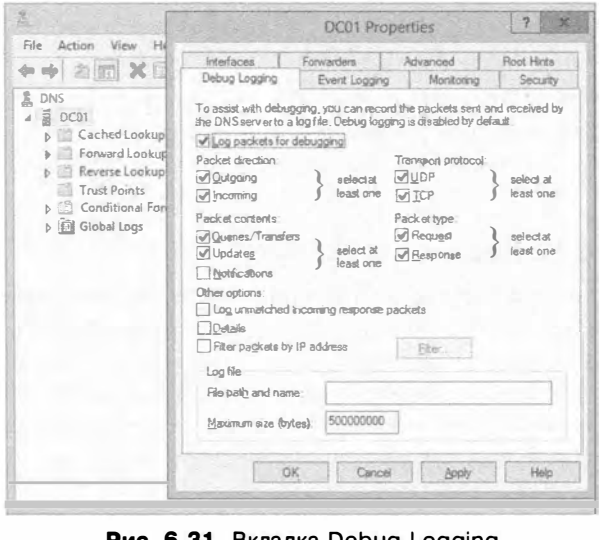


Рис. 6.31. Вкладка Debug Logging

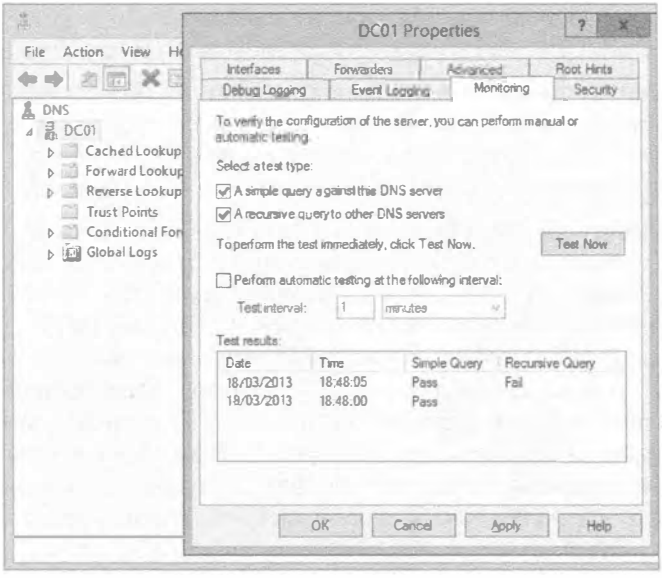


Рис. 6.32. Вкладка Monitoring

Инструмент PowerShell предлагает несколько диагностических командлетов, которые могут оказаться полезными при сборе и анализе данных.

- `Get-DNSServer` предоставляет конфигурационные настройки для DNS-сервера.
- `Get-DnsServer | Export-Clixml -Path "c:\config\DnsServerConfig.xml"` генерирует текстовый файл с конфигурацией и свойствами зон.
- `Get-DNSServerDiagnostics` предоставляет сведения о ведении журналов событий для специфических операций DNS на сервере.
- `Clear-DNSServerCache` опустошает кеш. Иногда устаревшие распознанные записи должны быть удалены после решения проблемы. Данная задача также доступна в консоли управления DNS.

Все эти инструменты предоставляют средства администрирования и мониторинга. Мы находим их полезными для проведения более глубоких исследований, когда передовые инструменты, такие как `NsLookup`, `DcDiag` и `DNSLint`, не сразу указывают на проблему.

Использование `NsLookup` и `DcDiag`

При устранении проблем с DNS чаще всего используются инструменты `NsLookup`, `DcDiag` и `DNSLint`. Утилита `NsLookup` предоставляет немедленное указание на проблемы с преобразованием имен. Утилиты `DcDiag` и `DNSLint` обеспечивают указание на наличие проблем, связанных с Active Directory, таких как регистрация DDNS и записи SRV. Если с помощью этих инструментов не удается идентифицировать проблему, можно положиться на средства консоли управления DNS и PowerShell.

NsLookup

Утилита NsLookup является первым инструментом, который мы применяем при поиске и устранении проблем с преобразованием имен. Она подключается к указанному в конфигурации IP-адресов основному DNS-серверу и делает запросы DNS.

Обратите внимание, что данная утилита не выполняет полный процесс преобразования имен, т.е. весь жизненный цикл. Она ограничивается одной частью этого цикла. Во время обсуждения клиентов приводились примеры команд ping и net view, демонстрирующие различные части процесса. Пример команды ping показывал процесс DNS, включающий первый шаг поиска имени в файле HOSTS. Если файл HOSTS содержит записи для того же имени хоста, вы заметите расхождение между ping и NsLookup.

Вирус Conficker

Одним из примеров вредоносного ПО, использующего DNS для нарушения нормальной работы, является вирус Conficker. Он появился в 2008 году, и, верите вы или нет, его до сих пор можно обнаружить на компьютерах, где не применялись исправления системы и обновления антивирусного ПО. В зараженных вирусом Conficker системах предотвращается доступ из браузеров к важным сайтам внутри определенных пространств имен DNS, таких как Microsoft.com, Symantec.com и Norton.com.

В результате ПО становится непригодным для использования. Компьютер не может загрузить обновления Windows; он не может найти возможные решения проблемы. Даже если на машине установлено ПО Norton AntiVirus, ему не удается получить доступ к сайту обновлений Symantec для загрузки последних обновлений. Машина не может исправить сама себя!

Когда мы столкнулись с Conficker, утилита NsLookup была первым инструментом, задействованным в процессе обнаружения проблемы. Запросы к Microsoft.com и Symantec.com проходили нормально, но обращение к указанным сайтам из браузера Internet Explorer или Firefox оказывалось невозможным. Это помогло сузить область поиска. Таким образом, браузеры были заражены.

Конечно, утилита NsLookup предоставляет IP-адреса для сайтов, к которым нам необходим доступ. Однако веб-сайты Microsoft не функционируют в случае указания в URL только IP-адреса. В результате такой обходной путь не срабатывает.

Мы нашли решение с применением инструмента удаления вредоносного ПО (Microsoft Windows Malicious Software Removal Tool — MSRT). Этот инструмент должен быть загружен на отдельном компьютере и затем физически перенесен на зараженный компьютер. С помощью MSRT вирус удалось идентифицировать и удалить. К счастью, в наши дни распространение вируса Conficker ограничивается старыми ОС с устаревшим или отсутствующим антивирусным ПО и обновлениями Windows. Тем не менее, это хороший пример того, как за счет изменения в преобразовании имен нарушается работа системы и каким образом с помощью инструментов, подобных NsLookup, найти и идентифицировать причину.

Если приложению не удается получить доступ к серверу, то после проверки подключаемости TCP/IP мы начинаем исследования с использованием команды NsLookup.

Ниже перечислены вопросы, которые требуют прояснения.

- Отвечает ли DNS-сервер? Команда в самом начале сообщит, можно ли подключиться к DNS-серверу. При наличии задержки или тайм-аута нет необходимости продолжать. Имеется проблема с подключаемостью.
- Является ли стандартный сервер неизвестным? Это указывает на сбой обратного просмотра, инициируемого утилитой NsLookup. При таком состоянии остальные проверки NsLookup становятся бессмысленными.
- Можно ли преобразовать локальное имя FQDN? Это обходит часть обработки со стороны клиента. Для поиска имен хостов клиент будет добавлять основные суффиксы DNS.
- Можно ли преобразовать имя хоста без суффикса DNS? Это то, что делает клиент, и данный шаг можно проверить.
- Можно ли преобразовать внешние имена FQDN? Это позволит проверить возможность выхода в Интернет стандартного DNS-сервера.

С утилитой NsLookup можно работать двумя способами: с помощью командных запросов и в интерактивном режиме. Интерактивный режим намного мощнее, поэтому вначале используется именно он. Он предлагает возможность выполнять запросы к разным типам записей ресурсов и позволяет переключаться на другой сервер. Ниже приведены примеры распространенных запросов (вместе с поясняющими комментариями):

```
C:\Users\Administrator.BF1>Nslookup
Default Server:  BF1.bigfirm.com
Address:  192.168.0.10

rem Запрос записи хоста
> BF1.bigfirm.com
Server:  BF1.bigfirm.com
Address:  192.168.0.10

Name:    BF1.bigfirm.com
Address:  192.168.0.10

rem Запрос обратной записи PTR
> set q=ptr
> 192.168.0.10
Server:  BF1.bigfirm.com
Address:  192.168.0.10

10.1.168.192.in-addr.arpa     name = BF1.bigfirm.com

rem Запрос записи SOA
> set q=soa
> bigfirm.com
Server:  BF1.bigfirm.com
Address:  192.168.0.10

bigfirm.com
      primary name server = BF1.bigfirm.com
```

```
        responsible mail addr = hostmaster.bigfirm.com
        serial  = 124
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
BF1.bigfirm.com     internet address = 192.168.0.10

rem Запрос записи NS
> set q=ns
> bigfirm.com
Server:  BF1.bigfirm.com
Address:  192.168.0.10

bigfirm.com         nameserver = BF1.bigfirm.com
BF1.bigfirm.com     internet address = 192.168.0.10

rem Запрос записи SRV
> set q=srv
> _ldap._tcp.bigfirm.com
Server:   BF1.bigfirm.com
Address:  192.168.0.10

_ldap._tcp.bigfirm.com  SRV service location:
        priority        = 0
        weight          = 100
        port            = 389
        svr hostname    = BF1.bigfirm.com
BF1.bigfirm.com     internet address = 192.168.0.10
```

DcDiag

Утилита DcDiag изначально была частью набора инструментов для поддержки администрирования (которые нужно было устанавливать отдельно) в ранних версиях Windows Server, но теперь она по умолчанию является частью установки Windows Server 2012 R2. Это инструмент, который нужно применять первым для быстрой проверки работоспособности структуры DNS. Поскольку утилита DcDiag проводит диагностику контроллеров домена, она должна проверить корректность работы DNS. После выполнения стандартного набора тестов вы можете заметить ошибки при попытках подключения к контроллерам домена. После этого можно запустить дополнительные тесты DcDiag, ориентированные специально на DNS. В следующем примере осуществляется проверка, может ли контроллер домена выполнять DDNS для регистрации записей SRV:

```
dcdiag /test:RegisterInDNS /DnsDomain:bigfirm.com
      /f:documents\dcdiagRegisterInDNS.txt
```

Ниже показан вывод этой команды:

```
Starting test: RegisterInDNS
   DNS configuration is sufficient to allow this domain controller to
   dynamically register the domain controller Locator records in DNS.
   The DNS configuration is sufficient to allow this computer to dynamically
   register the A record corresponding to its DNS name.
   ..... BF1 passed test RegisterInDNS
```

```
Запуск теста: RegisterInDNS
   Конфигурация DNS достаточна для того, чтобы позволить этому
   контроллеру домена динамически регистрировать записи Locator
   контроллеру домена в DNS.
   Конфигурация DNS достаточна для того, чтобы позволить этому
   контроллеру домена динамически регистрировать запись A,
   соответствующую его имени DNS.
   ..... BF1 прошел тест RegisterInDNS
```

Утилита DcDiag выполняет множество тестов, относящихся к контроллеру домена, включая несколько тестов DNS. Выше был упомянут один из таких тестов — RegisterInDNS. Эти тесты в первую очередь сосредоточены на интеграции между DNS-серверами внутри среды Active Directory. Тесты могут быть выполнены в отношении делегирования, серверов пересылки, обновлений и преобразовании внешних имен DNS.

Ниже приведена часть справочной информации по утилите DcDiag. В ней присутствует список тестов, доступных для DNS. При тестировании преобразования внешних имен мы обычно полагаемся на NsLookup, поэтому никогда не пользуемся тестами /DnsForwarders и /DnsResolveExtName, но для полноты они здесь показаны.

```
DNS
Этот тест проверяет работоспособность настроек DNS для целого
предприятия. Подтесты могут запускаться по отдельности с применением
перечисленных далее ключей. По умолчанию запускаются все тесты кроме
тех, которые проверяют преобразование внешних имен.

/DnsBasic               (базовые тесты, не могут быть пропущены)
/DnsForwarders          (тесты для серверов пересылки и корневых подсказок)
/DnsDelegation          (тесты для делегирования)
/DnsDynamicUpdate       (тесты для динамических обновлений)
/DnsRecordRegistration  (тесты для регистрации записей)
/DnsResolveExtName      (тесты для преобразования внешних имен)
/DnsAll                 includes all tests above)
/DnsInternetName:       <Интернет-имя> (для теста /DnsResolveExtName)
                        (по умолчанию www.microsoft.com)
```

Как обсуждалось ранее при рассмотрении записей SRV, количество таких записей, зарегистрированных контроллером домена, настолько велико, что определить на глаз, корректно ли они работают, достаточно трудно. В дополнение к тесту /registerinDNS прогоняются тесты /DnsDynamicUpdate и /DnsRecordRegistration, проверяющие регистрацию записей SRV контроллерами доменов. В отличие от /registerinDNS, они не обязательно должны запускаться локально на контроллере домена. Представленная ниже команда будет верифицировать записи SRV для контроллера домена. Опция /v означает "verbose" ("подробно"). Вывод получается длинным, поскольку в нем перечислены все записи SRV для контроллера домена.

```
C:\Users\Administrator.BF1>dcdiag /s:BF1.bigfirm.com
   /test:dns /dnsrecordregistration /v
```

Следующая команда будет проверять работоспособность обновлений DDNS для зоны. Она зарегистрирует хост и удалит его из зоны DNS сервера. В данном случае сервером является Ecoast.Bigfirm.com.

```
C:\Users\Administrator.BF1>dcdiag /s:ec1.Ecoast.Bigfirm.com
   /test:dns /dnsdynamicupdate /v
```

Инструмент DIG мощнее, чем NsLookup

Существует инструмент для устранения неполадок в DNS, который эксплуатируется в мире Unix на протяжении продолжительного времени и называется Domain Information Groper (Прощупывание доменной информации), или DIG. Если вы спросите у пользователей DIG их мнение о том, насколько сравнима утилита NsLookup с DIG как инструмент для устранения неполадок в DNS, то не удивляйтесь, если они сначала рассмеются, после чего вежливо скажут, что они вообще несравнимы!

Однако хорошая новость в том, что DIG можно загрузить совершенно бесплатно (http://www.isc.org/software/bind) и установить в среде Windows Server 2012 R2, тем самым серьезно усилив уровень устранения неполадок в DNS. Инструмент DIG можно запускать в обычном формате командной строки, но он располагает также пакетным режимом, который поддерживает чтение запросов просмотра из файла.

Сведения по установке DIG в системе Windows Server доступны по ссылке http://tinyurl.com/DIGinstall. Можете также просмотреть онлайновое руководство по работе с DIG, воспользовавшись ссылкой http://tinyurl.com/DIGusage.

Полезные ссылки по устранению неполадок в DNS

Все рассмотренные до сих пор инструменты основаны на том, что доступно в готовом виде в ОС Windows Server 2012 R2. Именно с этих инструментов вы должны начинать поиск и устранение проблем в сети. В настоящем разделе мы поделимся с вами адресами нескольких веб-сайтов, имеющих отношение к DNS, которые окажут содействие в решении проблем с внешними именами DNS.

- **www.IntoDNS.com.** Это простой, но эффективный веб-сайт, который вы должны добавить в свой арсенал инструментов для поиска и устранения неполадок в DNS. Когда вы достигаете домашней страницы, понадобится лишь ввести DNS-имя домена, о котором нужно получить информацию, и щелкнуть на кнопке Report (Отчет). В результате возвратится все доступные сведения по записям A (родительской), NS, SOA, MX и WWW для домена. Располагая этой информацией, вы можете быстро идентифицировать некорректно сконфигурированные записи или же просто использовать ее при перекрестном контроле предоставленных вам сведений.
- **www.MXToolbox.com.** Этот сайт делает намного больше того, что заявлено на его начальной странице. Он предназначен для содействия в поиске и устранении проблем с записями MX и может оказаться полезным при попытках выяснить, почему почтовый поток для отдельного домена электронной почты не работает. В отношении любого домена можно запускать несколько разных тестов, таких как просмотр MX, проверка черного списка (Blacklist), просмотр Whois и верификация SMTP. Если вы не пользовались этим сайтом ранее, то самое время добавить его в список закладок.

- **www.DNSStuff.com.** Это еще один популярный сайт, который можно применять для формирования отчетов по DNS, просмотров Whois и информации об IP-адресах. Здесь вы можете также получить доступ к большому количеству дополнительных инструментов для поиска и устранения проблем с DNS, если приобретете учетную запись на нем, но сначала имеет смысл оценить обещанные преимущества, воспользовавшись пробным периодом.

Резюме

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?

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?

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?

Глава 7

Active Directory в Windows Server 2012

Концепция, положенная в основу Active Directory, великолепна. Слово *Active* (активный) подразумевает динамическое поведение, а слово *Directory* (каталог) предполагает выполнение задач хранения и поиска компонентов. Полностью Active Directory можно описать так: центральное место, где хранятся и управляются все пользователи и компьютеры, а также формируется поведение инфраструктуры Windows. Компонент Active Directory появился в версии Windows 2000 Server и расширялся в версиях Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 и Windows Server 2008 R2. В современных бизнес-средах Active Directory играет важную роль в качестве централизованного решения по управлению идентификацией и доступом.

Хотя на протяжении некоторого времени Active Directory была очень устойчивой системой, специалисты из Microsoft настроили и добавили дополнительные средства, сделав Windows Server 2012 Active Directory еще более надежным, масштабируемым, защищенным и простым в управлении решением.

Однако один лишь факт того, что Active Directory очень легко устанавливать и настраивать, вовсе не означает, что можно просто запустить DCPROMO и пощелкать на кнопках Next (Далее), а в конце на Finish (Готово). Это больше не будет работать, к тому же имеются соображения, которые необходимо рассмотреть перед, во время и после установки Active Directory. В противном случае рано или поздно закончится тем, что вы получите неправильно сконфигурированную и некорректно функционирующую систему. В этой главе будет пролит свет не только на различные аспекты установки и конфигурирования Active Directory, но также на управление и обслуживание систем Active Directory.

Вероятно, вам наиболее интересно узнать, что появилось нового в версии Active Directory 2012; в этой и последующих главах вы научитесь устанавливать, конфигурировать и обслуживать Active Directory 2012.

В этой главе вы изучите следующие темы:

- создание леса с единственным доменом;
- добавление к домену второго контроллера домена (domain controller — DC);
- принятие решения о добавлении глобального каталога;
- создание учетных записей;
- создание детализированных политик паролей;
- понятие функционального уровня леса Windows Server 2012;
- модернизация домена до Windows Server 2012.

В настоящей главе мы собираемся ссылаться на версии Windows Server 2012 и Windows Server 2012 R2 просто как на Windows Server 2012. Если какие-то возможности доступны только в версии Windows Server 2012 R2, на это будет указано специально.

Введение в основы Active Directory

Лучше всего начать с изучения определений и терминов. Поскольку в Active Directory используется много специальных слов, ниже приведен словарь, который должны знать администраторы.

- **Рабочая группа (workgroup).** *Рабочая группа* — это по существу один или большее число компьютеров в локальной вычислительной сети Windows, которые *не* присоединены к домену. Каждый компьютер находится сам по себе, поэтому зависимости между ними отсутствуют. Например, на компьютере 1 имеется локальный пользователь по имени `Joe`, и на компьютере 2 также имеется локальный пользователь по имени `Joe`. Имена пользователей совпадают и принадлежат одному и тому же лицу, но это собой совершенно разные пользователи. Следовательно, если вы хотите управлять, к примеру, паролями этих пользователей, то вам придется подключиться или войти в систему на каждом компьютере и затем изменить пароль. Способа центрального управления такими пользователями не существует.
- **Домен (domain).** *Домен* — это коллекция объектов, которые совместно используют одну базу данных. Это значит, что в примере рабочей группы можно было бы создать одного пользователя `Joe` в центральной базе данных Active Directory и подключить к домену этой базы данных компьютеры 1 и 2 рабочей группы. Зачем нужен домен? Если все объекты управляются централизованно, нет необходимости в подключении или перемещению к каждому из них для изменения пароля у пользователя. Домен представляет собой намного более широкую концепцию, но для базового понимания такого примера вполне достаточно.
- **Служба домена Active Directory (Active Directory Domain Services).** Служба домена Active Directory (Active Directory Domain Services — AD DS) интегрирована в ОС Windows Server, но по умолчанию автоматически не устанавливается. Если вы планируете повысить сервер Windows до контроллера домена, либо существующего, либо полностью нового, то должны установить на этом сервере AD DS, создать базу данных Active Directory и добавить множество других компонентов, которые необходимы для надлежащего функционирования Active Directory. Поскольку Active Directory функционирует как служба Windows в фоновом

режиме, ее можно останавливать и запускать. Это крупное усовершенствование, т.к. устраняется необходимость загрузки в режиме восстановления для выполнения задач авторитетного восстановления или обслуживания базы данных Active Directory; взамен понадобится только остановить службу AD DS и выполнить интересующую операцию.

Каждый контроллер домена имеет собственную копию базы данных Active Directory, которая динамически обновляется другими контроллерами домена. Из-за того, что все системы, присоединенные или интегрированные с Active Directory, зависят от Active Directory, в целях избыточности очень важно иметь, по меньшей мере, два контроллера домена. В противном случае, если существующий в единственном экземпляре контроллер домена откажет, то остановится работа всей среды.

- **Сайт (site).** Сайты представляют физическую структуру или топологию сети. По определению *сайт* — это коллекция связанных друг с другом подсетей.

  Во многих случаях офисы филиалов создаются в виде сайтов. Мы предполагаем, что системы надежно соединены внутри сети офиса филиала, но имеют ограниченное сетевое подключение с головным офисом. В такой ситуации имеет смысл создать сайт для офиса филиала. О сайтах еще много чего можно сказать, но на данный момент этого вполне достаточно.

- **Репликация (replication).** *Репликация* является, пожалуй, самой сложной темой, относящейся к Active Directory. В Active Directory применяется система репликации с несколькими хозяевами. Это значит, что вы можете внести изменение, например, создав пользователя `Joe` на одном контроллере домена, и оно будет реплицировано на другой контроллер домена. Разумеется, объекты можно создавать, изменять и удалять. При этом любое изменение будет реплицировано на все контроллеры домена внутри сайта в пределах 15 секунд, а на контроллеры домена на разных сайтах не менее чем за 15 минут (по умолчанию за 180 минут). Active Directory строит наилучший путь репликации с использованием сложного алгоритма, так что каждый контроллер домена получает актуальные обновления.

- **Объекты (object).** Выражаясь кратко, все, что находится в Active Directory, является *объектом*. Например, пользователь `Joe` является объектом. Если вы измените его имя, то тем самым измените свойство пользователя `Joe`, которое хранится в атрибуте под названием First Name (Имя). К тому же, если вы создаете учетную запись компьютера, то группы, организационные единицы, сайты, подсети IP и т.д. будут объектами со свойствами.

- **Схема (schema).** *Схема* хранит классы для создаваемых вами объектов. Можете думать о схеме как о наборе шаблонов, которые будут применяться при создании пользователя `Joe`. Среде Active Directory необходимо знать, как будет выглядеть пользователь, к примеру, какие он имеет свойства — скажем, имя и фамилию. Это предоставляется схемой. Если вы планируете установить другое ПО, такое как Lync или Exchange, то схему понадобится расширить. Почему? Взглянув на объект пользователя до и после расширения схемы, вы обнаружите, что в нем появились дополнительные опции (свойства) вроде адреса SIP (Session Initiation Protocol — протокол инициирования сеанса). Адрес SIP используется для видео- и голосовых коммуникаций по протоколу Интернета (Internet Protocol — IP).

- **Групповая политика (Group Policy).** Как упоминалось ранее, *групповые политики* необходимы для конфигурирования настроек пользователей и компьютеров. Они очень удобны, поскольку в одной групповой политике можно сконфигурировать одну или большее количество настроек и применить их к одному и более пользователей и компьютеров, связав объект групповой политики (Group Policy object — GPO) с соответствующей организационной единицей (organizational unit — OU).

  В качестве примера давайте предположим, что на каждом сервере нужно включить удаленный рабочий стол, чтобы к серверам можно было подключаться с использованием клиента RDP. Установка этого вручную на каждом компьютере потребовала бы много работы. Вместо этого понадобится включить настройку удаленного рабочего стола в групповой политике и связать ее с OU, где находится ваш сервер, в результате чего на всех компьютерах внутри данной OU будет включен удаленный рабочий стол. Объекты GPO можно связывать с сайтами, доменами и организационными единицами. Когда вы повышаете сервер до контроллера домена, по умолчанию появляются две политики. Каждый домен имеет стандартную политику домена (Default Domain Policy) и стандартную политику контроллеров домена (Default Domain Controllers Policy).

- **Организационная единица (organizational unit).** Организационные единицы применяются для организации объектов в Active Directory, главным образом объектов пользователей и компьютеров. *Организационная единица* — это просто разновидность контейнера, который содержит похожие объекты. Существуют две главные причины для организации объектов в Active Directory. Первая причина касается связывания объектов GPO, а вторая объясняется необходимостью в наличии OU для делегирования управления.

  Предположим, что вы создали организационную единицу по имени `USERS` и поместили в нее пользователя `Joe`. Теперь нужно, чтобы пользователь `Joe` всегда получал свои сетевые диски. Следовательно, потребуется создать объект GPO и связать эту политику с организационной единицей `USERS`. После этого пользователь `Joe` будет получать настройки из объекта GPO и располагать всеми своими сетевыми дисками.

  Значок для OU выглядит как папка из проводника Windows, и поскольку она используется похожим образом, администраторы часто путаются и применяют OU подобно папкам Windows для группирования объектов с целью их более простого нахождения в будущем. Это не главное назначение организационных единиц. Конечно, вы можете использовать их для группирования и организации объектов с целью упрощения их поиска в Active Directory, но основной их замысел состоит в том, что администратор Active Directory должен иметь столько OU, сколько необходимо, чтобы применять делегирование управления и управлять объектами в OU посредством объектов GPO.

- **Стандартная политика домена (Default Domain Policy).** *Стандартная политика домена* создается сразу после создания первого домена. Эта политика содержит настройки для пользователей и компьютеров, которые будут применяться к целому домену. Важно понимать, что данная политика является неотъемлемой для среды и не должна удаляться. Ее можно модифицировать, но мы не рекоменду-

ем делать это. При необходимости применения к домену специальных настроек вы должны создать новую политику и сохранить эти настройки внутри нее.

- **Стандартная политика контроллеров домена (Default Domain Controllers Policy).** *Стандартная политика контроллеров домена* — также очень важная политика, которая связывается с контейнером Domain Controllers (Контроллеры домена) в Active Directory. Настройки, устанавливаемые в стандартной политике контроллеров домена, представляют собой специфичные конфигурации, которые применяются только к контроллерам домена. Если вы повышаете сервер, являющийся членом домена, до контроллера домена, он автоматически помещается в контейнер Domain Controllers. Существует очень мало случаев, когда придется касаться этой политики.
- **Лес (forest).** *Лес* — это одиночный экземпляр Active Directory. Внутри леса можно иметь один или несколько доменов, совместно использующих одну и ту же схему. В сущности, настроив единственный контроллер домена, вы создаете наименьший из возможных лес. Он также называется лесом с единственным доменом. На лес также ссылаются как на границу безопасности, внутри которой доступны пользователи, компьютеры и другие объекты.
- **Глобальный каталог (global catalog — GC).** *Глобальный каталог* содержит информацию о каждом объекте в любых доменах внутри леса с несколькими доменами Active Directory. Глобальный каталог хранится на контроллерах доменов, которые сконфигурированы как серверы глобального каталога, и его данные распространяются посредством репликации Active Directory. Внутри леса имеется только один глобальный каталог, но несколько его копий. Приложения вроде Exchange или клиенты обращаются к глобальному каталогу за информацией об объектах из леса. Глобальный каталог в домене содержит полные сведения об объектах в домене, но только частичную информацию об объектах в лесе. Глобальный каталог предлагает также другие службы, такие как предоставление ссылок на другие объекты в разных доменах, преобразование основных имен пользователей (user principal name — UPN) и кеширование членства в универсальных группах.
- **Доверительное отношение (trust).** *Доверительное отношение* — это соединение между доменами с целью доступа к их ресурсам, таким как серверы и приложения. Например, это можно было бы применять, если некоторым пользователям необходим доступ к общим файлам или информации из интрасети другого домена. Если вы установите домен и дочерние домены, Active Directory автоматически создаст транзитивное доверительное отношение. В результате вы сможете получать доступ из корневого домена к объектам в дочерних доменах и наоборот. Когда нужен доступ к ресурсам в другом лесе, можно создать доверительное отношение какой-нибудь формы для соединения обоих лесов.
- **Дерево (tree).** Если вы строите один или несколько доменов внутри того же самого леса, который имеет непрерывное пространство имен и/или совместно используют одну и ту же схему, то вы создаете *дерево*. Непрерывное пространство имен — это домен, разделяющий то же самое имя корневого домена. Например, для корневого домена `bigfirm.com` непрерывное пространство имен может выглядеть как `marketing.bigfirm.com`. Дерево Active Directory является коллекция доменов, которая построена на основе иерархии транзитивных доверительных отношений.

Создание леса с единственным доменом

Как вы уже знаете, лес с единственным доменом — это простейшая топология Active Directory, которую только можно построить. Согласно общей рекомендации, домен Active Directory необходимо создавать при наличии 10 или более пользователей. Домен можно было бы также создать и при меньшем количестве пользователей, поскольку никаких ограничений здесь не предусмотрено; все дело лишь в сложности и затратах. Преимущества создания домена очевидны:

- управление пользователями и разрешениями из центрального места;
- централизованная зашита и управление всеми системами с использованием объектов GPO;
- предоставление дополнительных зависимых от Active Directory служб.

Вас может интересовать, должны ли вы придерживаться одного домена или зачем может понадобиться добавление дополнительных доменов в инфраструктуру. Когда только возможно, вы должны создавать лес с единственным доменом, т.к. он проще в настройке и управлении. Существует ряд ситуаций, при которых может быть рассмотрен вопрос создания более одного домена. Поскольку служба Windows Server 2012 Active Directory в версии Windows Server 2008 R2 не изменялась, перечисленные ниже правила по-прежнему актуальны. Несколько доменов должны применяться в следующих случаях.

- Вы имеете дело с очень медленными каналами глобальной сети (WAN) и переживаете по поводу производительности репликации. Это становится даже более важным при наличии очень большого объема изменений в атрибутах или объектах внутри Active Directory.
- У вас есть унаследованный домен, который должен быть предохранен.
- Ваш домен очень динамичен и объекты в нем изменяются часто. В этом случае трафик репликации может оказаться чрезмерным при достижении порога в 100 000 объектов. Одной из опций для разделения трафика репликации является разделение домена.

Важно понимать, что причины создания нескольких доменов связаны не с тем, что один домен приближается к своим техническим пределам; проблема кроется в репликации, которая может привести к возникновению множества проблем в инфраструктуре. Ранее мы обсуждали, что единственный домен — это наименьший лес, который можно создать. Точно так же, как можно установить несколько доменов в лесе, имеется возможность создания множества лесов. Ниже приведены некоторые причины для создания нескольких лесов.

- Вы должны обеспечить так называемую административную автономию. Возможно, некоторые отделы внутри вашей компании не доверяют друг другу. Или, может быть, существуют причины, связанные с безопасностью, вроде полной изоляции инфраструктуры IT отдела кадров. Также, возможно, нет соглашения по изменениям схемы.
- Вам необходимо отделить приложения и службы от остальной инфраструктуры. Может потребоваться установить кластеры Hyper-V в отдельном лесе (структуре) и установить инструменты управления, такие как продукты системного центра (System Center), в другом лесе. Имейте в виду, что чем больше лесов Active Directory вы строите, тем быстрее растет сложность и затраты на управление, достигая уровня, которого вы могли не ожидать.

Преимущества наличия единственного домена

Преимущества наличия единственного домена вполне очевидны.

- **Стоимость.** В случае построения одного домена рекомендуется установить хотя бы два контроллера домена для обеспечения избыточности. Конечно, при установке дополнительных контроллеров доменов для новых доменов или лесов стоимость лицензий, оборудования, ПО, а также затраты на управление и обслуживание добавочных серверов всегда увеличивается. Несмотря на возможность виртуализации любого контроллера домена, все равно придется платить за хранение и управление такими серверами.
- **Управление.** Любой добавляемый домен будет иметь дополнительные объекты, которыми необходимо управлять. Кроме того, есть много сложных задач по настройке разрешений между доменами или даже между лесами, а также по применению вложения групп для совместного использования ресурсов либо поддержания всех доменов и лесов в работоспособном состоянии.
- **Восстановление в аварийных ситуациях.** Active Directory — очень сложный компонент в плане восстановления домена или даже леса. Всегда проще восстановить один домен, а не два и более.

В Windows Server 2008 были введены детализированные политики паролей. Они решают давнишнюю проблему, которая вынуждала создавать еще один отдельный домен. Детализированные политики паролей позволяют создавать несколько политик в отношении паролей. В ранних версиях Active Directory могла существовать только одна политика паролей. В Windows Server 2012 детализированные политики паролей остались теми же, что и в версии Windows Server 2008, но был предложен дружественный к пользователю интерфейс для более простого управления ими.

Создание леса с единственным доменом

Вы можете обнаружить, что основы Active Directory не претерпели никаких изменений. Поскольку большинство терминов уже раскрыты, все готово к рассмотрению процесса построения леса с единственным доменом. Но прежде чем приступить к созданию нового домена, необходимо прояснить ряд моментов:

- версия Windows Server 2012;
- конфигурация сервера;
- конфигурация развертывания;
- совместимость операционной системы;
- имя домена;
- функциональный уровень леса;
- функциональный уровень домена;
- DNS;
- расположение файлов;
- пароль администратора DSRM (Directory Services Restore Mode — режим восстановления службы каталогов).

Все эти моменты будут подробно обсуждаться в последующих разделах главы.

Версия Windows Server 2012

В Microsoft упростили ситуацию с версиями и предлагают всего две редакции Windows Server 2012, которые можно использовать при настройке контроллеров домена: Standard и Datacenter. Между ними нет отличий в функциональности, доступности или компонентах. Разница касается условий лицензирования и количества виртуальных машин, которые можно запускать под управлением каждой редакции. В начале книги отличия между этими двумя версиями объяснялись более подробно. Когда необходимо установить контроллер домена, вы всегда можете выбрать редакцию Windows Server 2012 Standard, а если позволяет лицензионное соглашение, можете установить редакцию Windows Server 2012 Datacenter. Следует также иметь в виду, что ОС Windows Server 2012 доступна только в виде 64-разрядных версий; 32-разрядных версий не существует в принципе. Это важно при планировании модернизации контроллеров доменов. Модернизация на месте 32-разрядной системы до 64-разрядной невозможна.

Конфигурация сервера

После установки редакции Windows Server 2012 Standard понадобится сконфигурировать имя и IP-адрес сервера. Просто ради ясности: мы используем редакцию Windows Server 2012 Standard, потому что ее функциональность идентична редакции Windows Server 2012 Datacenter. Единственное отличие связано с лицензией.

Имя сервера

Перед повышением до контроллера домена компьютеру необходимо назначить окончательное имя. Какие имена серверов следует считать удачными? Об именовании серверов можно было написать отдельную книгу, но есть несколько основных аспектов, которые должны быть приняты во внимание.

- Не применяйте в именах серверов название компании, отдела, региона или другие имена, которые со временем могут измениться.
- Выбирайте короткие имена; администратор будет вам благодарен.
- Используйте аббревиатуры для идентификации серверных ролей.

Общепринятой схемой именования контроллеров доменов является `DC01`, `DC02` и т.д. Переименовать контроллер домена можно с помощью графического пользовательского интерфейса либо инструмента `Netdom`.

IP-адрес

Поскольку клиенты и серверы ищут контроллер домена с использованием DNS, и ваш контроллер домена преимущественно имеет установленную роль DNS, вы должны всегда назначать ему статический IP-адрес. В противном случае ваш контроллер домена превратится для других систем в движущуюся мишень при попытке его нахождения. Если вы конфигурируете только адрес IPv4, рекомендуется оставить включенным IPv6.

Вам может показаться, что все уже готово к запуску `DCPromo`. Неплохая идея, но вы получите лишь окно с сообщением о том, что это больше не работает.

Установка серверной роли контроллера домена

Чтобы установить серверную роль контроллера домена, понадобится запустить диспетчер серверов (Server Manager) и выбрать в меню Manage (Управление) пункт Add Roles and Features (Добавить роли и компоненты), как показано на рис. 7.1.

Рис. 7.1. Добавление к серверу роли Active Directory

Запустится мастер, который позволит выбрать роль или компонент для установки. В Windows Server 2008 R2 для роли или компонента предусмотрены два отдельных мастера. Мастер добавления ролей и компонентов (Add Roles and Features Wizard) установит все двоичные файлы, необходимые для последующего запуска мастера конфигурирования службы домена Active Directory (Active Directory Domain Services Configuration Wizard — ADDSCW).

Когда мастер завершит работу, вам нужно вернуться в окно диспетчера серверов и щелкнуть на значке с восклицательным знаком желтого цвета (рис. 7.2).

Это предоставит возможность повысить сервер до контроллера домена (рис. 7.3). Последующие шаги очень похожи на работу утилиты `DCPromo`, которая применялась в версии Windows Server 2008 R2.

Мастер предложит несколько вариантов; вы должны либо выбрать, либо ввести соответствующую информацию. В зависимости от выбранного варианта мастер будет изменять отображаемые экраны.

Конфигурация развертывания

Опция конфигурации развертывания позволяет указать, должен ли новый домен создаваться в новом лесе или же добавляться в существующий лес. Если выбран вариант добавления в существующий лес, можно добавить контроллер домена к существующему домену (это будет показано позже в данной главе) либо создать новый домен.

Для первого контроллера домена выбор прост — будет создан новый домен в новом лесе.

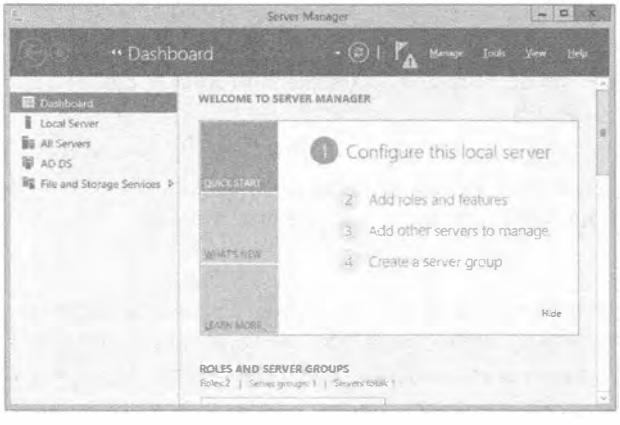


Рис. 7.2. Запуск мастера установки

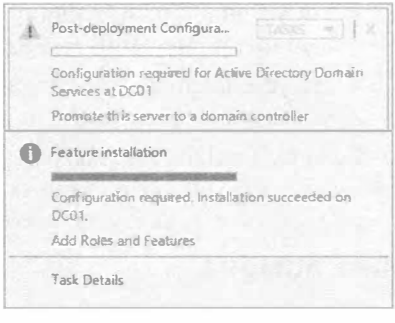


Рис. 7.3. Повышение сервера до контроллера домена

Проблема аутентификации

Контроллеры доменов, функционирующие под управлением Windows Server 2008 и последующих версий, в том числе Windows Server 2012, имеют опцию Allow cryptography algorithms compatible with Windows NT 4.0 (Разрешить криптографические алгоритмы, совместимые с Windows NT 4.0), которая по умолчанию отключена. Унаследованные криптографические алгоритмы, используемые в Windows NT 4.0, могут быть взломаны с помощью современных технологий.

По этой причине в Microsoft усилили защиту контроллера домена за счет настройки групповой политики, которая предотвращает вход из оборудования и клиентов, применяющих слабые криптографические алгоритмы Windows NT 4.0. Это может быть клиент SAMBA Server Message Block (SMB), который не способен установить безопасный канал с контроллером домена Windows Server 2008 или выше, либо устройство хранения SMB, не умеющее создать безопасный канал с контроллером домена. Чтобы обойти указанное ограничение, потребуется включить эту настройку в стандартной политике контроллеров домена (Default Domain Controllers Policy). Дополнительные сведения доступны по ссылке `http://support.microsoft.com/kb/942564/`.

Совместимость операционной системы

В Windows Server 2012 появилась файловая система ReFS (Resilient File System — отказоустойчивая файловая система). Эта файловая система более устойчива к отказам, чем NTFS. Она предоставляет более высокую целостность и масштабируемость, а также обладает встроенной проактивной идентификацией ошибок. Из-за ее высоких качеств у вас может возникнуть искушение выбирать файловую систему ReFS для всех предстоящих проектов по развертыванию серверов, но, к сожалению, ей присущи ограничения, которые вы должны иметь в виду.

- Файловая система ReFS доступна только в Windows Server 2012.
- Файловая система ReFS используется только для томов данных. Не существует методов применения ReFS на томе ОС или загрузочном томе.

Как администратор Active Directory, вы должны знать следующий передовой опыт.

- Для хранения папки SYSVOL, базы данных Active Directory и журнальных файлов Active Directory используйте только NTFS.
- Не устанавливайте папку SYSVOL на томе или диске, сформатированном с файловой системой ReFS.
- Не устанавливайте базу данных Active Directory на томе или диске, сформатированном с файловой системой ReFS.

Если вы попытаетесь выбрать диск, сформатированный с файловой системой ReFS, для папки SYSVOL, базы данных Active Directory или журнального файла, вы получите сообщение об ошибке, указывающее на необходимость выбора диска NTFS.

Имя домена

Поскольку это первый контроллер домена, вы выберете вариант с добавлением нового леса. Таким образом, понадобится также установить DNS и глобальный каталог. И DNS, и GC являются обязательными для первого контроллера домена в лесе. Установить в качестве первого контроллера домена контроллер домена только для чтения (read-only domain controller — RODC) невозможно, так что данная опция недоступна.

Именование корневого домена

Назначение имени корневому домену является, пожалуй, наиболее трудной частью работы. При настройке контроллера домена в испытательной среде заботиться об имени нет необходимости. Но ситуация меняется, когда нужно построить домен или лес в производственной среде. Поскольку NetBIOS-имя домена будет появляться где-то на стороне клиента, руководству может не понравиться видеть это имя на своих рабочих столах после входа в систему. Мы настоятельно рекомендуем обсудить и утвердить выбранное имя домена у ответственного менеджера.

На что должно быть похоже имя домена? Как вам известно, допустимое имя корневого домена Active Directory выглядит подобно полному имени домена (fully qualified domain name — FQDN). В нем присутствуют две части: действительное имя и суффикс, такой как `bigfirm.com`, `mydomain.local` или `forest.com`. Все они являются допустимыми именами доменов. В Windows Server 2003 можно было выбирать имя домена с единственной меткой наподобие `bigfirm`, `mydomain` или `forest`, и оно поддерживалось Microsoft. Но по мере того, как приложения вроде Exchange развивались и начали зависеть от Active Directory и DNS, имена доменов с единственной меткой больше не разрешены. Если вы попытаетесь создать домен с единственной меткой в Windows Server 2012, то получите сообщение об ошибке.

Во второй части домена верхнего уровня можно применять суффикс, такой как `.com`, `.gov`, `.ch` либо `.net`, или, возможно, вы отдадите предпочтение другому суффиксу, подобному `.local` или `.domain`.

Ниже перечислены преимущества наличия одного и того же имени для Active Directory и публичного DNS-имени, такого как `bigfirm.com`.

- Адреса URL веб-приложений компании одинаковы независимо от того, внутренние они или внешние.
- Открытые сертификаты можно использовать внутренне.
- Адрес SIP в Lync имеет тот же самый вид, как адрес электронной почты и адрес входа в систему.
- Учетные данные для входа в систему могут применяться в качестве адреса электронной почты.

Один из крупных недостатков заключается в том, что с точки зрения брандмауэра нелегко различать внутренние и внешние зоны. Многие администраторы специально стараются избегать использования имен доменов верхнего уровня Интернета, чтобы не путать их с внутренними сетями.

Как видите, с каждым вариантом связаны свои достоинства и недостатки. В целом мы не можем рекомендовать какое-то одно соглашение об именовании. В конце концов, имя должно соответствовать существующим у вас техническим требованиям и также удовлетворять политике безопасности, принятой в компании.

Active Directory и DNS

Важно знать, что Active Directory сильно зависит от DNS. Нет DNS, не будет и Active Directory. Почему? Active Directory регистрирует все типы записей служб (SRV) в DNS, чтобы находить специфичные службы, которые необходимы для корректного функционирования Active Directory. Приблизительно 80% проблем нерабочей службы Active Directory имеют отношение к DNS.

Когда вы установите свой контроллер домена, отобразится диалоговое окно с предупреждением о том, что не удается создать делегирование для DNS. Причина связана с тем, что мастер настройки Active Directory конфигурирует DNS; он также пытается создать делегирование для DNS-сервера, однако он еще не установлен. Закройте это диалоговое окно и продолжайте.

Функциональные уровни домена

Во время работы мастер настройки Active Directory предложит выбрать функциональный уровень домена. Функциональный уровень домена зависит от операционной системы, используемой на контроллере домена. Выбрать более высокий функциональный уровень, нежели тот, который имеет самая старая версия ОС, не удастся.

В Windows Server 2012 доступны следующие функциональные уровни домена:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Минимальным уровнем, требуемым для присоединения контроллера домена Windows Server 2012 к другому домену, является функциональный уровень леса Windows Server 2003. Это значит, что операционные системы версий, предшествующих Windows Server 2003, не будут допустимыми. Другими словами, установить контроллер домена в лес с функциональным уровнем леса Windows 2000 Server нет никакой возможности.

Если вы устанавливаете контроллер домена, то можете выбрать любой функциональный уровень домена вплоть до Windows Server 2012. Учтите, что если вы выберете функциональный уровень домена Windows Server 2012, то не сможете добавлять контроллеры домена, отличные от Windows Server 2012. Таким образом, если вы присоедините контроллер домена Windows Server 2012 к функциональному уровню домена Windows Server 2008 R2, то не сможете поднять функциональный уровень до Windows Server 2012 при наличии контроллера домена Windows Server 2008 R2.

Необходимо запомнить следующие два важных аспекта.

- Если требования удовлетворены, вы всегда сможете поднять функциональный уровень.
- Практически никогда вы не сможете понизить функциональный уровень.

  Существует одно исключение. Можно понизить функциональный уровень леса и домена от Windows Server 2012 до Windows Server 2008 R2. За деталями обращайтесь на врезку "Функциональный уровень (не) может быть понижен" далее в этой главе.

Это похоже на то, когда нужно посолить бульон. Вы всегда можете добавить еще соли, но если вы пересолите, то изъять соль обратно не удастся. Если нет уверенности, лучше сначала выбрать более низкий функциональный уровень наподобие Windows Server 2008.

Функциональный уровень применяется к контроллерам домена, а не к серверам-членам

Если функциональным уровнем является Windows Server 2012, то домен будет поддерживать только те контроллеры домена, на которых установлена ОС Windows Server 2012. Серверы-члены с более старыми версиями ОС допускаются, но это не относится к контроллерам домена.

С функциональными уровнями всегда возникает путаница. Пользователи часто задают вопросы вроде перечисленных ниже.

- Можно ли добавить в домен с функциональным уровнем домена Windows Server 2012 сервер-член Windows Server 2008? Да!
- Может ли домен с функциональным уровнем домена Windows Server 2012 поддерживать контроллер домена Windows Server 2008 R2? Нет!
- Можно ли добавить сервер Windows Server 2012 в домен с функциональным уровнем домена Windows Server 2008 R2? Да. Вы добавляете всего лишь сервер-член, а не контроллер домена.

При работе с мастером ADDSCW функциональный уровень домена можно выбирать (рис. 7.4).

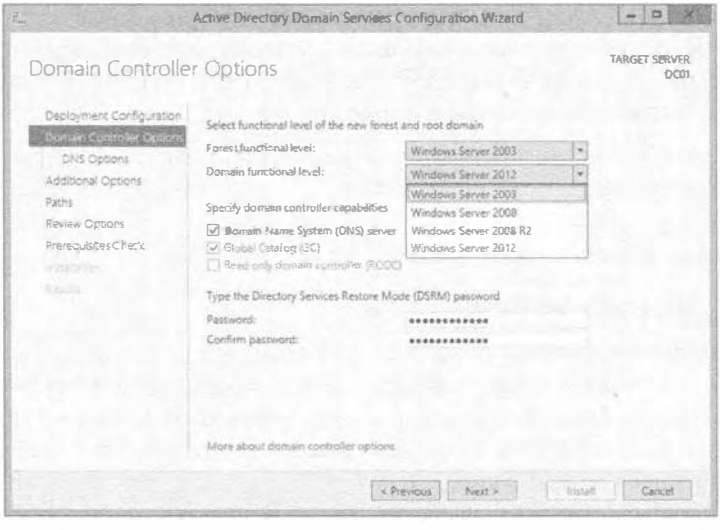


Рис. 7.4. Выбор функционального уровня домена в мастере ADDSCW

В ранних версиях Windows Server компоненты, доступные в лесе домена, зависели от функциональных уровней Active Directory.

Функциональный уровень домена Windows Server 2003

- Можно переименовывать контроллеры доменов с помощью `Netdom.exe`.
- Добавлен атрибут `lastLogonTimestamp`.
- Имеется возможность переадресации контейнеров `Users` (Пользователи) и `Computers` (Компьютеры).

- Поддерживается избирательная аутентификация для указания, кто имеет доступ к тем или иным ресурсам в доверенном лесе.
- Имеется ограниченное делегирование с целью зашиты учетных данных делегированного пользователя с применением Kerberos.

Функциональный уровень домена Windows Server 2008

- Предоставляется поддержка DFS-R для папки SYSVOL.
- Доступна поддержка алгоритмов шифрования AES 128 и AES 256 для Kerberos.
- Предоставляется детальная информация о последнем интерактивном входе в систему.
- Используются детализированные политики паролей.

Функциональный уровень домена Windows Server 2008 R2

- Обеспечение механизма аутентификации определяет метод входа в систему, применяемый пользователем. Это хранится в маркере Kerberos.
- Автоматическое управление SPN доступно для учетных записей управляемых служб (Managed Service Accounts).

Функциональный уровень домена Windows Server 2012

- Поддержка KDC доступна для утверждений, комплексной аутентификации и защиты Kerberos через две настройки: Always provide claims (Всегда предоставлять утверждения) и Fail unarmored authentication requests (Отклонять незащищенные запросы на аутентификацию).

За подробным списком возможностей, доступных на каждом функциональном уровне, обращайтесь по следующему URL:

```
http://technet.microsoft.com/en-us/library/
  understanding-active-directory-functional-levels(WS.10).aspx
```

Функциональные уровни леса

Функциональные уровни леса идентифицируют возможности внутри леса. Функциональные уровни домена зависят от операционной системы контроллеров домена, а функциональные уровни леса — от функционального уровня домена. Поднять функциональный уровень леса выше самого низкого функционального уровня домена в лесе невозможно.

Функциональный уровень леса также можно выбирать во время установки Active Directory. Поддерживаются следующие функциональные уровни леса:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Как и с функциональным уровнем домена, функциональный уровень леса можно поднимать после того, как был повышен DC. Сначала понадобится поднять функциональный уровень каждого домена в лесе до одного и того же уровня, а затем поднять до такого же уровня функциональный уровень леса. Помните, что прежде чем

можно будет поднять функциональный уровень леса, все функциональные уровни домена должны быть одинаковыми (рис. 7.5).

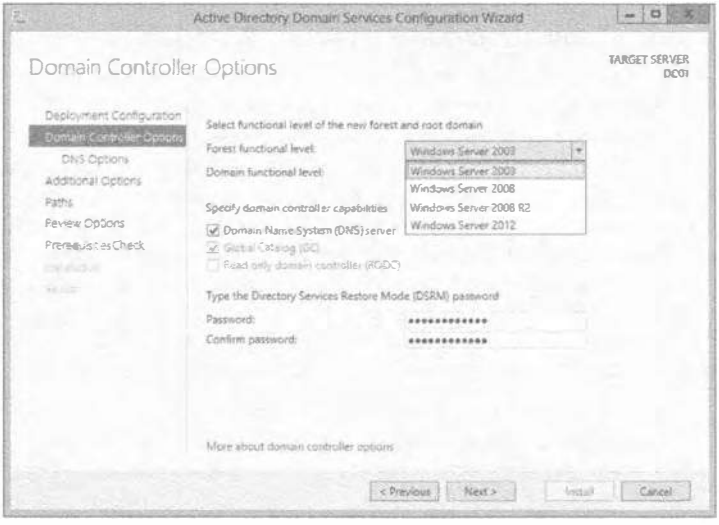


Рис. 7.5. Выбор функционального уровня леса в мастере ADDSCW

Точно так же как разные функциональные уровни домена добавляют средства к домену, разные функциональные уровни леса предоставляют разнообразные возможности.

- **Windows Server 2003.** Функциональный уровень леса Windows Server 2003 поддерживает следующие средства.
  - Возможность создания доверительных отношений в лесе.
  - Возможность переименования домена.
  - Возможность развертывания контроллера домена только для чтения (RODC).
  - Усовершенствованное средство проверки целостности знаний (Knowledge Consistency Checker — KCC).
  - Усовершенствованная репликация связанных значений (linked-value replication), при которой реплицируются только различия членства в группах.
  - Перечисление на основе доступа в пространстве имен DFS.
- **Windows Server 2008.** Функциональный уровень леса Windows Server 2008 не предлагает каких-то дополнительных возможностей.
- **Windows Server 2008 R2.** Корзина Active Directory (Active Directory Recycle Bin) позволяет восстанавливать удаленные объекты без необходимости в перезапуске контроллера домена в режиме восстановления Active Directory (Active Directory Restore Mode). Вы должны включать поддержку Active Directory Recycle Bin с использованием командлетов PowerShell. Корзина Active Directory — это великолепное средство, которое было улучшено в Windows Server 2012. Теперь корзину намного проще настраивать и управлять ею, как будет показано далее в этой книге.

- **Windows Server 2012.** Функциональный уровень леса Windows Server 2012 не предлагает каких-то дополнительных возможностей.

Что изменилось в функциональных уровнях Windows Server 2012 R2

При написании этой книги мы пользовались предварительной версией Windows Server 2012 R2. Хотя в Active Directory мало что изменилось, внесены определенные изменения в функциональные уровни по сравнению с предшествующей версией.

Контроллер домена Windows Server 2012 R2 можно добавить в существующую среду с функциональным уровнем Windows Server 2003. Но примите во внимание, что функциональные уровни домена и леса Windows Server 2003 объявлены устаревшими. Во время развертывания Windows Server 2012 R2 в существующей среде Windows Server 2003 будет предложено перейти на более высокий функциональный уровень. Самым низким функциональным уровнем, который можно выбрать в Windows Server 2012 R2, является функциональный уровень домена и леса Windows Server 2008. Полномасштабный обзор нового функционального уровня доступен по следующей ссылке:

```
http://technet.microsoft.com/en-us/library/
  understanding-active-directory-functional-levels.aspx
```

Местоположения для файлов и папки SYSVOL

Мастер Active Directory Domain Services Configuration Wizard запросит местоположение для различных файлов Active Directory и для общей папки SYSVOL.

Общая папка SYSVOL применяется для совместного использования информации, такой как сценарии и элементы объектов групповой политики, контроллерами домена. Папка SYSVOL, база данных Active Directory и журнальные файлы должны быть помещены на диск, сформатированный с файловой системой NTFS. База данных и журнальные файлы могут располагаться на разных дисках при условии, что они сформатированы как NTFS (рис. 7.6).

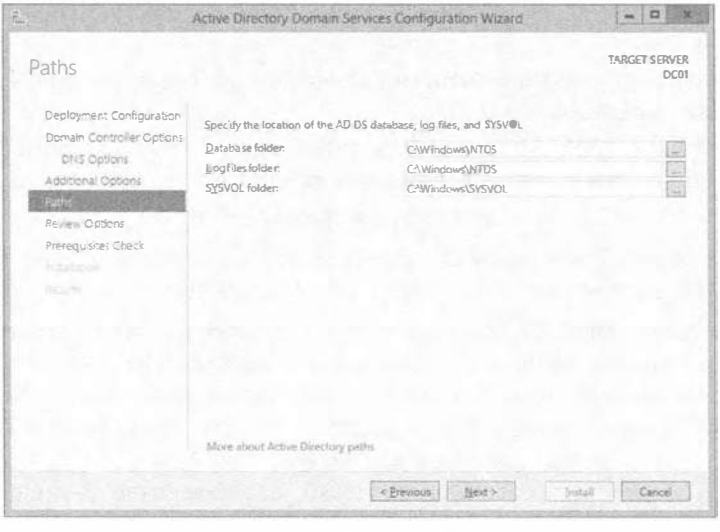


Рис. 7.6. Пути к файлам

В Windows Server 2012 появилась новая файловая система Resilient File System (ReFS), которая предлагает более высокую целостность и масштабируемость и обладает встроенной проактивной идентификацией ошибок. Вы можете подумать, что она была бы наилучшим местом для размещения какого-то компонента Active Directory, но как обсуждалось ранее, это не поддерживается, т.е. в ReFS нельзя помещать ни базу данных Active Directory, ни журнальный файл Active Directory, ни папку SYSVOL.

В своей основе Active Directory является крупной базой данных, а базы данных имеют основной файл данных и файл журнала транзакций. Изменения, предназначенные для базы данных, сначала записываются в файл журнала транзакций, который впоследствии периодически проверяется — это просто необычный способ указать, что изменения в файле журнала транзакций зафиксированы в базе данных.

Журнал транзакций обеспечивает для базы данных Active Directory высокую отказоустойчивость и возможности восстановления. Если на сервере пропадает электропитание где-то в середине процесса внесения изменения, с помощью этого журнала Active Directory может гарантировать, что после перезагрузки сервера база данных будет находиться в согласованном состоянии. Любые изменения, занесенные в журнал, фиксируются в базе данных, а незавершенные изменения, записанные в журнале, игнорируются.

С точки зрения производительности возможно увеличение производительности DC путем перемещения файлов журнала транзакций на другие диски. Для достижения оптимальной производительности Active Directory вы можете применять конфигурацию, подобную показанной ниже:

- диск C:\ — операционная система;
- диск D:\ — файл базы данных Active Directory и папка SYSVOL;
- диск E:\ — файл журнала транзакций.

При такой конфигурации каждый диск должен быть отдельным шпинделем (отдельным физическим диском). Единственный диск с тремя разделами не даст никакого выигрыша в производительности. Вдобавок, если дисковые устройства имеют разные скорости, вы должны поместить ОС на самый быстрый диск, файл журнала транзакций — на следующий в порядке убывания скорости диск, а папку SYSVOL — на самый медленный диск. С операционной системой и журналом транзакций связано наиболее интенсивное использование.

Чтобы еще немного оптимизировать контроллер домена, можно провести различие между интенсивными операциями чтения и интенсивными операциями записи. При наличии интенсивных операций чтения вы должны предоставить контроллеру домена столько памяти, чтобы было достаточно для кеширования базы данных в памяти. В случае интенсивных операций записи улучшить производительность можно за счет добавления следующего оборудования:

- аппаратные контроллеры RAID;
- диски с высоким числом оборотов в минуту;
- батарейный модуль кеширования (battery backed write-caching — BBWC) на контроллере RAID.

Все это звучит хорошо и имеет смысл, но что произойдет, если вы виртуализируете свой контроллер домена? В таком случае неплохо добавить к контроллеру домена достаточный объем памяти, чтобы он мог кешировать базу данных. Если вы собираетесь размещать журнал транзакций, базу данных и папку SYSVOL на разных виртуальных дисках, то улучшения производительности, скорее всего, окажутся минимальными. Проблема в том, что все виртуальные диски находятся под одним и тем же номером логического устройства (Logical Unit Number — LUN), и данный номер LUN распространяется на весь массив дисков. Это значит, что все виртуальные диски совместно используют те же самые физические диски в хранилище. С теоретической точки зрения было бы лучше поместить каждый файл в отдельный массив или LUN. В любом случае вы должны применять самое быстрое устройство хранения из тех, что есть в наличии.

Хорошей отправной точкой при выяснении, имеется ли проблема с дисковой производительностью, может быть просмотр перечисленных ниже счетчиков производительности. Каждый из этих счетчиков должен иметь низкое значение:

- Avg. Disk Queue Length (Средняя длина очереди к диску)
- Avg. Disk Read Queue Length (Средняя длина очереди к диску на чтение)
- Avg. Disk Write Queue Length (Средняя длина очереди к диску на запись)

Давайте рассмотрим пример. Если домен включает 100 пользователей, вы можете хранить файлы базы данных и журнала транзакций на диске C: вместе с операционной системой и не заметить никаких проблем с производительностью. С другой стороны, если вы поддерживаете 50 000 пользователей, то наверняка стремитесь контролировать малейшие аспекты производительности сервера, поэтому хотите разнести файлы базы данных и журнала транзакций по разным дискам. При построении тестовой системы можно благополучно оставить все на диске C:.

Перемещение файлов базы данных и журнала транзакций

В Windows Server 2012 была введена перезапускаемая служба Active Directory Domain Services (AD DS), которую можно применять для выполнения задач по управлению базой данных без необходимости в перезапуске контроллера домена в режиме восстановления службы каталогов (Directory Services Restore Mode — DSRM). Если нужно переместить журнал или базу данных на другой диск, можно воспользоваться утилитой командной строки `NTDSUtil`. Из-за характеристики AD DS перезапускать контроллер домена в режиме DSRM не придется; понадобится лишь остановить службу Windows AD DS и выполнить задачу.

Пароль администратора Directory Services Restore Mode

Если когда-либо придется проводить обслуживание или восстановление Active Directory, вы будете применять режим Directory Services Restore Mode. Для доступа к режиму DSRM нажмите клавишу <F8>, чтобы попасть в меню Advanced Options (Дополнительные опции). Это меню также позволяет получить доступ к различным опциям Safe Mode (Безопасный режим).

После выбора Directory Services Restore Mode будет предложено войти в систему. Тем не менее, Active Directory не запускается, поэтому использовать учетную за-

пись Active Directory нельзя. Вместо этого будет применяться специальная учетная запись администратора с другим паролем. Мастер Active Directory Domain Services Configuration Wizard предлагает установить этот пароль, как показано на рис. 7.7.

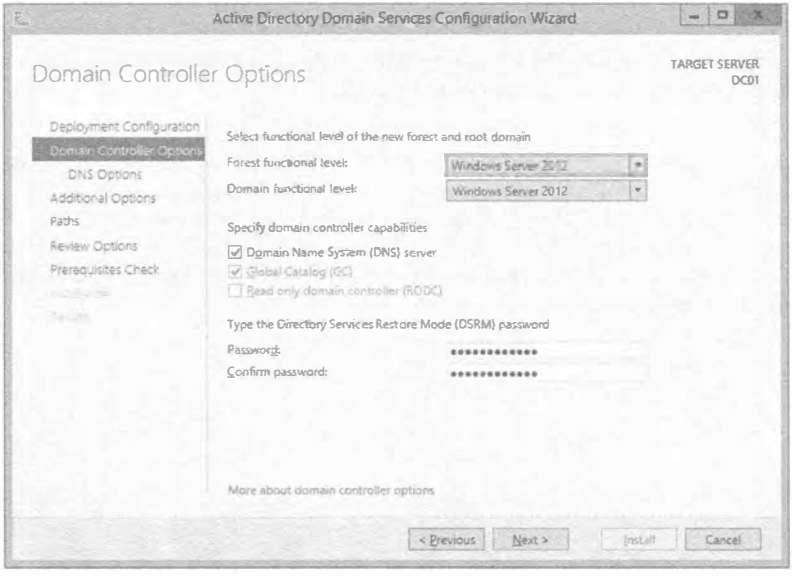


Рис. 7.7. Установка пароля администратора режима Directory Services Restore Mode

Обязательно документируйте устанавливаемый здесь пароль. Многие организации документируют критически важные пароли, записывая их и сохраняя в безопасном месте. Без этого пароля доступ к режиму DSRM невозможен. Иногда пароль учетной записи администратора DSRM путают с паролем обычного администратора, устанавливаемым для учетной записи Domain Admins (Администраторы домена), но это разные пароли. С точки зрения безопасности пароль администратора DSRM критически важен для того, чтобы локально войти в систему контроллера домена и получить доступ к базе данных Active Directory. Если вы осознаете, что в этой базе данных хранятся все пароли, то весьма ответственно отнесетесь к тому, где сохранить пароль администратора DSRM.

Запуск мастера Active Directory Domain Services Configuration Wizard

Теперь, когда вам известно, с чем вы столкнетесь, можно переходить к добавлению роли Active Directory и запуску мастера Active Directory Domain Services Configuration Wizard. В Windows Server 2012 добавление роли Active Directory по существу приводило к добавлению всех необходимых двоичных файлов, после чего можно было конфигурировать Active Directory.

В приведенных далее шагах предполагается наличие чистой установки Windows Server 2012 без каких-либо дополнительных установленных ролей.

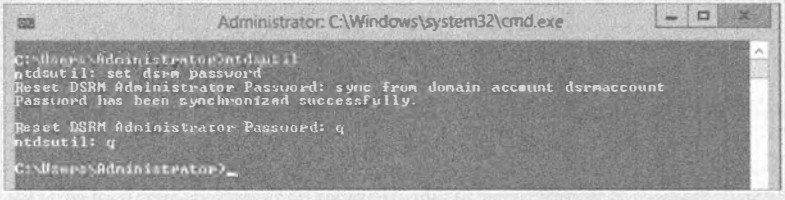
Изменение пароля администратора DSRM

При наличии 100 контроллеров домена довольно трудно контролировать каждый пароль администратора DSRM. Вдобавок может потребоваться изменить какой-то пароль DSRM. Изменить пароль можно старым способом, запустив утилиту DSMGMT или NTDSUtil на функционирующем контроллере домена. Для изменения пароля DSRM входить в режим DSRM не понадобится. За дополнительными сведениями по этому поводу обращайтесь к следующей ссылке:

```
http://technet.microsoft.com/en-us/library/cc753343.aspx
```

Один странный способ сохранения пароля DSRM известным в случае его изменения предполагает его синхронизацию с паролем учетной записи какого-то пользователя домена. Как это работает? Для начала необходимо создать учетную запись пользователя домена, к примеру, DSRMAccount. Это может быть учетная запись обычного пользователя домена. Затем откройте окно командной строки с повышенными разрешениями и введите следующую команду:

```
NTDSUtil
Set dsrm password
SYNC FROM DOMAIN ACCOUNT DSRMAccount
Q
Q
```



Теперь учетная запись администратора DSRM синхронизирована с учетной записью DSRMAccount в Active Directory. Однако это синхронизирует пароль не навсегда, а только на данный момент. Таким образом, если вы измените пароль учетной записи DSRMAccount, вам придется выполнять показанную выше команду еще раз. Здесь можно либо применять объект GPO ко всем контроллерам домена посредством запланированной задачи, чтобы запускать эту команду на регулярной основе, либо написать сценарий PowerShell для выполнения команды на всех контроллерах домена. В будущем нужно лишь запустить утилиту C:\Windows\System32\NTDSUtil.exe и предоставить ей следующие параметры:

```
"SET DSRM PASSWORD" "SYNC FROM DOMAIN ACCOUNT DSRMAccount" Q Q
```

По данной теме в TechNet имеется исчерпывающая статья:

```
http://blogs.technet.com/b/askds/archive/2009/03/11/
  ds-restore-mode-password-maintenance.aspx
```

В случае если есть дополнительные установленные роли, вы можете столкнуться с небольшими отличиями.

1. Войдите на сервер Windows Server 2012 с использованием учетной записи, имеющей полномочия администратора.
2. Откройте диспетчер серверов (Server Manager) и выберите в меню пункт Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты).

3. Просмотрите сведения на экране Before you begin (Прежде чем начать) мастера.
4. Выберите переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) и щелкните на кнопке Next (Далее).
5. Выберите целевой сервер из пула серверов (рис. 7.8).

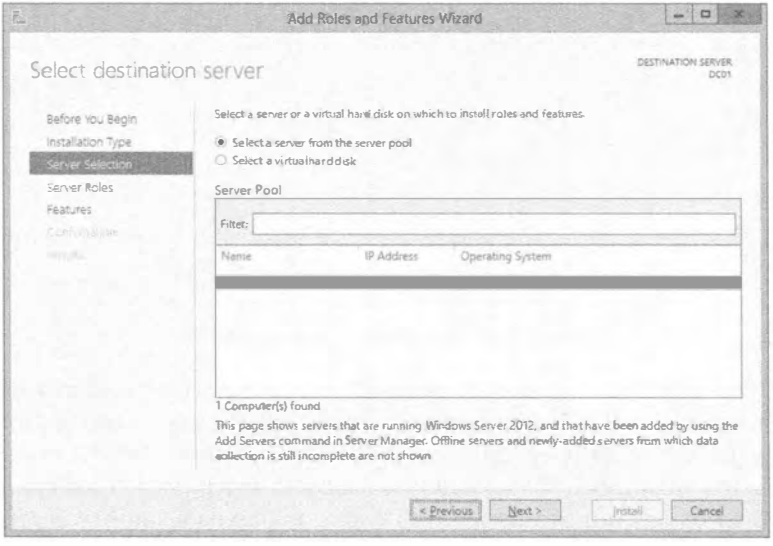


Рис. 7.8. Выбор сервера

6. Выберите роль Active Directory Domain Services (Служба домена Active Directory) и добавьте рекомендуемые компоненты, такие как Remote Server Administration Tools (Инструменты дистанционного администрирования серверов).
7. На экране Features (Компоненты) ничего выбирать не придется.
8. Просмотрите сведения на экране Active Directory Domain Services.
9. Если вы хотите перезапустить сервер автоматически, отметьте флажок Restart the destination server automatically if required (При необходимости автоматически перезапускать целевой сервер).

   После установки двоичных файлов в диспетчере серверов появляется значок с восклицательным знаком желтого цвета.
10. Щелкните на этом значке с восклицательным знаком и затем щелкните на ссылке Promote this server to a domain controller (Повысить этот сервер до контроллера домена).

    Это приведет к запуску мастера Active Directory Domain Services Configuration Wizard.
11. На экране Deployment Configuration (Конфигурация развертывания) мастера выберите переключатель Add a new forest (Добавить новый лес) и введите имя корневого домена (рис. 7.9). Укажите желаемое имя домена, состоящее из двух частей. Щелкните на кнопке Next.

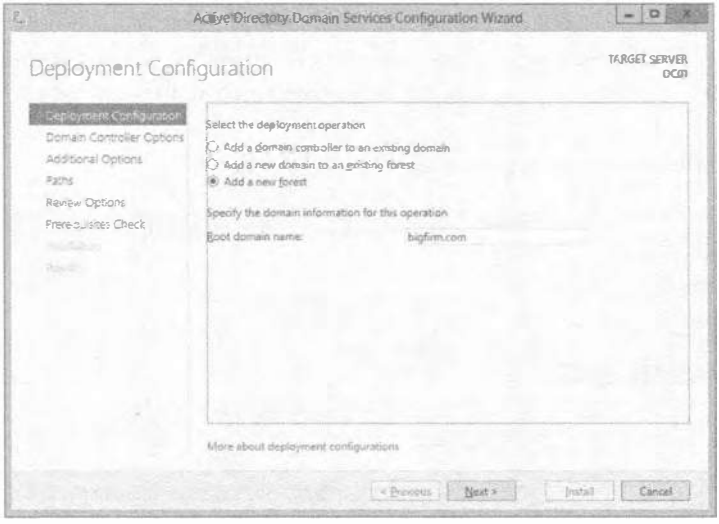


Рис. 7.9. Добавление нового леса

12. Оставьте для функциональных уровней леса и домена стандартные варианты Windows Server 2012. Удостоверьтесь в том, что флажок возле Domain Name System (DNS) Server (Сервер системы доменных имен (DNS)) отмечен, чтобы установить роль DNS. Флажок возле Global Catalog (GC) (Глобальный каталог (GC)) уже отмечен и это изменить нельзя, поскольку данный сервер является первым контроллером домена в домене. Два раза введите пароль администратора Directory Services Restore Mode (DSRM). Щелкните на кнопке Next.

    Active Directory попытается найти DNS-сервер. Если предварительно настроенный DNS-сервер отсутствует, вы получите предупреждение с указанием на то, что зона для вашего домена не может быть создана. Это вполне нормально.

13. Для продолжения щелкните на кнопке Next.

14. Нет никаких причин изменять имя NetBIOS для домена. Оставьте имя, предложенное по умолчанию, и щелкните на кнопке Next.

15. Отобразятся пути к файлу базы данных, файлу журнала и папке SYSVOL. Эти пути можно было бы изменить, но примите стандартные варианты и щелкните на кнопке Next.

16. Просмотрите выбранные опции на экране обзора и щелкните на кнопке Next. Обратите внимание на кнопку View script (Просмотреть сценарий) справа внизу (рис. 7.10). В результате щелчка на этой кнопке откроется окно редактора Notepad с подготовленными командами PowerShell для настройки леса согласно выбранным ранее опциям.

17. Просмотрите команды и их опции (рис. 7.11).

    Командное окно PowerShell можно открыть на любом сервере Windows Server 2012, где установлена роль Active Directory Domain Services, и скопировать в него эти команды. В окне командной строки PowerShell будет запрошен пароль DSRM. По причинам безопасности мастер скрывает пароль, поэтому он не виден в сценарии PowerShell.

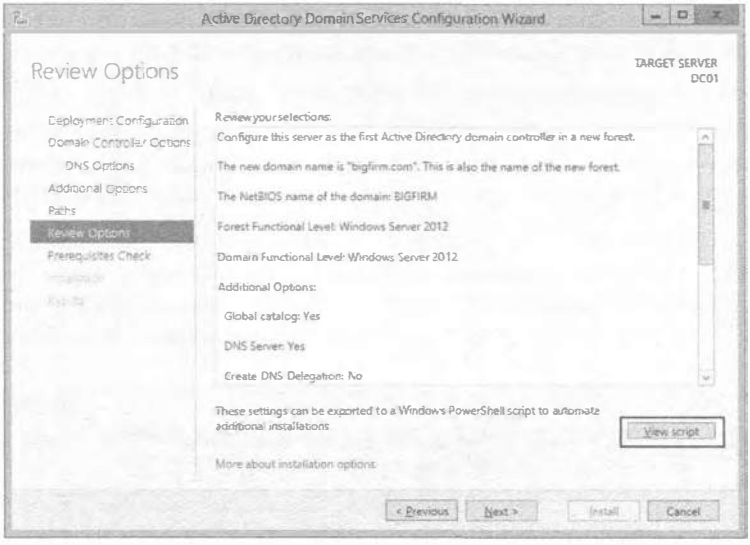


Рис. 7.10. Кнопка View script

Рис. 7.11. Команды PowerShell, сгенерированные мастером

Но если вы хотите, чтобы пароль не запрашивался каждый раз при запуске сценария, можете воспользоваться строкой, добавленной в предыдущем примере, которая поместит пароль в сценарий:

```
-SafeModeAdministratorPassword (ConvertTo-SecureString "P@ssw0rd"
-AsPlainText -Force)`
```

18. По завершении мастера вы окажетесь на экране Prerequisite Check (Проверка предварительных условий), на котором отобразятся два предупреждения, но мастер с помощью галочки зеленого цвета укажет на то, что проверка всех предварительных условий прошла успешно. Как обсуждалось ранее, выдача таких предупреждений вполне нормальна. Щелкните на кнопке Install (Установить).

Установка леса займет некоторое время. По завершении работы мастера и нескольких перезагрузок вам будет предложено войти в систему.

19. Нажмите комбинацию клавиш <Ctr+Alt+Del>, чтобы войти в систему.

    Пароль для учетной записи администратора домена — это тот же самый пароль, который был указан для учетной записи локального администратора до запуска мастера Active Directory Domain Services Configuration Wizard.

На этом все. Вы создали лес с единственным доменом. Следующий логический шаг заключается в создании резервного контроллера домена.

На рис. 7.12 показан экран для шага 17, когда осуществлялось повышение сервера до контроллера домена Windows Server 2012 с применением PowerShell.

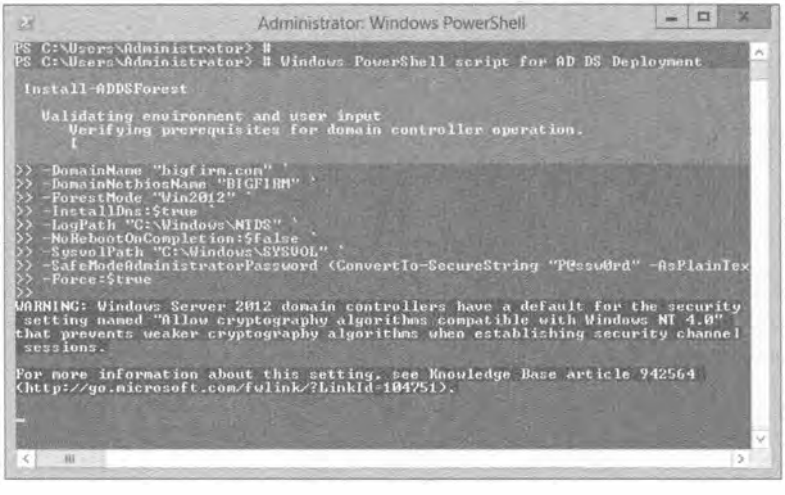


Рис. 7.12. Установка контроллера домена с использованием PowerShell

Дистанционное администрирование Windows Server 2012

Сервер Windows рекомендуется администрировать, не входя в систему самого сервера; взамен на клиенте можно установить инструменты Remote Server Administration Tools (RSAT). Инструменты RSAT предлагаются в виде отдельно загружаемого файла.

Инструменты RSAT для Windows 8 могут управлять Windows Server 2012, а также имеют ограниченную функциональность для Windows Server 2008 и Windows Server 2003. Обзор о том, чем можно управлять в той или иной версии Windows Server доступен по ссылке:

`http://support.microsoft.com/kb/2693643`

Чтобы загрузить RSAT для Windows 8, проследуйте по ссылке:

`http://www.microsoft.com/en-us/download/details.aspx?id=28972`

Инструменты RSAT для Windows 8.1 необходимы для управления Windows Server 2012 R2 и Windows Server 2012. Они также предлагают ограниченную функциональность для управления Windows Server 2008 R2 и Windows Server 2008. Чтобы загрузить RSAT для Windows 8.1, проследуйте по ссылке:

`http://www.microsoft.com/en-us/download/details.aspx?id=39296`

Добавление второго контроллера домена

Всегда когда это возможно, вы должны иметь второй контроллер домена, который намного упростит задачу восстановления после аварии. Единственный контроллер домена создает значительный риск, т.к. становится точкой потенциального отказа. В случае утери его работоспособности перестанет функционировать вся сеть и ситуация станет критической. В этом отношении в Windows Server 2012 ничего не изменилось.

Когда есть второй контроллер домена, то при отказе одного из контроллеров сеть продолжит работать. Пользователи по-прежнему будут иметь возможность входа в домен, их работа не прерывается, групповые политики применяются, и могут выполняться обычные задачи администрирования. Ситуация не будет критической, хотя работы вам прибавится. Кроме того, восстанавливать отказавший DC намного проще, если в домене имеется другой функционирующий DC. Если уж на то пошло, то вы можете даже создать совершенно новый DC, не прибегая к резервной копии. Когда откажет последний DC в домене, вам придется воспользоваться резервной копией Active Directory, и восстановление домена потребует значительного объема работы. Помимо этого, вам придется терпеть нависающих над головой нервных менеджеров, непрерывно вопрошающих "Долго еще?" или "Могу я чем-нибудь помочь?".

Точно так же как вы запускали мастер Active Directory Domain Services Configuration Wizard для создания первого DC, вы запустите его для создания второго DC. Для добавления контроллера домена необходима учетная запись с разрешением Domain Admins. Также понадобится принять во внимание следующие аспекты:

- конфигурация развертывания;
- DNS;
- глобальный каталог.

Прежде чем запускать мастер Active Directory Domain Services Configuration Wizard

Установите роль Active Directory Domain Services на сервере с чистой установкой Windows Server 2012 с помощью мастера Add Roles and Features Wizard. Затем нужно иметь статический IP-адрес, назначенный второму контроллеру домена. IP-адрес DNS-сервера указывает на первый DC, чтобы сервер мог найти домен.

Вам необходим доступ к свойствам TCP/IP сетевого адаптера. Для этого выполните перечисленные ниже шаги.

1. Нажмите комбинацию клавиш <Windows+R> на клавиатуре сервера с Windows Server 2012.
2. Введите `ncpa.cpl` и щелкните на кнопке OK.
3. Щелкните правой кнопкой на элементе Local Area Connection (Подключение по локальной сети) и выберите в контекстном меню пункт Properties (Свойства).
4. Выберите в списке компонент Internet Protocol Version 4 (TCP/IPv4) (Протокол Интернета версии 4 (TCP/IPv4)) и щелкните на кнопке Properties (Свойства).

   Удостоверьтесь в наличии статического IP-адреса, совместимого с вашей сетью.
5. Введите IP-адрес DNS-сервера, как показано на рис. 7.13.

   В рассматриваемом примере DNS-сервер имеет IP-адрес 192.168.0.45.

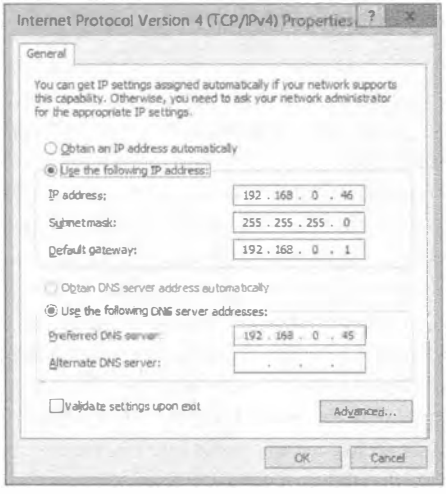


Рис. 7.13. Конфигурирование настроек сети

6. Закройте все отрытые окна.

Вам не придется присоединять сервер к домену до того, как вы повысите его до контроллера домена. Мастер конфигурирования автоматически выполнит необходимые шаги и поместит объект этого компьютера в контейнер Domain Controllers внутри Active Directory.

Конфигурация развертывания для второго контроллера домена

Поскольку домен уже имеется, вам доступны различные варианты конфигурации развертывания. Чтобы добавить второй DC, понадобится выбрать переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен), как показано на рис. 7.14.

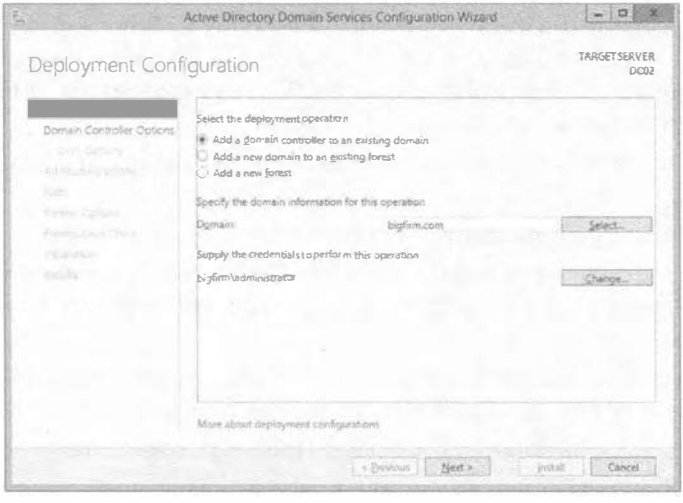


Рис. 7.14. Добавление второго контроллера домена

Упомянутый переключатель необходимо выбирать для каждого нового контроллера домена, добавляемого в домен. Чтобы создать дочерний домен, следует выбрать переключатель Add a new domain to an existing forest (Добавить новый домен в существующий лес).

DNS-сервер для второго контроллера домена

Должны ли вы добавлять DNS-сервер ко второму DC? Конечно!

Если на первом DC функционирует DNS-сервер (что рекомендуется), то на втором DC также должен быть запущен DNS-сервер. Если вы следовали шагам по повышению первого DC, то он функционирует в зоне, интегрированной с Active Directory. Добавляя DNS-сервер ко второму DC, вы обеспечите избыточность с совсем небольшими накладными расходами. Второй DNS-сервер можно также использовать для балансировки нагрузки.

Вспомните, что Active Directory зависит от DNS. Если нет доступных DNS-серверов для DC, чтобы просматривать записи SRV в поисках контроллеров доменов и необходимых служб, Active Directory функционировать не будет. Для Active Directory чрезвычайно важно иметь работающую систему DNS.

При наличии двух DNS-серверов можно сконфигурировать серверы и клиенты на взаимодействие с ними обоими. Для компьютеров в сети рекомендуется указывать один предпочитаемый и один альтернативный DNS-сервер. Если предпочитаемый DNS-сервер не отвечает на запросы, компьютеры будут обращаться к альтернативному DNS-серверу.

Одна половина компьютеров должна использовать в качестве предпочитаемого первый DNS-сервер, а другая половина — второй DNS-сервер.

В случае динамически назначаемых IP-адресов можно сконфигурировать одну половину областей видимости клиентов DHCP для развертывания первого DNS-сервера как предпочитаемого, а вторую половину — для развертывания второго DNS-сервера как предпочитаемого.

Очень важно запомнить, что после повышения сервера до контроллера домена необходимо изменить настройки DNS сети. Удостоверьтесь, что у контроллера домена в качестве предпочитаемого DNS-сервера указан его собственный IP-адрес. По установившейся практике контроллеры домена всегда указывают на самих себя, если на них установлены DNS-серверы.

Глобальный каталог для второго контроллера домена

Должен ли второй DC быть сервером глобального каталога? Да!

В этой главе создается только лес с единственным доменом. В таком лесе всегда следует делать все контроллеры домена серверами глобального каталога. Никаких дополнительных расходов это не требует, но зато появляется гарантия того, что один DC будет предоставлять полную функциональность в случае отказа другого DC.

Запуск мастера ADDSCW для второго контроллера домена

Чтобы повысить второй сервер до контроллера домена, выполните описанные ниже шаги. В этих шагах предполагается, что сервер не является членом домена.

Отличия по размещению глобального каталога

Вопросы относительно размещения GC возникают постоянно. Это хорошо прояснено в статье KB223346, которая доступна по ссылке `http://support.microsoft.com/kb/223346/ru`.

Лес с единственным доменом

В лесе, который содержит единственный домен Active Directory, фантомы отсутствуют. Фантом — это ссылка на объект в другом контексте именования. Например, если вы добавите пользователя B из домена B к группе A в домене A, то можете заметить, что на вкладке Members (Члены) окна свойств этой группы отображается значок другого вида. Он является фантомом. Поскольку такие фантомы не создаются, работа для хозяина инфраструктуры отсутствует. Хозяин инфраструктуры может быть размещен на любом контроллере домена вне зависимости от того, содержит этот контроллер домена глобальный каталог или нет. Если вы пока не знаете, что собой представляет роль хозяина инфраструктуры и другие роли FSMO, прочитайте раздел "Роли FSMO и их передача" далее в этой главе.

Лес с несколькими доменами

Если на каждом контроллере домена, входящего в лес с несколькими доменами, хранится также и глобальный каталог, то фантомы отсутствуют, а хозяин инфраструктуры бездействует. В таком домене хозяин инфраструктуры может быть помещен на любой контроллер домена. На практике большинство администраторов размещают глобальный каталог на каждом контроллере домена в лесе.

Если в данном домене, входящем в лес с несколькими доменами, нет ни одного контроллера домена с глобальным каталогом, то хозяин инфраструктуры должен быть помещен на контроллер домена, на который не планируется добавлять глобальный каталог.

Если вы уже присоединили его к домену, то столкнетесь с небольшими отличиями.

1. Войдите на сервер с использованием учетной записи, имеющей полномочия локального администратора.
2. Если это еще не сделано, установите роль Active Directory Domain Services, для чего откройте диспетчер серверов и выберите в меню пункт Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты). После этого следуйте шагам мастера, как поступали при добавлении первого контроллера домена.

   В качестве альтернативы можно было бы открыть окно командной строки PowerShell и запустить следующий командлет; он установит те же самые компоненты, как и в случае запуска мастера:

   ```
   Add-WindowsFeature AD-Domain-Services,RSAT-AD-AdminCenter,
   RSAT-ADDS-Tools,GPMC
   ```

3. В диспетчере серверов щелкните на значке с восклицательным знаком желтого цвета и затем щелкните на ссылке Promote this server to a domain controller (Повысить этот сервер до контроллера домена).

   Если после выполнения командлета PowerShell значок с восклицательным знаком желтого цвета не появился, щелкните на значке обновления в окне диспетчера серверов.

4. На экране Deployment Configuration (Конфигурация развертывания) мастера выберите переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен). Укажите имя домена и предоставьте учетные данные администратора домена `bigfirm.com`. Если учетная запись, которую вы применяли для входа на сервер, не является членом группы Domain Administrators (Администраторы домена), вам также понадобится ввести другие учетные данные. Щелкните на кнопке Next (Далее).

Проблемы с AD? Проверьте DNS!

Если вы получаете ошибку, указывающую на то, что с каким-то контроллером домена не удается установить связь, проверьте корректность написания имени домена и удостоверьтесь в наличии функционирующей службы DNS на DNS-сервере. Проверьте, сконфигурирована ли система на использование этого DNS-сервера. Проще всего пропинговать имя домена. Например, если домен имеет имя `bigfirm.com`, то выполнение команды `ping bigfirm.com` должно дать четыре ответа. Если не получено ни одного ответа, это четко указывает на то, что либо DNS-сервер недостижим (проверьте настройки TCP/IP и брандмауэра), либо служба DNS функционирует некорректно.

5. На экране Domain Controller Options (Параметры контроллер домена) отметьте флажки Domain Name System (DNS) server (Сервер системы доменных имен (DNS)) и Global Catalog (GC) (Глобальный каталог (GC)), как показано на рис. 7.15. Удостоверьтесь, что для имени сайте выбрано Default-First-Site-Name. Вам также необходимо ввести пароль DSRM. Распространенная практика предусматривает выбор в качестве пароля DSRM на втором DC такого же пароля, как и на первом DC. Щелкните на кнопке Next.
6. Если появится предупреждение о делегировании DNS, щелкните на кнопке Next.

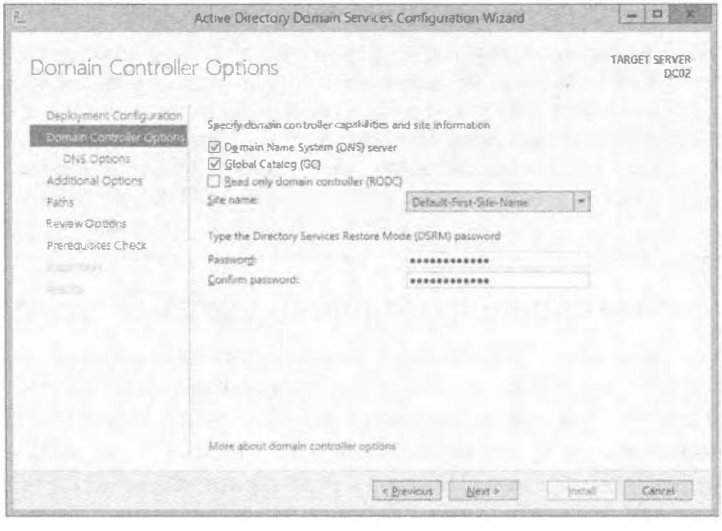


Рис. 7.15. Добавление ролей DNS-сервера и GC ко второму DC

7. На экране Additional Options (Дополнительные параметры) можно указать, что установка Active Directory должна проводиться из носителя.

   Для создания установочного носителя из текущей базы данных Active Directory можно воспользоваться утилитой `NTDSUtil`. Эта утилита создаст снимок состояния базы данных на определенный момент времени, который впоследствии можно предоставить мастеру ADDSCW в качестве источника. Преимущество заключается в том, что в таком случае придется реплицировать только изменения, внесенные после момента создания снимка. Эта возможность очень удобна, когда есть медленный канал WAN и нежелательно реплицировать базу данных Active Directory целиком по медленному каналу.

8. В данном случае выберите для репликации переключатель Any domain controller (Любой контроллер домена). Щелкните на кнопке Next.
9. На экране Paths (Пути) оставьте без изменений пути для базы данных, файла журнала и папки SYSVOL, а затем щелкните на кнопке Next.
10. На экране Review Options (Обзор параметров) просмотрите параметры и при желании щелкните на кнопке View Script (Просмотреть сценарий), чтобы сохранить выбранные параметры для выполнения той же самой настройки в будущем. Щелкните на кнопке Next.
11. На экране Prerequisites Check (Проверка предварительных условий) удостоверьтесь в том, что проверка прошла успешно. Вы заметите те же самые предупреждения, которые обсуждались во время установки первого контроллера домена. Щелкните на кнопке Install (Установить).
12. После завершения установки щелкните на кнопке Close (Закрыть) и контроллер домена будет автоматически перезагружен.
13. Войдите в систему на контроллере домена, и мастер Active Directory Domain Services Configuration Wizard завершит задачу.

Установка Active Directory из носителя

Ранее мы упоминали, что с помощью утилиты `NTDSUtil` можно создать снимок текущего состояния базы данных Active Directory и затем применять его для повышения до нового контроллера домена. Следующий шаг заключается в копировании этого снимка на переносной диск или устройство и последующая установка контроллера домена с использованием данного носителя. Создание носителя подобного рода описано в детальном руководстве по установке AD DS, доступном в TechNet:

`http://technet.microsoft.com/en-us/library/cc770654.aspx`

Создание организационных единиц, учетных записей и групп

После создания домена понадобится создать организационные единицы (OU), учетные записи пользователей, учетные записи компьютеров, группы и т.д. На выбор доступны два средства: унаследованный инструмент Active Directory Users and Computers (Пользователи и компьютеры Active Directory), или ADUC, либо Active Directory Administrative Center (Центр администрирования Active Directory), или ADAC. Будущие новые возможности и задачи по управлению Microsoft будет помещать в ADAC, поэтому имеет смысл приступить к работе с этой новой консолью.

Оба инструмента позволяют создавать что угодно с помощью простого приема "указал и щелкнул". Тем не менее, все задачи можно также выполнить из командной строки, предпочтительно PowerShell. Это очень удобно в паре ситуаций:

- требуется создать или модифицировать множество объектов, и вы желаете написать сценарий для процесса;
- на сервере установлена версия Server Core, и вы не хотите пользоваться инструментом ADUC или графическим интерфейсом ADAC.

Создание организационных единиц

Организационные единицы применяются для организации объектов в рамках Active Directory. Любой объект (такой как пользователи, компьютеры, группы и т.д.) может быть помещен внутрь OU, чтобы упростить администрирование ним. Вот две главные технические причины, по которым будет создаваться OU:

- управление посредством групповой политики (Group Policy);
- делегирование администрирования.

Управление посредством групповой политики

Объекты групповой политики (Group Policy object — GPO) могут быть созданы и привязаны к сайтам, доменам и организационным единицам. Если вы хотите, чтобы некоторым пользователям была назначена определенная групповая политика, можете создать организационную единицу, поместить в нее учетные записи и связать с ней объект GPO.

Однако если вы не создали ни одной организационной единицы, то единственный способ назначения объектов GPO обычным учетным записям — делать это через стандартную политику домена (Default Domain Policy), которая в равной степени применяется к пользователям и компьютерам. Представьте себе, что вы хотите развернуть приложение для всех пользователей в отделе продаж, используя групповую политику. Но если вы привяжете объект GPO к домену, то данное приложение получат все пользователи компании, а не только пользователи отдела продаж.

Вместо этого имеет смысл создать OU (скажем, по имени `Sales`), переместить в нее учетные записи пользователей и компьютеров отдела продаж и затем привязать объект GPO к организационной единице `Sales`. При наличии других групп или пользователей, к которым желательно применить специфичные объекты GPO, для них также можно создать OU и поместить туда соответствующие объекты пользователей и компьютеров.

Еще один способ применения объектов GPO к определенным объектам пользователей и компьютеров предусматривает создание группы доступа Active Directory и добавления в эту группу всех пользователей, к которым требуется применить настройки политики. После создания и наполнения группы ее можно добавить в раздел Security Filtering (Фильтрация безопасности) объекта GPO и удалить стандартную группу `Authenticated Users` (Аутентифицированные пользователи) из настроек Security Filtering. За более подробными шагами обращайтесь в главу 9, где показано, как выполнять эту и другие задачи.

Центр администрирования Active Directory

В версии Windows Server 2008 R2 центр администрирования Active Directory (Active Directory Administrative Center) уже был встроенным, но создавать объекты с его помощью было проблематично, так что использовалась консоль Active Directory Users and Computers. В Windows Server 2012 появился более развитый центр администрирования Active Directory. Он был перепроектирован и полностью основывается на PowerShell. Теперь можно копировать последние команды из окон хронологии Windows PowerShell, изменять их и создавать собственный сценарий, позволяющий ускорить выполнение задачи.

Тем не менее, консоль Active Directory Users and Computers по-прежнему доступна и работает в Windows Server 2012, предлагая ту же самую функциональность, что и в версии Windows Server 2008 R2.

Создание организационных единиц с помощью ADAC

Чтобы создать организационную единицу с применением Active Directory Administrative Center, выполните следующие шаги.

1. Войдите в систему Windows Server 2012. Щелкните на значке Active Directory Administrative Center (Центр администрирования Active Directory). В качестве альтернативы можно нажать комбинацию клавиш <Windows+R>, чтобы открыть окно Run (Выполнить), ввести **dsac.exe** и щелкнуть на кнопке OK.
2. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт New⇨Organizational Unit (Создать⇨Организационная единица).
3. Введите **Sales** в текстовом поле Name (Имя) и удостоверьтесь, что флажок Protect from accidental deletion (Защитить от случайного удаления) отмечен (рис. 7.16).

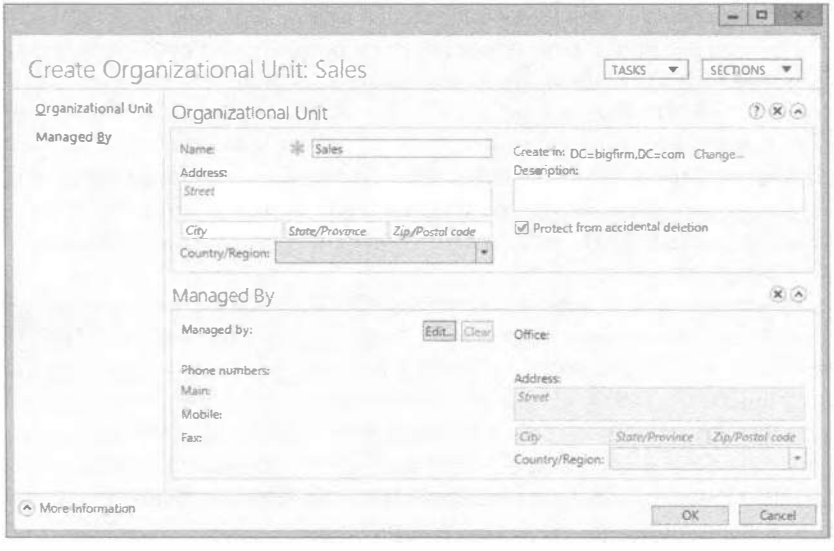


Рис. 7.16. Создание организационной единицы по имени `Sales`

4. Щелкните на кнопке OK, и организационная единица будет создана.
5. Допускается также создавать дочерние OU. Щелкните правой кнопкой мыши на только что созданной организационной единице `Sales` и выберите в контекстном меню пункт New⇨Organizational Unit.
6. Введите **`Users`** в текстовом поле Name и щелкните на кнопке OK. На рис. 7.17 можно видеть окно Active Directory Administrative Center с организационной единицей `Users`, которая является дочерней по отношению к организационной единице `Sales`.

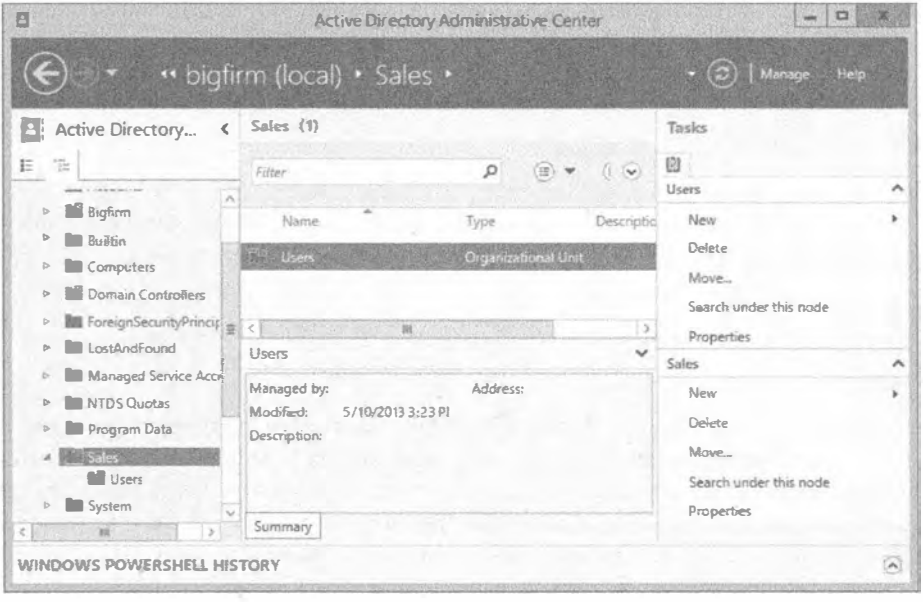


Рис. 7.17. Организационные единицы в Active Directory Administrative Center

Защита от удаления

Средство защиты от случайного удаления, включаемое путем отметки флажка Protect from accidental deletion, позволяет предотвратить неумышленное удаление объекта кем-нибудь (даже администратором). Несмотря на то что ADAC предлагает подтвердить удаление, многие из нас щелкают в таких диалоговых окнах, не замечая вопроса. Тем не менее, если удалить объект действительно нужно, это можно сделать. Для этого в ADAC щелкните на объекте правой кнопкой мыши, выберите в контекстном меню пункт Properties (Свойства) и снимите отметку с флажка Protect from accidental deletion.

Вы можете обнаружить два объекта `Users` внутри Active Directory, но они совершенно разные. Организационная единица `Users` внутри OU под названием `Sales` — это организационная единица, с которой связаны объекты GPO. Контейнер `Users` внутри домена является только контейнером (не организационной единицей) и не может иметь связанные объекты GPO. Организационные единицы идентифициру-

ются немного отличающимися значками — не просто папкой, а папкой с изображением поверх; это напоминает о том, что они представляют собой нечто большее, чем всего лишь контейнер.

Отличительные имена LDAP

Для коммуникаций в Active Directory используется облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol — LDAP). В протоколе LDAP для уникальной идентификации каждого объекта в каталоге применяется отличительное имя (distinguished name — DN). Прежде чем взглянуть, как объекты создаются в командной строке или сценарии, необходимо разобраться с компонентами DN.

Формат DN выглядит как список конструкций *типОбъекта=имяОбъекта*, разделенных запятыми. Например, домен по имени `bigfirm.com` содержит два компонента (`bigfirm` и `com`), которые идентифицируются следующим образом:

```
dc=bigfirm, dc=com
```

Организационные единицы имеют тип объекта `ou`, а контейнеры `Users` и `Computers` идентифицируются посредством `cn` (common name — общее имя). Ниже приведено отличительное имя для организационной единицы `Sales`:

```
ou=Sales,dc=bigfirm,dc=com
```

Контейнер `Users` имеет такое отличительное имя:

```
cn=Users,dc=bigfirm,dc=com
```

Контейнер — это объект Active Directory, который создается внутри Active Directory, когда вы повышаете сервер до контроллера домена. Такой объект содержит стандартные пользователи и группы для Active Directory и также имеет полностью отличающиеся от организационной единицы атрибуты. Другое крупное отличие заключается в том, что к этому контейнеру не могут применяться групповые политики.

Учетная запись с именем `Sally.Smith`, находящаяся в организационной единице `Sales`, имеет следующее имя DN:

```
cn=Sally.Smith,ou=Sales,dc=bigfirm,dc=com
```

Учетная запись с именем `Joe.Johnson`, находящаяся в контейнере `Users`, имеет такое имя DN:

```
cn=Joe.Johnson,cn=Users,dc=bigfirm,dc=com
```

Если организационная единица является вложенной или содержит внутри себя другие OU, то в имени DN первой будет указана самая глубоко вложенная OU. Например, если организационная единица `Sales` имеет дочернюю OU по имени `Users`, внутри которой содержится пользователь по имени `Maria`, то DN будет выглядеть следуюшим образом:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
```

Если имя DN включает пробелы, оно должно быть помещено в кавычки, чтобы гарантировать его корректную интерпретацию. Например, приведенное ниже имя не содержит пробелов, поэтому кавычки не требуются:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
```

Однако то же самое имя DN с пробелом должно включать кавычки:

```
"cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com"
```

Имена DN в LDAP не чувствительны к регистру символов. Следующие два имени DN будут интерпретироваться как один и тот же объект:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
CN=Maria,OU=Users,OU=Sales,DC=bigfirm,DC=com
```

Создание организационных единиц с помощью PowerShell

Средство PowerShell существует на протяжении нескольких лет, и со временем важность его знания растет. В Windows Server 2008 R2 версия PowerShell 2.0 была встроенной и уже обладала развитой поддержкой для множества компонентов и ролей. Благодаря объектной ориентации, PowerShell имеет цельную и хорошо спроектированную архитектуру. В Microsoft интенсивно продвигают PowerShell, поэтому его можно использовать для управления практически всеми аспектами в Windows Server 2012.

В Windows Server 2012 встроена версия PowerShell 3.0, а в Windows Server 2012 R2 — версия PowerShell 4.0, которые имеют огромное количество новых команд, предназначенных для более легкого управления сервером. Исследование всех новых возможностей могло бы потребовать написания нескольких книги по этой теме. Здесь мы лишь продолжим наш пример, чтобы дать вам о них общее представление. Если вы не знаете, каким инструментом командной строки воспользоваться, скажем, DSAdd, Windows Script Host (WSH) или PowerShell, то изучайте PowerShell — он представляет собой технологию настоящего и будущего.

Если вы устанавливали второй контроллер домена в соответствии с приведенным выше пошаговым руководством, то уже должны иметь доступ к командам Active Directory PowerShell. Проверьте, установлен ли компонент AD DS Snap-Ins and Command-Line Tools (Инструменты оснасток AD DS и командной строки). Чтобы найти его, запустите мастер Add Roles and Features Wizard и щелкайте на кнопке Next (Далее) до тех пор, пока не попадете на экран, где выбираются компоненты. Он должен выглядеть так, как показано на рис. 7.18.

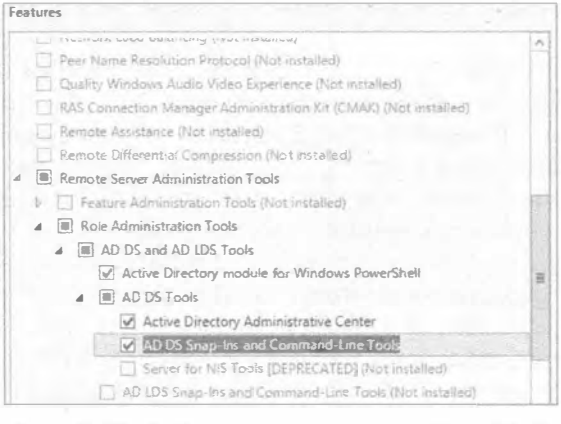


Рис. 7.18. Добавление командлетов PowerShell

В среде Windows Server 2012 щелкните на значке PowerShell в панели задач; это приведет к открытию командного окна PowerShell, отображающего командную подсказку `PS C:\Users\administrator>`. В следующем разделе вы узнаете, как с помощью PowerShell создать организационную единицу по имени `PS_OU`.

PowerShell и Active Directory

В PowerShell доступен крупный набор команд, для работы которых необходимо предоставить только несколько дополнительных параметров. Такие команды называются командлетами и они являются главными рабочими лошадками в PowerShell. При наличии определенных ролей, установленных в Active Directory, доступны новые командлеты, но для работы с ними сначала понадобится их импортировать в сеанс PowerShell. В большинстве случаев новые командлеты поступают в виде модулей, и для того, чтобы сделать доступной их функциональность, эти модули необходимо загрузить.

Модуль импортируется следующим образом:

```
Import-Module ActiveDirectory
```

Процесс импорта требует некоторого времени, после чего снова появится командная подсказка. Затем введите команду для создания организационной единицы по имени `PS_OU`:

```
New-ADOrganizationalUnit -Name PS_OU -Server DC02.bigfirm.com
   -Path "DC=bigfirm,DC=com"
```

Возможно, придется изменить имя сервера `DC02.bigfirm.com` и компонент домена `"DC=bigfirm,DC=com"`, чтобы они соответствовали вашим действительным именам. Если команда не работает, и вы получаете ошибку, первым делом удостоверьтесь в отсутствии опечаток. Вообще PowerShell нечувствителен к регистру символов, т.е. совершенно неважно, какими символами записана команда — прописными или строчными.

В PowerShell 3.0 исчезла необходимость в предварительном импорте модуля с помощью команды `Import-Module ActiveDirectory`, как делалось в примере. PowerShell 3.0 распознает командлет `New-ADOrganizationalUnit` и импортирует соответствующий модуль. Если модуль был импортирован ранее, этот шаг пропускается.

Первый командлет `New-ADOrganizationalUnit` состоит из глагола и существительного английского языка, которые разделены дефисом (-). Это базовый проектный принцип в PowerShell, направленный на упрощение запоминания командлетов. Например, если вы хотите извлечь (get) организационную единицу AD (AD organizational unit), то можете ввести `Get-ADOrganizationalUnit`, а для удаления (remove) организационной единицы ввести `Remove-ADOrganizationalUnit`.

Командлету `New-ADOrganizationalUnit` предоставлялось несколько параметров, так что давайте кратко рассмотрим их. Параметр `-Name` указывает имя OU; обратите внимание на наличие пробела между `-Name` и именем `PS_OU`. Параметр `-Server` задает контроллер домена, где необходимо создать OU, а в параметре `-Path` указано местоположение новой OU. Предоставить можно намного больше параметров. Чтобы увидеть все опции, введите `Get-Help New-ADOrganzationalUnit` или просто `help New-ADOrganzationalUnit`.

Вас может интересовать, существует ли способ создания сценария, который бы ускорил выполнение задач. В рассматриваемом примере в этом мало смысла, потому что мы имеем дело всего лишь с одной строкой кода. Мы даже не затронули верхушку айсберга, но что, если вы хотите одновременно создать 10 организационных единиц, например, `PS_OU1`, `PS_OU2` и т.д., удалить такие OU и воссоздать их? Для таких действий стоит создавать сценарий.

В Windows Server 2012 вы получаете интегрированную среду для разработки и запуска сценариев PowerShell в готовом виде. Этот инструмент называется Windows PowerShell ISE (Integrated Scripting Environment — интегрированная среда написания сценариев). Она представляет собой редактор сценариев, который помогает быстрее строить сценарии и также позволяет запускать сценарии прямо из консоли. Среда Windows PowerShell ISE имеет ряд великолепных средств наподобие Intellisense, которое содействует в поиске подходящего командлета и предоставляет в разделе команд детальные сведения о командлетах. Есть еще много чего для исследований; здесь мы лишь кратко коснемся особенностей написания сценария в Windows PowerShell ISE. Выполните перечисленные ниже шаги.

1. Запустите Windows PowerShell ISE, щелкнув правой кнопкой мыши на значке PowerShell в панели задач. В открывшемся контекстном меню вы увидите задачу под названием Windows PowerShell ISE.

   Значок PowerShell должен быть закреплен в панели задач; если это не так, запустите Windows PowerShell ISE через меню Start (Пуск).

2. В меню View (Вид) удостоверьтесь, что возле Show Script Pane (Показать панель сценария) имеется отметка.

3. В панели сценария (верхняя область белого цвета) среды Windows PowerShell ISE введите следующие строки (рис. 7.19):

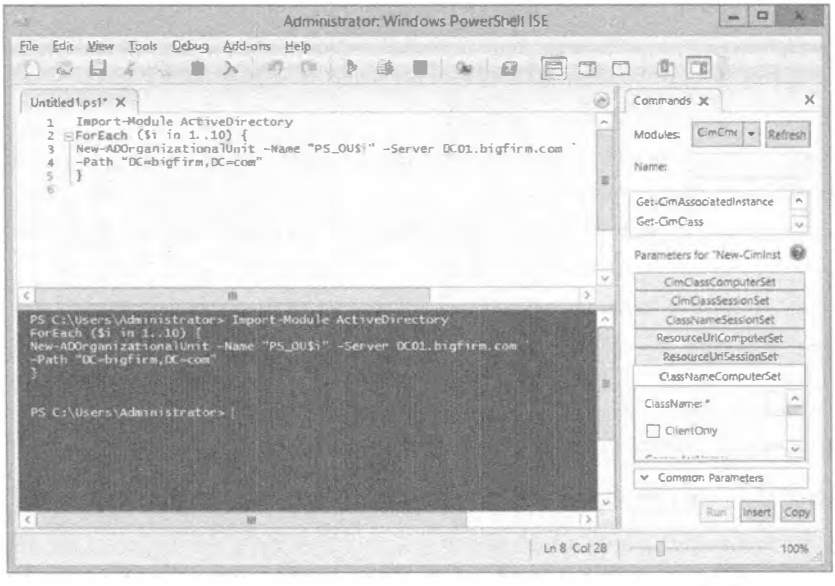


Рис. 7.19. Запуск командлетов PowerShell в среде PowerShell ISE

```
Import-Module ActiveDirectory
ForEach ($i in 1..10) {
New-ADOrganizationalUnit -Name "PS_OU$i" -Server DC01.bigfirm.com `
-Path "DC=bigfirm,DC=com"
}
```

Обратите внимание, что во второй строке применяется цикл `ForEach` для выполнения 10 итераций. `$i` содержит текущий номер итерации. Например, при первой итерации цикла `$i` хранит число `1`, при второй итерации `$i` содержит число `2` и т.д. На каждой итерации цикла выполняется командлет `New-ADOrganizationalUnit`. Поскольку вызов этого командлета необходимо разнести на две строки, в конце третьей строки имеется символ обратной галочки (`), который позволяет перенести команду на следующую строку.

4. Выберите пункт меню File⇨Save As (Файл⇨Сохранить как) и сохраните сценарий в библиотеке `Documents` (Документы) под именем `Create10OUs.ps1`.

   В этот момент вы имеете сценарий PowerShell, который можно запускать, но, скорее всего, он не может быть выполнен без изменения среды.

5. Возвратитесь в среду Windows PowerShell ISE. Введите `Get-Ex` и нажмите клавишу <Tab>. Обратите внимание на открывшееся меню, отображающее все команды, которые начинаются с `Get-Ex*`. Такая функция называется Intellisense. В данном случае в списке присутствует только один командлет, `Get-ExecutionPolicy`.

6. Итак, командой будет `Get-ExecutionPolicy`. Нажмите <Enter>. В панели меню щелкните на значке воспроизведения в виде треугольника зеленого цвета или нажмите клавишу <F5>.

   В случае стандартной установки результатом будет вывод слова `Restricted` (Ограничено) в окне синего цвета ниже панели сценария, а это значит, что запустить сценарий не удастся.

7. Очистите панель сценария, введите следующую команду для изменения политики выполнения (Execution Policy) и нажмите клавишу <F5>:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

8. В ответ на запрос изменения щелкните на кнопке Yes (Да). Это разрешит выполнять локальные сценарии.

9. Выберите пункт меню File⇨Open (Файл⇨Открыть) и укажите ранее сохраненный сценарий, `Create10OUs.ps1`.

10. Теперь сценарий можно выполнить нажатием клавиши <F5>.

Если все прошло успешно, вы можете запустить Active Directory Administrative Center и увидеть новые организационные единицы. В случае возникновения ошибок пересмотрите сценарий. Когда сценарий вводится впервые, ошибки будут нередким явлением, особенно при вводе длинных строк.

Создание учетных записей

После создания ряда организационных единиц понадобится создать определенные учетные записи. Для доступа в домен пользователям и компьютерам необходимы учетные записи.

PowerShell 4.0 в Windows Server 2012 R2

ОС Windows Server 2012 R2 поставляется с последней и самой лучшей версией PowerShell 4.0. Важно понимать, что версия PowerShell 4.0 обратно совместима с более ранними версиями. Это означает, что наши примеры будут работать в Windows Server 2012 PowerShell 3.0 и Windows Server 2012 R2 PowerShell 4.0.

Как и в случае организационных единиц, для создания учетных записей можно использовать либо Active Directory Users and Computers, Active Directory Administrative Center и `DSAdd`, либо PowerShell.

Создание учетных записей компьютеров часто автоматизируется. Когда компьютер присоединяется к домену, для него автоматически создается учетная запись компьютера. По умолчанию такая учетная запись создается в контейнере `Computers` (Компьютеры), но это можно изменить с применением инструмента командной строки `Redircmp`, синтаксис использования которого выглядит следующим образом:

```
Redircmp DN
```

Например, если пользователь присоединил компьютер к домену, и вы хотите создать учетную запись компьютера в организационной единице `Sales`, то должны ввести такую команду:

```
Redircmp "OU=Sales,DC=bigfirm,DC=com"
```

Если необходимо вернуть стандартную настройку, введите команду:

```
Redircmp "CN=Computers,DC=bigfirm,DC=com"
```

Не забудьте привести настройки контроллера домена (`DC=`**`xxx`**) в соответствие с вашей средой.

Создание учетных записей с помощью Active Directory Administrative Center

Чтобы создать учетную запись пользователя с применением Directory Administrative Center, выполните следующие шаги.

1. Запустите Active Directory Administrative Center, нажав комбинацию клавиш <Windows+R> для открытия диалогового окна Run (Выполнить), введите **`dsac.exe`** в текстовом поле и щелкните на кнопке OK.
2. Щелкните правой кнопкой мыши на созданной ранее организационной единице `Sales` и выберите в контекстном меню пункт New⇨User (Создать⇨Пользователь).
3. Введите для пользователя имя, фамилию и имя для входа в систему.
4. Здесь же введите пароль, подтвердите его и удостоверьтесь, что выбран переключатель User must change password at next log on (Пользователь должен изменить пароль при следующем входе в систему).

   Это гарантирует, что пользователь изменит свой пароль, и никто другой не будет знать его, даже вы. Диалоговое окно выглядит подобно показанному на рис. 7.20.

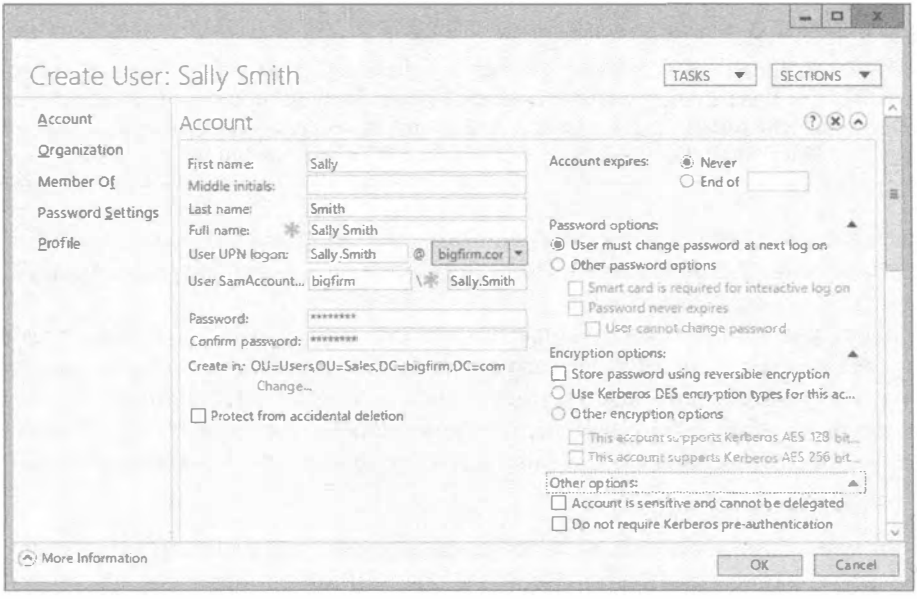


Рис. 7.20. Создание учетной записи пользователя в ADAC

Пользовательское имя для входа в систему

Компании обычно имеют установившийся стандарт, касающийся создания имя для входа в систему. Распространены методы взятия инициала имени и полной фамилии, полных имени и фамилии, имени, точки и фамилии и т.п. Если вы начинаете работу в новой компании, то должны ознакомиться с таким стандартом и следовать ему при создании учетных записей.

Если учетная запись совместно используется несколькими пользователями (соответствует, к примеру, временной должности, занимаемой разными работниками), может понадобиться отметить флажок User cannot change password (Пользователь не может изменять пароль). При создании учетных записей служб (учетных записей пользователей, применяемых для запуска служб) вы можете отметить флажок Password never expires (Срок действия пароля никогда не истекает), чтобы устаревание паролей не блокировало такие учетные записи. Наконец, если учетную запись не планируется использовать в течение какого-то времени, подумайте о том, чтобы ее отключить.

5. Просмотрите выбранные установки и щелкните на кнопке OK.

Создание пользователей с помощью PowerShell

До появления PowerShell для создания пользователей и других объектов Active Directory применялся инструмент под названием `DSAdd`. На то время это был хороший инструмент, а сейчас он считается унаследованным, но по-прежнему великолепно работает. Он может быть шагом в направлении пакетных сценариев и позволяет заглянуть в автоматизированный мир командной строки. Но единственный

путь для получения полноценных возможностей автоматизации предусматривает использование PowerShell.

Подобно тому, как вы применяли PowerShell для создания организационных единиц, можно также создавать учетные записи пользователей. Вы будете удивлены, узнав, что базовый командлет не особенно отличается от команды DSAdd. Вот этот командлет:

```
New-ADUser -Path "OU=Sales,DC=bigfirm,DC=com" -AccountPassword
(ConvertTo-SecureString P@ssword -AsPlainText -force)
-Name "Maria Smith" -Givenname Maria -Surname Smith `
-DisplayName "Maria Smith" -SamAccountName "Maria.Smith" `
-UserPrincipalName "Maria.Smith@bigfirm.com" -ChangePasswordAtLogon 1
-Enabled 1
```

Приведенный пример команды PowerShell создает пользователя с именем Maria Smith. Преимущество инструмента PowerShell заключается в том, что он объектно-ориентирован.

Обратите внимание в этом примере, что мы можем не просто указать пароль в форме строки; мы сначала преобразовываем строку в SecureString и затем передаем результат преобразования параметру -AccountPassword. Параметрам -ChangePasswordAtLogon и -Enabled необходимо значение булевского типа — 0 (для "ложь") или 1 (для "истина"). Остальная часть команды не требует особых пояснений.

Создание групп

Также может понадобиться создать несколько групп. Самой распространенной причиной создания групп является необходимость в объединении пользователей. Более конкретно, глобальные группы доступа создаются для организации пользователей и последующего назначения этим группам нужных разрешений. Когда только возможно, вы должны назначать разрешения группам, а не пользователям. Вы могли слышать старое высказывание: "Пользователи приходят и уходят, но группы остаются навсегда". Даже если вы слышали его раньше, оно по-прежнему имеет смысл и позволяет запомнить, что разрешения следует назначать не пользователям, а группам.

Для примера предположим, что у вас есть несколько пользователей в отделе продаж. Вместо назначения разрешений каждому индивидуальному пользователю из отдела продаж вы можете создать одну глобальную группу доступа по имени G_Sales, поместить в нее всех пользователей указанного отдела и назначить разрешения группе G_Sales.

Если пользователь покидает отдел продаж, вы удаляете его из группы G_Sales, после чего он больше не будет иметь разрешений данной группы. Когда в отделе продаж появляется новый пользователь, вы помещаете его в группу G_Sales, и он получит те же разрешения, что и остальные пользователи группы.

Это звучит довольно просто, однако существуют и другие типы групп, каждая из которых имеет свое предназначение. Группы бывают двух типов — рассылки и доступа. Группы рассылки используются для электронной почты, а группы доступа — для назначения разрешений. Группы доступа также могут применяться для электронной почты.

Различают три области действия группы.

- **Глобальная (global).** Глобальные группы предназначены для объединения пользователей. Это наиболее часто используемые группы, и одна такая группа будет создаваться далее в главе. Пользователи помещаются в глобальные группы, которым назначены нужные разрешения.
- **Локальная домена (domain local).** В некоторых реализациях доменов локальные группы домена применяются согласно принципу AGDLP, где *A* означает "accounts" (учетные записи), *G* указывает на "global groups" (глобальные группы), *DL* означает "domain local groups" (локальные группы домена), а *P* указывает на "permissions" (разрешения). Учетные записи пользователей помещаются в глобальные группы. Глобальные группы помещаются в локальные группы домена, а локальным группам домена назначаются разрешения. При таком использовании локальные группы домена являются дополнительным уровнем для идентификации ресурсов. Рекомендуемый подход к разработке своей стратегии группирования предполагает применение принципа AGDLP.
- **Универсальная (universal).** Универсальные группы используются только в средах с несколькими доменами. Например, в сети имеются два домена, `Europe` и `UnitedStates`, в каждом из которых есть глобальная группа `G_Sales`. Можно создать универсальную группу `UG_Sales`, членами которой будут эти две группы `G_Sales`, т.е. `UnitedStates\G_Sales` и `Europe\G_Sales`. Затем группу `UG_Sales` можно использовать повсюду внутри предприятия. Любые изменения в членстве в отдельных группах `G_Sales` не будут приводить к репликации группы `UG_Sales`. Теперь универсальную группу можно добавить в локальную группу домена и обеспечить распознавание ресурсов для отдела продаж по всему миру. Такая стратегия называется AGUDLP, где дополнительная буква *U* означает "universal group" (универсальная группа).

Самый распространенный способ создания описанных выше групп предусматривает применение инструмента Active Directory Users and Computers или Active Directory Administrative Center. Чтобы создать глобальную группу доступа, выполните следующие шаги.

1. Запустите Active Directory Administrative Center, нажав комбинацию клавиш <Windows+R> для открытия диалогового окна Run (Выполнить), введите **`dsac.exe`** в текстовом поле и щелкните на кнопке OK.
2. Щелкните правой кнопкой мыши на организационной единице `Sales` и выберите в контекстном меню пункт New⇨Group (Создать⇨Группа).
3. Введите **`G_Sales`** в поле Group name (Имя группы). Диалоговое окно должно выглядеть похожим на показанное на рис. 7.21. Щелкните на кнопке OK.
4. Щелкните правой кнопкой мыши на организационной единице `Sales` и выберите в контекстном меню пункт New⇨Group. Введите **`G_SalesAdmins`** в поле Group name. Щелкните на кнопке OK.

Группа `G_SalesAdmins` создана, и ей можно назначить разрешения, например, делегировав управление организационной единице, как будет описано далее в главе.

Рис. 7.21. Создание группы с использованием Active Directory Administrative Center

Создание групп с помощью PowerShell (ADAC Windows PowerShell History)

В предыдущих примерах посредством PowerShell создавались организационные единицы и пользователи. Мы показывали команды, необходимые для создания того или иного объекта. А что если вы не знаете, какую команду применить, или хотите получить определенную помощь? Если при создании групп с использованием Active Directory Administrative Center вы следовали приведенным выше шагам, то все должно быть вам доступно.

1. После создания группы `G_SalesAdmins` щелкните на стрелке вниз внутри круга справа от надписи Windows PowerShell History (Хронология Windows PowerShell) в окне консоли (рис. 7.22). Вы увидите все задачи, которые были ранее выполнены в ADAC. Также вы должны видеть последние две команды `New-ADGroup` (рис. 7.22).

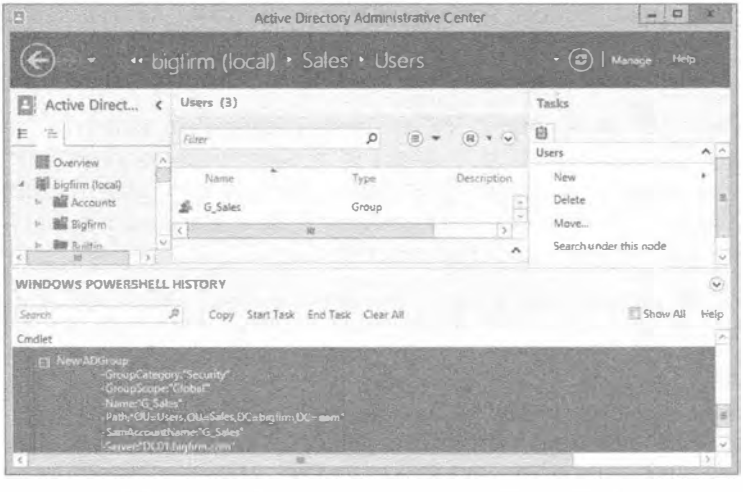


Рис. 7.22. Просмотр хронологии PowerShell

2. Щелкните на значке + слева от командлета, чтобы развернуть его и увидеть все параметры.

3. Щелкните правой кнопкой мыши на первом командлете New-ADGroup, вырежьте и скопируйте его в окно PowerShell. Затем измените значения параметров -Name и -SamAccountName группы на что-нибудь другое, например:

```
New-ADGroup -GroupCategory:"Security"
   -GroupScope:"Global"
   -Name:"G_SalesPowerUsers" `
   -Path:"OU=Sales,DC=bigfirm,DC=com"
   -SamAccountName:"G_SalesPowerUsers" `
   -Server:"DC02.bigfirm.com"
```

4. Запустите команду, нажав <Enter>.

Если ошибок не возникло, то вы только что создали еще одну глобальную группу.

Просмотр хронологии PowerShell

Вы видели на рис. 7.22, что задачи, которые ранее выполнялись в Active Directory Administrative Center, транслируются в команды PowerShell и отображаются в панели Windows PowerShell History. Поскольку средство ADAC построено поверх PowerShell, все действия будут представлены внутри панели Windows PowerShell History в виде команд. В Windows Server 2012 Active Directory имеется свыше 140 командлетов PowerShell, поэтому изучение синтаксиса их всех займет очень много времени. Таким образом, мы рекомендуем чаще заглядывать в панель Windows PowerShell History, которая поможет в освоении этих команд.

В верхней части панели Windows PowerShell History присутствует несколько элементов управления.

- **Copy (Копировать).** Ссылка Copy предназначена для копирования одной или нескольких команд. Чтобы скопировать несколько команд, можно при нажатой клавише <Ctrl> шелкать на нужных командах.
- **Search (Поиск).** С помощью поля Search можно искать любой командлет внутри хронологии PowerShell. Просто начинайте вводить несколько первых букв и панель сузится, отображая только результаты поиска.
- **Start Task (Начать задачу) и End Task (Завершить задачу).** Если вы хотите сгруппировать свои команды, то перед выполнением любого действия в ADAC можете щелкнуть на ссылке Start Task и указать имя задачи, а по завершении действия щелкнуть на ссылке End Task. Для создания следующей группы команд эти шаги потребуется повторить.
- **Clear All (Очистить все).** Щелчок на ссылке Clear All приводит к очистке хронологии команд.
- **Show All (Показать все).** Когда флажок Show All отмечен, то каждая задача, выполняемая в ADAC, будет показана в панели Windows PowerShell History. Если этот флажок не отмечен, будут отображаться только задачи, манипулирующие Active Directory. По умолчанию флажок Show All не отмечен.

Делегирование управления с использованием организационных единиц

Ранее в этой главе упоминалось, что одной из причин создания организационной единицы является делегирование управления и, безусловно, одно из преимуществ AD заключается в том, что вам позволено наделять частичными или полными административными полномочиями определенную группу пользователей. Это значит, что сеть с одним доменом можно разделить на такие организационные единицы, как `Uptown` (спальный район) и `Downtown` (деловой район), или `Marketing` (отдел маркетинга), `Engineering` (конструкторский отдел) и `Management` (отдел управления), либо же иным образом. Вероятно, наиболее распространенным требованием или причиной делегировать управление организационной единице является предоставление персоналу технической поддержки разрешения сбрасывать пароли пользователей. Еще одним часто запрашиваемым разрешением считается возможность изменения только определенных атрибутов в объектах пользователей или групп. Разумеется, на протяжении своей карьеры как администратора Active Directory вы столкнетесь со многими другими требованиями. Даже если вы не особо заинтересованы в делегировании, в главе 9 будет дан хороший старт к делегированию управления в Active Directory.

Задачи обслуживания домена

После установки домена придется проводить определенное обслуживание. Хотя в этом разделе не раскрываются абсолютно все задачи, которые понадобится делать, здесь описаны самые основные из них:

- присоединение к домену;
- вывод из эксплуатации контроллера домена;
- устранение неполадок в DNS, интегрированной с Active Directory;
- поднятие функциональных уровней домена и леса;
- использование утилиты `Netdom`;
- управление временем в домене;
- передача ролей FSMO.

Присоединение к домену

Чтобы присоединить сервер Windows Server 2012 к домену, выполните перечисленные ниже шаги. После присоединения к домену сервер станет сервером-членом.

1. Войдите в систему на локальном сервере.
2. Откройте диспетчер серверов и щелкните на элементе Local Server (Локальный сервер).
3. Щелкните на ссылке справа от слова Domain (Домен) в верхнем левом углу.
4. Откроется диалоговое окно System Properties (Свойства системы). Перейдите в нем на вкладку Computer Name (Имя компьютера) и щелкните на кнопке Change (Изменить).

5. Выберите переключатель Domain (Домен) и введите имя домена, к которому нужно присоединиться. Диалоговое окно должно выглядеть похожим на показанное на рис. 7.23, где видно, что система находится в рабочей группе WORKGROUP, а на рис. 7.24 мы добавили домен, к которому необходимо присоединиться. Щелкните на кнопке OK. Будет предложено предоставить данные учетной записи, имеющей разрешение на вход в домен.
6. Введите учетные данные и щелкните на кнопке OK.
7. Спустя некоторое время вы увидите диалоговое окно с приветствием. Щелкните в нем на кнопке OK. Будет выдано сообщение о необходимости последующей перезагрузки компьютера. Щелкните на кнопке OK.
8. Щелкните на кнопке Close (Закрыть), чтобы закрыть диалоговое окно System Properties.
9. Вы получите еще одно напоминание о том, что сервер должен быть перезагружен. Щелкните на кнопке Restart Now (Перезагрузить сейчас).

После того, как сервер перезагрузится, он станет членом домена, т.е. сервером-членом.

Автономное присоединение к домену

В Windows Server 2008 R2 появилась новая возможность, позволяющая присоединять систему Windows 7 / Windows 8 или Windows Server 2008 R2 / Windows Server 2012 к домену, не контактируя с контроллером домена. Это может быть удобно в ситуации, когда компьютер не располагает надежным подключением к корпоративной сети. ОС Windows Server 2012 также предлагает эту возможность, но графический пользовательский интерфейс для ее конфигурирования по-прежнему отсутствует. Более подробные сведения об автономном присоединении к домену приведены в статье TechNet по адресу `http://technet.microsoft.com/en-us/library/dd392267.aspx`, которая была обновлена для Windows Server 2012.

Рис. 7.23. В текущий момент система находится в рабочей группе

Рис. 7.24. Система присоединяется к домену

Вывод из эксплуатации контроллера домена

Если возникает необходимость вывести из эксплуатации один из контроллеров домена, крайне важно делать это корректно. При выведении его из эксплуатации вы удаляете все компоненты Active Directory и возвращаете контроллеру домена роль сервера-члена.

Правильный вывод из эксплуатации контроллера домена особенно важен, когда это делается для первого DC. Первый DC в домене включает несколько ролей хозяина операций (Operations Master), иногда называемых ролями FSMO (Flexible Single Master Operations — гибкие операции с одним хозяином), которые являются неотъемлемыми для корректного функционирования домена. Если этот сервер просто откажет, и вы не сможете вернуть ему работоспособность, приготовьтесь к появлению некоторых проблем, пока вы не выведете его правильно из эксплуатации.

Самый легкий метод вывода из эксплуатации контроллера домена предусматривает запуск командлета PowerShell по имени `Uninstall-ADDSDomainController`. В Windows Server 2008 R2 была возможность запустить утилиту `DCPromo`, чтобы понизить контроллер домена, но в версии Windows Server 2012 утилита `DCPromo` отсутствует. Указанный командлет будет выполнять задачи, очень похожие на те, что делала утилита `DCPromo` в прошлых версиях Windows. Если контроллер домена, на котором запускается данный командлет, все еще функционирует и содержит все роли FMSO, то командлет передаст эти роли новому контроллеру домена, понизит текущий контроллер домена, переместит объект компьютера из организационной единицы `Domain Controllers` (Контроллеры домена) в контейнер `Computers` (Компьютеры) и позаботится о ряде других деталей. Роль сервера DNS по-прежнему будет установлена и работать, но если ваши зоны DNS были интегрированными с Active Directory (Active Directory integrated — ADI), они больше не будут доступны.

Если такой сервер просто откажет, и вы не сможете запустить на нем `Uninstall-ADDSDomainController`, то потребуется удалить из домена все зависимости от него, такие как записи SRV в DNS, которые указывают на этот контроллер домена, и другие глубоко скрытые следы в Active Directory. В предшествующих версиях Windows это был довольно долгий и утомительный процесс, при котором использовалась утилита `NTDSUtil` и проводилось много ручной работы. Тем не менее, с помощью оснастки Active Directory Users and Computers, доступной в Windows Server 2012, можно просто удалить объект контроллера домена из организационной единицы `Domain Controllers` и на этом все.

Для тех, кто проходил через длительный процесс анализа метаданных с помощью `NTDSUtil` и других инструментов, это стало великолепным дополнением.

1. Запустите оснастку Active Directory Users and Computers и найдите в ней организационную единицу `Domain Controllers`.
2. Отыщите контроллер домена, который необходимо вывести из эксплуатации. Щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Delete (Удалить).
3. Удостоверьтесь в том, что выбрали корректный DC, и щелкните на кнопке Yes (Да) в диалоговом окне с запросом подтверждения.

   Откроется диалоговое окно с предупреждением, что вы пытаетесь удалить DC из AD, не используя мастер Active Directory Installation Wizard.

4. Отметьте флажок This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO) (Этот контроллер домена постоянно отключен и не может больше понижаться с использованием мастера установки AD DS (DCPROMO)) и щелкните на кнопке Delete (Удалить), как показано на рис. 7.25.

   Если этот DC является сервером глобального каталога, вы получите диалоговое окно с запросом, желаете ли продолжить.

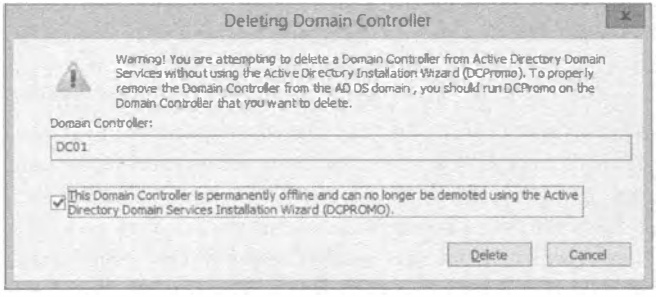


Рис. 7.25. Удаление контроллера домена

5. Щелкните на кнопке Yes (Да).

   Если сервер имел любые роли Operations Master, будет выдано сообщение о необходимости передачи этих ролей (или роли) на другой контроллер домена.

6. Щелкните на кнопке OK, и другой контроллер домена захватит эти роли (роль).

Если отказавший контроллер домена позже восстановить, вы не сможете удалить Active Directory с применением `Uninstall-ADDSDomainController`. Однако существует обходной путь. Вместо ввода просто `Uninstall-ADDSDomainController` введите `Uninstall-ADDSDomainController -ForceRemoval`. Переключатель `-ForceRemoval` позволит Active Directory удалиться без доступа к другому DC в домене. Этот командлет поддерживает и другие параметры, которые можно просмотреть, введя `Get-Help Uninstall-ADDSDomainController`. Например, переключатель `-Force` будет подавлять любые предстоящие предупреждения, что может быть удобно при его использовании внутри сценария, а переключатель `-DemoteOperationMasterRole` принудительно запустит понижение Active Directory, даже если обнаружена какая-нибудь роль Operations Master. Естественно, вы можете комбинировать все эти параметры для удаления Active Directory из висячего контроллера домена.

Устранение неполадок в AD DNS

Распространенная проблема, возникающая в DNS, заключается в том, что записи SRV не создаются, когда сервер перезагружается. За создание этих записей отвечает служба `netlogon`, и временами она дает небольшие сбои после перезагрузки сервера. В качестве напоминания: записи SRV применяются для нахождения в домене контроллеров домена, выполняющих специфические службы или удерживающих определенные роли.

Спрашивайте, прежде чем уничтожать

Согласитесь, было бы неплохо иметь какое-то представление о будущем, чтобы увидеть, что произойдет, если предпринять определенные действия. Предположим, что у вас есть контроллер домена, который вы хотели бы понизить, но не уверены, что были удовлетворены все предварительные условия. Ваш друг PowerShell 3.0 предлагает командлеты, которые вы можете опробовать, прежде чем действительно что-то сделать.

В данном примере вы можете запустить командлет `Test-ADDSDomainController Uninstallation`. Он выполнит проверку, чтобы выяснить, удовлетворены ли все предварительные условия для понижения. После запуска этого командлета вам будет сообщено состояние успеха или отказа, а также другая полезная информация. Как и со всеми остальными командлетами, вы можете запустить `Get-Help` или просто `Test-ADDSDomainControllerUninstallation`, чтобы получить сведения о других необязательных параметрах для него.

По мере все большего погружения в PowerShell 3.0, вы обнаружите и другие командлеты `Test-`, например, `Test-ADDSDomainControllerInstallation`, `Test-ADDSDomainInstallation`, `Test-ADDSReadOnlyDomainControllerAccountCreation` и т.д. За дополнительной информацией по этой теме обращайтесь к статье TechNet по адресу `http://technet.microsoft.com/en-us/library/hh974719.aspx`.

К примеру, службы внутри домена часто нуждаются в обнаружении сервера глобального каталога, эмулятора PDC, контроллера домена внутри заданного сайта или просто контроллера домена в рамках домена. Службы запрашивают у DNS соответствующие записи SRV, и при условии, что они существуют, сервер может быть найден. Тем не менее, иногда такие записи не создаются после перезагрузки. На рис. 7.26 показано окно консоли DNS Manager (Диспетчер DNS), открытое для отображения того, какие записи были созданы корректно. Обратите внимание, что имена некоторых папок начинаются с символа подчеркивания (`_msdcs`, `_sites`, `_tcp` и `_udp`). Каждая из этих папок содержит записи SRV.

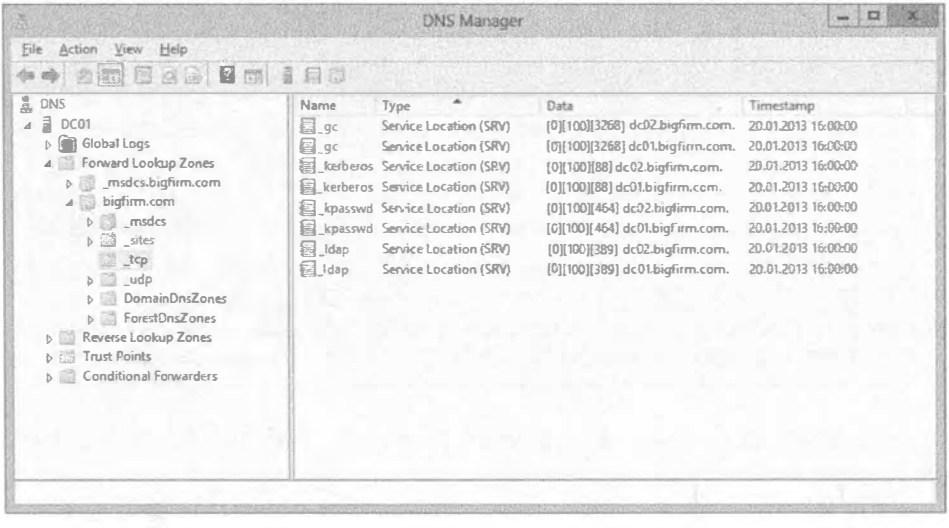


Рис. 7.26. Записи служб DNS (SRV)

Если вы столкнулись с проблемами подключаемости и заметили, что записи SRV отсутствуют в DNS, это просто исправить. Перейдите в окно командной строки и выполните следующие две команды:

```
Net stop netlogon
Net start netlogon
```

Служба `netlogon` воссоздаст записи и все станет работоспособным.

Поднятие функциональных уровней домена и леса

После первоначального создания леса или после проведения модернизации от среды Windows Server 2008 может понадобиться поднять функциональные уровни домена и леса. Основной причиной является получение преимуществ от дополнительных возможностей, доступных на более высоких уровнях. Хотя функциональные уровни леса Window Server 2012 не предлагают каких-то новых возможностей, вы можете все равно стремиться к поднятию функционального уровня домена до Windows Server 2012. Так или иначе, потребуется выполнить следующие общие шаги.

1. Удостовериться, что на всех контроллерах домена функционирует Windows Server 2012.
2. Поднять функциональный уровень домена до Windows Server 2012.
3. Поднять функциональный уровень леса до Windows Server 2012.

Важно помнить, что после поднятия уровня откатиться обратно не получится. Если текущий функциональный уровень домена Windows Server 2008 R2, и вы поднимете его до Windows Server 2012, вы больше не будете иметь возможность поднятия чего-либо меньшего, чем сервер Windows Server 2012 до контроллера домена. В случае если это вписывается в ваши планы, поднимайте уровни.

Функциональный уровень (не) может быть понижен

Хорошо, это не совсем так. При наличии функционального уровня леса Windows Server 2012 функциональные уровни леса и домена можно было бы понизить до Windows Server 2008 R2. Это нельзя сделать в графическом пользовательском интерфейсе, но для решения такой задачи можно запустить две команды PowerShell.

Вот как понизить функциональный уровень леса до Windows Server 2008 R2:

```
Set-ADForestMode -Identity "bigfirm.com"
   -ForestMode Windows2008R2Forest
```

А так понизить функциональный уровень домена до Windows Server 2008 R2:

```
Set-ADDomainMode -Identity "bigfirm.com"
   -DomainMode Windows2008R2Domain
```

Помните, что понижение функционального уровня леса также нарушит работу зависимых средств, например, Dynamic Access Control (Динамический контроль доступа).

Ниже перечислены четыре инструмента, которые можно использовать для поднятия функциональных уровней домена и леса:

- Active Directory Users and Computers (Пользователи и компьютеры Active Directory) — для поднятия функционального уровня домена;

- Active Directory Domains and Trusts (Домены и доверительные отношения Active Directory) — для поднятия функционального уровня леса;
- Active Directory Administrative Center (Центр администрирования Active Directory) — для поднятия функциональных уровней домена и леса;
- PowerShell 3.0 — для поднятия функциональных уровней домена и леса.

Выберите подходящий метод в зависимости от версии. Поскольку инструмент Active Directory Administrative Center является новым, мы рассмотрим эту консоль и покажем, как с ее помощью поднимать функциональные уровни домена и леса.

Чтобы поднять функциональный уровень домена, выполните следующие шаги.

1. Запустите Active Directory Administrative Center, нажав комбинацию клавиш <Windows+R> для открытия диалогового окна Run (Выполнить), введите **dsac.exe** в текстовом поле и щелкните на кнопке OK.
2. Откроется консоль Active Directory Administrative Center.
3. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт Raise the domain functional level (Поднять функциональный уровень домена), как показано на рис. 7.27.
4. Просмотрите информацию в окне Raise Domain Functional Level (Поднятие функционального уровня домена).

   Обратите внимание, что это окно информирует о текущем функциональном уровне и предоставляет возможность поднять его. Выберите в раскрывающемся списке вариант Windows Server 2012.
5. Щелкните на кнопке OK.

   Вы получите еще одно предупреждение о том, что это действие необратимо.
6. Щелкните на кнопке OK.

   Спустя некоторое время отобразится диалоговое окно с сообщением о том, что уровень был успешно поднят.
7. Щелкните на кнопке OK.

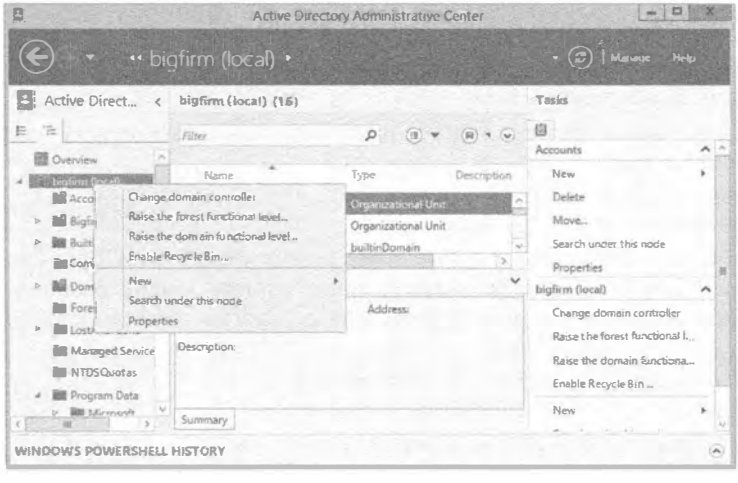


Рис. 7.27. Поднятие функциональных уровней в Active Directory Administrative Center

Поднятие функционального уровня леса осуществляется аналогично.

1. Запустите Active Directory Administrative Center, нажав комбинацию клавиш <Windows+R> для открытия диалогового окна Run (Выполнить), введите **dsac.exe** в текстовом поле и щелкните на кнопке OK.
2. Откроется консоль Active Directory Administrative Center.
3. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт Raise the forest functional level (Поднять функциональный уровень леса).
4. Просмотрите информацию в окне Raise Forest Functional Level (Поднятие функционального уровня леса).

   Обратите внимание, что это окно информирует о текущем функциональном уровне и предоставляет возможность поднять его. Выберите в раскрывающемся списке вариант Windows Server 2012.
5. Щелкните на кнопке OK.

   Вы получите еще одно предупреждение о необратимости этого действия.
6. Щелкните на кнопке OK.

   Спустя некоторое время отобразится диалоговое окно с сообщением о том, что уровень был успешно поднят.
7. Щелкните на кнопке OK.

Многие дополнительные возможности более высоких функциональных уровней станут доступными автоматически и лишь некоторые (такие как корзина Active Directory (Active Directory Recycle Bin)) для своего включения требуют выполнения добавочных шагов.

Поднятие функциональных уровней домена и леса с помощью PowerShell

Поднятие функциональных уровней домена или леса не входит в число ежедневных задач администратора. Возможно, вы будете делать это несколько раз за всю свою карьеру и, скорее всего, не станете применять сценарий для поднятия уровней. Следовательно, это не особенно удачный случай использования PowerShell. Но для того чтобы показать, что это возможно с помощью нового PowerShell 3.0, ниже приведено соответствующее описание.

Чтобы поднять функциональный уровень домена, откройте командное окно PowerShell и введите:

```
Set-ADDomainMode -Identity "bigfirm.com"
   -DomainMode Windows2012Domain
```

Вам понадобится подтвердить действие путем ввода `Y`. После этого домен `bigfirm.com` будет поднят до функционального уровня домена Windows Server 2012. Чтобы поднять функциональный уровень леса, откройте командное окно PowerShell и введите:

```
Set-ADForestMode -Identity "bigfirm.com"
   -ForestMode Windows2012Forest
```

Это действие также необходимо подтвердить путем ввода `Y`. Затем лес `bigfirm.com` будет поднят до функционального уровня леса Windows Server 2012.

Использование утилиты Netdom

Одним из полезных инструментов командной строки является Netdom (диспетчер доменов). Он доступен на любом сервере, повышенном до контроллера домена. Хотя Netdom главным образом используется для управления доверительными отношениями в средах с более чем одним доменом, существуют также и другие применения.

Переименование компьютеров (включая контроллеры доменов)

Команда netdom computername позволяет безопасно переименовывать контроллеры доменов и серверы-члены. В ранних версиях Windows переименование контроллера домена было невозможно без его предварительного понижения до сервера-члена. Примите во внимание, что даже при использовании Netdom для переименования контроллера домена может требоваться пара перезагрузок, прежде чем все будет приведено в порядок — особенно это касается DNS. Что более важно, вы не должны переименовывать серверы, которые являются серверами сертификатов (т.е. на них функционируют службы сертификатов Active Directory (Active Directory Certificate Services)). Сервер сертификатов должен сохранять свое имя. Имя, встроенное в сертификат, идентифицирует сервер, которому он выдан, и сервер, который выпустил сертификат. Сертификаты проверяются путем запроса исходного сервера, но если имя изменилось, то сертификаты не смогут быть подтверждены.

Переименование контроллера домена предусматривает назначение ему альтернативного имени и изменение альтернативного имени на основное имя контроллера домена. Например, если в домене bigfirm.com есть контроллер домена по имени DC01, и его нужно переименовать на DC03, то сначала потребуется назначить ему альтернативное имя DC03 с помощью следующей команды:

```
Netdom computername DC01 /add:DC03.bigfirm.com
```

В этот момент сервер имеет два имени: основное и альтернативное. Теперь измените имя компьютера на альтернативное посредством такой команды:

```
Netdom computername DC01 /makeprimary:DC03.bigfirm.com
```

Инструмент Netdom сообщит об успешном завершении процесса и запросит перезагрузку сервера. После перезагрузки контроллер домена изменит альтернативное имя на имя, которое ранее было основным.

Последний шаг заключается в удалении старого имени DC01 из объекта компьютера для контроллера домена:

```
Netdom computername DC03 /remove:DC01.bigfirm.com
```

Теперь контроллер домена имеет новое имя.

Присоединение компьютера к домену

Если вы хотите присоединить компьютер к домену из командной строки или через сценарий, можете воспользоваться Netdom. Ниже показан простейший вариант команды:

```
Netdom join server01 /d:bigfirm.com /reboot
```

Эта команда присоединит компьютер по имени server01 к домену bigfirm.com и выполнит перезагрузку. Обычно учетная запись компьютера, присоединенного к

домену, помещается в контейнер Computers (Компьютеры). Как упоминалось ранее, с помощью команды redircmp учетные записи компьютеров можно создавать где-то в другом месте.

Решить данную задачу возможно также и с применением Netdom, но это труднее, чем с использованием инструментов командной строки для службы каталогов (наподобие DSMove). Например, чтобы переместить учетную запись компьютера из контейнера Computers в организационную единицу Sales, после команды NetDom join введите следующую команду DSMove:

```
Dsmove "CN=Server01,CN=Computers,DC=bigfirm,DC=com"
  -newparent "OU=Sales,DC=bigfirm,DC=com"
```

Присоединение компьютера к домену с помощью PowerShell

Утилита Netdom — очень хороший инструмент для управления доменом, и определенные задачи могут быть выполнены только посредством Netdom. С точки зрения присоединения компьютеров к домену PowerShell может помочь, когда к домену необходимо добавить несколько компьютеров или даже дистанционно добавить к нему компьютеры рабочей группы. Ниже показана базовая команда для добавления сервера Windows Server 2012 по имени Server01 к домену bigfirm.com:

```
Add-Computer -ComputerName Server01
    -LocalCredential Server01\Administrator
    -DomainName "bigfirm.com"
    -OUPath "OU=Sales,DC=bigfirm,DC=com"
    -Credential bigfirm\administrator -Restart -Force
```

Эту команду можно запустить на контроллере домена Windows Server 2012 и дистанционно присоединить сервер Server01 к домену. Во время выполнения этой команды два раза запрашиваются пароли; первый раз понадобится ввести пароль локального администратора (параметр -LocalCredential), а второй раз необходимо ввести пароль для учетной записи, которая имеет разрешение на создание учетной записи компьютера в домене (параметр -Credential).

Другие команды Netdom

Инструмент Netdom поддерживает множество других команд, которые можно применять для управления доменом. Полный справочник по Netdom доступен по ссылке http://technet.microsoft.com/en-us/library/cc772217.aspx.

Ниже перечислено несколько других команд, которые могут быть интересными.

- NetDom Reset. Сбрасывает учетную запись компьютера. Иногда система не может войти в домен из-за утери учетной записи в домене. Зачастую обычного сброса учетной записи оказывается достаточно для решения проблемы.
- NetDom Reset Pwd. Сбрасывает пароль для входа компьютера в домен. Если компьютер долго не подключался к домену, возможно, истек срок действия пароля для учетной записи. Эта команда может решить данную проблему.
- NetDom Remove. Удаляет компьютер из домена.
- NetDom query fsmo. Временами требуется быстро найти роли Operations Master внутри домена. Вместо того чтобы щелкать в разных окнах графического пользовательского интерфейса, с помощью этой команды можно легко отобразить все роли Operations Master.

Управление временем в домене

Протокол аутентификации Kerberos, используемый Active Directory, требует, чтобы все компьютеры в домене были синхронизированы друг с другом. Если какой-то компьютер теряет связь с контроллером домена на период более пяти минут, будет возможность подключиться к сети, но все службы могут работать неправильно до тех пор, пока не будет скорректировано время. По этой причине синхронизация времени очень важна в домене. Синхронизация времени достигается посредством иерархии. Она начинается с сервера, содержащего роль PDC Operations Master (Хозяин операций основного контроллера домена), которым обычно является первый контроллер домена, созданный в домене, и распространяется на все системы внутри домена. Чтобы выяснить, на каком сервере находится эта роль, выполните следующие шаги.

Рис. 7.28. Вкладка PDC диалогового окна Operations Masters

1. Запустите оснастку Active Directory Users and Computers.
2. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт Operations Masters (Хозяева операций).
3. В открывшемся диалоговом окне Operations Masters (Хозяева операций) перейдите на вкладку PDC (Основной контроллер домена), как показано на рис. 7.28.

В идеальном случае контроллер домена, на котором расположена роль PDC, сконфигурирован для синхронизации с действительным источником NTP (Network Time Protocol — протокол сетевого времени). Остальные компьютеры в домене будут получать показания времени от этого сервера.

- Все контроллеры домена будут синхронизировать свое время со временем на PDC.
- Все компьютеры и серверы-члены будут синхронизировать свое время со временем на контроллере домена, где они прошли аутентификацию.
- Если компьютер специально сконфигурирован так, чтобы не получать показания времени от контроллера домена, на котором он прошел аутентификацию, он должен быть синхронизирован с сервером NTP в точности как контроллер домена с ролью PDC Operations Master.

При условии, что основной контроллер домена имеет корректное время, а пользователи не изменяют показания времени в своих системах, все будет работать нормально.

Ограничение изменений показания времени с помощью групповой политики

Нередко администраторы настраивают групповую политику (Group Policy), чтобы пользователи не могли изменять показания времени и непредумышленно изымать свои системы из домена. Настройка System Time Group Policy (Групповая политика системного времени) находится в Computer/Policies/Windows Settings/Security Settings/Local Policies/User Right Assignment (Компьютер/Политики/Настройки Windows/Настройки безопасности/Локальные политики/Назначение прав пользователям).

Для проверки и синхронизации времени будет применяться служба времени Windows (Windows Time Service; `w32tm`). Служба `w32tm` запускается из командной строки.

Представленная ниже команда позволяет сравнить пять выборок текущего времени с данными из сервера времени Microsoft (`time.windows.com`) и проконтролировать, насколько точными они являются. В выводе будет отражено, опережают ли показания времени на вашем сервере (обозначено с помощью +) или же отстают (обозначено с помощью -):

```
w32tm /stripchart /computer:time.windows.com /samples:5 /dataonly
```

Синхронизировать время на контроллере домена с ролью PDC Operations Master можно с использованием внутреннего источника времени, если он есть, и внешнего источника времени в противном случае. При синхронизации с внешним сервером NTP посредством службы `w32tm` удостоверьтесь, что UDP-порт 123 открыт в брандмауэре.

С помощью показанной далее команды время в системе можно синхронизировать с внешним сервером времени. Доступно несколько серверов времени, но в данном примере применяется сервер времени Microsoft (`time.windows.com`) и сервер времени NIST (`time.nist.gov`):

```
W32tm /config "/manualpeerlist:time.nist.gov,time.windows.com"
      /syncfromflags:manual /reliable:yes /update
```

Параметр `syncfromflags` указывает, что сервер будет синхронизироваться с одним из серверов в группе `manualpeerlist`. Можно задать только один сервер времени (и тогда опустить кавычки) или доставить множество таких серверов, разделенных запятыми, как сделано в примере команды.

Кроме того, имеет смысл перезапустить службу времени с использованием следующих команд:

```
Net stop w32time
Net start w32time
```

После перезапуска службы можно ввести показанную ранее команду `w32tm`, чтобы проверить точность показания времени. Если вы измените время, то может пройти пять минут, прежде чем служба `w32tm` снова проведет синхронизацию и установит правильное показание времени.

В этом разделе рассматриваются различные задачи и приемы обслуживания, которые вы наверняка сочтете полезными для поддержания своей сети в работоспособном состоянии. Это определенно неполный список, но в нем отражены основы. Новейшим средством, которое поможет сократить объем необходимых действий по обслуживанию, являются *детализированные политики паролей*. Это средство позволяет устанавливать множество политик блокировки паролей для учетных записей, не создавая новый домен.

Роли FSMO и их передача

Служба Active Directory содержит в себе роли FSMO (Flexible Single Master Operations — гибкие операции с одним хозяином), которые применяются для выполнения различных задач внутри леса и домена. Существуют две роли на уровне леса и три роли на уровне домена. В табл. 7.1 описаны названия, области действия и назначение этих ролей.

Таблица 7.1. Роли FSMO

Роль FSMO	Область действия	Назначение
Schema Master (Хозяин схемы)	Лес	Содержит в себе схему леса
Domain Naming Master (Хозяин именования доменов)	Лес	Управляет именами доменов
Infrastructure Master (Хозяин инфраструктуры)	Домен	Обеспечивает междоменные ссылки на объекты
PDC Emulator (Эмулятор основного контроллера домена)	Домен	Отвечает за время в лесе Обрабатывает изменения паролей Является точкой подключения для управления объектами GPO Блокирует учетные записи
RID Master (Хозяин относительных идентификаторов (RID))	Домен	Управляет и пополняет пулы RID (relative identifier — относительный идентификатор)

В определенных ситуациях, например, при выводе из эксплуатации контроллера домена, модернизации домена или в случае возникновения проблем с производительностью, понадобится передать эти роли новому контроллеру домена. Каждая из указанных ролей должна быть все время доступной в Active Directory. Один из способов переноса или передачи этих ролей новому контроллеру домена предусматривает использование утилиты `NTDSUtil`.

Чтобы передать роли FSMO домена, выполните описанные далее шаги.

1. Откройте окно командной строки (`cmd.exe`), введите `NTDSUtil` и нажмите <Enter>.
2. Введите `roles` и нажмите <Enter>.
3. Введите `connections` и нажмите <Enter>.
4. Теперь необходимо подключиться к серверу, который в будущем будет содержать эти роли FSMO. Введите `connect to server [Имя_сервера]` и нажмите <Enter>.
5. Введите `quit` и нажмите <Enter>.
6. Первой будет передаваться роль PDC Emulator. Введите `transfer pdc` и нажмите <Enter>. Вы должны подтвердить запрос, щелкнув на кнопке Yes (Да).
7. При необходимости можно ввести `transfer rid master` и нажать <Enter> для перемещения роли RID Master. Вы должны подтвердить запрос, щелкнув на кнопке Yes (Да).
8. При необходимости можно ввести `transfer infrastructure master` и нажать <Enter> для перемещения роли Infrastructure Master. Вы должны подтвердить запрос, щелкнув на кнопке Yes (Да).
9. Теперь, когда передача всех ролей FSMO домена завершена, введите `quit` и нажмите <Enter>, затем снова введите `quit` и нажмите <Enter>, чтобы закрыть окно командной строки.

Разумеется, приведенные шаги должны быть выполнены в каждом домене.

Если вы решите передать роли FSMO уровня леса, выполните следующие шаги.

1. Откройте окно командной строки (`cmd.exe`), введите `NTDSUtil` и нажмите <Enter>.
2. Введите `roles` и нажмите <Enter>.
3. Введите `connections` и нажмите <Enter>.
4. Теперь необходимо подключиться к серверу, который в будущем будет содержать эти роли FSMO. Введите `connect to server [Имя_сервера]` и нажмите <Enter>.
5. Введите `quit` и нажмите <Enter>.
6. Первой будет передаваться роль Schema Master. Введите `transfer schema master` и нажмите <Enter>. Вы должны подтвердить запрос, щелкнув на кнопке Yes (Да).
7. При необходимости можно ввести `transfer naming master` и нажать <Enter> для перемещения роли Domain Naming Master. Вы должны подтвердить запрос, щелкнув на кнопке Yes (Да).
8. Теперь, когда передача всех ролей FSMO леса завершена, введите `quit` и нажмите <Enter>, затем снова введите `quit` и нажмите <Enter>, чтобы закрыть окно командной строки.

После переноса всех ролей FSMO на новый контроллер (или контроллеры) домена может понадобиться проверить, все ли работает так, как ожидается. Мы предполагаем, что вы запустите в окне командной строки команду `netdom query fsmo role`, которая отобразит сведения о том, какой контроллер домена содержит в себе те или иные роли FSMO.

Детализированные политики паролей

Прежде чем реализовывать детализированные политики паролей, необходимо удостовериться в том, что ваша среда удовлетворяет минимальным требованиям.

- В домене развернут контроллер домена Windows Server 2012.
- Функциональный уровень домена должен быть установлен в Windows Server 2008.

Создавать объекты настройки паролей (password-settings object — PSO) могут только члены группы `Domain Admins` (Администраторы домена).

Создание объекта настройки паролей

В Windows Server 2012 для создания объектов настройки паролей доступен великолепный графический пользовательский интерфейс. По сравнению с Windows Server 2008 R2 внутренне ничего не изменилось; возможности остались теми же. Однако огромное преимущество заключается в том, что управлять объектами PSO теперь можно через графический пользовательский интерфейс, особенно когда дело доходит до набора значений времени для записей продолжительности, что ранее требовало больших усилий.

Чтобы создать объект PSO для группы G_ITAdmins, выполните перечисленные ниже шаги.

1. Запустите Active Directory Administrative Center, нажав комбинацию клавиш <Windows+R> для открытия диалогового окна Run (Выполнить), введите **dsac.exe** в текстовом поле и щелкните на кнопке OK. Можете также запустить Active Directory Administrative Center.
2. Переключитесь на древовидное представление и выполните прокрутку вниз, пока не увидите элемент System/Password Settings Container (Система/Контейнер настроек паролей).
3. Щелкните правой кнопкой мыши на элементе Password Settings Container и выберите в контекстном меню пункт New⇨Password Settings (Создать⇨Настройки паролей), как показано на рис. 7.29.

Рис. 7.29. Контейнер настроек паролей в ADAC

4. В поле Name (Имя) открывшегося диалогового окна Create Password Settings (Создание настроек паролей) введите **PSO_G_ITAdmins**, а в поле Precedence (Приоритет) укажите значение **10**.
5. Удостоверьтесь, что флажок Enforce minimum password length (Установить минимальную длину пароля) отмечен, и укажите длину **15** символов.
6. Удостоверьтесь, что флажок Enforce minimum password age (Установить минимальный срок действия пароля) отмечен, и укажите продолжительность **30** дней.
7. Удостоверьтесь, что флажок Enforce account lockout policy (Применить политику блокирования учетных записей) отмечен, и укажите в поле Number of failed logon attempts allowed (Количество попыток неудачного входа в систему) значение **5**.
8. В области Directly Applies To (Напрямую применять к) щелкните на кнопке Add (Добавить). Выберите группу G_ITAdmins и щелкните на кнопке OK.

9. Для остальных настроек оставьте то, что выбрано по умолчанию. Диалоговое окно должно иметь вид, подобный показанному на рис. 7.30.
10. Щелкните на кнопке OK, чтобы закрыть это диалоговое окно.

Вы должны увидеть, что в контейнере настроек паролей внутри Active Directory Administrative Center появился объект PSO под названием `PSO_G_ITAdmins`.

Теперь вам нужно какое-то доказательство того, что этот объект PSO работает, и просмотреть имеющиеся настройки. В предшествующих примерах мы создавали пользователя по имени `Sally Smith`. Давайте предположим, что этот пользователь является IT-администратором и, следовательно, данного пользователя необходимо добавить в группу `G_ITAdmins`. Пользователь `Sally Smith` должен получить новые настройки паролей; в этом легко убедиться, войдя в систему на сервере с помощью учетной записи `sally.smith`. Еще один способ выяснить, какие правила объекта PSO применяются к пользователю, предполагает выполнение следующих шагов.

1. Запустите Active Directory Administrative Center.
2. Перейдите в организационную единицу `Sales`, в которой был создан пользователь `Sally Smith`.
3. Щелкните правой кнопкой мыши на имени `Sally Smith` и выберите в контекстном меню пункт View resultant password settings (Просмотреть результирующие настройки паролей), как показано на рис. 7.31.
4. Откроется диалоговое окно для группы `PSO_G_ITAdmins` и вы увидите объект PSO, применяемый к пользователю `Sally Smith`.
5. Щелкните на кнопке OK, чтобы закрыть это диалоговое окно.

Важно знать о том, что объекты PSO можно связывать с другими группами в дополнение к глобальным группам доступа. Однако когда для пользователя определен результирующий набор политики (Resultant Set of Policy — RSOP), принимаются во внимание только те объекты PSO, которые напрямую связаны с объектом пользователя или с глобальной группой доступа, членом которой является пользователь. Объекты PSO, связанные с группами рассылки или другими группами доступа, игнорируются.

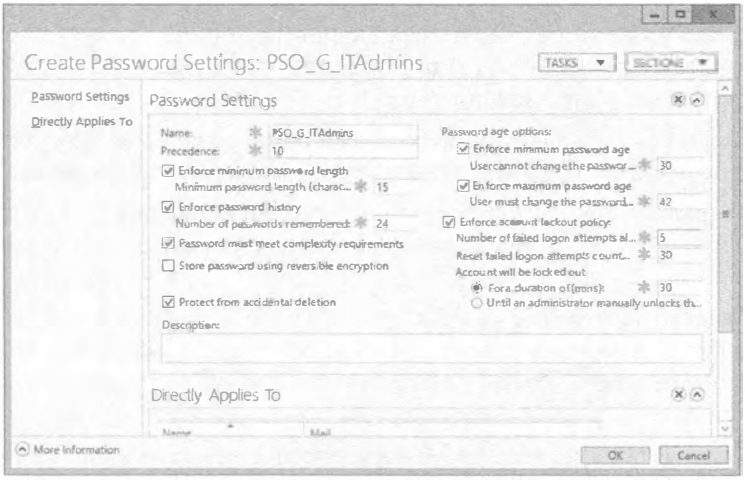


Рис. 7.30. Окончательные настройки паролей

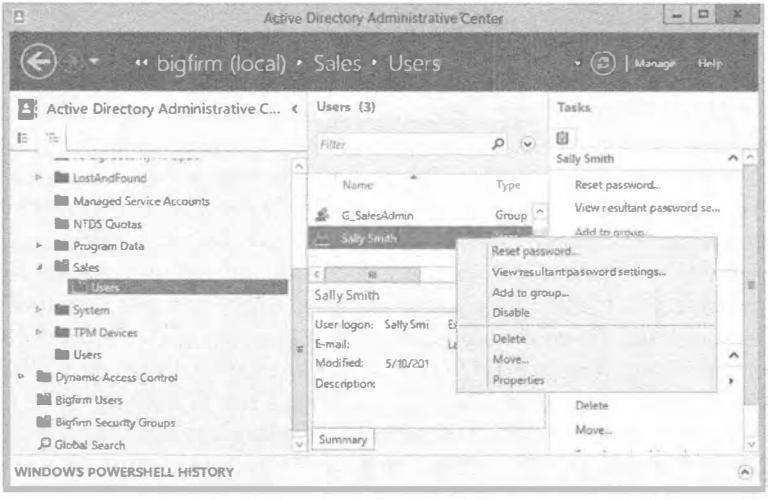


Рис. 7.31. Просмотр результирующих настроек паролей

Приоритет объекта настроек паролей

В предыдущем примере было сконфигурировано несколько настроек паролей, которые установлены аналогично настройкам стандартной политики домена (Default Domain Policy) в домене. Есть еще одна настройка, на которую следует взглянуть. В диалоговом окне Create Password Settings (см. рис. 7.30) можно было указать значение в поле Precedence (Приоритет). Приоритет определяет, какому объекту PSO будет отдано предпочтение, если к объекту пользователя применятся сразу несколько объектов PSO.

Давайте применим к группе `G_ITAdmins` два объекта PSO, один с приоритетом 10, а другой с приоритетом 5. Объект PSO с приоритетом 5 получит преимущество, поскольку предпочтение отдается более низким значениям приоритета по сравнению с более высокими.

Это имеет смысл, если вы просто используете группы и применяете объект PSO на уровне группы. Но что произойдет, когда вы примените объект PSO к группе `G_ITAdmins`, в которой состоит пользователь `Sally Smith`, и еще один объект PSO напрямую к пользователю `Sally Smith`?

Давайте снова возьмем группу `G_ITAdmins`, членом которой является пользователь `Sally Smith`, и применим к ней объект PSO с приоритетом 10. Создайте еще один объект PSO с приоритетом 15 и примените его напрямую к пользователю `Sally Smith`. Объект PSO, примененный к пользователю `Sally Smith` напрямую, получит предпочтение, хотя значение его приоритета больше.

Способ применения объекта PSO определяется следующим образом.

> *Объект PSO, который связан напрямую к объекту пользователя, является результирующим объектом PSO. Если с объектом пользователя никакие объекты PSO не связаны, сравнивается членство пользователя в глобальных группах доступа, а также все объекты PSO, применимые к пользователю на основе его членства в этих глобальных группах. Результирующим объектом PSO будет такой объект, который имеет наименьшее значение приоритета.*

Папка SYSVOL: старое и новое

Действительно замечательной характеристикой Active Directory, которая сохраняется еще с 2000 года и по-прежнему актуальна, является то, что Active Directory представляет собой распределенную базу данных. Могут существовать более одного контроллера домена, на которых хранятся записываемые копии базы данных каталога, что устраняет необходимость в наличии первичного (поддерживающего запись) и вторичного (не поддерживающего запись) серверов. Внутри каждого контроллера домена Active Directory имеется пара папок, которые содержат общие ресурсы, используемые для предоставления функций доступа и репликации различным контроллерам домена. Папка, хранящая эти общие ресурсы, называется SYSVOL. В ней хранятся общая папка NETLOGON (со сценариями входа и объектам GPO для клиентских компьютеров в домене), сценарии входа пользователей, групповая политика Windows, промежуточные папки и файлы службы репликации файлов (File Replication Service — FRS), папки и файлы для синхронизации и соединения файловой системы.

В этом разделе рассматриваются следующие темы:

- введение в службу репликации файлов;
- переход на репликацию распределенной файловой системы (Distributed File System Replication);
- обнаружение текущего состояния перехода с применением команды `dfsrmig`.

Старое: служба репликации файлов

Часто, когда мы считаем что-то в мире технологий старым, с ним ассоциируется негативный подтекст. В данном конкретном случае "старая" означает ссылку на способ, которым выполнялась определенная работа в прошлом. Изменения, внесенные в SYSVOL версией Windows Server 2008 R2 и также Windows Server 2012, охватывают новую методологию проведения репликации материалов SYSVOL между партнерами репликации через весь домен.

Изменилась ли служба FRS в Windows Server 2012?

Нет. Служба FRS работает таким же образом, как в Windows Server 2008 R2, но ее преемник называется DFS-R.

Репликация распределенной файловой системы (Distributed File System Replication — DFS-R) обладает значительными преимуществами по сравнению со службой FRS, однако это вовсе не означает, что старый метод является неудачным. В действительности во всех версиях Active Directory за исключением Windows Server 2008 R2 и Windows Server 2012 применяется "старый" метод. Службу FRS полезно исследовать и понять ее работу, поскольку она преобладает в сетях, в которые планируется добавлять серверы Windows Server 2012.

Понимание функциональности FRS упростит переход от FRS на DFS-R. Но когда нужен такой переход? Он необходим при модернизации домена Windows Server 2003 до Windows Server 2012 либо при модернизации домена Windows Server 2008 (R2), в котором не была реализована DFS-R, но который планируется обновить до

Windows Server 2012. Для поддержания целостности папки SYSVOL репликация FRS использует то, что называется соединениями файловой системы (file system junction). Вы должны освоить работу FRS и некоторые операции, ассоциированные с репликацией FRS. Каждый контроллер домена, на котором функционирует FRS, содержит следующие общие ресурсы и компоненты SYSVOL:

- общая папка NETLOGON;
- сценарии входа пользователей;
- групповая политика Windows;
- промежуточные папки и файлы FRS;
- соединения файловой системы.

Соединения файловой системы широко применяются во всей структуре SYSVOL. Они являются функцией файловой системы NTFS 3.0, которая была введена в Windows 2000 Server. Точки соединения предназначены для устранения утери или разрушения данных, которое может произойти при изменении структуры SYSVOL.

Точки соединения в SYSVOL предназначены для управления хранилищем единственных копий (single-instance store — SIS), которое представляет собой место, где одиночные копии содержимого используются множеством потребителей, например, компьютерами. Точки соединения также называют точками повторной обработки (reparse point). Точка соединения — это физическое местоположение на жестком диске, которое указывает на порцию данных, находящуюся где-то в другом месте на этом диске или на каком-то другом физическом устройстве хранения. В хранилище единственных копий физические файлы существуют только в одном экземпляре внутри файловой системы, а в SYSVOL файл находится в `SYSVOL\staging\domain` или в `SYSVOL\enterprise` и `SYSVOL\staging\enterprise`. Эти дополнительные структуры папок являются точками повторной обработки, которые переадресуют файловый ввод или вывод в исходные местоположения.

Такая конфигурация точек соединения / точек повторной обработки поддерживает согласованность данных за счет гарантии существования данных в единственном экземпляре. Кроме того, конфигурация разрешает иметь более одной точки доступа к отдельной порции данных. Идея состоит в том, чтобы обеспечить избыточность данных без их дублирования. Точки соединения привязывают пространство имен целевой файловой системы к локальному тому NTFS. Лежащие в основе точки повторной обработки позволяют файловой системе NTFS прозрачно переадресовать операцию на целевой объект. В итоге, если вы модифицируете данные в структуре SYSVOL, изменения будут происходить непосредственно в физических файлах. Например, при выполнении операции вырезания и вставки в структуре SYSVOL, которая содержит точки соединения, эта операция произойдет в точке соединения.

Что собой представляет служба FRS

Служба FRS была введена в Windows 2000 Server для репликации папок в распределенной файловой системе (Distributed File System — DFS) и папки SYSVOL. Она реплицирует файлы и папки, хранящиеся в SYSVOL на контроллерах домена и общие папки DFS. Когда служба FRS обнаруживает, что в файл или папку внутри реплицируемого общего ресурса внесено изменение, она автоматически реплицирует обновленную папку на другие серверы. FRS является службой репликации

с несколькими хозяевами, т.е. любой сервер, участвующий в репликации, может инициировать обновления и последующие репликации, а также может разрешать конфликты между файлами и папками, обеспечивая согласованность данных между серверами-партнерами репликации. Служба FRS сохраняет данные синхронизированными между множеством серверов и позволяет сетям увеличивать доступность данных для своих клиентов. Если один сервер становится недостижимым, файлы и папки по-прежнему доступны, поскольку они существуют на другом сервере. Служба FRS полезна при репликации в географически рассредоточенных средах региональных сетей, т.к. данные могут быть синхронизированы с каждым физическим местоположением, что устраняет необходимость использовать клиентами подключения к WAN для доступа к информации из SYSVOL или DFS. Служба FRS, пожалуй, наиболее известна по своей роли в репликации данных SYSVOL между контроллерами внутри домена. Каждый контроллер домена имеет структуру папки SYSVOL, содержащую файлы и папки, которые должны быть доступными и синхронизированными между контроллерами в домене. Общая папка NETLOGON, системные политики и настройки групповой политики являются частью структуры SYSVOL и нуждаются в репликации на все контроллеры домена в домене.

Преимущества репликации с помощью FRS

Когда вы совершаете добавления, изменения или удаления в SYSVOL, служба FRS вступает в действие и реплицирует эти изменения на другие контроллеры домена в домене. Ниже перечислены преимущества службы FRS.

- **Шифрованный протокол RPC.** Служба FRS применяет аутентификацию Kerberos к удаленным вызовам процедур (remote procedure call — RPC) для шифрования данных, которые передаются между участниками репликации.
- **Сжатие.** Служба FRS сжимает файлы в промежуточной папке, используя сжатие NTFS. Файлы пересылаются по сети между участниками репликации в сжатой форме, экономя пропускную способность сети.
- **Разрешение конфликтов.** Служба FRS разрешает конфликты между файлами и папками, чтобы обеспечивать согласованность данных у участников репликации. Если создаются или модифицируются два файла с идентичными именами, то FRS применяет простое правило для разрешения конфликта, которое выглядит как "выигрывает последний записывающий". Служба определяет самое последнее обновление и считает этот файл авторитетным, после чего реплицирует данную версию файла другим участника репликации. Если на разных серверах создаются две одинаково именованных папки, FRS идентифицирует этот конфликт, но будет использовать другую методику для его разрешения. В таком случае служба FRS переименует папку, которая была создана последней, и реплицирует обе папки членам репликации. Затем администратор может вручную разрешить конфликт без потенциальной потери данных.
- **Непрерывная репликация.** Служба FRS обеспечивает непрерывную репликацию между членами групп репликации. Изменения реплицируются FRS в пределах трех секунд после того, как были сделаны.
- **Отказоустойчивый путь репликации.** Служба FRS не применяет широковещательные рассылки при репликации. Она может предоставить множество путей

для поддержки связности между серверами. Если член репликации недоступен, FRS отправит данные по другому пути. Служба FRS предотвращает отправку идентичных файлов любому члену репликации более одного раза.

- **Планирование репликации.** Интересной особенностью службы FRS является возможность планирования репликации на определенные моменты времени и интервалы. Это становится по-настоящему удобным, когда необходимо реплицировать данные по каналам WAN. Можно запланировать выполнение репликации на часы, когда линия WAN минимально загружена.
- **Целостность репликации.** Служба FRS поддерживает целостность репликации с использованием порядковых номеров обновлений, чтобы регистрировать изменения в журнале на сервере-члене репликации. Служба FRS способна управлять репликацией, даже если один из членов без уведомления прекращает работу. Когда этот член восстановит работоспособность, FRS реплицирует изменения, которые произошли в его отсутствие, а также обновления, сделанные в локальных файлах на сервере-члене до того, как он перестал функционировать. В средах, предшествующих Windows Server 2008, служба FRS применяется главным образом в двух целях — репликация DFS и репликация SYSVOL. Службу FRS можно использовать для поддержания данных в иерархиях DFS синхронизированными между членами топологии репликации. FRS и DFS являются независимыми топологиями, и для DFS не требуется наличие FRS. Чтобы обеспечить актуальность данных на серверах-членах DFS, можно применять и другие методы репликации.

Источник

Большая часть сведений, предлагаемых в этом и следующем разделах, взята из веб-сайта Microsoft TechNet:

`http://technet.microsoft.com/en-us/library/cc781582(v=WS.10).aspx`

Обращайтесь на указанный веб-сайт за дополнительной информацией.

Требования и зависимости FRS

Репликация SYSVOL поддерживается FRS. Служба FRS реплицирует SYSVOL с использованием топологии, сгенерированной средством проверки целостности знаний (Knowledge Consistency Checker — KCC), и также имеет собственные объекты Active Directory, которые реплицируются посредством репликации Active Directory. Средство KCC отвечает за построение топологии репликации Active Directory. Оно применяет очень сложный алгоритм для нахождения наиболее эффективного способа построения объектов подключений между контроллерами домена.

Как насчет AD?

Важно запомнить, что хотя служба FRS используется для репликации SYSVOL, она не применяется в качестве механизма для репликации Active Directory. Есть две части, которые необходимо реплицировать. Одна часть — это содержимое Active Directory, такое как пользователи, компьютеры и группы, а другая часть — содержимое папки SYSVOL наподобие групповых политик. Служба FRS используется только для репликации части SYSVOL, но не части Active Directory.

Для работы службы FRS должны быть удовлетворены некоторые требования и зависимости.

- **Репликация Active Directory.** Служба FRS требует правильного функционирования репликации Active Directory, чтобы объекты FRS в Active Directory находились на всех контроллерах домена в домене.
- **DFS.** Если вы собираетесь применять FRS для поддержания данных синхронизированном состоянии в папках на отдельных физических серверах, то должны сначала построить пространство имен DFS. (Для репликации SYSVOL в этом нет необходимости.)
- **DNS.** Служба FRS требует работающей инфраструктуры DNS. Служба FRS использует DNS для преобразования имен членов репликации.
- **Аутентификация Kerberos.** Служба FRS требует функционирующей среды Kerberos.
- **NTFS.** Служба FRS применяет журнал USN (update sequence number — порядковый номер обновления) на томах NTFS, чтобы идентифицировать изменения или обновления файлов.
- **Удаленные вызовы процедур (RPC).** Служба FRS требует традиционных подключений IP и RPC для взаимодействия с членами репликации и контроллерами домена в домене.

Каково будущее FRS?

В ближайшем будущем служба FRS исчезнет. ОС Windows Server 2012 все еще поддерживает репликацию SYSVOL с помощью FRS, но это старая технология и будущее за файловой системой DFS-R, которая обладает множеством преимуществ по сравнению с FRS. Если вы устанавливаете совершенно новую среду Active Directory на сервере Windows Server 2012, то получите DFS-R сразу после повышения сервера.

FRS в Windows Server 2012 R2

Служба репликации файлов (File Replication Service) в Windows Server 2012 R2 объявлена устаревшей, но она по-прежнему доступна. По этой причине самое время приступить к планированию использования DFS-R.

Новое: репликация распределенной файловой системы

Как было показано ранее в этой главе, служба FRS применялась с момента появления Active Directory в Windows 2000 Server для репликации SYSVOL на контроллеры домена во всем домене Active Directory. В Windows Server 2008 R2 была введена новая опция для репликации SYSVOL в домене, которая называлась Distributed File System Replication (Репликация распределенной файловой системы), или DFS-R. Эта опция присутствует также и в Windows Server 2012. Она представляет собой основанный на состоянии механизм репликации с несколькими хозяевами, который поддерживает планирование репликации и регулировку полосы пропускания. Репликация DFS-R использует алгоритм сжатия RDC (Remote Differential Compression — удаленное раз-

ностное сжатие). Алгоритм RDC — это протокол "передачи разницы по проводам", применяемый для обновления клиентов и серверов через сеть. Он обнаруживает вставки, удаления и модификации в файлах данных и реплицирует партнерам по репликации только изменения, а не целые файлы. Алгоритм RDC может предоставить значительные изменения репликации SYSVOL между контроллерами домена в домене.

Что собой представляет DFS-R

Многие из вас знакомы с распределенной файловой системой (Distributed File System — DFS). Файловая система DFS используется для формирования единого прозрачного пространства имен, в котором пользователи могут получать доступ к общим ресурсам, расположенным в разнообразных местах во всей сети. Такое пространство имен DFS может находиться во множестве местоположений. Как говорит само название, это по-настоящему распределенная файловая система. DFS не является нововведением Windows Server 2012; она существовала на протяжении многих лет. На самом деле, пространство имен DFS — это один из двух сценариев (наряду с репликацией SYSVOL), в которых вы обнаружите службу FRS.

Когда была выпущена версия Windows Server 2008 R2, разработчики из Microsoft обновили способ, которым служба DFS реплицировала файлы и папки. Вместе с DFS было включено новое средство под названием DFS-R. Репликация DFS-R заменяет FRS в DFS, а также в репликации SYSVOL внутри доменов Active Directory, в которых функциональный уровень домена не ниже Windows Server 2008.

Алгоритм RDC, упомянутый в предыдущем разделе, очень эффективен, поскольку благодаря тому, что он обнаруживает изменения в файлах и папках, то вместо репликации целого файла или папки (как делала служба FRS) реплицируются только изменения, произведенные в файле или папке. Во время репликации алгоритм RDC может сэкономить громадный объем полосы пропускания сети. Для репликации файлов и папок DFS-R применяет группы репликации.

Группа репликации — это просто набор серверов, в котором каждый сервер называется *членом* группы. Каждый член участвует в репликации одной или более реплицированных папок.

Реплицированная папка — это такая папка, которая остается синхронизированной на каждом сервере-члене группы репликации.

Топология, планирование и регулировка полосы пропускания для группы репликации применимы к каждой реплицированной папке. Каждая реплицированная папка имеет уникальные настройки, такие как фильтры файлов и папок, позволяющие фильтровать файлы и подпапки внутри нее. Управлять DFS-R можно с использованием инструмента управления DFS либо из командной строки с помощью `DFSRADMIN`, `DFSRDIAG`, `DFSUTIL`, `DFSCMD` и `DFSDIAG`.

Недостаток DFS-R в том, что на контроллерах домена должна быть установлена ОС версии не ниже Windows Server 2008, Windows Server 2008 R2 или Windows Server 2012. Если у вас все еще функционирует Window Server 2003 или давно забытая ОС Windows 2000 Server, вам придется придерживаться FRS до тех пор, пока вы не решите перейти на контроллеры домена более новой версии и воспользоваться DFS-R.

Что нового в DFS-R версии Windows Server 2012

Репликация DFS-R в Windows Server 2012 не содержит особо много новых функций. Усовершенствования в основном ограничиваются исправлением ошибок и улучшениями в области устранения неполадок; механизм стал более отказоустойчивым. Детальную информацию о том, что появилось нового, читайте в TechNet: для Windows Server 2012 — `http://technet.microsoft.com/en-us/library/dn281957.aspx` и для Windows Server 2012 R2 — `http://technet.microsoft.com/en-us/library/dn281957.aspx`.

Миграция на DFS-R

Требование для использования DFS-R состоит в том, что функциональный уровень домена должен быть не ниже Windows Server 2008. Это означает всего лишь повышение всех контроллеров домена до Windows Server 2008 или выше. Вам может показаться, что достаточно просто модернизировать контроллеры домена Windows Server 2003 до Windows Server 2008 или выше, и все было бы в порядке. Однако это не сработает. Процесс миграции из FRS на DFS-R в действительности предусматривает проход по нескольким состояниям, во время которых репликация SYSVOL переходит с репликации FRS на репликацию DFS-R. Точные определения шагов и состояний приводятся в следующем разделе.

Мы настоятельно призываем вас провести миграцию репликации FRS на DFS-R. Служба FRS поддерживается в Windows Server 2012, но ходят слухи, что FRS может больше не поддерживаться в будущих версиях Windows Server. По этой причине планируйте заранее и предпринимайте эти шаги.

Шаги миграции

Описанные далее шаги миграции для Windows Server 2012 остались такими же, как они были в Windows Server 2008 R2. Процесс миграции включает в себя правила миграции настроек на контроллере домена, являющемся эмулятором основного контроллера домена (PDC Emulator), и ожидание, пока остальные контроллеры домена последуют этим правилам. Состояния миграции могут быть определены как локальные на контроллере домена или глобальные в отношении контроллеров в домене. Глобальное состояние миграции устанавливается с помощью утилиты командной строки `dfsrmig`, которая применяется для установки одной из фаз процесса миграции. Эта настройка делается в Active Directory и затем реплицируется на все контроллеры домена. Каждый контроллер домена имеет собственное состояние миграции. Репликация DFS-R на каждом DC опрашивает Active Directory, чтобы выяснить глобальное состояние миграции, в которое DC должен перейти. Если глобальное состояние миграции отличается от локального состояния миграции, то DFS-R попытается перевести локальное состояние так, чтобы оно соответствовало глобальному состоянию. Локальное состояние миграции может быть любым из набора устойчивых или переходных состояний. Миграция SYSVOL проходит через четыре основных состояния (обычно называемых устойчивыми состояниями) и шесть временных состояний (обычно называемых переходными состояниями). Переходные состояния ведут DC в устойчивые состояния.

При миграции SYSVOL из FRS в DFS-R существуют четыре устойчивых состояния, или фазы. Эти состояния называются Start (Начало), Prepared (Подготовлена), Redirected (Переадресована) и Eliminated (Устранена). На них также ссылаются посредством порядковых чисел.

- **Start (состояние 0).** Прежде чем начнется миграция SYSVOL, служба FRS реплицирует общую папку SYSVOL.
- **Prepared (состояние 1).** Служба FRS по-прежнему реплицирует общую папку SYSVOL, которая используется доменом, в то время как DFS-R реплицирует копию общей папки SYSVOL. Эта копия SYSVOL не применяется для обслуживания запросов от других DC.
- **Redirected (состояние 2).** Копия DFS-R общей папки SYSVOL становится ответственной за обслуживание запросов от других DC. Служба FRS продолжает реплицировать исходную папку SYSVOL, но DFS-R теперь реплицирует производственную папку SYSVOL, которую используют контроллеры домена, находящиеся в состоянии Redirected.
- **Eliminated (состояние 3).** DFS-R продолжает поддерживать всю репликацию SYSVOL. Исходная папка SYSVOL удаляется, и служба FRS больше не реплицирует данные SYSVOL.

Источник

Большая часть сведений, предлагаемых в этом разделе, взята из веб-сайта Microsoft TechNet:

`http://technet.microsoft.com/en-us/library/dd641052.aspx`

Обращайтесь на указанный веб-сайт за дополнительной информацией.

Во время миграции с помощью команды `dfsrmig` осуществляется проход по четырем устойчивым состояниям. Во время этого процесса можно наблюдать некоторые видимые изменения.

1. Процесс миграции создает копию папки SYSVOL. Служба FRS реплицирует исходную папку SYSVOL, расположенную в `c:\windows\SYSVOL`. Механизм DFS-R реплицирует копию папки SYSVOL, находящуюся в `c:\windows\SYSVOL_dfsr`.
2. Отображение общей папки SYSVOL изменяется с FRS на DFS-R. Изначально отображение общей папки SYSVOL, `c:\windows\SYSVOL`, использовалось для информации, которая активно реплицируется службой FRS. Позже в процессе миграции местоположение общей папки SYSVOL будет отображено на `c:\windows\SYSVOL_dfsr`, и данные, активно потребляемые Active Directory, будут реплицироваться DFS-R.
3. Процесс миграции удалит исходную копию папки SYSVOL.

Переходные состояния

По мере перемещения из одного устойчивого состояния в другое, каждый контроллер домена будет также проходить через последовательность переходных состоя-

ний. Существуют пять переходных состояний, пронумерованных от 4 до 9. Каждое состояние имеет название, поясняющее то, что происходит во время перехода:

- Подготовка (состояние 4)
- Ожидание начальной синхронизации (состояние 5)
- Переадресация (состояние 6)
- Устранение (состояние 7)
- Откат переадресации (состояние 8)
- Откат подготовки (состояние 9)

На рис. 7.32 иллюстрируется процесс миграции через четыре устойчивых состояния и переходные состояния, возникающие между устойчивыми состояниями.

Рис. 7.32. Состояния миграции на DFS-R

Возможно, вас интересует, как в точности DFS-R переходит между состояниями. Вспомните, что служба DFS-R на каждом DC запрашивает у Active Directory текущее глобальное состояние миграции. Если глобальное состояние отличается от локального состояния на контроллере домена, то DFS-R предпринимает шаги (переходные состояния) для достижения соответствия глобальному состоянию.

Когда вы готовы к миграции контроллеров домена в своем домене на DFS-R, все они начнут с состояния Start. Вы откроете окно командной строки и воспользуетесь инструментом `dfsrmig` для перемещения контроллеров домена и состояния Start в состояние Eliminated. Интересная особенность процесса миграции связана с тем, что по нему можно двигаться не только вперед, но также и при необходимости назад, если пока еще не завершен шаг 3, т.е. устранение. Например, после перевода DC в состояние Prepared по какой-то причине вы решили возвратиться обратно в состояние Start. Можно с помощью инструмента `dfsrmig` изменить состояние на Start. Важно помнить, что как только достигнуто состояние 3, возврат назад уже невозможен. В этой точке миграция будет завершена, а исходная папка SYSVOL удалена.

Миграция в состояние Prepared

Прежде чем действительно начинать процесс миграции, должны быть удовлетворены некоторые требования. Вспомните, что для использования DFS-R домен необходимо поднять до функционального уровня Windows Server 2008. Это значит, что на всех контроллерах домена должна быть установлена ОС Windows Server 2008, Windows Server 2008 R2 или Windows Server 2012. Если у вас имеются контроллеры

домена с Windows 2000 Server или Windows Server 2003, то вы не полностью готовы к переходу на DFS-R. Повторимся еще раз: в Windows Server 2012 служба FRS по-прежнему поддерживается, но не исключено, что она исчезнет из будущих версий Windows Server.

Верификация Active Directory

Перед поднятием функционального уровня домена до Windows Server 2008 вы должны проверить работоспособность Active Directory и удостовериться в корректной репликации существующей папки SYSVOL. Если репликация Active Directory не работает должным образом, то прежде чем пытаться выполнить миграцию, необходимо решить данную проблему. Отказ одного из контроллеров домена повлияет на остальную часть домена. У вас есть возможность исправить существующие проблемы с AD. Ниже описаны соответствующие действия.

1. В Microsoft рекомендуют применять команду `net share` для проверки того, что папка SYSVOL совместно используется всеми контроллерами домена, и что эта открытая папка отображается на папку SYSVOL, реплицируемую службой FRS. В выводе команды `net share` будут присутствовать общие имена для папок NETLOGON и SYSVOL наряду с текущими их местоположениями.
2. Вы должны удостовериться в наличии достаточного объема свободного пространства на диске, чтобы можно было создать копию структуры папки SYSVOL.
3. Используйте инструмент Ultrasound для мониторинга службы FRS и проверки ее функциональности. Этот инструмент доступен для бесплатной загрузки по ссылке `http://www.microsoft.com/en-us/download/details.aspx?id=3660`.
4. На одном из контроллеров домена откройте окно командной строки и введите `repadmin /replsum`. Эта команда позволит удостовериться в корректной работе репликации Active Directory. В выводе не должны присутствовать сообщения об ошибках. Если же они есть, устраните проблемы, прежде чем продолжить.
5. Откройте окно командной строки и введите `DCDIAG`. Эта утилита выполнит несколько проверок в системе. Вывод не должен содержать сообщения об ошибках. Если это не так, устраните проблемы, прежде чем продолжить. Чтобы запустить `DCDIAG` на удаленном сервере, введите `DCDIAG /s:DC02.bigfirm.com`. В результате утилита `DCDIAG` запустится на контроллере домена `DC02.bigfirm.com`.
6. В редакторе реестра на каждом контроллере домена перейдите в раздел `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters` и удостоверьтесь в том, что значением параметра SYSVOL является `диск:|\windows_folder\SYSVOL\SYSVOL`, а значением параметра `SYSVOLReady` — число `1`.
7. На каждом контроллере домена с помощью окна служб удостоверьтесь, что служба DFS Replication запущена, а тип ее запуска установлен в Automatic (Автоматически).

Поднятие функционального уровня домена

Теперь, когда проверено функционирование Active Directory, FRS и SYSVOL, а также корректность значений упомянутых выше параметров реестра, все готово к поднятию функционального уровня домена до Windows Server 2008. Для этого выполните следующие шаги.

1. Откройте Active Directory Administrative Center.
2. Щелкните правой кнопкой мыши на имени домена и выберите в контекстном меню пункт Raise Domain Functional Level (Поднять функциональный уровень домена).
3. В окне Domain Functional Level (Функциональный уровень домена) выберите вариант Windows Server 2008.
4. Щелкните на кнопке OK.
5. В открывшемся окне предупреждения щелкните на кнопке OK.
6. В открывшемся окне подтверждения щелкните на кнопке OK.

При каждом переходе из одного состояния в другое вы будете выполнять последовательность действий по верификации. После завершения этих действий происходит переход в следующее состояние. В данном случае вы удостоверились в корректном функционировании Active Directory и SYSVOL. Затем вы проверили параметры реестра и подняли функциональный уровень домена. Перед миграцией в состояние Prepared осталась еще одна деталь — создать резервную копию. Самое время убедиться в наличии правильной текущей резервной копии данных состояния системы. Если что-то пойдет совершенно неподходящим образом, у вас будет возможность возвратиться в эту точку. Итак, уделите несколько минут на создание и последующую проверку резервной копии состояния системы. После этого вы будете готовы к миграции в состояние Prepared.

Выполнение миграции

Процесс миграции из состояния Start в состояние Prepared является коротким. Понадобится открыть окно командной строки и ввести следующую команду (рис. 7.33):

```
dfsrmig /setglobalstate 1
```

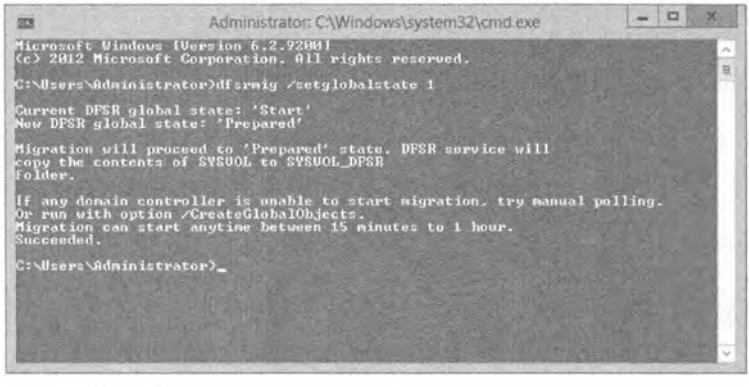


Рис. 7.33. DFS-R устанавливает глобальное состояние миграции в 1

В этот момент вы должны проверить, что глобальное состояние миграции было обновлено. Для этого снова откройте окно командной строки и введите следующую команду:

```
dfsrmig /getglobalstate
```

Эта команда возвратит текущее глобальное состояние с сообщением, указывающим на успешный переход (рис. 7.34).

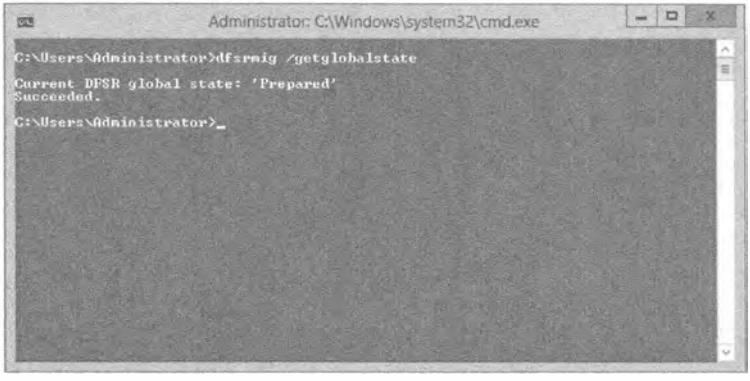


Рис. 7.34. DFS-R получает глобальное состояние

Есть еще одна, последняя команда, позволяющая проверить, что все контроллеры домена перешли в состояние Prepared:

```
dfsrmig /getmigrationstate
```

Учтите, что эта команда может требовать некоторого времени на выяснение того, что все контроллеры домена благополучно мигрировали в состояние Prepared, после чего выдаст соответствующее сообщение (рис. 7.35). Будьте терпеливы, т.к. Active Directory нужно время, чтобы провести репликацию. Теперь, когда вы довели процесс до состояния Prepared, имеет смысл проверить корректность перехода в это состояние, прежде чем переходить к следующей фазе процесса миграции. Ниже приведены очень простые шаги, которые позволят удостовериться в успешности перехода в состояние Prepared.

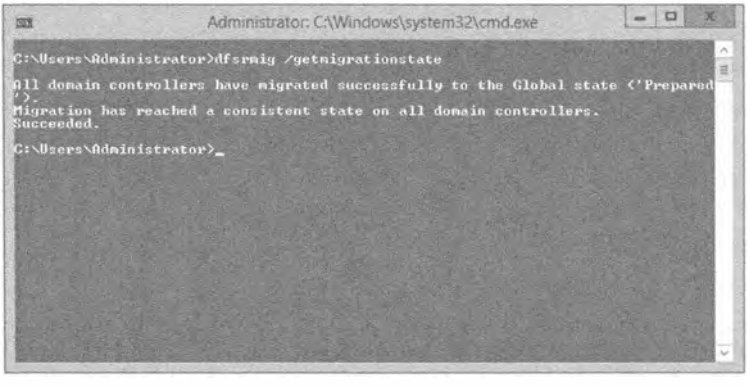


Рис. 7.35. Вывод команды `dfsrmig /getmigrationstate`

7. На каждом контроллере домена откройте окно командной строки и введите команду `net share`, чтобы проверить, используется ли папка SYSVOL совместно всеми контроллерами домена, и отображается ли эта открытая папка на папку SYSVOL, которая реплицируется службой FRS.
8. Воспользуйтесь инструментом Ultrasound для проверки того, что служба FRS остается работоспособной на исходной папке.
9. Проверьте файловую систему, создана ли папка SYSVOL_DFSR в каталоге `c:\windows\SYSVOL_dfsr`, и что в нее скопировано содержимое исходной папки SYSVOL (рис. 7.36).

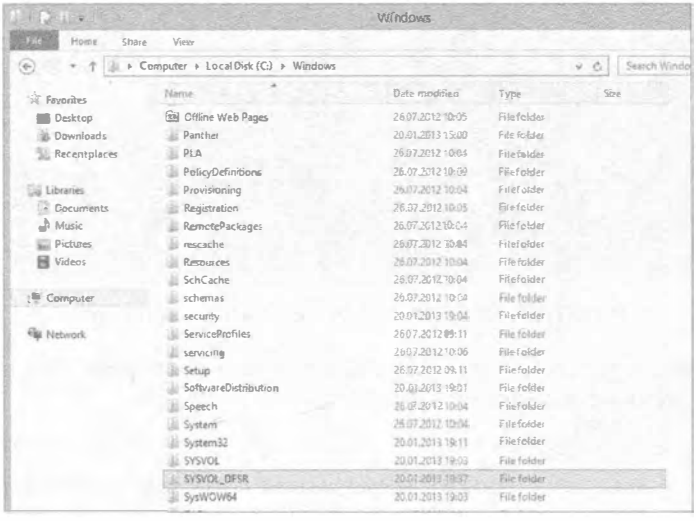


Рис. 7.36. Новая папка SYSVOL_DFSR

10. Сгенерируйте с помощью инструментов управления DFS диагностический отчет. Если инструменты управления DFS у вас еще не установлены, можете добавить его как компонент в диспетчере серверов, для чего выберите в меню пункт Manage⇨Add Roles and Features (Управление⇨Добавить роли и компоненты) и затем в открывшемся мастере отметьте флажок возле компонента DFS Management Tools (Инструменты управления DFS), последовательно развернув узлы Remote Server Administration Tools (Инструменты дистанционного администрирования серверов) и File Services Tools (Инструменты файловых служб).

Когда применяется оснастка DFS Manager (Диспетчер DFS), возможно сгенерировать два типа диагностических отчетов, которые называются Health report (Отчет о работоспособности) и Propagation report (Отчет о распространении). Для проверки на предмет наличия проблем вы должны сформировать оба эти отчета (рис. 7.37). Чтобы сгенерировать указанные отчеты, выполните следующие шаги.

1. Откройте диспетчер DFS.
2. В дереве консоли внутри узла Replication (Репликация) щелкните на элементе Domain System Volume (Системный том домена).
3. Щелкните на вкладке Membership (Членство).

4. Щелкните на Membership Status (Состояние членства).
5. Удостоверьтесь, что для локального пути `c:\windows\SYSVOL_dfsr\ваш_домен` отмечен флажок Enabled (Включен).
6. Щелкните правой кнопкой мыши на элементе Domain System Volume.
7. Щелкните на Create Diagnostic Report (Создать диагностический отчет).
8. Когда откроется мастер создания диагностического отчета (Diagnostic Report Wizard), выберите тип генерируемого отчета и следуйте дальнейшим шагам мастера.

После проверки, успешно ли контроллеры домена перешли в состояние Prepared, вы готовы переходить в состояние Redirected. В этом состоянии DFS-R возьмет на себя ответственность за репликацию папки SYSVOL для домена. Данная порция процесса миграции состоит из двух частей. Сначала вы выполните переход в состояние Redirected, а затем проверите успешность этого перехода.

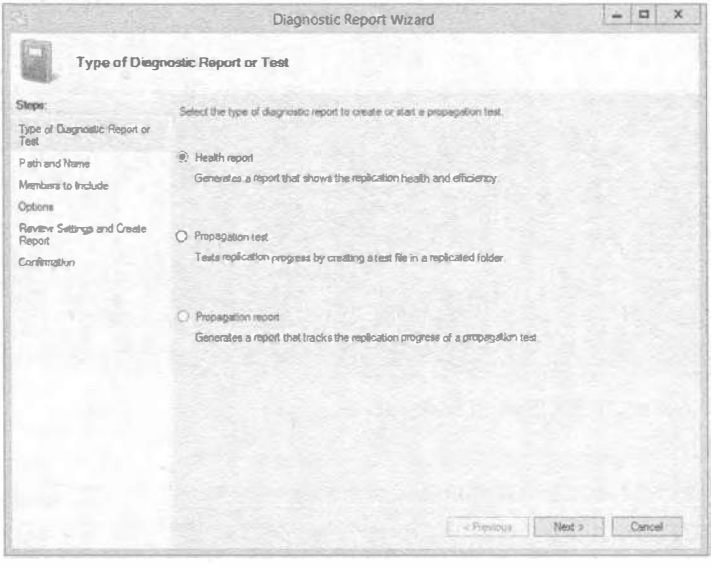


Рис. 7.37. Создание отчета с помощью диспетчера DFS

Миграция в состояние Redirected

Чтобы перевести домен в состояние Redirected, понадобится выполнить перечисленные ниже шаги.

1. В окне командной строки введите команду `dfsrmig /setglobalstate 2`.
   Вывод команды показан на рис. 7.38.
2. В окне командной строки введите команду `dfsrmig /getglobalstate`.
   Вывод команды показан на рис. 7.39.
3. Введите команду `dfsrmig /getmigrationstate`, чтобы удостовериться в том, что все контроллеры домена достигли состояния Redirected (рис. 7.40).

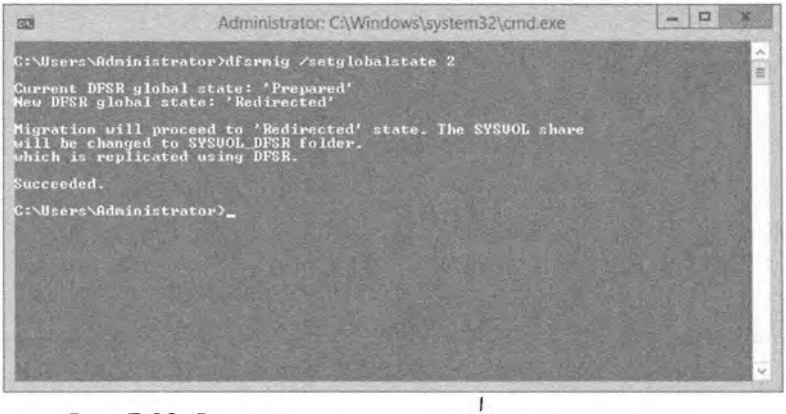


Рис. 7.38. Вывод команды `dfsrmig /setglobalstate 2`

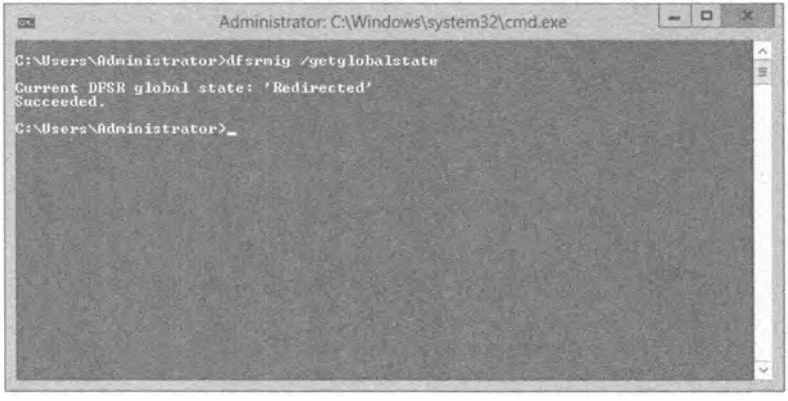


Рис. 7.39. Вывод команды `dfsrmig /getglobalstate`

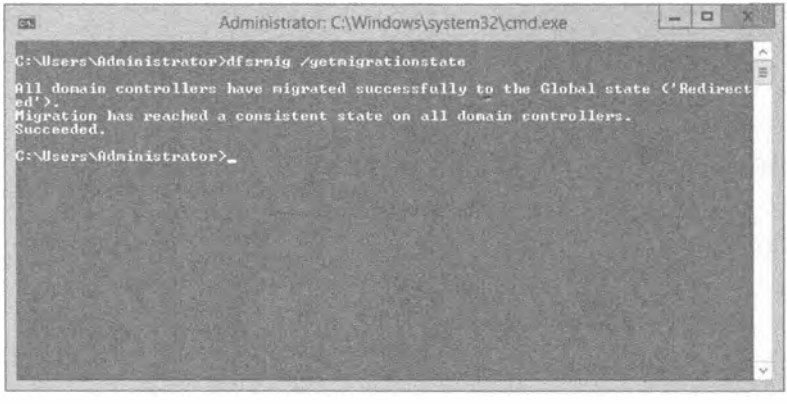


Рис. 7.40. Вывод команды `dfsrmig /getmigrationstate`

К этому моменту вы успешно завершили шаги, необходимые для миграции домена в состояние Redirected; тем не менее, перед переходом в состояние Eliminated необходимо удостовериться, что домен был успешно перемещен в состояние Redirected. Для этого выполните следующие шаги.

1. Откройте окно командной строки и введите команду `net share`.

   В выводе этой команды вы увидите новую общую папку SYSVOL_DFSR в полномочном состоянии (рис. 7.41).

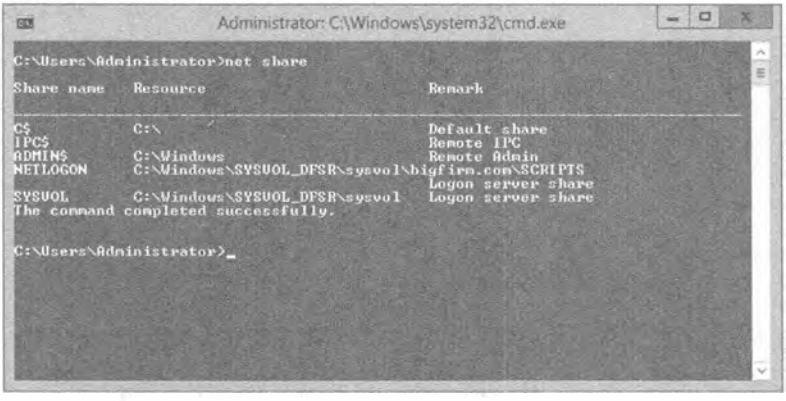


Рис. 7.41. Новое местоположение папки SYSVOL

2. Воспользуйтесь диспетчером DFS для создания еще одного диагностического отчета, как это делалось при верификации перехода в состояние Prepared.
3. С помощью инструмента Ultrasound проверьте работоспособность репликации FRS исходной папки SYSVOL.

   Вы хорошо помните, что DFS-R отвечает за репликацию новой общей папки SYSVOL в домене; тем не менее, важно проверить функционирование процесса репликации FRS, если потребуется возвратиться обратно в состояние Prepared.

Когда контроллеры домена успешно прошли миграцию в состояние Redirected, можно сделать финальное перемещение в состояние Eliminated.

Миграция в состояние Eliminated

Итак, вами пройден долгий путь. Наступило время сделать последний шаг миграции из FRS на DFS-R. К этому моменту все контроллеры домена должны функционировать в состоянии Redirected. Механизм DFS-R успешно реплицирует общие папки SYSVOL, а служба FRS сохранена со старыми общими папками SYSVOL. Теперь можно вывести из эксплуатации, или в данном случае устранить, службу FRS. Прежде чем действительно переходить в состояние Eliminated, необходимо предпринять несколько действий. Не забывайте, что после этого шага возврата назад уже не будет. Таким образом, еще раз проверьте состояние Redirected, чтобы выяснить, корректно ли работают все компоненты.

1. Введите команду `dfsrmig /getmigrationstate` и удостоверьтесь, что все контроллеры домена находятся в состоянии Redirected.

2. Введите команду `repadmin /replsum`, чтобы проверить правильность работы репликации Active Directory. Удостоверьтесь в отсутствии ошибок.
3. Сохраните состояние Active Directory на случай, если потребуется восстановление из резервной копии.

Если домен функционирует в состоянии Redirected, как ожидалось, самое время провести миграцию в состояние Eliminated. Выполните описанные ниже действия на контроллере домена.

1. Введите команду `dfsrmig /setglobalstate 3` (рис. 7.42).

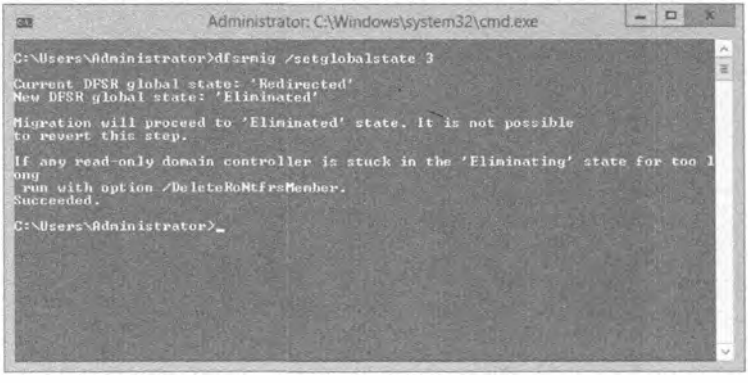


Рис. 7.42. Вывод команды `dfsrmig /setglobalstate 3`

2. Введите команду `dfsrmig /getglobalstate`, чтобы удостовериться в том, что глобальным состоянием является Eliminated (рис. 7.43).

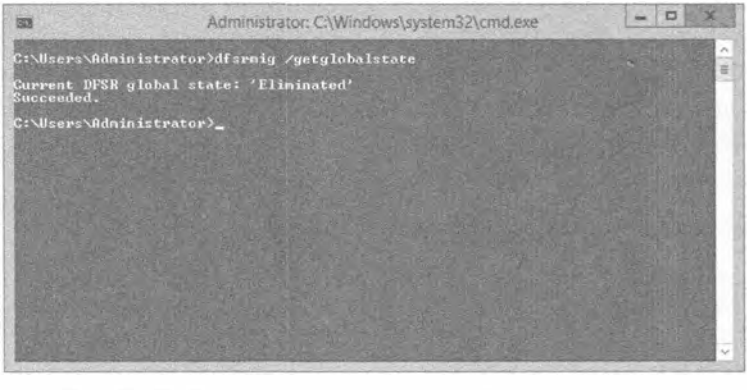


Рис. 7.43. Вывод команды `dfsrmig /getglobalstate`

3. Введите команду `dfsrmig /getmigrationstate` для проверки того, что все контроллеры домена успешно прошли миграцию (рис. 7.44).
4. На каждом контроллере домена откройте окно командной строки и введите `net share`, чтобы проверить местоположение открытой папки SYSVOL (рис. 7.45).
5. Сгенерируйте в диспетчере DFS те же самые отчеты Health report и Propagation report, которые вы создавали при проверке состояний Prepared и Redirected.

6. На каждом контроллере домена откройте окно проводника Windows и удостоверьтесь в удалении открытой папки `c:\windows\SYSVOL`.

   Вполне нормально, если некоторые папки остаются постоянными; тем не менее, вы должны проверить, что они пусты. В итоге должна остаться только новая инфраструктура SYSVOL_DFSR, как показано на рис. 7.46.

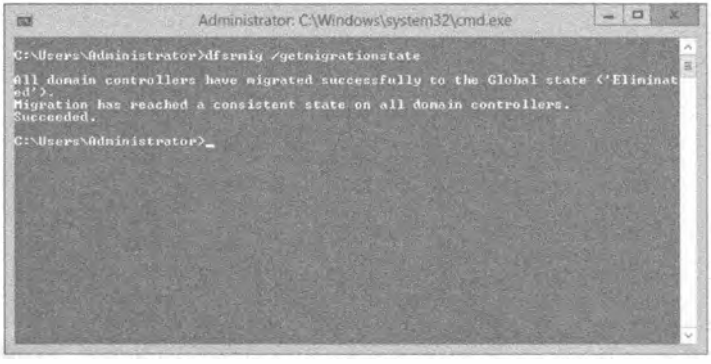


Рис. 7.44. Вывод команды `dfsrmig /getmigrationstate`

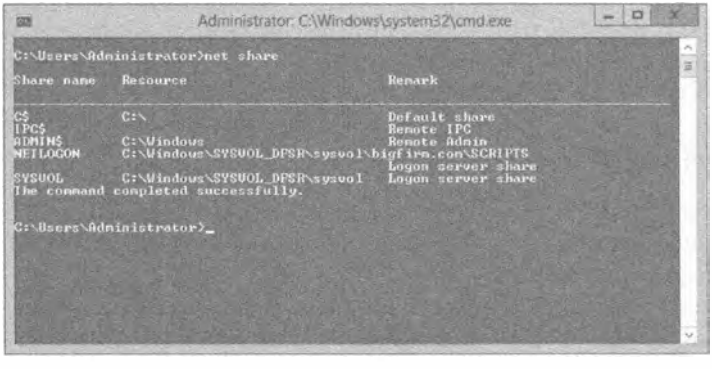


Рис. 7.45. Финальный вывод команды `net share`

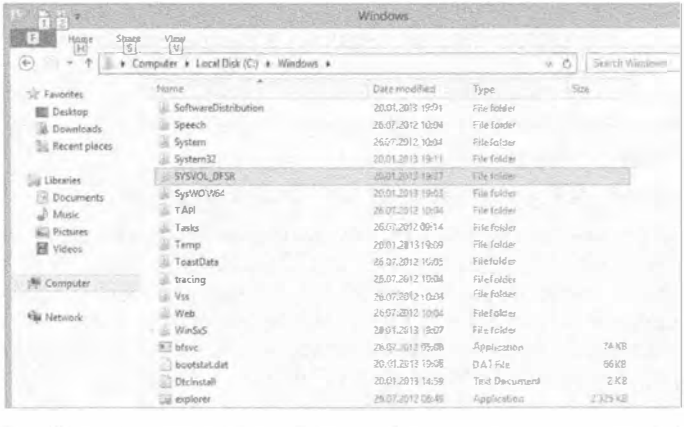


Рис. 7.46. Файловая система в состоянии Eliminated, не содержащая старой папки SYSVOL

Если вы заглянете в консоль служб Windows, то увидите, что служба File Replication Service установлена в состояние Disabled (Отключена), как иллюстрируется на рис. 7.47.

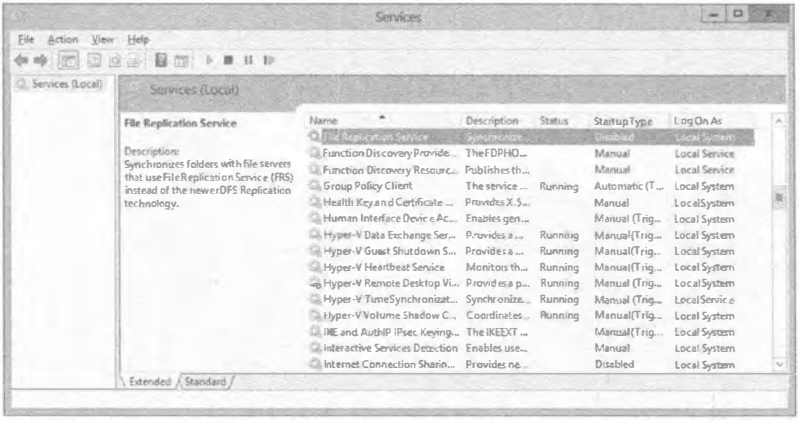


Рис. 7.47. После миграции служба FRS отключена

Благодаря выполненным действиям, вы успешно провели миграцию инфраструктуры репликации SYSVOL из FRS на DFS-R и получили все преимущества удаленного разностного сжатия. Действительно старая репликация папки SYSVOL посредством службы FRS теперь заменена новой репликацией DFS папки SYSVOL_DFSR.

Модернизация Active Directory

Стала доступной версия Active Directory Server 2012, и вы озабочены тем, чтобы обновить текущую инфраструктуру до последнего выпуска, поскольку хотите удерживать ее в актуальном состоянии.

Раньше мы предполагали, что никакой изначальной сети не существует, поэтому строили новую сеть с нуля. В большинстве ситуаций это не так. Служба Active Directory появилась более десяти лет тому назад, и многие компании располагают той или иной версией Active Directory. В этом разделе мы собираемся сосредоточить внимание на модернизации домена до Windows Server Active Directory 2012. Но прежде чем начать это приключение, необходимо понять путь следования и возможные предварительные условия.

Готовы ли ваши серверы?

Серверы Windows NT на вечеринку не приглашаются!

Нет никакой возможности обеспечить сосуществование контроллера домена Windows NT 4.0 и контроллера домена Windows Server 2012. После выхода Windows Server 2008 R2 доверительные отношения для домена NT 4.0 больше не поддерживаются, и устанавливать сервер Windows NT 4.0 Server внутри домена Windows Server 2012 нельзя. Кроме того, поддержка Windows NT 4.0 Server со стороны Microsoft давно закончилась. Следовательно, Windows NT 4.0 Server является, пожалуй, самой незащищенной системой во всем мире.

Модернизация схемы до Windows Server 2012

При планировании модернизации домена в ранних версиях Windows Server необходимо было запускать инструмент под названием `adprep.exe`. Этот инструмент подготавливает и расширяет схему леса для поддержки новых функций, а также подготавливает домен к созданию новых групп и контейнеров. С помощью дополнительной опции `/gpprep` домен можно подготовить к установке объектов групповой политики для репликации контроллера домена Windows Server, а опции `/rodcprep` — для добавления поддержки учетных записей контроллера домена только для чтения (Read-only Domain Controller — RODC).

Хорошая новость состоит в том, что в Windows Server 2012 инструмент `adprep.exe` по-прежнему существует в папке `\support\adprep` установочной копии Windows Server 2012. Однако 32-разрядной версии `adprep.exe` больше нет, есть только 64-разрядная версия, которую можно запускать под управлением 64-разрядной ОС Windows Server 2008 и выше. Запускать инструмент `adprep.exe` не обязательно на контроллере домена; его можно запустить дистанционно на сервере Windows, который является сервером-членом домена или даже сервером рабочей группы. Чтобы просмотреть все доступные опции, запустите `adprep.exe /?`.

Если нужно расширить схему из сервера с 64-разрядной ОС Windows Server 2008, введите следующую команду:

```
adprep /forestprep /forest w2k3domain.com /user administrator
  /userdomain w2k3domain.com /password P@ssw0rd
```

После успешного расширения схемы введите показанную ниже команду, чтобы расширить домен:

```
adprep /domainprep /gpprep /domain w2k3domain.com /user administrator
  /userdomain w2k3domain.com /password P@ssw0rd
```

Для расширения поддержки RODC понадобится выполнить следующую команду:

```
adprep /rodcprep /domain w2k3domain.com /user administrator
  /userdomain w2k3domain.com /password P@ssw0rd
```

Еще лучшая новость заключается в том, что вы не обязаны запускать `adprep.exe` вообще. В Windows Server 2012 имеется новый мастер конфигурирования службы домена Active Directory (ADDSCW), который применялся ранее в этой главе для повышения первого контроллера домена. Этот мастер становится доступным после установки роли Active Directory Domain Services. Мастер позаботится обо всех шагах, необходимых для успешного повышения сервера-члена Windows Server 2012 до контроллера домена. Инструмент `adprep.exe` был интегрирован в данный мастер, чтобы обеспечить максимально комфортную процедуру повышения.

Если вы собираетесь повысить сервер и предоставили всю нужную информацию, после щелчка на кнопке Install (Установить) мастер проверит среду и подготовит лес, схему и домен (рис. 7.48).

На рис. 7.49 показано окно мастера ADDSCW, модернизирующее лес через `adprep /forestprep`. Затем мастер модернизирует домен, используя `adprep.exe /domainprep` (рис. 7.50).

Но почему в Microsoft решили предоставлять инструмент `adprep.exe` и также реализовали его в мастере ADDSCW? Причина в том, что есть компании, в которых необходимо документировать каждый шаг, выполняемый над их инфраструктурой,

в системе управления службами или системе управления изменениями, т.к. это требуется принятым у них процессом управления изменениями. В этом случае запуск `adprep.exe` из командной строки дает возможность отслеживать, что в точности изменяется.

Если процесс управления изменениями отсутствует, можете использовать комфортный способ расширения леса или домена, выполняя всю работу в мастере ADDSCW.

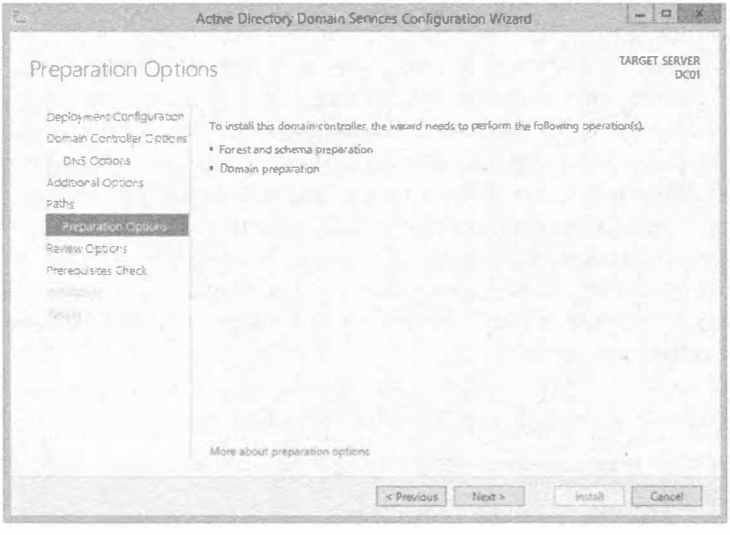


Рис. 7.48. Мастер ADDSCW подготавливает целевой домен

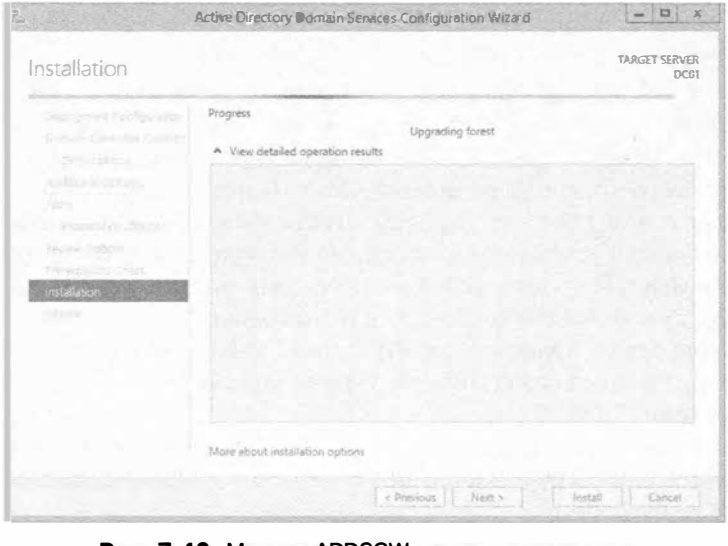


Рис. 7.49. Мастер ADDSCW подготавливает лес

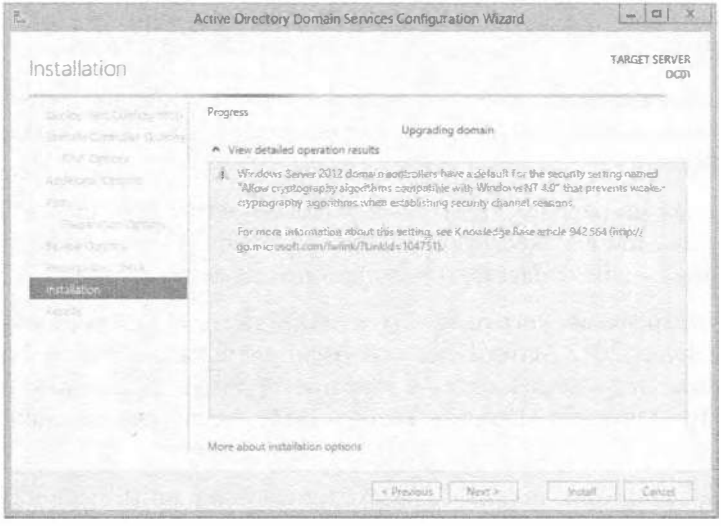


Рис. 7.50. Мастер ADDSCW подготавливает домен

Новые группы в Windows Server 2012

В Windows Server 2012 Active Directory доступны новые группы, которые создаются в течение процесса модернизации.

Следующие группы находятся в контейнере `BUILTIN` внутри ADAC или ADUC:

- Access Control Assistance Operators (Операторы поддержки управления доступом)
- Hyper-V Administrators (Администраторы Hyper-V)
- RDS Endpoint Servers (Серверы конечных точек RDS)
- RDS Management Servers (Серверы управления RDS)
- RDS Remote Access Servers (Серверы удаленного доступа RDS)
- Remote Management Users (Пользователи дистанционного управления)

Следующая группа находится в контейнере `Users` внутри ADAC или ADUC:

- Cloneable Domain Controllers (Клонируемые контроллеры домена)

Модернизация домена до Windows Server 2012

Перед тем, как начать обсуждение миграции, мы хотим дать небольшой совет, не последовать которому было бы крайне неразумно. Если вы производите миграцию, значит, у вас, вероятно, уже есть домен, функционирующий в текущий момент. Вы намерены преобразовать этот домен в работоспособный домен Windows Server 2012, интегрированный с AD. Самая сложная часть заключается в успешном прохождении из состояния "до" в состояние "после". Если вы запутаетесь на этом пути, то пользователи вряд ли будут в восторге, потому что работающий домен, хоть он и старой версии, все же лучше, чем полное отсутствие какого-либо домена, а путаница может привести к разрушению существующего домена. Итак, вот совет: даже и не думайте начинать миграцию до тех пор, пока не опробуете сам процесс в лабораторной сети. Наличие технологии виртуализации делает процесс тестирования быстрым и безболезненным.

Существуют три философских подхода к миграции на домен Windows Server 2012.

- **Модернизация на месте.** Предусматривает прохождение через процесс установки ОС Windows Server 2012 поверх имеющегося 64-разрядного контроллера домена Windows.
- **Постепенная миграция.** Сервер-член Windows Server 2012 повышается до контроллера домена в существующем домене. Такой подход также называют модернизацией Active Directory или миграцией домена.
- **Чистая изначальная миграция.** Создается "чистый как первый снег" домен Windows Server 2012 Active Directory. Пользовательские учетные записи, группы и компьютеры переносятся в этот новый домен с помощью инструментов вроде Active Directory Migration Tool (ADMT), последней версией которого является 3.2.

Все указанные подходы подробно рассматриваются в последующих разделах.

Миграция путем модернизации на месте

Модернизация на месте означает установку Windows Server 2012 на существующем контроллере домена. Процесс модернизации более или менее сводится к многократным щелчкам на кнопках Next (Далее) и в конце на кнопке Finish (Готово). Однако вы должны быть осведомлены о некоторых последствия. Все в домене останется почти тем же самым. Это означает, что пользователи, компьютеры и группы не затрагиваются, и все счастливы оттого, что немногое изменилось. Но недостаток такого подхода в том, что вместе с хорошим в новый домен перешло и все то плохое, что присутствовало в старом домене, или же приложения, установленные в системе, оказываются несовместимыми с новой ОС.

Если что-то идет не так, вы можете попасть в действительно трудную ситуацию, поскольку модернизация, по большому счету, выполняется по принципу "все или ничего". Следовательно, удостоверьтесь в наличии проверенной резервной копии. Несмотря на что в Microsoft уверяют, что ничего плохого не должно произойти, законы Мерфи никто не отменял.

Важно знать, что все роли, установленные на контроллере домена, также будут модернизированы. Это значит, что если в системе есть, например, роли DNS и DHCP, они модернизируются до версий Windows Server 2012.

Если вы решили проводить модернизацию на месте своего контроллера домена, то должны знать, какие версии Windows Server в действительности можно модернизировать.

Контроллеры домена, на которых функционируют 64-разрядные версии Windows Server 2008 или Windows Server 2008 R2, могут быть модернизированы до Windows Server 2012 (как показано в табл. 7.2). Нет никакого способа модернизировать контроллеры домена с Windows Server 2003 или 32-разрядными версиями Windows Server 2008. Чтобы заменить их, вы должны установить в домене контроллеры домена с Windows Server 2012 и затем удалить контроллеры домена с Windows Server 2003.

Прежде чем планировать модернизацию на месте, проверьте, удовлетворены ли требования к установке Windows Server 2012.

Таблица 7.2. Пути модернизации

Существующая ОС	Поддерживаемая модернизация
Windows Server 2008 Standard с пакетом обновлений SP2 или Windows Server 2008 Enterprise с пакетом обновлений SP2	Windows Server 2012 Standard или Windows Server 2012 Datacenter
Windows Server 2008 Datacenter с пакетом обновлений SP2	Windows Server 2012 Datacenter
Windows Web Server 2008	Windows Server 2012 Standard
Windows Server 2008 R2 Standard с пакетом обновлений SP1 или Windows Server 2008 R2 Enterprise с пакетом обновлений SP1	Windows Server 2012 Standard или Windows Server 2012 Datacenter
Windows Server 2008 R2 Datacenter с пакетом обновлений SP1	Windows Server 2012 Datacenter
Windows Web Server 2008	Windows Server 2012 Standard

- Удостоверьтесь, что оборудование сервера поддерживает 64-разрядные операционные системы.
- Поскольку ОС Windows Server 2012 доступна только в виде 64-разрядных версий, использовать 32-разрядное оборудование нельзя.
- Минимальные требования к оборудованию для Windows Server 2012: 64-разрядный процессор с тактовой частотой 1,4 ГГц, ОЗУ объемом 512 Мбайт, свободное пространство на диске размером 32 Гбайт и монитор с экранным разрешением 800×600. Удовлетворить эти требования в наши дни довольно легко.
- Проводить модернизацию на месте имеет смысл только на сервере, предполагаемый добавочный срок эксплуатации которого составляет три-четыре года. Также удостоверьтесь, что в течение всего этого срока вы будете получать поддержку со стороны поставщика оборудования.
- Проверьте, что все программное обеспечение, установленное на сервере, поддерживается в Windows Server 2012, особенно антивирусное ПО, драйверы оборудования и прикладные приложения. Если вы попытаетесь устранить проблемы несовместимости во время процесса модернизации, может возникнуть серьезное затруднение. Если вы не уверены, мы рекомендуем удалить антивирусное ПО перед модернизацией и установить его повторно после успешного завершения модернизации.
- Создайте резервную копию контроллера домена и состояния системы.

Путь модернизации для Windows Server 2012 R2

Важно отметить, что Windows Server 2012 R2 больше не разрешает модернизацию от Windows Server 2008 с пакетом обновлений SP2. Чтобы модернизация была возможна, потребуется иметь, по крайней мере, Windows Server 2008 R2 с пакетом обновлений SP1.

Если необходимо провести модернизацию от Windows Server 2012 Datacenter, вы можете модернизировать до Windows Server 2012 R2 Datacenter. При наличии установленной версии Windows Server 2012 Standard можно модернизировать до Windows Server 2012 R2 Standard или Windows Server R2 Datacenter.

Минимальные требования к оборудованию для установки Windows Server 2012 R2 такие же, как для Windows Server 2012.

В качестве установившейся практики мы рекомендуем создать резервную копию всего раздела C:\ и состояния системы. Также настоятельно рекомендуем создавать резервные копии с помощью двух разных инструментов резервного копирования. В первую копию поместите раздел C:\ и состояние системы с применением инструмента резервного копирования, принятого в компании. В вторую копию поместите раздел C:\ и состояние системы с использованием внутреннего инструмента резервного копирования Windows. Причина создания двух копий связана с тем, что в случае возникновения проблем в Microsoft принимают при предоставлении поддержки только резервные копии, созданные с помощью собственной утилиты.

На этой стадии вы убедились, что система готова для модернизации и имеются достоверные резервные копии. Следующие шаги направлены на выяснение того, что на контроллере домена отсутствуют ошибки или проблемы с репликацией.

Для проверки, находится ли контроллер домена в работоспособном состоянии, запустите утилиту `repadmin`, которая протестирует репликацию:

```
repadmin /replsum /bysrc /bydest /sort:delta
```

Эта команда выдаст перечень ошибок репликации в домене, отсортированный по источнику, цели и наибольшей разницы репликации. Если в выводе сообщается о каких-либо ошибках, постарайтесь исправить проблемы заблаговременно.

AD Replication Status Tool

В 2012 году Microsoft был выпущен инструмент для анализа состояния репликации Active Directory (AD Replication Status Tool), представляющий собой небольшое средство с графическим пользовательским интерфейсом, которое можно устанавливать в среде клиентской или серверной ОС Windows. Этот инструмент позволяет анализировать состояние репликации для контроллера домена в домене или лесе. Он отображает любые ошибки и позволяет экспортировать результаты в файл CSV или XPS для дальнейшего анализа. Он доступен для загрузки по ссылке `http://www.microsoft.com/en-us/download/details.aspx?id=30005`.

На контроллере домена запустите команду `DCDIAG` и удостоверьтесь в прохождении всех тестов. На контроллере домена Windows Server 2003 утилиту `DCDIAG` понадобится устанавливать отдельно. Исходный файл `suptools.msi` находится в папке `\support\tools` установочной копии.

Если все тесты проходят, откройте программу просмотра событий Windows (Event Viewer) на контроллере домена, просмотрите журналы событий на предмет наличия любых ошибок или предупреждений и попробуйте устранить проблемы. Ниже описано, как проводить модернизацию на месте AD версии Windows Server 2008.

1. Подготовьте схему леса, чтобы она была совместимой с Windows Server 2012.
2. Подготовьте домен для Windows Server 2012.
3. Запустите программу установки, чтобы модернизировать контроллер домена.

Подготовка леса/схемы и домена

Во время модернизации на месте не все контроллеры домена должны быть на уровне Windows Server 2008. Тем не менее, в этой системе должны быть размещены некоторые роли FSMO. Хозяином именования доменов леса, которым по умолчанию

является первый контроллер домена в лесе, должен быть сервер Windows Server 2008. Также сервером Windows Server 2008 должен быть эмулятор PDC каждого домена внутри леса. По умолчанию им является первый контроллер домена в каждом домене. Процесс модернизации рекомендуется начинать на контроллере домена, который не содержит ни одной роли FSMO. Если контроллер домена, подлежащий модернизации, в настоящий момент содержит какую-то роль FSMO, ее можно передать и затем, после успешной модернизации, возвратить обратно на новый контроллер домена Windows Server 2012. Вдобавок на всех контроллерах домена должна функционировать ОС Windows Server 2003 или последующей версии. Кроме того, функциональным уровнем домена должен быть Windows Server 2003 Native или лучше.

Перед тем как модернизировать даже один домен в лесе Windows Server 2003/2008 до Windows Server 2012, вам потребуется изменить всю схему леса на Windows Server 2012. Вы будете делать это на контроллере домена с ролью FSMO хозяина операций схемы леса. Вставьте диск Windows Server 2012 Setup DVD в привод компьютера, откройте окно командной строки и перейдите в папку `\support\adprep` на этом диске. Таким образом, например, если DVD-привод имеет букву диска D, вы должны открыть окно командной строки, ввести `D:` и нажать <Enter>, после чего ввести `cd \support\adprep` и нажать <Enter> еще раз. Утилита `adprep.exe` доступна только в виде 64-разрядной версии, но не 32-разрядной.

1. Запустите `adprep` на сервере с ролью хозяина схемы, введя

   ```
   adprep /forestprep
   ```

   и нажав <Enter>.

   Отобразится предупреждение о проверке того, что на всех серверах функционирует Windows Server 2003 или выше.

2. Подтвердите, введя `C` и нажав <Enter>.
3. Далее на сервере с ролью хозяина инфраструктуры в подготавливаемом домене введите `adprep /domainprep /gpprep` и нажмите <Enter>.
4. Наконец, запустите `adprep /rodcprep` на сервере с ролью хозяина инфраструктуры.

На шаге 1 при расширении схемы леса вы могли заметить во время выполнения команды, что в командной строке запускается много связанных друг с другом команд. На этом шаге импортируются все необходимые изменения схемы. Если у вас ранее было установлено приложение Exchange, Lync или какое-то другое, требующее расширения схемы, шаг 1 не повлияет на эти изменения.

На шаге 4 производится подготовка домена для Windows Server 2012, а также изменение разрешения для объектов GPO с целью репликации посредством Windows Server 2012. На этом последнем шаге появляется возможность добавить контроллер домена только для чтения (Read-only Domain Controller). Сейчас имеет смысл запустить `adprep /rodcprep`, поскольку позже в производственной среде это может потребовать больших усилий. Итак, перед тем, как домен AD на основе Windows Server 2008 можно будет модернизировать до домена AD на базе Windows Server 2012, вы должны выполнить перечисленные ниже действия.

1. Примените пакет обновлений Service Pack 2 ко всем контроллерам домена Windows Server 2008 и пакет обновлений Service Pack 1 ко всем контроллерам домена Windows Server 2008 R2, чтобы удовлетворить требования к модернизации.

2. Модернизируйте лес, выполнив команду `adprep /forestprep` на компьютере с ролью FSMO хозяина схемы для леса, даже если он не находится в домене, который вы собираетесь модернизировать.
3. Модернизируйте структуру домена, выполнив команду `adprep /domainprep /gpprep` на компьютере с ролью FSMO хозяина инфраструктуры для домена, который вы собираетесь модернизировать.
4. Дополнительно выполните команду `run /rodcprep`, чтобы подготовить контроллеры домена только для чтения.

Запуск программы установки

Теперь вы готовы запустить программу установки. Вставьте установочный DVD-диск, дважды щелкните на его значке в окне My Computer (Мой компьютер), если автозапуск не произошел, и выберите опцию Upgrade (Модернизация). Когда будет предложено получить последние обновления, выберите этот вариант. Мастер будет предупреждать, если что-то изменяется во время модернизации. Он также проверит, подготовлены ли должным образом лес и домен. До запуска собственно процесса установки откроется диалоговое окно, в котором отображаются обнаруженные проблемы с совместимостью приложений и драйверов. Если вы принимаете результаты, программа установки продолжит свою работу безо всякого вмешательства, по завершении которой вы сможете войти в модернизированную систему контроллера домена с Windows Server 2012.

Модернизация на месте: доводы за и против

Подводя итоги, ниже перечислены доводы в пользу проведения модернизации на месте.

- Она не требует новых компьютеров.
- У пользователей сохраняются старые идентификаторы защиты (security identifier — SID), а у домена — старые доверительные отношения, так что любые серверы в других доменах (к примеру, в доменах ресурсов, содержащих файловые серверы, серверы печати или почтовые серверы) будут по-прежнему без проблем опознавать пользователей.
- У пользователей сохраняются их старые пароли.
- Это простая и быстрая модернизация.
- При переходе с Windows Server 2008 AD на Windows Server 2012 AD модернизация проводится без особых проблем.

Тем не менее, во многих случаях мы не рекомендуем делать модернизацию на месте по указанным далее причинам.

- Путь модернизации очень ограничен. ОС Windows Server 2012 является 64-разрядной. Многие организации все еще имеют 32-разрядные контроллеры домена, поэтому модернизация для них невозможна.
- Модернизация производится по принципу "все или ничего". Вы модернизируете все учетные записи, причем в одном направлении — откат AD невозможен. (Тем не менее, можно восстановить данные состояния системы из резервной копии.) Мы предпочитаем более детализированные подходы.
- Любой существовавший ранее мусор остается в базе данных Active Directory.

Постепенная миграция

Последовательные и плавные шаги в направлении домена Windows Server 2012 называются постепенной миграцией. Она также широко известна как миграция Active Directory. По существу вы добавляете в домен сервер-член Windows Server 2012 и затем повышаете этот сервер до контроллера домена. После репликации данных Active Directory вы получите первый контроллер домена Windows Server 2012. При таком сценарии все остается без изменений, лишь добавляются дополнительные серверы. Недостаток этой процедуры в том, что в случае установки физического сервера необходимо дополнительное оборудование, а при виртуализации потребуется иметь больше памяти и ресурсов ЦП. Это не означает, что количество контроллеров домена увеличится, т.к. вы можете понизить старые контроллеры домена. Если вы не желаете тратить деньги и ресурсы, можете установить запасной сервер в качестве контроллера домена Windows Server 2012 и понизить старый контроллер домена, а затем после успешного понижения повторно развернуть сервер с Windows Server 2012.

Миграция такого вида является очень безопасным способом модернизации домена; вы не находитесь в ситуации "все или ничего". Хотя вам понадобится расширить схему леса, этот шаг не будет критически сложным.

Повторное развертывание контроллера домена может быть отдельным проектом. В зависимости от того, какой контроллер домена вы собираетесь заменить, вы должны тщательно планировать каждый шаг. Могут существовать зависимые службы, такие как DNS, DHCP, роли FSMO, приложения, запрашивающие этот контроллер домена, или открытые файловые ресурсы, которые зависят от данного контроллера домена. Следовательно, потребуется уделить время на проведение внимательных исследований имеющейся среды.

Подготовка к повышению сервера-члена

Перед тем как повышать сервер-член Windows Server 2012 до контроллера домена, удостоверьтесь в том, что домен имеет функциональный уровень леса не ниже Windows Server 2003. Если вы попытаетесь повысить сервер Windows Server 2012 до контроллера домена в домене с функциональным уровнем леса Windows 2000 Server, то получите ошибку.

Выполнение постепенной миграции

Постепенная миграция предусматривает выполнение следующих базовых шагов.

1. Проверьте домен на предмет наличия ошибок.
2. Добавьте на сервер-член роль Active Directory Domain Services.
3. Запустите мастер ADDSCW с разрешениями Schema Admin (Администратор схемы), Enterprise Admin (Администратор предприятия) и Domain Admin (Администратор домена). Мастер ADDSCW автоматически запустит на сервере хозяина инфраструктуры команды `adprep /forestprep` и `adprep /domainprep`.
4. Выполните действия, проводимые после миграции, такие как размещение ролей FSMO, изменение IP-адреса и другие изменения.
5. При необходимости повторно разверните исходный контроллер домена.

Подготовка леса/схемы и домена

Как и в случае модернизации на месте, существующий лес и целевой домен необходимо подготовить к изменениям Windows Server 2012 Active Directory. Для этого потребуется запустить утилиты `ForestPrep`, `DomainPrep` и `GPprep`, как было описано в разделе "Миграция путем модернизации на месте" ранее в главе.

Другой способ расширения схемы и домена предполагает запуск мастера ADDSCW. Как упоминалось ранее, инструмент `adprep.exe` интегрирован в этот мастер, и он позаботится обо всех нужных шагах. Какой бы способ ни был выбран, процедуры отката в этот момент процесса такие же, как при модернизации на месте: восстановление данных состояния системы на контроллере домена хозяина схемы.

Построение сервера-члена Windows Server 2012

Целевой контроллер домена начинается как сервер-член Windows Server 2012 в исходном домене. Во время подготовки до запуска мастера ADDSCW должны быть установлены роли Active Directory Domain Services и DNS.

Верификация DNS

Поскольку новый контроллер домена будет поддерживать DNS, он должен быть добавлен в качестве сервера имен в подходящие зоны прямого и обратного просмотра. После того как сервер-член будет повышен, зоны DNS начнут реплицироваться.

Чтобы удостовериться в корректном преобразовании имен контроллерами домена, потребуется верифицировать DNS. Проведите проверки записей SRV с использованием утилит `NsLookup` и `DcDiag`, описанных ранее в этой главе.

Подготовка исходного контроллера домена

До выполнения этой операции вы должны решить, что конкретно будет делаться на исходном контроллере домена. Если сервер остается в домене как контроллер домена, объем работы небольшой. Если же он будет развернут повторно, потребуется обдумать, каким образом обеспечить на нем подключаемость к сети.

На исходном сервере должны быть собраны перечисленные ниже данные, чтобы применить похожие настройки к целевому серверу-члену после повышения до контроллера домена.

- Имя сервера.
- IP-адрес сервера (IPv4 и IPv6).
- Назначенный сайт Active Directory.
- Назначенная организационная единица.
- Примененные объекты GPO и результирующий набор политики (RSOP). Чтобы поместить эти данные в текстовый файл, воспользуйтесь следующей командой:

  ```
  gpresult /scope computer > GPOResult.txt
  ```

- Назначенные роли FSMO. Они должны быть переданы, если сервер планируется вывести из эксплуатации.

- Роль глобального каталога.
- Дополнительные службы, такие как DHCP, общий доступ к файлам и принтерам, а также службы аутентификации Интернета (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 с целью их переноса за пределы Active Directory Domain Services.

Повышение сервера-члена

Мастер ADDSCW выполняет основные работы. В качестве конфигурации развертывания должен быть выбран переключатель Add a domain controller to an existing domain (Добавить контроллер домена в существующий домен). Кроме того, понадобится отметить флажки для ролей DNS и Global Catalog.

После того как мастер завершит работу, необходимо перезагрузить систему и сконфигурировать службу DNS на целевом контроллере домена. Несмотря на то что зоны DNS, интегрированные с Active Directory, были реплицированы на контроллера домена, служба DNS может их не видеть.

1. Выполните перечисление зон DNS и разделов приложений на исходном сервере:

   ```
   dnscmd /enumzones
   dnscmd /enumdirectorypartitions
   ```

2. Выполните перечисление зон DNS и разделов приложений на целевом сервере с использованием приведенных выше команд.
3. Сравните результаты, полученные на двух серверах. Если зоны в списках отсутствуют, с помощью команды `dnscmd /enlistdirectorypartitions` можно заставить новый DNS-сервер открыть свои разделы для совместного использования. Зоны должны присутствовать в списках сразу после того, как контроллер домена появится в списке как сервер имен для этих зон.

   ```
   dnscmd /EnlistDirectoryPartition <Имя FQDN раздела>
   ```

4. Просмотрите настройки DNS-сервера и сконфигурируйте их согласно стандарту, принятому в вашей компании.

Процедуры, выполняемые после миграции

Вы должны проверить службы домена. Можно прогнать тесты, основанные на инструментах, и с помощью программы просмотра событий, `DcDiag` и `NetDiag` просмотреть, имеются ли изначальные проблемы. Вы также должны провести тесты на приемлемость для пользователя, такие как вход в систему и доступ к сетевым ресурсам с новым контроллером домена в качестве доступной службы аутентификации.

Учитывая планы для процесса миграции, вы должны выполнить следующие действия.

- Передачу ролей FSMO и назначение GC.
- Повторное назначение IP-адреса.

- Повторное назначение сетевого имени. Контроллер домена может быть переименован в окне System (Система), или `sysdm.cpl`, панели управления либо посредством команды `netdom renamecomputer`.
- Для DNS может потребоваться повторное назначение стандартных основных зон.

Полезно знать...

После добавления контроллера домена Windows Server 2012 в существующий домен вы должны передать роли FSMO самому новому контроллеру домена.

Переналадка оборудования

Постепенная миграция предоставляет возможность повторно развернуть существующий контроллер домена как контроллер домена Windows Server 2012, хотя для него может быть не доступен корректный путь модернизации. Например, имеющийся контроллер домена способен выполнять и 64-, и 32-разрядные версии Windows Server. Как вы должны помнить, Windows Server 2012 поступает только в 64-разрядном виде, поэтому модернизация исходного сервера окажется невозможной.

Эта процедура требует доступной виртуальной машины или оборудования, поддерживающего Windows Server 2012. Такая запасная машина обеспечивает промежуточную фазу между двумя состояниями Active Directory. Выполните перечисленные ниже шаги.

1. Подготовьте лес/схему и домен.
2. Постройте на запасной машине сервер-член Windows Server 2012.
3. Удостоверьтесь, что DNS адекватно поддерживает Active Directory.
4. Подготовьте исходный сервер.
5. Повысьте запасной сервер-член.

   Подобно процедурам, выполняемым после миграции, вы должны проверить, что внутри сети все работает, а пользователи имеют доступ к ресурсам.
6. Запустите `DCPromo`, чтобы удалить Active Directory из исходного контроллера домена. После этого он станет сервером-членом в домене.
7. Постройте на исходной машине сервер-член Windows Server 2012.

   Можно использовать то же самое имя и IP-адрес, что и на исходном сервере, при условии удаления учетной записи компьютера из Active Directory.
8. Повысьте сервер-член до контроллера домена.
9. Проведите процедуры, выполняемые после миграции, в том числе пересмотр размещения ролей FSMO.

   Запасной контроллер домена может иметь роли FSMO, назначенные ему из-за вывода из эксплуатации исходного контроллера домена.
10. После проверки домена и служб контроллера домена запасной сервер можно вывести из эксплуатации, удалив роль Active Directory Domain Services или запустив командлет PowerShell под названием `Uninstall-ADDSDomainController`.

Постепенная миграция: доводы за и против

Подводя итоги, ниже перечислены доводы в пользу проведения постепенной миграции.

- Постепенная миграция последовательна в реализации. После ввода в строй контроллера домена Windows Server 2012 оставшиеся контроллеры домена при необходимости можно модернизировать или заменить.
- У пользователей сохраняются старые идентификаторы SID, а у домена — старые доверительные отношения, так что любые серверы в других доменах (к примеру, в доменах ресурсов, содержащих файловые серверы, серверы печати или почтовые серверы) будут по-прежнему без проблем опознавать пользователей.
- У пользователей сохраняются их старые пароли.
- Постепенная миграция предлагает возможность повторного развертывания Windows Server 2012 на исходном сервере.

С этим подходом связаны также и недостатки.

- Для обеспечения гладких результатов требуется больший объем подготовки и планирования.
- Любой существовавший ранее мусор остается в базе данных Active Directory.

Чистая изначальная миграция

Подход с чистой изначальной миграцией существующие домены оставляются без изменений, и создается новый пустой домен AD. Затем можно воспользоваться инструментом миграции для копирования учетных записей пользователей и компьютеров из старого домена (или доменов) в новый домен AD.

Преимущество этого метода в том, что он является постепенным. Миграция может охватывать период времени, когда еще возможно тестирование и решение проблем. На протяжении этого периода пользователям по-прежнему будет нужен доступ к своим данным. Доступ может поддерживаться путем повторного назначения разрешений или зависимости от возможности хронологии SID.

Чистая изначальная миграция является постепенной

Подход с чистой изначальной миграцией необходим в особых случаях. Прежде всего, она последовательна, когда требуется реструктуризация леса. Модернизация на месте является односторонней. Если позже выяснится, что Active Directory версии Windows Server 2012 не подходит, придется все восстанавливать с нуля. Но если есть новый домен, то в него можно скопировать какое-то подмножество пользователей, сообщив им о необходимости входа в этот новый домен. Если спустя неделю или две обнаружится, что данная версия AD является неприемлемой, учетные записи пользователей всегда можно вернуть обратно в старый домен.

Хотя постепенная миграция также последовательна, после ее проведения существовавший ранее мусор остается, приводя к ухудшению производительности и проблемам. В какой-то момент плохо информированные администраторы могут сконфигурировать Active Directory способом, который нарушает рекомендации, приводимые в этой книге. И такие изменения останутся в домене после его миграции на последующую версию.

Чистая изначальная миграция также предоставляет промежуточную фазу, отсутствующую в двух других подходах. В течение этой фазы у вас имеется возможность протестировать процесс, выясняя, могут ли пользователи обращаться к своим ресурсам, а также вскрывая общие проблемы, которые могут возникать при более позднем продвижении процесса миграции в производственной среде. Это уменьшает сложности, присущие односторонней модернизации на месте.

Миграция внутри леса

Имейте в виду, что те же самые процессы применимы также к миграции внутри леса. Как вам известно, лес — это группа доменов, связанных друг с другом.

Пользователи, компьютеры и группы может понадобиться перенести на другой домен внутри леса. Миграция таких объектов из одного домена в другой в лесе осуществляется с помощью описанных выше процедур. Основное отличие в том, что объекты, подобные пользователям и группам, должны перемещаться, а не копироваться. После создания целевой учетной записи пользователя его исходная учетная запись удаляется. В случае отката учетные записи возвращаются обратно в исходный домен с использованием инструмента ADMT. Новые учетные записи компьютеров создаются в новом домене, но старые учетные записи не удаляются, а отключаются в целях возможного отката.

Существуют две комбинации объектов, которые необходимо мигрировать вместе. Они называются замкнутыми множествами.

- **Пользователи и глобальные группы.** Глобальные группы разрешают быть своими членами пользователям и другим глобальным группам только из одного и того же домена. Когда пользователь изменяет домен, он не может быть членом глобальной группы, в которой он находился первоначально. При перемещении глобальной группы члены из исходного домена также удаляются. Они должны мигрировать вместе, чтобы поддерживать доступ в пределах ограничений, устанавливаемых правилами членства в глобальных группах.
- **Компьютеры ресурсов и локальные группы домена.** Ресурсы не могут назначать разрешения локальным группам домена из других доменов. Если компьютер перемещен без назначенных локальных групп домена, он не сможет "увидеть" идентификатор SID группы в маркере безопасности пользователя, чтобы предоставить ему доступ. В качестве альтернативы вы можете изменить область действия локальной группы домена на универсальную, но это повлияет на размер глобального каталога.

Обработка разрешений в новом домене

Предположим, что вы избрали путь чистой изначальной миграции. Поскольку в нем предусмотрена промежуточная фаза, можно ожидать, что пользователи организации будут членами старого домена или созданного нового домена. Это требует, чтобы пользователи в новом домене имели возможность доступа к файлам и другим ресурсам в старом домене. Разнесенная по двум доменам организация будет сильно зависеть от доверительных отношений между контроллерами доменов до тех пор, пока все серверы, содержащие ресурсы, не окажутся на той же самой стороне, что и пользователи.

Как сохранить пользователям из нового домена доступ к тем же ресурсам, который они имели в старом домене? Непрерывность бизнеса — это важный управ-

ленческий аспект; пользователям необходимо гарантировать возможность доступа к своим данным. Плавная миграция минимизирует перебои с доступом.

Существуют два подхода к поддержанию доступа к ресурсам: списки ACL и хронологии SID. Аббревиатура ACL расшифровывается как "access control list" (список управления доступом) — технический термин для обозначения вкладки Security (Безопасность) диалогового окна свойств ресурса, подобного открытой папке. Аббревиатура SID означает "security identifier" (идентификатор безопасности), который представляет собой уникальный номер, назначаемый учетным записям с целью их опознавания в рамках структуры разрешений. Если вы не моргнете после открытия вкладки Security диалогового окна свойств файла, то можете заметить SID, присутствующий в ACL, прежде чем компьютер преобразует этот SID в дружественное отображаемое имя.

Пример из практики

Случайное скопление и разный хлам

Группа венчурного капитала приобрела две частные IT-фирмы. Руководство вновь сформированной корпорации захотело слить леса Active Directory двух фирм в один, чтобы получить единую систему сообщений на базе Exchange и сократить издержки.

Казалось, что сетевая среда одной фирмы удерживалась в относительно целостном состоянии только за счет постоянного "склеивания". Неожиданные простои системы были общим явлением, а производительность снижалась по прошествии всего нескольких дней работы после очередной перезагрузки.

Вы могли подумать, что IT-фирма могла бы воспользоваться собственным опытом по управлению своей средой. Действительно, они владели технологией доставки высококачественных служб. Однако располагали ли они временем и деньгами, чтобы заняться своей средой? К сожалению, нет.

Как объяснил один сотрудник, среда была результатом случайного скопления. 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. (Пароль администратора был утерян.) Таким образом, модернизация на месте или постепенная миграция потенциально могли бы привести к уничтожению туннеля в сеть для удаленных пользователей. Чистая изначальная миграция стала необходимостью.

Списки ACL на сервере

Один из подходов вполне очевиден (и довольно утомителен): нужно просто пройтись по всем старым серверам и добавить новую учетную запись для пользователя `Joe` в списки разрешений на этих серверах. Такая работа может доставить действительно много хлопот, но некоторые инструменты миграции помогают ее автоматизировать.

Не принимая во внимание общее "удовольствие" от этого процесса, особенно когда его нужно делать для более сотни общих ресурсов и свыше ста групп или

пользователей, весьма высока вероятность допустить ошибку. Возможное нечаянное удаление разрешений на доступ для одной группы, добавление разрешений на доступ для не той группы или упущение из виду разрешений на доступ для требуемой группы гарантированно обеспечит насыщенное приключение всем участникам!

Использование хронологий SID

Вы знаете, что каждый пользователь имеет идентификатор SID. Это было верно со времен NT 3.1. Но на функциональных уровнях домена Windows 2000 Native и Windows Server 2003 среда Active Directory позволяет пользователям поддерживать более одного SID. Поскольку инструменты миграции создают новые учетные записи AD, эти учетные записи, конечно же, получают новые SID. Но инструменты миграции могут также дополнять старые SID пользователя новой учетной записью пользователя, эксплуатируя функцию, которая называется хронологией SID. Затем, когда пользователь пытается получить доступ к ресурсам, к которым он имел доступ под своей старой учетной записью, его рабочая станция войти на ресурсы с применением новой учетной записи Active Directory.

Как и со всеми попытками входа в домен, AD строит для пользователя маркер, который содержит идентификатор SID пользователя и идентификаторы SID любых глобальных и универсальных групп, к которым пользователь принадлежит. Вот как выглядит трюк с использованием хронологии SID. Среда AD говорит: "Он является членом группы с данным идентификатором SID", после чего отправляет параллельно старый SID пользователя из старого домена. Несмотря на то что это идентификатор SID учетной записи пользователя, контроллер домена AD передает его так, как если бы он был SID глобальной группы, и, несомненно, это приятно. 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 'Joe из старого домена'. Я имею ACL для этой 'группы', так что я догадываюсь, кто он такой". Таким образом, хотя пользователь `Joe` 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" для доступа к ресурсу.

Что необходимо для созданий хронологий SID

Ниже приведены важные замечания о хронологиях 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 во время копирования учетных записей пользователей из старого домена в новый домен с функциональным уровнем Windows Server 2003/2008/2012. (Вспомните, что Windows Server 2012 может существовать с этими функциональными уровнями.) 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.
- 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.

Вы можете держать хронологии SID продолжительное время, но на самом деле хронологии SID являются просто временными мерами, поскольку старые идентификаторы SID нужны лишь на период существования старых доменов. Вероятно, это продлится недолго. После вывода всех серверов и рабочих станций из старого домена старые идентификаторы SID не потеряют свою ценность. Таким образом, было бы удобно иметь возможность устранить эти старые хронологии SID из учетных записей пользователей. Вы можете сделать это с помощью короткого сценария VBScript, описанного в статье 295758 базы знаний Microsoft по адресу `http://support.microsoft.com/kb/295758`.

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 первой версии и также добавляет ряд удобных возможностей.

Пример проведения миграции

Чтобы провести базовую демонстрацию применения миграции, мы рассмотрим следующий пример: фирма Bigfirm приобрела компанию OtherDomain. Компания OtherDomain имеет домен Windows Server 2003 Active Directory. Фирма Bigfirm построила чистый изначальный домен Windows Server 2012 по имени `Bigfirm.com` для консолидации своих доменов в один. В Microsoft не выпустили новой версии ADMT для Windows Server 2012; таким образом, для совместимости в Bigfirm также имеется контроллер домена Windows Server 2008 R2, установленный только для нацеливания на ADMT. После миграции этот контроллер домена будет выведен из эксплуатации в OtherDomain. Функциональный уровень леса установлен в Windows Server 2008 R2. Инструмент ADMT будет также установлен на сервере-члене Windows Server 2008 R2 по имени `ADMT01`.

Необходимо провести миграцию административного отдела из домена Windows Server 2003 в OtherDomain. В административном отделе открыт общий доступ к рабочей станции (работы у них было немного), а папки пользователей расположены на контроллере домена с именем DC2003.

Во время миграции членам отдела понадобится иметь доступ к своим домашним папкам и входить на их рабочую станцию для выполнения своей работы, пока они не переместятся в новый домен.

Чистая изначальная миграция: доводы за и против

Подводя итоги, ниже перечислены доводы в пользу проведения постепенной миграции.

- Она позволяет делать постепенную модернизацию.
- Чистая изначальная миграция копирует учетные записи пользователей, а не перемещает их. Старые учетные записи остаются на случай, если что-то пойдет не так.
- Она позволяет создавать контроллеры домена из чистой установки, избегая излишней сложности и потенциальных ошибок, которые присущи модернизации на месте.
- Чистая изначальная миграция позволяет консолидировать домены, сводя множество доменов в один или небольшое их число.

Хотя было указано, что чистая изначальная миграция обладает преимуществом обратимости, тем самым помогая управлять рисками, достается это не бесплатно.

- Вам понадобится иметь больше машин, чем при простой модернизации. В новом домене потребуются 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 малого масштаба, 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. вы не вывели из эксплуатации старые домены, когда проводили чистую изначальную миграцию).
- 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 перемещение локальных профилей и т.д.

Несовместимость версий

На момент написания этих строк последней версией инструмента была ADMT 3.2. Тем не менее, она совместима только с Windows Server 2008 R2. При попытке установки Active Directory Migration Tool (ADMT) 3.2 на сервере Windows Server 2012 вы получите следующее сообщение об ошибке: "The Active Directory Migration Tool v3.1 must be installed on Windows Server 2008" ("Инструмент Active Directory Migration Tool v3.1 должен быть установлен на Windows Server 2008"). ADMT 3.2 и PES 3.1 не поддерживают установку на сервере Windows Server 2012. Программы установки преднамеренно блокируют неподдерживаемые ОС. В базе знаний имеется статья, описывающая эту проблему: `http://support.microsoft.com/kb/2753560/en-us`.

Как выглядит рекомендуемое решение? Установите ADMT 3.2 на сервере Windows Server 2008 R2 в целевом домене. Чтобы получить поддерживаемый сценарий, понадобится также установить Windows Server 2008 R2 в качестве целевого контроллера домена в новом домене.

Но что произойдет, если вы уже указали функциональный уровень леса Windows Server 2012? К счастью, функциональные уровни леса и домена можно понизить до Windows Server 2008 R2 с применением двух командлетов PowerShell.

Сначала необходимо понизить функциональный уровень леса:

```
Set-AdForestMode -identity bigfirm.com
  -forestmode Windows2008R2Forest
```

Вам придется подтвердить действие и подождать несколько секунд до успешного завершения команды. Затем нужно понизить функциональный уровень домена:

```
Set-AdDomainMode -identity bigfirm.com
  -domainmode Windows2008R2Domain
```

Здесь снова придется подтвердить действие и после успешного понижения функционального уровня домена можно установить контроллер домена Windows Server 2008 R2.

Если вы использовали средство Dynamic Access Control (Динамический контроль доступа), то больше не сможете это делать, потому что оно требует функционального уровня леса Windows Server 2012.

В этом примере будут раскрыты следующие задачи.

- Как провести миграцию учетных записей пользователей и групп через два леса.
- Каким образом хронологии SID позволяют мигрированным пользователям получать доступ к ресурсам в старом домене, списки ACL которых не изменялись.
- Как инструмент ADMT может изменить списки ACL на рабочей станции в старом домене ресурсов. Это также переназначит локальные профили пользователей их новым учетным записям.
- Каким образом инструмент ADMT может выполнить миграцию серверов-членов из старого домена в новый домен AD.

Чтобы все это заработало, мы настроим пять систем — две в `OtherDomain.local` и три в `Bigfirm.com`. Ниже описаны две системы в `OtherDomain.local`.

Мы настроим DC для `OtherDomain.local` с именем `DC2003`. На `DC2003` будут созданы указанные далее объекты.

- Открытая папка по имени `Users` с правами доступа Full Control (Полный доступ), выданными группе Everyone (Все). В оснастке Active Directory Users and Computers будут сконфигурированы разрешения NTFS для конкретных учетных записей пользователей.
- Организационная единица под названием `Administration` (Администрация).
- Учетные записи пользователей домена для персонала административного раздела.
- Домашняя папка, отображенная на диск Z, с UNC-путем `\\DC2003\users\%username%`.
- Глобальная группа по имени `Administration Group` (Группа администрации) и ее члены.
- Общая папка под названием `Administration` с правами доступа Full Control (Полный доступ), выданными группе `Administration Group`.
- Клиент Windows 7 по имени `Win7`, который должен быть мигрирован в домен `bigfirm.com`.

Домен `Bigfirm.com` будет содержать три системы.

- Чистый контроллер домена Windows Server 2012 по имени `DC01`.
- Временный контроллер домена Windows Server 2008 R2, который будет использоваться для нацеливания на ADMT. Он имеет имя `W2K8DC`.
- Сервер-член Windows Server 2008 R2 домена, где будет установлен инструмент ADMT. Этот сервер называется `ADMT01`.

Весь сценарий изображен на рис. 7.51.

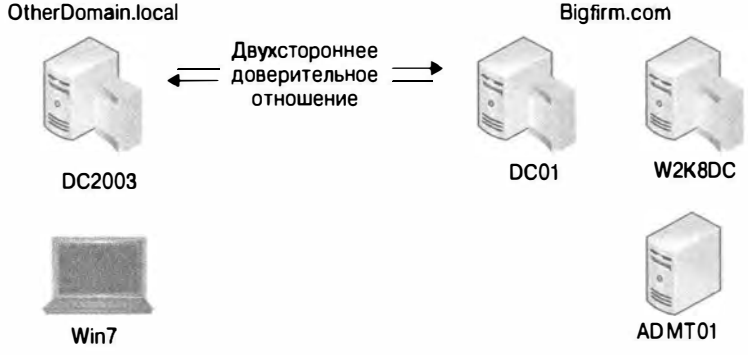


Рис. 7.51. Сценарий миграции

Установка доверительного отношения

Далее мы установим доверительное отношение между двумя доменами. В данном примере быстрее всего это делается с помощью консоли Active Directory Domains and Trusts (`domain.msc`). Выполните в мастере New Trust Wizard следующие действия.

1. Укажите тип доверительного отношения. Простым и эффективным здесь будет внешнее доверительное отношение.

2. Укажите двухстороннее доверительное отношение. Учетным записям из каждого домена нужен будет доступ к ресурсам в другом домене.
3. Создайте доверительное отношение в другом домене. Это требует наличия полномочий администратора домена в данном домене.
4. Проверьте доверительное отношение, убедившись в том, что все работает корректно.

В этой точке мы предпочитаем остановиться и провести тестирование — работает ли доверительное отношение и корректны ли разрешения на `DC2003`? Поскольку пользователи и глобальные группы из любого домена могут быть членами локальных групп домена и членами локальных групп сервера-члена, мы пытаемся добавить пользователя из противоположного домена во встроенную группу на контроллере домена. Это обязательный шаг на пути движения. Итак, мы находим и добавляем пользователя `Bigfirm\Administrator` во встроенную группу `Administrators` домена `OtherDomain` 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 мигрированных учетных записей. Если вы не обращали внимания на экраны мастера New Trust Wizard и подобно автомату щелкали на кнопках Next (Далее) и OK, то вполне могли пропустить диалоговое окно, показанное на рис. 7.52.

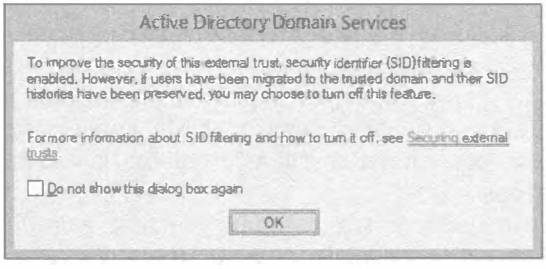


Рис. 7.52. Предупреждение о фильтрации SID

Что это было? Фильтрация SID включена. 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 наших 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 этом окне, мы узнали, что с помощью команды `netdom` можно отключать и включать фильтрацию SID для миграции, такой как проводимая в настоящее время.

Команда netdom в Windows Server 2012 устанавливается сразу, но в ранних версиях она была доступна в составе инструментов поддержки (Support Tools). В Microsoft выпустили последнюю версию Support Tools после Windows Server 2003 Service Pack 2, поэтому поищите ее на веб-сайте Microsoft.

Для отключения фильтрации SID запустите показанную ниже команду. Само отключение делает параметр /quarantine:no. Вы должны быть способны сами догадаться, как включить фильтрацию.

```
Rem выполняется на dc01.bigfirm.com
Netdom trust otherdomain /domain:bigfirm /quarantine:No
/usero:administrator /passwordo:P@ssw0rd

Rem выполняется на DC2003.OtherDomain.local:
Netdom trust bigfirm /domain:otherdomain /quarantine:No
/usero:administrator /passwordo:P@ssw0rd
```

Обеспечение дружественности к ADMT на обеих сторонах

Из-за своих потребностей ADMT может считаться совершенно пугающей программой. Эта программа 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

Утилита ADMT нуждается 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 OtherDomain.local. Это позволит утилите ADMT 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. Используя доверительное отношение между двумя доменами, она была также помещена во встроенную группу Administrators внутри домена OtherDomain.local и в локальную группу Administrators на рабочей станции Win7.bigfirm.com.

В исходном домене OtherDomain.local необходимо удовлетворить похожее требование для службы шифрования паролей (Password Encryption Service — 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 OtherDomain.local и членом встроенной группы Administrators в целевом домене Bigfirm.com.

Мы создали учетную запись с не менее незамысловатым именем PES в домене OtherDomain.local. 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, по-видимому потому, чтобы он мог проводить мониторинг того, как и что он делает. В исходном домене — домене, из которого копируются пользователи, т.е. `OtherDomain.local` — должен быть включен аудит успехов и отказов для управления пользователями и группами.

На целевой и исходной машинах (`W2K8DC.Bigfirm.com` и `DC2003.OtherDomain.local`) мы включаем аудит путем модификации групповой политики, которая называется стандартной политикой контроллеров домена (Default Domain Controllers Policy). В стандартной установке Windows Server 2003 для этого можно применять оснастку Active Directory Users and Computers. Щелкните правой кнопкой мыши на организационной единице Domain Controllers (Контроллеры домена) и выберите в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом окне перейдите на вкладку Group Policy (Групповая политика), дважды щелкните на элементе Default Domain Controllers Policy (Стандартная политика контроллеров домена), в результате чего откроется редактор групповой политики. В версии Windows Server 2008 R2 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), но не закрывайте окно редактора групповой политики; ваша работа пока еще не закончена.

Включение криптографических настроек в целевом домене

Для проведения миграции компьютеров с предшествующими версиями Windows в целевой домен с контроллерами домена, функционирующими под управлением Windows Server 2008 и выше, в целевом домене требуется еще одна настройка объекта GPO. В разделе параметров безопасности объекта GPO контроллера домена включите опцию Allow cryptography algorithms compatible with Windows NT 4.0 (Разрешить криптографические алгоритмы, совместимые с Windows NT 4.0).

В узле Computer Configuration последовательно разверните узлы Administrative Templates (Административные шаблоны), System (Система) и Netlogon (Папка Netlogon). Щелкните правой кнопкой мыши на элементе Allow cryptography algorithms compatible with Windows NT 4.0 (Разрешить криптографические алгоритмы, совместимые с Windows NT 4.0), выберите в контекстном меню пункт Edit (Редактировать), в открывшемся окне щелкните на переключателе Enabled (Включено) и щелкните на кнопке OK.

Прежде чем запускать ADMT

Как упоминалось ранее, при чистой изначальной миграции вы оставляете все существующие объекты на своих местах и перемещаетесь в новый лес или домен. Исходя из нашего опыта, хотя вы оставляете все нежелательные объекты позади, стрессогенный фактор можно ослабить, если перед миграцией приступить к очистке старой среды. Провести уборку в старой квартире, несмотря на то, что вы переезжаете на новую квартиру? Да, правильно! В отношении миграции домена мы рекомендуем выполнить несколько шагов по очистке в исходном домене.

Первым делом, выясните, имеют ли объекты какие-то старые хронологии SID. Если вы собираетесь проводить миграцию пользователей, групп и компьютеров, то вам не нужны старые хронологии SID в учетных записях. Далее проверьте актуальность пользователей, групп и компьютеров, которые вы собираетесь переносить. Нет смысла выполнять миграцию старых и зависших пользователей, групп и компьютеров. По этой причине перед миграцией устаревшие неиспользуемые объекты потребуется удалить.

После очистки среды удостоверьтесь, что вложенность групп соответствует принципу AGDLP (AGUDLP). Этот принцип означает, что учетная запись вложена в глобальную группу, глобальная группа является членом универсальной группы (если необходимо), а универсальная или глобальная группа является членом локальной группы домена. Такой локальной группе домена назначены разрешения на доступ к ресурсам.

Вероятно, это самые важные шаги, которые необходимо выполнить перед миграцией, и они помогают добиться успеха и мигрировать только те объекты, которые действительно нужны.

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 стандартный экземпляр SQL Server. В большинстве случаев предпочтение следует отдавать SQL Express.

Проблемы с установкой ADMT

Поскольку существует много причин, по которым установка ADMT может завершиться неудачно, мы рекомендуем почитать следующую статью (на английском языке), посвященную устранению проблем: `http://blogs.technet.com/b/askds/archive/2010/07/09/admt-3-2-common-installation-issues.aspx`.

Создание ключа пароля в целевом домене

Теперь вы хотите, чтобы пароли пользователей передавались вместе с их учетными записями. Утилита ADMT может делать это с помощью службы шифрования паролей (Password Encryption Service — PES). Перед тем, как будет проводиться миграция паролей, ADMT требует от вас создания файла шифрования паролей на сервере-члене `ADMT01` и его копирования на контроллер домена `DC2003`, который будет применять этот файл при отправке паролей по сети в зашифрованном виде.

Для этого потребуется запустить ADMT из командной строки. Ниже приведен пример синтаксиса команды:

```
admt key /option:create /sourcedomain:otherdomain
  /keyfile:c:\temp\password.pes /keypassword:P@ssw0rd
```

Команда указывает на необходимость подготовки ключа, который может использоваться доменом `OtherDomain.local` для передачи паролей в домен `Bigfirm.com`. (Домен `Bigfirm.com` не был явно упомянут потому, что команда вводится на контроллере домена `Bigfirm.com`.) В параметре `/keyfile` просто указано, куда помещать файл — `C:\temp\password.pes`. Если на вашем сервере имеется флоппи-дисковод, то подойдет и `A:\`. Совершенно не имеет значения, где вы разместите этот файл — важно лишь понимать, что вам придется каким-то образом транспортировать его на контроллер домена `OtherDomain.local`, т.е. `DC2003`. Если все прошло нормально, утилита ADMT возвратит примерно такое сообщение:

```
The password export server encryption key for domain 'otherdomain' was
successfully created and saved to 'c:\temp\password.pes'
```

Ключ шифрования для сервера экспорта паролей для домена otherdomain успешно создан и сохранен в c:\temp\password.pes

На данный момент вы завершили работу с `ADMT01.Bigfirm.com`. Время переходить на `DC2003`.

Перемещение файла PES

После входа в систему контроллера домена `DC2003` вам нужно поместить файл PES из `ADMT01.bigfirm.com` на локальный диск; мы обычно создаем общую папку и копируем в нее этот файл по сети. В качестве альтернативы его можно поместить на флоппи-диск, CD-ROM или любой другой носитель по своем желанию — тем или иным способом файл PES должен попасть на `DC2003`.

Установка DLL-библиотеки миграции паролей на исходном контроллере домена

Служба Password Encryption Service была включена только в ранние версии ADMT. В случае версии ADMT 3.1 она доступна в виде отдельного загружаемого файла.

Служба PES устанавливается посредством файла MSI по имени `PWMIG.MSI`; дважды щелкните на нем, чтобы запустить мастер установки DLL-библиотеки миграции паролей ADMT (ADMT Password Migration DLL Installation Wizard). Ключевыми ингредиентами, требуемыми при установке, являются файл PES и созданная ранее учетная запись службы. После установки вам будет предложено перезагрузить систему. Не забывайте, что служба сконфигурирована на запуск вручную. Именно поэтому утилита ADMT не будет работать, пока вы не обеспечите функционирование службы PES.

Небольшие работы на рабочей станции

Если компьютеры должны быть перенесены, нам необходимо выполнить дополнительные действия. Утилита ADMT устанавливает на компьютере службу агента для модификации настроек безопасности и запуска изменения членства в домене. Перед установкой утилита выполнит несколько проверок, чтобы обеспечить успеш-

ный результат. Одной из них является проверка службы общего доступа к файлам и принтерам. В Windows XP, Windows Vista и Windows 7 брандмауэр будет препятствовать таким тестам.

- Запустите `firewall.cpl`, щелкните на вкладке Advanced (Дополнительные параметры) и сконфигурируйте для настроек ICMP опцию Allow Incoming Echo Request (Разрешить входящий эхо-запрос). Это делается для вашей же пользы.
- На вкладке Exception (Исключения) выберите File and Printer Sharing (Общий доступ к файлам и принтерам).

Вдобавок мы рекомендуем выполнить следующие действия.

- Добавьте учетную запись `ADMT` в качестве члена локальной группы `Administrators`, как упоминалось ранее.
- Установите для локальной учетной записи `Administrator` известный пароль. Если изменения членства в домене даст сбой, то эта учетная запись может оказаться единственным способом входа в систему рабочей станции с целью устранения проблем.

Запуск ADMT и миграция

При миграции пользователей и компьютеров из одного домена в другой базовая последовательность действий выглядит так, как описано ниже.

1. Настройте доверительные отношения, параметры реестра и т.д.
2. Проведите миграцию учетных записей служб.

   Для краткости здесь это детально не рассматривается. Учетная запись службы переносится в новый домен, и в настройки серверов исходного домена вносятся изменения, чтобы они использовали уже новую учетную запись.
3. Проведите миграцию глобальных групп из старого домена в новый.

   Новые глобальные группы получают хронологии SID от старых таких групп, поэтому любой член новой группы `BIGFIRM\Administration` будет иметь доступ ко всем ресурсам, к которым имели доступ члены группы `OtherDomain.local\Administration`. Это означает, что после миграции пользователей из `OtherDomain.local` в `Bigfirm.com` они могут быть автоматически помещены в группу `Administration` внутри домена `Bigfirm.com` и будут иметь непосредственный доступ к своим старым ресурсам.
4. Проведите миграцию пользователей.

   Как только выполнена миграция глобальных групп, можно приступать к миграции пользователей в любом приемлемом для вас рабочем темпе. Пользователи, перемещенные в новый домен, будут иметь возможность доступа к общим файлам, принтерам и другим ресурсам из старого домена, т.к. учетные записи эти пользователей содержат хронологии SID из старого домена.
5. Проведите миграцию рабочих станций и серверов в домен `Bigfirm.com`. Поменяйте членство в домене с `OtherDomain.local` на `Bigfirm.com`.
6. Переместите объекты безопасности.

Права доступа пользователей, разрешения файлов и общих ресурсов и членство в локальных группах являются теми несколькими объектами, для которых утилита ADMT может скорректировать списки ACL. Чтобы обеспечить доступ к ресурсу, к серверам и рабочим станциям должны быть применены идентификаторы SID новых учетных записей и групп. В зависимости от того, как проводится миграция, операция такого типа может происходить перед миграцией серверов. В рассматриваемом примере локальные профили рабочей станции должны быть отображены на новые учетные записи. Во время длительной миграции пользователи и их рабочие станции могут переноситься не одновременно. Таким образом, профили должны быть перемещены перед изменением членства компьютера в домене.

7. Повторите процессы миграции для ликвидации брешей.

   Может понадобиться изменение членства в группах, учетные записи пользователей могут требовать включения или отключения, а дополнительные объекты безопасности могут нуждаться в переносе. Все это требует плановых запусков утилиты ADMT.

8. Проведите миграцию локальных групп домена.

9. После того как все серверы-члены перемещены в домен `Bigfirm.com` и выполнена проверка корректности изменения во всех разрешениях ссылок к `OtherDomain.local` на ссылки к `Bigfirm.com`, домен `OtherDomain.local` можно выводить из эксплуатации — разорвать доверительное отношение, изолировать контроллеры домена `OtherDomain.local` и удалить хронологии SID из перемещенных учетных записей пользователей.

Наступило время провести миграцию глобальных групп и пользователей, так что давайте приступим к ней. Перейдите на сервер `ADMT.Bigfirm.com` и запустите утилиту ADMT, выбрав в меню Start (Пуск) пункт Administrative Tools⇨Active Directory Migration Tool (Администрирование⇨Инструмент миграции Active Directory). Как показано на рис. 7.53, утилита обладает пользовательским интерфейсом довольно-таки спартанского вида, в котором есть всего несколько доступных функций:

- миграция групп;
- миграция учетных записей служб;
- миграция пользователей;
- перемещение локальных профилей пользователей;
- миграция рабочих станций и серверов-членов.

Утилита делает *очень* многое, больше чем можно раскрыть в этой главе. Здесь приводятся только основы. Мы *настоятельно* рекомендуем почитать справочный файл, поступающий с утилитой, поскольку ADMT является мощным и удобным инструментом, который позволяет проводить миграцию пользователей, групп, машин и даже настроенных сред Exchange! Кроме того, на веб-сайте Microsoft доступно для загрузки руководство по миграции (Migration Guide).

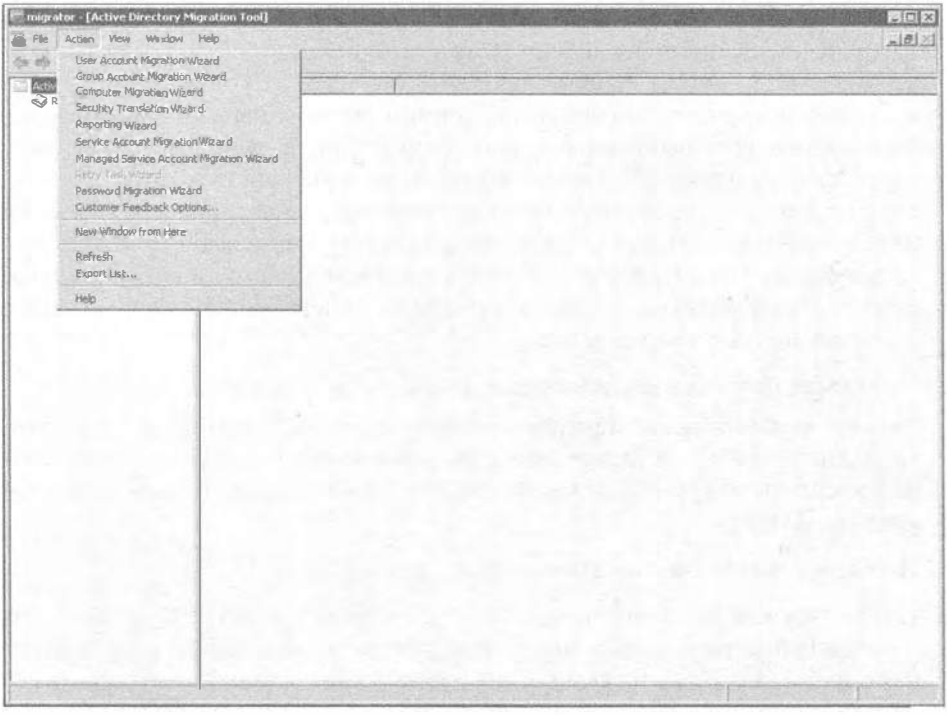


Рис. 7.53. Спартанский пользовательский интерфейс консоли ADMT

Графический пользовательский интерфейс, командная строка или VBScript

Утилита ADMT предлагает три интерфейса для проведения миграции. Каждый из них обладает своими преимуществами.

- **Графический пользовательский интерфейс.** Основанная на технологии консоли управления Microsoft (Microsoft Management Console), оснастка ADMT предоставляет набор мастеров для пошагового выполнения каждой функции. Это удобно, когда вы не знакомы с вариантами и обязательными параметрами для миграции определенного объекта. Тем не менее, проход со щелчками в мастере при большом количестве объектов довольно утомителен.
- **Командная строка.** С использованием инструмента командной строки ADMT можно создавать пакетные файлы. Они удобны при миграции крупного числа учетных записей. Каждая команда ограничена перемещением учетных записей в одну организационную единицу, поэтому она не может охватить все. Ниже приведен список доступных функций. Некоторые примеры применения будут продемонстрированы в последующих разделах.

```
admt
Синтаксис этой команды:

ADMT [ USER | GROUP | COMPUTER | SECURITY | SERVICE |
       REPORT | KEY | PASSWORD | CONFIG | TASK ]
```

- **VBScript.** Сценарии VBScript предлагают логику для управления операциями ADMT. Они также предоставляют функциональность чтения входных текстовых файлов и выполнения отдельных операций над каждой записью. Таким образом, большое количество операций с отличающимися требованиями могут объединяться в пакетное задание без особого труда. Написание сценариев предусматривает наличие специальных знаний.

Мы настоятельно рекомендуем выполнить такие операции в тестовой среде, чтобы получить представление об утилите и разработать план конкретной миграции. Смешивание разных методов может оказаться более эффективным, чем применение только какого-то одного из них.

Информация, необходимая каждому методу и каждой функции, подобна, поэтому их описание может выглядеть повторяющимся. Далее мы рассмотрим несколько примеров выполнения операций с использованием графического пользовательского интерфейса и командной строки.

Миграция пользователей и групп с помощью оснастки ADMT

Миграция групп и миграция пользователей очень похожи. В этом примере мы будем проходить по экранам мастера миграции учетных записей пользователей (User Account Migration Wizard).

1. В окне ADMT выберите в меню Action (Действие) пункт User Account Migration Wizard (Мастер миграции учетных записей пользователей) и щелкните на кнопке Next (Далее); откроется знакомый экран приветствия мастера.

   Ранние версии ADMT предлагали тестовый запуск операций. Версия 3.1 не настолько робкая. Следовательно, обязательно выполняйте эти действия сначала в тестовой среде в целях ознакомления, а затем проделайте их для испытательных учетных записей в производственной среде.

2. Щелкните на кнопке Next, чтобы перейти на экран, показанный на рис. 7.54.

   На этом экране просто выбирается домен, из которого будет осуществляться перемещение, и домен, куда это будет делаться. Но на самом деле это действие очень полезно, т.к. оно служит проверкой подключаемости. Если контроллер домена `DC2003` не функционирует, единственным вариантом в списках Domain (Домен) внутри разделов Source (Исходный) и Target (Целевой) был бы домен `Bigfirm.com`, что вряд ли можно посчитать интересной миграцией.

3. После выбора доменов щелкните на кнопке Next (рис. 7.55) и вы заметите небольшую паузу, связанную с подключением контроллеров доменов. Переключатель Read objects from an include file (Читать объекты из включенного файла) на экране User Selection Option (Опция выбора пользователей), показанном на рис. 7.55, требует импорта в мастере файла со списками пользователей и групп.

4. В данном случае выбран переключатель Select users from domain (Выбрать пользователей из домена). Выбор этого переключателя приводит к отображению экрана User Selection (Выбор пользователей), представленного на рис. 7.56, который позволяет выбрать объекты для миграции, в этом случае пользователей. Щелчок на кнопке Add (Добавить) обеспечивает открытие типового диалогового окна поиска, которое вы видели в оснастке Active Directory Users and Computers.

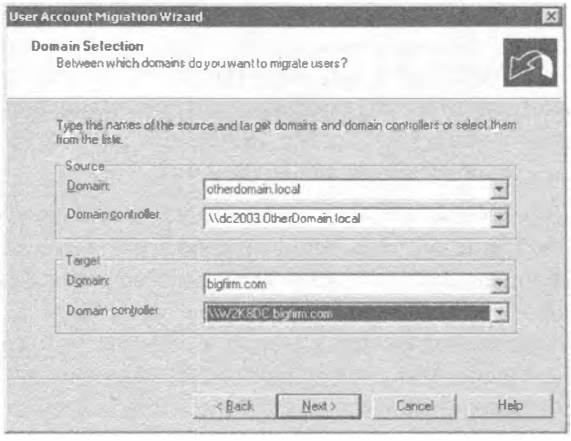


Рис. 7.54. Выбор исходного и целевого доменов

Рис. 7.55. Экран User Selection Option мастера

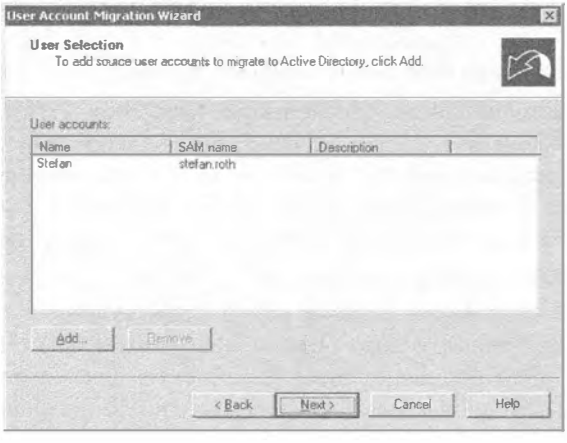


Рис. 7.56. Экран User Selection мастера

5. Для этого примера щелкните на кнопке Add и выберите одного пользователя `stefan.roth`, хотя можно было бы выбрать любое количество пользователей и групп.
6. Щелкните на кнопке Next; откроется экран Organizational Unit Selection (Выбор организационной единицы), показанный на рис. 7.57, который дает возможность выбрать организационную единицу в целевом домене.

   Подобно всем качественным инструментам, осведомленным об AD, утилита ADMT позволяет выбирать организационную единицу, в которую должны быть помещены перенесенные группы. Но не стоит переживать по поводу того, что вам придется овладеть этим громоздким протоколом LDAP.

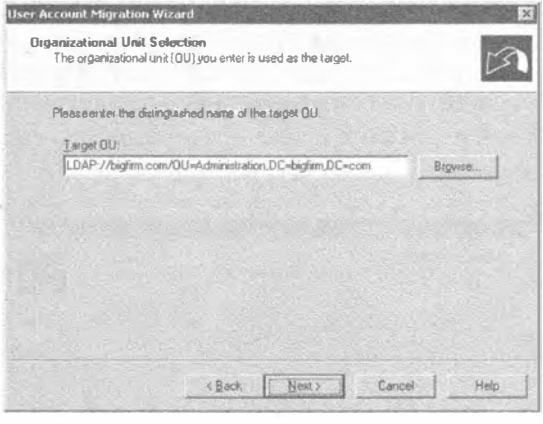


Рис. 7.57. Экран Organizational Unit Selection мастера

7. Щелкните на кнопке Browse (Обзор), в результате чего ADMT позволит выполнить навигацию по структуре AD.
8. Щелкните на кнопке Next, чтобы перейти на экран Password Options (Опции паролей), показанный на рис. 7.58, на котором отображаются опции паролей.

   Поскольку пароли присущи только учетным записям пользователей, экран Password Options открывается только в мастере User Account Migration Wizard. По существу вы можете перенести пароли или заставить ADMT предоставить новые пароли для пользователей. Первый вариант требует наличия сервера PES. Во втором варианте необходимо указать местоположение для сохранения текстового файла, содержащего все эти новые пароли. Как вы наверняка догадались, распространение этого файла среди пользователей не должно делаться в виде почтового вложения для группы рассылки `All Users` (Все пользователи). Следовательно, у вас будет дополнительная задача по передаче новых паролей пользователям после миграции.
9. Щелкните на кнопке Next.

   Появится следующий экран мастера, Account Transition Options (Опции перемещения учетных записей), показанный на рис. 7.59. На нем определяется способ обработки целевых и исходных учетных записей после миграции. В зависимости от сценария, учетные записи может понадобиться отключить на

какой-то период времени. Утилита ADMT может обрабатывать обе стороны. Обратите внимание на флажок Migrate user SIDs to target domain (Перенести идентификаторы SID пользователей в целевой домен). Отметка этого флажка приводит к созданию хронологии SID для пользователя или группы. Таким способом утилита ADMT говорит: "Создать элемент хронологии SID в домене `Bigfirm.com` для учетной записи пользователя `stefan.roth`".

10. Щелкните на кнопке Next, чтобы получить нечто вроде полезной диагностики — если что-то не на месте для нормального функционирования механизма хронологии SID, утилита ADMT выдаст сообщение об ошибке. Или же будет выдано предупреждение, например, о создании вспомогательной группы `OtherDomain$$$` и включении аудита, если вы забыли сделать это.

    Всякий раз, когда вы применяете хронологию SID, утилита ADMT сверяется со старым доменом, в данном случае `OtherDomain.local`, для выяснения, приемлемо ли создание вспомогательной группы. Эта группа имеет некоторое отношение к тому, как ADMT гарантирует, что хронологии SID будут работать корректно, но мастер в любом случае предпринимает проверку, удостоверяясь в возможности создания данной группы.

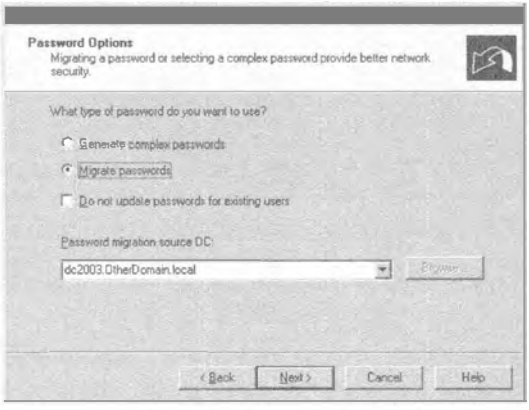


Рис. 7.58. Экран Password Options мастера

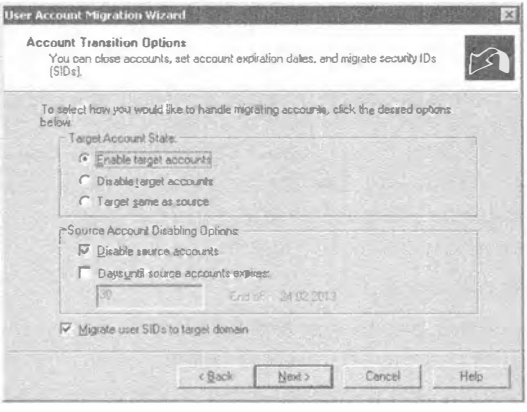


Рис. 7.59. Экран Account Transition Options мастера

11. Щелкните на кнопке Yes (Да), и вы увидите экран входа в систему (рис. 7.60), как будто вы еще не предоставляли свои учетные данные.

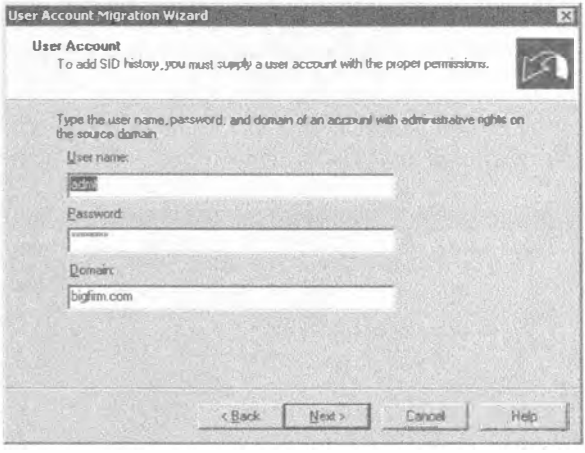


Рис. 7.60. Учетные данные для хронологии SID

12. Щелкните на кнопке Next, чтобы перейти на экран User Options (Опции пользователей), приведенный на рис. 7.61.

    Обычно предпочтительной опцией для первой миграции является Fix users' group memberships (Скорректировать членство в группах для пользователей). Отметка этого флажка приведет к обновлению идентификаторов SID в группах, к которым принадлежат пользователи. Другие опции можно использовать позже в повторных миграциях учетной записи для содействия в отбрасывании старой хронологии SID. Флажок Update user rights (Обновить права доступа пользователей) отвечает за замену идентификаторов SID новыми SID. Флажок Translate roaming profiles (Перенести блуждающие профили) позволяет переназначить разрешения новому идентификатору SID.

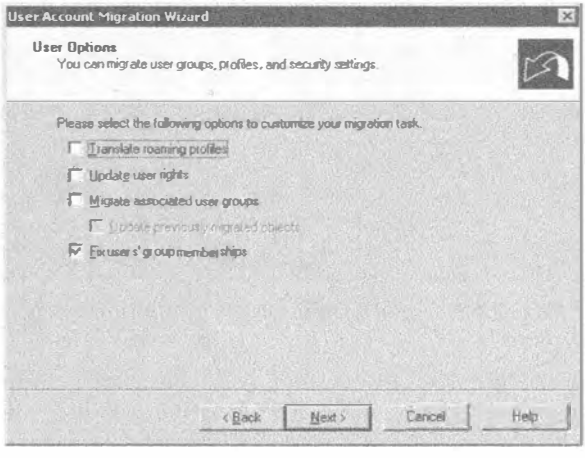


Рис. 7.61. Экран User Options мастера

Экран Object Property Exclusion (Исключение свойств объектов), показанный на рис. 7.62, дает возможность исключить из процесса миграции определенные свойства. Предположим, что в Bigfirm не хотят, чтобы перемещались поля учетной записи пользователя с информацией об отделе или компании; посредством этого экрана такие поля можно выделить и исключить.

Вы осуществляете миграцию группы под названием `Administration`, но что если группа с таким именем уже *имеется*? Ответ на этот вопрос дает экран Conflict Management (Управление конфликтами), представленный на рис. 7.63.

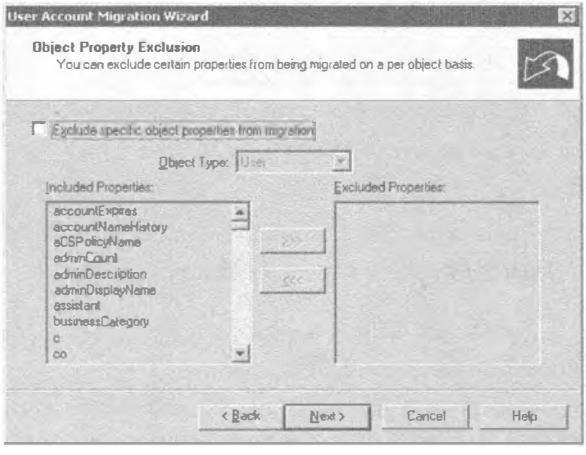


Рис. 7.62. Экран Object Property Exclusion мастера

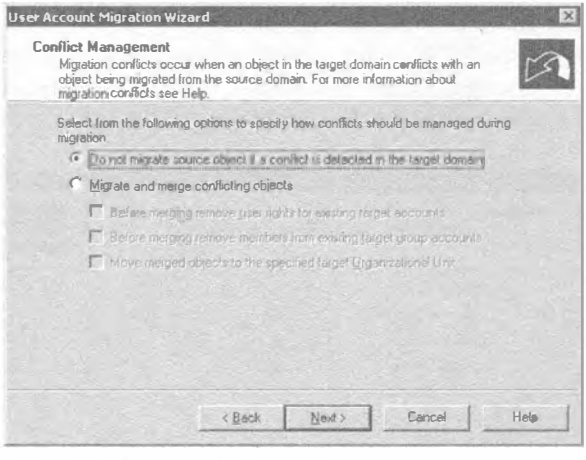


Рис. 7.63. Экран Conflict Management мастера

13. Вы можете пропустить миграцию этой группы, затереть существующую группу `Administration` или добавить в имени группы какой-то префикс.
14. Пройдите по оставшимся экранам мастера до появления кнопки Finish (Готово), после чего процесс миграции запустится.

В диалоговом окне Migration Progress (Продвижение миграции) будет отображаться статистические данные по процессу миграции (рис. 7.64). В случае возникновения ошибок просмотрите соответствующий журнал, щелкнув на кнопке View Log (Просмотреть журнал). Кроме того, можно обратиться к журнальным файлам в папке `c:\windows\admt`. Журнальные файлы именуются с применением даты/времени.

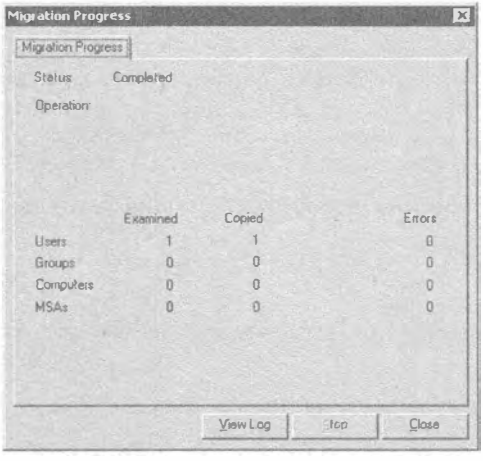


Рис. 7.64. Диалоговое окно Migration Progress

Миграция с помощью командной строки

Как упоминалось ранее, утилита командной строки `ADMT.exe` предлагает организацию пакетных операций, что устраняет необходимость в угомительных проходах со щелчками по экранам мастеров консоли.

Ниже приведен пример миграции глобальной группы `Administration`:

```
rem миграция глобальной группы
admt group /N "administration group" /sd:"otherdomain.local"
 /td:"bigfirm.com" /to:"administration" /mss:yes /fgm:yes
 /ugr:yes /mms:no /co:Merge+REMOVEUSERRIGHTS+REMOVEMEMBERS
```

Хотя в этом примере присутствуют далеко не все параметры данной команды, каждый параметр представляет экран мастера.

- `/N`. Учетная запись SAM (Security Account Manager — диспетчер учетных записей безопасности) группы. Также могут быть указаны имена дополнительных групп.
- `/sd`. Исходный домен.
- `/td`. Целевой домен.
- `/to`. Целевая организационная единица.
- `/mss`. Перемещение идентификаторов SID. Эквивалент флажка Migrate user SIDs to target domain.
- `/fgm`. Корректировка членства в группах.
- `/ugr`. Обновление прав доступа группы.

- /mms. Перемещение членов. Если указано yes (да), все учетные записи пользователей, являющихся членами, также будут подвергнуты миграции.
- /co. Опции разрешения конфликтов. В этом случае группа будет сливаться с группой, имеющей совпадающее имя, из этой группы будут удалены права доступа пользователей, и любые существующие члены будут удалены.

Следующая команда проводит миграцию оставшихся учетных записей пользователей в организационной единице Administration:

```
rem миграция учетных записей пользователей
admt user /N "stefan.roth" "marcel.zehner" "philipp.witschi" "chris.greuter"
/sd:otherdomain.local /td:bigfirm.local /to:"administration"
/mss:yes /co:ignore /po:copy /ps:dc2003.otherdomain.local
/dot:disablesource+enabletarget /uur:yes /fgm:yes
```

Дополнительные параметры являются специфичными для пользователей.

- /po. Опция паролей.
- /ps. Сервер PES.
- /dot. Опции перемещения, которые управляют состоянием учетных записей после миграции.
- /uur. Обновление прав доступа пользователей.

Тестирование доступа к ресурсам перемещенной группой

Поскольку перемещенная группа Administration в Bigfirm.com имеет идентификатор SID, совпадающий с SID группы Administration в домене OtherDomain.local, и старая группа имела доступ к \\DC2003\Administration, то любой член новой группы Administration должен быть в состоянии обращаться к общему ресурсу \\DC2003\Administration. Давайте проверим это.

1. В домене Bigfirm.com войдите в систему от имени учетной записи Administrator и попытайтесь получить доступ к общему ресурсу \\Dc2003\Administration.

   Это должно привести к выдаче сообщения о запрете доступа, поскольку учетная запись не имеет разрешений на доступ к этому общему ресурсу.

2. Сделайте учетную запись Administrator членом новой перемещенной группы Administration в Bigfirm.com.
3. Выйдите из системы и снова войдите как администратор.

   Это должно делаться для того, чтобы перестроился маркер безопасности.

4. Попробуйте подключиться к общему ресурсу \\DC2003\Administration еще раз.

Итак, общий ресурс Administration открывается! Значит, хронология SID работает.

Перенос локальных профилей

Предполагая, что учетные записи пользователей были успешно перемещены, пользователи будут иметь возможность доступа к ресурсам внутри домена OtherDomain.local. Однако они по-прежнему вынуждены работать на рабочей

станции, расположенной в этом домене. Если пользователи войдут в систему на рабочей станции Win7 сейчас, им придется создавать новые профили. Они начнут ворчать, что не могут найти фотографии своих близких, или, даже хуже, свои любимые веб-сайты в Интернете!

Чтобы предотвратить эти сложности, мастер переноса объектов безопасности (Security Transition Wizard) обеспечивает переназначение идентификаторов SID для существующих профилей на всех платформах Windows.

Мастер Security Translation Wizard используется для выполнения процедур нескольких типов. Одной из них является перенос локальных профилей. Мастер может также переназначить разрешения для прав доступа пользователей, файлов и общих ресурсов, принтеров и реестра. Это будет подробно рассмотрено в следующем разделе.

Перенос профилей с помощью оснастки ADMT

Запустить мастер Security Translation Wizard можно через меню Action (Действие) консоли ADMT (см. рис. 7.53). Он запрашивает многие данные, которые также требуются мастерам миграции пользователей и групп.

- Исходный домен и контроллер домена.
- Целевой домен и контроллер домена.
- Выбор объектов, на этот раз компьютеров. Они выбираются посредством типового диалогового окна поиска. В нашем примере целевым компьютером является Win7, локальные профили которого будут переназначены перемещенным пользователям.

После этого на экране Translate Objects (Переносимые объекты) мастера необходимо указать объекты безопасности, подлежащие переносу (рис. 7.65). Детальное описание каждого из них можно найти в справочном файле ADMT. В данном примере просто отметьте флажок User profiles (Профили пользователей).

На экране Security Translation Options (Опции переноса объектов безопасности), показанном на рис. 7.66, доступны три опции для обращения со старым идентификатором SID — Replace (Заменить), Add (Добавить) и Remove (Удалить).

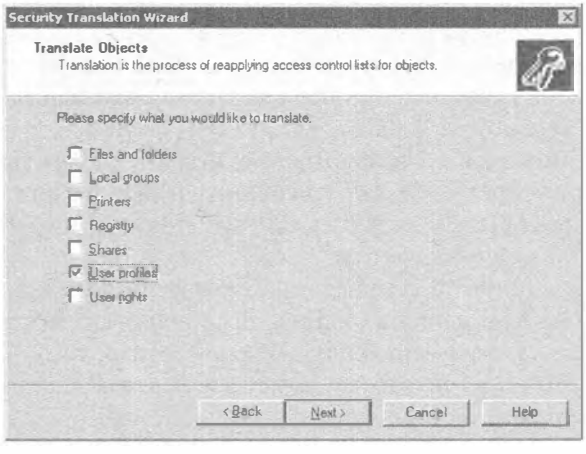


Рис. 7.65. Экран Translate Objects мастера

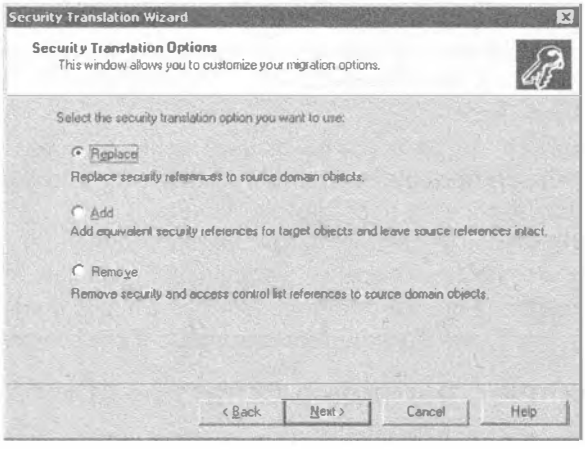


Рис. 7.66. Экран Security Translation Options мастера

В справочном файле ADMT указано, какая опция требуется для каждого типа объекта безопасности. В этом случае для локальных профилей необходимо выбрать Replace. Применение опции Add с локальными профилями имеет тенденцию нарушать работу пакетов прикладных приложений, развернутых с помощью объектов групповой политики.

Старый идентификатор SID будет заменен новым SID учетной записи пользователя, так что когда пользователь `Bigfirm\Stefan.Roth` входит в систему на рабочей станции, он отождествляет исходный профиль с новой учетной записью.

После завершения работы мастера откроется окно Active Directory Migration Tool Agent Dialog (Диалоговое окно агента ADMT), представленное на рис. 7.67, которое позволит выполнить действительную операцию на рабочей станции. Вы должны запустить операцию, выбрав желаемый переключатель: Run pre-check (Запустить предварительную проверку) или Run pre-check and agent operation (Запустить предварительную проверку и операцию агента). (Если вы используете утилиту командной строки ADMT, операция запустится автоматически.) Предварительная проверка, как упоминалось ранее, протестирует службы файлов и печати (File and Print Services), а более конкретно — проверит, может ли учетная запись `ADMT` получить доступ к административному общему ресурсу наподобие `\\Win7\admin$`. Операция агента установит этот агент на рабочей станции `Win7` и затем выполнит перенос.

В разделе Agent Summary (Сводка агента) отображается продвижение. Просмотреть дополнительную информацию можно, щелкнув на кнопках View Migration Log (Просмотреть журнал миграции) и Agent Detail (Детали агента). Щелчок на кнопке Agent Detail вызывает открытие окна с подробными сведениями о событиях установки и запуска агента.

На время выполнения этой операции пользователи должны выйти из системы рабочей станции, а не блокировать систему. Заблокированная рабочая станция будет также блокировать доступ к профилю. Это приводит к тому, что агент выполнит операцию добавления, но по-прежнему может сообщать об ошибке или реагировать непредсказуемым образом. Исходя из нашего опыта, некоторые пользователи могут не понимать разницу между выходом из системы и ее блокированием.

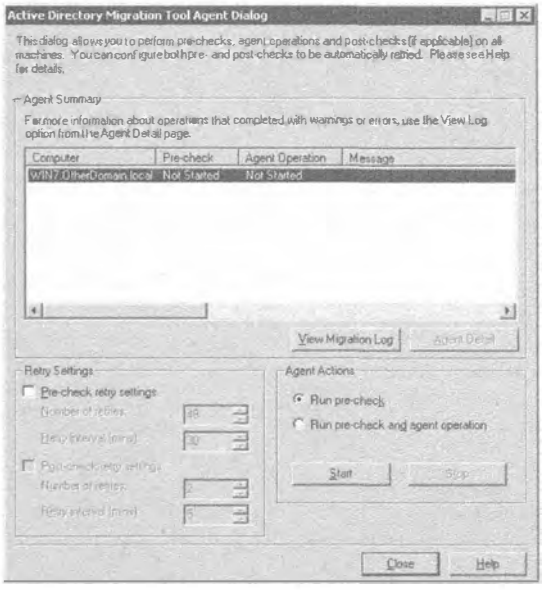


Рис. 7.67. Окно Active Directory Migration Tool Agent Dialog

Мы рекомендуем пользователям перезагружать свои рабочие станции в конце работы. Затем можно запустить операцию агента в нерабочее время.

После завершения операции агента пользователь может войти в систему с применением новой учетной записи. Должен появиться старый рабочий стол и быть доступными все прочие настройки, специфичные для профиля. В этом случае должны быть доступными диски, отображенные на домашние папки. Возможность доступа в домашние папки также подтверждает работу хронологии SID.

При дополнительных запусках мастера Security Translation Wizard могут быть скорректированы разрешения для домашних папок.

Миграция учетных записей компьютеров

Процесс миграции учетных записей компьютеров выглядит похожим на использование мастера Security Translation Wizard и окна Active Directory Migration Tool Agent (рис. 7.68).

Раздел Agent Summary включает столбец Post-check (Постпроверка). Операция агента производит изменение членства в домене, что потребует перезагрузки. Верификация изменения выполняется в постпроверке. Перезагрузка делает важными настройки повторения постпроверки, которыми являются количество повторений и интервал между попытками. Через некоторое время операция завершается.

Соображения относительно отката

Наибольшим преимуществом чистой изначальной миграции является ее постепенная природа. Она также приспосабливается к планам постепенного отката. Фазы миграции будут вскрывать любые затруднения и сбои. Вы должны застраховаться от них, проводя эксперименты. Если проблемы или затруднения возникают, их можно избежать за счет выполнения отката.

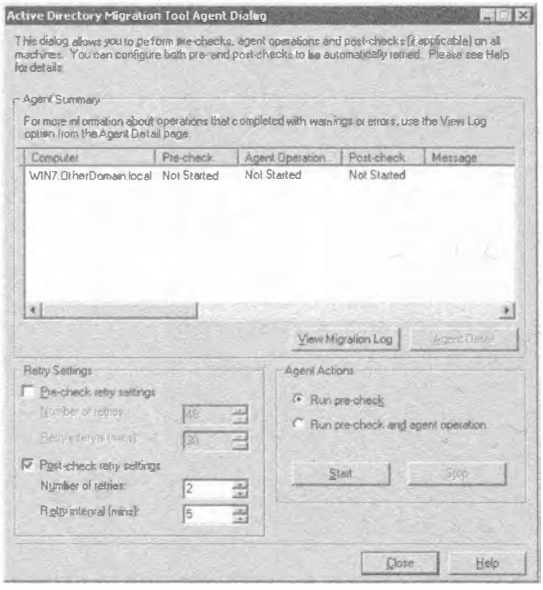


Рис. 7.68. Окно Active Directory Migration Tool Agent Dialog для миграции учетных записей компьютеров

Проблемы могут быть разрешены на индивидуальной основе, а при правильном планировании можно учесть обходные пути и промежуточные состояния.

Процесс миграции предусматривает создание копий учетных записей и групп. Таким образом, исходные учетные записи и группы останутся на месте и при необходимости могут быть снова включены для использования. Проведения процедур отката требуют только несколько объектов безопасности, такие как локальные профили пользователей.

Следовательно, для каждой фазы миграции планируйте и тестируйте откат в состояние, предшествующее внесению определенного изменения внутри фазы.

Путь к функциональному уровню леса Windows Server 2012

Приняв решение о том, какой метод миграции применять, вы приступите к процессу модернизации или миграции, как было описано в соответствующих разделах.

В лесе с единственным доменом вы модернизируете каждый контроллер домена до Windows Server 2012. После установки Windows Server 2012 на всех контроллерах домена можно поднять функциональный уровень домена до Windows Server 2012, после чего также поднять функциональный уровень леса до Windows Server 2012.

В среде с множеством доменов можно независимо модернизировать каждый домен внутри леса с несколькими доменами. Например, вы можете начать модернизацию контроллеров домена в дочернем домене, а потом заняться модернизацией контроллеров домена в корневом домене того же самого леса. После модернизации все контроллеров домена до Windows Server 2012 можно поднять функциональный уровень этого домена. Продолжайте модернизировать каждый домен до Windows Server 2012 до тех пор, пока все домены внутри леса не будут иметь функциональный уровень домена Windows Server 2012. Затем можно поднять функциональный уровень леса до Windows Server 2012.

Детальная процедура по поднятию функциональных уровней домена и леса была описана в разделе "Поднятие функциональных уровней домена и леса" ранее в этой главе.

Введение в Windows Azure Active Directory

Ранее мы обсуждали среду Active Directory, находящуюся внутри помещений. Это означает, что среда Active Directory внутри компании защищена от внешнего мира. Давайте кратко повторим, почему используется Active Directory. Эта служба каталогов необходима для централизованного хранения и управления всеми пользователями и компьютерами с целью контроля над поведением существующей инфраструктуры Windows.

За несколько лет до разработки Active Directory в отрасли IT имелась крупная проблема. В отсутствие Active Directory каждое приложение должно было хранить свои учетные данные для доступа локально в хранилище, таком как база данных, или локально на самом сервере. ОС Windows NT располагала довольно строгим способом управления пользователями и компьютерами, но то решение было далеко от потребностей предприятия. Одной из главных причин разработки Active Directory была необходимость в централизованном управлении инфраструктурой. В наши дни та же самая проблема возникает в облаке Windows Azure. Ландшафт приложений снова стал фрагментированным. Некоторые облачные приложения в компании имеют хранилище конфигурации, содержащее в себе имена пользователей и пароли, так что такое приложение может аутентифицировать и авторизовать пользователя для работы с этим приложением в Windows Azure. Но теперь в игру вступает Windows Azure Active Directory. В настоящем разделе мы называем среду Active Directory, находящуюся внутри помещений, просто Active Directory, а среду Active Directory, размещенную в облаке Azure — Windows Azure Active Directory (WAAD, Windows Azure AD или Azure Active Directory).

Windows Azure Active Directory — это служба, которая предоставляет возможности управления идентичностью и контроля доступа для облачных приложений. Многие онлайновые облачные приложения от Microsoft уже используют Windows Azure AD. Наиболее распространенным из них является Office 365; среди других можно упомянуть Dynamics CRM Online и Windows Intune.

WAAD представляет собой службу со множеством владельцев (tenant), которая способна управлять миллионами компаний, сотней миллионов пользователей и тысячами владельцев на единой платформе. Она оптимизирована для обеспечения высокой доступности и постоянной производительности и для поддержки максимальной масштабируемости. Означает ли это, что вы больше не нуждаетесь в среде Active Directory внутри помещений? И да, и нет. Windows Azure Active Directory может применяться сама по себе, но самый распространенный сценарий заключается в том, что компании интегрируют Windows Azure AD со своими Active Directory внутри помещений. В архитектурном смысле это может рассматриваться как Active Directory в облаке, простирающаяся от текущей среды Active Directory внутри помещений (рис. 7.69).

Благодаря такому расширению из Active Directory внутри помещений в облако, появляется возможность управления пользователями и группами локально с последующей репликацией изменений в WAAD, используя инструмент DirSync, который вскоре будет обсуждаться.

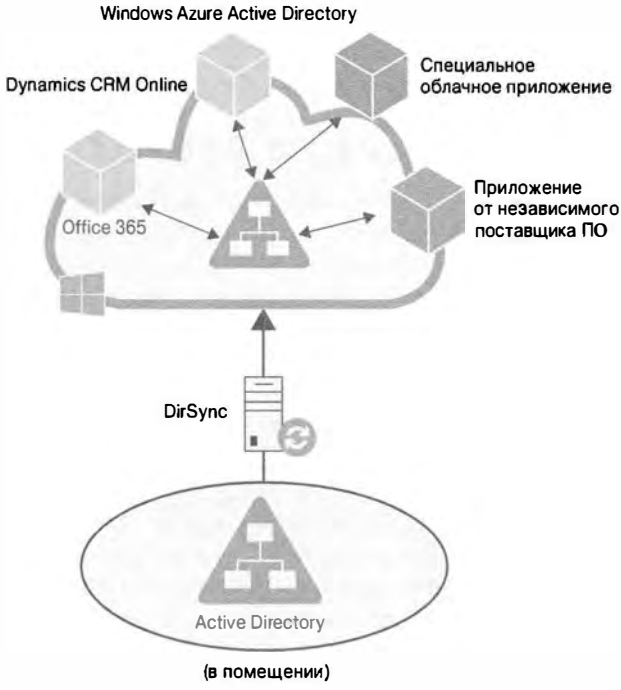


Рис. 7.69. Интеграция Windows Azure Active Directory

С помощью этого механизма вы сможете создать для своих облачных приложений механизм единого входа (single sign-on — SSO). Учтите, что с применением только DirSync вы не получите возможность единого входа. Для SSO в Active Directory, находящейся внутри помещений, необходимо также развернуть службы федерации Active Directory (Active Directory Federation Services — AD FS). За дополнительной информацией обратитесь в раздел "Разновидности входа в Active Directory" далее в главе.

Начало работы с Windows Azure Active Directory

Как получить учетную запись для владельца AD в Windows Azure Active Directory? Простейший способ предусматривает подписку на учетную запись Office 365, вместе с которой вы немедленно обретете Windows Azure Active Directory. Причина в том, что Office 365 использует Windows Azure Active Directory. Другой способ получения WAAD предполагает онлайновую подписку на Windows Azure (`http://www.windowsazure.com/`). Независимо от выбранного метода, вы будете иметь возможность управлять своей учетной записью из обоих порталов.

После подписки на Windows Azure вы можете приступать к управлению своим каталогом (рис. 7.70).

Портал Windows Azure Management (Управление Windows Azure), портал Windows Azure AD, портал Office 365 Account (Учетная запись Office 365), портал Windows Intune Account (Учетная запись Windows Intune) и командлеты PowerShell для Windows Azure читают и записывают в единственный общий экземпляр Windows Azure AD, который ассоциирован с владельцем вашей организации, как показано на рис. 7.71.

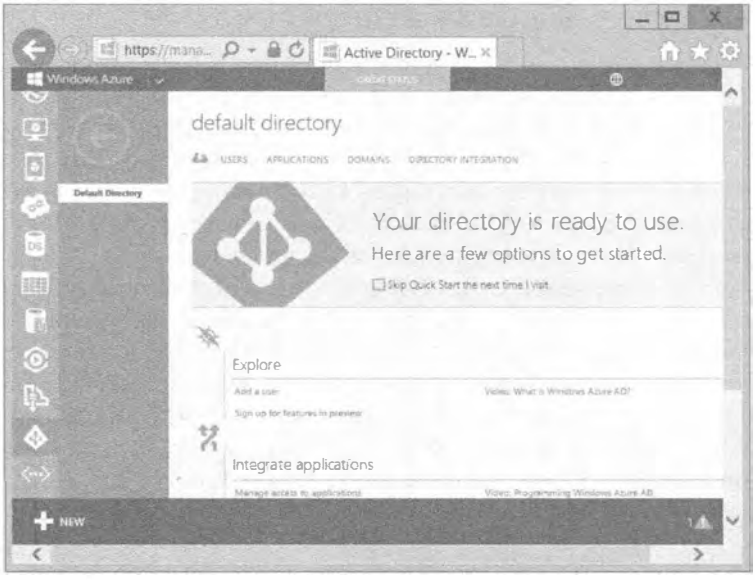


Рис. 7.70. Портал WAAD

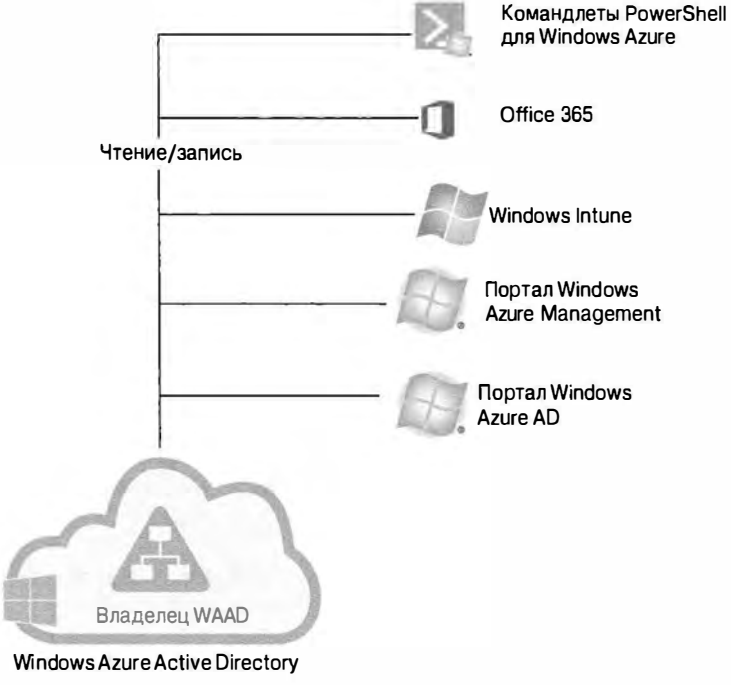


Рис. 7.71. Управление Windows Azure Active Directory

Взаимодействие с Windows Azure Active Directory

Если вы уже знакомы с Active Directory, то, скорее всего, применяли протокол LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам) для запрашивания объектов из каталога. LDAP — это протокол уровня приложений, предназначенный для доступа и обслуживания информации каталога. Тем не менее, вы не можете использовать LDAP для доступа в WAAD, поскольку LDAP не был предназначен для сценария с множеством владельцев. Еще одна проблема связана с тем, что протокол должен быть пригодным к эксплуатации на многих платформах с разнообразными технологиями. По этой причине для доступа в WAAD разработчики из Microsoft построили интерфейс REST (Representational State Transfer — передача репрезентативного состояния). REST является архитектурой, которая использует протокол HTTP для выполнения действий по созданию, чтению, обновлению и удалению (create, read, update, delete — CRUD) с применением методов `GET`, `POST`, `PATCH` и `DELETE`. В Microsoft ссылаются на этот интерфейс REST как на API-интерфейс Windows Azure Active Directory Graph.

С использованием интерфейса такого вида связано несколько преимуществ.

- Независимость от платформы. Любое устройство способно применять HTTP и вызывать HTTP-методы.
- Независимость от языка программирования. Код на любом языке программирования может использовать архитектуру REST для взаимодействия с кодом на других языках программирования; например, код C# может взаимодействовать с кодом Java.
- Базирование на стандартах. Поскольку он выполняется поверх HTTP и основан на стандарте HTTP, API-интерфейс Windows Azure AD Graph может применяться на любой платформе.
- Легкая управляемость. Брандмауэры можно легко сконфигурировать на пропуск трафика HTTP.

Тестирование Windows Azure Active Directory Graph

Чтобы получить представление о том, как работает Graph API, можете опробовать его. В Windows Azure предлагается тестовое приложение под названием Graph Explorer (Проводник по Graph), которое позволяет запускать запросы от имени владельца. Перейдите по ссылке `http://graphexplorer.cloudapp.net/` и зарегистрируйтесь с использованием своей учетной записи Microsoft, после чего щелкните на ссылке Use Demo Company (Использовать демонстрационную компанию) в правом верхнем углу. Ссылка отправит вам тестового владельца (`GraphDir1`) на `https://graph.windows.net/GraphDir1.OnMicrosoft.com`, где вы можете оценить, как выглядит данная технология.

Например, если вы хотите запустить запрос для получения всех пользователей из этого владельца, то просто добавьте выражение **`users`** в конец URL: `https://graph.windows.net/GraphDir1.OnMicrosoft.com/users`. Или же если необходимо возвратить атрибуты пользователя по имени `Daniel@GraphDir1.onmicrosoft.com`, запустите `https://graph.windows.net/GraphDir1.OnMicrosoft.com/users/Daniel@GraphDir1.onmicrosoft.com`.

В верхнем правом углу находится также ссылка Documentation (Документация), которая позволяет перейти к документации по Windows Azure Active Directory Graph.

В Windows Azure Active Directory имеются дополнительные протоколы. REST/HTTP является лишь одним из четырех протоколов, необходимых для доступа и работы с WAAD. В табл. 7.3 приведен краткий обзор стека протоколов и указано назначение каждого из них. В цели этой главы не входит погружение в данные технологии, поэтому мы ограничимся только кратким описанием.

Таблица 7.3. Протоколы Windows Azure Active Directory

Протокол	Назначение
Доступ к каталогу REST/HTTP	Создание, чтение, обновление и удаление объектов и отношений в каталоге
OAuth 2.0	Аутентификация между службами Делегированный доступ
SAML 2.0	Аутентификация веб-приложений Механизм единого входа
WS-Federation 1.3	Аутентификация веб-приложений Механизм единого входа

Синхронизация Windows Azure Active Directory

К этому моменту вы уже имеете определенное представление о том, что такое WAAD, где можно управлять пользователями WAAD и как взаимодействовать с Windows Azure Active Directory. Реальное преимущество WAAD начинает проявляться, когда вы интегрируете WAAD с Active Directory внутри помещений. На показанном ранее рис. 7.69 демонстрировалось высокоуровневая концепция интеграции.

Основная цель — заставить каталог внутри помещений действовать в качестве авторитетного источника данных, чтобы каталог Azure получил всех пользователей, группы и объекты контактов. "Авторитетный источник данных" означает, что вы управляете только своим каталогом внутри помещений, а все внесенные в него изменения переопределяют настройки в Windows Azure AD. Обновления Windows Azure AD выполняются с помощью инструмента под названием DirSync, который позволяет синхронизировать ваши объекты с WAAD и удерживать их в актуальном состоянии с каталогом внутри помещений. После установки инструмент DirSync запускается в фоновом режиме и синхронизирует WAAD раз в несколько часов. Последняя версия DirSync также способна синхронизировать пароли пользователей в облаке. Инструмент DirSync синхронизирует не точные пароли, что создавало бы проблему в плане безопасности, а хеш-значения паролей. Только подумайте, какие преимущества это сулит вашей компании.

Ваши пользователи могут получать доступ к облачным приложениям с применением тех же самых учетных данных, которые они используют в корпоративной сети, развернутой внутри помещений.

Разновидности входа в Active Directory

Мы обсудили два каталога и указали на возможность синхронизации объектов (пользователей, групп и контактов) между каталогом внутри помещений и облаком, включая синхронизацию паролей пользователей с применением DirSync. После синхронизации двух каталогов и развертывания в них приложений вы можете предположить, что механизм единого входа стал доступным, но это не так.

Инструмент DirSync

Инструмент DirSync относительно прост в настройке. Он представляет собой 64-разрядное средство, которое требует наличия SQL Server 2008 R2 Express Edition или полной версии SQL Server. После его установки обычно никаких дополнительных действий предпринимать не придется.

Важно понимать, что если вы собираетесь включить синхронизацию Active Directory, то ваша среда Active Directory внутри помещений станет авторитетным источником данных, и будет перезаписывать изменения, сделанные синхронизированными пользователями в облаке. Существует одно исключение: если вы планируете развертывание Exchange Server в гибридном сценарии, то некоторые атрибуты должны быть записаны в Active Directory внутри помещений. Эти атрибуты описаны в статье базы знаний по адресу `http://support.microsoft.com/kb/2256198/en-us`.

Если вам нужна дополнительная информация по конфигурированию синхронизации каталогов, хорошей отправной точкой послужит следующая статья в TechNet: `http://technet.microsoft.com/ru-ru/library/hh967642.aspx`.

Рис. 7.72. Единый вход в Windows Azure Active Directory

К настоящему времени пользователи могут входить в корпоративную сеть и использовать приложения. При попытке доступа к облачному приложению у них снова будут запрошены учетные данные. Да, учетные данные те же самые, но они не передаются облачному приложению. Такое поведение называется одинаковым входом (same sign-on).

Чтобы получить механизм единого входа, понадобится развернуть службы федерации Active Directory (Active Directory Federation Services — AD FS). Развертывание инфраструктуры AD FS внутри корпоративной сети позволяет установить отношение доверия проверяющей стороны между вашей фермой серверов AD FS и Windows Azure Active Directory. Такое отношение доверия проверяющей стороны делает возможной передачу маркеров аутентификации между корпоративной сетью и Windows Azure AD. На рис. 7.72 показано, как это работает на высоком уровне.

Если вы развернете AD FS в Active Directory, то не только получите действительный единый вход для облачных приложений, но также сможете развернуть механизм двухфакторной аутентификации. Метод двухфакторной аутентификации вынуждает пользователей помимо предоставления своих учетных данных добавлять еще один защитный код, чтобы пройти аутентификацию для приложений Windows Azure. Этот дополнительный код формирует добавочный уровень защиты внутри инфраструктуры.

Чтобы вы получили лучшее представление о доводах за (+) и против (-) каждого уровня развертывания, в табл. 7.4 приведена краткая сводка.

Таблица 7.4. Интеграция с Windows Azure Active Directory

Учетная запись Windows Azure Active Directory	Учетная запись Windows Azure Active Directory + DirSync	Учетная запись Windows Azure Active Directory + DirSync + ADFS
+ Дополнительное конфигурирование не требуется	+ Среда Active Directory внутри помещений является авторитетным источником данных + Пользователь имеет одну пару учетных данных	+ Среда Active Directory внутри помещений является авторитетным источником данных + Механизм единого входа + Двухфакторная аутентификация
– Пользователь имеет две пары учетных данных – Отсутствует механизм единого входа для облачных приложений – Двухфакторная аутентификация не может быть реализована	– Отсутствует механизм единого входа для облачных приложений – Двухфакторная аутентификация не может быть реализована – Инструмент DirSync должен быть установлен на выделенном сервере внутри помещений	– Инструмент DirSync должен быть установлен на выделенном сервере внутри помещений – Ферма серверов AD FS должна быть развернута внутри помещений

В этом разделе был представлен каталог Windows Azure Active Directory и показано, как управлять и интегрировать его в свою среду. Теперь вы должны обладать базовым пониманием большинства важных терминов, необходимых для того, чтобы приступить к работе с WAAD.

Обзор технологии Workplace Join

Современные компании сталкиваются с крупными проблемами, связанными со всем многообразием устройств в своих сетях. Представьте себе консультанта, который привлечен к работе над IT-проектом. Генеральный директор этой компании использует в своей работе iPad. Сотрудникам из отдела маркетинга необходимо презентовать товары на другом устройстве, таком как проектор. Все эти люди применяют свои устройства дома и в офисе, и для всех них не существует устройства, которое можно было бы считать стандартным. Одной общей характеристикой является потребность доступа к определенным ресурсам в сети.

Поскольку все эти устройства требуют доступа к корпоративной сети и приложениям, предоставление безопасного и согласованного способа для обеспечения доступа к нужным ресурсам, а также для управления устройствами и данными было сложной задачей. До сих пор выбирать можно было один из двух вариантов: либо присоединять устройство к Active Directory (если это возможно), либо не присоединять. Оба подхода обладают достоинствами или недостатками для пользователя, получающего доступ к данным и приложениям, а также для управления устройствами. Технология Workplace Join (Подключение к рабочему месту) родилась из политики BYOD (bring-your-own-device — принеси свое собственное устройство), которая разрешает сотрудникам приносить свои персональные устройства на рабочие места и пользоваться ими.

Что собой представляет технология Workplace Join

Технология Workplace Join поставляется в составе Windows Server 2012 R2Ю, а также интегрирована в Windows 8.1; она позволяет своим пользователям получать

доступ к приложениям и данным, где бы они ни были, без присоединения к домену из любого устройства. Вдобавок Workplace Join предлагает пользователям механизм единого входа для корпоративных приложений, и администратор компании по-прежнему может контролировать, кто имеет доступ к ресурсам компании. Конечно, такая тесная интеграция устройств привносит определенные риски, но по этой причине в Microsoft предоставили многофакторную аутентификацию и также добавили к Active Directory Federation Services в Windows Server R2 функциональность для управления этими рисками.

Регистрация очень проста. В зависимости от устройства вы либо регистрируете устройство через URL, либо конфигурируете настройки компьютера. В обоих сценариях для регистрации устройства предоставляется основное имя пользователя (user principal name — UPN), которое во многих компаниях соответствует адресу электронной почты пользователя. После этого клиентское устройство подключается либо изнутри сети компании, либо снаружи (по Интернет) через службу Web Application Proxy компании и выполняется аутентификация пользователя.

Служба Web Application Proxy, появившаяся в Windows Server 2012, является частью службы роли Remote Access, которая позволяет предоставить пользователям вне организации доступ к приложениям, функционирующим на серверах внутри организации. Мощь Web Application Proxy заключается в опубликованных приложениях, которые доступны на любом устройстве. Если учетные данные соответствуют, новая служба в Windows Server 2012 R2 AD FS под названием DRS (Device Registration Service — служба регистрации устройств) зарегистрирует устройство пользователя в Active Directory. Для такой цели в Active Directory был создан новый класс объектов. Этот новый объект устройства может применяться для предоставления условного и детализированного доступа к данным и ресурсам в корпоративной среде. Вы можете считать Workplace Join облегченной версией присоединения к домену (рис. 7.73).

Пользователи, подписавшиеся на это новое средство, не передают полный контроль над устройством администратору, но администратор контроллеров домена Windows Server 2012 R2 может применять набор политик безопасности и проводить ограниченную очистку классифицированных корпоративных данных.

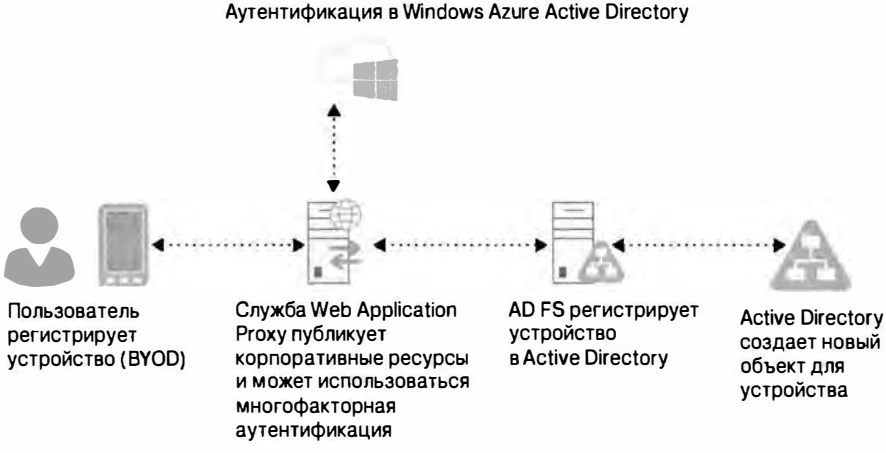


Рис. 7.73. Технология Workplace Join

Это дает администратору хороший контроль над тем, что происходит с корпоративными данными и как к ним производится доступ. С другой стороны, пользователи по-прежнему эксплуатируют свои устройства так, как хотят, а также получают простой и комфортный доступ к сетевым ресурсам.

Начало работы с Workplace Join

Технология Workplace Join является частью Windows Server 2012 R2 и Windows 8.1, поэтому мы предоставили вам краткое введение о том, что собой представляет Workplace Join. Об этой технологии можно рассказать еще многое, но это сильно бы увеличило объем данной книги.

Если вы желаете опробовать Workplace Join в испытательной среде, по следующей ссылке доступно удобное пошаговое руководство (на английском языке) о присоединении устройства iOS и устройства Windows с использованием Workplace Join: `http://technet.microsoft.com/en-us/library/dn452410.aspx`.

Резюме

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?

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?

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?

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.

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?

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?

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?

Глава 8

Создание и управление учетными записями

Вероятно, одной из наиболее распространенных задач, которые администратор будет делать, причем не только во время развертывания, но также на протяжении существования среды Windows Server, является создание и управление учетными записями пользователей. Это звучит как довольно простая задача, однако она очень важна по причинам, связанным с управлением временем и с возможными последствиями в отношении безопасности. Администраторы сервера или консультанты должны хорошо понимать процесс. Им может показаться, что допустимо его проигнорировать, поскольку в обычной своей деятельности администраторы сервера или консультанты не создают учетные записи пользователей. Это может быть и так, но они, как правило, являются теми людьми, которые отвечают за создание первых пользователей в новой сети, определение процессов и передачу операции другой бригаде, отделу либо их потребителям. Те же самые старшие сотрудники также должны иметь возможность создания и управления учетными записями для служб и приложений на своих серверах, следуя передовому опыту.

Мы раскроем основы создания и управления учетными записями пользователей, поэтому любому специалисту найдется, что почерпнуть из этой главы. В любой ситуации, когда доступен только PowerShell, эта глава послужит источником знаний о том, как справиться с подобной ситуацией. Мы покажем, каким образом создавать и управлять учетными записями пользователей из командной строки и PowerShell. Переживать не стоит. В предшествующих главах вы уже видели, что клавиатурные альтернативы иногда позволяют сберечь немало времени и усилий, и в данной ситуации тенденция остается неизменной.

Мы обсудим распространенные свойства и настройки, которые можно конфигурировать для учетных записей пользователей. Мы также рассмотрим группы, причины их использования, методы добавления/удаления пользователей в/из групп, а также рекомендуемые приемы назначения членства в группах. Мы раскроем все эти темы в трех средах: автономная машина Windows Server, установка Server Core и Active Directory.

Мы продемонстрируем опции Windows Server 2012, большая часть которых идентична опциям Windows Server 2008 R2. В Windows Server 2012 доступен ряд новых приемов в форме новой задачи и управляющего инструмента на основе PowerShell, который называется центром администрирования Active Directory (Active Directory Administrative Center) и полностью построен поверх PowerShell. Было добавлено намного больше модулей Active Directory для управления посредством инструмента PowerShell, его процессора командной строки и языка сценариев. Эти темы будут рассмотрены в конце главы. Мы уверены, что после чтения этой главы вы поймете значимость данных инструментов в плане экономии времени.

В этой главе вы изучите следующие темы:

- управление пользователями и группами;
- использование Active Directory Administrative Center в Windows Server 2012;
- управление пользователями и группами с помощью PowerShell.

Совместимость с Windows Server 2012 (R2)

Примите во внимание, что когда мы упоминаем Windows Server 2012, то имеем в виду также и Windows Server 2012 R2; все возможности применимы к обеим версиям.

Создание и управление учетными записями пользователей

В этом разделе будет показано, как создавать, управлять и удалять локальные и доменные учетные записи пользователей. Вы узнаете, как выполнять указанные задачи с применением инструментов администрирования с графическим пользовательским интерфейсом, командной строки и PowerShell, хотя вы должны осознавать, что инструменты командной строки скоро, по всей видимости, выйдут из употребления. В Microsoft собираются усиленно продвигать PowerShell.

Рабочая среда для этой главы содержит контроллер домена по имени `DC01.bigfirm.com` и сервер-член под названием `Server01.bigfirm.com`. Такая среда позволит продемонстрировать методы создания и управления локальными и доменными учетными записями пользователей.

Создание локальных учетных записей пользователей

Первыми мы рассмотрим способы создания локальных учетных записей пользователей. Для управления локальными учетными записями пользователей предусмотрен один главный инструмент — Computer Management (Управление компьютером), который можно открыть из диспетчера серверов, выбрав в меню Tools (Сервис) пункт Computer Management (Управление компьютером). Этот инструмент предоставляет все те же самые опции, что и при управлении пользователями и группами в Windows Server 2008 R2.

Для целей нашего примера войдите в систему на сервере `Server01.bigfirm.com` в качестве администратора, откройте окно Computer Management и раскройте папку `\Local Users and Groups\Users` (Локальные пользователи и группы \ Пользователи), как показано на рис. 8.1.

Вы должны видеть две существующих учетных записи пользователей.

- **`Administrator` (Администратор).** Это стандартная учетная запись пользователя-администратора. Ниже она будет обсуждаться более подробно.
- **`Guest` (Гость).** Назначение этой учетной записи — позволить людям, не имеющим действительной учетной записи пользователя, войти в систему локального компьютера. Такая учетная запись может понадобиться администратору при наличии многочисленных приходящих и уходящих пользователей.

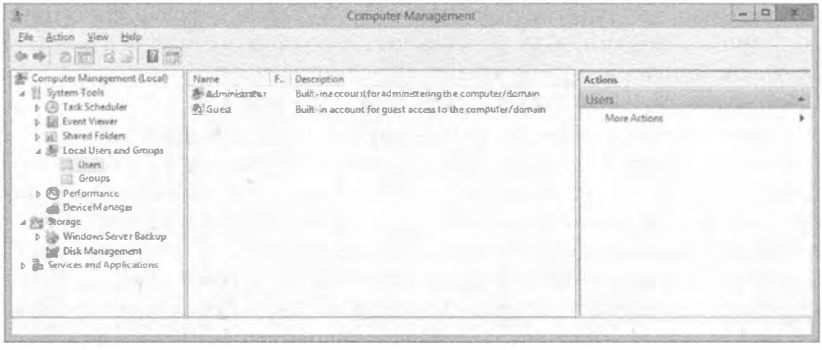


Рис. 8.1. Локальные пользователи в окне Computer Management

Вы заметите, что на значке учетной записи `Guest` имеется изображение небольшой стрелки, указывающей вниз. Причина в том, что согласно рекомендуемым приемам эта учетная запись должна быть отключена и это делается по умолчанию. Наличие учетной записи `Guest` не является распространенным требованием на сервере, поэтому необходимость в ее включении может никогда и не возникнуть.

Пример из практики

Учетная запись `Administrator`

Критически важно защитить учетную запись `Administrator` подходящим для организации способом. Локальная учетная запись `Administrator` имеет полный контроль над сервером, а доменная учетная запись `Administrator` — над всей сетью! Таким образом, для них должны быть выбраны очень строгие пароли.

В крупных организациях `Administrator` представляет собой анонимную учетную запись. Загляните в журналы безопасности с помощью программы просмотра событий (Event Viewer) и задайте себе вопрос: "Как узнать, кто сделал данное действие, используя учетную запись `Administrator`?" Именно поэтому вы должны создать учетную запись пользователя с подходящими административными или делегированными правами для любого администратора, который в них нуждается. Применение стандартной учетной записи `Administrator` часто запрещено, если только не возникла чрезвычайная ситуация. Чтобы обеспечить безошибочный аудит каждого сотрудника отдела IT в журнале безопасности, понадобится создать учетную запись пользователя `Administrator` для каждого администратора. Затем вы должны удостовериться в том, что каждый администратор имеет только те права и разрешения, которые ему необходимы для выполнения своей работы.

В некоторых организациях принимают решение полностью отключить учетную запись Administrator. Такое решение нельзя назвать выдающимся, поскольку эта учетная запись является великолепным "черным входом" на случай блокировки паролей. Пользователь Administrator является таким, который блокировать нельзя. Организации могли бы избрать альтернативный подход. Вы можете думать об этом как о "ядерной" опции. Вы наверняка видели фильмы, по сюжету которых два генерала должны ввести два разных ключа, чтобы запустить ракету с ядерной боеголовкой. Нечто похожее вы можете сделать с паролем учетной записи Administrator. Он может устанавливаться двумя разными особами или даже отделами, причем один вводит первую половину пароля, а другой — вторую половину. Организации, нуждающиеся в опции подобного рода, возможно, располагают отделом IT-безопасности или внутреннего аудита, который владеет первой половиной пароля, в то время как бригаде администраторов сервера оставляется вторая половина.

Последняя опция предполагает переименование учетной записи Administrator. По поводу этой опции ведутся споры, поскольку идентификатор безопасности (security identifier (SID) — код, используемый Windows для уникальной идентификации объекта) учетной записи может быть предсказан, раз вы имеете доступ к серверу или домену. Некоторые утверждают, что переименовывать эту учетную запись нецелесообразно. Однако большинство атак из Интернета в действительности роботизированы, а не интеллектуальны. Они нацелены на типовые имена, такие как SA, root или Administrator, и предпринимают атаки грубой силой, пытаясь угадать пароль. Чтобы защититься от таких форм атак, учетную запись Administrator полезно переименовать.

В конечном счете, применимы те же самые старые правила безопасности. Устанавливайте очень строгие пароли для учетных записей Administrator, сокращайте круг лиц, осведомленных о паролях, ограничивайте удаленный доступ, где только можно, и контролируйте физический доступ к своим серверам.

В рассматриваемом примере мы покажем, как создать учетную запись пользователя для нового сотрудника по имени Steve Red. В папке \Local Users and Groups\Users щелкните правой кнопкой мыши в центральной панели и выберите в контекстном меню пункт New User (Создать пользователя). Откроется диалоговое окно New User (Новый пользователь). Заполните сведения о пользователе в перечисленных ниже полях этого диалогового окна (рис. 8.2).

Рис. 8.2. Создание новой локальной учетной записи пользователя

- **User Name (Имя пользователя).** В этом поле указывается имя, которое пользователь будет вводить при входе в систему. Мы настоятельно рекомендуем внедрить какой-то стандарт именования. Организация меньшего размера может остановиться на имени SRed для сотрудника по Steve Red. Вы можете решить воспользоваться какой-то числовой схемой, к примеру, SRed1SRed, SRedSRed01 или SRed10SRed. Некоторые организации предпринимают дальнейшие действия. Другие применяют в качестве имени пользователя идентификатор сотрудника компании. Еще одни

организации используют инициалы персоны (включая отчество) вместе с числом, к примеру, SMRedl0. Такие более анонимные системы могут оказаться подходящими, когда персональные данные считаются чувствительными.

- **Full Name (Полное имя).** В поле Full Name указывается имя особы, которая будет пользоваться учетной записью. Вряд ли вы решите хранить такие имена на серверах, видимых из Интернета.
- **Password (Пароль).** В поле **Password** необходимо установить пароль. Один из наилучших способов установки пароля предусматривает применение *кодовой фразы* (passphrase). За дополнительными сведениями о кодовых фразах обращайтесь к учебному примеру далее в главе.
- **User Must Change Password at Next Logon (Пользователь должен изменить пароль при следующем входе).** В рассматриваемом примере мы оставляем этот флажок отмеченным. Вы можете установить простой для сообщения пароль вроде "ваша новая кодовая фраза" и оставить флажок User Must Change Password at Next Logon отмеченным (его состояние по умолчанию). Новый пользователь получит возможность войти в систему, но будет *обязан* изменить свой пароль, чтобы завершить процесс входа. Это гарантирует, что ни один из сотрудников отдела IT не будет знать пароль пользователя. Вы заметите, что следующие два флажка отображаются серым цветом и недоступны для использования. Они станут доступными, если снять отметку с флажка User Must Change Password at Next Logon. Указанные флажки противоположны по смыслу.
- **User Cannot Change Password (Пользователь не может изменять пароль).** Вы можете принять решение предотвратить изменение пользователем пароля своей учетной записи. Такая ситуация может возникать при создании учетной записи, которая будет применяться приложением или службой. Отметка этого флажка лишает возможности изменить пароль программу или злоумышленника, атакующего программу.
- **Password Never Expires (Срок действия пароля никогда не истекает).** Отметка флажка Password Never Expires приводит к переопределению любых политик истечения срока действия паролей, которые могут быть установлены где-то в другом месте, например, в локальной системе или в групповой политике. Скорее всего, вы будете использовать эту опцию только для учетных записей служб. Вряд ли вы захотите, чтобы служба наподобие SQL Server прекратила работу по причине истечения срока действия пароля для ее учетной записи.
- **Account Is Disabled (Учетная запись отключена).** Данный флажок должен быть вполне понятен. Когда он отмечен, созданную учетную запись применять нельзя. Это то, что было сделано с учетной записью пользователя Guest. Такое действие также предпринимается при заблаговременном создании учетных записей для пользователей и последующим их включением по мере того, как пользователи действительно приступают к работе.

Вспомните, что установить простой для сообщения пароль можно только для учетной записи пользователя, и это является тем действием, которое сотрудники отдела IT выполняют на регулярной основе. Данная опция защитит такую учетную запись от неавторизованного использования до тех пор, пока сотрудник не начнет работать с ней и изменит пароль по своему усмотрению.

Щелчок на кнопке Create (Создать) приведет к созданию пользователя `SRed` и очистке полей в диалоговом окне New User. Это позволяет быстро добавить дополнительных пользователей, не выбирая снова пункты меню. После создания пользователя щелкните на кнопке Close (Закрыть), чтобы закрыть диалоговое окно New User.

Как показано на рис. 8.3, пользователь теперь создан, и можно продолжить работу с этой учетной записью, чтобы ее использовать в дальнейшем.

Рис. 8.3. Новый пользователь в окне Computer Management

Пример из практики

Случай для кодовых фраз

О кодовых фразах в Microsoft говорят на протяжении уже нескольких лет. О том, какой подход к выбору кодовых фраз считать лучшим, всегда велись дебаты. Люди обычно выбирают пароли, состоящие из семи или восьми символов. Они повышают сложность, применяя заглавные буквы, цифры или символы для усиления пароля. Тем не менее, эта же сложность затрудняет запоминание пароля и его ввод с клавиатуры. В результате служба технической поддержки каждое утро по понедельникам имеет дело с запросами на сброс паролей, поступающими от заблокированных пользователей. Обстоятельства еще больше усложняются, когда пользователи обязаны изменять свои пароли каждые 30 дней, что призвано защитить от возможных взломов этих паролей. Альтернатива заключается в использовании более длинных паролей, таких как 12-символьные, без привнесения дополнительной сложности. Такое удлинение делает пароли математически более строгими. Наверное, вы думаете, что больше никогда не будете сталкиваться по поводу паролей с руководством или пользователями? Подождите немного. Ключом к решению является представление концепции кодовой фразы. До сих пор некоторые люди вводят что-то вроде "November1982-1" и инкрементируют число каждый месяц, когда срок действия пароля истекает. Как насчет того, чтобы предложить пользователям ввести что-нибудь значащее для них или же то, что легко запоминается? Например, владелец желтого спортивного автомобиля мог бы ввести фразу "мой желтый гарцующий пони". Это длинный пароль, но данному человеку его легко запомнить, к тому же его несложно вводить. А вот и дополнительная выгода: пароль является настолько строгим, что вы могли бы разрешить им пользоваться в течение полугода. И такой подход оказался бы популярным! Если вы решили вводить эту политику, то могли бы презентовать концепцию кодовой фразы с применением плакатов, электронной почты, совещаний и тому подобного. Благодаря детализированным политикам паролей, вы можете вводить ее постепенно, привлекая благожелательно настроенных пилотных пользователей, которые помогут распространять добрые слова в ваш адрес.

Создавать пользователей можно также в командной строке. Это полезно при использовании установки Server Core операционной системы Windows Server 2012, но вы можете счесть такой подход удобным также и для изучения методов написания сценариев. Чтобы создать на сервере локального пользователя SRed, запустите следующую команду:

```
C:\Users\administrator>net user SRed1 Skyisblue2013 /ADD
The command completed successfully.
Команда успешно завершена.
```

Ниже приведен синтаксис этой команды:

```
net user <имя создаваемого пользователя> <пароль для установки> /ADD
```

Эта команда создает пользователя на локальном компьютере. По большому счету она ничего другого не делает. Остальные опции, о которых шла речь выше, не используются. Если пароль длиннее 14 символов, будет выдано сообщение о том, что пароли такой длины могут вызвать проблемы в унаследованных системах Windows, и предложено подтвердить свой выбор. Если в пароль необходимо добавить пробелы, его придется поместить в двойные кавычки, например:

```
net user SRED "My d0g is yellow" /ADD
```

Чтобы полностью воссоздать то, что вы делали в окне Computer Management, добавьте к команде несколько опций:

```
net user SRed Skyisblue2013 /fullname: "Steve Red"
  /comment: "Manager of the server team" /logonpasswordchg:yes /add
```

Далее приведены краткие описания всех опций.

- **/fullname**. Назначает учетной записи пользователя имя для будущих ссылок на него.
- **/comment**. Заполняет поле Description (Описание) в окне свойств учетной записи пользователя.
- **/logonpasswordchg:yes**. Заставляет пользователя изменить свой пароль при первом входе в систему сервера.
- Ниже перечислено несколько других опций, которые встречались в окне Computer Management.
- **/passwordchg**. Устанавливается в yes или no для указания, может ли пользователь изменять свой пароль.
- **/expires**. Устанавливается либо в какую-то дату (в формате мм/дд/гг[гг]), либо в NEVER.
- **/active**. Включает или отключает учетную запись.

Чтобы получить дополнительную информацию о других опциях, введите команду **net help user**. Не попадитесь в ловушку, введя вместо этого команду net user /?. Там вы найдете мало сведений.

Создание доменных учетных записей пользователей

Давайте возвратимся к тому, по какой причине вы можете отдать предпочтение доменным учетным записям пользователей перед локальными учетными записями.

Получается так, что пользователю Steve Red нужна возможность входа в системы многих серверов в сети, а не только в данный автономный сервер. Этот пользователь собирается работать с множеством служб, и ему необходим механизм единого входа. Администраторы также хотят настроить только одну учетную запись пользователя и располагать возможностью выдать права лишь одной этой учетной записи. Пользователь Steve Red желает иметь только одну учетную запись и один пароль. Решение выглядит простым — создать доменную учетную запись пользователя.

Чтобы сделать это, войдите в систему контроллера домена (в рассматриваемом примере это DC01.bigfirm.com) и откройте инструмент Active Directory Users and Computers (Пользователи и компьютеры Active Directory), который находится в папке Administrative Tools (Администрирование) на любом контроллере домена. С помощью бесплатно загружаемых инструментов дистанционного администрирования серверов (Remote Server Administration Tools) можно установить этот и другие инструменты управления серверами на компьютере Windows 8, чтобы проводить из него дистанционное управление.

Пример из практики

Разделение администраторов

Одним из решений, которые администраторы Windows не спешат принимать, является концепция разделения ролей на офисных сотрудников и сетевых администраторов. Администраторы Unix делали это десятилетиями, просто применяя команду su. Другими словами, они входили в сеть от имени рядовой учетной записи с нормальными правами пользователя и поднимали привилегии до более высокой учетной записи, когда требовалось выполнять работы по администрированию. Зачем это может понадобиться? Все очень просто. Представьте, что вы блуждаете по Интернету или читаете свою электронную почту. В это время фрагмент вредоносного ПО ускользнул от защитных механизмов и выполнился. От имени кого он будет запущен? Все верно, от имени вашей учетной записи. Что остановит его от наведения беспорядка в корпоративной сети, если вы вошли как администратор домена или от имени другой привилегированной учетной записи? Ровным счетом ничего! В Windows предлагается определенная защита посредством системы контроля пользовательских учетных записей (User Account Control — UAC), но эта защита не идеальна. Подобно физической защите, иногда простейшие решения оказываются наилучшими.

Решение довольно-таки простое и не настолько устрашающее, как могут вообразить себе многие администраторы Windows, когда слышат о нем. Сотрудники с административными правами должны иметь по две учетных записи. Первая учетная запись будет предназначена для повседневной офисной работы, такой как использование Microsoft Word, путешествия по Интернету или чтение электронной почты. Вторая учетная запись предназначена для выполнения работ по администрированию. Именно в этот момент люди начинают протестующе размахивать руками. Но дайте нам закончить — очень скоро вы увидите, насколько все это просто в действии.

Предположим, что вы настраиваете такой сценарий для пользователя Steve Red. Его обычной ежедневной учетной записью является SRed, под которой он входит в систему на компьютере для выполнения работы, не связанной с администрированием. Вы также настроили еще одну учетную запись, которая имеет права на управление частями Active Directory, определенными серверами и рабочими станциями в офисе.

Эта учетная запись называется SRed-Admin. Вы могли бы применить детализированную политику паролей, обеспечив более строгие требования для административной учетной записи, но вы решили оставить всех с кодовыми фразами. Это вполне безопасно.

Каким образом пользователю Steve Red переключаться между разными ролями в течение дня? Вот как звучит распространенный аргумент против разделения администраторов: "Я не хочу постоянно выходить и потом снова входить в систему". Справиться с данной проблемой можно несколькими путями.

Вы располагаете возможностью использовать средство Run As (Запуск от имени) для запуска программ из-под других учетных записей пользователей. В Microsoft Windows Server и в клиентских ОС Windows программы можно запускать от имени пользователя, отличающегося от текущего, под которым был совершен вход в систему. Это средство известно под названием Run As. Вы должны выполнить следующие базовые шаги.

1. Отыщите программу, которую нужно запустить.
2. Удерживая нажатой клавишу <Shift>, щелкните правой кнопкой мыши на значке программы и выберите в контекстном меню пункт Run as different user (Запуск от имени другого пользователя).
3. Введите учетные данные пользователя, от имени которого хотите запустить программу.

Некоторые организации применяли такой прием и даже изменяли ярлыки для административных оснасток консоли MMC в папке Administrative Tools, чтобы делать это по умолчанию. Операционные системы Windows 8 и Windows Server 2012 позволяют быстро переключать пользователей без необходимости в выходе из системы.

Существуют и другие подходы к обеспечению решения. Некоторые подходы в прошлом использовали продукты виртуализации презентаций от Citrix для предоставления среды администрирования. Теперь службы удаленного рабочего стола (Remote Desktop Services) в Windows Server 2008 R2/2012 могут легко дублировать такой подход, публикуя либо рабочие столы, либо приложения для компьютеров пользователей. Или же можно было бы предложить вариацию решения виртуального административного ПК, запустив такой виртуальный ПК на клиенте Windows 8 Client; он уже располагает полнофункциональным продуктом Windows Server Hyper-V 3.0. Финальным реализуемым решением являются серверы управления. Это выделенные серверы Windows, предназначенные специально для управления IT-инфраструктурой. Все необходимые инструменты устанавливаются и открываются для совместного использования любым администратором, которому необходимо управлять серверами. Крупное преимущество этого подхода состоит в том, что на таких серверах управления можно заблокировать подключение к Интернету, а за счет определения соответствующих правил доступа в брандмауэре обеспечить, что только этим серверам управления разрешено управлять остальными серверами. Администратору придется только подключаться к этим серверам управления с применением протокола удаленного рабочего стола (Remote Desktop Protocol — RDP).

Теперь вы должны понимать необходимость в разделении двух жизненных аспектов администратора и убедиться, что не все решения трудны; на самом деле они могут благотворно влиять на экономию времени и усилий.

На рис. 8.4 показано окно Active Directory Users and Computers с контейнером Users (Пользователи), содержащим несколько встроенных пользователей и групп, которые являются важными для функционирования Active Directory.

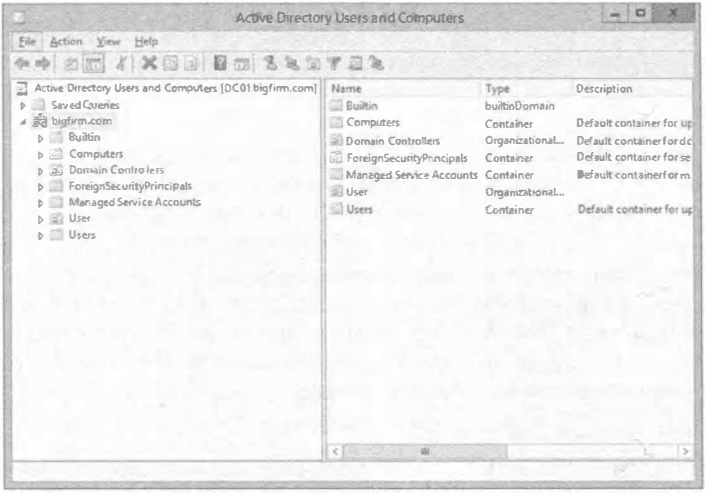


Рис. 8.4. Окно Active Directory Users and Computers

Одни из них используются сейчас, а другие будут применяться, когда вы развернете другую функциональность в сети. Нередко в данный контейнер помещают создаваемые учетные записи пользователей. Это значит, что отделить ваши обычные учетные записи пользователей от встроенных учетных записей становится труднее, равно как усложняется применение политик и делегирование прав администрирования. Мы бы хотели, чтобы в Microsoft решили использовать для этого контейнера другое имя. Решение особой сложностью не отличается.

1. Создайте в корне домена еще одну организационную единицу (OU), обычно имеющую имя домена или организации. В этом случае создается OU по имени `BigFirm` под `bigfirm.com`.
2. Создайте архитектуру организационных единиц, чтобы соответствовать политике и административной иерархии организации внутри этого домена. Вы имеете организацию с единственным сайтом, поэтому выполните следующие шаги.

   а. Создайте организационную единицу для пользователей (`Users`).

   б. Создайте вторую организационную единицу для компьютеров (`Computers`).

   в. Создайте третью организационную единицу для групп доступа (`Security Groups`).

   Решение показано на рис. 8.5. Оно позволяет назначить права доступа объектам каждого типа с детализированным контролем и трактовать их по-разному. Вы создадите пользователей в `OU\BigFirm\Users` внутри домена `bigfirm.com`.
3. Перейдите в организационную единицу, где вы хотите создать нового пользователя.
4. Щелкните правой кнопкой мыши на имени организационной единицы и выберите в контекстном меню пункт New⇨User (Создать⇨Пользователь), чтобы создать пользователя. Запустится мастер создания нового объекта-пользователя (New Object — User Wizard).

   Как видите, все довольно просто.

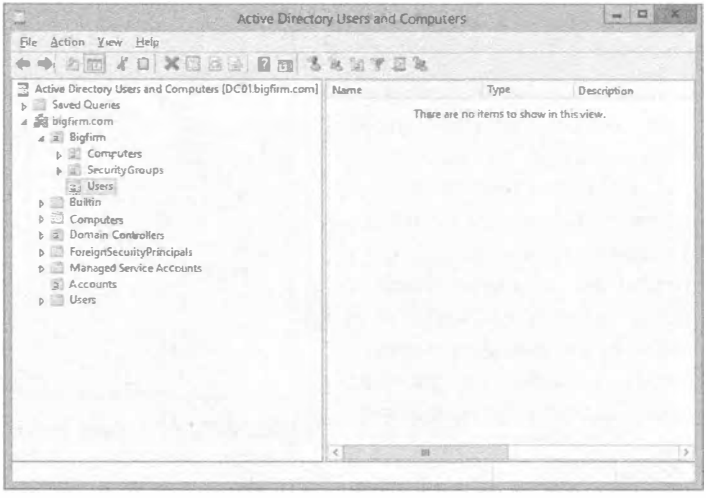


Рис. 8.5. Организационная единица `Users`

5. Введите имя и фамилию пользователя.

   Это приведет к автоматическому заполнению полного имени, которое при желании можно изменить.

6. Введите имя для входа, такое как **SRed** (рис. 8.6).

   Возможно, это самое подходящее время для напоминания базовой терминологии тем, кто не знаком с Active Directory и управлением учетными записями пользователей. Каждый пользователь имеет имена двух типов, с помощью которых он может получать доступ к ресурсам в сети.

   Входное имя пользователя. Это имя, которое вы знаете лучше других, такое как `SRed`.

   Основное имя пользователя (user principal name — UPN). Это имя пользователя, которое выглядит похожим на адрес электронной почты. На рис. 8.6 видно, что именем UPN для пользователя `Steve Red` является `SRed@bigfirm.com`. Суффикс UPN (`@bigfirm.com`) по умолчанию выводится из имени домена. В нашем сценарии это `bigfirm.com`. Обратите внимание, что суффиксы UPN можно добавлять к лесу Active Directory, следуя инструкциям, которые доступны по ссылке `http://support.microsoft.com/kb/243629`.

   Входное имя пользователя, которое было сохранено ради обратной совместимости, выглядит как `SRed`. Вы также видите имя пользователя для версий, предшествующих Windows 2000 Server — `Bigfirm\SRed`. Как ни странно, это имя пользователя для версий, предшествующих Windows 2000 Server, является в точности тем именем, кото-

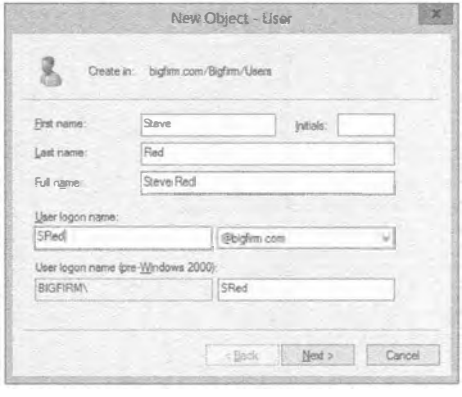


Рис. 8.6. Создание нового пользователя Active Directory

рое пользователю предлагается ввести для входа в домен.

7. Щелкните на кнопке **Next** (Далее) для перехода на экран, показанный на рис. 8.7. Опции на этом экране подобны тем, которые доступны для локальной учетной записи пользователя. Они были описаны ранее, когда рассматривалось создание локальной учетной записи пользователя. Распространенная ошибка здесь — ввести пароль, который не удовлетворяет определенным требованиям к сложности.

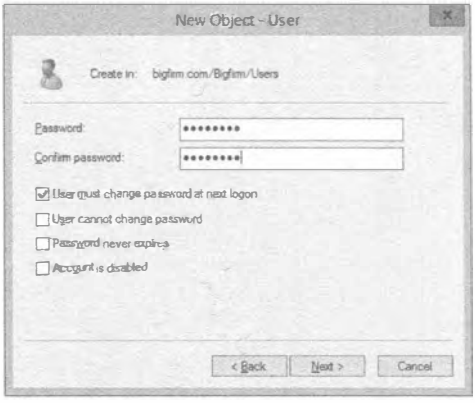


Рис. 8.7. Установка пароля для нового пользователя AD

Стандартные настройки определены в стандартной политике домена (Default Domain Policy). Возможно, вы настроили их посредством другого объекта политики. Пока требования не будут удовлетворены, мастер не сможет быть завершен.

8. Завершите мастер, чтобы создать учетную запись пользователя.

На рис. 8.8 видно, что пользователь создан и находится в организационной единице `\BigFirm\Users`. Довольно просто, не так ли? Давайте посмотрим, как сделать то же самое в командной строке.

Первой командой, которую мы опишем, является `dsadd`. Следующая команда создаст такую же учетную запись пользователя, как это делалось с помощью графического пользовательского интерфейса:

```
dsadd user "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-samid SRed -upn SRed@bigfirm.com -fn Steve -ln Red -display "Steve Red"
-pwd Mydogisblu3 -mustchpwd yes
```

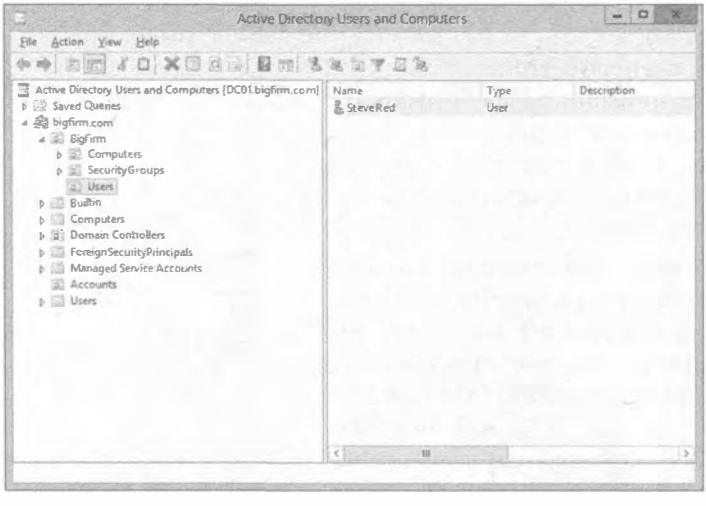


Рис. 8.8. Новый пользователь в Active Directory

Ниже приведен синтаксис этой команды:

```
dsadd user <отличительное имя пользователя>
  -samid <входное имя пользователя>
  -upn <основное имя пользователя> -fn <имя> -ln <фамилия>
  -display <полное имя> -pwd <пароль>
  -mustchpwd <пользователь должен изменить свой пароль при первом входе в
систему: yes (да) или no (нет)>
```

Что собой представляет отличительное имя (distinguished name — DN)? Имя DN описывает, где объект пользователя создается в Active Directory и как он именуется. В данном случае имя DN выглядит так: `CN=Steve Red,OU=Users,OU=BigFirm, DC=bigfirm,DC=com`. Рассмотрим его составные части.

- **Общее имя (Common Name — CN).** Это имя объекта. В этом случае оно представляет собой имя объекта пользователя.
- **Организационная единица (Organization Unit — OU).** Для определения пути `\BigFirm\Users` используется несколько таких частей. В имени DN путь указывается в обратном порядке: `CN=Steve Red,OU=Users,OU=BigFirm`.
- **Компонент домена (Domain Component — DC).** Описывает имя домена, например, `bigfirm.com`. Обратите внимание, что оно *не* указывается в обратном порядке.

Чтобы получить дополнительную справочную информацию по созданию пользователей с помощью команды `dsadd`, введите **`dsadd user /?`**. Вероятно, вы видели, что команда `net user` имеет опцию `/domain`. Возможно, теперь вы думаете, что эта команда была проще, и интересуетесь, по какой причине она не применяется здесь. Дело в том, что команда `net user` не позволяет указать, где именно в домене должен быть создан объект пользователя. Пользователя необходимо создать в `\BigFirm\Users`, и команда `dsadd` дает возможность сделать это. А теперь посмотрим, что было создано, и каким образом управлять учетными записями пользователей.

Установка свойств локальной учетной записи пользователя

Щелкните правой кнопкой мыши на учетной записи пользователя `Steve Red`, созданной на сервере-члене `Server01`, и выберите в контекстном меню пункт Properties (Свойства). Откроется диалоговое окно свойств, показанное на рис. 8.9. Это диалоговое окно должно выглядеть очень знакомым. Здесь присутствуют настройки, которые вы определили для учетной записи пользователя при ее создании. Недоступный флажок Account is locked out (Учетная запись заблокирована) будет доступным и отмеченным, если пользователь окажется заблокированным. Учетная запись блокируется, если политика паролей определяет, что это должно произойти после установленного количества неудавшихся попыток ввода

Рис. 8.9. Общие свойства локального пользователя

пароля в рамках заданного промежутка времени. По умолчанию это определено в Default Domain Policy. Обратите внимание, что флажком Account is locked out нельзя пользоваться до тех пор, пока учетная запись пользователя не станет заблокированной; диалоговое окно свойств не может применяться для блокировки пользователя. В последующих разделах рассматриваются свойства объекта пользователя и разнообразные атрибуты локальной учетной записи пользователя.

Вкладка Member Of

Вкладка Member Of (Членство в группах) используется для управления членством в группах данной учетной записи пользователя (рис. 8.10). Мы еще вернемся к этой вкладке после того, как раскроем понятие групп далее в главе.

Вкладка Profile

Вкладка Profile (Профиль), представленная на рис. 8.11, применяется для управления несколькими настройками.

- **Profile Path (Путь к профилю).** Данная настройка указывает местоположение, где находится профиль пользователя. *Профиль* — это структура папок, содержащая настройки, которые являются уникальными для данного пользователя. Он также включает такие вещи, как папки `My Documents` (Мои документы) и `Favorites` (Избранное) пользователя.
- **Logon Script (Сценарий входа).** Эта настройка позволяет определить сценарий, который сохраняется на контроллерах домена и запускается каждый раз, когда пользователь входит в систему. Для локальной учетной записи пользователя сценарий входа может храниться локально.
- **Home Folder (Домашняя папка).** Данная настройка позволяет определить сетевой диск, который выделяется данному пользователю и отображается на указанную букву диска после входа пользователя в систему.

Рис. 8.10. Членство в группе локального пользователя

Рис. 8.11. Настройки профиля локального пользователя

Простой способ получения имени DN

Администраторы иногда могут быть достаточно ленивыми, чтобы вручную вводить имя DN организационной единицы с клавиатуры. Ниже описан альтернативный способ.

1. Откройте окно Active Directory Users and Computers.
2. Отметьте в меню View (Вид) пункт Advanced Features (Дополнительные возможности).
3. В оснастке станут видимыми многие дополнительные элементы.
4. Перейдите к организационной единице, имя DN которой нужно узнать, и откройте окно ее свойств.
5. Щелкните на вкладке Attribute Editor (Редактор атрибутов) и прокрутите список Attributes (Атрибуты) вниз до появления атрибута `distinguishedName`, как показано ниже.

6. Дважды щелкните на `distinguishedName` и скопируйте имя DN для дальнейшего использования.

Совсем недавно упоминались профили. Все очень просто: администратор создает для пользователя папку, в которую будут автоматически сохраняться персональные данные и настройки пользователя, и открывает общий доступ к этой папке на файловом сервере. Она будет иметь такие разрешения безопасности, что получать к ней доступ могут только соответствующий пользователь (а также локальная система и локальные администраторы). Это позволит профилю пользователя храниться в данном месте после выхода пользователя из системы и загружаться, когда он входит в систему.

Примером такой папки может служить `\\DC01\profiles\SRed`.

Ниже описаны составные части.

- `DC01` — файловый сервер.
- `profiles` — открытая папка.

  Все аутентифицированные пользователи могут производить чтение и запись в этот открытый ресурс. Папка в файловой системе разрешает чтение своего содержимого только пользователям, прошедшим аутентификацию. Локальные администраторы, скорее всего, будут иметь полный доступ к этому открытому ресурсу и папке. Вы можете сделать такой открытый ресурс невидимым при просмотре сети, назначив ему имя `Profiles$`.
- `SRed` — папка, которая создана для хранения профиля пользователя по имени `Steve Red`.

  Разрешение безопасности Modify (Изменение) для этой папки позволяет читать и записывать в нее только пользователю по имени `Steve Red`. Администраторы файлового сервера и системы будут иметь к ней полный доступ.

Рис. 8.12. Настройки среды локального пользователя

Вкладка Environment

Вкладка Environment (Среда), показанная на рис. 8.12, управляет тем, как рабочая среда конфигурируется, когда пользователь входит в систему сервера с применением терминальных служб Windows Server 2008 (Terminal Services) или служб удаленных рабочих столов Windows Server 2012 (Remote Desktop Services), например, за счет использования клиента подключения к удаленному рабочему столу (Remote Desktop Connection). Вы можете сконфигурировать определенную программу на запуск при каждом входе пользователя, отметив флажок Start the following program at logon (Запустить при входе следующую программу). При этом понадобится ввести команду для запуска программы и указать папку, которая будет для программы стартовой. Клиент Remote Desktop Connection позволяет пользователю выбрать отображение своих локальных дисков и принтеров, а также конфигурировать печатные задания для использования сервером стандартного принтера клиентского компьютера. Администраторы могут дополнительно управлять этими опциями на данной вкладке.

Remote Desktop Services или Terminal Services

Функциональность Terminal Services в Windows Server 2012 расширена с целью включения инфраструктуры виртуальных рабочих столов. В Microsoft провели ребрендинг служб Terminal Services из Windows Server 2008 R2, которые получили название Remote Desktop Services (RDS), сохранив их и в версии Windows Server 2012. Может возникнуть небольшая путаница, если вы читаете эту главу и все еще работаете в среде Windows Server 2008. Просто запомните, что когда мы ссылаемся на Remote Desktop Services, то обычно имеем в виду также и Terminal Services в Windows Server 2008/2012.

Вкладка Sessions

Вкладка Sessions представлена на рис. 8.13. С ее помощью также можно управлять тем, как службы Remote Desktop Services будут функционировать для данного пользователя. Сеанс пользователя на сервере будет оставаться в отключенном состоянии, если пользователь решил не выходить из системы. Это значит, что сеанс продолжит использовать ресурсы, а программы продолжат выполнение. Более важно то, что будут потребляться два свободно доступных параллельных сеанса, которые используются администраторами на серверах. Забывчивые администраторы могут быстро задействовать оба эти сеанса, что будет препятствовать нормальному входу на серверы другим администраторам посредством клиента Remote Desktop Connection. Следует отметить, что администраторы могут завершать такие сеансы с применением диспетчера служб удаленных рабочих столов (Remote Desktop Services Manager) либо локально, либо с удаленного компьютера.

Рис. 8.13. Вкладка Sessions для локального пользователя

Можно обеспечить принудительное завершение отключенных сеансов через указанное время. Хотя эффективнее сконфигурировать это централизованно с использованием средства настройки хост-сервера сеансов удаленных рабочих столов (Windows Server 2012 Remote Desktop Services Configuration), принудительное завершение может быть установлено для каждого пользователя индивидуально с помощью раскрывающегося списка End a disconnected session (Прекратить отключенный сеанс) на вкладке Sessions.

Ценные сеансы администрирования можно делать более доступными, ограничивая длительность сеанса администратора. Максимальное время указывается в раскрывающемся списке Active session limit (Предел для активного сеанса).

Простаивающие сеансы могут быть завершены автоматически путем выбора промежутка времени в раскрывающемся списке Idle session limit (Предел для простаивающего сеанса).

В качестве действия завершения для Idle session limit и Active session limit может быть выбрано либо Disconnect from session (Отключиться от сеанса), т.е. сеанс продолжает выполняться, но не в интерактивном режиме, либо End session (Прекратить сеанс). Пользователь может повторно подключиться к отключенному сеансу, чтобы продолжить выполняемую ранее работу. Это очень удобно в следующих ситуациях:

- сеанс стал отключенным из-за выхода из строя сети между клиентом и сервером;
- пользователь или администратор мог преднамеренно отключить сеанс, оставив какую-то задачу в функционирующем состоянии безо всякого взаимодействия.

В нижней части вкладки Sessions видно, что допускается управлять тем, каким образом пользователь может повторно подключаться к отключенному сеансу. На выбор доступны варианты From any client (Из любого клиента) и From originating client only (Только из первоначального клиента). Второй вариант может применяться из соображений безопасности, однако он довольно ограничен.

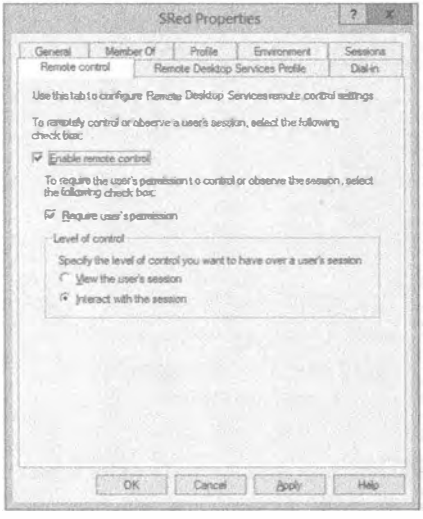


Рис. 8.14. Вкладка Remote Control для локального пользователя

Вкладка Remote Control

Вкладка Remote Control (Удаленное управление), показанная на рис. 8.14, позволяет администраторам управлять тем, как администратор может взаимодействовать с сеансом Remote Desktop Services пользователя. Концепция заключается в том, что администратор может присоединяться к сеансу пользователя, чтобы помочь ему в выполнении какой-то задачи.

По умолчанию удаленное управление включено. Возможно, какому-то пользователю никогда не потребуется удаленное управление. Чтобы отключить его, снимите отметку с флажка Enable remote control (Включить удаленное управление).

Концепция удаленного управления может звучать так, как будто бы оно происходит исподтишка. Тем не менее, по умолчанию пользователю выдается запрос, разрешает ли он попытку удаленного управления со стороны администратора. Если снять отметку с флажка Require user's permission (Требуется разрешение пользователя), то пользователь никогда не будет вовлечен в данный процесс.

Если вы разрешили удаленное управление, то можете сконфигурировать уровень взаимодействия, который администратор будет иметь с сеансом пользователя. Его можно установить так, чтобы администратор имел возможность только просматривать сеанс пользователя; другими словами, располагать доступом только для чтения без какого-либо управления. По умолчанию разрешен интерактивный сеанс, при котором администратор может использовать мышь и клавиатуру в сеансе пользователя.

Вкладка Remote Desktop Services Profile

Вкладка Remote Desktop Services Profile (Профиль служб удаленных рабочих столов), приведенная на рис. 8.15, дает возможность указать специальный профиль для применения, когда пользователь войдет в систему с помощью Remote Desktop Services. Это позволяет администраторам предоставлять выделенный профиль Remote Desktop Services или даже ограниченный профиль для данного сеанса пользователя, который называется *обязательным профилем*. Путь к специальному профилю будет логически помещен в поле Profile Path (Путь к профилю).

Можно также предложить этому профилю специальную домашнюю папку для хранения персональной информации, если он подключается к серверу с использованием Terminal Services.

В нижней части вкладки вы заметите флажок, отметив который, можно запретить вход в систему сервера через Terminal Services. Вы можете решить поступать так в отношении учетных записей, применяемых для служб. Это означает, что даже если пароль учетной записи окажется скомпрометированным, она не может быть использована злоумышленником через Remote Desktop.

Вкладка Dial-in

Вкладка Dial-in (Дозвон), показанная на рис. 8.16, позволяет администратору управлять тем, может ли пользователь дистанционно подключаться к этому серверу и каким образом, например, создавая туннель VPN или применяя модем для дозвона.

Как вы, вероятно, уже заметили вносить изменения в любое свойство внутри этого диалогового окна очень легко, используя оснастку Active Directory Users and Computers. Посредством команды `net user` можно управлять только *некоторыми* из этих настроек. Давайте рассмотрим несколько из них. Следующая команда изменит полное имя локальной учетной записи пользователя:

```
net user SRed /fullname:"Steve Red"
```

А эта команда установит путь к домашней папке:

```
net user SRed /homedir:"D:\Home\SRed"
```

До действительного запуска команды необходимо удостовериться в корректности этого пути, поскольку сама команда его не проверяет. Понадобится также верифицировать разрешения для данного пользователя.

Показанная ниже команда конфигурирует настройку пути к профилю для пользователя:

```
net user SRed /profilepath:"D:\Profiles\SRed"
```

Опять-таки, команда не осуществляет проверку на предмет ошибок, поэтому вы должны сначала убедиться в правильности пути и разрешений.

Рис. 8.15. Вкладка Remote Desktop Services Profile для локального пользователя

Рис. 8.16. Вкладка Dial-in для локального пользователя

Установка свойств доменной учетной записи пользователя

Давайте посмотрим, чем отличается установка свойств доменной учетной записи пользователя от недавно описанной установки свойств локальной учетной записи пользователя.

1. Войдите в систему контроллера домена `DC01.bigfirm.com`.
2. Найдите объект пользователя.
3. Щелкните правой кнопкой мыши на имени объекта пользователя и выберите в контекстном меню пункт Properties (Свойства).

   Обратите внимание, что вы должны отметить пункт Advanced Features (Дополнительные возможности) в меню View (Вид) оснастки Active Directory Users and Computers (ADUC). Диалоговое окно свойств пользователя показано на рис. 8.17.
4. Снимите отметку с пункта Advanced Features в меню View оснастки ADUC и ознакомьтесь со сравнительными характеристиками, приведенными в последующих разделах.

Вы заметите, что расширенное представление предлагает намного больше возможностей. Здесь следует упомянуть два момента.

- В диалоговом окне свойств для доменной учетной записи пользователя имеется намного больше вкладок с множеством настроек, чем в аналогичном окне для локальной учетной записи пользователя.

  Доменная учетная запись предоставляет администраторам намного больший контроль над пользователями. Она также позволяет сохранять для каждой учетной записи пользователя дополнительную информацию, которая может применяться пользователями или приложениями.
- Локальные и доменные учетные записи пользователей разделяют между собой множество общих настроек.

Мы не собираемся здесь повторять описание этих настроек, а предполагаем, что вы читали предшествующие разделы, посвященные локальным учетным записям пользователей.

Давайте начнем с рассмотрения вкладки General (Общие).

Вкладка General

На рис. 8.17 вы видели описательную информацию для пользователя — обычные имя и фамилию. У вас также имеется возможность хранить в объекте пользователя внутри Active Directory и другие сведения о пользователе, такие как офис, где он работает, телефонный номер, адрес электронной почты и адрес веб-страницы. Вы обнаружите, что можете использовать настройки адреса электронной почты или веб-страницы для данного пользователя, щелкнув правой кнопкой мыши на объекте пользователя в оснастке Active Directory Users and Computers. Это дает возможность открыть веб-страницу пользователя или отправить сообщение по его адресу электронной почты.

Рис. 8.17. Свойства учетной записи пользователя Active Directory

Рис. 8.18. Вкладка Address для пользователя Active Directory

Вкладка Address

Вкладка Address (Адрес) представлена на рис. 8.18. Она позволяет определить почтовый адрес для заданного пользователя. Зачем это может понадобиться? Среда Active Directory может применяться в качестве каталога для пользователей; другими словами, пользователи могут ее использовать для выяснения информации о других пользователях в сети или же она может применяться приложениями для сохранения, извлечения и распространения информации среди пользователей.

Вкладка Account

На вкладке Account (Учетная запись), показанной на рис. 8.19, можно видеть входное имя пользователя, имя UPN, а также входное имя пользователя для версий, предшествующих Windows 2000 Server, которые были установлены во время создания пользователя. На данной вкладке все эти имена можно изменить.

Щелчок на кнопке Logon Hours (Часы входа) приводит к открытию диалогового окна Logon Hours (Часы входа), представленного на рис. 8.20. Оно позволяет управлять тем, когда пользователь может входить в сеть для доступа к ресурсам. Это может понадобиться при наличии исключительно строгих требований к безопасности. Данная настройка конфигурируется не особенно часто.

Рис. 8.19. Вкладка Account для пользователя Active Directory

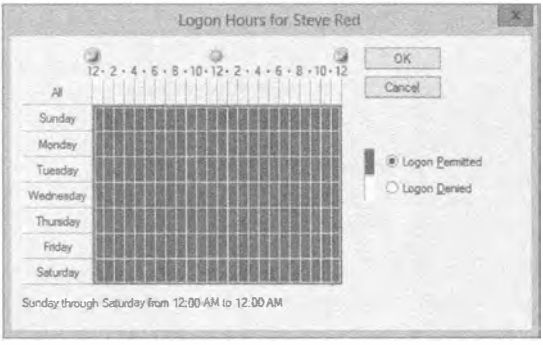


Рис. 8.20. Диалоговое окно Logon Hours для пользователя Active Directory

Рис. 8.21. Диалоговое окно Logon Workstations для пользователя Active Directory

На вкладке Account имеется также кнопка Log On To (Входить в), щелчок на которой приводит к открытию диалогового окна Logon Workstations (Рабочие станции для входа), показанного на рис. 8.21.

Диалоговое окно Logon Workstations позволяет управлять тем, какие компьютеры данный пользователь может применять для входа в Active Directory. Это может быть необходимым в нескольких случаях.

- Нужен контроль над тем, где некоторые или даже все пользователи совершают вход в систему. Это определенно нестандартный вариант конфигурации, но уровень безопасности, принятый в определенных организациях, может того требовать.
- К вам приходит консультант или технический специалист, и вы хотите ограничить круг компьютеров, на которых он должен работать.
- Вы создаете учетную запись для приложения или службы и хотите, чтобы она использовалась только на определенных серверах. Это ограничит ущерб (хотя и временно), который может быть нанесен в случае компрометации данной учетной записи.

Настройки, доступные посредством кнопок Log On To и Logon Hours на вкладке Account, могут применяться вместе для исполнения ограничений входа в систему, принятых в отношении доменной учетной записи пользователя.

Вернемся снова к рис. 8.19. Обратили ли вы внимание на множество других опций для управления учетной записью? Чтобы увидеть их, придется прокрутить вниз список Account options (Параметры учетной записи), находящийся в середине вкладки Account диалогового окна.

- **User Must Change Password at Next Logon (Пользователь должен изменить пароль при следующем входе).** Применяется для того, чтобы заставить пользователя изменить свой пароль после того, как администратор установит или сбросит его. Это значит, что администратор не должен знать, что пользователь выбрал в качестве пароля.

- **User Cannot Change Password (Пользователь не может изменять пароль).** Используется для учетных записей служб, чтобы гарантировать неизменность пароля.
- **Password Never Expires (Срок действия пароля никогда не истекает).** Переопределяет любые политики устаревания паролей, которые могут быть сконфигурированы в Active Directory. В идеале применяется для учетных записей служб, а не рядовых пользователей.
- **Store Password Using Reversible Encryption (Сохранять пароли с использованием обратимого шифрования).** Никогда не отмечайте данный флажок, если только не имеете стопроцентную уверенность в том, что данное действие необходимо. Это требуется, когда приложению нужно знать пароль пользователя в целях аутентификации. В Microsoft говорят, что это в точности то же самое, что и хранение пароля в виде простого текста.
- **Account Is Disabled (Учетная запись отключена).** Администратор может отключить учетную запись пользователя, чтобы устранить возможность аутентификации или авторизации с ее помощью.
- **Smart Card Is Required for Interactive Logon (Для интерактивного входа требуется смарт-карта).** Среду Active Directory можно сконфигурировать так, чтобы пользователям было разрешено входит в сеть только при наличии у них *смарт-карт*. Такой подход называется *двухфакторной аутентификацией*. Другими словами, пользователь применяет для входа то, чем он располагает (уникальный маркер), и то, что ему известно (секретный PIN-код). Этот подход считается намного лучшим решением аутентификации, чем пароли и кодовые фразы, по следующим причинам.
  - Маркером затруднительно поделиться или похитить.

    Смарт-карта является уникальной, и ее владельцу сразу станет известным факт ее похищения, а в случае передачи ее кому-то другому владелец сам не сможет войти в сеть.
  - Используется простой для запоминания PIN-код. Кроме того, применяются механизмы очень строгого шифрования.

    Это означает, что пользователь не имеет дела с часто изменяемыми паролями, которые являются распространенной причиной для беспокойств из-за того, что сложные пароли нередко забываются.

  Потребность в усиленной безопасности может побудить администраторов к внедрению смарт-карт для некоторых или даже для всех пользователей. Отметка флажка Smart Card Is Required for Interactive Logon вынудит пользователей входить в сеть с применением выданных им смарт-карт и запретит вход с предоставлением традиционных имени пользователя и пароля.
- **Account Is Sensitive and Cannot Be Delegated (Учетная запись является важной и не может быть делегирована).** С помощью этого флажка указывается, может ли служба заимствовать права у пользователя. Это делается для того, чтобы разрешить службе выступать в качестве пользователя. Возможно, вы столкнетесь с таким поведением на среднем уровне в многоуровневой архитектуре, такой как часть веб-клиента, сервер приложений среднего уровня и сервер баз

данных. По умолчанию этот флажок не отмечен, что разрешает заимствование прав данной учетной записи.

- **Use Kerberos DES Encryption Types for This Account (Использовать для этой учетной записи типы шифрования Kerberos DES).** Некоторые приложения могут требовать учетной записи службы, которая использует алгоритм шифрования DES. Для таких учетных записей служб необходимо отметить этот флажок. После изменения этой настройки может понадобиться сбросить пароль.
- **This Account Supports AES 128-Bit Encryption (Эта учетная запись поддерживает 128-битное шифрование AES).** Некоторые приложения могут требовать учетной записи службы, которая использует алгоритм 128-битного шифрования AES. Для таких учетных записей служб необходимо отметить этот флажок.
- **This Account Supports AES 256-Bit Encryption (Эта учетная запись поддерживает 256-битное шифрование AES).** См. описание предыдущего флажка.
- **Do Not Require Kerberos Preauthentication (Не требовать предварительной аутентификации Kerberos).** Этот флажок предназначен для предоставления пользователям возможности входить в сеть, когда в ней содержится смесь разных областей Kerberos, таких как Active Directory и центры распределения ключей Unix (key distribution center — KDC).

Обратили внимание, что в списке не предусмотрено недоступного флажка, который бы указывал на заблокированное состояние учетной записи? Это делает совершенно очевидным тот факт, что применять данное диалоговое окно для блокировки пользователя нельзя. Разблокировать пользователя можно с помощью флажка Unlock account (Разблокировать учетную запись), расположенного выше списка Account options на вкладке Account.

Последние элементы управления на этой вкладке предназначены для управления автоматическим истечением срока действия учетной записи. Вы можете определить дату, по прошествии которой учетная запись больше не будет использоваться. Это удобно при создании учетной записи пользователя для приходящих инженеров/консультантов или для временного/контрактного персонала. Поскольку вам известно, сколько времени они будут находиться в офисе, вы можете заранее сконфигурировать учетную запись так, чтобы срок ее действия истекал, и войти с ее помощью стало невозможно. Это изящно защищает сеть от злоупотреблений с учетными записями пользователей.

Вкладка Profile

Назначение вкладки Profile (Профиль), представленной на рис. 8.22, обсуждалось при рассмотрении локальных учетных записей пользователей.

Вкладка Telephones

Вкладка Telephones (Телефоны) должна быть очевидной (рис. 8.23). Здесь указываются телефонные номера для связи с пользователем.

Вкладка Organization

Вкладка Organization (Организация) является еще одной информационной вкладкой (рис. 8.24). Мы несколько раз упоминали, что приложения могут использовать информацию такого рода.

Рис. 8.22. Вкладка Profile для пользователя Active Directory

Рис. 8.23. Вкладка Telephones для пользователя Active Directory

Например, настройки на этой вкладке могли бы применяться реализацией служб Windows SharePoint (SharePoint Services — WSS). Данная информация отображается в веб-интерфейсе, когда пользователи ищут дополнительные сведения о владельце определенной документации или о сайте внутри реализации WSS. Службы WSS загружают эту информацию из объекта пользователя, сконфигурированного в Active Directory. Скажем, если вы просматриваете сведения о пользователе `Steve Red` на сервере WSS, то свойства учетной записи `SRed` будут читаться службой WSS из Active Directory.

Эта вкладка позволяет описать роль пользователя внутри организации — это не более чем сведения о кадрах, не имеющие отношения к делегированию или администрированию Active Directory. Можно также указать руководителя, перейдя к другой учетной записи пользователя в Active Directory.

Вкладка COM+

На вкладке COM+ вы углубляетесь в область программирования приложений (рис. 8.25). *Раздел* (partition) — это конфигурация приложения. Приложение может иметь множество конфигураций. Это значит, что вы можете иметь несколько разделов COM+ внутри Active Directory. Дополнительные сведения о разделах приложений приведены в документации MSDN.

Набор разделов может содержать множество разделов. Пользователей можно привязывать к наборам разделов и, в свою очередь, к содержащимся разделам. Привязывать можно не только какого-то одного пользователя; можно привязать всех пользователей в организационной единице за счет привязки этой OU к набору разделов. Создание набора разделов внутри Active Directory описано в MSDN по ссылке `http://tinyurl.com/2naoft`.

Рис. 8.24. Вкладка Organization для пользователя Active Directory

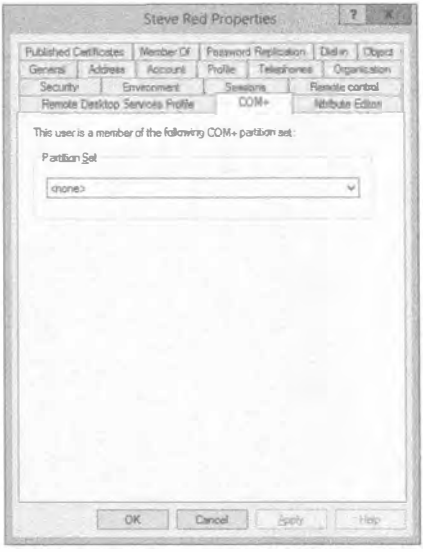


Рис. 8.25. Вкладка COM+ для пользователя Active Directory

Вкладка Attribute Editor

Вы уже сталкивались с вкладкой Attribute Editor (Редактор атрибутов), когда имели дело со свойствами организационной единицы (рис. 8.26). При желании на ней можно просматривать или напрямую редактировать свойства объекта, представляющего пользователя.

Вкладка Published Certificates

Вкладка Published Certificates (Опубликованные сертификаты) показана на рис. 8.27. Сертификаты предоставляют механизм защиты, основанный на шифровании, который применяется для подтверждения идентичности.

Здесь можно просматривать сертификаты, которые были автоматически назначены пользователю через Active Directory с использованием служб сертификатов (Certificate Services). У вас есть возможность вручную назначить пользователю сертификат из собственного локального хранилища сертификатов либо из файловой системы.

Вкладка Member Of

Вкладка Member Of (Членство в группах) позволяет управлять членством в группах данной учетной записи пользователя (рис. 8.28). Мы вернемся к ней позже в этой главе, когда будем рассматривать группы и членство в группах.

Как видите, можно также управлять основной группой пользователя. Это требуется только в приложениях POSIX (Portable Operating System Interface for Computer Environment — интерфейс переносимой операционной системы) или на клиентских компьютерах Macintosh. Когда один из таких клиентов создает файл или папку на сервере Windows, этому новому объекту назначается основная группа. Эта группа должна находиться в собственном домене пользователя и быть либо глобальной, либо универсальной группой доступа.

Рис. 8.26. Вкладка Attribute Editor для пользователя Active Directory

Рис. 8.27. Вкладка Published Certificates для пользователя Active Directory

Вкладка Password Replication

Вкладка Password Replication (Репликация паролей) позволяет просматривать, на какие контроллеры домена только для чтения (read-only domain controller — RODC) был реплицирован пароль данного пользователя (рис. 8.29). Опция RODC была добавлена в архитектуру Active Directory в версии Windows Server 2008. Контроллер домена RODC можно добавлять в офис филиала, где не может быть обеспечена физическая защита, достаточная для размещения обычного контроллера домена. В случае похищения или компрометации RODC вы можете изолировать учетные записи пользователей, детали которых хранились на этом RODC.

Вкладка Object

Вкладка Object (Объект), представленная на рис. 8.30, должна быть очень полезна при поиске и устранении неполадок. На ней можно видеть важную информацию, такую как:

- когда объект был создан;
- когда объект последний раз изменялся;
- информация USN (update sequence number — порядковый номер обновления), которая применяется для управления репликацией Active Directory.

Удобной новой опцией на этой вкладке является возможность защиты учетной записи пользователя от случайного удаления, для чего необходимо отметить флажок Protect object from accidental deletion (Защитить объект пользователя от случайного удаления). Это позволяет гарантировать, что никто не сможет неумышленно удалить учетную запись для критически важной службы.

Рис. 8.28. Вкладка Member Of для пользователя Active Directory

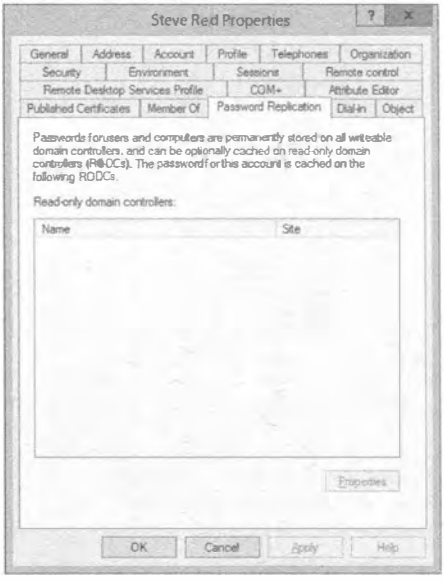


Рис. 8.29. Вкладка Password Replication для пользователя Active Directory

Вкладка Security

Вкладка Security (Безопасность), показанная на рис. 8.31, позволяет управлять тем, кто и что может делать с помощью этой учетной записи пользователя. Это называется *делегированием*. Мы обсудим данную тему более подробно далее в книге.

Рис. 8.30. Вкладка Object для пользователя Active Directory

Рис. 8.31. Вкладка Security для пользователя Active Directory

Просмотрите разрешения, назначенные объекту SELF, щелкнув на нем. Объект SELF представляет текущего пользователя. Другими словами, что пользователю Steve Red позволено делать посредством учетной записи SRed? Прокрутив список Permissions for SELF (Разрешение для SELF), вы увидите, что пользователь Steve Red может изменять много настроек в своей учетной записи. Это значит, что он может модифицировать такие настройки, как его руководитель, контактные данные и тому подобное. Теоретически вы могли бы предложить пользователям веб-приложение, которое позволило бы им легко редактировать эти настройки. Такой подход был бы намного проще в понимании, чем заставлять их запускать оснастку Active Directory User and Computers и редактировать в ней свои учетные данные.

Редактирование нескольких учетных записей пользователей одновременно

Как вы уже убедились, изменять все настройки для отдельной учетной записи довольно просто. А что, если вы хотите модифицировать более одной учетной записи за раз? Это тоже делается легко. В рассматриваемом примере давайте создадим пару новых пользователей в организационной единице Users, как показано на рис. 8.32.

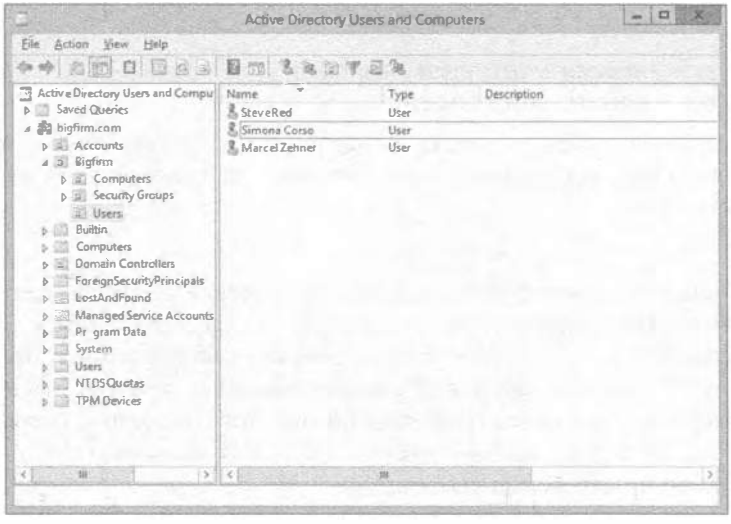


Рис. 8.32. Дополнительные пользователи Active Directory

Предположим, что вы хотите изменить настройки для всех пользователей в этой организационной единице. Выделите все учетные записи пользователей, щелкните правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства).

Откроется диалоговое окно свойств, представленное на рис. 8.33. Для нескольких пользователей в действительности мало смысла предоставлять абсолютно все настройки, поэтому вы увидите только подмножество опций.

Чтобы модифицировать настройку, отметьте связанный с ней флажок. Это сделает доступным поле редактирования. Теперь эту настройку можно отредактировать для всех ранее выделенных пользователей (рис. 8.34).

Управление доменными учетными записями пользователей с помощью оснастки Active Directory Users and Computers выполняется очень легко. А теперь посмотрим, как поступить, когда единственным вариантом является командная строка.

Рис. 8.33. Свойства нескольких объектов пользователей Active Directory

Рис. 8.34. Изменение атрибутов множества объектов Active Directory

Управление доменными учетными записями пользователей в командной строке

Давайте посмотрим, как решать те же задачи в командной строке. Будет использоваться команда `dsmod` с опцией `user`. Получить справку по этой команде можно следующим образом:

```
dsmod user /?
```

Обратите внимание, что для модификации настроек пользователя должно быть указано его имя DN. Вспомните данный ранее в главе совет по получению такого имени из свойства `distinguishedName` объекта учетной записи пользователя на вкладке Attribute Editor (см. врезку "Простой способ получения имени DN"). Это можно сделать, когда доступен графический пользовательский интерфейс. Но что, если это не так? В случае, когда известно имя UPN пользователя, для получения имени DN можно ввести команду `dsquery`:

```
dsquery user -upn SRed@bigfirm.com
"CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

В качестве альтернативы команду `dsquery` можно запустить с применением имени учетной записи SAM, которое представляет собой дружественное имя, известное как `SRed`:

```
C:\Users\Administrator>dsquery user -samid SRed
"CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

`dsquery` — это действительно мощная команда, поэтому ее полезно изучить, введя `dsquery /?`.

Теперь можно продолжить, выполнив команду `dsmod`. Вот как сконфигурировать домашнюю папку и отобразить ее на букву диска для пользователя `Steve Red`:

```
dsmod user "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-hmdir \\DC01\home$\SRed -hmdrv P
```

Команда настроит домашнюю папку (специальную сетевую открытую папку, специфичную для этого пользователя) с буквой диска P, которая отображается на \\DC01\home$\SRed всякий раз, когда пользователь Steve Red входит в сеть.

Далее необходимо сконфигурировать руководителя для пользователя Steve Red. Вы только что узнали, что пользователь по имени Marcel Zehner повышен до начальника отдела. Введите следующую команду:

```
dsmod user "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-mgr "CN= Marcel Zehner,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Обратите внимание, что вы не вводили для руководителя что-то похожее на bigfirm\mzehner или mzehner. В действительности вы использовали имя DN учетной записи пользователя, являющегося руководителем.

На первых порах команда dsmod выглядит сложной в применении. Поработайте с ней некоторое время, и вы увидите, что на самом деле не все так плохо.

Переименование и удаление объектов

Как вы наверняка догадались, решение о переименовании или удалении чего-либо должно приниматься взвешенно. Такие действия имеют весьма серьезные последствия.

Переименование объектов

Каждый объект в Windows имеет имя. Это имя используется для входа в систему, внутри сценариев, в конфигурации приложений и т.д. Например, если вы создали учетную запись SCorso, то пользователь по имени Simona Corso будет применять ее для входа. Это имя не отслеживается в Windows, поскольку оно может измениться, к примеру, на Simona Red, что повлечет за собой изменение имени пользователя на SiRed. ОС Windows не должна искать в сети все ресурсы, где использовалась учетная запись SCorso, чтобы изменить в них ссылку на SiRed: членство в группах, права доступа к файлам, связи с почтовыми ящиками и тому подобное.

Понятие идентификатора безопасности

Людям проще запоминать и вводить дружественные имена, но Windows назначает каждому объекту специальный код, который называется *идентификатором безопасности* (security identifier — SID) и представляет собой глобально уникальный идентификатор в пределах Active Directory. Все объекты пользователей и компьютеров обладают идентификатором SID. Каждая группа также имеет SID.

Что произойдет, когда вы переименовываете пользователя или группу, являющуюся *участником безопасности* (security principal)? Конечно, известное вам имя изменяется. В случае Simona Red необходимо помнить имя пользователя. Однако Windows отслеживает объекты пользователей только по идентификаторам SID. Любые разрешения на доступ к ресурсам, назначенные объекту пользователя, и его членство в группах не изменятся, т.к. идентификатор SID остался прежним. Обратите внимание, что приложения от независимых поставщиков, работающие с именами объектов, а не с идентификаторами SID, потребуют корректировки ссылок на имена объектов, но приложения, тесно интегрированные с Active Directory, такие как SQL, SharePoint или Exchange, продолжат нормально функционировать.

Здесь важно запомнить, что после изменения имени объекта Active Directory, представляющего пользователя или группу, Windows по-прежнему трактует его как тот же самый объект. Разрешения, выданные этому объекту, его атрибуты, членство в группах и прочие аспекты не меняются.

Удаление объекта

Другой сценарий, который вы должны обдумать, связан с удалением объекта. При назначении разрешений учетной записи `SiRed` в Windows поддерживается список разрешений, ассоциированный с идентификатором SID этого пользователя. То же самое происходит и в случае группы пользователей — разрешения будут ассоциированы с SID объекта группы, а не с его именем.

Восстановление удаленного объекта

При удалении объекта пользователя или группы следует проявлять крайнюю осторожность. Если вы случайно удалили его и хотите восстановить в прежнем состоянии, то не сможете сделать это, просто создав новый объект с тем же самым именем. Вспомните, что идентификатор SID является глобально уникальным, и он не привязан к имени объекта. Созданный в качестве замены объект пользователя `SiRed` будет иметь другой SID. Открытый файловый ресурс или почтовый ящик, к которому учетная запись `SiRed` получала доступ, не распознает новый объект пользователя из-за того, что его идентификатор SID отличается по сравнению со старым объектом. Единственный способ восстановления доступа к удаленному объекту пользователя или группы предусматривает его восстановление из резервной копии.

Существует несколько способов сделать это, которые обсуждаются по ссылке `http://tinyurl.com/2wgo4g`. В версии Windows Server 2012 появилось средство под названием корзина Active Directory (Active Directory Recycle Bin), упрощающее процесс восстановления недавно удаленных объектов.

Важно помнить, что Windows идентифицирует объект не по имени, а по SID. В результате повторного создания копии объекта с тем же самым именем будет получен другой объект.

Передовой опыт

По изложенным причинам мы настоятельно рекомендуем отключать пользователей, когда поступает запрос на их удаление от руководства или отдела кадров. Это заблокирует их доступ в сеть. Вдобавок мы рекомендуем создать отдельную организационную единицу для учетных записей, которые были отключены, и перемещать в нее отключаемых пользователей. Поступая подобным образом, вы сможете получить немедленный обзор всех неиспользуемых учетных записей. Всегда есть шанс, что случилось недопонимание или человек возвратился к работе. Восстановить доступ легко: просто включите его учетную запись. По истечении согласованного периода хранения в 30 или 60 дней объект может быть удален.

Для поиска неактивных и отключенных учетных записей в домене Active Directory можно применять следующую команду:

```
dsquery user -inactive <количество недель> -disabled
```

Например, эта команда найдет пользователей, которые отключены или были неактивными в течение восьми недель:

```
dsquery user -inactive 8 -disabled
```

Чтобы удалить одного или нескольких пользователей, их необходимо выделить, щелкнуть правой кнопкой мыши и выбрать в контекстном меню пункт Delete (Удалить). Удаление пользователя в командной строке также выполняется несложно с помощью следующей команды:

```
net user <имя пользователя> /delete
```

Вот команда для удаления локальной учетной записи пользователя SRed:

```
net user SRed /delete
```

Для удаления учетной записи пользователя Active Directory должна использоваться команда dsrm с указанием имени DN объекта пользователя:

```
dsrm "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Будет выдан запрос на подтверждение удаления. Иногда требуется отключить выдачу такого запроса, например, внутри сценария. Это делается так:

```
dsrm "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com" -noprompt
```

Управление группами

Трактовка коллекции пользователей как единой сущности для какой-то одной или нескольких целей упрощает решение множества задач администрирования. Например, вместо выполнения 100 операций по назначению каждому из 10 пользователей разрешений на доступ к 10 ресурсам можно поместить пользователей в группы (1 операция) и назначить этой группе разрешения на доступ к ресурсам (11 операций). Приведенные подсчеты делают вполне понятной необходимость в применении групп. Вместо того чтобы иметь дело с индивидуумами, вы взаимодействуете с коллективом, т.е. группой.

В сущности, при назначении разрешений рекомендуется всегда использовать группы. По этой причине вы должны научиться создавать группы, изменять членство, а также удалять их. Вы узнаете, как создавать, управлять и удалять локальные группы и группы домена с применением оснастки Active Directory Users and Computers, а также командной строки.

Локальные группы

Подобно локальному пользователю, локальная группа существует внутри сервера-члена или автономного компьютера, будь то сервер, ноутбук или настольный компьютер. Она содержит локальные учетные записи пользователей, существующие на сервере. Эта группа также может содержать пользователей или группы Active Directory, членами которых является сервер. Управлять группами можно с использованием тех же самых инструментов с графическим интерфейсом, что и при управлении локальными пользователями.

На рис. 8.35 показано, где производится управление локальными группами на сервере. Как видите, по умолчанию таких групп имеется немало. При добавлении определенных ролей будут добавляться дополнительные группы.

Создание группы

В этом разделе мы создадим новую группу под названием Fileshare. Данную группу можно применять для назначения ее членам разрешений на доступ к общему файловому ресурсу, расположенному на этом сервере.

1. Выберите в меню Action (Действие) пункт New Group (Создать группу) или щелкните правой кнопкой мыши в центральной панели и выберите в контекстном меню пункт New Group.

   Откроется диалоговое окно New Group (Новая группа).

Рис. 8.35. Стандартные локальные группы

2. Введите `Fileshare` в качестве имени группы, как показано на рис. 8.36.

   Мы рекомендуем вводить описание для любой создаваемой группы. Непосредственно после создания группы вы можете помнить, для чего она предназначена, но будете ли вы помнить об этом, когда спустя полгода работы над бесконечным числом других проектов, вы вернетесь к данной машине, чтобы устранить какую-то проблему? Поймут ли ваши коллеги, что конкретно делает эта группа, когда вы находитесь на больничном или в отпуске?

   При желании группу можно было бы создать без членов. Но в рассматриваемом примере локальный пользователь `Steve Red` должен стать членом группы, поэтому сделаем это.

3. Щелкните на кнопке **Add** (Добавить).

   На рис. 8.37 видно, что открывшееся диалоговое окно Select Users, Computers, Service Accounts, or Groups (Выбор пользователей, компьютеров, учетных записей групп или групп) позволяет искать и добавлять члены.

Рис. 8.36. Создание новой локальной группы

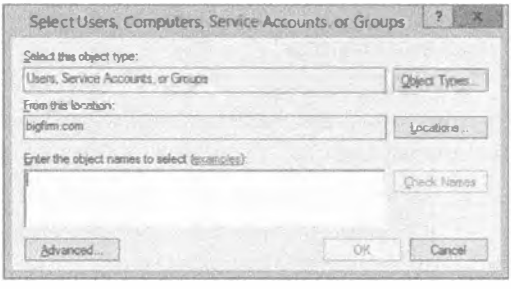


Рис. 8.37. Выбор членов группы

4. В группу могут быть добавлены следующие члены:
   - пользователи Active Directory или локальные пользователи;
   - учетные записи компьютеров из Active Directory;
   - группы Active Directory.

   Варианты, основанные на Active Directory, будут доступны, только если данный север является членом домена. Сервер, на котором выполняется работа, `SERVER01`, является членом `bigfirm.com`.

   В текущий момент настройка Select this object type (Выбирать этот тип объектов) позволяет добавлять в группу пользователей, группы или учетные записи служб. Это можно изменить, щелкнув на кнопке Object Types (Типы объектов).

   Как показано на рис. 8.38, можно отмечать или снимать отметку с флажков Computers (Компьютеры), Groups (Группы), Users (Пользователи) и Service Accounts (Учетные записи служб). Что понимается под учетными записями служб? В Windows Server 2012 теперь также есть возможность выбора учетных записей управляемых служб (Managed Service Accounts — MSA). В зависимости от отмеченных флажков вы изменяете то, что можно добавлять или удалять из группы во время редактирования членства.

   Возвратившись обратно в диалоговое окно Select Users, Computers, Service Accounts, or Groups, вы увидите, что настройка From this location (Из этого местоположения) установлена в домен, членом которого сервер является. Это делается по умолчанию для компьютера-члена домена. Местоположение определяет, откуда можно выбирать объекты для помещения в группу. На автономном сервере местоположением может быть только он сам. В данном примере можно выбирать пользователи или компьютеры из домена `bigfirm.com`.

5. Это необходимо изменить, чтобы выбрать локальную учетную запись пользователя. Щелкните на кнопке Locations (Местоположения).

   Обратите внимание, что в открывшемся диалоговом окне Locations (Местоположения) можно также выбрать другой доверенный домен. Можно даже перейти внутри домена к конкретной организационной единице, чтобы сузить область поиска доменного пользователя или компьютера.

   На рис. 8.39 узел домена раскрыт, чтобы продемонстрировать возможность прохода по организационным единицам. Тем не менее, нас интересует локальная учетная запись пользователя.

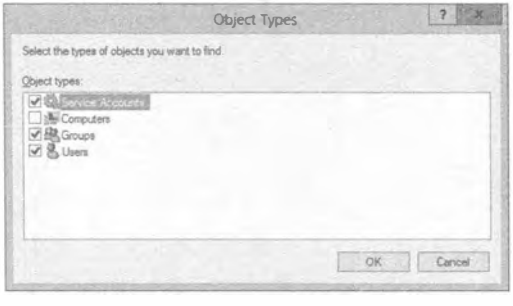


Рис. 8.38. Возможные типы объектов для членов группы

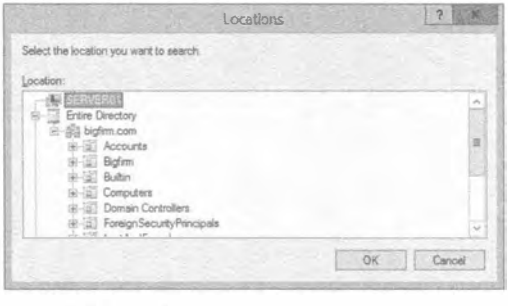


Рис. 8.39. Выбор местоположения источника объектов

6. Выберите имя локального сервера, `Server01`.

   В качестве альтернативы вы могли бы выбрать домен, чтобы добавить группу или пользователя из домена Active Directory в свою локальную группу. Если вам точно известно имя пользователя добавляемой локальной учетной записи, то просто введите его.

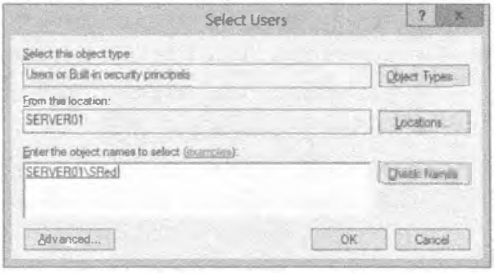


Рис. 8.40. Добавление пользователя в локальную группу

7. Введите **`SRed`** (например) и щелкните на кнопке Check Names (Проверить имена). Производится поиск в базе данных локальных учетных записей и в диалоговом окне Select Users (Выбор пользователей) выводится подтверждение того, что пользователем `SRed` в действительности является `SERVER01\SRed` (рис. 8.40). Если же вы уверены в правильности имени, можете просто ввести его и щелкнуть на кнопке OK.
8. Если точное имя не известно, щелкните на кнопке Advanced (Дополнительно), чтобы открыть диалоговое окно, показанное на рис. 8.41.

   Многие опции поиска здесь недоступны, т.к. вы указали для местоположения локальный компьютер. Эти опции работают, только когда в качестве местоположения установлен домен.
9. Щелкните на кнопке Find Now (Найти сейчас), чтобы вывести список доступных учетных записей, которые можно добавить в группу, на основе определенного ранее критерия.

   На рис. 8.42 приведены результаты поиска. Здесь вы можете выбрать объект или объекты для добавления в группу.

Рис. 8.41. Расширенное представление членства в группе

Рис. 8.42. Выбор пользователя для добавления в группу внутри расширенного представления

10. Выберите объект SRed и щелкните на кнопке OK.

    Выбранные объекты отображаются в диалоговом окне Select Users, как показано на рис. 8.43.

11. Щелкните на кнопке OK, чтобы сохранить это членство. На рис. 8.44 видно, что группа готова к созданию со своим начальным членством.

12. Завершите процесс, щелкнув на кнопке Create (Создать).

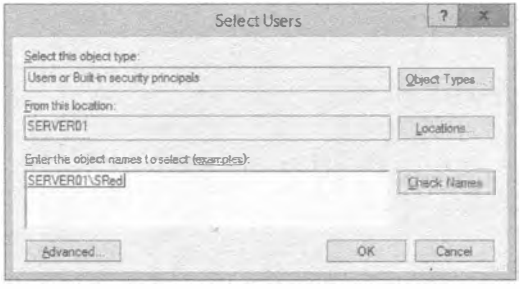


Рис. 8.43. Проверенный потенциальный член группы

Рис. 8.44. Отображение потенциальных новых членов

На рис. 8.45 можно заметить, что новая группа была создана, и в нее был добавлен пользователь Steve Red.

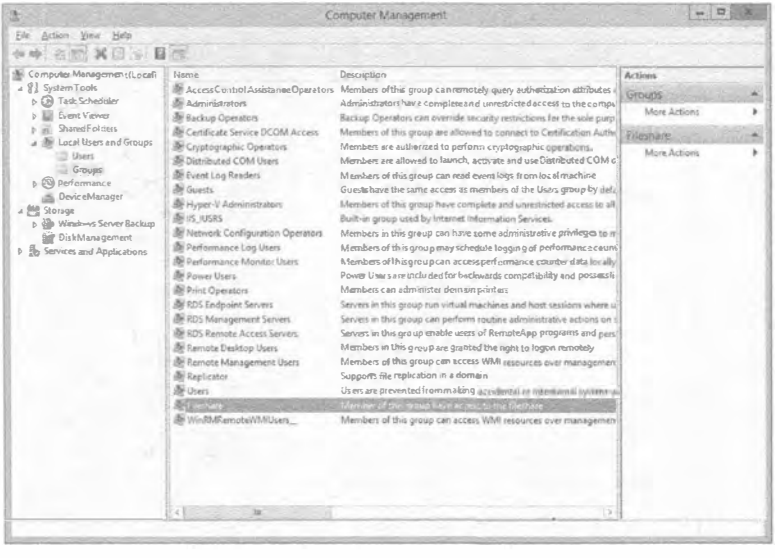


Рис. 8.45. Созданная новая группа

Вход с новым членством в группах

Есть одно важное замечание, которое применимо к работе как с группами Active Directory, так и с локальными группами. Пользователь может использовать свое членство в группах, только когда он выполняет вход *после* изменения членства. Пользователь `Steve Red` не может работать со своим новым членством в группе, т.к. в текущий момент он находится в системе. Вы должны уведомить его о необходимости выйти и снова войти.

Создание группы в командной строке

Группу можно создать в командной строке с помощью команды `net localgroup`. Для получения справки введите:

```
net help localgroup
```

Для создания группы запустите следующую команду:

```
net localgroup Fileshare /add
/comment:"Members assigned permission to the fileshare on this server"
```

Ниже приведен синтаксис этой команды:

```
net localgroup <имя новой группы> /add /comment:"<описание группы>"
```

Обратите внимание, что вы не можете добавить пользователя в группу во время ее создания в командной строке.

Добавление пользователя в группу

Давайте добавим в группу новый член. Это можно сделать через оснастку консоли MMC.

1. Откройте диалоговое окно свойств группы, представленное на рис. 8.46.

   Здесь вы можете видеть существующие члены в группе.

Рис. 8.46. Диалоговое окно свойств группы

2. Щелкните на кнопке Add (Добавить), чтобы добавить новый член в группу.

   Как и ранее, вы можете установить критерий для объектов, добавляемых в группу, и указать их источник. Вы собираетесь добавить группу домена в локальную группу. Вы хотите, чтобы все пользователи, находящиеся в домене, были в составе локальной группы. Вам известно, что для этого предназначена встроенная группа домена под названием `Domain Users` (Пользователи домена).

3. Введите имя этой группы и щелкните на кнопке Check Names (Проверить имена).

   На рис. 8.47 видно, что встроенная группа домена `Domain Users` будет добавлена в локальную группу.

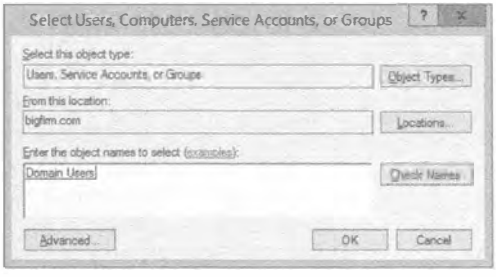


Рис. 8.47. Добавление группы домена в локальную группу

Удобный прием: добавление группы домена в локальную группу

Сценарий добавления группы домена в локальную группу является довольно мощным. Он позволяет администратору повторно использовать коллекцию объектов Active Directory в форме группы Active Directory и предоставляет им права доступа к ресурсу на этом сервере. Это может понадобиться в ситуации, когда владелец приложения выдал права локального администрирования единственному серверу и ничему больше. Тогда администраторы могут создать локальные группы и наполнить их группами и пользователями домена. Администратор приложения может открыть общий доступ к своему приложению членам домена, без необходимости в наличии каких-либо прав администрирования домена.

4. Вы также заметите, что группа `BIGFIRM\Domain Users` присоединит пользователя `SRed` в качестве члена. Щелкните на кнопке OK (рис. 8.48).

Самое время взглянуть на добавление членов в группу с применением командной строки. Для этого снова будет использоваться команда `net localgroup`:

```
net localgroup Fileshare SRed /add
```

Приведенная команда добавляет пользователя в группу. Синтаксис команды довольно прост:

```
net localgroup Fileshare <имя объекта, добавляемого в группу> /add
```

Следующая команда добавляет группу `Domain Users` из домена BigFirm в новую локальную группу:

```
net localgroup Fileshare "bigfirm\domain users" /add
```

Рис. 8.48. Потенциальное новое членство в группе

Рис. 8.49. Членство пользователя в группах

Помните вкладку Member Of (Членство в группах) в диалоговом окне свойств локальной учетной записи пользователя? А теперь посмотрим на диалоговое окно свойств учетной записи пользователя `SRed`, показанное на рис. 8.49.

Как видите, членство пользователя в группах было обновлено. Здесь вы можете так же легко добавить пользователя `Steve Red` в группу. Вас попросили добавить пользователя `Steve Red` в локальную группу `Administrators`. Это сделает его администратором этого и только этого сервера.

1. Щелкните на кнопке Add (Добавить), в результате чего откроется диалоговое окно, представленное на рис. 8.50.
2. Введите имя группы, в которую хотите добавить этого пользователя, и затем щелкните на кнопке Check Names (Проверить имена), чтобы удостовериться в корректности имени группы.

   Обратите внимание, что локальные учетные записи пользователей можно добавлять только в локальные группы, но не в группы домена.

   Список членства в группах для локальной учетной записи пользователя теперь обновился (рис. 8.51).

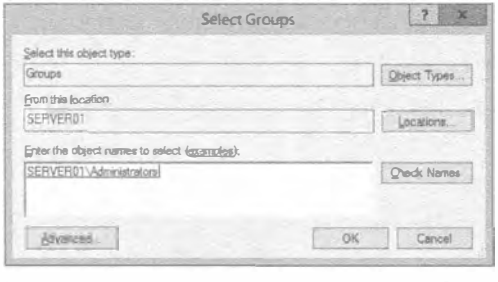


Рис. 8.50. Добавление пользователя в группу через диалоговое окно его свойств

Рис. 8.51. Обновление членства пользователя в группах

Рис. 8.52. Удаление пользователя из локальной группы

3. Щелкните на кнопке OK, чтобы сохранить изменения.

Единственный способ воспроизведения этого в командной строке предусматривает манипулирование самой группой, а не пользователем:

```
net localgroup administrators SRed /add
```

Удаление пользователя

Удалить пользователя из локальной группы также легко. Делать это можно одним из перечисленных далее способов.

- Использование учетной записи пользователя. Применяйте учетную запись пользователя, если это одноразовая операция или если вы удаляете несколько прав доступа у какого-то пользователя.
- Использование группы. Применяйте группу, если вы удаляете идентичные права доступа у нескольких пользователей.

Теперь мы покажем, каким образом модифицировать членство в группе `Fileshare` путем удаления из нее пользователя `Steve Red`.

1. Откройте диалоговое окно свойств группы `Fileshare` (рис. 8.52).
2. Выберите пользователя `SRed`.

   Удерживая клавишу <Shift> или <Ctrl>, можно выбрать более одного члена с целью их удаления.
3. Выделив члены, подлежащие удалению, щелкните на кнопке Remove (Удалить).

На этом все; ничего другого для удаления члена из группы предпринимать не придется. Следующая команда удалит пользователя `Steve Red` из группы `Fileshare`:

```
net localgroup fileshare SRed /delete
```

Чтобы удалить группу с использованием оснастки MMC, выполните следующие шаги.

1. Найдите нужную группу.
2. Щелкните правой кнопкой мыши на группе и выберите в контекстном меню пункт Delete (Удалить).

Обратите внимание на диалоговое окно, показанное на рис. 8.53, которое открывается при удалении группы. Оно сообщает, что удаление повлияет на множество пользователей или компьютеров, которые являются членами этой группы.

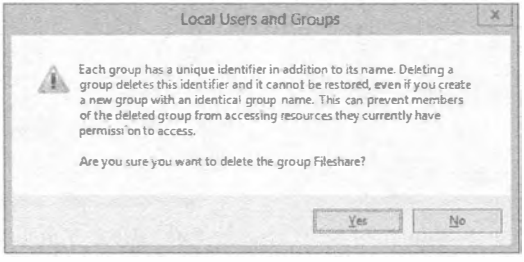


Рис. 8.53. Запрос о том, действительно ли вы уверены в удалении группы

Снова время повышенного внимания

Это настолько важно, что стоит повторить: хотя вы видите пользователей, компьютеры и группы как относительно дружественные имена, такие как `SRed`, `SERVER01` или `Fileshare`, со стороны Windows они распознаются по-другому. Уникальная идентификация этих *участников безопасности* осуществляется с помощью SID. Идентификатор SID создается каждый раз, когда создается новый участник безопасности. Это значит, что в случае создания учетной записи `SRed`, ее удаления и повторного создания Windows будет трактовать старый и новый объекты как два разных участника безопасности, хотя вы считаете их одним. В результате разрешения, назначенные старой учетной записи, в новой учетной записи отсутствуют.

Во всплывающем окне на рис. 8.53 предупреждается об этом. Вы должны быть на сто процентов уверены в том, что организации больше не нуждается в участнике безопасности, прежде чем удалять его. Следует помнить, что после удаления группы теряются назначенные ей разрешения, а также членство в группе. Любой пользователь, которому были выданы права доступа к определенному ресурсу посредством членства в данной группе, утратит доступ к этому ресурсу.

Приведенная ниже команда `net localgroup` удалит группу `Fileshare` безо всяких предупреждений или запросов на подтверждение:

```
net localgroup fileshare /delete
```

Группы Active Directory

Базовые концепции групп Active Directory или домена и локальных групп не отличаются. Они применяются для коллективного обращения к нескольким объектам идентичным способом. Однако с группами Active Directory можно выполнять намного больше операций. Это становится возможным из-за того, что группы такого типа хранятся в Active Directory на контроллерах домена, подмножество кото-

рых сконфигурировано как глобальный каталог. В результате единственная группа может содержать многих участников безопасности домена, подобных пользователям и компьютерам, и использоваться всеми компьютерами внутри домена, к которому эта группа принадлежит. В действительности группы можно применять за пределами их доменов, и существует даже категория групп, которые могут содержать членов из любого домена в лесе.

Для целей этого раздела вы должны полагать, что когда мы упоминаем *группу*, то имеем в виду группу Active Directory. Есть два базовых типа групп.

- **Группа рассылки (distribution group).** Группа рассылки используется для объединения вместе нескольких объектов с целью коллективной адресации. Почтовый сервер вроде Microsoft Exchange может предоставлять пользователям группу рассылки как целевой адрес. Пользователь может отправить сообщение группе рассылки и почтовый сервер попытается разослать его всем членам группы при условии, что они имеют настроенные адреса электронной почты.
- **Группа доступа (security group).** Группа доступа также может выполнять функцию почтовой рассылки. Но основная цель этого типа групп, как должно быть понятно из названия, связана с доступом. Группу доступа можно применять для назначения разрешений или прав доступа к объекту или множеству объектов, таких как организационная единица, папка или компонент приложения. Это позволяет Active Directory стать не только единым механизмом аутентификации для сети, но также механизмом авторизации. Конечный пользователь может использовать единственную учетную запись для получения авторизации к защищенным ресурсам по всему лесу Active Directory, а не только в домене или каком-то одном компьютере.

Различают три области действия групп.

- **Локальная группа домена (domain local group).** 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.
- **Глобальная группа (global group).** Это стандартная область действия при создании группы в Active Directory. 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 (universal group).** Одна черта универсальных групп делает их весьма отличающимися от групп других двух типов. Группы других двух типов хранятся и реплицируются на все контроллеры внутри домена, в котором они были созданы. Универсальная группа хранится на контроллерах домена, сконфигурированных в качестве глобального каталога. Это влияет на то, как 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.

Краткое предостережение относительно универсальных групп

При проектировании универсальной группы в крупных средах необходимо проявлять крайнюю осторожность, т.к. возникает дополнительная нагрузка репликации, когда группа создается или модифицируется. Active Directory будет реплицировать только изменения в универсальных группах, однако будьте аккуратны, чтобы не допустить масштабных изменений. Кроме того, необходимо удостовериться в том, что контроллеры домена с глобальным каталогом находятся близко к службам, на которые они интенсивно полагаются.

В сетях с единственным доменом особо переживать по поводу универсальных групп не придется, поскольку они применяются не слишком часто. Универсальные группы могут содержать учетные записи пользователей/компьютеров, глобальные группы и другие универсальные группы из любого домена в лесе.

Возможно, вы отметили один аспект. Группы могут содержать другие группы. Обычно это называют *вложением групп*. Для чего вкладывать группы друг в друга? Ниже описаны два аргумента в пользу этого.

- **Одновременное управление несколькими группами.** Представьте, что у вас есть группы под названиями `Accounts Management` (Управление расчетными счетами) и `Sales Management` (Управление продажами). Вы хотите иметь возможность работать с этими двумя группами одновременно, например, предусмотреть для них один адрес электронной почты, который будет трактоваться как контактный список. Для этого создайте группу по имени `Management` (Управление) и поместите в нее в качестве членов группы `Accounts Management` и `Sales Management`. Затем сконфигурируйте адрес электронной почты для группы `Management`.
- **Управление организационными единицами в разных отделах.** В другом сценарии (рис. 8.54) созданы организационные единицы для разных отделов; например, пусть имеется домен `\BigFirm`, который содержит организационные единицы `\BigFirm\Accounts` и `\BigFirm\Sales`. Существуют два уровня IT-обслуживания. В `BigFirm` имеется отдел IT, который отвечает за Active Directory и корпоративные функции IT. Именно в этом отделе вы работаете. В организационных единицах `Accounts` и `Sales` присутствуют небольшие бригады IT, которые управляют только внутренними объектами в своих OU. Это называется *делегированием*. Вы хотите получить возможность создания группы по имени `Management`, которая будет содержать начальников всех отделов. Вы не планируете управлять этими членами, а взамен поручить делать это IT-персоналу внутри отделов. Создайте группу `Accounts Management` в `\BigFirm\Accounts` и группу `Sales Management` в `\BigFirm\Sales`. Это позволит IT-персоналу внутри отделов управлять двумя указанными группами. Создайте группу `Management` в `\BigFirm`. Теперь можете добавить группы, предназначенные для IT-персонала внутри отделов, в качестве членов группы `Management`.

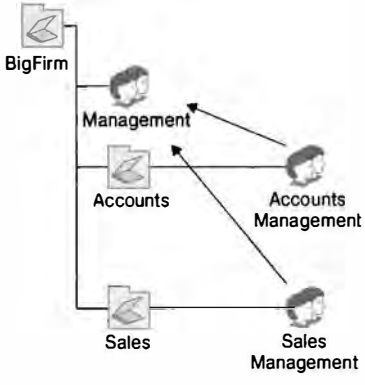


Рис. 8.54. Вложенные группы

Как видите, группы Active Directory позволяют несколько большее, чем локальные группы. Перед созданием группы важно осознавать, по какой причине она создается, и как будет использоваться. Области действия и типы групп можно изменять, но вы должны понимать, какое влияние это окажет.

Например, смена типа группы с глобальной на универсальную изменит репликацию Active Directory с выполняющейся между контроллерами домена внутри домена на репликацию, проводимую между серверами глобального каталога через целый лес. Дополнительный объем планирования определенно стоит потраченных на него усилий, как вы увидите по мере чтения остального материала данной книги. Со временем вы обнаружите, что применяете группы для самых разнообразных целей:

- назначение разрешений общим файловым ресурсам;
- создание почтовых групп рассылки, содержащих члены из всего корпоративного леса;
- назначение прав доступа для развертываемых операционных систем;
- управление тем, какие компьютеры будут получать автоматизированное развертывание Microsoft Visio;
- управление тем, на кого будет нацелен объект групповой политики (Group Policy);
- делегирование административных прав части Active Directory.

Вам может показаться, что концепция вложения групп является слишком сложной и трудно разрешимой. Когда вы объедините ее с описательным стандартом именования для своих групп, вы сможете сформировать механизм групп, который очень прост в развертывании и управлении и делает возможным детализированное делегированное функций администрирования.

Создание групп Active Directory

Самое время создать какие-нибудь группы Active Directory. Предположим, что вы хотите создать группу, которая будет использоваться только внутри домена. Она будет применяться для назначения прав доступа любому, кто является руководителем в организации. Такое описание говорит о том, что вам нужна область доступа локальной группы домена и тип группы доступа. Ранее вы создали организационную единицу под названием `\BigFirm\Security Groups` внутри домена `bigfirm.com`.

1. Откройте оснастку Active Directory Users and Groups.
2. Щелкните правой кнопкой мыши в центральной панели и выберите в контекстном меню пункт New Group (Создать группу). Откроется диалоговое окно New Object — Group (Новый объект — группа).
3. Введите **`Management`** в качестве имени группы. Это автоматически заполнит поле имени группы для версий, предшествующих Windows 2000 Server (рис. 8.55), которое поддерживается в целях обратной совместимости с унаследованными операционными системами.

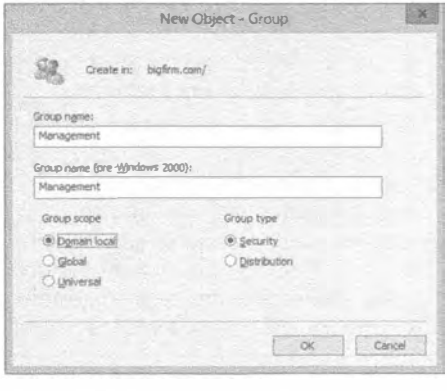


Рис. 8.55. Создание новой группы Active Directory

4. Выберите переключатель Domain local (Локальная домена) в разделе Group scope (Область действия группы) и оставьте выбранным переключатель Security (Доступа) в разделе Group type (Тип группы).
5. Щелкните на кнопке OK, чтобы создать группу.

Рис. 8.56. Добавление описания группы

Вероятно, вы заметили, что во время создания группы отсутствовала возможность редактирования ее свойств. Вполне вероятно, что вы хотите добавить описание и члены в группу. Для этого щелкните правой кнопкой мыши на имени группы и выберите в контекстном меню пункт Properties (Свойства), чтобы открыть диалоговое окно Management Properties (Свойства `Management`), представленное на рис. 8.56.

Вы уже вводили описание для группы. Такой вид документирования позволяет администраторам немедленно понять, для чего предназначена группа. Мы обсуждали необходимость в наличии описания при рассмотрении локальных групп. Документирование подобного рода становится бесконечно более важным в средах Active Directory средних и больших размеров, где могут существовать множество бригад администраторов, работающих с серверами.

Стандарты именования групп

Если домен будет разрастаться до крупных размеров или станет частью леса, то при именовании групп важно выбрать какой-нибудь стандарт и неуклонно придерживаться его. Вспомните, что группы могут использоваться где угодно внутри домена или даже леса Active Directory. При наличии всего лишь двух доменов может поддерживаться большая база данных пользователей и сложная организация. Насколько значащим можно считать имя `Management` в организации, содержащей сотни или тысячи пользователей? А что скажете о корпоративном или правительственном лесе с множеством доменов и десятками тысяч сотрудников? Имя `Management`, вероятно, подойдет для малой или средней организации с единственным сайтом и небольшой бригадой IT-специалистов.

Если вы работаете в организации с множеством отделов или сайтов, можете обдумать создание групп `Milan-Accounts Management` и `Milan-IT Management`, например. Они делают очевидным тот факт, что каждое имя группы ассоциировано с офисом в городе Милане, а члены группы входят в состав руководства отдела. При наличии множества доменов в лесе можно было бы предусмотреть группу вроде `BigFirm-Milan-Senior Management`. Любому администратору в любом домене внутри леса известно, что это группа из домена `BigFirm`, а ее члены работают в офисе в Милане, к тому же все члены входят в состав старшего руководства в данном офисе.

Мы также рекомендуем добавлять к имени группы какой-то префикс, отражающий тип этой группы, например, DL для локальной группы домена, DG для глобальной группы домена или UG для универсальной группы. В итоге получается имя группы вида DG-IT-Management-Milan или DL-IT-Management-Milan. Это позволит легко различать типы групп, что может быть удобно при поиске групп или указании их в сценариях.

В нижней части вкладки General (Общие) отображается тип и область действия группы. Вы можете заметить, что их разрешено изменять. Тем не менее, есть несколько соображений, которые должны быть учтены, прежде чем вносить здесь изменения.

Изменение типа группы с доступа на рассылки означает, что она больше не сможет применяться для назначения разрешений. Вам выдается предупреждение о том, что любые разрешения, назначенные этой группе, могут прекратить свое функционирование. Это особенно важно, если посредством этой группы вы запрещаете доступ к критическим ресурсам.

Мы протестируем, как это работает на общих файловых ресурсах, открыв доступ к папке с использованием группы доступа и добавив в нее несколько членов. Мы также применили разрешения к этой папке в файловой системе. Далее мы проверили, что члены группы имеют доступ к общему ресурсу и все работает должным образом. Затем мы изменили тип группы, сделав ее группой рассылки. Мы проверили разрешения общего ресурса и папки, и группа рассылки по-прежнему имеет права доступа к нему. Тестирование доступа пользователя показывает, что пользователь все еще располагает правами доступа к этой папке. Пока все хорошо. Затем пользователь вышел из системы и снова вошел. И вот тут пользователь теряет права доступа. Группа, ставшая группой рассылки, по-прежнему располагает правами, но они больше не действуют. После этого мы возвратили тип группы обратно, сделав ее группой доступа. Чтобы удостовериться в возобновлении доступа пользователя к общему ресурсу, нужно еще раз выйти и войти в систему.

Такое поведение вовсе не должно считаться плохим — ничуть. Давайте подумаем о сценарии, когда есть много глобальных групп доступа, которым были назначены где-нибудь разрешения на доступ к каким-то общим ресурсам. Вы даже не можете вспомнить, где делались назначения этой группы. Вы принимаете все меры, чтобы выяснить, где эта группа находится и к какому общему ресурсу она принадлежит. Позже вы решаете удалить эту группу, поскольку думаете, что она больше не используется. В такой ситуации вы могли бы просто изменить ее тип на группу рассылки, и все разрешения станут неактивными. Это означает, что группа в какой-то мере отключена. Если спустя некоторое время пользователи начнут жаловаться на отсутствие у них доступа к общему ресурсу XYZ, следовательно, группа все еще эксплуатируется. Мы сознаем, что подход с вовлечением пользователей нельзя назвать особо гладким, но во многих случаях просто нет другого выхода.

Любое действие, которое будет влиять на членов группы, обычно требует от пользователя выйти и снова войти. Вот уже третий раз в данной главе мы заявляем: это определенно было решением практически всех вопросов с членством в группах и назначением прав доступа, с которыми нам приходилось сталкиваться в своей работе. Помните о нем, когда выдаете пользователю права доступа к ресурсу, добавляя его в группу.

Рис. 8.57. Добавление новых членов в группу Active Directory

Вы не можете изменить группу, являющуюся локальной группой домена, чтобы превратить ее в глобальную группу, или наоборот. Однако вы можете поменять область действия группы, сделав ее универсальной группой. После этого вы сможете изменить ее либо на локальную группу домена, либо на глобальную группу. Удостоверьтесь в том, что список членов не конфликтует с предпочитаемой областью действия группы. Если вы изменяете область действия группы с глобальной на локальную домена, то должны быть уверены, что группа не используется в другом домене. Изменение может привести к утере доступа к защищенным ресурсам для членов группы. Администраторы в крупных реализациях лесов должны давать себе отчет, что преобразование существующей группы в универсальную группу потенциально увеличивает трафик репликации глобального каталога.

Функциональность членства в группах домена и в локальных группах работает похожим образом. Откройте диалоговое окно свойств группы (рис. 8.57). Добавлять и удалять члены можно посредством кнопок Add (Добавить) и Remove (Удалить).

На рис. 8.58 видно, что группы домена способны содержать большее число типов объектов, чем локальные группы; новые типы описаны ниже.

- **Other objects (Другие объекты).** Это гибкое решение позволяет добавлять члены, которые создаются приложениями, т.е. это не обычные пользователи, компьютеры или группы.
- **Contacts (Контакты).** Такие объекты создаются в Active Directory для хранения контактной информации о людях или организациях. Это могло бы использоваться для групп рассылки.
- **Service accounts (Учетные записи служб).** Это новая возможность Windows Server 2012, позволяющая настраивать выделенные учетные записи служб вместо создания учетных записей пользователей и назначения их службам.

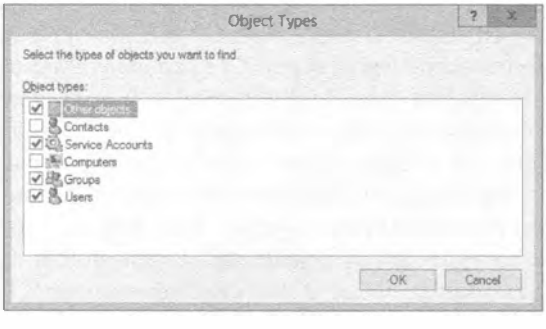


Рис. 8.58. Выбор типов объектов для потенциальных членов

Поскольку вы имеете дело со списком членов группы домена, вы не можете добавлять участников безопасности, основанных на локальной машине, т.е. локальных пользователей или локальные группы. Такие участники безопасности существуют только на своем компьютере, поэтому нет никакого смысла добавлять их группу уровня домена или леса. По этой причине диалоговое окно Locations (Местоположения), показанное на рис. 8.59, предлагает только домены, которые существуют в лесе.

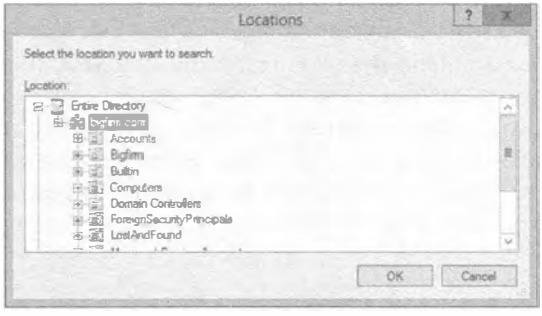


Рис. 8.59. Выбор местоположения для нового объекта члена

Группы домена можно вкладывать друг в друга; другими словами, группа может быть членом другой группы. Членством группы в других группах можно управлять на вкладке Member Of (Членство в группах), приведенной на рис. 8.60.

Вкладка Managed By (Управляется), показанная на рис. 8.61, обладает интересной новой возможностью. Будучи администратором, возможно, вы не имеете понятия, по какой причине осуществляется доступ к защищенным данным. У вас достаточно возможностей, чтобы войти в сеть, не говоря уже о том, чтобы знать о полных бизнес-операциях. Решение лучше всего принимать владельцу данных, обычно начальнику отдела или ведущему специалисту бригады.

Рис. 8.60. Членство группы в других группах

Рис. 8.61. Вкладка Managed By для группы Active Directory

Как часто (но не всегда) выглядит наилучшее решение? Вы можете передать все полномочия по контролю доступа в руки владельца данных. Устраните посредника, в данном случае IT-специалиста. Если владелец данных может управлять доступом к ресурсу, то бизнес сумеет приспособиться к возникающим требованиям.

Вкладка Managed By позволяет выбрать пользователя или группу в качестве владельца данной группы. Этой группе можно назначить права доступа к ресурсам. Но самое интересное мы оставили на закуску. Выбранному владельцу можно выдать права на управление членством в группе, отметив флажок Manager can update membership list (Руководитель может обновлять список членства). Великолепно! Вы не должны выдавать права руководителя для управления правами доступа к общей папке. Можете ли вы представить себе, какие бедствия возникли бы в результате этого? Простое решение заключается в том, чтобы позволить руководителю управлять членством в группах, которые имеют права доступа к общей папке. Понадобится всего лишь предоставить механизм для редактирования членства в группах, такой как оснастка Active Directory Users and Computers, сценарий или, возможно, веб-аплет.

Создание группы в командной строке

Важно освоить управление группами из командной строки. Сначала мы посмотрим, как создать группу, используя команду `dsadd group`. Справку по этой команде можно получить следующим образом:

```
dsadd group /?
```

Ниже приведена простая команда, которая воссоздает то, что можно делать с помощью графического пользовательского интерфейса. Она создает локальную группу домена под названием `Management` внутри организационной единицы `\BigFirm\Security Groups` в домене `bigfirm.com`.

```
dsadd group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -scope l
```

Вот синтаксис команды:

```
dsadd group <отличительное имя новой группы> -scope <локальная домена = l |
глобальная = g | универсальная = u>
```

По умолчанию создается группа доступа. Если необходимо создать глобальную группу, опцию `-scope` можно не указывать. Глобальная группа рассылки создается так:

```
dsadd group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -secgrp no -scope g
```

Изменение в синтаксисе выглядит следующим образом:

```
-secgrp <группа доступа = yes | группа рассылки = no>
```

По умолчанию создается группа доступа, т.е. опцию `-secgrp` можно опустить, если это и требуется.

Помните ли вы, что в графическом пользовательском интерфейсе для создания групп домена предлагалась только возможность создать группу и ничего больше? Для установки свойств или добавления членов приходилось открывать диалоговое окно свойств группы.

В командной строке можно воспользоваться следующей командой:

```
dsadd group "CN=Senior Management, OU=Security Groups,OU=BigFirm,
DC=bigfirm,DC=com" -scope g -desc "This group contains senior managers"
 -memberof "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -members "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
 "CN=Simona Corso,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Эта команда выполняет довольно много действий. В организационной единице `Security Groups` (Группы доступа) создается глобальная группа доступа по имени `Senior Management` (Старшее руководство). В качестве описания группы указывается строка `This group contains senior managers` (Эта группа содержит старших руководителей). Группа `Senior Management` добавляется в виде члена в группу `Managers`. И, наконец, в новую группу `Senior Managers` добавляются два пользователя.

Для модификации существующей группы применяется команда `dsmod`. Вот как получить справочную информацию по ней:

```
dsmod group /?
```

Показанная ниже команда добавляет пользователей `Steve Red` и `Simona Corso` в группу `Management`:

```
dsmod group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -addmbr "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
 "CN=Simona Corso,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Синтаксис выглядит следующим образом:

```
dsmod group <имя DN группы для управления>
 -addmbr <имена DN пользователей, добавляемых в группу>
```

А вот как удалить пользователя `Steve Red` из группы:

```
dsmod group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
-rmmbr "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

С помощью приведенной далее команды можно очистить существующий список членов группы и добавить список на замену:

```
dsmod group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -chmbr "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Посредством следующей команды можно изменить область действия группы, сделав ее универсальной:

```
dsmod group "CN=Management,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com"
 -scope u
```

Вот синтаксис опции `-scope`:

```
-scope <локальная домена = l | глобальная = g | универсальная = u>
```

К сожалению, с помощью команды `dsmod group` нельзя установить свойства руководителя для группы.

Каким образом удалить группу? Это очень легко:

```
dsrm "CN=Management, OU=Security Groups,OU=BigFirm,DC=big firm,DC=com"
```

Эта команда удалит группу Management. Она запрашивает подтверждение удаления. Пропустить такой запрос можно следующим образом:

```
dsrm "CN=Management, OU=Security Groups,OU=BigFirm,DC=big firm,DC=com"
 -noprompt
```

Задачи администрирования, выполняемые в понедельник утром

А теперь мы рассмотрим распространенные операционные задачи, которые могут делаться на регулярной основе. Наш опыт показывает, что любой сотрудник службы поддержки обнаружит, что утро каждого понедельника расходуется на выполнение этих задач, если механизм аутентификации спроектирован недостаточно тщательно. Чтобы понять, что мы имеем в виду, почитайте еще раз обсуждение кодовых фраз и смарт-карт ранее в этой главе. Мы рассмотрим участников безопасности домена, поскольку именно они отнимают большую часть времени.

Забытые пароли

Первая задача имеет отношение к сотруднику, который не может запомнить свой пароль. Обычно это самая частая причина обращения в службу поддержки после выходных. Давайте посмотрим, как сбросить пароль для пользователя. В конце концов, пользователь является вашим заказчиком, и вы должны обеспечить для него качественное и своевременное обслуживание.

1. Если вы пользуетесь графическим интерфейсом, перейдите к учетной записи нужного пользователя внутри оснастки Active Directory Users and Computers.
2. Щелкните правой кнопкой мыши на имени пользователя и выберите в контекстном меню пункт Reset Password (Сбросить пароль), чтобы открыть диалоговое окно Reset Password (Сброс пароля).
3. Введите новый пароль для пользователя, как показано на рис. 8.62

Новый пароль должен удовлетворять политикам паролей, которые применяются к пользователю. Необычность ситуации в том, что вы собираетесь диктовать этот пароль пользователю по телефону. Согласно нашему опыту, вы должны выбрать такой пароль, который легко продиктовать. Будьте осторожны, т.к. вы можете иметь дело с людьми, для которых родным языком является не английский. Пароль наподобие Password123456789 легко сообщить по телефону, и он удовлетворяет стандартным требованиям к паролям.

Рис. 8.62. Сбрасывание пароля для пользователя

Заметили ли вы, что флажок User must change password at next logon (Пользователь должен изменить пароль при следующем входе) отмечен? Это его состояние по умолчанию. Он очень удобен, потому что, как вы увидите, вполне допустимо передавать один и тот же пароль всем обратившимся к вам пользователям. Принуждение пользователя к изменению своего пароля защитит его учетную запись, к тому же это означает, что никто в отделе IT не будет знать пароль пользователя.

В нижней части диалогового окна Reset Password находится флажок Unlock the user's account (Разблокировать учетную запись пользователя). Он доступен для отметки только в случае, если учетная запись пользователя была заблокирована. Пользователи, не имеющие навыков в области IT, могут быть не в состоянии понять сообщения на своих рабочих столах, которые объясняют причины невозможности входа в систему. Изменение пароля пользователя без разблокирования его учетной записи не поможет ему войти в систему. Не будет никакого вреда от того, что вы отметите данный флажок, если имеете дело с неуверенно выражающимся пользователем или многократным нарушителем.

Ниже показано, как можно изменить пароль пользователя с применением команды dsmod user:

```
C:\Users\Administrator>dsmod user "CN=Steve Red,OU=Users,OU=BigFirm,
DC=bigfirm, DC=com" -pwd *
Enter User Password:
Введите пароль для пользователя:

Confirm user password:
Подтвердите пароль для пользователя:

dsmod succeeded:CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
dsmod выполнилась успешно:CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
```

Опция -pwd * указывает на то, что вы введете пароль и подтвердите его. В качестве альтернативы пароль можно сбросить в самой команде:

```
dsmod user "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
 -pwd Password12345678
```

К любой из этих команд можно добавить дополнительную опцию, чтобы заставить пользователя изменить свой пароль при следующем входе:

```
dsmod user "CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
 -pwd Password12345678 -mustchpwd yes
```

Заблокированные пользователи

Ох уж эти политики блокирования паролей... Подавляющему большинству "экспертов по безопасности", которых вы встретите в Интернете или лично, нравится политика "три неудавшихся попытки входа в систему в течение 30 минут должны приводить к блокировке учетной записи". Знаете что? Это отличный рецепт для упрощения атаки типа "отказ в обслуживании". Получите на пару минут доступ к настольному компьютеру внутри леса посредством учетной записи обычного пользователя, и вы сможете запустить сценарий, который вмиг совершит по пять неудавшихся попыток входа для каждого пользователя в Active Directory. В итоге будут заблокированы все пользователи кроме стандартных учетных записей администраторов домена. Бизнес-деятельность организации прекратится. Именно по этой при-

чине настоящие эксперты по безопасности рекомендуют вам очень хорошо обдумать применение варианта блокирования для паролей. (Внутри врезки "Случай для кодовых фраз" ранее в этой главе была описана альтернатива.) Как раз по этим соображениям блокировки по умолчанию отключены в стандартной политике домена (Default Domain Policy). И по нашему мнению это очень хорошо. Тем не менее, некоторые организации включают данную политику. Они могут иметь веские основания для этого. Следовательно, важно знать, каким образом разблокировать учетную запись пользователя. Отметим, что это определено в объекте стандартной групповой политики (GPO) домена внутри Active Directory. Стандартной настройкой в Windows Server 2012 является 0, т.е. не блокировать учетные записи пользователей после неудавшихся попыток входа.

Рис. 8.63. Пользователь Active Directory заблокирован

Два простых сценария блокировки

Первый сценарий связан с ситуацией, когда пользователь сообщил о том, что компьютер проинформировал о его блокировании. Ему известен пароль, поэтому сбрасывать его не придется. С помощью оснастки Active Directory Users and Computers найдите учетную запись пользователя и откройте для нее диалоговое окно свойств. Как показано на рис. 8.63, вкладка Account (Учетная запись) содержит сообщение, информирующее о том, что учетная запись заблокирована. Решение очень простое — вы разблокируете учетную запись. Конечно, пользователь вдобавок мог забыть свой пароль, и тогда его нужно будет сбросить.

Второй сценарий касается ситуации, когда знание пользователя о проблеме ограничивается тем, что он не может войти. Проблем может быть две. Пользователь мог забыть свой пароль, или его учетная запись оказалась заблокированной. Вы должны убить двух зайцев одним выстрелом, имея дело с обеими возможностями. Откройте диалоговое окно Reset Password (рис. 8.64).

Рис. 8.64. Разблокирование учетной записи пользователя и сброс пароля

К сожалению, похоже, что способ разблокирования учетных записей в командной строке отсутствует — разумеется, исключая PowerShell.

Итак, мы раскрыли все возможности базового управления пользователями и группами, которые являются общими для всех версий Windows Server. А теперь давайте посмотрим, что появилось нового в Windows Server 2012.

Использование новых средств для управления пользователями и группами

Все, что обсуждается в данном разделе, применимо к версиям Windows Server 2008 R2, Windows Server 2012 и Windows Server 2012 R2. В Windows Server 2012 были внесены два значительных изменения, имеющие отношение к управлению пользователями и группами.

- Центр администрирования Active Directory (Active Directory Administrative Center — ADAC) был обновлен и построен поверх PowerShell. Кроме того, в консоль были интегрированы новые средства, такие как корзина Active Directory с графическим пользовательским интерфейсом и детализированные политики паролей.
- В ADAC была добавлена хронология PowerShell для более простого управления и создания пользователей и групп, а также других объектов.

В Windows Server 2008 R2 уже был интегрирован инструмент PowerShell 2.0, и в плане управления пользователями и группами каких-либо новых командлетов в Windows Server 2012 не появилось. Хотя в Windows Server 2012 интегрирован новый инструмент PowerShell 3.0, а в Windows Server 2012 R2 — PowerShell 4.0, большинство новых командлетов, связанных с Active Directory, предназначены для управления компонентами Active Directory, а не пользователями и группами.

Тем не менее, по ссылке `http://tinyurl.com/5otmff` можно загрузить бесплатные команды PowerShell для Active Directory от Quest (Free PowerShell Commands for Active Directory). Эти командлеты обладают синтаксисом, похожим на синтаксис встроенных командлетов Windows Server 2012, но в некоторых отношениях предлагают чуть лучшую поддержку и гибкость, например, при доступе к атрибутам пользователей. В настоящем разделе мы рассмотрим встроенные командлеты PowerShell в Windows Server 2012.

Центр администрирования Active Directory

Разработчики из Microsoft расширили и привели в порядок графический пользовательский интерфейс нового центра администрирования Active Directory, сделав его больше ориентированным на задачи. Ходят слухи о том, что инструмент Active Directory Users and Computers (Пользователи и компьютеры Active Directory), или ADUC, в дальнейшем не будет поддерживаться, и основное внимание будет сосредоточено на Active Directory Administrative Center (ADAC). Тем не менее, в Windows Server 2012 доступны оба инструмента, и один не может работать без другого. Мы считаем ADUC унаследованным, а ADAC — будущим инструментом.

Стратегия Microsoft предельно ясна: PowerShell. Учитывая, что ADAC — это просто графический пользовательский интерфейс для доступа к функциональности

PowerShell, полезно исследовать возможности данного инструмента. В Microsoft хотели предоставить инструмент для быстрого и простого выполнения часто повторяющихся задач, таких как обработка блокировок пользователей утром по понедельникам. Инструмент ADAC доступен через меню Tools (Инструменты) диспетчера серверов на контроллере домена Windows Server 2012. Его можно также использовать на компьютере Windows 8, на котором установлены инструменты дистанционного администрирования серверов (Remote Server Administration Tools) для Windows 8 (`http://www.microsoft.com/en-us/download/details.aspx?id=28972`). Если на компьютере функционирует версия Windows 8.1, и вы хотите управлять из него сервером Windows Server 2012 R2, проследуйте по ссылке `http://www.microsoft.com/en-us/download/details.aspx?id=39296`. Данный инструмент загружается несколько дольше, чем Active Directory Users and Computers, так что можете запускать его утром и оставлять в работающем состоянии до конца дня.

Основные элементы ADAC

Открыв ADAC, вы увидите, что означает ориентация на *задачи* (рис. 8.65). В центральной панели находится интерфейс, специально предназначенный для сброса паролей и разблокирования учетных записей пользователей. Это наиболее распространенные задачи Active Directory, выполняемые персоналом IT, так что их наличие в инструменте имеет смысл.

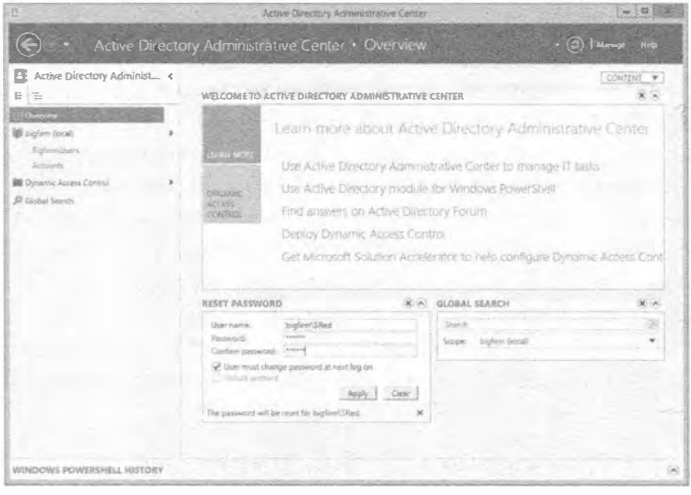


Рис. 8.65. Сброс пароля для пользователя в ADAC

Что бы происходило в отсутствие ADAC, когда пользователь позвонил в корпоративную службу поддержки с просьбой сбросить его пароль или разблокировать учетную запись? Техническим специалистам из службы поддержки понадобится найти этого пользователя в организационных единицах Active Directory. После этого они могут щелкнуть правой кнопкой мыши на имени пользователя, открыть диалоговое окно его свойств и выполнить задачу. Это предполагает знание инженером службы поддержки способа поиска в Active Directory. Кроме того, тратится также и время. На рис. 8.65 видно, что с помощью ADAC инженер службы поддержки просто вво-

дит имя пользователя и новый пароль. Флажок Unlock account (Разблокировать учетную запись) недоступен, т.к. эта учетная запись не заблокирована.

Инструмент ADAC также облегчает нахождение объектов службой поддержки. На рис. 8.66 показано, что для поиска объекта можно ввести его имя.

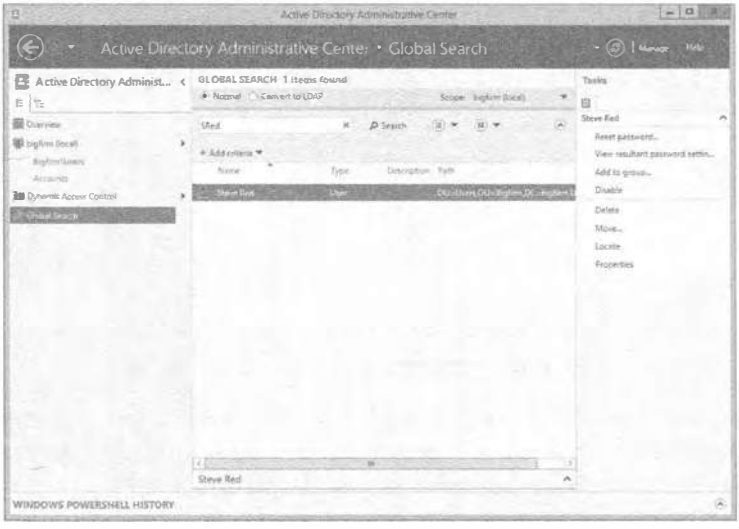


Рис. 8.66. Поиск объекта в Active Directory

На рис. 8.66 представлены результаты поиска. Вы видите, насколько легко было найти объект пользователя SRed. Теперь инженер службы поддержки может щелкнуть правой кнопкой мыши на объекте пользователя и выполнить для него необходимые задачи администрирования. Средство поиска довольно интеллектуально, потому что оно ищет в атрибутах объекта, т.е. свойствах объекта. Инженер мог бы искать *S*, *Steve* или *Steve Red* и все равно найти объект пользователя SRed. Поиск совершенно не ограничивается объектами пользователей! Искать в домене можно объект любого типа, такой как группы и компьютеры.

Чтобы добраться до средства Global Search (Глобальный поиск), щелкните на элементе Global Search в навигационной панели слева. В панели справа отобразятся поисковые опции средства Global Search.

Щелчок на раскрывающемся списке Add criteria (Добавить критерий) предоставляет доступ к действительно мощным опциям для уточнения поиска (рис. 8.67). Взгляните на эти встроенные критерии и подумайте, насколько полезными они могут оказаться. Каждое утро вы можете начинать с поиска заблокированных учетных записей и разблокирования их до того, как сотрудники прибудут на свои рабочие места. При рассмотрении локальных учетных записей пользователей мы рекомендовали отключать учетные записи вместо немедленного их удаления. Чтобы установить один из критериев поиска, отметьте флажок рядом с критерием и щелкните на кнопке Add (Добавить).

На рис. 8.67 выбрана опция Users with enabled accounts who have not logged on for more than a given number of days (Пользователи с включенными учетными данными, которые не входили на протяжении заданного количества дней).

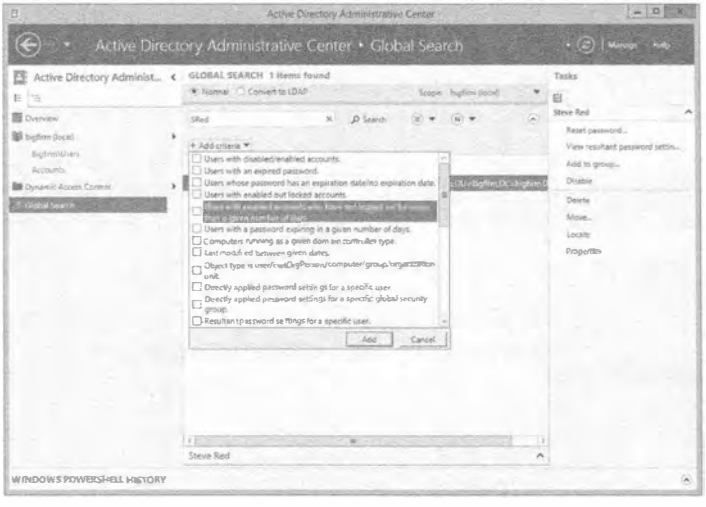


Рис. 8.67. Потенциальный критерий поиска

В центре диалогового окна, показанного на рис. 8.68, видно, что вы можете выбрать количество дней из заранее определенного диапазона опций. Это очень удобно. В идеальном случае отдел кадров должен связываться с IT-отделом всякий раз, когда сотрудник покидает компанию. Тем не менее, все мы люди, и все мы допускаем ошибки. Применяя такой поисковый запрос, вы можете идентифицировать "просроченные" учетные записи пользователей и отключить их. Чтобы удалить критерий поиска, щелкните на значке × серого цвета справа.

Вы даже можете построить более сложный запрос, щелкнув на раскрывающемся списке Add criteria. Например, типом объекта мог бы быть Computer (Компьютер), а имя объекта начинаться с *B*. Это значит, что вы получите результаты поиска, которые не содержат объекты других типов наподобие групп, пользователей и организационных единиц.

Рис. 8.68. Нахождение всех пользователей, которые не входили в течение 15 дней

Щелкнув на небольшом значке с дискетой правее поля поиска, запрос можно сохранить для последующего использования. Запросу назначается имя (лучше описательное), а доступ к нему осуществляется по щелчку на значке, расположенном слева от значка с дискетой. Раскроется список всех сохраненных запросов. Выбор сохраненного запроса приводит к его загрузке и выполнению.

После того, как объект найден, с ним необходимо что-то делать. Когда объект выбран, в панели Tasks (Задачи) справа отобразятся контекстно-чувствительные действия. Для управления выбранным объектом понадобится щелкнуть на одной из задач.

Навигация в ADAC

Ознакомившись с основами, давайте начнем с изучения навигации в ADAC. Навигационная панель имеет списковое представление (отображаемое по умолчанию) и древовидное представление. Списковое представление содержит предварительно выбранное множество местоположений, включая перечисленное ниже:

- область ADAC Overview (Обзор ADAC), с которой вы начинаете и в которой можно быстро обработать базовые запросы пользователей и производить простой поиск;
- домен, откуда можно переходить в любую организационную единицу или контейнер;
- контейнеры `Users` (Пользователи) и `Computers` (Компьютеры), где в идеальном случае ничего не добавляется;
- инструмент Global Search, с которым вы уже знакомы.

Чтобы добавить другие местоположения, щелкните правой кнопкой мыши в навигационной панели и выберите в контекстном меню пункт Add Navigation Nodes (Добавить узлы для навигации). Откроется окно, в котором можно проходить по структуре Active Directory (рис. 8.69).

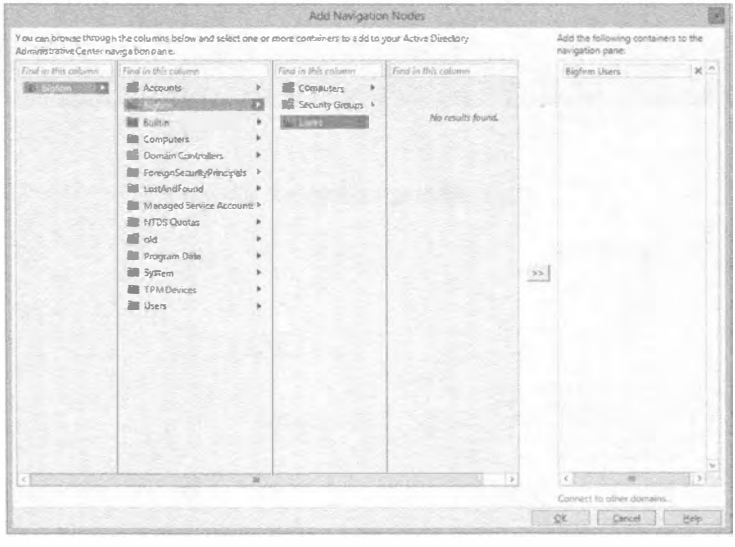


Рис. 8.69. Добавление узла для навигации

Мы перешли к \BigFirm\Users и добавили эту организационную единицу в правую часть окна. Заметили ли вы элемент управления Connect to other domains (Подключиться к другим доменам) в нижнем правом углу, который предназначен для перехода к организационным единицам или контейнерам в других доменах внутри леса? Его можно применять для управления несколькими доменами во множестве лесов с помощью ADAC.

На рис. 8.70 видно, что мы щелкнули на кнопке OK, чтобы добавить организационную единицу \BigFirm\Users к списковому представлению в ADAC. Теперь вы можете быстро переходить в организационную единицу для управления учетными записями пользователей — еще один метод, позволяющий сберечь время при ежедневном администрировании. Панель Tasks содержит новые действия, позволяющие проводить администрирование внутри этой организационной единицы.

Обратите внимание, что создаваемые узлы для навигации будут отображаться и в древовидном, и в списковом представлении.

Древовидное представление в навигационной панели на рис. 8.71 предлагает более традиционный метод навигации, который вы применяли до появления ADUC.

Давайте проделаем определенную работу. В этом примере будет создаваться пользователь. Перейдите к контейнеру \BigFirm\Users, используя только что созданный узел для навигации в списковом представлении, и щелкните на элементе New⇨User (Создать⇨Пользователь) в панели Tasks. Откроется диалоговое окно, представленное на рис. 8.72. Ого! Это огромное диалоговое окно поначалу может слегка приводить в растерянность. Давайте осмотримся вокруг, прежде чем что-то делать. Для начала упростим обстоятельства. Чтобы создание пользователя стало возможным, вам необходимо заполнить только поля, помеченные символом звездочки (*) красного цвета. Навигационная панель слева подсказывает, что данное окно разбито на разделы. С помощью кнопки Sections (Разделы), находящейся в правом верхнем углу, можно сворачивать или разворачивать эти разделы. Это позволяет скрывать любые разделы, которыми вы никогда не пользуетесь. Инструмент ADAC запомнит, какие разделы свернуты или развернуты.

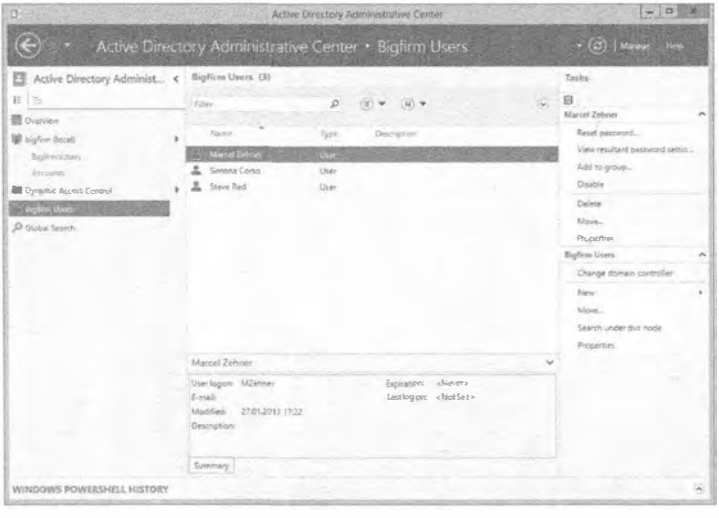


Рис. 8.70. Использование узла для навигации

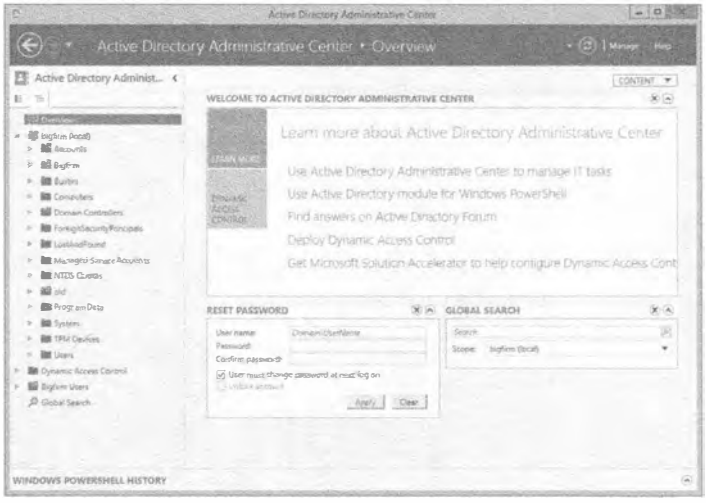


Рис. 8.71. Древовидное представление в ADAC

Рис. 8.72. Создание нового пользователя в ADAC

На рис. 8.73 показано это же диалоговое окно, в котором были свернуты разделы Organization (Организация) в центре окна и Encryption options (Параметры шифрования) справа вверху. Кроме того, в нем заполнены поля, чтобы создать нового пользователя по имени `Kevin Greene`. Вместо прохода по экранам мастера и затем открытия диалогового окна свойств пользователя для завершения операции, все необходимое можно сделать здесь. В этом диалоговом окне доступны все распространенные опции для настройки пользователя. Такое первоначально приводящее к растерянности окно сокращает время, затрачиваемое на создание и конфигурирование учетной записи пользователя.

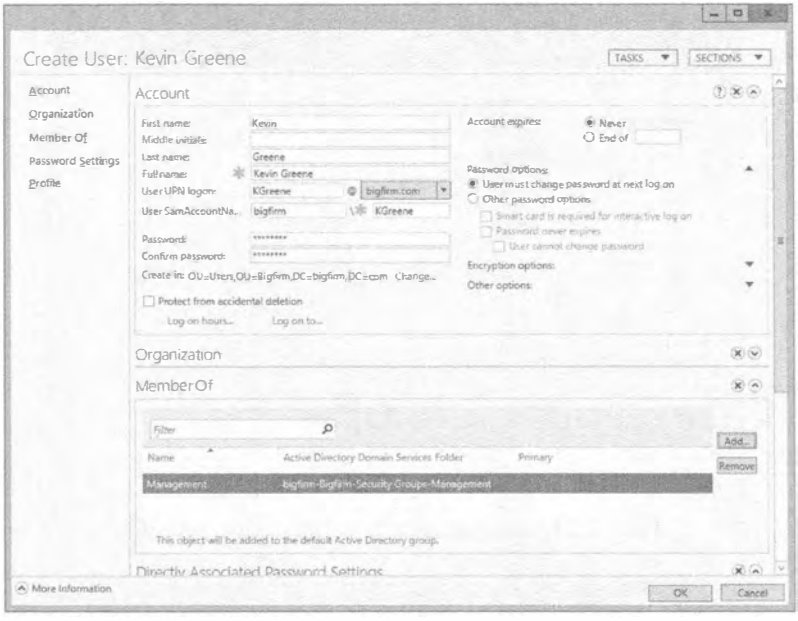


Рис. 8.73. Диалоговое окно со свернутыми разделами в ADAC

Для создания этого пользователя мы могли бы просто ввести полное имя и имя учетной записи SAM. Что произойдет, если вы не введете пароль, поле которого не помечено как обязательное? Учетная запись будет создана, но заблокирована. Вы не сможете ее включить, поскольку отсутствие пароля идет вразрез со стандартной политикой паролей в домене. Вы должны сначала сбросить пароль и только затем можно будет включить учетную запись.

Ниже перечислены шаги, которые придется выполнить.

1. Введите имя пользователя.
2. Укажите пароль.
3. Добавьте пользователя в группу.
4. Щелкните на кнопке OK.

Учетная запись создается и добавляется в организационную единицу, в которой вы находитесь.

Возможно, вы заметили, что для объектов пользователей доступны далеко не все атрибуты или свойства. Общие свойства на месте, но множество других отсутствует. Скорее всего, эти свойства будут конфигурироваться в Active Directory через политики. Тем не менее, к ним по-прежнему можно получить доступ.

На рис. 8.74 показаны свойства учетной записи пользователя в ADAC. В окне появился новый раздел под названием Extensions (Расширения). Он позволяет просматривать и конфигурировать расширенные возможности объекта.

Как видно на рис. 8.75, мы возвратились к списковому представлению и создали дополнительный узел для администрирования организационной единицы `\BigFirm\Security Groups`. Наступило время заняться управлением группами в ADAC. Щелкните на элементе New⇨Group (Создать⇨Группа) в панели Tasks.

На рис. 8.76 показано, что подобно диалоговому окну для создания пользователя, некоторые разделы можно сворачивать. Сейчас это и будет сделано.

Чтобы упростить представление, можете щелкнуть на кнопке Sections и свернуть раздел Member Of (Членство в группах), например.

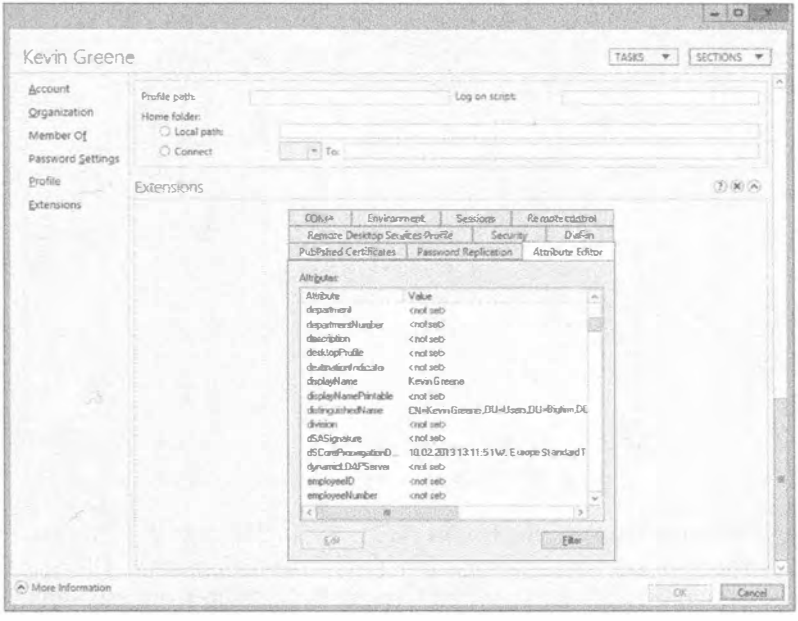


Рис. 8.74. Просмотр свойств пользователя в ADAC

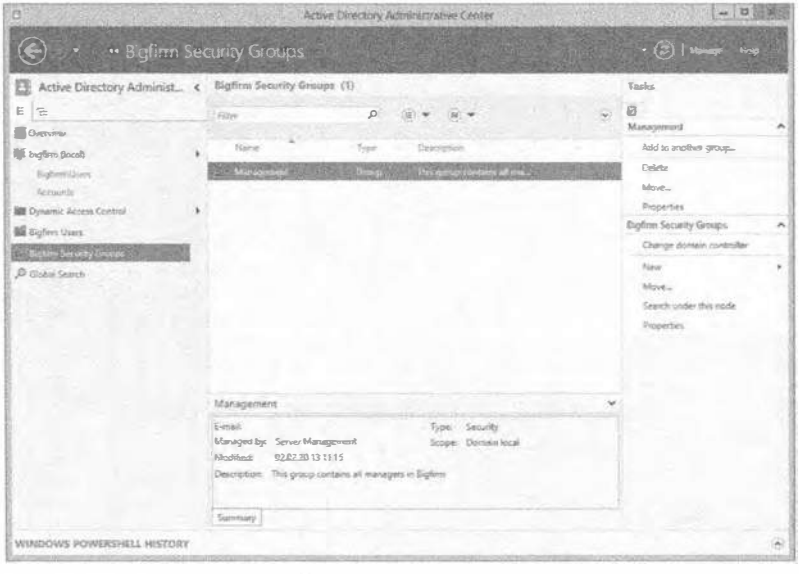


Рис. 8.75. Дополнительный узел для администрирования групп доступа

Рис. 8.76. Создание новой группы в ADAC

Давайте создадим группу по имени `Helpdesk`. На рис. 8.77 приведено заполненное диалоговое окно для создания новой группы `Helpdesk`. Опять-таки, в этом единственном диалоговом окне можно вводить большой объем информации, не проходя по экранам мастера и затем редактируя свойства объекта группы.

Рис. 8.77. Создание группы `Helpdesk` в ADAC

Выполните перечисленные ниже шаги.

1. Введите имя группы и заполните поле Group (SamAccountName) (Имя учетной записи SAM для группы).
2. Укажите тип и область действия группы.
3. Отметьте флажок Protect from accidental deletion (Защитить от случайного удаления), чтобы эту группу нельзя было непредумышленно удалить.
4. Укажите адрес электронной почты для распространения почты (это требует совместимой почтовой службы).
5. Введите описание и примечания.
6. Укажите руководителя группы, который будет управлять членством в группе.

   Теперь члены старшего руководства могут изменять членство в группе `Helpdesk`.
7. Добавьте двух пользователей в группу `Helpdesk`.
8. Щелкните на кнопке OK, чтобы создать группу.

Возвратившись в окно свойств объекта группы, можно отредактировать конфигурацию или членство в группе (рис. 8.78).

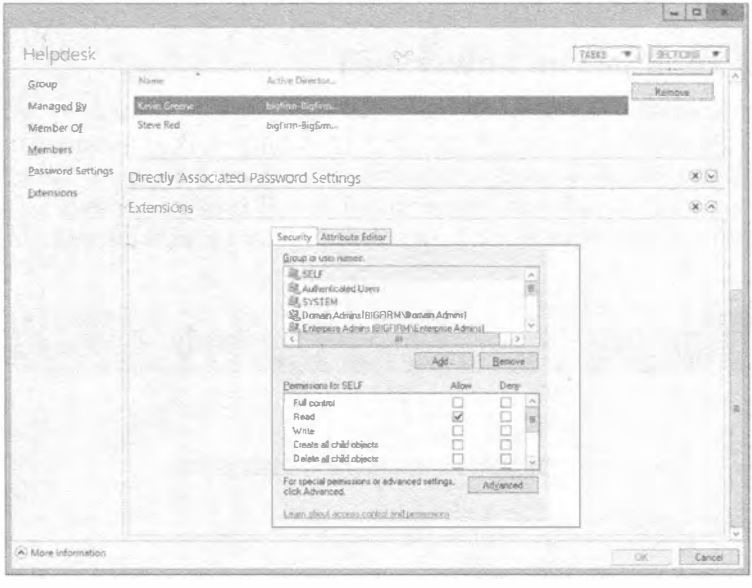


Рис. 8.78. Просмотр свойств объекта группы в ADAC

Как и со свойствами объекта пользователя, в диалоговом окне для создания объекта группы атрибуты из раздела Extensions не видны.

В завершение работы с Active Directory Administrative Center мы приведем еще несколько советов.

- Инструмент ADAC может быть остановлен только на машинах с Windows Server 2012 и компьютерах с Windows 8, на которых функционируют Remote Server Administrative Tools (RSAT).

- Вы можете управлять доменами в своем лесе или в других лесах, связанных доверительными отношениями, и вы располагаете для этого соответствующими разрешениями.
- В навигационной панели вы можете щелкнуть правой кнопкой мыши на имени домена и посредством контекстного меню подключиться к другим контроллерам доменов.

  Это может делаться для выполнения работ на контроллере домена в другом сайте с целью, например, управления локальными пользователями и получения немедленных результатов, не ожидая репликации между сайтами.
- Чтобы можно было использовать ADAC для управления доменом, по крайней мере, на одном контроллере этого домена должны быть установлены веб-службы Active Directory (Active Directory Web Services — ADWS).

  Если вы устанавливаете контроллер домена Windows Server 2012, то службы ADWS установятся и запустятся автоматически. Они предоставляют интерфейс в виде веб-служб для управления Active Directory с помощью таких средств, как ADAC и PowerShell.

Внутри области ADAC Overview в ADAC вы найдете гиперссылки на онлайновое содержимое по ADAC и новым модулям PowerShell для управления Active Directory с применением PowerShell.

Просмотр хронологии PowerShell

Вы могли заметить, что в ADAC имеется один новый раздел, который называется Windows PowerShell History (Просмотр хронологии PowerShell). По обыкновению он свернут, и если вы не осведомлены о нем, то будете спокойно работать в ADAC, даже не подозревая о его существовании. Чтобы развернуть раздел Windows PowerShell History, понадобится щелкнуть на кнопке со стрелкой, указывающей вниз (рис. 8.79).

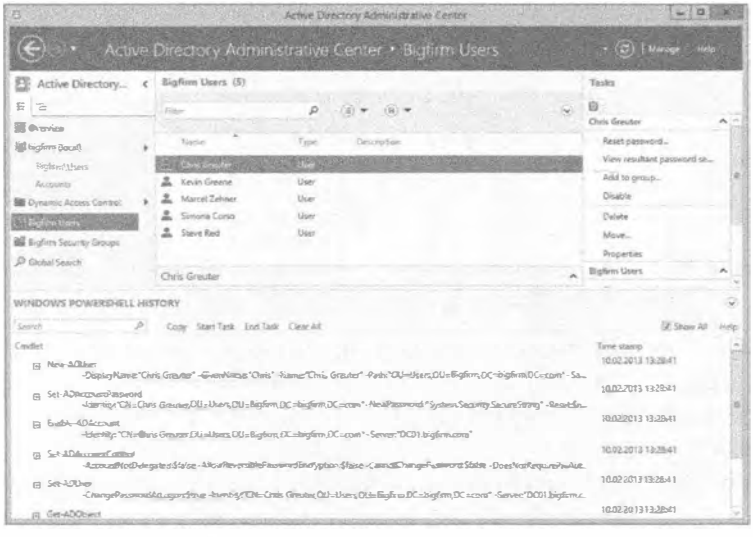


Рис. 8.79. Отображение раздела Windows PowerShell History

На рис. 8.79 видно, что есть новый пользователь по имени `Chris Greuter`. Непосредственно после щелчка на кнопке OK в диалоговом окне создания пользователя в хронологии PowerShell появляются команды PowerShell. Например, чтобы создать простого включенного пользователя с минимальным вводом, запускаются пять разных командлетов. Внимательно взглянув на эти команды, вы увидите, что они предпринимают следующие действия.

1. Командлет `New-ADUser` настраивает базовую структуру объекта пользователя без пароля. Вследствие этого учетная запись блокируется.
2. Командлет `Set-ADAccountPassword` устанавливает пароль для пользователя.
3. Командлет `Enable-ADAccount` включает учетную запись пользователя, т.к. пароль был установлен.
4. Командлет `Set-ADAccountControl` устанавливает все параметры учетной записи AD, которые расположены на вкладке Account (Учетная запись) диалогового окна свойств объекта пользователя. Эти параметры предназначены для указания таких характеристик, как имеет ли пользователь возможность изменять пароль либо истекает ли срок действия его пароля.
5. Командлет `Set-ADUser` устанавливает дополнительные параметры пользователя, вроде того, должен ли пользователь изменить пароль при следующем входе или требуется ли для входа смарт-карта.

Именно так ADAC работает "за кулисами". Разумеется, если вы собираетесь создать объект пользователя, то не будете запускать пять командлетов по отдельности; вместо этого вы упакуете всю необходимую информацию в одну строку.

Нет разницы в том, создаете вы пользователя, группу или даже организационную единицу; инструмент ADAC регистрирует в этом окне каждый шаг PowerShell. Чтобы просмотреть полные детали по каждой команде, можете щелкнуть на значке + слева от командлета. Это приведет к разворачиванию всех параметров, как показано на рис. 8.80.

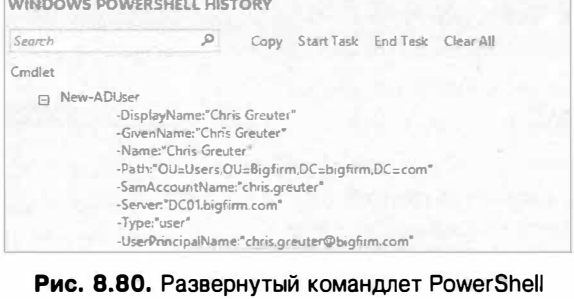


Рис. 8.80. Развернутый командлет PowerShell

При желании можете щелкать на всех значках +, и ADAC обучит вас этим командам. Разве это не хорошая возможность? На самом деле все даже еще лучше. В верхней части раздела Windows PowerShell History расположены ссылки на различные действия. В поле Search (Поиск) можно искать определенную команду. По мере набора панель результатов будет корректироваться согласно введенным данным в этом поле.

Рядом с полем Search находятся ссылки на пять действий, а также ссылка Help (Справка):

- Copy (Копировать)
- Start Task (Начать задачу)
- End Task (Завершить задачу)
- Clear All (Очистить все)
- Show All (Показать все)

Действие Copy позволяет скопировать полную строку команды из хронологии PowerShell с целью последующей ее вставки в окно редактора, такого как Notepad (Блокнот). Можно даже выбрать несколько строк команд, щелкая на них при удерживаемой в нажатом состоянии кнопке <Ctrl>, и затем щелкнуть на Copy.

Скорее всего, вы уже поняли, что этот небольшой раздел быстро заполняется, и если необходимо отследить некоторое действие, то могут возникнуть проблемы с выяснением, к какому шагу относится тот или иной командлет. По этой причине могут использоваться действия Start Task, End Task и Clear All. Прежде чем начать, удостоверьтесь в том, что флажок Show All, показанный ранее на рис. 8.79, не отмечен. Позже мы объясним, что он делает, но пока оставьте его неотмеченным и выполните следующие шаги.

1. Щелкните на Clear All.

   Это приведет к очистке всех команд в панели Windows PowerShell History.

2. Щелкните на Start Task. Откроется прямоугольная область, где необходимо ввести значащее описание задачи, которую планируется выполнить, например, **`New User`** (Новый пользователь).

3. Создайте нового пользователя в Active Directory с применением ADAC, щелкните на кнопке OK в диалоговом окне создания пользователя и затем щелкните на End Task.

4. Щелкните на Start Task еще раз и введите в прямоугольной области описания задачи **`Delete User`** (Удалить пользователя).

5. Перейдите к ранее созданному пользователю в ADAC и удалите его.

6. Снова щелкните на End Task. Вы должны получить сгруппированное представление команд, как на рис. 8.81.

   Вы получаете не только структурированный обзор в окне; скопировав команды внутрь редактора, вы увидите, что описания `New User` и `Delete User` добавлены к сценарию в виде комментариев, что действительно удобно.

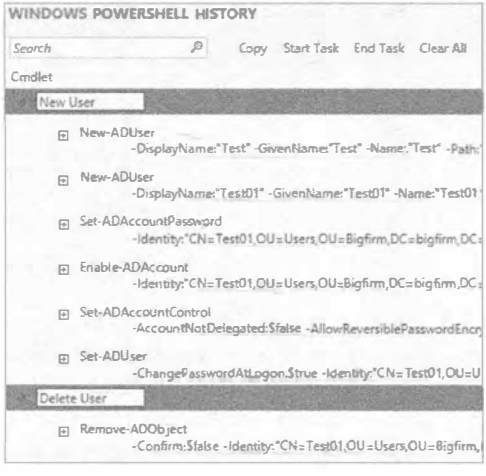


Рис. 8.81. Группирование команд PowerShell

Последней опцией является Show All. Если вы отметите этот флажок, в панели Windows PowerShell History отображается больше команд.

7. Выберите организационную единицу \BigFirm\Users и нажмите клавишу <F5>, чтобы обновить ее содержимое.

   Обратите внимание, что отобразились команды, которых вы ранее не видели. Почему это произошло? Подумайте о следующем: инструмент ADAC построен поверх PowerShell, так что когда вы обновляете организационную единицу, на самом деле вы заставляете ADAC повторно запросить ее. В PowerShell это делается с помощью командлета `Get-ADObject`. Скорее всего, вам не нужно такое обилие команд PowerShell, поэтому лучше снимите отметку с флажка Show All.

Итак, вы ознакомились с основами создания объектов в PowerShell. В следующем разделе PowerShell будет рассматриваться более глубоко.

Модуль Active Directory для Windows PowerShell

Модуль Active Directory для Windows PowerShell позволяет выполнять операции в командной строке и внутри сценариев с использованием нового языка оболочки Microsoft. Подобно ADAC, он доступен только в Windows Server 2012 и Windows 8 (с установленными инструментами Remote Server Administration Tools). Также подобно ADAC, в домене, которым нужно управлять, должна быть установлена роль ADWS хотя бы на одном контроллере домена. Чтобы обеспечить оптимальную производительность, на контроллерах домена Windows Server 2003 или Windows Server 2008 внутри сайта можно установить службу шлюза для управления Active Directory (Active Directory Management Gateway Service; `http://tinyurl.com/yblxwey`). Теперь мы рассмотрим, как управлять пользователями и группами с применением данного модуля PowerShell. Мы опишем наиболее распространенные сценарии, но настоятельно рекомендуем продолжить изучение этой темы на веб-сайте Microsoft:

```
http://technet.microsoft.com/en-us/library/hh852274.aspx
```

Вы не будете использовать обычное окно PowerShell. Вместо этого необходимо запустить модуль Active Directory для Windows PowerShell через меню Administrative Tools (Администрирование) либо на контроллере домена Windows Server 2012, либо на машине Windows 8 с установленными инструментами RSAT.

В случае Windows Server 2008 R2 при открытии окна PowerShell в первый раз понадобится загрузить модуль Active Directory с помощью следующей команды:

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
```

В Windows Server 2012 ситуация более комфортная, т.к. этот модуль загружается автоматически. Как только вы введете команду, которую оболочка распознает как командлет Active Directory, модуль автоматически загрузится.

Базовые команды PowerShell для создания объектов Active Directory, подобных пользователям, группам, компьютерам, организационным единицам и т.д., в Windows Server 2012 не изменились. Таким образом, если вы создавали сценарии с помощью Active Directory для PowerShell 2.0, они будут также работать в Windows Server 2012 и Windows Server 2012 R2.

Обновление справочных файлов

Перед тем, как погружаться в исследования PowerShell 3.0/4.0, мы настоятельно рекомендуем обновить локально хранящиеся справочные файлы. Это легко делается запуском командлета `Update-Help`. Он подключится к Интернету и загрузит последние справочные файлы для текущих модулей, загруженных в оболочку, и для модулей, установленных в переменной среды `PSModulePath`. Сами справочные файлы являются файлами CAB, содержащими XML-файлы, которые будут автоматически извлечены и скопированы по соответствующему пути.

Хорошо, а как быть, если подключение к Интернету отсутствует? Вы можете воспользоваться командлетом `Save-Help`, в котором указывается путь для сохранения файлов. Вы просто переносите справочные файлы на отключенный компьютер и запускаете команду, например, `Update-Help -SourcePath C:\Temp`, чтобы импортировать их на этот компьютер с устаревшими данными.

Доступен намного больший объем информации; если вы интересуетесь этой темой, проследуйте по ссылке `http://technet.microsoft.com/en-us/library/hh849720.aspx`.

Создание пользователей

Давайте приступим к выполнению каких-нибудь операций по администрированию пользователей. Имеет смысл сначала создать пользователя. Для этого предназначен командлет PowerShell под названием `New-ADUser`:

```
PS C:\Users\Administrator> New-ADUser "Philipp Witschi"
```

Инструмент PowerShell содержит справку и примеры. Чтобы получить справку по `New-ADUser`, введите следующую команду:

```
PS C:\Users\Administrator> Get-Help New-ADUser
```

Получить примеры применения командлета можно так:

```
PS C:\Users\Administrator> Get-Help New-ADUser -examples
```

Наконец, с помощью приведенной ниже команды можно извлечь более детальные сведения о командлете:

```
PS C:\Users\Administrator> Get-Help New-ADUser -detailed
```

Эти команды получения справки совместимы со всеми командлетами, поставляемыми модулями Microsoft в PowerShell. Есть еще несколько удобных моментов, на которые стоит обратить внимание. Командлету можно указать флаг `-whatif`, чтобы посмотреть, что произойдет, если он будет выполнен:

```
PS C:\Users\Administrator> New-ADUser PWitschi -whatif
What if: Performing operation "New" on Target "CN=PWitschi,CN=Users,
DC=bigfirm,DC=com"
```

В действительности ничего не делается; это всего лишь имитирует команду и сообщает, каким был бы результат в случае запуска команды без флага `-whatif`. Кроме того, можно указать на необходимость запроса подтверждения, прежде чем выполнять команду. Это позволяет дважды обдумать набранную команду перед тем, как ее запускать:

```
PS C:\Users\Administrator> New-ADUser PWitschi -confirm

Confirm
Are you sure you want to perform this action?
Performing operation "New" on Target "CN=PWitschi,CN=Users,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):

Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "New" на цели "CN=PWitschi,CN=Users,DC=bigfirm,DC=com".
[Y] Да  [A] Да для всех  [N] Нет  [L] Нет для всех  [S] Приостановить  [?] Справка
(по умолчанию "Y"):
```

Флаги `-whatif` и `-confirm` можно использовать во всех последующих примерах командлетов, чтобы иметь уверенность в том, что все совершаемые действия корректны.

Предыдущая команда `New-ADUser` создает нового пользователя `PWitschi` в стандартном местоположении для новых пользователей, которым обычно является контейнер `Users`. Как утверждалось ранее, это не самое лучшее место для хранения учетных записей пользователей. Здесь содержится несколько специальных пользователей и групп, поэтому вы должны трактовать контейнер `Users` как специальный. Местоположением для учетных записей ваших пользователей является `\BigFirm\Users`. Если необходимо сконфигурировать некоторые свойства для пользователя, можно поступить так:

```
PS C:\Users\Administrator> New-ADUser "Philipp Witschi"
 -SamAccountName "PWitschi"
 -GivenName "Philipp"
 -Surname "Witschi"
 -DisplayName "Philipp Witschi"
 -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com'
 -UserPrincipalName "PWitschi@bigfirm.com"
```

Ниже описаны флаги, указанные в команде.

`-SamAccountName`. Входное имя пользователя (до Windows 2000 Server). Например, выше было указано `PWitschi`, поэтому пользователь сможет войти, используя доменное имя `BigFirm\PWitschi`.

`-GivenName`. Имя этого пользователя.

`-Surname`. Фамилия этого пользователя.

`-DisplayName`. Данное свойство объекта пользователя хранит отображаемое имя.

`-Path`. Отличительное имя организационной единицы, где необходимо создать новый объект пользователя. В этом случае указана организационная единица `\BigFirm\Users` в домене `bigfirm.com`.

`-UserPrincipalName`. Имя участника безопасности (UPN) — это входное имя пользователя, имеющее похожую на адрес электронной почты форму.

Запустив приведенную выше команду, вы увидите, что в указанной организационной единице создан новый пользователь. Вы также обнаружите, что этот пользователь отключен. Почему? Инструмент PowerShell требует явно указания на то, что пользователь должен быть включен.

Зачем может понадобиться такой способ создания пользователя? Вы можете выполнять большой объем работ по созданию множества учетных записей для пользователей. Но вы не хотите, чтобы эти учетные записи были включены до того, как связанные с ними люди окажутся готовыми использовать их. Когда этот момент наступит, вы можете установить уникальный пароль для пользователя и затем включить учетную запись. PowerShell допускает подобную гибкость.

Установка паролей

Ведь вы не устанавливали пароль, не так ли? Вы и не обязаны делать это. Однако при желании вы можете указать пароль с применением флага `-AccountPassword`. Здесь есть одна загвоздка: флаг `-AccountPassword` требует ввода защищенной строки, поэтому нельзя ввести просто `My PasswOrd`. Вы должны создать защищенную строку до создания пользователя. Для этого существует много способов; инструмент PowerShell весьма открыт в том, как можно решать ту или иную задачу.

Предположим, что вам нужно создать 10 объектов пользователей и установить для них один и тот же пароль, а также включить пользователей. Кроме того, необходимо заставить пользователей изменить свои пароли при первом входе в систему. Вот как можно поступить:

```
PS C:\Users\Administrator> $pw = Read-Host "Please Enter The Password"
 -AsSecureString

Please Enter The Password: ****************
Введите пароль: ****************

PS C:\Users\Administrator> New-ADUser "Philipp Witschi"
 -SamAccountName "PWitschi" -GivenName "Philipp" -Surname "Witschi"
 -DisplayName "Philipp Witschi"
 -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com'
 -UserPrincipalName "PWitschi@bigfirm.com"
 -AccountPassword $pw -Enabled 1 -ChangePasswordAtLogon 1
```

Первая строка предлагает администратору ввести пароль. Введенный текст будет преобразован в защищенную строку, которая затем сохраняется в переменной `$pw`. Символ `$` указывает PowerShell, что `pw` является переменной, т.е. контейнером, где можно сохранять значение. Командлет `Read-Host` запросит значение. Флаг `-AsSecureString` преобразует введенное вами значение в защищенную строку. Значение переменной `$pw` находится в памяти данного сеанса PowerShell до тех пор, пока либо не будет перезаписано, либо не закроется окно PowerShell.

После запуска команды вам предлагается ввести пароль. Введите легкую для передачи строку, которая удовлетворяет требованиям к сложности и длине пароля.

Вторая команда создаст пользователя. Чтобы удовлетворить своим требованиям, можно добавить несколько флагов.

`-AccountPassword`. Указывает на использование переменной `$pw` из предыдущей команды. Позволяет передавать желаемый пароль для нового пользователя в виде защищенной строки.

`-Enable`. Принимает значение `1` (объект пользователя должен быть включен) или `0` (объект пользователя должен быть отключен).

`-ChangePasswordAtLogon`. Принимает значение `1` (заставлять изменить пароль) или `0` (не заставлять изменить пароль).

В результате такой комбинации объект пользователя создается с заданным паролем и во включенном состоянии, к тому же пользователю придется изменить свой пароль, когда он первый раз входит в систему.

Запускать целых две команды только для одного пользователя выглядит расточительным, не правда ли? Однако с помощью этого подхода вы можете обеспечить повторение второй команды для оставшихся девяти пользователей, которые необходимо создать. Все 10 пользователей получать один и тот же пароль.

Если вы хотите создать только одного пользователя, то можете сделать все в одной команде. Этот подход задействует всю мощь PowerShell. Запуск командлета `Read-Host` можно вкладывать:

```
PS C:\Users\Administrator> New-ADUser "Philipp Witschi"
 -SamAccountName "PWitschi" -GivenName "Philipp" -Surname "Witschi"
 -DisplayName "Philipp Witschi"
 -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com'
 -UserPrincipalName "PWitschi@bigfirm.com"
 -AccountPassword (read-host "Please Enter The Password"
 -AsSecureString) -Enabled 1 -ChangePasswordAtLogon 1

Please Enter The Password: **********
```

Здесь вы заменяете переменную `$pw` командлетом `Read-Host`, которая применялась в предыдущем подходе. Это приводит к тому, что командлет `Read-Host` выполняется перед тем, как командлет `New-ADUser` может быть завершен, и затем требуемая защищенная строка передается в качестве значения флагу `-AccountPassword`. Когда вы запустите данную команду, запрашивается пароль, после чего пользователь будет создан.

Создание множества пользователей за раз

Представьте, что вы работаете администратором Active Directory в университете. Вероятно, у вас есть лес для учетных записей студентов. Ежегодно летом вы удаляете все старые учетные записи студентов, после чего создаете новые учетные записи для студентов, приступивших к учебе в первом семестре года. Вы имеете дело с задачей, предполагающей создание десятков тысяч объектов пользователей. Действительно ли вы собираетесь использовать для этого ADUC, ADAC или один из ранее показанных примеров PowerShell? Мы надеемся, что вы не планируете применять такие подходы.

Выполнить эту работу, приложив весьма небольшие усилия, можно с помощью однострочной команды PowerShell. Вам понадобится создать файл значений с разделителями-запятыми (comma-separated value — CSV) в Excel или в какой-то другой программе редактирования электронных таблиц. Более сложная сеть может иметь систему управления персоналом, которая позволяет создать такой файл через процесс экспорта.

Файл CSV — это текстовый файл, который содержит строку заголовков, описывающую значения, и последовательность строк, по одной на пользователя. Каждая строка включает значения, которые описывают пользователя.

Ниже показано содержимое файла по имени `users.csv`, который можно использовать для создания трех пользователей.

Name	SamAccount Name	GivenName	Surname	DisplayName	Path	UserPrincipal Name	Account Password
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	Tomasz Kozlowski	OU=Users, OU=BigFirm, DC=bigfirm, DC=com	TKozlowski@ bigfirm.com	NewPassw0rd

Если вы откроете CSV-файл `users.csv` в редакторе Notepad (Блокнот), он будет выглядеть примерно так:

```
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
```

Обратите внимание на строку заголовков

В строке заголовков указаны те же самые флаги, которые применялись ранее с командлетом `New-ADUser`. Строки, следующие за строкой заголовков в файле CSV, содержат значения для создания пользователей.

Теперь необходимо запустить команду, которая прочитает все строки файла `C:\users.csv`. Затем эта команда выполнит командлет `New-ADUser`, используя значения из файла. Вот эта команда:

```
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}
```

Пусть размер этой команды вас не пугает и не запутывает. Как только вы разобьете ее на компоненты, вы легко ее поймете.

`Import-CSV`. Этот командлет PowerShell будет читать файл CSV, созданный ранее и сохраненный как `C:\users.csv`.

`|`. Это символ конвейера. Часть мощи инструмента PowerShell связана с тем, что он предоставляет вам возможность передавать результаты выполнения одного командлета другому командлету. В рассматриваемом случае производится чтение файла CSV и передача находящихся в нем данных следующей части команды.

`foreach`. Этот командлет получает содержимое файла CSV, который читается как три элемента, точнее — три строки данных (исключая строку заголовков). Командлет `FOREACH` будет выполнять задачу с применением каждой из этих строк в качестве параметра.

`New-ADUser`. Вы уже знаете, что этот командлет создает пользователя. Но как он получает значения для своих флагов?

`$_`. Каждый флаг в командлете `New-User` требует значения. Как вам известно, значения в файле CSV указываются в соответствие со строкой заголовков. Каждая из записей `$_` в команде ссылается на один из элементов в строке заголовков. Вы должны знать, что `$_` представляет объект в PowerShell, а `$_.Name` — свойство `Name` этого объекта. Например, `$_.Name` ссылается на заголовок `Name` в файле CSV. Таким образом, командлет `New-ADUser` получит значение `Rachel Kelly` из первой строки и подставит его вместо `$_.Name`.

`AccountPasword`. Вы снова преобразуете пароль в защищенную строку, чтобы удовлетворить требованиям этого флага.

Введенная команда прочитает три строки данных из файла CSV. Она загрузит значения и создаст на их основе три объекта пользователей в организационной единице, указанной в файле CSV. Пользователи получат пароли, будут включенными и при первом входе должны будут изменить свои пароли.

Вы можете совершенно свободно добавлять в этот файл CSV дополнительные столбцы, соответствующие другим флагам в команде, чтобы в дальнейшем заполнять атрибуты объекта пользователя, такие как блуждающий профиль, домашняя папка и т.д.

Используя такой подход, вы можете вручную или автоматически (посредством какого-нибудь инструмента экспорта из системы управления персоналом) создать файл CSV и затем запустить *одну* команду для создания множества учетных записей для пользователей. Именно для этого предназначен инструмент PowerShell: упрощение выполнения работы за счет автоматизации.

Разблокирование учетной записи пользователя

Инструмент PowerShell можно также применять для выполнения более приземленной работы. Чтобы разблокировать учетную запись пользователя, можно запустить следующую команду:

```
PS C:\Users\Administrator> Unlock-ADAccount -identity SRed
```

С помощью флага `-identity` указывается имя объекта пользователя, подлежащего разблокировке. В этом примере мы используем дружественное входное имя. Для идентификации объекта пользователя может понадобиться указать имя DN:

```
PS C:\Users\Administrator> Unlock-ADAccount -identity "CN=Steve Red,
OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

Сбросить пароль пользователя можно с помощью такой команды:

```
PS C:\Users\Administrator> Set-ADAccountPassword -identity SRed -reset
 -newpassword (read-host "Please Enter The New Password"
 -AsSecureString)

Please Enter The New Password: **********
```

В командлете `Set-ADAccountPassword` также применяется флаг `-identity` для указания объекта пользователя, подлежащего управлению. Флаг `-reset` уведомляет PowerShell о том, что производится не обычное изменение пароля, которое предполагает знание старого пароля. Вместо этого вы хотите изменить пароль, поскольку пользователь его попросту забыл. При этом снова используется командлет `Read-Host` для чтения пароля и его преобразования в защищенную строку с целью ее передачи флагу `-newpassword` в качестве значения.

Командлет `Get-ADUser` позволяет получить свойства объекта пользователя:

```
PS C:\Users\Administrator> Get-ADUser SRed

DistinguishedName : CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
Enabled           : True
GivenName         : Steve
Name              : Steve Red
ObjectClass       : user
ObjectGUID        : 5fa7f3ac-93ec-4cf8-bf80-21368f8b3a8d
SamAccountName    : SRed
SID               : S-1-5-21-3625881918-2577536232-3089104624-1108
Surname           : Red
UserPrincipalName : SRed@bigfirm.com
```

По умолчанию он извлекает только небольшой набор доступных атрибутов. Если вы хотите просмотреть все, что доступно в объекте пользователя, запустите командлет `Get-ADUser` с запросом всех свойств, используя шаблон `*`:

```
PS C:\Users\Administrator> Get-ADUser SRed -properties * | more
```

Результаты, выдаваемые `Get-ADUser`, по конвейеру передаются командлету `More`, поэтому их вывод приостанавливается до нажатия любой клавиши. В противном случае результаты выводятся настолько быстро, что вы просто не успеете их прочитать. Если результаты включают намного больше атрибутов, чем вас интересует, измените предыдущую команду, указав желаемые свойства. Но в любом случае вы должны знать, какие свойства запрашивать, и в этом помогает шаблон `*`.

```
PS C:\Users\Administrator> Get-ADUser SRed -properties HomeDirectory

DistinguishedName : CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
Enabled           : True
GivenName         : Steve
HomeDirectory     : \\DC01\home$\SRed
Name              : Steve Red
ObjectClass       : user
ObjectGUID        : 5fa7f3ac-93ec-4cf8-bf80-21368f8b3a8d
SamAccountName    : SRed
SID               : S-1-5-21-3625881918-2577536232-3089104624-1108
Surname           : Red
UserPrincipalName : SRed@bigfirm.com
```

В данном примере в стандартный вывод командлета Get-ADUser включается также и атрибут HomeDirectory.

Можно вывести атрибуты сразу нескольких пользователей, задав какой-то критерий поиска:

```
PS C:\Users\Administrator> Get-ADUser -Filter 'Name -like "*"'
 -SearchBase "OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

В команде применяются два флага.

-Filter. Здесь указывается любой объект с именем, соответствующим шаблону *, т.е. все объекты пользователей.

-SearchBase. Здесь поиск дополнительно уточняется путем указания организационной единицы \BigFirm\Users в домене.

Приведенная выше команда возвращает стандартные свойства всех объектов пользователей в организационной единице \BigFirm\Users.

Если вы хотите модифицировать свойство объекта пользователя, воспользуйтесь командлетом Set-ADUser:

```
PS C:\Users\Administrator> Set-ADUser SCorso -Description "IT Manager"
```

С помощью этой команды модифицируется атрибут -Description пользователя SCorso. После ее выполнения описание объекта пользователя изменяется на IT Manager. Получить список модифицируемых атрибутов можно, выполнив следующую команду:

```
PS C:\Users\Administrator> Get-Help Set-ADUser
```

Допускается изменять свойство большого количества объектов за один раз. В следующем примере будут модифицированы все объекты в организационной единице \BigFirm\Users. С применением командлета Get-ADUser осуществляется поиск пользователей в указанной организационной единице, а результаты передаются по конвейеру в командлет Set-ADUser:

```
PS C:\Users\Administrator> Get-ADUser -Filter 'Name -like "*"'
-SearchBase "OU=Users,OU=BigFirm,DC=bigfirm,DC=com" | Set-ADUser
-Description "Member of IT"
```

Поиск производится точно так же, как было описано немного ранее. Найденные объекты передаются посредством конвейера в Set-ADUser. Свойство описания всех обнаруженных пользователей изменяется на Member of IT.

Включение учетной записи

Ранее упоминалось о том, что может возникнуть необходимость создать объект пользователя, но включить его только тогда, когда сотрудник будет готов к его использованию. Вот как включить объект пользователя Philipp Witschi:

```
PS C:\Users\Administrator> Enable-ADAccount -Identity PWitschi
```

Отключение учетной записи

Мы уже обсуждали причины, по которым имеет смысл отключать учетные записи на определенное время, прежде чем окончательно удалять их. Ниже показано, как отключить учетную запись:

```
PS C:\Users\Administrator> Disable-ADAccount -Identity PWitschi
```

Наконец, вы добрались до момента, когда хотите удалить учетную запись пользователя:

```
PS C:\Users\Administrator> Remove-ADUser -Identity PWitschi -confirm

Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target
"CN=PWitschi,CN=Users,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Remove" на цели
"CN=PWitschi,CN=Users,DC=bigfirm,DC=com".
[Y] Да [A] Да для всех [N] Нет [L] Нет для всех [S] Приостановить [?] Справка
(по умолчанию "Y"):
```

Ради осторожности командлет `Remove-ADUser` запускается с флагом `-confirm`. Это дает возможность обдумать последствия выполнения командлета и решить, продолжать ли данное действие. Если командлет `Remove-ADUser` должен быть запущен внутри сценария, то, скорее всего, флаг `-confirm` указываться не будет, т.к. вряд ли вы захотите, чтобы сценарий остановился где-то на полпути своего выполнения и ожидал взаимодействия с ним.

На этом рассмотрение процесса управления пользователями с помощью PowerShell завершено. Мы переходим к управлению группами. Первым делом, мы создадим группу с применением командлета `New-ADGroup`. Заметили ли вы сходство между всеми командлетами подобного рода? Это характерная черта PowerShell. Имя командлета начинается с глагола, такого как `Get`, `Set` или `New`, после которого следует описание действия командлета.

```
PS C:\Users\Administrator> New-ADGroup -Name "IT Administrators"
-SamAccountName "IT Administrators" -GroupCategory Security -GroupScope
DomainLocal -DisplayName "IT Administrators" -Path "OU=Security Groups,
OU=BigFirm,DC=bigfirm,DC=com" -Description "Members of this group are in IT"
```

Приведенная команда создаст локальную группу доступа домена по имени `IT Administrators` в организационной единице `\BigFirm\Security Groups`. Ниже описаны флаги, используемые в команде.

`-Name`. Имя группы.

`-SamAccountName`. Имя группы до Windows 2000 Server.

`-GroupCategory`. Может быть либо `Security` (или `1`) для группы доступа, либо `Distribution` (или `0`) для группы рассылки.

`-GroupScope`. Может быть либо `DomainLocal` (или `0`) для локальной группы домена, либо `Global` (или `1`) для глобальной группы, либо `Universal` (или `2`) для универсальной группы.

`-DisplayName`. Отображаемое имя группы.

`-Path`. Отличительное имя организационной единицы, в которой будет располагаться группа.

`-Description`. Описание объекта группы для ссылки в будущем.

Имея группу, можно приступить к добавлению в нее членов. Для этого служит командлет Add-ADGroupMember. Его можно применять множеством разных способов. Мы начнем с простейшего из них:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators" -Member SRed
```

Флаг -Identify позволяет сообщить PowerShell, какую группу необходимо изменить. Затем с помощью флага -Member указывается добавляемый пользователь. В приведенном выше примере объект пользователя SRed добавляется в группу доступа IT Administrators. Особенности начинаются, когда нужно добавить сразу нескольких пользователей. Если вы делаете это из командной строки PowerShell, можете воспользоваться следующим подходом:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators"

cmdlet Add-ADGroupMember at command pipeline position 1
Supply values for the following parameters:
Members[0]:SCorso
Members[1]:MZehner
Members[2]:
```

В этом случае вы указываете в команде управляемую группу, но не список новых членов. В результате PowerShell начинает запрашивать члены по одному. Вы указываете имя пользователя SCorso как члена 0, имя пользователя MZehner как члена 1, после чего в ответ на запрос очередного пользователя нажимаете клавишу <Enter>, чтобы завершить команду. Введенные вами пользователи добавляются в группу.

В качестве альтернативы можно применить другой подход:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators"
 -Member SCorso,MZehner
```

Разделителем между именами объектов пользователей, подлежащих добавлению в группу IT Administrators, служит запятая.

Может понадобиться добавить в группу очень большое число пользователей. Для этого используются результаты поиска, генерируемые командлетом Get-ADUser:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators" -Member
(Get-ADUser -Filter 'Name -like "*"'
 -SearchBase "OU=Users,OU=BigFirm,DC=bigfirm,DC=com")
```

В показанной команде присутствует вложенный запрос Get-ADUser, который применялся ранее при управлении пользователями с помощью PowerShell. Вложенный командлет Get-ADUser выступает в качестве значения для флага -Member командлета Add-ADGroupMember. Командлет Get-ADUser находит всех пользователей в организационной единице \BigFirm\Users. Обнаруженные в результате поиска пользователи добавляются в группу IT Administrators.

Вспомните, что вы не ограничены добавлением в группу Active Directory только пользователей. Можно также добавлять другие группы, делая их вложенными:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators" "Helpdesk"
```

Эта команда добавит группу Helpdesk в группу IT Administrators.

Часто возникает потребность в получении списка членов той или иной группы. В следующей простой команде используется командлет Get-ADGroupMember для вывода списка членов группы IT Administrators:

```
PS C:\Users\Administrator> Get-ADGroupMember "IT Administrators"

distinguishedName : CN=Helpdesk,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com
name              : Helpdesk
objectClass       : group
objectGUID        : 93e9b21b-023a-4e46-88b5-3c4cbf71f218
SamAccountName    : Helpdesk
SID               : S-1-5-21-3625881918-2577536232-3089104624-1115

distinguishedName : CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
name              : Steve Red
objectClass       : user
objectGUID        : 5fa7f3ac-93ec-4cf8-bf80-21368f8b3a8d
SamAccountName    : SRed
SID               : S-1-5-21-3625881918-2577536232-3089104624-1108
```

Команда возвращает все непосредственные члены данной группы, но не члены вложенных в нее групп. Такой список не особенно полезен в качестве отчета. Инструмент PowerShell позволяет указывать, какие атрибуты возвращаемых объектов должны отображаться:

```
PS C:\Users\Administrator> Get-ADGroupMember "IT Administrators" |
 FT ObjectClass,Name

ObjectClass         Name
-----------         ----
group               Helpdesk
user                Steve Red
```

Результаты выполнения командлета `Get-ADGroupMember` по конвейеру передаются в командлет `FT`, который представляет собой псевдоним командлета `Format-Table`. Это дает возможность указывать свойства или атрибуты, которые должны присутствовать в списке.

Автоматическая подгонка столбцов

Вполне возможно, что при запуске команды с множеством свойств она будет отображаться в окне командной строки некорректно, т.е. выглядеть так, как будто столбцы имеют неправильные размеры. Чтобы решить эту проблему, добавьте в конец команды ключ `-auto`. Как вам известно, в PowerShell не всегда нужно указывать имя флага полностью. Например, ключ `-auto` обозначает флаг `-AutoSize`, который инструктирует командлет `FT` о том, что ширина столбцов должна быть автоматически подогнана с учетом содержимого. Команда будет выглядеть следующим образом:

```
PS C:\Users\Administrator> Get-ADGroupMember "IT Administrators"
-recursive | FT
-auto
```

В предыдущем примере запрашиваются свойства `ObjectClass` и `Name`. В результате получается удобный отчет с объектами, являющимися непосредственными членами группы `IT Administrators`.

Тем не менее, если группа содержит в качестве членов другие группы, понадобится полный рекурсивный список членов:

```
PS C:\Users\Administrator> Get-ADGroupMember "IT Administrators"
-recursive | FT DistinguishedName

DistinguishedName
-----------------
CN=Steve Red,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
CN=Kevin Greene,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
CN=Marcel Zehner,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
```

К командлету добавляется флаг `-Recursive`, а его результаты через конвейер передаются командлету `FT` или `Format-Table` для получения отличительных имен всех объектов, которые имеют членство в группе `IT Administrators`.

Следующей операцией, которая может потребоваться, является удаление членов из группы. Для этого применяется командлет `Remove-ADGroupMember`:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
 -Member SRed

Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):

Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Set" на цели "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Да  [A] Да для всех  [N] Нет  [L] Нет для всех  [S] Приостановить  [?] Справка
(по умолчанию "Y"):
```

Здесь вы инициируете удаление пользователя `SRed` из группы `IT Administrators`. Командлет `Remove-ADGroupMember` всегда запрашивает подтверждение действия. В ответ на запрос подтверждения можно вводить несколько вариантов.

`Yes` (Да). Продолжить удаление указанного пользователя из группы.

`Yes to All` (Да для всех). Используйте этот вариант, если вы затребовали удаление нескольких членов из группы и уверены, что хотите удалить их все.

`No` (Нет). Не удалять указанного пользователя из группы.

`L` (Нет для всех). Отказаться от всех операций удаления, запрошенных в команде.

`S` (Приостановить). Приостановить выполнение операции. Произойдет возврат в режим командной строки. Возобновить выполнение команды до этого момента можно, введя **`Exit`**.

Следующая команда удалит несколько пользователей, перечисленных через запятые:

```
PS C:\Users\Administrator> Remove-ADGroupMember -Identity "IT
Administrators" -Member SCorso,SRed

Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU=Security
```

```
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Set" на цели "CN=IT Administrators,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Да [A] Да для всех [N] Нет [L] Нет для всех [S] Приостановить [?] Справка (по умолчанию "Y"):

Имена пользователей SCorso и SRed разделены запятой. Подобным образом можно добавлять множество пользователей или даже групп.

Может понадобиться удалить множество пользователей или групп, используя результаты поиска какого-то вида. В приведенном ниже примере с помощью командлета Get-ADUser находятся все пользователи в организационной единице \BigFirm\Users и удаляются из группы IT Administrators:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
-Member (Get-ADUser -Filter 'Name -like "*"'
         -SearchBase "OU=Users,OU=BigFirm,DC=bigfirm,DC=com")
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Set" на цели "CN=IT Administrators,OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Да [A] Да для всех [N] Нет [L] Нет для всех [S] Приостановить [?] Справка (по умолчанию "Y"):

Как видите, значение для флага -Member не указывается. Вместо этого вы используете вложенный командлет Get-ADUser. Он находит всех пользователей, подлежащих удалению, и результат передается командлету Remove-ADGroupMember. Если вы подтвердите выполнение действия, все пользователи в организационной единице \BigFirm\Users будут удалены из группы IT Administrators.

Здесь имеется похожее затруднение, как во время применения такого же подхода с запросом при добавлении пользователей в группу. Если любой из результирующих объектов вложенного запроса Get-ADUser не является членом указанной группы, потерпит неудачу вся операция Remove-ADGroupMember. Таким образом, если вы запросите всех пользователей в организационной единице \BigFirm\Users и один из них *не* находится в данный момент внутри группы IT Administrators, то операция удаления завершится неудачей.

Возможно, необходимо удалить всех членов из группы. Для этого потребуется запросить члены группы и вложить эту команду в команду удаления членов из группы:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
-Member (Get-ADGroupMember "IT Administrators")
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

```
Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Set" на цели "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Да  [A] Да для всех  [N] Нет  [L] Нет для всех  [S] Приостановить  [?] Справка
(по умолчанию "Y"):
```

С помощью командлета `Get-ADGroupMember` извлекаются все члены группы `IT Administrators`. Данный запрос вложен в команду `Remove-ADGroupMember` и возвратит результаты как значение для флага `-Member` команды.

Это дает много способов для создания группы, используя PowerShell, добавления в нее членов, запрашивания членства и удаления членов. Осталось только взглянуть на то, как удалять группу.

Удаление группы

Удаление группы — очень простая задача. Необходимо запустить командлет `Remove-ADGroup` и указать имя группы:

```
PS C:\Users\Administrator> Remove-ADGroup "IT Administrators"

Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=IT
Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

```
Подтверждение
Вы уверены, что хотите выполнить это действие?
Выполнение операции "Remove" на цели "CN=IT Administrators,OU=Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Да  [A] Да для всех  [N] Нет  [L] Нет для всех  [S] Приостановить  [?] Справка
(по умолчанию "Y"):
```

Здесь удаляется группа `IT Administrators`. При этом не имеет значения, содержит ли группа какие-то члены или нет — она будет удалена. Убедитесь, что эта группа больше не нужна. Не забывайте, что вы не сможете просто воссоздать группу и тем самым восстановить все назначенные разрешения, поскольку идентификатор SID, присвоенный старой группе, является глобально уникальным.

Наконец, раздел, посвященный модулю Active Directory для Windows PowerShell, завершен. Поначалу этот модуль казался сложным в применении. Конечно, в небольших средах использование PowerShell может не дать ощутимых преимуществ, но это, чему вы должны научиться. В средах среднего размера вы обнаружите, что применение PowerShell обеспечит более быстрое получение результатов. В крупных средах вы сочтете PowerShell средством, с помощью которого появляется возможность выполнять сложные операции очень быстро и с минимальными усилиями.

Резюме

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?

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.

Управляйте пользователями и группами 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?

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 эти-

ми 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.

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?

Глава 9

Групповая политика: инструменты и делегирование Active Directory

Когда ведутся разговоры на разнообразные темы, связанные с Active Directory, необходимо также говорить о групповой политике (Group Policy). Групповая политика не является новой технологией для Active Directory, но с момента своего появления в Windows 2000 Server она разрасталась и совершенствовалась с каждой выпущенной версией ОС и пакетом обновлений. Технология Group Policy и возможности, которые она предлагает в Windows Server 2012 R2, претерпели настолько радикальные улучшения по сравнению с первоначальной версией, что ее впору считать полностью новой технологией. Изменениям и усовершенствованиям были подвергнуты средства управления групповой политикой (консоль управления групповой политикой (Group Policy Management Console) и редактор управления групповыми политиками (Group Policy Management Editor)), управление доступными настройками (теперь их более 5000), управление целевыми объектами и устранение неполадок в инфраструктуре Group Policy. Если вы — опытный пользователь Group Policy, то непременно сосредоточите внимание на разделах этой главы, посвященных предпочтениям групповой политики, консоли управления групповой политикой (Group Policy Management Console — GPMC) и устранению неполадок.

В этой главе вы изучите следующие темы:

- понятие локальных политик и объектов групповой политики (Group Policy object — GPO);
- создание объектов GPO;
- устранение неполадок в групповых политиках;

- делегирование управления с использованием организационных единиц;
- применение расширенного делегирования для установки отдельных разрешений вручную;
- выяснение, какие делегирования были установлены.

Концепции групповой политики

Давайте начнем с рассмотрения важных концепций, терминов и правил, которые необходимо знать, чтобы овладеть групповой политикой. Во время объяснения функциональности групповой политики мы будем упоминать отдельные настройки, не показывая, как их в действительности включать в оснастке Group Policy. В настоящий момент просто сосредоточьтесь на концепциях. Позже в этом разделе мы предоставим полный экскурс в консоль управления групповой политикой (GPMC); мы рассмотрим использование групповой политики (включая опции Enforce (Применить) и Block Inheritance (Блокировать наследование политики)) и расширенные настройки.

Администраторы конфигурируют и развертывают групповую политику путем построения *объектов групповой политики* (Group Policy object — GPO). Объекты GPO — это контейнеры для групп настроек (*настроек политики*), которые могут быть применены к учетным записям пользователей и компьютеров через Active Directory. Объекты групповой политики создаются с использованием редактора управления групповыми политиками (Group Policy Management Editor — GPME), который запускается при редактировании объекта GPO из консоли GPMC. В одном объекте GPO можно указать набор приложений, предназначенных для установки на рабочих столах всех пользователей, реализовать очень строгую политику дисковых квот и ограничений на просмотр, а также определить политики паролей и блокировки учетных записей, действующие на уровне домена. Возможно создание одного всеохватывающего объекта GPO или нескольких объектов GPO, по одному на каждый тип функции.

Объект GPO состоит из двух частей, представленных в виде узлов.

- **Computer Configuration (Конфигурация компьютера).** Политики конфигурации компьютера управляют настройками, специфичными для машины, такими как дисковые квоты, аудит безопасности и ведение журналов событий.
- **User Configuration (Конфигурация пользователя).** Политики конфигурации пользователя управляют настройками, специфичными для пользователя, такими как конфигурация приложений, управление меню Start (Пуск) и переадресация папок.

Однако между этими двумя частями есть немало общего, особенно теперь, когда введен набор предпочтений групповой политики (Group Policy Preferences), о котором пойдет речь далее в этой главе. Нередко одна и та же политика встречается и в узле User Configuration, и в узле Computer Configuration. Будьте готовы к тому, что придется обдумывать, где активизировать необходимую политику — на уровне пользователя или на уровне компьютера. Имейте в виду, что вы можете создать политику, которая использует оба типа настроек, или предусмотреть разные объекты GPO для управления настройками User Configuration и Computer Configuration.

Вопреки своему названию, объекты групповой политики совершенно не ориентированы на группы. Может быть, их так назвали из-за того, что разные настройки управления конфигурацией *сгруппированы* в одном месте. Не обращая внимания на это, объекты групповой политики не могут напрямую применяться к группам. Вы можете применять их локально, к сайтам, доменам и организационным единицам (в Microsoft вместе это называют LSDOU (Local, Site, Domain, OU — локально, к сайту, к домену, к организационной единице)) внутри имеющегося леса. Такое действие по назначению объектов GPO сайту, домену или организационной единице называется *связыванием*. Отношение между объектом GPO и LSDOU может иметь тип "многие к одному" (например, многие объекты GPO связаны с одной организационной единицей) или "один ко многим" (один объект GPO связан с несколькими разными организационными единицами). После связывания с LSDOU политики пользователя оказывают воздействие на учетные записи пользователей внутри организационной единицы (и во вложенных в нее организационных единицах), а политики компьютера — на учетные записи компьютеров внутри организационной единицы (и во вложенных в нее организационных единицах). Оба типа настроек политики применяются в соответствии с частотой периодического обновления, которая составляет каждые приблизительно 90 минут.

Утверждение о том, что объекты GPO хранятся в AD, не совсем точно. Объекты GPO хранятся в виде двух частей — контейнер групповой политики (Group Policy container — GPC) и шаблон групповой политики (Group Policy template — GPT), который является структурой папок. Часть контейнера хранится в базе данных Active Directory и содержит информацию о свойствах, сведения о версии, состояние и список компонентов. Путь к структуре папок выглядит как `Windows\SYSVOL\sysvol\<Имя_домена>\Policies\GUID\`, где *GUID* — это глобально уникальный идентификатор для объекта GPO. Эта папка содержит настройки администрирования и безопасности, информацию о доступных приложениях, настройки реестра, сценарии и многое другое.

Политики работают по принципу "все или ничего"

Любой объект GPO содержит множество возможных настроек для многих функций; обычно в каждом объекте GPO вы будете конфигурировать только небольшое их количество. Остальные настройки можно оставить "неактивными" подобно помещению комментария `REM` перед командой в сценарии либо использованию точки с запятой в начале строки внутри файла INF. После конфигурирования настроек политики и сообщения AD о том, что этот объект GPO связан с доменом `Bigfirm.com`, например, отдельные настройки или типы настроек не могут быть применены выборочно. Все настройки User Configuration будут применяться ко всем учетным записям пользователей, входящих в системы Windows 7, Windows 8 и Windows Server 2012 R2 внутри связанного домена. Все настройки Computer Configuration будут применяться ко всем машинам Windows 7, Windows 8 и Windows Server 2012 R2 в домене. Предположим, что вы создали объект GPO, который развертывает набор стандартных настольных приложений, таких как Word, Excel и Outlook, и ввели несколько ограничений, предотвращающих изменение пользователями своих конфигураций. Если вы не хотите, чтобы пользователи IT-отдела подпадали под эти излишне строгие ограничения, то можете предпринять пару действий.

- Вы можете создать отдельный объект GPO для таких настроек политики и связать этот объект GPO с организационной единицей, которая содержит всех рядовых пользователей. Но эта организационная единица будет единственной, которая получит приложения Office.
- Вы можете установить разрешения в объекте GPO так, чтобы предотвратить применение политики к пользователям из IT-отдела (это называется фильтрованием). Однако если для решения данной проблемы вы используете фильтрование, то ни одна из настроек в объекте GPO не будет применена к пользователям из IT-отдела.

Политики наследуются и накапливаются

Настройки групповой политики являются накопительными и наследуются от родительских контейнеров Active Directory. Например, домен `Bigfirm.com` имеет несколько разных объектов GPO. Один из объектов GPO, связанных с доменом, устанавливает ограничения паролей, блокировку учетных записей и стандартные настройки безопасности. Каждая организационная единица в домене также имеет связанный с ней объект GPO, который развертывает и поддерживает стандартные приложения, а также настройки переадресации папок и ограничения рабочего стола. Учетные записи пользователей и компьютеров, находящиеся в организационной единице, получают настройки от объекта GPO, связанного с доменом, и от объекта GPO, связанного с этой организационной единицей. Таким образом, некоторые всеохватывающие настройки политики могут быть применены ко всему домену, тогда как другие могут быть нацелены на учетные записи согласно организационным единицам, с которыми они связаны.

Интервалы обновления групповой политики

Политики применяются в фоновом режиме каждые 90 минут, с "рандомизацией" в пределах до 30 минут, что защищает контроллер домена от одновременного обращения сотен или даже тысяч компьютеров. Контроллеры домена отличаются от обычных компьютеров и обновляют групповые политики каждые 5 минут. Однако, как будет показано далее в главе, имеется политика для конфигурирования всего этого. В интервал обновления не входят переадресация папок, установка ПО, применение сценариев, предпочтения групповой политики для принтеров и отображений сетевых дисков. Они применяются только при входе (для учетных записей пользователей) или загрузке системы (для учетных записей компьютеров); в противном случае может оказаться, что вы удалите какое-то приложение, тогда как кто-то пытается им воспользоваться. Или же пользователь может работать в папке, которая переадресуется на новый сетевой ресурс. По существу для обеспечения целостности данных эти настройки политики применяются только в "фоновом" обновлении групповой политики.

Основы групповой политики

Чтобы лучше понять, как технология Group Policy функционирует в среде Active Directory, необходимо разобраться с тем, каким образом она работает "за кулисами". Если вы только начали знакомство с групповой политикой, то довольно быстро

увидите, что многие предлагаемые ею средства обладают преимуществами по сравнению со старыми технологиями, такими как системные политики.

Репликация групповой политики является встроенной

Объекты GPO реплицируют себя автоматически, не требуя какой-либо работы с вашей стороны. Среда Active Directory реплицируется с использованием репликации AD Replication (управляемой средством проверки целостности знаний (Knowledge Consistency Checker) и генератором межсайтовой топологии (Intersite Topology Generator)) и управляется службой репликации файлов (File Replication Service) или службой распределенной репликации файлов (Distributed File Replication Service).

Объекты GPO самостоятельно выполняют очистку при удалении

Все настройки административных шаблонов GPO записывают свою информацию в определенные части реестра и самостоятельно производят очистку, когда настройка политики или объект GPO удаляется.

Это исправляет давнюю проблему, присущую технологии управления политиками при первом ее появлении. Например, предположим, что вы создали в унаследованной системе системную политику, которая устанавливает для всех пользователей цвет фона в какой-то раздражающий оттенок и также настроили политику, препятствующую им изменять этот цвет. Такие настройки записываются в реестр. Ранее после удаления политики записи в реестре не уничтожались, следовательно, раздражающий цвет фона оставался в системе. Часто это называли "татуировкой". Вам пришлось бы настроить *вторую* политику, чтобы исправить настройки в реестре. В случае объектов GPO в этом нет необходимости. Удаление политики устраняет все ее влияние.

Для применения настроек GPO вход не требуется

Реальную славу групповой политике приносит фоновое обновление. Поскольку все компьютеры в домене проверяют наличие изменений каждые 90 минут или около того, настройки политики применяются непрерывно. Это означает, что настройка, которую вы сделали в понедельник в 6:00, предназначенная для управления какой-то настройкой безопасности на каждом рабочем столе, не требует, чтобы все компьютеры находились в функционирующем состоянии. Взамен к компьютеру будет применено фоновое обновление, когда пользователь в 8:00 прибудет на свое рабочее место.

Машины Windows 2000 Server и более поздних версий с Active Directory получают свои настройки политики из домена, членами которого являются, после включения электропитания (вспомните, что машины также входят в домен), а пользователи получают политики из *своего* домена, когда входят в него.

Локальные политики и объекты групповой политики

Когда вы открываете инструмент редактора групповой политики (`gpedit.msc`), он автоматически выбирает объект GPO локальной машины (рис. 9.1).

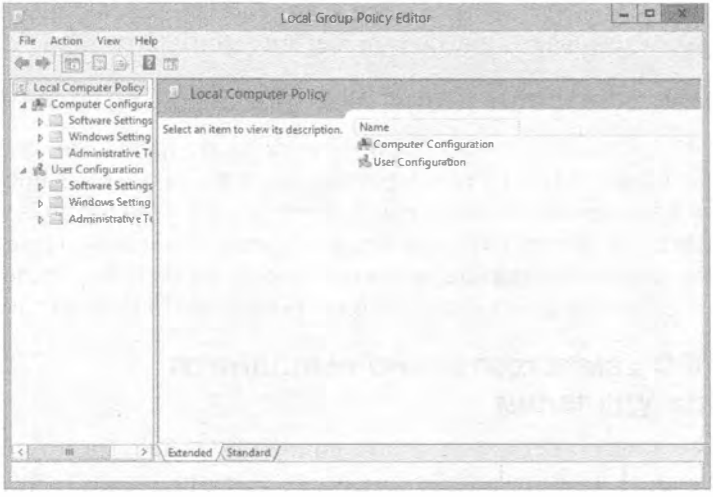


Рис. 9.1. Редактор управления групповыми политиками для локальной машины

Администраторы могут использовать этот инструмент для конфигурирования настроек учетных записей (таких как минимальная длина пароля и количество неудавшихся попыток входа, прежде чем учетная запись заблокируется), чтобы настроить аудит и указать другие смешанные настройки. Тем не менее, редактор политики домена, т.е. редактор управления групповыми политиками (Group Policy Management Editor — GPME), включает набор настроек (в том числе установку ПО и переадресация папок), которые для локальных политик являются недоступными.

> **Структура папок групповой политики**
>
> Локальная структура папок групповой политики похожа такую структуру других объектов GPO домена и находится в `\Windows\system32\GroupPolicy`.

Если вы работаете на компьютере Windows Server 2012 R2 или Windows 8, то можете конфигурировать не только локальный объект GPO (local GPO — LGPO). На таких компьютерах вы также можете иметь объекты GPO, которые могут быть нацелены на группы локальных пользователей (объект LGPO для администраторов и не администраторов) и отдельных пользователей (объект LGPO, специфичный для пользователя).

Объект LGPO для администраторов и не администраторов

Настройки в объектах LGPO для администраторов и не администраторов будут нацелены либо на пользователей в группе `Administrators`, либо на пользователей во всех других группах. Идея заключается в том, что когда пользователь имеет членство в локальной группе `Administrators`, то он должен обладать большими привилегиями, чем пользователь, не входящий в эту группу.

Обратите внимание на то, что объекты LGPO, управляющие такими настройками, модифицируют только настройки, связанные с пользователями. В объектах LGPO нет настроек, управляющих настройками уровня компьютера, которые находятся в узле Computer Configuration (Конфигурация компьютера).

Из-за наличия двух "типов" групп, для управления ими предусмотрены два объекта LGPO. Чтобы управлять обоими типами пользователей, понадобится сконфигурировать оба объекта LGPO. Для доступа к этим объектам LGPO должна применяться консоль MMC. Шаги подобны рассмотренным ранее; имеется лишь небольшое отличие в области действия объекта групповой политики, который загружен в MMC. Вместо выбора Local Computer (Локальный компьютер) из списка объектов групповой политики щелкните на кнопке Browse (Обзор), чтобы найти на вкладке Users (Пользователи) группу `Administrators` (Администраторы) или `Non-Administrators` (Не администраторы), как показано на рис. 9.2.

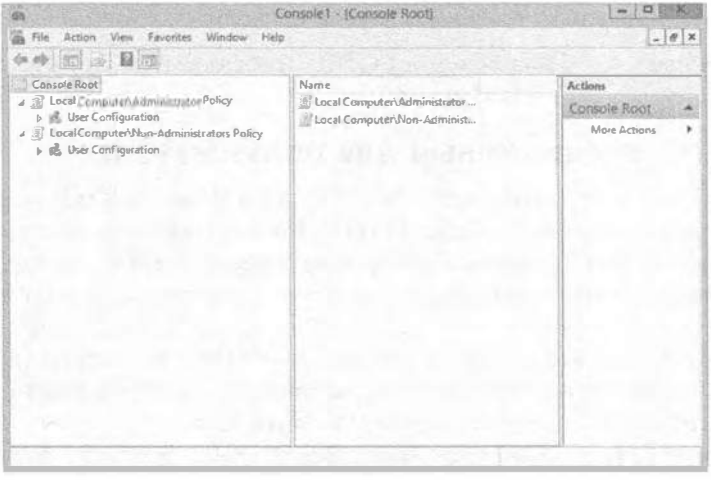


Рис. 9.2. С помощью консоли MMC можно просматривать объекты LGPO для групп `Administrators` и `Non-Administrators`

Для доступа к этим локальным объектам GPO с целью редактирования выполните перечисленные ниже шаги.

1. Выберите в меню Start (Пуск) пункт Run (Выполнить).
2. В поле Open (Открыть) введите **MMC** и щелкните на кнопке OK.

> **Требуются разрешения**
>
> Это задача администрирования; следовательно, при включенной функции управления учетными записями пользователей вы должны согласиться с повышенными разрешениями, которые требует оснастка Group Policy Management Editor консоли MMC.

3. В окне консоли MMC откройте меню File (Файл).
4. Выберите пункт Add/Remove Snap-in (Добавить или удалить оснастку).
5. В списке оснасток выберите Group Policy Object Editor (Редактор объектов групповой политики).
6. Оставьте вариант Local Computer (Локальный компьютер) в поле Group Policy Object (Объект групповой политики).
7. Щелкните на кнопке Browse (Обзор).

8. Перейдите на вкладку Users (Пользователи) в диалоговом окне поиска объекта групповой политики.
9. Выберите в списке группу `Administrators` (Администраторы) и щелкните на кнопке OK.
10. Щелкните на кнопке Finish (Готово) в диалоговом окне Select Group Policy Object (Выбор объекта групповой политики).
11. Щелкните на кнопке OK в диалоговом окне Add or Remove Snap-ins (Добавление и удаление оснасток).
12. Разверните узел Local Computer\Administrators Policy (Политика "Локальный компьютер \ Администраторы") в окне консоли.

Повторите шаги 4–12 для объекта LGPO, относящемуся к не администраторам, но вместо `Administrators` указывайте `Non-Administrators`.

Объект LGPO, специфичный для пользователя

На любом компьютере Windows Server 2012 R2 и Windows 8 можно конфигурировать очень детализированный объект LGPO. Эта политика направлена на индивидуальные учетные записи пользователей. В этом объекте LGPO есть только настройки политики, специфичные для пользователя, и они нацелены только на одиночного пользователя.

Чтобы можно было использовать этот объект LGPO, пользователь должен иметь локальную учетную запись SAM (Security Account Manager — диспетчер учетных записей безопасности) на конфигурируемом компьютере.

Для просмотра и настройки данного объекта LGPO вы также будете применять консоль MMC и следовать тем же самым шагам, что и при работе с объектами LGPO администраторов и не администраторов. Однако во время добавления оснастки Group Policy Object Editor к консоли MMC на вкладке Users диалогового окна поиска объекта групповой политики вы выберете учетную запись пользователя, для которого хотите создать объект LGPO. В случае выбора учетной записи администратора окно консоли MMC будет выглядеть примерно так, как показано на рис. 9.3.

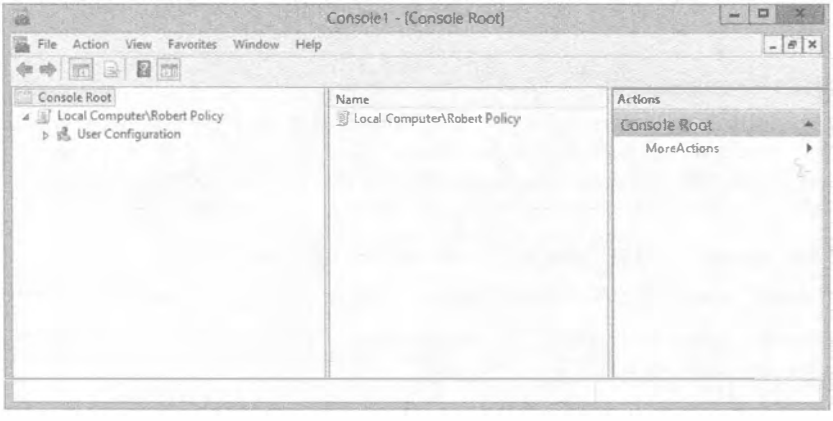


Рис. 9.3. После выбора пользователя для управления его объектом LGPO он отобразится в консоли MMC со всеми настройками User Configuration

Ниже перечислены шаги, необходимые для доступа к объектам LGPO, специфичным для пользователей.

1. Выберите в меню Start (Пуск) пункт Run (Выполнить).
2. В поле Open (Открыть) введите MMC и щелкните на кнопке OK.

> **Требуются разрешения**
>
> Это задача администрирования; следовательно, при включенной функции управления учетными записями пользователей вы должны согласиться с повышенными разрешениями, которые требует оснастка Group Policy Management Editor консоли MMC.

3. В окне консоли MMC откройте меню File (Файл).
4. Выберите пункт Add/Remove Snap-in (Добавить или удалить оснастку).
5. В списке оснасток выберите Group Policy Object Editor (Редактор объектов групповой политики).
6. Оставьте вариант Local Computer (Локальный компьютер) в поле Group Policy Object (Объект групповой политики).
7. Щелкните на кнопке Browse (Обзор).
8. Перейдите на вкладку Users (Пользователи) в диалоговом окне поиска объекта групповой политики.
9. Выберите в списке учетную запись нужного пользователя и щелкните на кнопке OK.
10. Щелкните на кнопке Finish (Готово) в диалоговом окне Select Group Policy Object (Выбор объекта групповой политики).
11. Щелкните на кнопке OK в диалоговом окне Add or Remove Snap-ins (Добавление и удаление оснасток).
12. Разверните узел Local Computer \ <Имя пользователя> Policy (Политика "Локальный компьютер \ <Имя пользователя>") в окне консоли.

Создание объектов GPO

Теперь, когда вы понимаете главные концепции групповой политики и знаете об отличиях между локальными и доменными объектами GPO, давайте посмотрим, какие шаги необходимо выполнить для создания и редактирования объекта доменного GPO. В этом разделе мы продемонстрируем все настройки, которые обсуждались в предыдущем "теоретическом" разделе.

> **Доменные объекты GPO**
>
> Начиная с этого момента, мы будем сконцентрированы только на доменных объектах GPO, поскольку они являются предпочтительным, логичным и безопасным способом развертывания настроек, которые существуют в объекте GPO.

Для управления всеми доменными объектами GPO вы будете пользоваться консолью GPMC. В Windows Server 2012 R2 консоль GPMC понадобится установить с применением диспетчера серверов, как было показано в главе 2.

После установки консоли GPMC она будет доступна через меню Start⇨Administrative Tools (Пуск⇨Администрирование). После выбора инструмента GPMC из упомянутого меню он откроется и отобразит домен, в котором управляющий компьютер имеет членство (рис. 9.4).

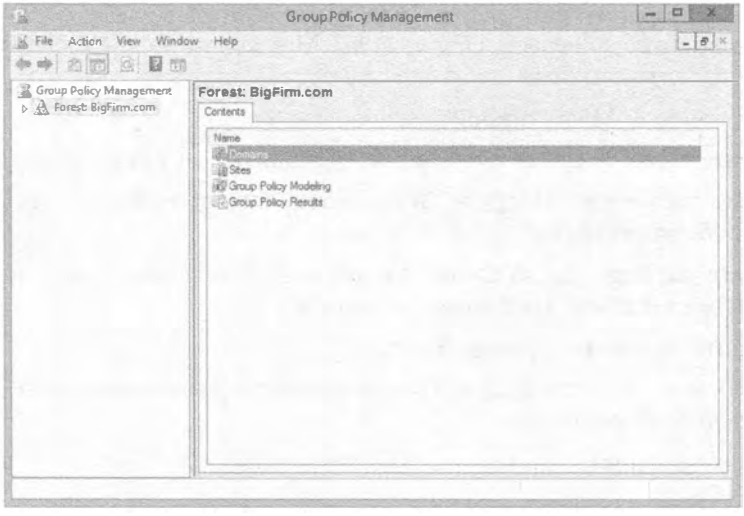


Рис. 9.4. Консоль GPMC является предпочтительным инструментом для управления объектами GPO

Для создания нового объекта GPO в домене нужно развернуть структуру GPMC, чтобы можно было видеть все узлы, существующие в домене (рис. 9.5).

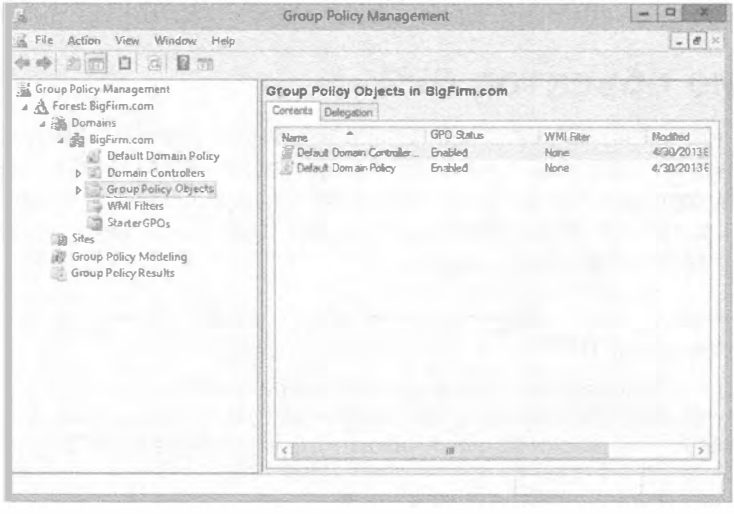


Рис. 9.5. Разворачивание структуры GPMC с целью отображения всех узлов внутри домена

Чтобы создать объект GPO в домене, выполните следующие шаги.

1. Щелкните правой кнопкой мыши на узле Group Policy Objects (Объекты групповой политики) и выберите в контекстном меню пункт New (Создать).
2. В диалоговом окне New GPO (Новый объект GPO) введите имя объекта GPO (в данном случае **Desktop Security**) и щелкните на кнопке OK.

В результате создается пустой объект GPO по имени `Desktop Security`, который пока еще не связан ни с одним контейнером в домене. В этот момент вы хотите сконфигурировать настройки объекта GPO и затем связать его с сайтом, доменом или организационной единицей. Чтобы связать GPO с каким-то узлом в Active Directory, выполните перечисленные ниже шаги.

1. Щелкните правой кнопкой мыши на желаемом узле (в этом случае на организационной единице `Desktops` (Рабочие столы)).
2. Выберите в контекстном меню пункт Link an Existing GPO (Связать с существующим объектом GPO).
3. В диалоговом окне Select GPO (Выбор объекта GPO) выберите объект GPO по имени `Desktop Security` и щелкните на кнопке OK.

   Обратите внимание, что организационная единица `Desktops` теперь имеет ассоциированный с ней объект GPO. Если вы хотите создать и связать объект GPO с организационной единицей, это можно сделать за один шаг. Для этого понадобится щелкнуть правой кнопкой мыши на организационной единицей (либо на домене или сайте, если уж на то пошло) и выбрать в контекстном меню пункт под названием Create a GPO in this domain, and link it here (Создать объект GPO в этом домене и связать его). Два шага выполнятся как одно действие.
4. Щелкните на объекте GPO (в данном случае `Desktop Security`).

   Обратите внимание, что с объектом GPO ассоциированы некоторые вкладки и свойства, отображаемые в правой панели GPMC. Как показано на рис. 9.6, для каждого GPO предусмотрено четыре вкладки: Scope (Область действия), Details (Детали), Settings (Настройки) и Delegation (Делегирование).

Вкладка Scope помогает отслеживать многие аспекты объекта GPO. Наиболее важные сведения находятся в областях Links (Ссылки) и Security Filtering (Фильтрация безопасности). В области Links перечислены сайты, домены и организационные единицы, с которыми в текущий момент связан объект GPO. Область Security Filtering отражает, какие группы и пользователи имеют разрешение применять настройки в GPO. На такую фильтрацию мы ссылались ранее, когда она использовалась для управления тем, какие пользователи в домене будут иметь настройки из примененного объекта GPO, путем их добавления или удаления из этой вкладки. В последней области этой вкладки, WMI Filtering (Фильтрация WMI), указывается фильтр WMI, на который объект GPO имеет ссылку, если он предусмотрен. Фильтры WMI позволяют нацеливать объекты GPO на учетные записи компьютеров в зависимости от состояния, в котором пребывает компьютер во время выполнения запроса WMI.

Как показано на рис. 9.7, вкладка Details помогает отслеживать информацию об объекте GPO, связанную с его созданием и состоянием. Здесь можно просмотреть идентификатор GUID, дату создания, версию и другие сведения, относящиеся

к GPO. Можно также включать или отключать весь или часть (компьютера и/или пользователя) объекта GPO.

Вкладка Settings содержит динамические данные, относящиеся к настройкам, которые сконфигурированы в объекте GPO.

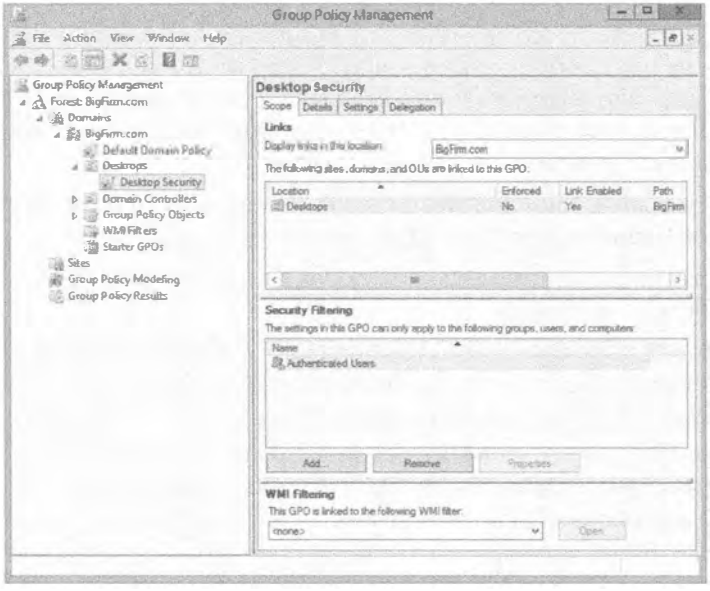


Рис. 9.6. Вкладки и свойства объекта GPO

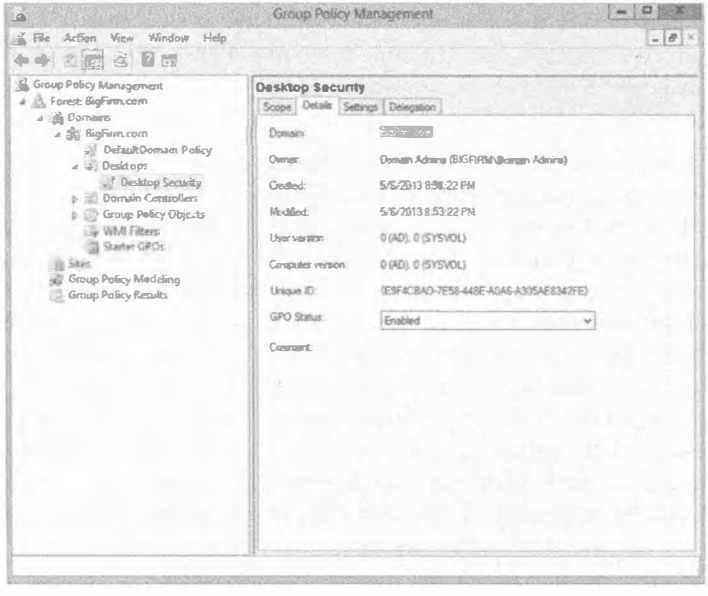


Рис. 9.7. Вкладка Details консоли GPMC предоставляет ключевую информацию об объекте GPO

На этой вкладке отображается HTML-версия отчета о настройках (рис. 9.8).

Наконец, вкладка Delegation показывает, кто может выполнять администрирование объекта GPO. Как показано на рис. 9.9, существуют три уровня администрирования GPO. Два из них предполагают редактирование GPO, а еще один — просто чтение настроек GPO.

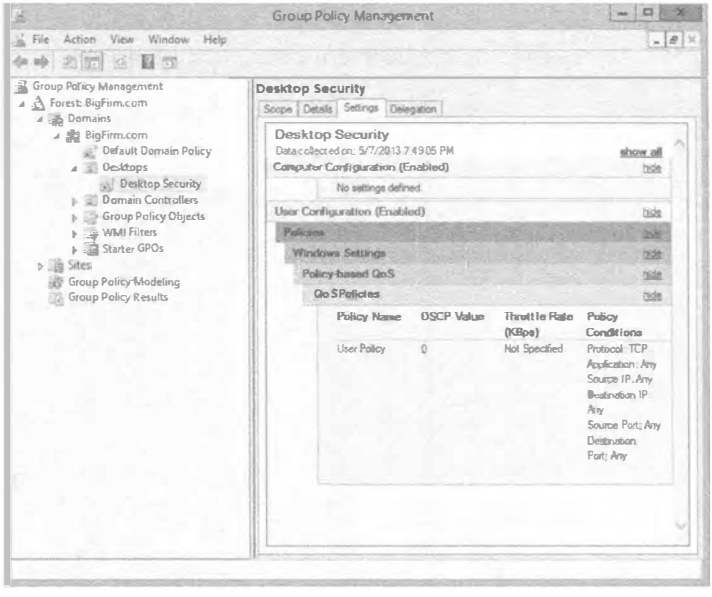


Рис. 9.8. Вкладка Settings консоли GPMC отображает текущие настройки в объекте GPO

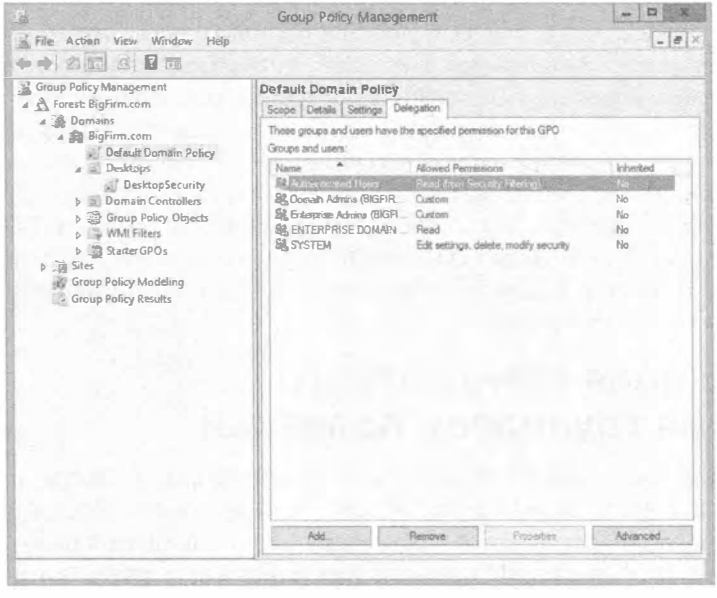


Рис. 9.9. Вкладка Delegation консоли GPMC отображает разрешения для уровней администрирования, выданные группам и пользователям

А теперь давайте просмотрим и модифицируем новый объект GPO. Вернитесь к узлу Group Policy Objects в консоли GPMC, щелкните правой кнопкой мыши на объекте GPO и выберите в контекстном меню пункт Edit (Редактировать). Откроется редактор GPME в отдельном окне, и вы увидите в корне пространства имен имя объекта политики, в данном случае Desktop Security [HOST1.BIGFIRM.COM] Policy. Это указывает на то, какая политика просматривается и редактируется. На рис. 9.10 представлена политика, развернутая в дереве консоли, чтобы были видны важные узлы объекта GPO. Вспомните, что `HOST1` — это is контроллер домена для домена `Bigfirm.com`.

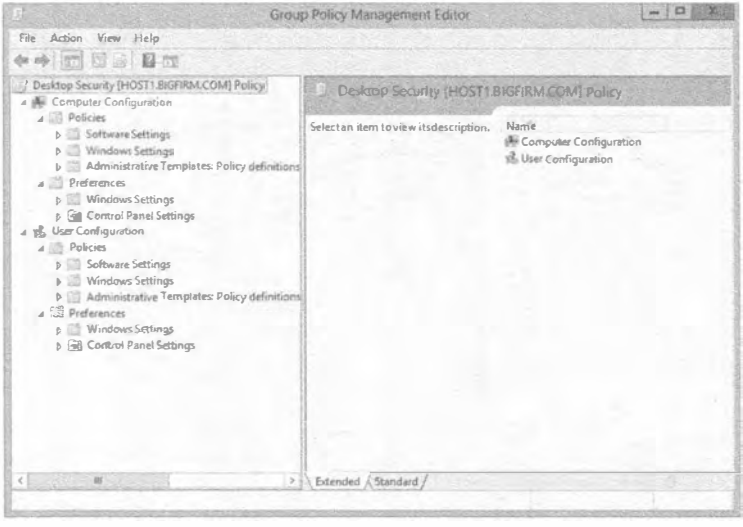


Рис. 9.10. Редактирование групповой политики в GPME

Как упоминалось ранее, существуют два основных типа настроек. Настройки Computer Configuration применяются к учетным записям компьютеров при их запуске и через интервалы фонового обновления. Настройки User Configuration применяются к учетным записям при их входе и также через интервалы фонового обновления.

После конфигурирования настроек групповой политики просто закройте окно GPME. Никаких опций вроде Save (Сохранить) или Save Changes (Сохранить изменения) не предусмотрено. Изменения записываются в объект GPO в результате щелчка на кнопке OK или Apply (Применить) для отдельной настройки, но пользователь или компьютер в действительности не увидит этих изменений до тех пор, пока политика будет обновлена.

Модификация стандартного поведения групповой политики

Сама по себе групповая политика превосходна, но есть аспекты поведения, которые вы можете решить подкорректировать или изменить. Доступны настройки GPO, позволяющие управлять поведением групповой политики рядом ее настроек. Вы обнаружите, что многие из этих настроек в конфигурировании не нуждаются, но в случаях, когда требуются какие-то небольшие корректировки, они становятся полезными.

Настройки для управления групповой политикой

Настройки GPO для управления групповой политикой находятся в узлах Administrative Templates (Административные шаблоны) внутри узлов User Configuration и Computer Configuration (`Policies\Administrative Templates\System\Group Policy`). Узел Computer Configuration содержит большинство обсуждаемых политик. На рис. 9.11 и 9.12 показаны опции конфигурирования Group Policy (Групповая политика) в узлах User Configuration и Computer Configuration.

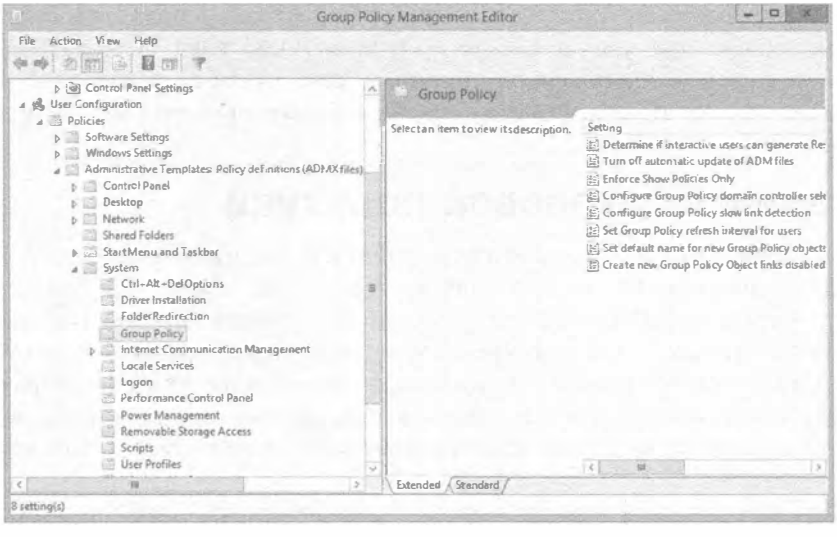


Рис. 9.11. Настройки User Configuration для Group Policy

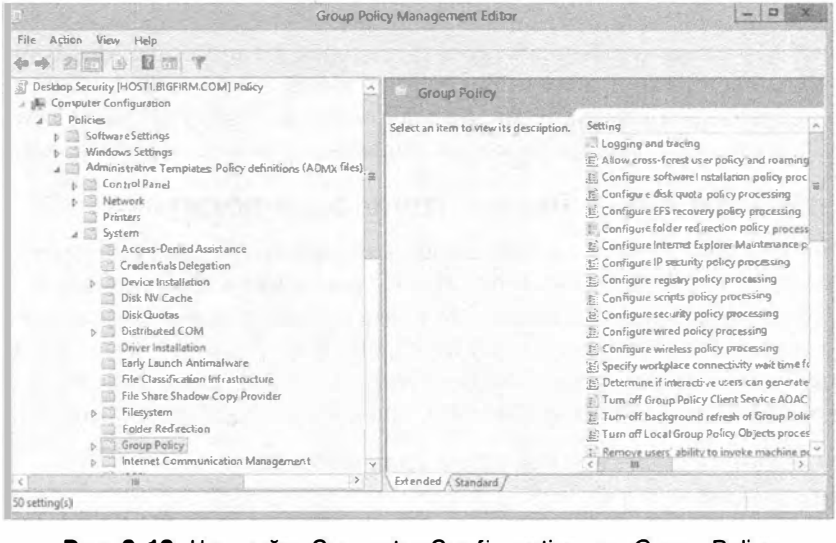


Рис. 9.12. Настройки Computer Configuration для Group Policy

Ниже приведен краткий обзор наиболее важных опций.

- **Интервалы обновления групповой политики (Group Policy Refresh Intervals) для пользователей/компьютеров/контроллеров домена.** Эти отдельные политики определяются, насколько часто объекты GPO обновляются в фоновом режиме, пока пользователи и компьютеры работают. Эти параметры разрешают вносить изменения в стандартные интервалы фонового обновления и подстраивать время смещения.
- **Turn Off Background Refresh of Group Policy (Отключить фоновое обновление групповой политики).** Если вы включите эту настройку, политики будут обновляться только при запуске систем и входе пользователей. Это оказывается полезным в офисах филиалов по причинам, связанным с производительностью, т.к. обновление политик, например, на 1500 компьютерах может привести к перегрузке канала WAN.

Применение групповой политики

Подобно большинству технологий, с групповой политикой ассоциирована логика, которая обеспечивает ее применение в надежной манере. По большей части применение групповой политики будет прямолинейным. Эта логика становится более сложной, только когда появляются конфликтующие настройки во множестве объектов GPO, и вы начинаете изменять стандартное поведение. Невзирая на это, когда вы принимаетесь за проектирование и реализацию своих настроек политики, вы должны полностью понимать, какой конечный результат будет у всех компьютеров и пользователей.

В этом разделе мы раскроем стандартное применение групповой политики, которое будет разрешать все вопросы, касающиеся конфликтов между настройками GPO. Примером таких вопросов может быть "Что, если есть связанный с доменом объект GPO, который удаляет из меню Start (Пуск) пункт Run (Выполнить), а другой объект GPO, связанный с организационной единицей `Desktops`, добавляет пункт Run в меню Start?" Мы также углубимся в области, которые помогут "нацеливать" настройки GPO, когда настройки политики получает слишком много (или наоборот, недостаточно) пользователей и компьютеров. Вам доступны на выбор фильтры WMI, принудительное применение, блокирование наследования и многие другие варианты.

Каким образом применяется групповая политика

Имея в наличии один или два работающих объекта GPO, вы столкнетесь с наиболее хлопотливой частью групповой политики: выяснением конечного результата для каждого компьютера и пользователя. Для примера представьте, что вам звонит пользователь и спрашивает "Почему у меня цвет фона фиолетовый?" Затем вы обнаружите, что имеется *много* мест, откуда система получает политики, и они могут противоречить друг другу в том, что касается цвета фона. Итак, какая же политика *выиграет*?

Политики выполняются снизу вверх в графическом пользовательском интерфейсе

Давайте начнем с рассмотрения простой ситуации: всего лишь политики в домене. Предположим, что вы просматриваете узел домена в консоли GPMC и видите, что он имеет много связанных объектов GPO (рис. 9.13).

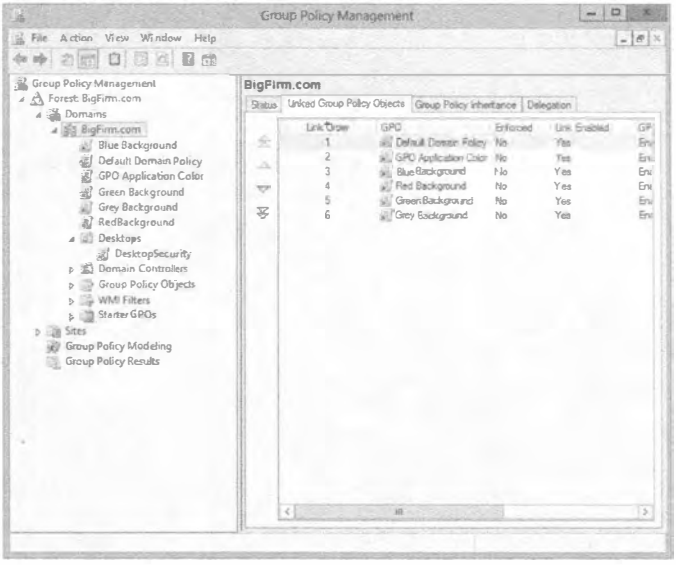


Рис. 9.13. Узел домена и связанные объекты GPO

В этой (надо сказать, воображаемой) ситуации домен имеет пять групповых политик, четыре из которых пытаются установить цвет фона на рабочей станции в серый, зеленый, красный или синий. (Еще одной политикой является стандартная политика домена (Default Domain Policy), которая ничего не предпринимает в этом отношении.) Чтобы ознакомиться с порядком применения объектов GPO, вы можете щелкнуть на узле домена и перейти на вкладку Linked Group Policy Objects (Связанные объекты групповой политики) в правой панели. Итак, глядя на рис. 9.13, какой цвет одержит победу: серый, красный, зеленый или синий?

Ответ кроется в двух базовых правилах разрешения конфликтов для объектов GPO.

Правило 1. Воспринимайте ту политику, которую вы слушали последней.

Правило 2. Выполняйте политики снизу вверх согласно тому, как они отображаются в графическом пользовательском интерфейсе.

Просматривая диалоговое окно снизу вверх, вы заметите, что система сначала видит политику, которая устанавливает цвет фона в серый, затем политику, устанавливающую его в зеленый, политику, которая устанавливает цвет фона в красный, и, наконец, политику, устанавливаюшую его в синий. Поскольку политика, которая устанавливает цвет фона в синий, оказалась последней примененной, она и выигрывает, а результаты действия предыдущих трех политик теряются.

Вы можете также перейти на вкладку Group Policy Inheritance (Наследование групповой политики), на которой отображается порядок применения объектов GPO, поступающих из всех местоположений внутри Active Directory. На рис. 9.14 можно видеть, что политика, устанавливающая синий цвет фона, выигрывает у остальных политик.

Но что, если вы *хотите*, чтобы выиграла политика, устанавливающая красный цвет фона? Заметили стрелки вверх и вниз в левой части вкладки Linked Group Policy Objects? Вы можете смешивать их как вашей душе угодно.

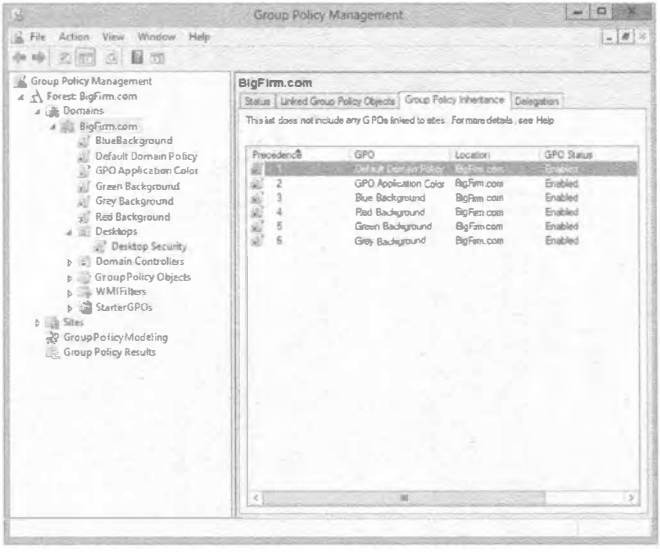


Рис. 9.14. Наследование объектов GPO для узла домена

Фильтрация групповой политики с помощью списков управления доступом

Но мы еще не подошли *близко* к завершению. Ситуация *может* выглядеть так, что к вашей системе применяется множество политик, но на самом деле политик совсем мало. Причина в том, что объекты GPO имеют списки управления доступом (access control list — ACL). Щелкните на любом объекте GPO в консоли GPMC (на Desktop Security в рассматриваемом примере) и взгляните на вкладку Scope в правой панели. В разделе Security Filtering вы увидите список ACL для этого объекта GPO (рис. 9.15).

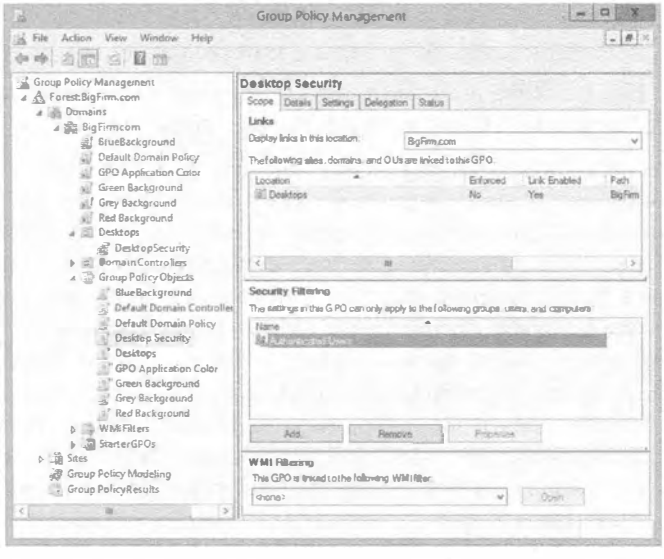


Рис. 9.15. Список ACL для объекта GPO в консоли GPMC

Как отмечалось ранее, администраторы домена (Domain Admins) и администраторы предприятия (Enterprise Admins) имеют разрешения Read (Чтение) и Modify (Изменение), а аутентифицированные пользователи (Authenticated Users) — разрешения Read и Apply Group Policy (Применение групповой политики). Тем не менее, обратите внимание, что в списке присутствует только группа Authenticated Users. Почему так? Дело в том, что это список только пользователей, компьютеров и групп, которые имеют разрешение применять настройки GPO. Для просмотра полного списка ACL вы должны сначала выбрать вкладку Delegation и затем щелкнуть на кнопке Advanced (Дополнительно). Отобразится хорошо знакомое диалоговое окно настроек безопасности, показанное на рис. 9.16.

Может случиться так, что вы создаете объект GPO для ограничения рабочих столов и не хотите применять его к определенной группе пользователей. В состав группы Authenticated Users входят все учетные записи (пользователей и компьютеров) кроме гостей, так что по умолчанию данный объект GPO будет применяться ко всем, исключая гостей; это означает, что настройки политики получат даже члены групп Domain Admins и Enterprise Admins. Чтобы предотвратить получение политики группами Domain Admins и Enterprise Admins, вы должны отметить флажок Deny (Запретить) рядом с разрешением Apply Group Policy (Применить групповую политику), как показано на рис. 9.17. Членам обеих групп достаточно отмеченного флажка Deny для одной из двух групп, но если члены групп Domain Admins и Enterprise Admins являются разными людьми, то придется отметить флажок Deny для обеих групп. Чтобы освободить остальных от получения политики, поместите их в отдельную группу доступа и добавьте ее в список. Недостаточно просто снять отметку с флажка Allow (Разрешить) для разрешений Read и Apply Group Policy; пользователи в этой специальной группе доступа являются также членами группы Authenticated Users, поэтому в действительности для данной группы необходимо отметить флажки Deny для упомянутых разрешений. Опция Deny имеет более высокий приоритет, чем Allow.

Рис. 9.16. Диалоговое окно настроек безопасности для объекта GPO

Рис. 9.17. Отключение разрешения Apply Group Policy

В качестве альтернативы установки всех списков ACL можно также удалить группу `Authenticated Users` из области Security Filtering вкладки Scope, поместить всех пользователей, которым нужны настройки, в новую группу доступа и затем добавить эту группу в область Security Filtering на вкладке Scope (рис. 9.18).

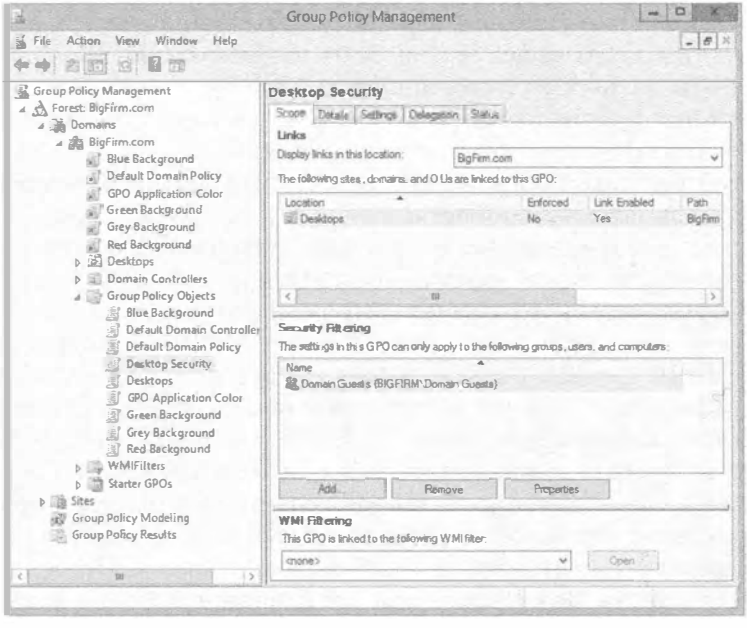


Рис. 9.18. Фильтрация безопасности для групповой политики без группы `Authenticated Users`

Между прочим, ничего не препятствует добавлению отдельных пользователей в список разрешений для объекта GPO. Однако это неудачный с точки зрения безопасности и управления прием, т.к. невозможно отслеживать индивидуальных пользователей, помещенных в списки ACL, по всему предприятию. Мы еще раз подчеркиваем, что фильтрация безопасности для групповой политики является исключительно мощным средством — его можно назвать инструментом, который позволяет "угнетать" отдельных лиц или группы. Тем не менее, в реальности добавление списков ACL в политику может стать настоящим кошмаром при попытках выяснения пару лет спустя причину, по которой политика присоединена к домену, но *не применяется к большинству пользователей в домене.*

Принудительное применение и блокирование наследования

Точно так же, как фильтрация безопасности может использоваться для предотвращения применения политики, специальная настройка Block Inheritance (Блокировать наследование) в узле AD (домена или организационной единицы) позволяет препятствовать продвижению вниз объектов GPO более высокого уровня. Когда настройка Block Inheritance включена, настройки находящихся выше политик не будут применяться к контейнерам, расположенным ниже.

Например, если вы создали объект GPO для определенной организационной единицы, скажем, Brunswick, и сконфигурировали все необходимые настройки для Brunswick, а затем хотите предотвратить влияние объектов GPO домена Bigfirm на организационную единицу Brunswick, то должны включить настройку Block Inheritance для организационной единицы Brunswick. После этого к Brunswick будут применяться только те объекты GPO, которые связаны непосредственно с этой организационной единицей.

Существует также противоположность блокированию наследования. Когда для объекта GPO включена настройка Enforce (Принудительно применять), то настройка Block Inheritance для этого объекта нейтрализуется. Кроме того, настройки в последующих объектах GPO не будут изменять настройки из принудительно применяемого объекта GPO.

Например, если администраторы домена имеют набор весьма спорных настроек, включенных на уровне домена, а мятежные администраторы Brunswick сконфигурировали собственные настройки политики на уровне своей организационной единицы и включили настройку Block Inheritance, то организационная единица Brunswick благополучно минует эти спорные настройки, но только до тех пор, пока администраторы домена не поймут, в чем дело, и не включат настройку Enforce. В результате администраторы домена выиграют, и пользователям организационной единицы Brunswick придется мириться с теми же ограничениями, что все остальные пользователи. Настройка Enforce побеждает настройку Block Inheritance (подобно тому, как бумага побеждает камень, накрывая его).

Как и все секретное оружие, настройки Enforce и Block Inheritance лучше использовать умеренно. Иначе при устранении неполадок станет довольно сложно определить, какие объекты GPO применяются в том или ином случае. Это может нанести вред психическому здоровью (и потенциально безопасности работы) сетевого администратора.

Ниже представлена сводка по факторам, которые позволяют принять решение о том, какой объект групповой политики получает приоритет.

- Просматривайте политики в следующем порядке: локальные объекты GPO, объекты GPO сайта, объекты GPO домена, объекты GPO организационной единицы, объекты GPO дочерней организационной единицы и т.д.
- Внутри любого узла AD — сайта, домена или организационной единицы — просматривайте политики в том порядке, в каком они отображаются в графическом пользовательском интерфейсе, снизу вверх.
- Когда настройки политики конфликтуют друг с другом, уделите внимание только настройке в последнем просмотренном объекте GPO при условии, что вы уже не столкнулись с политикой, имеющей включенную настройку Enforce. Это значит, что независимо от того, какая конфликтующая настройка поступит впоследствии, она должна игнорироваться, поскольку в этом объекте GPO включена настройка Enforce.
- Перед тем, как действительно применить объект GPO, проверьте его список ACL. Если целевой пользователь или компьютер не имеет разрешений Read и Apply Group Policy (обычно через членство в группах), то этот объект GPO не будет применен.

Возможности настроек групповой политики

С помощью настроек групповой политики можно делать по существу все то, что есть возможность делать посредством реестра локальной системы и большей части конфигурирования. Ниже приводится несколько примеров.

- **Развертывание программного обеспечения.** Вы можете собрать все файлы, необходимые для установки нужной порции ПО, в *пакет*, разместить его где-то на сервере и затем воспользоваться групповыми политиками для указания пользовательскому рабочему столу на этот пакет. Пользователь увидит, что приложение доступно, и вы достигаете своих целей по его установке из центрального местоположения, не имея необходимости в визите к каждому рабочему столу по отдельности. Когда пользователь попытается запустить это приложение в первый раз, оно установится безо всякого вмешательства со стороны пользователя.
- **Ограничение набора приложений, которые пользователи могут запускать.** Вы можете управлять рабочим столом пользователя, разрешая ему запускать только заданное множество приложений, например, Outlook, Word и Internet Explorer.
- **Управление настройками системы.** Объекты GPO обеспечивают простейший способ управления дисковыми квотами. Многими системами Windows легче всего управлять с помощью настроек политики, а в некоторых системах политики являются *единственным* методом их контроля.
- **Установка сценариев входа, выхода, загрузки и завершения.** Объекты GPO позволяют любому событию входа, выхода, загрузки и завершения либо им всем запускать указанный сценарий.
- **Упрощение и ограничение программ.** Объекты GPO можно использовать для удаления многих функциональных средств из Internet Explorer, проводника Windows и других программ.
- **Общее ограничение рабочего стола.** Вы можете удалить большинство или все элементы из меню Start (Пуск), запретить добавление принтеров или отключить возможность выхода из системы либо изменения конфигурации рабочего стола. С помощью настроек политики в действительности можно даже полностью блокировать рабочий стол пользователя. (Однако чрезмерная блокировка может привести к появлению одного неэффективного сотрудника, так что будьте осторожны.)

Политики позволяют выполнять также множество других работ, но это введение дает вам базовое представление об их функциях.

Настройки конфигурации пользователя и компьютера

Операционные системы Windows Server 2012 R2 и Windows 8 поступают с совершенно по-новому выглядящими настройками конфигурации пользователя и компьютера в редакторе GPME. Тем самым разработчики из Microsoft оказали нам огромную услугу. Было введено свыше 3000 дополнительных настроек GPO. Чтобы лучше справляться с таким объемом настроек, в Microsoft решили также изменить способ представления настроек в GPME.

На рис. 9.19 видно, что в интерфейсе GPME имеются два главных узла: User Configuration (Конфигурация пользователя) и Computer Configuration (Конфигурация компьютера). Оба узла содержат следующие подузлы: Policies (Политики) и Preferences (Предпочтения). Подузел Policies в дальнейшем разбит на следующие подузлы: Software Settings (Настройки программного обеспечения), Windows Settings (Настройки Windows) и Administrative Templates (Административные шаблоны). Подузел Preferences разделен на такие подузлы: Control Panel (Панель управления) и Windows Settings (Настройки Windows).

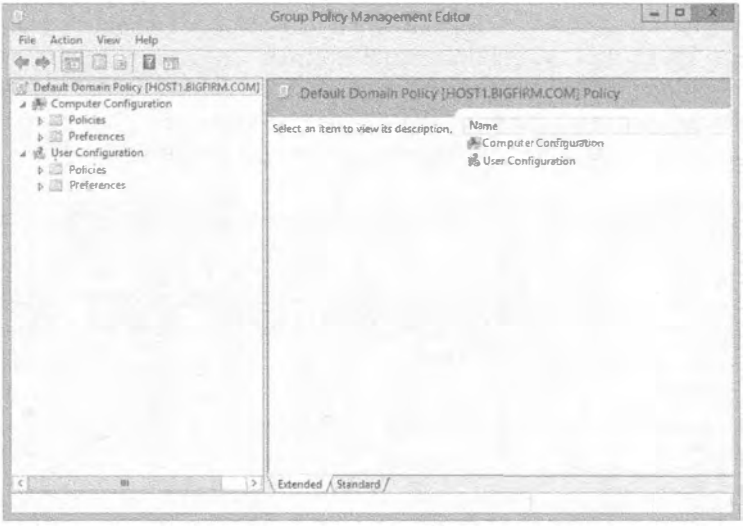


Рис. 9.19. Узлы и подузлы в редакторе GPME

Отличие между этими двумя уровнями узлов заключается в том, что настройки для User Configuration применяются к учетным записям пользователей, а настройки для Computer Configuration — к учетным записям компьютеров. Например, если задействованы настройки реестра, как в случае административных шаблонов, то изменения будут записываться в раздел HKEY_CURRENT_USER (HKCU) для настроек User Configuration и в раздел HKEY_LOCAL_MACHINE (HKLM) для настроек Computer Configuration. Создавать отдельные объекты GPO для компьютеров и пользователей может понадобиться в целях обеспечения простоты. Если значение, установленное в настройках компьютера, также присутствует в настройках пользователя, то по умолчанию приоритет получает настройка из Computer Configuration. Чтобы убедиться в таком поведении, просмотрите описание настройки GPO, но лучше всего выполнить тест.

При наличии более 5000 настроек GPO в Windows Server 2012 R2 совершенно нереально подробно останавливаться на каждой настройке. Тем не менее, в Microsoft предлагают электронные таблицы Excel, которые помогают в освоении настроек:

```
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID
=18c90c80-8b0a-4906-a4f5-ff24cc2030fb
```

Некоторые наиболее полезные настройки и категории политики рассматриваются в последующих разделах.

Указание сценариев с помощью групповой политики

Указать сценарии входа и выхода, а также сценарии для запуска при загрузке и завершении системы можно посредством настроек Windows Settings либо в узле User Configuration, либо в узле Computer Configuration. Раскройте Policies\Windows Settings, чтобы увидеть элемент Scripts (Сценарии), и затем выберите тип сценария (Startup (Загрузка), Shutdown (Завершение), Logon (Вход) или Logoff (Выход)) в панели деталей справа; на рис. 9.20 показаны сценарии, доступные в узле User Configuration. Для этого дважды щелкните на типе сценария (таком как Logon) или выделите его и выберите пункт меню Action⇨Properties (Действие⇨Свойства). Добавьте сценарий, щелкнув на кнопке Add (Добавить), после запроса введите имя сценария и его параметры (рис. 9.21) и щелкните на кнопке OK. Для редактирования имени и параметров сценария (но не самого сценария) выберите пункт меню Action⇨Edit (Действие⇨Редактировать). Если указано более одного сценария, используйте кнопки со стрелками вверх и вниз для установки порядка их запуска.

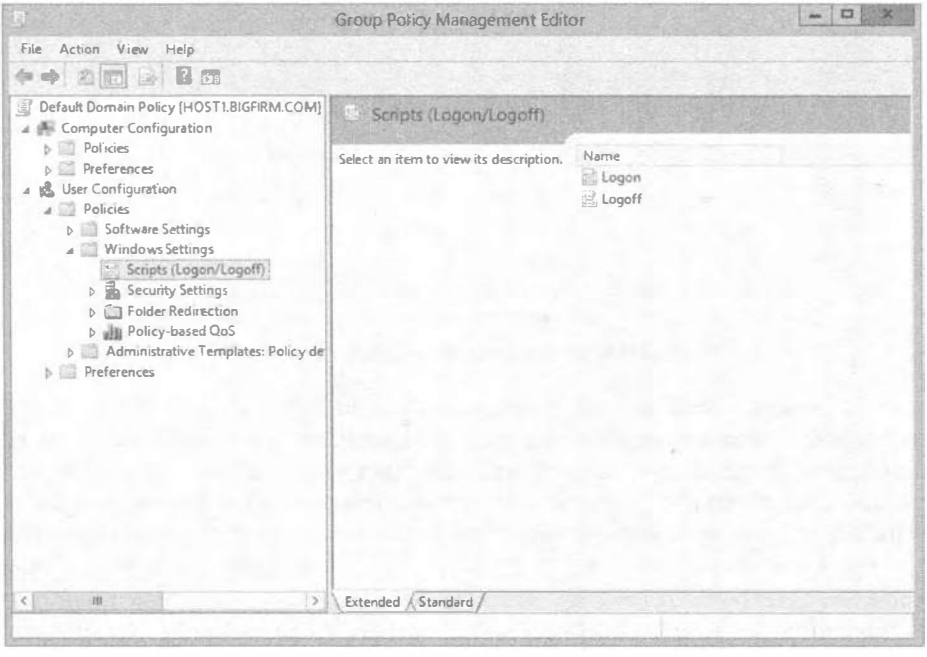


Рис. 9.20. Сценарии входа в групповой политике

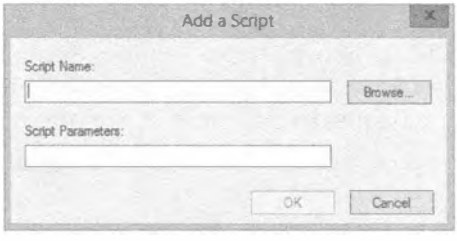


Рис. 9.21. Добавление сценария в групповую политику

Созданные и назначенные сценарии должны быть скопированы в следующую папку: \Windows\SYSVOL\SysVol\имя_домена\Policies\{GUID}\Machine\Scripts\Startup (or Shutdown). (Или же они могут быть скопированы в User\Scripts\Logon либо User\Scripts\Logoff, в зависимости от того, где назначаются сценарии — в узле Computer Configuration или в узле User Configuration.) Идентификатор GUID для объекта групповой политики представляет собой длинную строку, выглядящую как {FA08AF41-38AB-11D3-BD1FC9B6902FA00B}. Если вы хотите просмотреть сценарии, сохраненные в объекте GPO и, возможно, открыть их с целью редактирования, щелкните на кнопке Show Files (Показать файлы) в нижней части диалогового окна свойств. Это приведет к открытию соответствующей папки в проводнике Windows.

Как вам должно быть известно, указать сценарий входа можно также в диалоговом окне свойств учетной записи пользователя, открывающемся в результате запуска dsa.msc. В Microsoft называют это *унаследованными сценариями входа* и рекомендуют назначать сценарии для клиентов, осведомленных о Windows AD, с помощью групповой политики. Преимущество применения сценариев в групповой политике связано с тем, что они выполняются асинхронно в скрытом окне. Таким образом, если назначено множество сценариев или сценарии являются сложными, пользователю не придется ожидать их завершения. Унаследованные сценарии входа выполняются в окне на рабочем столе. С другой стороны, выполнять сценарии скрытым образом может быть нежелательно (а некоторые сценарии ожидают ввода пользователем определенной информации). На этот случай предусмотрено несколько настроек политики, которые помогают определять поведение сценариев для групповой политики. Такие настройки находятся в узле System\Scripts\Administrative Templates. Здесь вы обнаружите настройки для указания того, каким образом выполнять сценарий — синхронно или асинхронно, и должен он быть видимым или невидимым.

Переадресация папок

Одна из наиболее полезных работ, которые можно проделывать с помощью настроек User Configuration в групповой политике, связана с упорядочением папок AppData, Desktop, Start Menu, Documents, Favorites и Links для пользователя, что сопровождать его от компьютера к компьютеру. Эти папки являются важными элементами рабочей среды пользователя. В папке AppData хранится информация, специфичная для приложений пользователя (она нужна, например, Internet Explorer), а папка Desktop может содержать важные папки и ярлыки для пользователя. В папке Start Menu хранятся группы программ и ярлыки к программам, а папка Documents является стандартным местом для сохранения и извлечения файлов, своего рода разновидностью локального домашнего каталога.

Для использования переадресации папок существует несколько веских причин. Прежде всего, оно удобно для пользователей, которые входят в систему на разных компьютерах. Кроме того, если вы укажете сетевое местоположение для некоторых или всех таких папок, они будут регулярно копироваться и защищаться силами IT-отдела. Если по-прежнему применяются блуждающие профили, то настройка переадресации папок ускоряет синхронизацию серверного профиля с локальным профилем при входе и выходе, поскольку переадресованные папки в обновлении не нуждаются. Переадресация папок Desktop и Start Menu в централизованное, совместно используемое местоположение упрощает стандартизацию рабочих сред

пользователей и помогает устранять проблемы дистанционной поддержки, потому что персоналу технической поддержки будет известно, что все компьютеры сконфигурированы единообразно. Лучше всего то, что эти подходы можно смешивать и сочетать. Вполне допустимо указать общее местоположение для папок Desktop и Start Menu, в то время как разрешить пользователям иметь собственные папки Documents и AppData. Давайте взглянем на это.

Чтобы установить сетевое местоположение для папки Documents в групповой политике, выполните перечисленные ниже шаги.

1. Перейдите к папке User Configuration\Policies\Windows Settings\Folder Redirection\Documents.
2. Щелкните правой кнопкой мыши на выделенной папке Documents и выберите в контекстном меню пункт Properties (Свойства).

   Откроется диалоговое окно свойств, в котором обнаруживается, что данная настройка по умолчанию не сконфигурирована.
3. В раскрывающемся списке выберите вариант Basic (Базовая), чтобы указать единственное местоположение для папки Documents, совместно используемое всеми пользователями, или вариант Advanced (Расширенная), чтобы установить местоположения на основе членства в группах доступа.

   Если вы хотите иметь единственное местоположение для общей папки Documents, просто введите в поле Root Path (Корневой путь) сетевой путь или проследуйте к нему, щелкнув на кнопке Browse (Обзор).
4. Для обозначения разных местоположений сначала выберите группу доступа и затем укажите сетевой путь.

   На рис. 9.22 демонстрируется переадресация папки Documents для всех членов группы Domain Engineering на общий ресурс CentralEng на сервере Zooropa. Независимо от выбора варианта переадресации Basic или Advanced, политика разрешает выбрать одну из четырех опций:

   - Redirect the folder to the user's home directory (Переадресовать папку на домашний каталог пользователя)
   - Create a folder for each user under the root path (Создать папку для каждого пользователя в корневом пути)
   - Redirect to the following location (which you specify) (Переадресовать на следующее местоположение (которое вы укажете))
   - Redirect to the local user profile location (Переадресовать на местоположение локального профиля пользователя)
5. Для этого примера выберите вторую опцию; все члены группы Domain Engineering будут использовать один и тот же корневой путь, но иметь индивидуальные папки Documents.

   Когда выбрана данная опция, система создает подпапку, носящую имя пользователя, по указанному корневому пути.
6. Перейдите на вкладку Settings (Настройки), чтобы сконфигурировать настройки переадресации. Ради полноты настройки переадресации папки Documents показаны на рис. 9.23.

Рис. 9.22. Политика для переадресации папки `Documents` пользователя

Рис. 9.23. Дополнительные настройки в групповой политике, касающиеся переадресации папки `Documents` пользователя

Опции, которые вы видите на рис. 9.23, отражают стандартный выбор для папки `Documents`. Обратите внимание, что по умолчанию пользователь будет иметь эксклюзивные права доступа к этой папке. Также по умолчанию содержимое соответствующей папки будет перемещено в новое местоположение. Даже после удаления политики папка останется переадресованной, если только вы явно не отключите ее переадресацию.

Настройки безопасности

Настройки безопасности, наряду с административными шаблонами, формируют значительную часть групповой политики. Стандартные настройки безопасности специально открыты для минимизации головной боли при администрировании и для гарантии того, что пользователи и приложения работают ожидаемым образом. По мере усиления защиты пользователи и приложения имеют больше ограничений, и время их поддержки увеличивается. Другими словами, безопасность обратно пропорциональна удобству. Как только вы начинаете блокировать системы, обязательно что-то перестает работать. Эй, рядовые пользователи по умолчанию не могут даже устанавливать приложения в системе Windows Vista. Когда вы начнете принудительно применять пароли с длиной восемь и более символов, которые содержат буквы и цифры, не могут включать какую-либо часть имени пользователя и не могут повторно использоваться до тех пор, пока не будут применены 15 других паролей, все станет значительно сложнее. Для организаций, желающих усилить защиту, имеются инструменты и руководства.

Например, если вам приходилось когда-либо защищать сервер Windows согласно установленным руководствам в военном или другом ведомстве с высокими требованиями к безопасности, то вы знаете, что приходится устанавливать отдельные разрешения на определенных папках, изменять стандартные разрешения для доступа к некоторым ключам реестра, а также на изменение или создание других записей в реестре. В целом это отнимает несколько часов на одном сервере, даже у результа-

тивного администратора. А что если у вас есть 50 серверов и 500 рабочих станций? Для одних действий можно написать сценарии, но для других это не удастся. Не существует каких-то инструментов от Microsoft или независимых разработчиков, которые сделали бы все автоматически на всех компьютерах.

Именно здесь на помощь приходит групповая политика. Предполагая, что вы собираетесь заняться стандартизацией путем группирования серверов или рабочих станций либо даже части организации, вы должны изменить эти опасные разрешения в отношении реестра и настройки только однажды с применением групповой политики. Вам придется только один раз установить разрешения NTFS. Эти разрешения можно даже установить в одной политике и скопировать в другую. В любом случае, хотите вы высокую защиту или просто чуть большую, чем стандартная, велики шансы того, что вы пожелаете внести какие-то изменения, направленные на стандартизацию, и узел Security Settings (Настройки безопасности) определенно облегчит вам жизнь. Масса настроек безопасности находится в узле `Computer Configuration\Policies\Windows Settings\Security Settings`, хотя политики открытых ключей и политики ограничения программного обеспечения доступны по тому же пути, но в узле User Configuration.

Ниже перечислены важные категории настроек в Security Settings.

- **Account Policies (Политики учетных записей).** Указывает ограничения паролей, политики блокировка и политику Kerberos.
- **Local Policies (Локальные политики).** Конфигурирует аудит и назначение прав пользователям, а также смешанные настройки безопасности.
- **Event Log (Журнал событий).** Централизует опции конфигурации для журнала событий.
- **Restricted Groups (Ограниченные группы).** Принудительно применяет и управляет членством в определенных группах, таких как `Administrators`.
- **System Services (Системные службы).** Стандартизирует службы и конфигурации, а также защищает от изменений.
- **Registry (Реестр).** Создает шаблоны безопасности для разрешений на ключах реестра, чтобы управлять тем, кто и какие ключи может изменять, и управлять доступом по чтению к частям реестра.
- **File System (Файловая система).** Создает шаблоны безопасности для разрешений на файлах и папках, чтобы обеспечить наличие и сохранение файлами и папками желаемых разрешений.
- **Public Key Policies (Политики открытых ключей).** Управляет настройками для организаций, использующих инфраструктуру открытых ключей.
- **Software Restrictions Policies (Политики ограничений программного обеспечения).** Помещает ограничения на то, какое программное обеспечение может функционировать в системе. Это новое средство направлено на предотвращение запуска в системе вирусов и ненадежного ПО.

Использование шаблонов безопасности

Чтобы достичь "массового" внедрения мер защиты из предыдущего примера, вам понадобится какой-нибудь способ "ввести" настройки и затем их "развернуть".

Развертывание осуществляется довольно просто, т.к. имеется AD и групповая политика. Далее возникает вопрос о том, как "ввести" информацию безопасности, чтобы ее можно было отслеживать, многократно использовать и быстро модифицировать? Ответ: применить шаблоны безопасности. Мы полагаем, что если вы упустили их из виду, то просто-таки обязаны начать ими пользоваться. В этом разделе вы узнаете причины.

Предположим, вы решили, что группы `Power Users` (Опытные пользователи) на рабочих станциях гарантированно должны быть пустыми. Вы крайне утомлены процедурой избавления от последнего червя, приникшего в веб-сервер на всех компьютерах, на которых установлены службы IIS, так что вы собрались отключить службу веб-публикации на всех серверах, где она не нужна.

Однако это требует объемной работы. Таким образом, примите другой план: документ требований к безопасности. В этом документе вы обрисовываете, что должно быть сделано на каждой рабочей станции или сервере, согласно корпоративным требованиям. Вы распространяете готовый документ, но ни у кого нет времени, чтобы прочитать его. Также не существует простого способа проверить, удовлетворяют ли системы описанным требованиям. Или это только кажется?

Было бы замечательно щелкнуть на какой-то кнопке и внести нужные изменения в каждую систему. Это можно сделать с помощью нескольких инструментов: `secedit.exe` (оснастка консоли MMC под названием Security Configuration and Analysis (Конфигурирование и анализ безопасности)) и шаблоны безопасности.

Возможности шаблонов безопасности

В своей основе *шаблон безопасности* — это ASCII-файл, который вводится в программу по имени `secedit.exe`. Данный шаблон является набором инструкций (по существу сценарием), который сообщает инструменту `secedit.exe` о необходимости внесения разнообразных изменений в систему.

Шаблоны не позволяют изменять что-то, что вы не можете изменить другим способом; они просто предлагают удобный, сценарный и воспроизводимый метод внесения модификаций и затем легкого проведения аудита систем с целью проверки, удовлетворяют ли они требованиям этих шаблонов. Любое такое изменение можно было бы внести вручную через графический пользовательский интерфейс, но это отняло бы много времени. С помощью шаблонов можно модифицировать перечисленные ниже данные.

- **Разрешения NTFS.** Если необходимо выдать каталогу `C:\STUFF` разрешение Full Control (Полный доступ) для системы и группы `Administrators` и запретить доступ остальным, это можно сделать посредством шаблона. Поскольку шаблоны могут применяться не только к одному компьютеру, а также к их множеству (при условии, что вы пользуетесь групповыми политиками), вы применяете нужный набор разрешений NTFS ко всему домену.
- **Членство в локальных группах.** Возможно, у вас есть политика, настраивающая рабочие станции так, что членами локальной группы `Administrators` должны быть только учетная запись `Administrator` и доменная группа `Domain Admins`. Но кое-когда какой-то сотрудник службы поддержки "временно" повышает учетную запись пользователя до члена группы `Administrators`, простодушно намереваясь отменить это действие "как только в нем отпадет надобность". И

поскольку данный сотрудник службы поддержки постоянно занят, как и весь персонал этой службы, отмена никогда не будет сделана. За счет применения шаблона безопасности, который говорит "в локальной группе Administrators может быть только учетная запись Administrator и группа Domain Admins", любые другие учетные записи будут удалены из группы Administrators.

Принудительное применение настроек безопасности

Шаблоны автоматизируют процесс установки определенной информации, связанной с безопасностью, в точности как вы делаете это через графический пользовательский интерфейс. Не существует магического ангела-хранителя, который бы постоянно контролировал систему, обеспечивая постоянное применение желаемых настроек шаблона. Единственный способ гарантии того, что настройки остаются в силе, предусматривает либо повторное применение шаблона на какой-то регулярной основе, либо создание объекта GPO для применения шаблона, т.к. настройки безопасности в объекте GPO обновляются каждые 16 часов независимо от изменений.

- **Настройки локальной политики безопасности.** Каждый компьютер имеет десятки настроек локальной политики безопасности, такие как "Должно ли быть показано имя персоны, вошедшей в систему?", "Насколько часто должны меняться пароли для локальных учетных записей?" и "Кому разрешено изменять время в данной системе?", а также многие другие.

Работа с шаблонами

Продемонстрировать работу с шаблонами лучше всего на примере, поэтому давайте создадим шаблон для выполнения перечисленных ниже действий.

- Мы обеспечим, чтобы в систему не могли войти члены локальной группы Power Users.
- Мы установим такие разрешения NTFS, чтобы каталог C:\SECRET был доступен только для локальной группы Administrators.
- Наконец, мы завершим службы Internet Information Services, этот надоедливый веб-сервер, который, похоже, устанавливает себя сам в каждой операционной системе производства Microsoft.

Прежде всего, нам понадобятся некоторые инструменты. Давайте построим единый инструмент, используя консоль MMC. Кроме того, нам будут необходимы две оснастки: Security Templates (Шаблоны безопасности) и Security Configuration and Analysis (Конфигурирование и анализ безопасности). Выполните следующие шаги по настройке такого инструмента.

1. Откройте меню Start (Пуск), введите **mmc /a** в поле поиска и нажмите клавишу <Enter>, чтобы запустить пустую консоль MMC.
2. В пустой консоли MMC выберите пункт Add/Remove Snap-in (Добавить или удалить оснастку) в меню File (Файл).
3. В диалоговом окне Add or Remove Snap-ins (Добавление и удаление оснасток) выберите оснастку Security Configuration and Analysis и щелкните на кнопке Add (Добавить). Затем выберите оснастку Security Templates и снова щелкните на кнопке Add.

4. Щелкните на кнопке OK.
5. Сохраните новый специальный инструмент для будущего применения.

Инструмент должен выглядеть так, как показано на рис. 9.24.

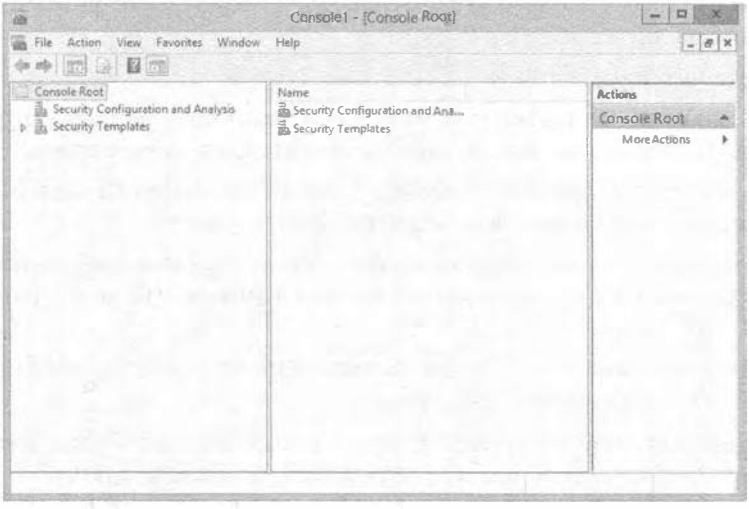


Рис. 9.24. Консоль MMC с оснастками Security Templates и Security Configuration and Analysis

Разверните узел Security Templates и добавьте новый путь для поиска шаблонов — `C:\Windows\Security\Templates`. Вы увидите предварительно построенный шаблон контроллера домена под названием `security.inf`.

Развертывание шаблонов безопасности

Развернув шаблон безопасности контроллера домена `security.inf`, в панели справа вы увидите папки, соответствующие всему тому, чем можно управлять.

- **Account Policies (Политики учетных записей).** Установка политик паролей, блокировок учетных записей и Kerberos.
- **Local Policies (Локальные политики).** Управление настройками аудита, правами доступа пользователей и параметрами безопасности.
- **Event Log Settings (Настройки журнала событий).** Управление параметрами сохранения событий.
- **Restricted Groups (Ограниченные группы).** Управление членством в разнообразных локальных группах.
- **System Services (Системные службы).** Включение и отключение служб, а также управление тем, кто имеет права на такие изменения.
- **Registry Security (Безопасность реестра).** Установка разрешений на изменение или просмотр любого заданного ключа реестра (и для каких ключей будет вестись аудит изменений).
- **File System (Файловая система).** Управление разрешениями NTFS для папок и файлов.

Но мы заинтересованы в построении нового шаблона с нуля. Чтобы сделать это, щелкните правой кнопкой мыши на пути к шаблону и выберите в контекстном меню пункт New Template (Создать шаблон). Введите имя шаблона и желаемое описание. Новый шаблон появится в виде папки в панели слева, наряду с предварительно построенным шаблоном. Новому шаблону назначено имя `Simple`. Первым делом очистим группу `Power Users`.

1. Откройте шаблон `Simple`.
2. Внутри вы увидите папку под названием Restricted Groups (Ограниченные группы). Щелкните на ней, чтобы она появилась в панели слева.
3. Щелкните правой кнопкой мыши на папке Restricted Groups и выберите в контекстном меню пункт Add Group (Добавить группу).
4. В открывшемся диалоговом окне Add Group (Добавление группы) введите **`Power Users`** или воспользуйтесь кнопкой Browse (Обзор), чтобы выбрать группу `Power Users`.

   Обратите внимание, что если вы работаете на контроллере домена, то группа `Power Users`, естественно, отсутствует.

По умолчанию включение группы в шаблон безопасности указывает этому шаблону на необходимость удаления из группы всех ее членов, так что дело сделано. Если вы хотите применить шаблон безопасности для помещения кого-то в группу, щелкните правой кнопкой мыши на имени группы и выберите в контекстном меню пункт Properties (Свойства), что позволит указать членов группы.

А теперь давайте настроим шаблон безопасности так, чтобы любая система, в которой имеется каталог `C:\SECRET`, была доступна только локальным администраторам.

1. В левой панели щелкните правой кнопкой мыши на папке File System (Файловая система) и выберите в контекстном меню пункт Add File (Добавить файл).
2. В открывшемся диалоговом окне вы можете либо перейти с помощью кнопки Browse (Обзор) к конкретному каталогу, либо просто ввести имя нужного каталога.

   Да, пункт контекстного меню назывался Add File, но допускается выбирать также и каталоги.
3. Введите **`C:\SECRET`** и щелкните на кнопке OK.

   Вы увидите стандартное диалоговое окно разрешений Windows NTFS.
4. Удалите разрешения для всех пользователей и групп кроме группы `Administrators`. Выдайте группе `Administrators` разрешение Full Control (Полный доступ).

   Будет задан вопрос о том, хотите вы применить это разрешение только к данной папке или также ко всем вложенным папкам.
5. Выберите предпочитаемый вами вариант и щелкните на кнопке OK.

Наконец, давайте завершим IIS.

1. Щелкните на папке System Services (Системные службы).

2. В панели справа щелкните правой кнопкой мыши на элементе World Wide Web Publishing Services (Службы веб-публикации) и выберите в контекстном меню пункт Properties (Свойства).
3. Отметьте флажок Define This Policy Setting in the Template (Определить эту настройку политики в шаблоне) и выберите переключатель Disabled (Отключена).
4. Щелкните на кнопке OK.

Теперь сохраните шаблон — щелкните правой кнопкой мыши на `Simple` (или как вы там назвали шаблон) и выберите в контекстном меню пункт Save (Сохранить). Если только вы не предусмотрели для своих шаблонов отдельную папку, как было описано ранее, вы получите файл по имени `simple.inf` в папке `\Windows\Security\Templates`.

Создание базы данных безопасности

Чтобы увидеть, как этот шаблон будет модифицировать систему, или чтобы применить настройку шаблона, используя оснастку MMC, вы должны создать базу данных безопасности. Для этого вам понадобится по существу скомпилировать ее из простой формы ASCII в двоичную форму, которая и называется *базой данных*. Это делается из другой оснастки, Security Configuration and Analysis.

1. Щелкните правой кнопкой мыши на оснастке Security Configuration and Analysis и выберите в контекстном меню пункт Open Database (Открыть базу данных), чтобы открыть диалоговое окно Open Database (Открытие базы данных), которое запрашивает базу данных для загрузки.

   В диалоговом окне Open Database вы хотите создать новую базу данных, но никаких опций для этого не предусмотрено; взамен просто введите имя новой базы данных.

2. Для целей рассматриваемого примера введите **`Simple`** и нажмите <Enter>.

   Ввод нового имени для базы данных приводит к тому, что оснастка определяет необходимость в *создании* новой базы данных, поэтому выдается запрос шаблона, из которого она должна быть построена. (Возможно, это звучит немного запутанно.) По умолчанию диалоговое окно отображает файлы с расширением `.inf` в папке `Windows\Security\Templates`.

3. Если вы следовали предыдущему примеру, выберите `simple.inf`.

   Однако прежде чем щелкать на кнопке Open (Открыть), обратите внимание на флажок Clear This Database Before Importing (Перед импортом очистить эту базу данных).

4. Отметьте этот флажок.

   В противном случае, когда вы экспериментируете с шаблоном, оснастка будет накапливать производимые вами изменения (что может хорошо подходить вам, но не всегда нам), а не переделываться сначала и начинать все с нуля.

5. Выберите шаблон и щелкните на кнопке Open.

   Ничего заметного не произошло, но на самом деле оснастка "скомпилировала" (это наш термин, а не Microsoft, и по нашему мнению он выглядит неплохим

сокращением для обозначения процесса преобразования шаблона ASCII в двоичную базу данных безопасности) шаблон в базу данных безопасности по имени `simple.sdb` в папке `My Documents\Security\Database`. В панели деталей вы увидите опции Configure (Конфигурировать) и Analyze (Анализировать).

6. Щелкните правой кнопкой мыши на оснастке Security Configuration and Analysis, и вы заметите в контекстном меню пункты Analyze Computer Now (Проанализировать компьютер сейчас) и Configure Computer Now (Сконфигурировать компьютер сейчас).

   Анализ не приводит к внесению изменений в компьютер. Вместо этого происходит сравнение состояния компьютера с состоянием, которое вы хотите создать с помощью шаблона. Затем анализ показывает (и сохраняет объяснения в файле журнала), каким образом ваша система изменится в результате применения шаблона. Файл журнала записывается в папку `\Documents\Security\Logs`.

7. Чтобы просмотреть, насколько ваш компьютер соответствует настройкам в базе данных, выберите пункт Analyze Computer Now, и вы увидите, насколько текущие настройки сравнимы с тем, к чему вы стремитесь.

8. Если вы хотите безрассудно прыгнуть вперед и применить настройки, то вместо Analyze Computer Now выберите пункт Configure Computer Now, чтобы модифицировать настройки системы, чтобы идти в ногу с шаблоном.

Все это очень хорошо, но как применить это к десяткам компьютеров? Придется подходить к каждому из них? Да, придется, если вы хотите использовать этот инструмент. Другим вариантом может быть инструмент командной строки, который называется `secedit.exe`. Он преобразует шаблоны в базы данных и применяет их. Чтобы прочитать, применить и в процессе работы создать базу данных, воспользуйтесь следующим синтаксисом:

```
secedit /configure /cfg имя_файла_шаблона /db имя_файла_базы_данных
  /overwrite /log имя_файла_журнала
```

Чтобы применить существующую базу данных без первоначального чтения шаблона, оставьте только ключ `/cfg` и его аргумент. Для применения шаблона к своим рабочим станциям вы могли бы поместить в сценарий входа (удостоверьтесь, что указали имена с полными путями для файлов шаблона, базы данных и журнала), чтобы это делалось при каждом входе. Также можно было бы воспользоваться службой планировщика задач (Task Scheduler), чтобы запускать пакетный файл и повторно применять шаблон через заданные интервалы. Или же можно было бы включить сервер Telnet на компьютерах с сервером Windows и просто применять шаблон, когда вам заблагорассудится.

Автоматизация и написание сценариев хороши, но что, если вы хотите использовать в своих интересах "автоматические" фоновые обновления, которые предлагает групповая политика, а также принудительное 16-часовое обновление настроек безопасности? Нет никаких проблем. Вы узнаете, как это делать, в следующем разделе.

Использование доменных групповых политик для применения шаблонов

Инструмент `secedit` удобен, но его приходится вызывать вручную либо из пакетного файла, а это означает беспорядочное редактирование сценариев входа или возню с запланированными задачами во всех системах. В случае использования сце-

нариев входа шаблон безопасности применяется только во время входа в систему. А как обеспечить более частое применение настроек безопасности? С помощью объекта GPO.

Доменные объекты GPO обладают рядом преимуществ.

- Легко управлять тем, к чему они применяются, что намного проще, чем исследование содержимого пакетных файлов.
- Они применяются повторно не только при входе в систему, но и на протяжении дня — рабочая станция обращается к ним с периодичностью от 60 до 120 минут.
- Настройки безопасности "применяются повторно" каждые 16 часов, на случай, если какая-то настройка была изменена пользователем, приложением и т.д.

Импорт шаблонов безопасности

В предыдущем разделе вы создали собственный шаблон безопасности `simple.inf`. Теперь вы хотите развернуть настройки безопасности из шаблона с использованием объекта GPO.

Шаги по импортированию шаблона очень просты. Ниже перечислены шаги для импорта шаблона `simple.inf` в объект GPO.

1. Запустите консоль GPMC.
2. Перейдите к организационной единице, содержащей компьютеры, к которым вы хотите применить настройки безопасности.

   Например, шаблон `simple.inf` мог бы применяться ко всем рабочим столам в организации.
3. Щелкните правой кнопкой мыши на организационной единице Desktops (Рабочие столы) и выберите в контекстном меню пункт Create a GPO in this domain, and link it here (Создать объект GPO в этом домене и привязать его).
4. Введите имя нового объекта GPO, скажем, Desktop Enforcement Policy (Политика применения к рабочим столам).
5. Щелкните правой кнопкой мыши на объекте Desktop Enforcement Policy и выберите в контекстном меню пункт Edit (Редактировать).
6. Внутри редактора GPME доберитесь до узла Security Settings (Настройки безопасности), который находится в Computer Configuration\Policies\Windows Settings (Конфигурация компьютера \ Политики \ Настройки Windows).
7. Щелкните правой кнопкой мыши на узле Security Settings и выберите в контекстном меню пункт Import Policy (Импортировать политику).
8. Щелкните на шаблоне безопасности `simple.inf` (можете воспользоваться кнопкой Browse (Обзор), если он хранится в сетевом общем ресурсе или на внешнем устройстве USB) и затем на кнопке Open (Открыть).
9. Удостоверьтесь в том, что настройки были импортированы, пройдя к узлу Restricted Groups (Ограниченные группы) под узлом Security Settings.
10. Щелкните на узле Restricted Groups и убедитесь, что в нем присутствует ваша политика в отношении группы `Power Users`.

Основной вопрос в том, что вы собираетесь делать сейчас? Хорошо, если есть возможность подождать 90 минут, то ничего делать не придется. Просто позвольте выполниться стандартному фоновому обновлению политики — и все ваши настройки будут применены ко всем компьютерам в организационной единице Desktops.

Новые административные шаблоны (ADMX/ADML)

Административные шаблоны старого стиля были неплохи, но не лишены проблем. Так, эти шаблоны ADM страдали проблемами с размером, сложностью написания сценариев и языковыми барьерами. Для решения всех этих проблем в Microsoft разработали новый тип файла, который заменяет шаблон ADM, появившийся в версии Windows Server 2008. Новые шаблоны основаны на XML и встречаются парами. Новыми файловыми расширениями являются ADMX и ADML.

Файлы ADMX и ADML теперь хранятся в `C:\Windows\PolicyDefinitions`. Открыв эту папку, вы обнаружите в ней более 100 файлов ADMX, наряду со стандартной папкой для английского языка, которая называется `en-US`. Папка `en-US` содержит всю специфичную для языка информацию, используемую при отображении настроек в редакторе GPME.

Новые файлы ADMX/ADML обладают несколькими преимуществами.

- Эти файлы не хранятся внутри структуры папок объекта GPO.
- Эти файлы могут переноситься практически на любой язык при условии, что для него подготовлен новый файл ADML и структура папок.
- Имеется возможность создания центрального хранилища, что позволяет проводить централизованное администрирование файлов ADMX/ADML.

Создание центрального хранилища для хранения и администрирования этих файлов так же просто, как создание копии структуры папок! Да, именно так — для централизации управления данными файлами понадобится всего лишь скопировать структуру папок на контроллеры домена. Чтобы создать центральное хранилище, выполните следующие шаги.

1. Откройте на компьютере Windows 8 или Windows Server 2012 R2 проводник и отобразите в нем папку `C:\Windows\PolicyDefinitions`.
2. Щелкните правой кнопкой мыши на папке `PolicyDefinitions` и выберите в контекстном меню пункт Copy (Копировать).
3. Откройте папку `C:\Windows\Sysvol\sysvol\<имя_домена>\Policies` на любом контроллере домена.
4. Щелкните правой кнопкой мыши на папке `Policies` и выберите в контекстном меню пункт Paste (Вставить).

В результате на контроллере домена появится дубликат структуры папок и файлов ADMX/ADML, как показано на рис. 9.25. Поскольку папка находится на контроллере домена, она будет автоматически реплицирована на все остальные контроллеры домена в этом домене.

Чтобы удостовериться в том, что теперь используются файлы ADMX из центрального хранилища, отредактируйте объект GPO и просмотрите текст после узла Administrative Templates внутри редактора GPME.

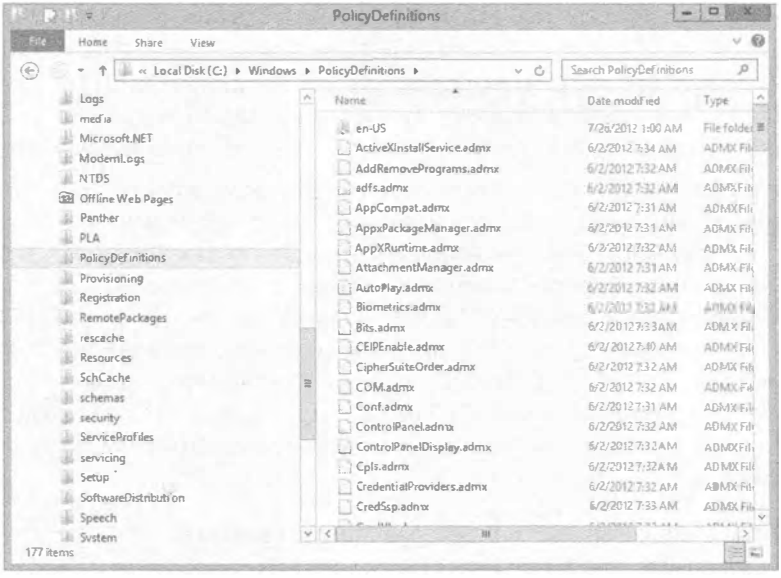


Рис. 9.25. Центральное хранилище для файлов ADMX/ADML

Имея специальное сочетание файлов ADMX/ADML после создания центрального хранилища, останется лишь скопировать файл ADMX в папку `PolicyDefinitions`, а файл ADML — в папку `en-US`. Новые настройки отобразятся в редакторе GPME.

Ограничение Internet Explorer

Похоже, для каждой настройки в Internet Explorer предусмотрена политика, позволяющая ее отключить. Учитывая, что немалое время на работе тратится на путешествия в Интернете, более чем разумно наложить контроль над настройками IE (к сожалению, многие компании применяют браузер Firefox, а не Internet Explorer).

Ниже описаны настройки, которые вы можете счесть полезными.

- Если вы хотите, чтобы пользователи не могли вмешиваться в настроенные вами зоны безопасности или чтобы в Internet Explorer использовались одинаковые настройки зон безопасности и прокси для всех пользователей на компьютере, тогда включите настройки Security Zones and Proxy (Зоны безопасности и прокси) в узле Computer Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer (Конфигурация компьютера / Политики / Административные шаблоны / Компоненты Windows / Internet Explorer).
- Чтобы предотвратить загрузку пользователями автономного содержимого на свои рабочие станции, включите политику по имени Disable Adding Schedules for Offline Pages (Отключить добавление графиков для автономного содержимого) в узле User Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Offline Pages (Конфигурация пользователя / Политики / Административные шаблоны / Компоненты Windows / Internet Explorer / Автономные страницы).
- Чтобы запретить пользователям внесение любых изменений в настройки на страницах Security (Безопасность), Connections (Подключения) или Advanced

Properties (Расширенные свойства) в IE, отключите доступ к этим и другим управляющим страницам в узле User Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel (Конфигурация пользователя / Политики / Административные шаблоны / Компоненты Windows / Internet Explorer / Панель управления Интернетом).

- Однако если вы хотите, чтобы пользователи имели возможность загружать любое программное обеспечение из Интернета, то это несколько сложнее. В узле User Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Browser Menus (Конфигурация пользователя / Политики / Административные шаблоны / Компоненты Windows / Internet Explorer / Меню браузера) существует политика, которая отключает опцию Save This Program to Disk (Сохранить эту программу на диск). Тем не менее, это не предотвращает установку пользователями ПО без его предварительного сохранения, и есть пара других способов, которыми опытные пользователи могут обойти данное ограничение.

Предотвращение установки или запуска пользователями неавторизованного программного обеспечения

Принимая меры по предотвращению установки программного обеспечения пользователями, включите политику под названием Prevent Removable Media Source for Any Install (Предотвратить любую установку со съемного носителя), находящуюся в узле User Configuration/Policies/Administrative Templates/Windows Components/Windows Installer (Конфигурация пользователя / Политики / Административные шаблоны / Компоненты Windows / Установщик Windows), чтобы сохранить пользователям возможность установки из CD-ROM или устройства для флоппи-дисков (помните о таких?). И если собираетесь сделать это, то должны также включить в узле User Configuration/Policies/Administrative Templates/Windows Components/Control Panel/Add or Remove Programs (Конфигурация пользователя / Политики / Административные шаблоны / Компоненты Windows / Панель управления / Добавление или удаление программ) политику для сокрытия опции Add a program from CD-ROM or floppy disk (Добавить программу из CD-ROM или флоппи-диска). Узел Control Panel содержит различные опции для отключения или удаления всех либо части опций аплета Add/Remove Programs (Добавление или удаление программ).

Тем не менее, отключение аплета Add/Remove Programs не лишит пользователей возможности запускать процедуры установки другими способами. Любой, имеющий доступ к командной строке, может обойти данные ограничения, поэтому вам придется открыть узел System (Система) политик User Configuration и включить политику Prevent access to the command prompt (Предотвратить доступ к командной строке). Если вы ищете печально известную политику под названием Run only specified Windows applications (Запускать только указанные приложения Windows), то она находится в узле System административных шаблонов конфигурации пользователя (рис. 9.26). Однако будьте осторожны с этой политикой; вам понадобится подготовить список всех приложений, которые могут быть запущены из проводника Windows. Здесь также располагается политика Don't run specified Windows applications (Не запускать указанные приложения Windows). А в таком случае потребуется создать список запрещенных программ.

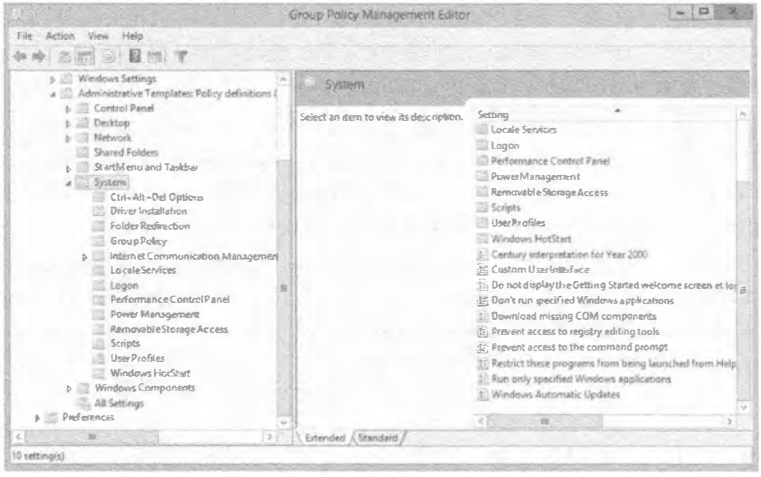


Рис. 9.26. Политика запуска только указанных приложений

Предотвращение редактирования реестра

Вы можете создать политику для предотвращения доступа к инструментам редактирования реестра. Включение этой политики запрещает пользователям запускать утилиты `regedt32.exe` и `regedt.exe`, хотя рядовые пользователи в любом случае имеют доступ только для чтения к подавляющему большинству содержимого реестра.

Аналогичный принцип применяется к меню Start и опции панели задач через политику Run from the Start menu (Запустить из меню "Пуск"). Опытные пользователи не потеряют возможность запуска несанкционированных программ только потому, что пункт Run (Выполнить) устранен из меню Start, поэтому вы должны выяснить все другие пути запуска программ и отключить их также (пользователи могут также запускать программы из диспетчера задач, если только вы не отключите опции, доступные по нажатию <Ctrl+Alt+Del>).

Создание согласованного рабочего стола и меню Start

Если вы хотите обеспечить в организации или в отделе упрощенный и согласованный рабочий стол и меню Start, то вам, скорее всего, придется комбинировать переадресацию папок с ограничениями, которые доступны в административных шаблонах.

Использование групповой политики для установки политики паролей и блокировки учетных записей

Одним из самых недопонимаемых и сложных аспектов Windows AD является то, каким образом и где конфигурируются и управляются политики паролей. В этом разделе вы получите общие сведения о том, как все работает, чтобы устранить любые неопределенности в будущем. Ниже приведен список фактов и мифов о настройках политики учетных записей (Account Policy), которые должны ответить на любые часто возникающие вопросы.

Факты

- Единственным методом модификации настроек политики Account Policy для доменных учетных записей является объект GPO, связанный с доменом.
- Детализированные политики паролей могут быть настроены, чтобы пользователи в одном домене имели отличающиеся настройки политики Account Policy. Другими словами, сотрудники IT-отдела могут иметь 20-символьные пароли, а управленческий персонал — скажем, трехсимвольные.
- Объект GPO, связанный с организационной единицей, будет модифицировать настройки политики локальных учетных записей SAM (SAM Account Policy) для локальных пользователей в SAM всех учетных записей компьютеров внутри данной организационной единицы.

Мифы

- Объект GPO может быть связан с организационной единицей `Domain Controllers` (Контроллеры домена), чтобы изменять настройки политики Account Policy для доменных учетных записей пользователей.
- Объект GPO может быть связан с организационной единицей, чтобы модифицировать настройки политики Account Policy для учетных записей пользователей, содержащихся внутри этой организационной единицы.
- Список ACL для стандартной политики домена (Default Domain Policy) может быть изменен с целью включения только определенных групп доступа, таким образом, разрешая применение разных политик паролей в одном домене.

По умолчанию в домене Windows Server 2012 R2 стандартная политика домена (Default Domain Policy) используется в целях установки настроек Account Policy для всех учетных записей пользователей в домене. (Это относится как к доменным учетным записям пользователей, так и ко всем локальным учетным записям SAM пользователей для компьютеров, присоединенных к домену.) Настройки политики паролей и блокировки учетных записей расположены в узле Computer Configuration/Policies/Windows Settings/Security Settings (Конфигурация компьютера / Политики / Настройки Windows / Настройки безопасности). Политики паролей включают перечисленные ниже опции.

- **Enforce Password History (Принудительно применять хронологию паролей).** Включайте эту опцию, чтобы указать требуемое количество следующих друг за другом уникальных паролей, прежде чем заданный пароль может использоваться снова.
- **Maximum Password Age (Максимальный возраст пароля).** Эта опция устанавливает период времени, в течение которого можно применять пароль, после чего система потребует у пользователя выбрать новый пароль. Организации обычно устанавливают этот промежуток где-то между 30 и 90 днями.
- **Minimum Password Age (Минимальный возраст пароля).** Эта опция устанавливает период времени, в течение которого пароль должен применяться, до того как пользователю будет разрешено изменить его.
- **Minimum Password Length (Минимальная длина пароля).** Эта опция определяет наименьшее количество символов, которые может содержать пароль пользовате-

ля. Хорошим значением минимальной длины для паролей может быть семь или восемь символов. Установка этой политики также запрещает пустые пароли.

- **Passwords Must Meet Complexity Requirements (Пароли должны удовлетворять требованиям к сложности).** В случае если вы интересуетесь, что это за требования, данная опция обычно называлась Passwords Must Meet Complexity Requirements of Installed Password Filter (Пароль должен удовлетворять требованиям к сложности, которые заданы установленным фильтром паролей). Библиотека DLL фильтров паролей была встроена в Windows 2000 Server и последующие версии ОС. Фильтры паролей определяют такие требования, как разрешенное количество символов, необходимость использования букв и цифр, возможность применения в пароле любой части имени пользователя и тому подобное.

  Если вы включите эту политику, то все новые и измененные пароли должны удовлетворять следующим требованиям:

  - они должны иметь длину, по крайней мере, шесть символов;
  - они не могут содержать имя пользователя целиком или его часть;
  - они должны использовать три из четырех типов символов: буквы верхнего регистра (A–Z), буквы нижнего регистра (a–z), цифры (0–9) и специальные символы (например, @, %, &, #).

- **Store Passwords Using Reversible Encryption (Хранить пароли с использованием обратимого шифрования).** Да, эта политика определенно снижает уровень защиты, сообщая контроллеру домена о возможности хранения паролей с применением обратимого шифрования. Это не намного лучше сохранения в виде простого текста; пароли обычно хранятся с использованием однонаправленного шифрования с помощью хеширования. Если это необходимо для отдельных учетных записей пользователей (вроде пользователей Mac), включите для них данную политику. Тем не менее, обратимое шифрование является обязательным в случае применения аутентификации CHAP (Challenge Handshake Authentication Protocol — протокол аутентификации по методу "вызов-приветствие") с удаленным доступом или службами Интернет-аутентификации (Internet Authentication Services).

Политика блокировки учетной записи (Account Lockout Policy) при включении предотвращает вход в систему от имени данной учетной записи после определенного количества неудавшихся попыток. Ниже описаны доступные опции.

- **Account Lockout Duration (Продолжительность блокировки учетной записи).** Эта настройка определяет промежуток времени, на протяжении которого учетная запись будет заблокирована. По истечении этого промежутка блокировка с учетной записи снимается, и пользователь может пробовать входить в систему снова. Если вы включите эту опцию, но оставите поле Minutes (Минуты) незаполненным, то учетная запись будет оставаться заблокированной до тех пор, пока ее не разблокирует администратор.

- **Account Lockout Threshold (Пороговое значение блокировки учетной записи).** Эта опция определяет, сколько раз пользователь может безуспешно пытаться войти в систему, прежде чем его учетная запись будет заблокирована. При определении этой настройки укажите количество разрешенных попыток, иначе учетная запись никогда не будет разблокирована.

- **Reset Account Lockout Counter After (Сбрасывать счетчик блокировки учетной записи через).** Эта опция задает промежуток времени, по прошествии которого подсчет неудавшихся попыток входа будет начат заново. Например, предположим, что вы сбрасываете данный счетчик через две минуты и разрешаете три попытки входа. Тогда в случае если три раза не удается войти в систему, придется подождать две минуты, после чего снова предоставляются три попытки входа.

Предпочтения групповой политики

Одним из наиболее впечатляющих аспектов Windows Server 2012 R2 (относящихся не только к групповой политике, но полностью к новой операционной системе) являются предпочтения групповой политики (Group Policy preferences — GPP). Предпочтения групповой политики — это расширения групповой политики, которые по-другому можно назвать "новыми настройками в объекте GPO". Число таких новых настроек превышает 3000, и некоторые из них просто удивительны! Например, теперь вы можете изменять пароль локальной учетной записи `Administrator` на любом рабочем столе внутри среды в рамках интервала около 90 минут. Вы также можете управлять членством в локальной группе `Administrators` на всех рабочих столах и серверах, не удаляя учетные записи ключевых служб и другие доменные группы, которые являются уникальными для каждого компьютера.

Настройки GPP

Настройки GPP немного отличаются от других настроек групповой политики, главным образом потому, что они дублируются в областях, относящихся к компьютеру и пользователю, объекта GPO. Появляется высокая гибкость и мощь в определении того, что требуется обеспечить для рабочих столов и пользователей в среде.

Настройки GPP описаны в табл. 9.1.

Таблица 9.1. Настройки предпочтений групповой политики

Настройка предпочтений групповой политики	Доступна ли в узле Computer Configuration?	Доступна ли в узле User Configuration?
Applications (Приложения)	Нет	Да
Drive Maps (Отображения устройств)	Нет	Да
Environment (Среда)	Да	Да
Files (Файлы)	Да	Да
Folders (Папки)	Да	Да
Ini Files (Файлы INI)	Да	Да
Network Shares (Общие сетевые ресурсы)	Да	Нет
Registry (Реестр)	Да	Да
Shortcuts (Ярлыки)	Да	Да
Data Sources (Источники данных)	Да	Да
Devices (Устройства)	Да	Да
Folder Options (Опции папок)	Да	Да
Internet Settings (Настройки Интернета)	Нет	Да

Окончание табл. 9.1

Настройка предпочтений групповой политики	Доступна ли в узле Computer Configuration?	Доступна ли в узле User Configuration?
Local Users and Groups (Локальные пользователи и группы)	Да	Да
Network Options (Опции сети)	Да	Да
Power Options (Опции электропитания)	Да	Да
Printers (Принтеры)	Да	Да
Regional Options (Региональные опции)	Нет	Да
Scheduled Tasks (Запланированные задачи)	Да	Да
Services (Службы)	Да	Нет
Start Menu (Меню "Пуск")	Нет	Да

Большинство настроек в табл. 9.1 не требуют особых пояснений. Тем не менее, мы предоставим краткую информацию о том, как можно использовать некоторые из настроек. Например, вопросы безопасности всегда приходят на ум первыми у персонала IT-отдела, когда речь заходит о защите рабочих столов, но никогда нет достаточного времени, ведь правда? Возьмем проблему переустановки пароля для локальной учетной записи `Administrator` на каждом рабочем столе внутри компании. Да, мы знаем, что это болезненная тема! Но когда вы последний раз выполняли данную задачу на своих рабочих столах? Во время установки? Два года назад? Какие только ответы не приходилось нам слышать, но теперь благодаря GPP вы можете изменять пароли для `Administrator` как угодно часто. Чтобы это произошло, выполните следующие шаги.

1. Модифицируйте объект GPO, который нацелен на все ваши рабочие столы (лучше всего будет связать этот объект GPO с организационной единицей, содержащей все настольные компьютеры).
2. После открытия редактора GPME для объекта GPO перейдите к узлу Computer Configuration\Preferences\Control Panel\Local Users and Groups (Конфигурация компьютера \ Предпочтения \ Панель управления \ Локальные пользователи и группы).
3. Щелкните правой кнопкой мыши на этом узле и выберите в контекстном меню пункт New⇨Local User (Создать⇨Локальный пользователь). Откроется диалоговое окно New Local User Properties (Свойства нового локального пользователя), представленное на рис. 9.27.

Понятие новой политики пользователя

Когда вы выбираете в контекстном меню пункт New⇨Local User для GPP, то на самом деле не создаете нового пользователя. Думайте об этом, как о создании новой политики пользователя! Вы можете создать нового пользователя, но здесь имеется намного большее число опций, чем доступно при одном лишь создании пользователя. Принятие точки зрения "новая политика XYZ" во время создания любой новой настройки GPP поможет понять то, что вы будете делать с этой настройкой.

Рис. 9.27. Диалоговое окно New Local User Properties для GPP

4. Введите имя пользователя, которым вы хотите управлять, в данном случае **`Administrator`**.
5. Введите желаемый пароль и подтвердите его.

Вуаля! Это переустановит пароль локальной учетной записи `Administrator` на каждом рабочем столе, который подпадает под область действия объекта GPO. По прошествии примерно двух часов все рабочие столы, подключенные к домену и сети, обновят указанную установку.

Все очень просто, не так ли? Остальные настройки столь же просты, и мощь GPP поистине впечатляет. Чтобы дать вам представление о том, что еще можно делать с помощью GPP, ниже приведен список идей по настройкам политик, с воплощения которых вы можете начать.

- Applications (Приложения)
- Включите проверку правописания в Microsoft Word.
- Сконфигурируйте средство автоматической архивации Outlook.
- Сконфигурируйте "утвержденную компанией и согласованную" подпись для электронной почты Outlook.
- Drive maps (Отображения устройств)
- Замените все отображения устройств в сценарии входа с помощью настройки предпочтений групповой политики.
- Отобразите устройства только для сеансов Terminal Services.
- Environment (Среда)
- Создайте переменную среды ноутбуков, которая используется с другими настройками предпочтений групповой политики.
- Предусмотрите переменные среды для имени, фамилии, адреса и тому подобного, которые затем могут применяться в подписи Outlook.

- Files (Файлы)
- Передавайте базу определений вирусов из сервера на рабочий стол.
- Развертывайте файлы конфигураций приложений на рабочих столах.
- Folders (Папки)
- Очищайте папку `Temporary Internet Files` (Временные файлы Интернета).
- Создайте папку приложений для рабочих столов, на которых запускаются защищенные приложения.
- Network shares (Общие сетевые ресурсы)
- Управляйте общими сетевыми ресурсами на сервере только в рабочее время.
- Включите для сервера перечисление, основанное на доступе.
- Registry (Реестр)
- Что бы вы ни назвали — все это можно делать с реестром.
- Data sources (Источники данных)
- Создайте централизованную конфигурацию источников данных для специалистов по продажам.
- Создайте специальную конфигурацию источников данных для персонала службы поддержки.
- Folder options (Параметры папок)
- Позвольте всем сотрудникам IT-отдела видеть все скрытые и суперскрытые файлы на каждом администрируемом ими рабочем столе.
- Позвольте всем сотрудникам IT-отдела видеть файловые расширения в проводнике Windows на всех рабочих столах, которых они касаются.
- Internet settings (Настройки Интернета)
- Сконфигурируйте настройку прокси Internet Explorer для всех пользователей офиса филиала 1.
- Сконфигурируйте специальные настройки Internet Explorer, которые стандартные настройки глобальной политики обрабатывать не могут, такие как все настройки на вкладке Advanced (Дополнительно) диалогового окна конфигурации Internet Explorer.
- Local users and groups (Локальные пользователи и группы)
- Переустанавливайте пароли локальных учетных записей `Administrator` на каждом рабочем столе.
- Управляйте членством в локальной группе `Administrators` на каждом рабочем столе и сервере (кстати, без предварительного удаления членов из группы!).
- Power options (Параметры электропитания)
- Создайте 24-часовую схему параметров электропитания, при которой пользователи никогда не видят эту схему в рабочее время, но когда сотрудники покидают систему, компьютер переводится в режим сна после того, как в течение пяти минут не наблюдается какой-либо активности. (Доказано, что такой подход позволяет экономить около $50 на ПК в год.)

- Printers (Принтеры)
- Устраните принтеры из сценариев входа.
- Сконфигурируйте принтеры для пользователей ноутбуков, которые перемещаются из одного удаленного офиса в другой, предоставив им только те принтеры, которые им нужны, на основе их местонахождения.
- Scheduled tasks (Запланированные задачи)
- Пробудите компьютер в полночь, чтобы разрешить проведение обслуживания (великолепная комбинация с параметрами электропитания!).
- Services (Службы)
- Сконфигурируйте другую учетную запись службы для усиления общей защиты.
- Сконфигурируйте пароль для учетной записи службы.
- Сконфигурируйте поведение службы на случай отказа функционирования, чтобы обеспечить ее гладкий перезапуск.

Нацеливание на уровне элементов

Еще одним замечательным аспектом GPP являются возможность нацеливания на уровне элементов. Теперь любую настройку GPP можно нацеливать и применять ее, только предварительно удостоверившись, что в среде компьютера присутствует тот или иной аспект. Для примера предположим, что в отделе кадров функционирует приложение, которое существует в среде Terminal Services. Когда сотрудники этого отдела запускают свое приложение, они нуждаются в отображенном устройстве для него. Решение, применяемое многими компаниями в наши дни, предусматривает отображение устройства для учетной записи пользователя, получая в итоге "неоправданное" отображенное устройство, которое существует, даже когда сотрудники работают на своих рабочих столах. Нацеливание на уровне элементов GPP позволяет предоставлять отображение устройства, *только* если они находятся в среде Terminal Services. Получить контроль такого типа можно, воспользовавшись одной из множества разнообразных опций, нацеливаемых на уровне элементов. Ниже приведен полный их список:

- Battery Present (Наличие батареи)
- Computer Name (Имя компьютера)
- CPU Speed (Скорость ЦП)
- Date Match (Соответствие даты)
- Dial-up Connection (Коммутируемое подключение)
- Disk Space (Дисковое пространство)
- Domain (Домен)
- Environment Variable (Переменная среды)
- File Match (Соответствие файла)
- IP Address Range (Диапазон IP-адресов)
- Language (Язык)
- LDAP Query (Запрос LDAP)

- MAC Address Range (Диапазон MAC-адресов)
- MSI Query (Запрос MSI)
- Operating System (Операционная система)
- Organizational Unit (Организационная единица)
- PCMCIA Present (Наличие PCMCIA)
- Portable Computer (Переносимый компьютер)
- Processing Mode (Режим обработки)
- RAM (ОЗУ)
- Registry Match (Соответствие реестра)
- Security Group (Группа доступа)
- Site (Сайт)
- Terminal Session (Терминальный сеанс)
- Time Range (Диапазон времени)
- User (Пользователь)
- WMI Query (Запрос WMI)

Пример из практики

Устранение сценариев входа с применением предпочтений групповой политики

Многие компании по-прежнему используют унаследованные сценарии входа для применения к рабочим столам таких настроек, как отображение устройств и принтеров. Использование сценариев входа является устаревшим приемом по сравнению с новыми и усовершенствованными возможностями GPP.

Многие другие компании переключились на применение GPP, где только возможно, для устранения некоторых, а то и всех настроек в своих сценариях входа. Вы можете использовать следующие предпочтения вместо сценариев входа.

Drive Mappings (Отображения устройств). Отображения устройств теперь может быть нацелено на создание "своевременных" отображений, которые имеют больший смысл для пользователей. Цели на уровне элементов могут применяться в сочетании с отображениями устройств для предоставления доступа к данным только при условии того, что у пользователя установлено корректное приложение, применены последние исправления, и это сеанс Terminal Services.

Printers (Принтеры). Принтерами зачастую трудно управлять в средних и крупных организациях, в которых имеются мобильные пользователи. Когда пользователь прибывает в офис филиала компании, ему может быть нелегко найти и сконфигурировать подходящий принтер. С помощью предпочтений GPP для принтеров можно отобразить все принтеры в компании. В случае использования с целью уровня элемента (такой как диапазон IP-адресов или сайт AD) пользователи получат доступ к нужному принтеру в офисе филиала всего лишь потому, что находятся в этом офисе.

Registry (Реестр). Благодаря этому предпочтению, любые записи реестра теперь могут быть помещены в объект GPO без какого-либо специального шаблона ADM или файла ADMX. Это касается также двоичных и многострочных значений, что было невозможно в шаблонах ADM.

Новая и усовершенствованная консоль GPMC

Консоль GPMC существует уже довольно долгое время. Первое поколение консоли GPMC было на тот момент кардинально новым и намного упрощало администрирование объектами GPO. Текущее поколение GPMC продолжает поддерживать простое, эффективное и надежное администрирование объектов GPO. Ушли те времена, когда необходимо было запускать оснастку Active Directory Users and Computers, чтобы просматривать, создавать, связывать и управлять объектами GPO. Мягко выражаясь, это стало архаичным. Теперь новую консоль GPMC можно запускать в среде Windows Server 2012 R2 и Windows 8.

Консоль GPMC потребуется установить, т.к. по умолчанию она не устанавливается. На компьютерах Windows Server 2012 R2 ее можно установить из диспетчера серверов.

1. Откройте окно диспетчера серверов и выберите пункт меню Features (Компоненты).
2. Здесь вам необходимо только выбрать переключатель Add Features (Добавить компоненты), что приведет к отображению полного списка инструментов, которые можно установить (рис. 9.28).

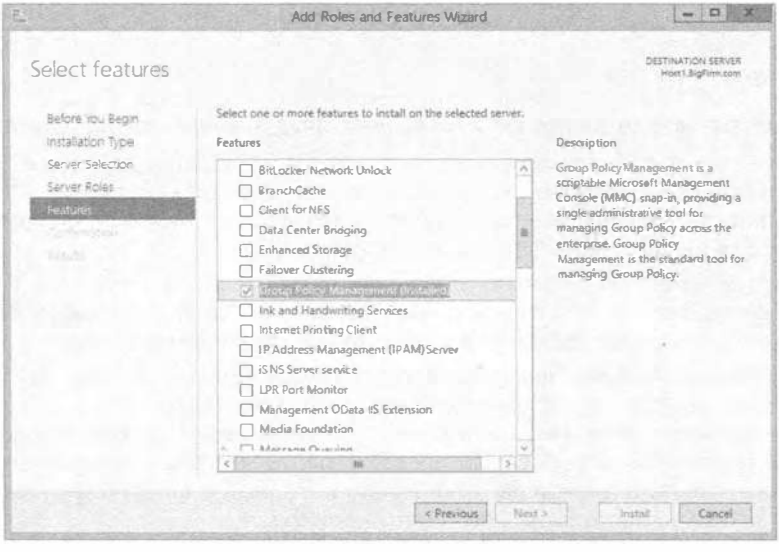


Рис. 9.28. Установка консоли GPMC через диспетчер серверов

3. Выберите элемент Group Policy Management (Управление групповой политикой), что инициирует процесс получения установленного инструмента.
4. После перезагрузки вы будете иметь установленную консоль GPMC.

На компьютерах Windows 7 или Windows 8 для консоли GPMC понадобится установить инструменты дистанционного администрирования серверов (Remote Server Administration Tools).

Для этого выполните следующие действия.

1. Установите актуальные пакеты обновлений (некоторые загружаемые файлы могут уже их включать).
2. Установите инструменты Remote Server Administrative Tools.
3. Откройте панель управления из меню Start (Пуск).
4. Щелкните на аплете Programs and Features (Программы и компоненты).
5. Щелкните на ссылке Turn Windows features on or off (Включение или отключение компонентов Windows).

Стартовые объекты GPO

В Microsoft прилагают большие усилия, чтобы сделать управление объектами GPO более простым и эффективным. Первая попытка в этом направлении — стартовые объекты GPO (Starter GPO). Объект Starter GPO можно использовать для воссоздания набора настроек GPO, применяя только Starter GPO снова, снова и снова. Предположим для примера, что вы отвечаете за обеспечение корректной конфигурации Internet Explorer внутри организации. Вы можете создать объект Starter GPO, который включает все обязательные настройки Internet Explorer. Затем при создании любого нового объекта GPO будет использоваться этот объект Starter GPO, чтобы гарантировать включение настроек Internet Explorer.

Для создания нового объекта Starter GPO выберите узел Starter GPO (Стартовый объект GPO) в консоли GPMC и выполните перечисленные ниже шаги.

1. Щелкните правой кнопкой мыши на узле Starter GPO и выберите в контекстном меню пункт New (Создать).
2. Введите имя объекта Starter GPO, например, `IE Starter GPO`.
3. Чтобы сконфигурировать настройки IE, объект Starter GPO необходимо отредактировать, как это делалось бы с любым другим объектом GPO — щелкните на нем правой кнопкой мыши в консоли GPMC и выберите в контекстном меню пункт Edit (Редактировать).

Теперь, когда объект Starter GPO создан, любой, кто имеет полномочия создавать объект GPO в домене, может применять его в качестве "стартового набора настроек". При создании любого нового объекта GPO с помощью консоли GPMC в диалоговом окне New GPO (Новый объект GPO) имеется раскрывающийся список Source Starter GPO (Исходный стартовый объект GPO), как показано на рис. 9.29. Однако имейте в виду, что значительное ограничение объектов Starter GPO состоит в том, что они могут включать только настройки административных шаблонов GPO.

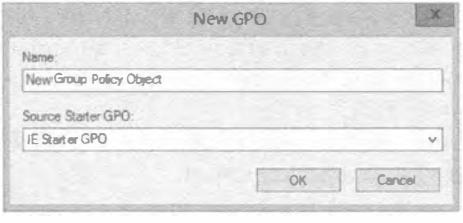


Рис. 9.29. При создании объектов GPO можно использовать раскрывающийся список Source Starter GPO

Резервное копирование и восстановление объектов GPO

Консоль GPMC является универсальным инструментом для всех задач по управлению объектами GPO. Одним из наиболее важных аспектов защиты существующих ресурсов GPO является их резервное копирование. (В мире компьютеров это относится к чему угодно; вы защищены настолько, насколько свежа резервная копия ваших данных!)

Консоль GPMC предоставляет возможности резервного копирования и восстановления, позволяющие архивировать каждую версию объекта GPO, которую вы создали и внедрили. Очень удобно то, что эти возможности предлагаются прямо в графическом пользовательском интерфейсе консоли GPMC, не требуя запуска другого инструмента для проведения такой работы.

Резервное копирование объекта GPO выполняется просто.

1. Щелкните правой кнопкой мыши на объекте GPO, подлежащем резервному копированию.
2. Выберите в контекстном меню пункт Back up (Резервное копирование).

   Откроется диалоговое окно Back Up Group Policy Object (Резервное копирование объекта групповой политики).
3. Укажите местоположение, где хранятся резервные копии.

   Это может быть заранее определенное местоположение или же можно создать папку во время процесса резервного копирования.
4. Введите местоположение или щелкните на кнопке Browse (Обзор) в зависимости от того, что вам больше подходит.
5. Щелкните на кнопке Back up (Копировать).

   Отобразится индикатор хода работ по резервному копированию.
6. После успешного создания резервной копии закройте диалоговое окно Back Up Group Policy Object.

> **Резервное копирование до и после изменения**
>
> Подобно любым изменениям данных и других аспектов операционной системы, резервные копии должны создаваться непосредственно до внесения изменения, а также сразу после него, чтобы сохранить оба состояния объекта GPO.

Наступит время, когда вы захотите просмотреть список объектов GPO, резервные копии которых были созданы. Для этого щелкните правой кнопкой мыши на узле Group Policy Objects (Объекты групповой политики) внутри консоли GPMC и выберите в контекстном меню пункт Manage Backups (Управлять резервными копиями). Откроется диалоговое окно Manage Backups (Управление резервными копиями), представленное на рис. 9.30.

В этом диалоговом окне можно восстанавливать, удалять и просматривать настройки объекта GPO внутри резервной копии.

- **Restore (Восстановить).** Кнопка Restore позволяет восстановить "архивированный объект GPO" поверх "производственного объекта GPO". Вам должно быть понятно, насколько это может быть важно!

- **Delete (Удалить).** Кнопка Delete позволяет удалить архивированные объекты GPO, главным образом те, которые больше не используются или *действительно* устарели. Нет никаких причин захламлять свои серверы информацией, которая не понадобится в будущем.
- **View Settings (Просмотреть настройки).** Кнопка View Settings позволяет просмотреть содержимое объекта GPO, а также другие ключевые сведения, такие как делегирование, безопасность, связи и т.д. На рис. 9.31 показана HTML-страница, которая отображается в результате щелчка на кнопке View Settings.

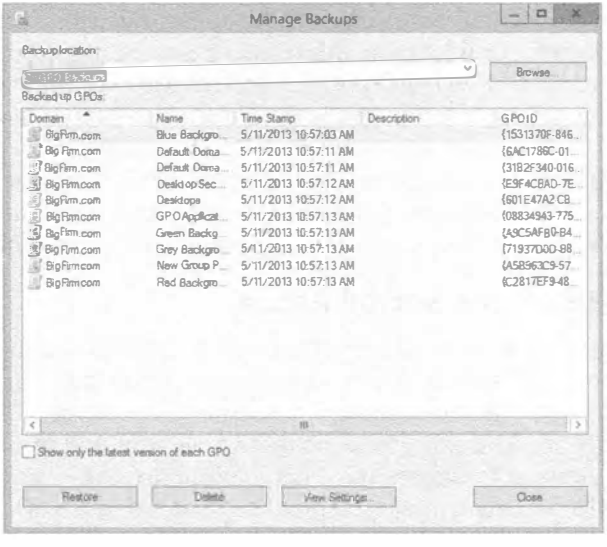


Рис. 9.30. Консоль GPMC позволяет управлять резервными копиями объектов GPO

Рис. 9.31. Кнопка View Settings позволяет просмотреть всю информацию, связанную с объектом GPO

Поиск и устранение неполадок в групповых политиках

На тот случай, если это еще не прояснилось к настоящему моменту: групповые политики мощны, но вместе с тем и сложны. К тому же они могут быть непрозрачными — иногда вы создаете для контроллера домена множество настроек политики, которые направлены на управление определенным рабочим столом, и затем перезапускаете рабочий стол, входите в систему, ждете результатов применения новой политики, но ничего не происходит.

Для поиска и устранения неполадок в групповых политиках предназначено несколько инструментов. Оснастка и инструмент консоли RSOP (Resultant Set of Policy — результирующая политика) предоставляет графический интерфейс, а утилита `gpresult.exe` позволяет выполнять эквивалентные функции в командной строке. Утилита `gpotool.exe` входит в состав набора ресурсов Windows (Windows Resource Kit), и она ищет несоответствия между объектами GPO, которые хранятся на контроллерах домена. Эта небольшая утилита помогает идентифицировать проблемы с репликацией, которые вызывают проблему с применением групповой политики.

Инструмент Resultant Set of Policy

Поиск и устранение неполадок в групповых политиках были для администраторов крупным препятствием к обретению полного контроля над сетевой средой. Проблема заключалась в невозможности просмотра совокупных настроек политики, которые в итоге воздействовали на пользователя или на компьютер. Небольшое средство отображения действительных настроек политики — инструмент Resultant Set of Policy (RSOP) — является встроенным в Windows Server. Используя RSOP, вы можете проверять версии "что, если" в целях диагностики проблем. Без RSOP придется просмотреть свойства каждого сайта, домена и организационной единицы, выясняя, каким образом связаны контейнеры и политики. Затем понадобится просмотреть списки ACL и информацию WMI, чтобы увидеть, проводится ли какая-нибудь фильтрация, и также проверить опции Disabled, Block Inheritance и Enforce. Не забывайте о нацеливании на уровне элементов, которое может быть очень детализированным и потому приводить к путанице при попытке оценки вручную. Наконец, необходимо просмотреть настройки интересующей политики, прежде чем станет ясным корень проблемы. Вам придется делать множество заметок. По этим причинам мы отдаем предпочтение инструменту RSOP.

Инструмент RSOP запускается простым вводом **`rsop.msc`** в командной строке. Сразу после запуска вы заметите, что он определяет результирующую политику, которая была применена на основе компьютера, где инструмент выполняется, и учетной записи пользователя, под которой был совершен вход в систему. Результирующее окно похоже на то, что отображается в редакторе GPME (рис. 9.32).

Относительно инструмента `rsop.msc` следует сделать несколько замечаний.

- Этот инструмент предоставляет только примененные объекты GPO и настройки из таких GPO.
- Этот инструмент выдает представление, в котором указано, из какого объекта GPO поступает каждая настройка.

Рис. 9.32. Инструмент `rsop.msc` генерирует представление реального времени настроек политики, которые были применены

Получение результатов групповой политики с использованием консоли GPMC

Консоль GPMC является инструментом, который похож на локализованную версию RSOP, но для получения RSOP позволяет запрашивать любой компьютер и любого пользователя в сети. Представьте, что пользователь звонит вам и сообщает о том, что не может получить доступ к веб-сайту, который необходим ему для выполнения своей работы. Вы могли бы подойти к пользователю физически, но это всего лишь отняло бы время, т.к. вы уверены, что пользователи получают настройки прокси Internet Explorer из объекта GPO. Таким образом, вместо этого выполните следующие шаги.

1. Запустите мастер результатов групповой политики (Group Policy Results Wizard) в консоли GPMC.

   Мастер Group Policy Results Wizard находится ближе к нижней части консоли GPMC. После запуска мастера вы должны лишь указать компьютер и пользователя, для которого хотите получить результаты, а об остальном позаботится сам мастер, как показано на рис. 9.33.

2. Выберите пользователя и рабочий стол, куда он вошел, после чего перейдите к настройке прокси IE.

   Вы заметите, что к компьютеру применяется некорректный объект GPO, поскольку кто-то настроил принудительное применение объекта GPO, связанного с вышестоящей организационной единицей, что сводит на нет нашу установку прокси. Проблема обнаружена.

3. Исправьте проблему с опцией Enforce в объекте GPO и дело сделано!

Результаты из мастера будут отображаться на трех вкладках в панели справа — Details (Подробности), Summary (Сводка) и Policy Events (События политики).

- **Details.** На вкладке Details (рис. 9.34) приведены все настройки, включая объекты GPO, которые были применены, те, что отказали, группы доступа, фильтры WMI и другие сведения.
- **Summary.** На вкладке Summary отображаются любые ошибки, которые возникали во время создания объектов GPO.
- **Policy Events.** Вкладка Policy Events уникальна тем, что на ней отображаются настройки из программы просмотра событий (Event Viewer), которые относятся к групповой политике.

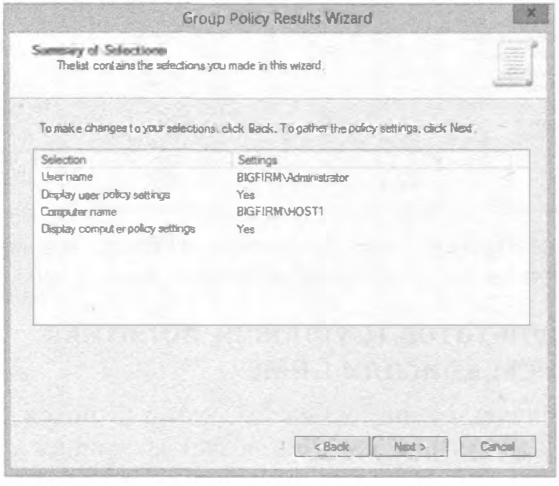


Рис. 9.33. Мастер Group Policy Results Wizard в консоли GPMC

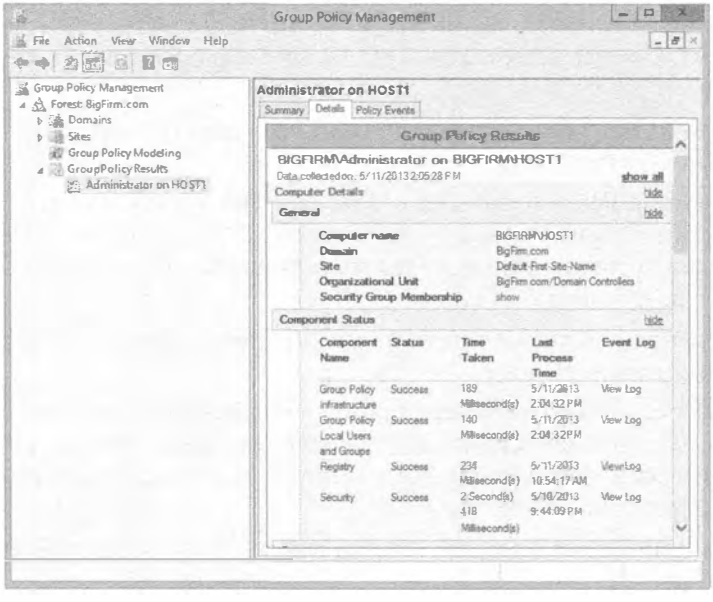


Рис. 9.34. Мастер Group Policy Results Wizard отображает информацию на трех вкладках в консоли GPMC

Если вы замечаете проблему с какой-то примененной настройкой, то можете воспользоваться содержимым всех трех вкладок для ее отслеживания.

Моделирование групповой политики с использованием консоли GPMC

Мастер Group Policy Results Wizard в консоли GPMC является мощным инструментом, который позволяет просматривать существующее состояние объектов GPO и их настройки для любого компьютера и пользователя в сети. Однако что, если возникла ситуация, когда нужно переместить компьютер в другую организационную единицу или перенести в другую организационную единицу пользователя, поскольку он получил повышение по службе? Вы не должны просто переместить учетную запись и ожидать, что настройки будут корректными в новом местоположении внутри AD.

gpresult.exe

`gpresult.exe` — это инструмент, предназначенный для поиска и устранения неполадок в групповой политике, а также для формирования отчетов, который дополняет оснастку RSOP, добавляя в арсенал RSOP возможности командной строки и пакетных файлов. При запуске без аргументов или опций утилита `gpresult.exe` сгенерирует следующую информацию RSOP для текущего пользователя на локальном компьютере:

- контроллер домена, из которого рабочая станция получила политики;
- когда политики были применены;
- какие политики были применены;
- какие политики не были применены из-за фильтрации;
- членство в группах;
- сведения о правах доступа пользователей (если запускается в многословном режиме).

Чтобы сгенерировать информацию RSOP для удаленного пользователя на удаленном компьютере, применяйте аргументы `/S` *имя_системы* и `/USER` *имя_пользователя*. Например, чтобы получить информацию RSOP на удаленной рабочей станции `WINDOWS8CLIENT1` для пользователя `dmelber`, введите команду

```
gpresult /S WINDOWS8CLIENT1 /USER dmelber
```

Ниже описаны опции, позволяющие получить более детальные сведения.

- `/V` указывает на необходимость в выдаче более многословной информации: `gpresult /V`.
- `/Z` указывает на необходимость в выдаче даже еще более многословной информации (Zuper-verbose): `gpresult /Z`.
- Для нацеливания только на политику компьютера добавьте опцию `/SCOPE MACHINE`; если вы заинтересованы лишь в политиках пользователя, добавьте опцию `/SCOPE USER`.

Таким образом, например, для получения максимальной информации о политиках пользователя, примененных к данной системе, добавьте опцию `gpresult /Z /SCOPE USER`. Вывод этой команды легко перенаправить в текстовый файл, чтобы сохранить отчет:

```
gpresult /S WINDOWS8CLIENT1 /USER dmelber /Z > c:\gpinfo.txt
```

Использование программы Event Viewer

Прекратите посмеиваться прямо сейчас! Мы полностью серьезны! Временами действительно нужно дружески похлопать Microsoft по спине, и это как раз тот случай. Программа Event Viewer (Просмотр событий) была полностью модернизирована, и сейчас, к изумлению многих, в ней появился целый узел, выделенный для групповой политики!

Журнал операций групповой политики (Operational) является заменой файла `Userenv.log`, который генерировался групповой политикой в прошлом. Теперь нет необходимости в специальной установке настроек многословной информации или аудита; это просто происходит. Чтобы просмотреть файлы журналов групповой политики в новой программе Event Viewer, достаточно ее запустить. В открывшемся окне Event Viewer разверните узел Applications and Services Logs\Microsoft\Windows\GroupPolicy (Журналы приложений и служб \ Microsoft \ Windows \ Групповая политика). Здесь вы найдете журнал Operational для групповой политики, щелкнув на котором, вы сможете просмотреть список событий в панели справа.

Ниже приведено несколько замечаний по возможностям новой среды.

- Журнал Operational заменяет файл `Userenv.log` из предшествующих версий групповой политики Windows.
- Вкладки General (Общие) и Details (Подробности) предоставляют полезную информацию для поиска и устранения проблем.
- Двойной щелчок на событии приводит к открытию собственного окна для события.
- Щелчок на знаке + во вкладке Details приводит к отображению дополнительной информации о событии.

Основы поиска и устранения неполадок: сохраняйте простоту

Мы прогнозируем, что даже имея в своем распоряжении инструмент RSOP, работа с групповыми политиками в большинстве случаев не будет похожа на легкую прогулку по парку. Ниже приведены соображения, которые помогают минимизировать время поиска и устранения неполадок.

- Сохраняйте простоту своей стратегии в отношении политик. По возможности храните пользователей и компьютеры в организационных единицах и применяйте политики на как можно более высоком уровне.
- Избегайте наличия большого количества объектов GPO с конфликтующими политиками, которые применяются к одним и тем же получателям.
- Минимизируйте использование опций Enforce и Block Inheritance.

- Документируйте свою стратегию групповой политики. Структуру политик можно изобразить визуально и вывесить рисунок на стенде подобно диаграмме топологии сети. Когда возникнет проблема, вы сможете свериться с диаграммой, прежде чем приступать к ее поиску и разрешению.
- Тестируйте настройки GPO до их развертывания! Абсолютно необходимо сохранять ресурсы службы поддержки и гарантировать работоспособность основных приложений и системных служб.

Делегирование Active Directory

Делегирование Active Directory является эффективным решением в часто встречающейся ранее ситуации с унаследованными доменами Windows, когда для обеспечения раздельного управления пользователями, группами и компьютерами создавалось множество доменов. За счет реализации делегирования внутри единственного домена Active Directory устраняется потребность в нескольких доменах, сохраняется бюджет, благодаря сокращению количества контроллеров доменов, упрощается управление предприятием из-за наличия всего лишь одного домена и т.д.

Это настолько захватывающая возможность Active Directory, что многие компании и предприятия перешли на Active Directory, чтобы получить в свое распоряжение все преимущества, предлагаемые делегированием Active Directory. Одно из наиболее интересных преимуществ применения делегирования связано с возможностью выдачи одной или нескольким группам привилегии на сброс паролей для учетных записей пользователей. Это значит, что вы можете разрешить какой-то группе пользователей сбрасывать пароли только для подмножества пользователей в домене. Например, вы можете позволить руководителю отдела кадров сбрасывать пароли для учетных записей сотрудников этого отдела.

Делегирование прав администрирования групповой политикой

Возможность делегирования операций создания и конфигурирования объектов GPO и их настроек административному персоналу (или другим, если уж на то пошло) исключительно полезна, особенно в крупной организации. В этом разделе мы объясним, как разрешить сотрудникам, не являющимся членами группы `Domain Admins` или `Enterprise Admins`, создавать и управлять объектами GPO для определенных сайтов, доменов или организационных единиц.

Консоль GPMC предоставляет простой, но распределенный массив опций для гарантии того, что вы реализуете делегирование правильному множеству администраторов. Ниже перечислены пять главных делегирований, которые вы захотите сконфигурировать:

- создание объектов GPO;
- связывание объектов GPO;
- управление объектами GPO;
- редактирование объектов GPO;
- чтение объектов GPO.

Все это конфигурируется в консоли GPMC. Основная путаница при установке делегирования для управления объектами GPO в консоли GPMC возникает с областями действия. Это означает необходимость знания мест, где устанавливается делегирование; вдобавок нужно знать, насколько далеко делегирование будет простираться. Например, предположим, что вы являетесь администратором организационной единицы отдела кадров, т.е. вы управляете всеми аспектами, включая учетные записи пользователей, группы и даже объекты GPO, связанные с этой организационной единицей. Как удостовериться в том, что вы — единственный администратор, который может связать какой-то объект GPO с организационной единицей отдела кадров? Хорошо, это одна из задач делегирования, которыми можно управлять с помощью консоли GPMC. Давайте рассмотрим каждый вид делегирования и его область действия.

По умолчанию объекты GPO могут создаваться членом группы `Administrators` для домена или членами глобальной группы под названием `Group Policy Creator Owners` (Владельцы создателей групповой политики). Однако хотя члены группы `Administrators` имеют полный контроль над всеми объектами GPO, члены группы `Group Policy Creator Owners` могут модифицировать только политики, которые создали сами, если только им специально не было выдано разрешение на изменение других политик. Таким образом, если вы поместите выбранного администратора групповой политики в группу доступа `Group Policy Creator Owners` (которая почти так же неудобна, как и группа `Active Directory Users and Computers`), то это лицо сможет создавать новые объекты политик и модифицировать их.

Чтобы делегировать возможность создания объекта GPO в домене, вы должны добраться до узла Group Policy Objects (Объекты групповой политики) в консоли GPMC. После щелчка на этом узле перейдите на вкладку Delegation (Делегирование) в правой панели для просмотра списка пользователей и групп, которым была предоставлена возможность создания объектов GPO в домене (рис. 9.35).

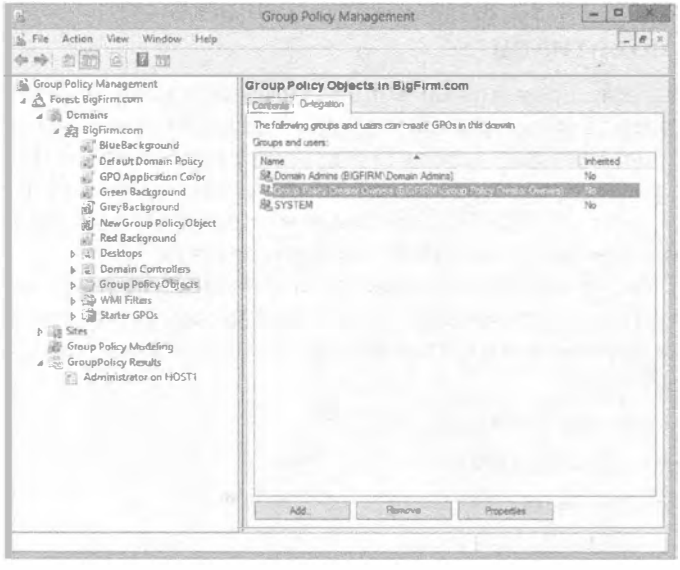


Рис. 9.35. Делегирование возможности создания объектов GPO с использованием консоли GPMC

Создание объекта GPO является лишь одним аспектом, а другим будет связывание этого GPO с сайтом, доменом или организационной единицей. Администраторы из группы `Administrators` способны делать это по умолчанию, но для предоставления такой возможности другим администраторам можно сконфигурировать специальное делегирование по каждому узлу AD. Здесь очень важно следовать области действия. В отличие от возможности создания объекта GPO, которая распространяется на весь домен, возможность связывания GPO с узлом AD касается только этого узла AD, что вполне имеет смысл. А как насчет конфигурирования такого делегирования?

Чтобы сконфигурировать тех, кто может связывать объект GPO с каким-либо узлом AD, вам необходимо выбрать целевой узел AD в консоли GPMC. Затем в панели справа перейдите на вкладку Delegation (Делегирование). Ее имеет каждый узел AD. Обратите внимание на то, что пользователи и группы в стандартном списке могут связывать объект GPO с этим узлом, как показано на рис. 9.36. Имейте в виду один ключевой момент: такое делегирование связывания с узлом AD не наследуется вглубь структуры AD. Следовательно, если вы делегируете возможность связывания объекта GPO узлу домена, это не приводит к предоставлению такой возможности всем организационным единицам в данном домене.

Финальные три вида делегирования обладают одной и той же областью действия — на каждый объект GPO. Опять-таки, в этом есть своя логика, но некоторым людям не всегда удается воспроизвести эту логику на клавиатуре. Если это логично, вы должны быть в состоянии выбрать объект GPO в консоли GPMC, а затем в панели справа перейти на вкладку Delegation, чтобы увидеть задачи делегирования для GPO. Это в точности то, что представлено на рис. 9.37 — три уровня делегирования для GPO. Здесь для просмотра полного списка задач делегирования понадобится щелкнуть правой кнопкой мыши на объекте GPO.

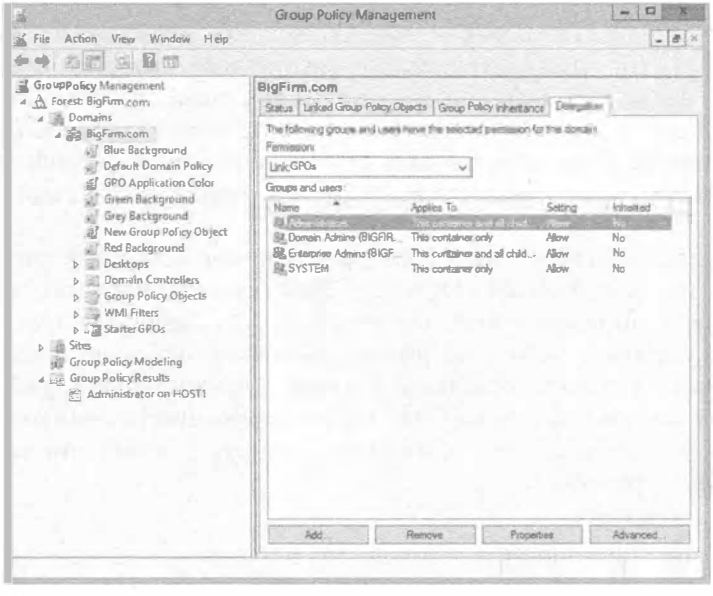


Рис. 9.36. Делегирование возможности связывания объекта GPO домену

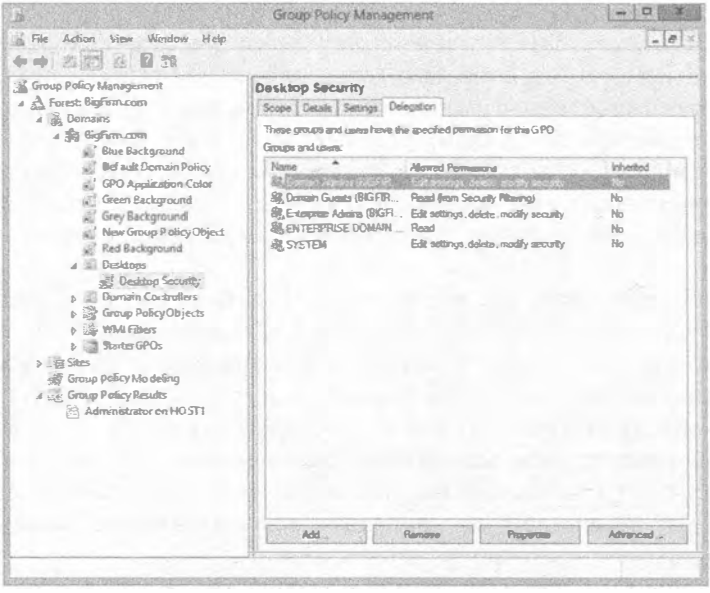


Рис. 9.37. Делегирование задачи управления, редактирования и чтения объекта GPO

В интерфейсе указано не "управлять объектом GPO", а Edit settings, delete, modify security (Редактировать настройки, удалять, изменять параметры безопасности) для объекта GPO.

Делегирование управления с использованием организационных единиц

Безусловно, одной из сильных сторон AD является возможность выдачи частичных или полных прав администрирования группе пользователей, предполагая, что это делается с целью разделения сети с одним доменом, скажем, на части Uptown (спальный район) и Downtown (деловой район), Marketing (отдел маркетинга), Engineering (конструкторский отдел) и Management (отдел управления), или еще как-нибудь. Давайте рассмотрим простой пример, демонстрирующий, как это можно сделать.

Предположим, что в отделе маркетинга работают пять сотрудников: Адам (Adam), Бетти (Betty), Чип (Chip), Дебби (Debbie) и Элен (Elaine). Они хотят, чтобы у одного сотрудника, Элен, была возможность сброса паролей. Причина в том, что проблема "Я забыл свой пароль — можете ли вы мне сбросить его?" чаще других озвучивается при звонках сотрудников отдела маркетинга в центральную службу поддержки. В центральной службе поддержки были бы счастливы иметь кого-то внутри отдела маркетинга, кто взял бы данную проблему в свои руки, освободив их для решения других насущных проблем.

Ниже описан процесс.

1. Создайте организационную единицу под названием `Marketing`.

   Конечно, организационной единице можно назначить любое другое имя, но `Marketing` впоследствии проще будет вспомнить.

2. Переместите существующие учетные записи Адама, Бетти, Чипа, Дебби и Элен в организационную единицу `Marketing`.
3. Создайте группу под названием `MktPswAdm`, где будут находиться учетные записи тех пользователей, которые могут сбрасывать пароли для персонала в организационной единице `Marketing`.

   И снова вы можете выбрать для группы какое-то другое имя.
4. Сделайте учетную запись пользователя `Elaine` членом группы `MktPswAdm`.
5. Делегируйте управления сбросом паролей для организационной единицы `Marketing` группе `MktPswAdm`.

Если вы хотите воспроизвести этот пример, проведите подготовку, создав учетные записи Адама, Бетти, Чипа, Дебби и Элен, но не делая их администраторами. Или сделайте это в командной строке; введите **`net user` *`имя_пользователя`* `/add`** и создайте в папке `Users` указанные учетные записи. Например, вот как создать учетную запись для Адама:

```
net user Adam Pa$$word /add
```

Для выполнения такой работы вы должны находиться на контроллере домена. Создавать пользователей домена в командной строке можно на любой другой системе, но тогда потребуется добавить опцию `/domain`:

```
net user adam /add /domain
```

Создание новой организационной единицы

Создавать новые организационные единицы несложно. Откройте оснастку Active Directory Users and Computers (ADUC), щелкните правой кнопкой мыши на имени домена в панели слева и выберите в контекстном меню пункт New⇨Organizational Unit (Создать⇨Организационная единица). Откроется диалоговое окно с запросом имени для новой организационной единицы. Введите **`Marketing`** и щелкните на кнопке OK. Дело сделано.

Перемещение учетных записей пользователей в организационную единицу

Далее, для перемещения учетных записей пользователей `Adam`, `Betty`, `Chip`, `Debbie` и `Elaine` в организационную единицу `Marketing` откройте оснастку ADUC, разверните узел домена (в данном случае это `Bigfirm.com`; ваш домен может называться иначе) и откройте папку `Users`. (Если вы создали пять учетных записей пользователей в другой папке, откройте ее.)

Чтобы переместить все пять учетных записей пользователей, шелкните на учетной записи Adam и, удерживая нажатой клавишу <Ctrl>, щелкните на оставшихся четырех учетных записях. Затем щелкните правой кнопкой мыши на одной из выделенных пяти учетных записей и выберите в контекстном меню пункт Move (Переместить); откроется диалоговое окно с запросом, куда переместить "объект". Изначально в нем будет видно имя домена со знаком "плюс" рядом с ним. Щелкните на этом знаке "плюс" и узел домена раскроется, отобразив имеющиеся в нем организационные единицы. Выберите организационную единицу `Marketing` и щелкните на кнопке OK; все пять учетных записей переместятся в `Marketing`.

Можете открыть организационную единицу Marketing в оснастке ADUC и удостовериться, что указанные учетные записи теперь находятся в ней.

В качестве альтернативы можно воспользоваться возможностью перетаскивания. Внутри оснастки ADUC щелкните на папке Users внутри левой панели. В правой панели должно отобразиться содержимое папки Users. В левой панели вы будете иметь возможность видеть не только папку Users, но также и организационную единицу Marketing. Выберите учетные записи пользователей и перетащите их из правой панели в организационную единицу Marketing. Мгновенное перемещение в организационную единицу! (Что-что вы говорите? Вы не впечатлены? Хорошо, тогда поверьте нам, что когда вам доведется выполнять большой объем работ по управлению пользователей, вы сочтете этот прием настоящим спасательным поясом. Просто доверьтесь нам.)

Создание группы MktPswAdm

Следующим действием будет создание группы для пользователей, которые могут сбрасывать пароли в организационной единице Marketing. Опять-таки, работа производится в оснастке ADUC. Щелкните на организационной единице Marketing, чтобы выделить ее, и выберите пункт меню Action⇨New⇨Group (Действие⇨Создать⇨Группа). (Можно также щелкнуть правой кнопкой мыши на организационной единице Marketing и выбрать в контекстном меню пункт New⇨Group (Создать⇨Группа).) Вы увидите диалоговое окно New Object — Group (Новый объект — Группа), подобное показанному на рис. 9.38.

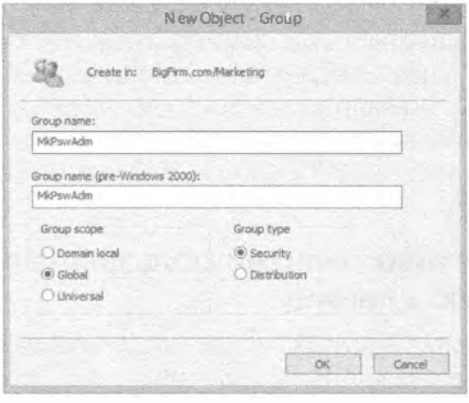


Рис. 9.38. Создание новой группы

Диалоговое окно New Object - Group предлагает опцию для создания группы любого из трех типов, доступных в Active Directory. Нашим целям соответствует глобальная группа, хотя в этом конкретном случае — группа в заданном домене, получающая контроль в организационной единице в том же домене, — подойдет локальная группа домена, глобальная или универсальная группа. Мы назначили группе имя MktPswAdm. Щелкните на кнопке OK.

Поместите учетную запись пользователя Elaine в группу MktPswAdm. Щелкните правой кнопкой мыши на имени группы MktPswAdm и выберите в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом окне свойств перейдите на вкладку Members (Члены), щелкните на кнопке Add (Добавить), выберите

учетную запись Elaine, щелкните на кнопке Add и затем на кнопке OK. Вы увидите, что пользователь Elaine теперь является членом группы MktPswAdm. Щелкните на кнопке OK, чтобы закрыть диалоговое окно.

Делегирование управления сбросом паролей в организационной единице Marketing группе MktPswAdm

Теперь давайте соберем все вместе. В оснастке ADUC щелкните правой кнопкой мыши на организационной единице Marketing и выберите в контекстном меню пункт Delegate Control (Делегировать управление). Откроется начальный экран мастера делегирования управления (Delegation of Control Wizard).

Этот мастер предлагает упрощенный способ установки делегирования и в рассматриваемом первом примере он работает хорошо. Щелкните на кнопке Next (Далее) и отобразится следующий экран мастера (рис. 9.39).

Затем вы должны сообщить о том, что часть задач управления делегируете группе, и указать эту группу. Щелкните на кнопке Add (Добавить) и выберите группу MkPswAdm. После щелчка на кнопке OK для закрытия диалогового окна Add (Добавление) экран мастера выглядит так, как показано на рис. 9.40.

Щелкнув на кнопке Next, вы получите меню задач, которые можно делегировать (рис. 9.41).

Здесь вы найдете очень много функций, которые могут быть делегированы. Вместо того чтобы заставить преодолевать длинный список функций, которые вас никогда не будут интересовать, в Microsoft решили выбрать из них десяток или около того функций, которые вероятнее всего захочется делегировать, и одной из них является возможность сброса паролей. На рис. 9.41 эта функция выбрана; щелкните на кнопке Next, в результате чего отобразится последний экран мастера (рис. 9.42).

Щелкните на кнопке Finish (Готово), чтобы завершить работу мастера.

Вспомните, что делегирование позволяет выбрать набор пользователей, которые будут иметь контроль определенного вида над другим набором пользователей и/или компьютеров. Это достигается путем помещения контролирующих пользователей в отдельную группу, помещения контролируемых пользователей и/или компьютеров в организационную единицу и делегирования группе необходимых задач управления этой организационной единицей.

Рис. 9.39. Перед выбором группы

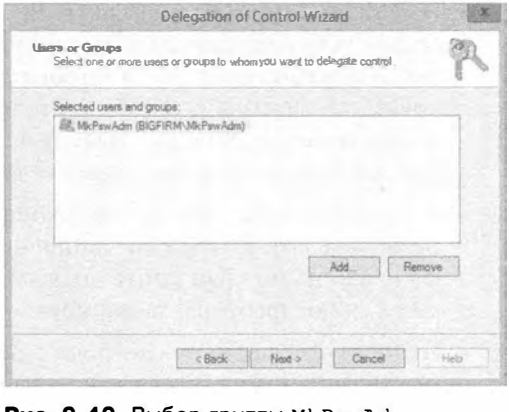


Рис. 9.40. Выбор группы MkPswAdm

Рис. 9.41. Задачи для делегирования

Рис. 9.42. Подтверждение выбора

Расширенное делегирование: ручная установка разрешений

Хотя предыдущий сценарий является удачным — и успешным — примером, он только слегка приоткрывает мощь делегирования. На самом деле для делегирования вы не обязаны использовать мастер; он всего лишь упрощает выполнение определенного диапазона распространенных задач.

Рекомендуемые приемы делегирования

Делегирование — это удобный инструмент для администрирования сети. При аккуратном применении оно приносит немалую пользу. До этого момента упоминалось только несколько рекомендуемых приемов делегирования, а сейчас мы расширим их перечень дополнительными советами.

- Создавайте группы и организационные единицы, к которым применяется делегирование. Этот облегчает их защиту, а также выполнение задач администрирования.
- Избегайте назначения разрешений непосредственно пользователю. Создайте группу (как обсуждалось ранее) и поместите в нее пользователя. Создание группы, содержащей одного пользователя, не так уж обременительно, как может показаться поначалу. В действительности это намного упрощает жизнь администратора, не заставляя выяснять, по какой причине тот или иной пользователь по-прежнему может выполнять действия, которые не должен выполнять.
- Назначайте пользователям и группам наименьший объем разрешений. Это поможет сделать сеть более защищенной. Пользователи могут думать, что имеют право на полный контроль абсолютно над всем, но им редко, если вообще когда-либо, требуется такой контроль.
- Используйте полный контроль продуманно. Полный контроль может нанести встречный удар по вам, когда пользователи или группы начнут извлекать выгоду от вашего щедрого дара. Полный контроль дает пользователю возмож-

ность работать с разрешениями объекта. Это означает, что пользователи могут предоставить себе более высокие разрешения, чем планировал администратор. Вдобавок, если кто-то получает контроль над учетной записью, то он сможет внести намного больше беспорядка, нежели в противном случае.

- Для дальнейшего усиления защиты и расширения удачных приемов администрирования делегируйте задачу создания объектов и задачу управления объектами разным группам. Такой подход известен как двухсубъектная целостность (two-person integrity — TPI). Если вы разделите ответственность между двумя персонами или группами, снизится вероятность некорректного управления со стороны любого из них. Думайте об этом как о разделении разрешений на создание резервных копий и восстановление из этих копий между двумя группами. Например, одной группе администраторов можно предоставить возможность создания групп в организационной единице, тогда как другой группе администраторов позволить управлять членством в группах.
- Создавайте представления панелей задач. Представления панелей задач удобны, когда вы хотите делегировать задачи персоналу службы поддержки или другим группам, которым требуются определенные разрешения, но не желаете, чтобы они имели доступ к полной консоли. Такой прием помогает обучать новых администраторов, прежде чем им будут предоставлены бразды правления всем доменом.
- Вы можете выполнять делегирование на уровнях выше организационной единицы, но в качестве правила избегайте поступать подобным образом. Если вы делегируете разрешения на уровне домена, то такой пользователь или группа могут потенциально получить возможность намного большего влияния на сеть, чем вы ожидали.

Оставайтесь с нами

Даже если вы не очень интересуетесь делегированием, все равно проработайте данный пример. Он демонстрирует навигацию по трем уровням с нарастающей сложностью в диалоговых окнах безопасности Windows Server 2012 R2.

Ниже показано, как можно напрямую манипулировать делегированием.

1. Откройте оснастку ADUC и выберите пункт меню View⇨Advanced Features (Вид⇨Дополнительные возможности). На экране отобразятся новые элементы (рис. 9.43).
2. Щелкните правой кнопкой мыши на организационной единице `Marketing` и выберите в контекстном меню пункт Properties (Свойства).

   Откроется диалоговое окно свойств организационной единицы `Marketing` с вкладкой Security (Безопасность). (Между прочим, если дополнительные возможности не включены, вкладка Security не отображается.)
3. Перейдите на вкладку Security и вы увидите примерно то, что показано на рис. 9.44.

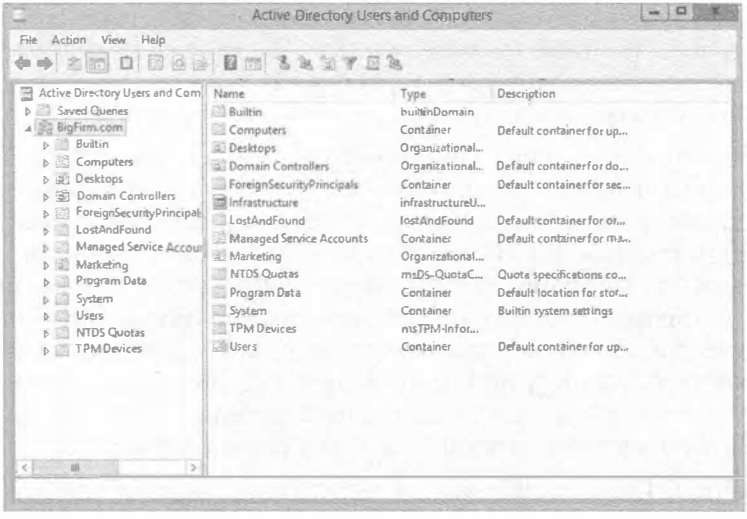


Рис. 9.43. Оснастка ADUC с включенными дополнительными возможностями

Список разрешений для группы `MkPswAdm` прокручен вниз, чтобы вы видели, что для нее предлагается. Здесь отмечен только флажок Special permissions (Специальные разрешения), что не особенно информативно. Это верхний уровень диалогового окна безопасности Windows Server 2012 R2. Считайте его обзорным уровнем для информации, связанной с безопасностью. Откровенно говоря, мы находим такое высокоуровневое представление довольно ограниченным. Все, на что оно действительно указывает — что в этом диалоговом окне существует много записей (все они на рисунке не уместились), и вы можете вспомнить, что каждая из них называется *записью управления доступом* (access control entry — ACE). Список таких записей называется *списком управления доступом* (access control list — ACL).

Теоретически вы должны иметь возможность щелкнуть на любой записи ACE в верхней части диалогового окна и получить в нижней части сведения о том, что конкретно эта запись ACE позволяет делать указанным объектам. Например, на рис. 9.44 видно, что группа `MkPswAdm` имеет "специальные" разрешения. Это одна из причин, почему нам не нравится данное диалоговое окно, поскольку понятие "специальные" дает не особенно много информации. Другая причина связана с тем, что это диалоговое окно показывает только крайне упрощенный список возможных разрешений, что иногда будет вводить в заблуждение. Вот почему хорошо, что есть возможность углубиться на следующий уровень, щелкнув на кнопке Advanced (Дополнительно).

4. Щелчок на кнопке Advanced приводит к отображению диалогового окна дополнительных настроек безопасности (рис. 9.45).
5. Прокрутите список Permission entries (Записи разрешений) до появления группы `MkPswAdm`, и вы увидите, что для нее есть две записи: в одной указано "специальное" разрешение, а в другой разрешения вообще не указаны, что в принципе не несет в себе сколько-нибудь полезной информации.

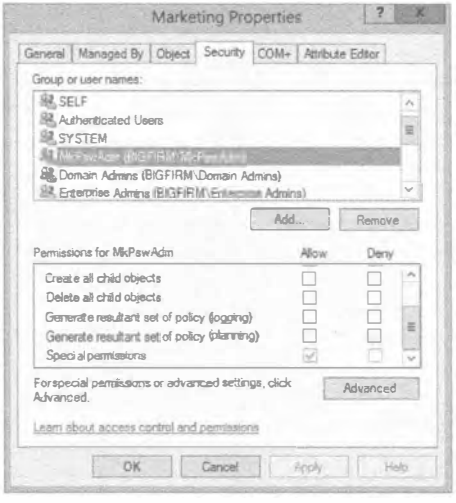


Рис. 9.44. Вкладка Security диалогового окна свойств организационной единицы `Marketing`

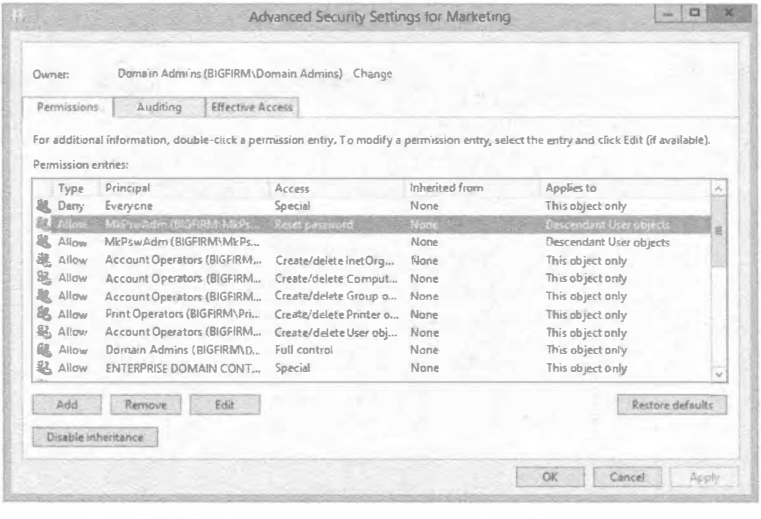


Рис. 9.45. Дополнительные настройки безопасности для организационной единицы `Marketing`

6. При выделенной первой из этих записей щелкните на кнопке Edit (Редактировать). Откроется диалоговое окно, показанное на рис. 9.46.

   Прокрутив содержимое окна, вы увидите, что группе `MkPswAdm` была предоставлена возможность чтения и записи свойств дочерних объектов пользователей (Descendant User objects), но *только* одного свойства `pwdLastSet` — именно так на языке AD называется возможность отметки флажка User must change password at next logon (Пользователь должен изменить пароль при следующем входе), который доступен в диалоговом окне Reset Password (Сброс пароля).

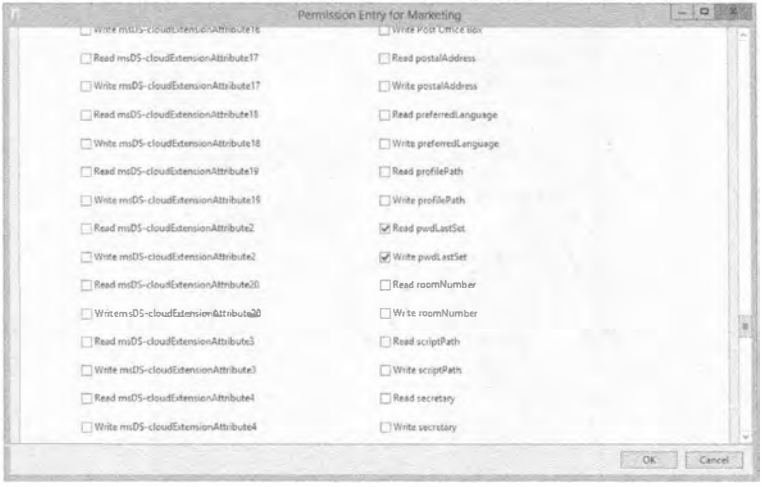


Рис. 9.46. Специальные возможности группы `MktPswAdm`

7. Возвратитесь в диалоговое окно дополнительных настроек безопасности и щелкните на кнопке Edit при выделенной второй записи для группы `MkPswAdm`. Откроется диалоговое окно, представленное на рис. 9.47.

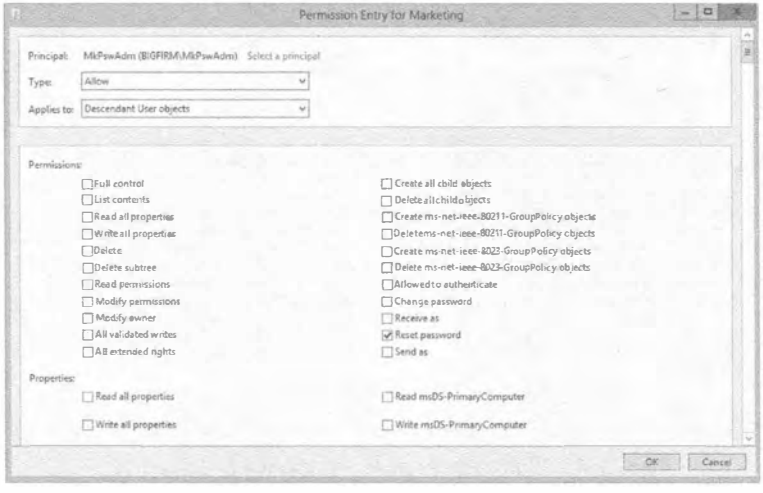


Рис. 9.47. Выдача разрешения на сброс паролей

Как видно на рис. 9.47, доступно *огромное* количество разрешений, которые могут быть выданы отдельной группе для управления организационной единицей. Верите или нет, но вы можете устанавливать более чем 10 000 отдельных разрешений всего лишь для одной организационной единицы. Причем подсчитаны только разрешения Allow (Разрешить) — если учесть также и Deny (Запретить), то указанное число удвоится.

Где вы можете использовать это? Итак, вы предоставили группе `MkPswAdm` возможность изменять пароли, но не устранили ее из групп, которые первоначально

имели ее — члены Domain Admins, Enterprise Admins и тому подобных групп по-прежнему могут сбрасывать пароли. Это не является плохой идеей, но если вы действительно *столкнетесь* со сценарием, так сказать, "феодальных поместий", где сотрудники отдела маркетинга желают иметь уверенность в том, что только они могут администрировать свои учетные записи, то должны будете сначала делегировать задачи управления организационной единицей Marketing определенной группе, а затем перейти на вкладку Security и отключить эту возможность для других администраторов.

Выяснение установленных делегирований, или отмена делегирования

Настало время для не очень хороших и совсем плохих новостей.

Предположим, что вы не являетесь администратором, который настраивал среду Active Directory. Наоборот, вы — *второй* по счету администратор, и вас наняли на работу, чтобы почистить "авгиевы конюшни", оставшиеся после *первого* администратора. Вы знаете такой сорт администраторов; они сродни "сумасшедшим ученым" — парни, щелкающие на чем попало внутри инструментов администрирования до тех пор, пока проблема не будет решена... как они думают. А как насчет *документирования*? Ха, настоящие администраторы никогда не документируют; у них никогда нет времени на документирование. В конце концов, эту сеть было трудно проектировать, так ее должно быть трудно и понимать!

Итак, вам интересно, что же этот парень натворил. Как он изменил среду AD компании по сравнению со стандартной средой AD, которая получается сразу после запуска утилиты DCPromo? На этот вопрос сложно ответить. Разумеется, созданные им организационные единицы вполне очевидны — просто загляните в Active Directory Users and Computers и увидите там новые папки. Но какие делегирования он создал?

А теперь не очень хорошая новость. К сожалению, не существует программы, которую можно было бы запустить, и она бы сравнила стандартную структуру AD и делегирования с текущей структурой AD и делегированиями, выдав отчет в стиле "вот то, что было изменено". Учитывая это ограничение, мы совершенно искренне советуем: всегда документируйте делегирования. *Всегда.* Попытайтесь контролировать, кто может устанавливать делегирование, и проясните, что делегирование разрешено делать только умеренно. Почему же тогда мы называли эту новость о сравнении лишь *не очень хорошей*, а не *плохой*? Причина в том, что есть небольшой инструмент, имеющий название dsacls.exe. Этот инструмент, входящий в состав основных утилит командной строки Windows Server 2012 R2, предоставляет детализированные листинги со списками ACL (порция acls названия) службы каталогов (порция ds названия).

Для запуска инструмента dsacls.exe вы должны перейти в окно командной строки.

1. Выберите в меню Start (Пуск) пункт Run (Выполнить).
2. В появившемся диалоговом окне введите **cmd**; откроется окно командной строки.

3. В окне командной строки введите **dsacls**, чтобы получить полный спектр помощи, предлагаемой этим инструментом.

   Как указано в справке, инструмент требует ввода пути к организационной единице, которую вы хотите просмотреть, с применением официального синтаксиса LDAP. В данном примере путь будет выглядеть подобно `ou=marketing, dc=bigfirm, dc=com`.

   Вы можете просто ввести **dsacls ou=marketing,dc=bigfirm,dc=com**. Это приведет к выводу информации в окне командной строки, что не очень удобно для проведения анализа.

4. Таким образом, направьте вывод в файл, используя следующий синтаксис:

```
dsacls ou=marketing,dc=bigfirm,dc=com > c:\marketing_OU_delegation.txt
```

Открыв файл `marketing_OU_delegation.txt`, вы увидите результат, похожий на показанный на рис. 9.48.

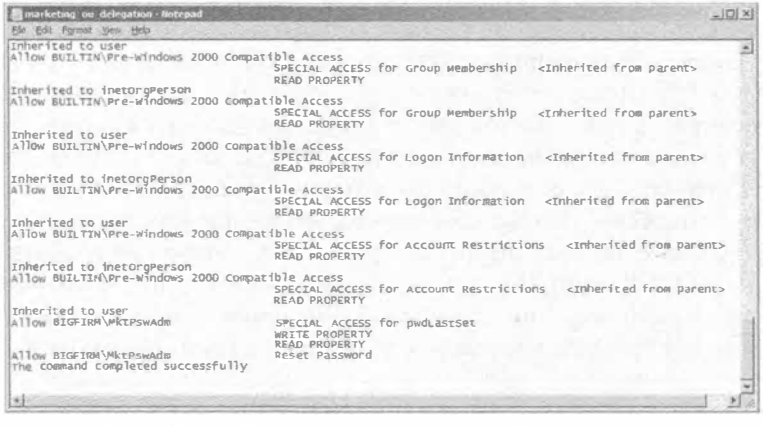


Рис. 9.48. Выдача разрешения на сброс паролей

Осталась по-настоящему плохая новость. Мастер Delegation of Control Wizard — удобный небольшой инструмент, но он является мастером только *делегирования*, но не *отмены* делегирования. Если вы хотите отозвать у группы `MkPswAdm` возможность изменения паролей учетных записей в отделе маркетинга, понадобится перейти на вкладку Security, найти ссылки на `MkPswAdm` и удалить их. Мы предупреждаем, что если вы хотите сохранить одни делегирования и удалить другие, вам придется вручную определить, какие из них соответствуют делегируемой задаче, которую вы конфигурируете.

Резюме

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, хра-

нящиеся 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)

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`.

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?

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.

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

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.

Глава 10

Службы федерации Active Directory

На протяжении многих лет управление доменами в Active Directory постоянно упрощалось для администраторов. Мы можем гораздо проще открывать совместное использование и подключаться к множеству приложений и организаций в защищенной манере. Одной из великолепных служб, предлагаемых семейством Windows Server со времен Windows Server 2003 R2, являются службы федерации Active Directory (Active Directory Federation Services — AD FS). Службы AD FS представляют собой разработанный в Microsoft программный компонент, который может быть установлен в операционных системах Windows Server для предоставления пользователям возможностей единого входа (single sign-on — SSO) в приложения и службы через границы, ранее не доступные для учетной записи с единым входом. Применяя модель авторизации доступа на основе утверждений, службы AD FS выдают сущности маркер безопасности, что позволяет пересекать границы организации, поддерживая при этом защиту приложений. Такая технология предоставляет пользователям свободу пересечения множества лесов, и даже аутентификации в облачных приложениях и на веб-сайтах, используя для входа куда угодно единственную доверенную учетную запись.

В Windows Server 2012 R2 возможности предыдущей версии AD FS задействованы для связи или объединения в федерацию множества лесов AD, и эта функциональность расширена возможностью объединения двух и более систем служб доменов Active Directory (Active Directory Domain Services — AD DS). Новейшая версия, AD FS 3.0, автоматически включена в эту редакцию сервера, позволяя управлять удостоверениями входа на множестве платформ, в том числе в средах, отличных от Microsoft. Такое дополнительное преимущество позволяет организациям с несколькими дочерними подразделениями, имеющими собственные среды Active Directory, совместно использовать и обмениваться между собой каталожной информацией безопасным образом. Мы можем распространить эту возможность даже более широко, предоставляя доступ к облачным службам и позволив пользователю SSO применять

единственный вход во множество служб и приложений, которые находятся за пределами корпоративной сети. Как вы можете предположить, управление всеми упомянутыми удостоверениями и паролями с поддержанием синхронизации между более крупными областями каталогов может оказаться трудным. К счастью, в Microsoft продолжают обеспечивать нас великолепными инструментами синхронизации каталогов наподобие диспетчера удостоверений Forefront (Forefront Identity Manager — FIM). Диспетчер FIM позволяет организациям синхронизировать информацию об удостоверениях между множеством разнообразных гетерогенных каталожных хранилищ. Службы AD FS и диспетчер FIM работают рука об руку, чтобы предложить пользователям и администраторам соответствующую функциональность и простоту использования, предоставляя доступ SSO к ресурсам во многих средах по всему миру.

В этой главе мы проведем глубокие исследования работы AD FS. Вы изучите следующие темы:

- установка роли AD FS на сервере;
- конфигурирование первого сервера федерации внутри фермы серверов;
- настройка мониторинга производительности AD FS.

Ключевые компоненты AD FS и принятая терминология

Прежде чем мы приступим к построению реализации AD FS, неплохо пройтись по ключевым компонентам и терминам, которые будут применяться повсеместно в данной главе. В AD FS используется терминология из нескольких технологий, включая информационные службы Интернета (Internet Information Services — IIS), службы домена Active Directory (Active Directory Domain Services — AD DS), службы сертификатов Active Directory (Active Directory Certificate Services — AD CS), службы облегченного доступа к каталогу Active Directory (Active Directory Lightweight Directory Services — AD LDS), а также веб-службы (Web Services). Ниже приведен список терминов и определений, применяемых в этой главе, который будет способствовать лучшему пониманию AD FS.

Распространенные термины и компоненты AD FS

Далее представлены ключевые компоненты и термины AD FS.

- **Партнер учетной записи (account partner).** Партнер учетной записи — это организация, выдающая маркеры безопасности, которые используются учетными записями пользователей для доступа к ресурсам, находящимся в среде партнера ресурса. Партнер учетной записи отвечает за хранение и аутентификацию учетных записей пользователей, создание утверждения пользователя и упаковку утверждений в маркеры безопасности, применяемые партнером ресурса во время аутентификации для своих приложений и служб. Партнеры учетных записей работают совместно в рамках доверительного отношения федерации, чтобы предоставить возможность доступа SSO к нужным ресурсам.
- **База данных конфигурации AD FS (AD FS configuration database).** База данных конфигурации AD FS используется для хранения всех конфигурационных данных, которые представляют одиночный экземпляр AD FS или службу федерации.

База данных конфигурации AD FS предусмотрена для каждой отдельной фермы серверов федерации. Службы AD FS предоставляют возможность хранения данных во внутренней базе данных Windows (Windows Internal Database — WID) или в базе данных Microsoft SQL Server. Имейте в виду, что в одном экземпляре AD FS можно запускать либо WID, либо SQL, но не то и другое вместе. Вы должны обдумать, какая топология базы данных будет лучше работать в вашем развертывании. SQL отличается высокой масштабируемостью, тогда как WID ограничивается пятью серверами WID на ферму серверов федерации.

- **Хранилище атрибутов (attribute store).** Хранилище атрибутов лучше всего определить как базу данных или службу каталогов, которая содержит атрибуты, описывающие клиентов. Эти атрибуты можно применять для выдачи утверждений от клиентов. Службы AD FS поддерживают несколько разных возможностей для хранилища атрибутов. В качестве хранилища атрибутов главным образом используются Active Directory и SQL Server. Можно построить и работать со специальными хранилищами атрибутов, но при этом требуется дополнительное конфигурирование вроде создания специальной строки подключения.
- **Утверждение (claim).** Утверждение — это заявление, которое один субъект делает о себе или о другом объекте. Например, заявление может касаться имени, адреса электронной почты, группы, полномочия или возможности. Утверждения выдаются и потребляются между партнерами учетных записей и ресурсов для предоставления учетным записям пользователей доступа SSO, обеспечивая свободное перемещение между организациями или службами. Такие утверждения применяются для целей входной аутентификации и авторизации в приложении, совместно используемом поставщиком и потребителем. Утверждения идентифицируют для учетной записи пользователя группу атрибутов, таких как имя или роль этого пользователя. Партнер учетной записи упаковывает утверждения в маркеры безопасности и затем отправляет эти маркеры партнеру ресурса, который запрашивает аутентификацию пользователя в приложениях и службах, размещенных партнером ресурса.
- **Метаданные федерации (federation metadata).** Метаданные федерации можно охарактеризовать как формат данных, который используется для передачи данных конфигурации между проверяющей стороной и поставщиком утверждений. Метаданные федерации могут применяться для создания доверительного отношения между поставщиком утверждений и проверяющей стороной. Доверительные отношения федерации требуются учетным записям пользователей для безопасного перемещения между организациями, приложениями и службами. Пример создания доверительного отношения будет приведен далее в этой главе.
- **Сервер федерации (federation server).** Сервер федерации — это сервер, который был построен и сконфигурирован для службы роли AD FS. Сервер федерации выступает как часть службы федерации, которая используется для перенаправления запросов аутентификации и размещения службы маркеров безопасности для учетных записей пользователей между доверенными организациями и службами. Работа сервера федерации заключается в создании и выдаче маркеров безопасности, применяемых учетными записями пользователей для аутентификации внутри служб федерации.

- **Ферма серверов федерации (federation server farm).** Когда вы кластеризуете множество серверов федерации, чтобы они действовали как единственная службы федерации в одной сети с балансировкой нагрузки, такой кластер серверов называется фермой серверов федерации. Эта ферма может состоять из многих устройств, таких как серверы федерации, прокси и веб-агенты AD FS.

- **Прокси-сервер федерации (federation server proxy).** Прокси-сервер федерации — это сервер федерации, который вынесен за пределы корпоративной сети, чтобы предоставлять промежуточную службу прокси между открыто недоступной корпоративной сетью, защищенной брандмауэром, и клиентами из Интернета. Для того чтобы разрешить удаленный доступ к облачной службе, например, со смартфона, домашнего компьютера либо Интернет-киоска, понадобится развернуть прокси-сервер федерации, который будет действовать в качестве посредника между Интернетом и корпоративной сетью.

- **Балансировщик сетевой нагрузки (network load balancer — NLB).** При наличии нескольких серверов федерации, функционирующих вместе внутри фермы таких серверов, существует требование AD FS по балансировке нагрузки между серверами с использованием какого-нибудь вида балансировщика сетевой нагрузки. Балансировщиком NLB может быть фрагмент программного обеспечения, такой как встроенная в Windows Server функциональность NLB. Добавление этого очень важного фрагмента дает огромные преимущества. В дополнение к балансировке нагрузки в среде AD FS наличие множества серверов федерации с балансировщиком NLB между ними обеспечит для инфраструктуры AD FS устойчивость к отказам и высокую готовность.

- **Проверяющая сторона (relying party).** Проверяющая сторона — это любая организация, приложение или служба, потребляющая утверждения, которые выдаются партнером учетной записи. Хорошим примером проверяющей стороны является партнерская организация или облачная служба, подобная Office 365.

- **Доверительное отношение для проверяющей стороны (relying party trust).** Доверительное отношение для проверяющей стороны создается между двумя службами федерации. Будучи очень похожим на доверительное отношение леса Active Directory, доверительное отношение для проверяющей стороны создает безопасный туннель, который предоставляет учетным записям пользователей возможность защищенным образом проходить аутентификацию в приложениях и службах между сущностями. Обратите внимание, что доверительные отношения леса Active Directory и доверительные отношения федерации работают независимо друг от друга.

- **Партнер ресурса (resource partner).** Партнер ресурса — это другая организационная часть доверительного отношения федерации с партнером учетной записи. Работа партнера ресурса заключается в размещении приложений и служб, к которым пользователи партнера учетной записи хотят получать доступ с применением технологии SSO. Партнер ресурса просматривает маркеры безопасности, отправленные партнером учетной записи, и решает, предоставлять ли учетной записи пользователя доступ к своим приложениям и службам.

Хотя существует много дополнительных фрагментов, которые образуют полный спектр терминологии AD FS, описанные выше термины помогут обрести общее понимание лежащей в основе инфраструктуры.

Давайте также уделим время исследованиям четырех типов сертификатов, применяемых в инфраструктуре AD FS. Такие доверенные сертификаты требуются службами AD FS; они рассматриваются в следующем разделе.

Сертификаты AD FS

Сертификаты являются фундаментальными строительными блоками, позволяющими AD FS функционировать должным образом. Каждый клиент, который нуждается в возможностях SSO, должен иметь и быть способным принимать эти сертификаты безопасности. Сертификаты создаются и выдаются IIS и AD FS, чтобы поддерживать доверительные отношения. Эти сертификаты можно использовать для защищенного взаимодействия со всеми объектами внутри среды AD FS. Без таких доверенных сертификатов реализовать AD FS в качестве решения SSO не удастся. Позже в этой главе мы создадим и добавим сертификаты с применением IIS и AD FS, но сначала давайте посмотрим, как ими пользоваться. Ниже перечислены требования к серверу федерации.

- **Сертификат для подписи маркера (token-signing certificate).** Сертификат для подписи маркера — это защищенный сертификат X.509, который используется сервером федерации для цифровой подписи маркеров безопасности, создаваемых и распространяемых по инфраструктуре AD FS. Вы обязаны применять сертификат для подписи маркера на сервере федерации для AD FS, чтобы данный сервер нормально функционировал. Именно этот сертификат из обсуждаемых здесь четырех службы AD FS фактически используют для подписания маркеров. Сертификатов для подписи маркера может быть несколько. На самом деле рекомендуется иметь их множество, причем с повторяющимся циклом, чтобы в случае, если активный сертификат устаревает или подвергается компрометации, на подхвате окажется резервный сертификат.
- **Сертификат для шифрования маркера (token-decryption certificate).** Сертификат для шифрования маркера применяется рука об руку с сертификатом для подписи маркера. Когда партнер учетной записи выдает маркер безопасности для учетной записи пользователя, чтобы он мог получить доступ к приложению или службе на стороне партнера ресурса, сервер федерации в среде партнера ресурса должен иметь возможность расшифровать этот маркер безопасности и удостовериться в том, что он не был изменен или подделан.
- **Сертификат уровня защищенных сокетов (Secure Sockets Layer certificate).** Сертификат Secure Sockets Layer (SSL) предназначен для использования с трафиком между прокси-серверами федерации и клиентами из Интернета. Для того чтобы веб-служба или клиент безопасно взаимодействовали с прокси-сервером федерации, клиент должен иметь возможность принятия сертификата SSL, выданного прокси-сервером. Заметили здесь закономерность? Весь трафик AD FS защищается шифрованием и доверенными сертификатами. Однако подумайте о следующем: теперь, когда вы выдали большие права доступа учетной записи, для поддержания ее безопасности придется проводить больший объем проверок и мер по уравновешиванию.

- **Сертификат для взаимодействия со службами (service communication certificate).** Сертификат для взаимодействия со службами предлагает ту же самую функциональность, что и сертификат SSL, но с дополнительным преимуществом. Вдобавок к защите трафика между веб-клиентами и прокси-серверами федерации этот сертификат защищает коммуникации между клиентами и приложениями Windows Communication Foundation (WCF). Поскольку на базе инфраструктуры WCF построено довольно много веб-служб и клиентских приложений для веб-служб, по умолчанию этот сертификат применяется сервером федерации для сертификата SSL в IIS.

Теперь, когда вы имеете общее понимание того, какие сертификаты требуются службами AD FS, и каким образом они используются, давайте обсудим ряд рекомендуемых приемов их применения. Несмотря на то что в испытательной или тестовой среде допустимо использовать самозаверяющие сертификаты, все производственные сертификаты должны быть подписаны доверенным центром сертификации (certificate authority — CA). Вы можете пользоваться доверенным CA, созданным с помощью служб AD CS, или доверенным сторонним CA наподобие `GoDaddy.com`. Это помогает обеспечить дополнительный уровень безопасности. Сертификаты AD FS установлены на корневом уровне серверов федерации, так что чем выше защита, тем лучше. Вы вовсе не хотите получить неавторизованный доступ ко всем ресурсам федерации. Сделайте установку и подготовку всех сертификатов на серверах федерации частью фаз планирования, установки и развертывания служб AD FS.

Планирование, установка и конфигурирование инфраструктуры AD FS

Службы AD FS являются крупным и всеохватывающим дополнением развертывания любой корпоративной инфраструктуры. Они полностью изменяют методику доступа пользователей к веб-сайтам, службам и приложениям по всему миру. Службы AD FS предоставляют фантастическую возможность безопасно обращаться к корпоративным, партнерским и облачным ресурсам, используя функции SSO. Применяя единственную учетную запись пользователя, вы можете пересекать многочисленные организационные границы. Это может оказаться гигантским облегчением для администраторов и пользователей, т.к. устраняются иногда выглядящие бесконечными списки различных учетных записей и паролей, которые используются ежедневно. Далее мы спланируем, установим и сконфигурируем инфраструктуру AD FS.

Планирование развертывания AD FS

На планирование развертывания AD FS тратится немалое время. При наличии доступных ресурсов было бы хорошо построить испытательную среду для имитированного развертывания. Поскольку службы AD FS поддерживаются такими платформами виртуализации, как Hyper-V и VMware, вы могли бы полностью виртуализировать тестовую реализацию AD FS. Та же самая концепция остается справедливой и в производственной среде. В настоящее время нет никакой возможности отката развертывания AD FS SSO после того, как оно было сконфигурировано, в результате чего пользователям стала доступна федерация. По этой причине мы настоятельно рекомендуем запустить пилотный проект по тестированию возможностей

SSO, прежде чем включать их. Применяйте набор пользователей производственной среды и удостоверьтесь, что эта группа всесторонне тестирует возможности SSO из различных источников, таких как компьютер, присоединенный к домену, домашний компьютер, партнерская организация и смартфон. После того как вы убедитесь, что пользователи чувствуют себя комфортно с возможностями SSO, вы можете безопасно завершить построение федерации в производственной среде.

Одним из первых аспектов, которые следует принять во внимание при планировании развертывания AD FS, является то, каким образом организация извлечет максимальные преимущества от этой технологии. Будет ли пользователям необходим доступ к облачным службам вроде Office 365 для обмена электронной почтой на ежедневной основе? Содержит ли ваша организация несколько лесов с общими ресурсами, которые требуют от пользователей многократного входа? Службы AD FS делают сценарии такого типа намного более гладкими, объединяя удостоверения пользователя. Обычно вы должны были останавливаться в каждой точке аутентификации и вспоминать один из многочисленных паролей, удерживаемых в голове. Используя AD FS, вы можете входить на свой рабочий стол, загружать данные в хранилище партнерской организации и получать доступ ко многим облачным приложениям, не совершая процедуру входа больше одного раза.

Важный шаг при построении надежной инфраструктуры AD FS заключается в планировании развертывания. Вы должны рассмотреть много разных аспектов, вроде того, сколько понадобится серверов, и где они будут размещены, требуется ли строить ферму серверов или достаточно одного автономного сервера, какой вид базы данных конфигурации будет применяться — WID или SQL, и какие другие службы понадобятся, к примеру, балансировка сетевой нагрузки или прокси-серверы федерации. Нарисуйте разные топологии развертывания на большой доске, чтобы посмотреть, каким требованиям по развертыванию лучше всего удовлетворяет ваша организация. Реализуйте и протестируйте различные развертывания в испытательной среде. Обдумайте, какие границы придется пересекать пользователям. Будут ли вовлечены в развертывание партнерские организации или облачные службы? В большинстве типов развертывания отдается предпочтение идее предоставления доступа SSO к облачным службам наподобие Microsoft Office 365 или к партнерским организациям, таким как службы каталогов или хранилища данных в дочерней компании. Многие современные корпорации предлагают свою функциональность электронной почты и Exchange через облачную веб-службу. Давайте рассмотрим несколько рекомендованных соображений относительно топологии при развертывании AD FS с возможностями SSO для облачной службы, подобной Office 365. При планировании предоставления пользователям доступа SSO к облачному приложению в среде с 60 000 и менее пользователей рекомендуется развертывать ферму серверов AD FS с базой данных конфигурации WID.

Сколько серверов AD FS должно быть развернуто?

Приведенная далее информация поможет в оценке необходимого количества серверов федерации AD FS и прокси-серверов федерации при развертывании фермы серверов на основе того, сколько пользователей будут применять доступ SSO к облачным службам и партнерским организациям.

- **До 1000 пользователей.** В небольшой среде при необходимости можно обойтись использованием контроллеров домена для размещения роли AD FS. При

наличии доступных ресурсов по-прежнему имеет смысл как можно лучше изолировать роли инфраструктуры и службы за счет построения выделенных серверов для AD FS, даже если это не является требованием. Когда количество пользователей не превышает 1000, строить выделенные серверы федерации или прокси-серверы федерации не обязательно. Тем не менее, вы по-прежнему должны использовать балансировщик NLB между двумя контроллерами домена, которые действуют в качестве двух серверов федерации внутри фермы серверов федерации.

- **От 1000 до 15 000 пользователей.** Если в среде имеется от 1000 до 15 000 пользователей, вам придется построить, по меньшей мере, два выделенных сервера федерации с внутренней стороны корпоративного брандмауэра, два прокси-сервера федерации с внешней стороны корпоративного брандмауэра (в демилитаризованной зоне (DMZ) или в экстрасети) и балансировщик NLB, сконфигурированный для каждой пары в целях балансировки нагрузки.
- **От 15 000 до 60 000 пользователей.** В случае крупной организации необходимо развернуть от трех до пяти выделенных серверов федерации и минимум два прокси-сервера федерации. Серверы федерации развертываются по принципу один дополнительный выделенный сервер на 15 000 пользователей. В настоящее время максимальное количество серверов федерации составляет пять, или 60 000 пользователей. Для действительно больших предприятий вполне возможно развертывание множества ферм с максимальным числом серверов федерации для предоставления функций SSO пользователям по всему миру.

Какая база данных конфигурации должна использоваться для развертывания — WID или SQL?

Традиционно для развертывания AD FS с доступом SSO вы будете применять базу данных конфигурации WID. Но в определенный момент, когда среда становится слишком большой, вы больше не сможете пользоваться WID. База данных WID ограничена пятью серверами федерации на ферму. В таком случае для хранения конфигурационной информации требуется база данных SQL Server. Если вы имеете дело с более чем 60 000 пользователей, которым необходим доступ SSO, то должны с самого начала планировать развертывание SQL Server для базы данных конфигурации. Вариант с SQL Server для AD FS привносит три дополнительных преимущества по сравнению с WID:

- поддерживается географическая балансировка нагрузки, помогающая справляться с высоким трафиком на основе местоположения;
- администраторы могут с выгодой использовать средства высокой готовности, предоставляемые SQL Server;
- ограничение в пять серверов федерации на ферму в SQL Server отсутствует.

Какой тип требований к сети ожидать?

Надлежащая организация сети крайне важна для успешного развертывания AD FS. Чтобы службы AD FS функционировали так, как ожидалось, должны существовать подключения TCP/IP между клиентом, контроллерами домена, серверами федерации, веб-агентом AD FS и прокси-серверами федерации. Еще одну важную

роль в работе AD FS играет DNS. В качестве части реализации вам, скорее всего, понадобится добавить записи A для дополнительных серверов и кластеров, которые развертываются во время реализации. За детальными инструкциями по использованию и конфигурированию DNS обращайтесь в главу 6.

Когда вы применяете балансировщики сетевой нагрузки или кластеры как внутри корпоративной сети, так и снаружи, например, в DMZ, серверы DNS преобразуют DNS-имя кластера в IP-адрес кластера для сконфигурированного кластера NLB. Скажем, `bf1.test.com` преобразуется в 172.100.1.3. Имейте в виду, что балансировщик сетевой нагрузки также требуется для правильного развертывания производственной среды. Балансировщиком NLB может быть фрагмент аппаратного или программного обеспечения, который предоставляет функции балансировки нагрузки, высокой готовности и устойчивости к отказам среди множества устройств и машин в сети.

Много ли браузеров поддерживают доступ AD FS SSO к облачной службе Microsoft?

Вы можете быть не в состоянии подписаться на облачную службу, используя встроенную аутентификацию Windows, изнутри корпоративной сети с помощью любого браузера, отличного от определенных версий Internet Explorer, если на компьютерах установлены исправления Extended Protection for Authentication (Расширенная защита для аутентификации). По умолчанию клиентские операционные системы Windows предварительно сконфигурированы с Extended Protection for Authentication. Если для подписки на облачную службу вы хотите применять другие браузеры наподобие Chrome, Safari и Firefox, может потребоваться удалить все исправления Extended Protection for Authentication из локальной машины. Такое решение не рекомендуется Microsoft по соображениям безопасности, но вы можете сделать это, чтобы работать со своим любимым браузером. Дополнительные сведения по требованиям AD FS к браузерам доступны по ссылке `http://technet.microsoft.com/ru-ru/library/ff678034.aspx`.

> **Cookie-наборы**
>
> Ключевым требованием к клиентским компьютерам для использования возможностей SSO является включение cookie-наборов. Чтобы поддерживался доступ SSO, службы AD FS создают сеансовые постоянные cookie-наборы, которые должны храниться локально на каждом клиенте. Имейте в виду, что если клиентский компьютер не сконфигурирован на прием cookie-наборов аутентификации HTTPS, то службы AD FS не смогут корректно функционировать.

Установка ролей и компонентов AD FS с использованием диспетчера серверов

Службы AD FS 3.0 в Windows Server 2012 R2 используют те же самые великолепные компоненты, которые были предоставлены в версии 2.1, одновременно предлагая новую и измененную функциональность, которая делает их сильнее и проще предшествующих версий. До выхода Windows Server 2012 программное обеспечение AD FS необходимо было загружать и устанавливать, прежде чем становилось возможным развертывание инфраструктуры сервера. Теперь с помощью диспетчера серверов можно легко добавлять роли и компоненты AD FS прямо на сервере.

Еще одним полезным дополнением в Windows Server 2012 R2 является то, что службы AD FS можно также использовать вместе с AD DS для предоставления расширенной функциональности. Службы AD FS могут потреблять утверждения пользователей и устройств AD DS, которые включены в билеты Kerberos вследствие аутентификации домена. Это всерьез расширяет возможности AD FS. В довершение всего разработчики из Microsoft не забыли позаботиться о службах AD FS и в командной строке, предложив новые и усовершенствованные командлеты PowerShell для автоматизации и администрирования AD FS. Командлеты PowerShell для AD FS рассматриваются позже в этой главе.

Давайте установим роль AD FS на первом сервере федерации с применением диспетчера серверов.

1. Запустите диспетчер серверов, щелкнув на значке Server Manager (Диспетчер серверов) в панели задач или на плитке Server Manager на экране Start (Пуск), как показано на рис. 10.1.

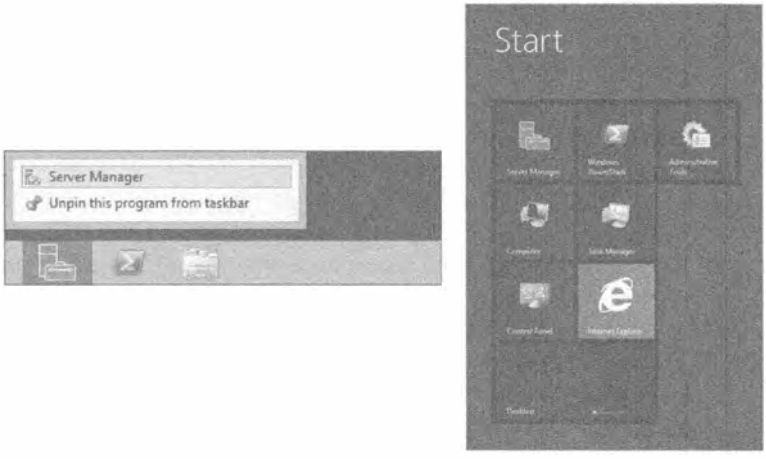


Рис. 10.1. Запуск диспетчера серверов из панели задач или экрана Start

2. На вкладке Dashboard (Управляющая панель) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты) для запуска мастера добавления ролей и компонентов (Add Roles and Features Wizard), как показано на рис. 10.2.
3. После открытия диалогового окна мастера выполните перечисленные ниже действия.
4. Просмотрите информацию на экране Before you begin (Прежде чем начать).
5. Оставьте выбранным переключатель Role-based or feature-based installation (Установка на основе ролей или на основе компонентов).
6. Выберите сервер, на котором необходимо установить новую роль и компоненты.
7. Щелкните на кнопке Next (Далее), чтобы перейти на экран Select server roles (Выбор серверных ролей).
8. На экране Select server roles отметьте флажок Active Directory Federation Services (Службы федерации Active Directory), как показано на рис. 10.3.

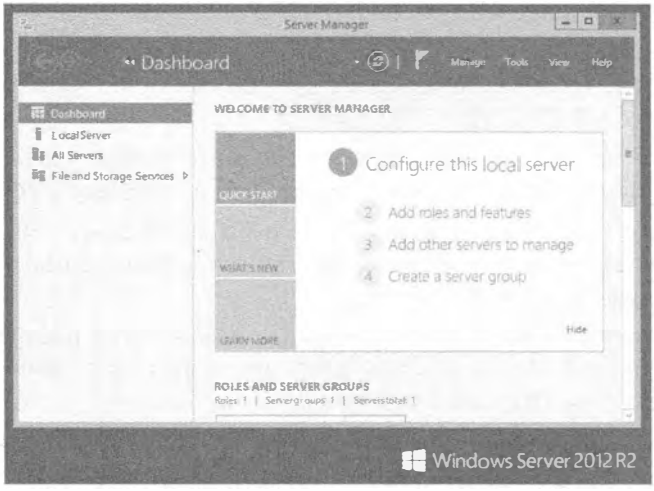


Рис. 10.2. Запуск мастера Add Roles and Features Wizard

Рис. 10.3. Выбор серверной роли AD FS

Если компоненты IIS, Windows Internal Database и Active Directory Certificate Services пока еще не доступны, добавьте их в этом мастере. Все можно сделать за один раз.

9. Щелкните на кнопке Next, чтобы перейти на экран Select features (Выбор компонентов).

   Вы получаете здесь возможность добавить любые дополнительные компоненты, в которых нуждаетесь.

10. Сделайте выбор и для продолжения щелкните на кнопке Next.

    На экране AD FS предоставляется описание технологии и несколько важных моментов, которые следует иметь в виду при установке. Обратите внимание, что роли Federation Service (Служба федерации) и Federation Service Proxy (Прокси службы федерации) не могут сосуществовать на одном сервере, и для успешной установки роли машина должна быть присоединена к домену.

11. Щелкните на кнопке Next.

    На экране Role Services (Службы роли) можно установить дополнительные службы роли, которые понадобятся для запуска полнофункциональной инфраструктуры AD FS.

12. Тщательно изучите и выберите все дополнительные службы роли кроме Federation Service Proxy, памятуя о замечании из предыдущего шага.

13. Пересмотрите сведения на экране Confirm Installation Selections (Подтверждение выбранных настроек для установки), чтобы удостовериться в том, что ничего не было упущено из виду.

    Мастер отображает все выбранные роли, компоненты и инструменты, которые их поддерживают. На этом экране доступно несколько дополнительных опций, которые могут оказаться полезными.

14. Автоматический перезапуск целевого сервера, если это требуется.

15. Экспорт настроек конфигурации.

16. Указание альтернативного исходного пути.

17. Щелкните на кнопке Install (Установить).

    Последним экраном мастера является Results (Результаты). Здесь будет отображаться ход процесса установки (рис. 10.4). Если вы решите закрыть диалоговое окно мастера, задача установки будет выполняться в фоновом режиме. Просмотреть связанные с этой задачей детали можно в области Notifications (Уведомления) панели задач.

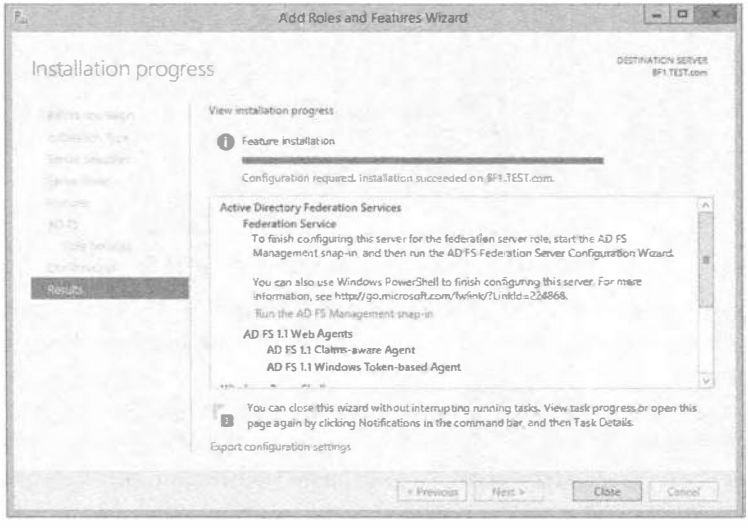


Рис. 10.4. Просмотр экрана Results и установка ролей и компонентов AD FS

18. После успешного завершения установки перезагрузите сервер вручную или же, если на экране Confirm Installation Selections был выбран переключатель Restart Automatically (Перезапустить автоматически), то сервер при необходимости перезагрузится самостоятельно по завершении процесса установки.

Теперь можете воспользоваться флагом Notifications в диспетчере серверов, чтобы завершить задачу конфигурации постразвертывания (Post-deployment Configuration) служб AD FS на сервере. Но прежде чем заняться этим, следует уделить время созданию доверенного сертификата SSL. До запуска мастера конфигурации сервера AD FS этот доверенный сертификат должен быть в наличии, т.к. этого требует мастер, чтобы завершить конфигурирование AD FS.

Создание доверенного сертификата SSL с использованием IIS

Мы говорили о требованиях к сертификатам ранее в этой главе. Теперь вы увидите, как эти сертификаты создавать и использовать с помощью IIS. До полного развертывания и конфигурирования сервера федерации с применением мастера конфигурации сервера AD FS (AD FS Server Configuration Wizard) вы должны настроить новый сертификат SSL домена, представляющий имя службы федерации. Ниже перечислены шаги по созданию сертификата, требуемого для развертывания AD FS.

1. Запустите диспетчер серверов и выберите в меню Tools (Сервис) пункт Internet Information Services (IIS) (Информационные службы Интернета (IIS)).

   Откроется диалоговое окно IIS Manager (Диспетчер IIS), позволяя выбрать ваш сервер в левой панели.

2. Выделите узел сервера и в представлении возможностей (Features View) дважды щелкните на значке Server Certificates (Сертификаты сервера).

   В этом примере будет создаваться и использоваться самозаверяющий сертификат. Такой сертификат не должен применяться в производственной среде из-за потенциальных уязвимостей в плане безопасности.

3. В панели Actions (Действия) щелкните на ссылке Create Self-Signed Certificate (Создать самозаверяющий сертификат), чтобы запустить мастер.

4. Укажите дружественное имя для сертификата: **AD FS**.

   Здесь имеется также возможность выбрать хранилище сертификатов для помещения в него нового сертификата.

5. Выберите в раскрывающемся списке вариант Personal (Персональное) или Web Hosting (Размещенное в веб) и щелкните на кнопке OK.

После успешного завершения диалоговое окно IIS Manager должно выглядеть примерно так, как показано на рис. 10.5.

Использование мастера AD FS Server Configuration Wizard

Создав доверенный сертификат SSL, можно продолжить конфигурирование AD FS на сервере. В зависимости от плана топологии, которого вы придерживаетесь в производственной среде, могут потребоваться дополнительные сертификаты, такие как сертификаты для подписи маркера и верификации для клиентов. Вы всегда можете возвратиться и создать другие сертификаты, если они нужны, но сейчас мастер будет устанавливать оставшиеся необходимые сертификаты как часть процесса конфигурирования.

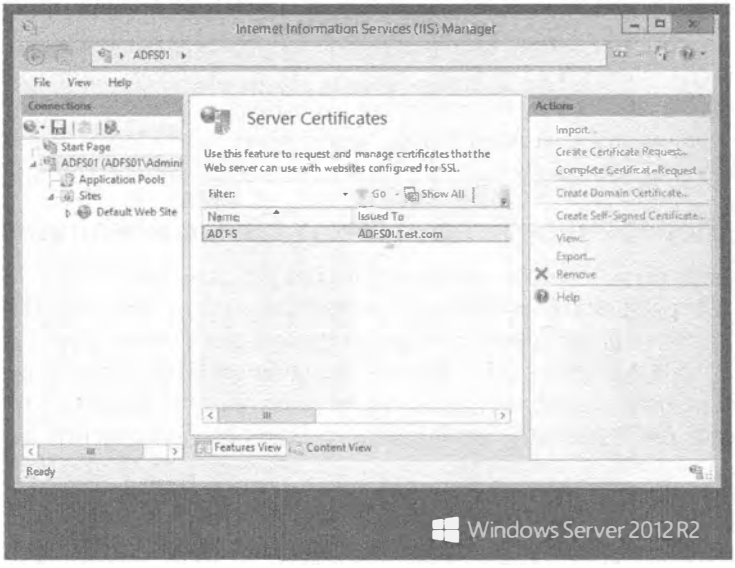


Рис. 10.5. Просмотр вновь созданного сертификата с помощью диспетчера IIS

Итак, продолжим конфигурирование AD FS на сервере.

1. В окне диспетчера серверов щелкните на флаге Notifications (Уведомления) и в открывшемся списке щелкните на пункте Configure the federation service on the server (Конфигурировать службу федерации на сервере).
2. Запустится мастер, который отобразит экран Welcome (Добро пожаловать), позволяя выбрать один из двух переключателей: Create the first federation server in a federation server farm (Создать первый сервер федерации в ферме серверов федерации) или Add a federation server to an existing federation service (Добавить сервер федерации в существующую службу федерации). Полезная особенность экрана Welcome заключается в том, что на нем имеется ссылка на все требуемые для AD FS ресурсы на тот случай, если по ходу дела вы пропустили какой-то шаг.
3. Поскольку это первый сервер AD FS, который вы устанавливаете, оставьте выбранным переключатель Create the first federation server in a federation server farm.
4. Щелкните на кнопке Next (Далее), чтобы перейти на экран Connect to AD DS (Подключение к AD DS). В качестве части процесса конфигурирования, службы AD FS будут регистрировать себя с помощью AD DS. Для продолжения вам потребуется ввести учетные данные администратора домена Active Directory.
5. После ввода учетных данных щелкните на кнопке Next, чтобы перейти на экран Specify Service Properties (Указание свойств службы). Здесь к службе федерации должен быть присоединен ваш доверенный сертификат SSL. Если вы создали SSL локально на сервере, то можете просто выбрать его в раскрывающемся списке. В противном случае щелкните на кнопке Import (Импортировать), чтобы получить сертификат из сетевого местоположения.

Вы заметите, что как только выберете нужный сертификат, поле Federation Service Name (Имя службы федерации) автоматически заполнится именем, которое указано в сертификате (рис. 10.6). Не переживайте особенно о синтаксисе имени в поле Federation Service Name либо имени сертификата SSL, поскольку в поле Federation Service Display Name (Отображаемое имя службы федерации) можно ввести дружественное имя, которое будет отображаться пользователю при входе. В большинстве случаев для отображаемого имени службы федерации применяется название компании.

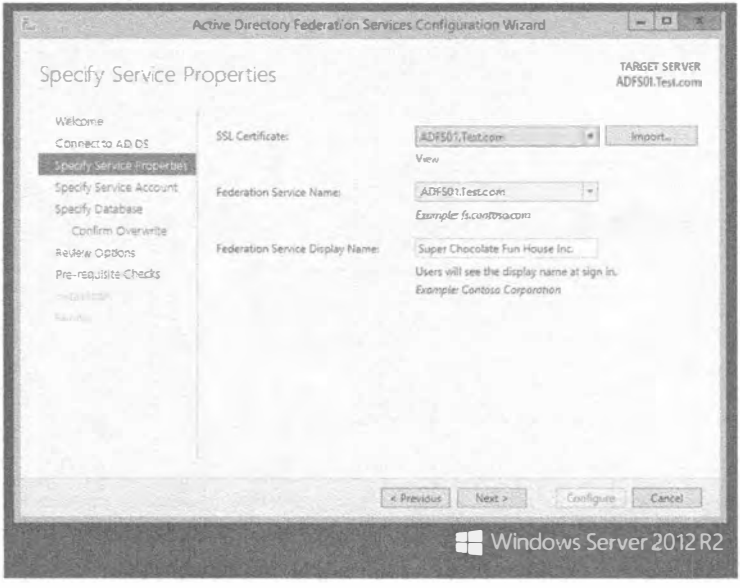


Рис. 10.6. Экран Specify Service Properties

6. Щелкните на кнопке Next, чтобы перейти на экран Specify Service Account (Указание учетной записи службы). На этом экране мастера конфигурации потребуется либо создать новую учетную запись для использования со службой федерации, либо выбрать существующую учетную запись службы из Active Directory. Рекомендуется иметь для всех служб отдельные учетные записи. Вряд ли вы захотите, чтобы от имени одной учетной записи запускалось много служб, т.к. блокировка или компрометация этой учетной записи повлияет сразу на несколько служб и приложений, а не только на какую-то одну. Поскольку мы впервые проходим через мастер конфигурации, создайте новую учетную запись, выделенную для AD FS.
7. Щелкните на кнопке Next для перехода на экран Specify Database (Указание базы данных). Как упоминалось ранее в этой главе, для хранения данных конфигурации службы AD FS могут использовать базу данных WID или SQL Server. В рассматриваемом примере мы будем применять WID. Если так случится, что вы когда-либо запустите мастер конфигурации на сервере, где уже были сконфигурированы службы AD FS, то может потребоваться перезаписать существующую базу данных. Мастер автоматически обнаруживает пре-

дыдущую установку и вам придется лишь отметить флажок Overwrite existing AD FS configuration database data (Перезаписать существующие данные в базе данных конфигурации AD FS) на дополнительном экране Confirm Overwrite (Подтверждение перезаписи), после чего продолжить работу в мастере обычным образом.

8. Щелкните на кнопке Next, чтобы перейти на экран Review Options (Пересмотр опций), показанный на рис. 10.7.

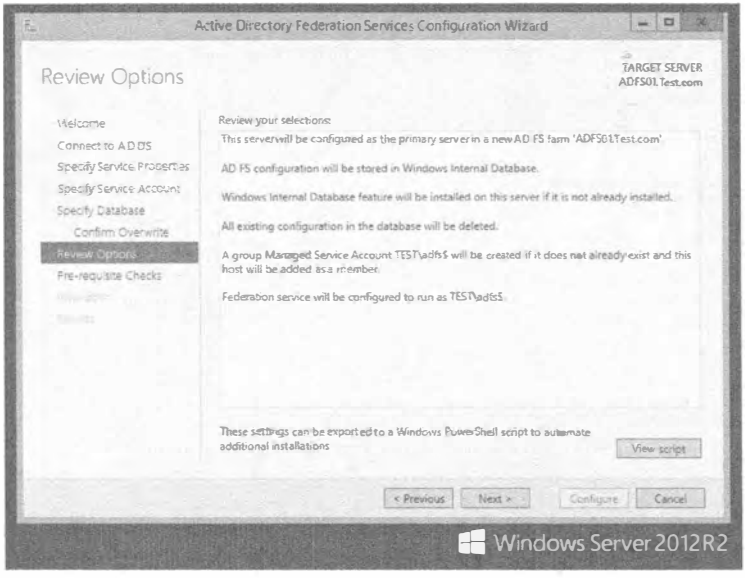


Рис. 10.7. Экран Review Options

9. Внимательно просмотрите предоставленную информацию и удостоверьтесь в том, что выбрано в точности то, что требуется. Здесь может понадобиться внесение каких-то изменений в опции конфигурации.

   Мастер конфигурации автоматически создаст дополнительные сертификаты для подписи и шифрования маркера, которые будут нужны для этого развертывания. Он также сконфигурирует базу данных WID на доступ с помощью учетной записи сетевой службы, предоставленной сервером. В дополнение к таким настройкам вход через браузер будет развернут в виртуальном каталоге под стандартным веб-сайтом в IIS.

10. Щелкните на кнопке Next для перехода на экран Pre-requisite Checks (Проверка предварительных условий). Это великолепное дополнение к мастеру, т.к. если вы по недосмотру что-то пропустили или в одном из полей указали некорректную информацию, то мастер конфигурации проверит все сведения на предмет ошибок или возможных конфликтов, которые могли возникнуть во время установки. В случае обнаружения ошибки вам придется исправить проблему, прежде чем можно будет завершить установку. Если до этого момента все шло должным образом, то экран мастера будет выглядеть подобным представленному на рис. 10.8.

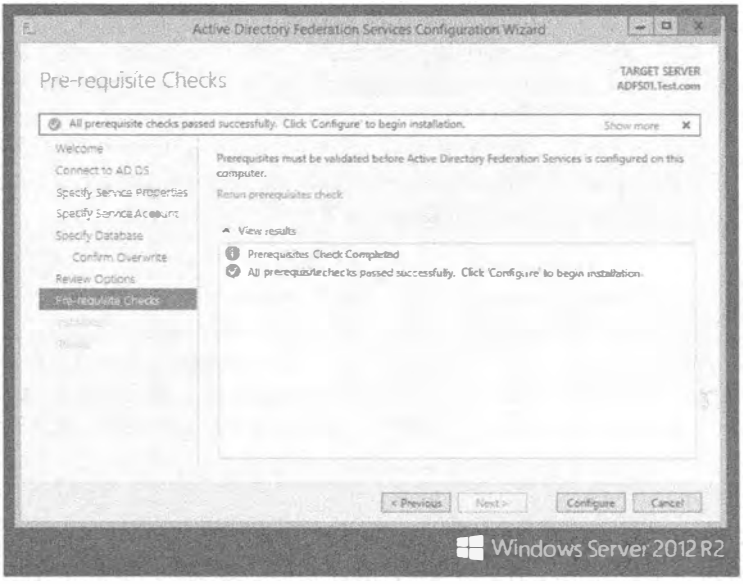


Рис. 10.8. Экран Pre-requisite Checks

11. Щелкните на кнопке Configure (Конфигурировать), чтобы запустить установку, которая может занять несколько минут. В конечном итоге отобразится сообщение об успешном завершении.

    В нашем примере пропущен компонент Deploy browser sign-in Web site (Развернуть веб-сайт для входа через браузер), поскольку веб-сайт был создан в предыдущем примере. На рис. 10.8 показан пример сообщения об успешном завершении.

12. Щелкните на кнопке Close (Закрыть) для завершения установки.

Использование Windows PowerShell для AD FS

Давайте кратко повторим, что было сделано до этого момента.

- Вы установили на своем сервере роли и компоненты AD FS.
- Вы создали и назначили все необходимые сертификаты.
- Вы сконфигурировали свой сервер для функционирования служб федерации AD FS.

Здесь следует отметить несколько моментов. Оснастка AD FS Management (Управление AD FS) должна быть установлена и зарегистрирована параллельно с командлетами Windows PowerShell, предназначенными для администрирования AD FS из командной строки. Если вы возвратитесь в оснастку AD FS Management, то увидите, что были добавлены дополнительные узлы конфигурации. Кроме того, вы заметите, что появилась возможность запуска нового мастера добавления доверительного отношения для проверяющей стороны (Add Relying Party Trust Wizard). Этот дополнительный шаг конфигурирования требуется для управления доступом SSO для приложений и служб. Мы добавим доверительное отношение для проверяющей стороны в следующем разделе.

Прежде чем мы перейдем к рассмотрению следующей порции установки, давайте взглянем на командлеты Windows PowerShell, которые доступны в Windows Server 2012 R2. Имея зарегистрированную оснастку, политику, разрешающую удаленный запуск, и открытое окно Windows PowerShell с правами администратора, введите команду `Get-Command *-ADFS*`. Отобразятся командлеты PowerShell, доступные для AD FS. Чтобы увидеть все командлеты, которые поддерживаются для определенного ресурса, воспользуйтесь следующей командой:

```
Get-Command *-ADFS<имя_объекта>
```

В команде `Help` применяются те же самые принципы. Для дальнейшего изучения работы с AD FS в PowerShell можете ввести команду `Get-Help *-ADFS*` или `Get-Help *-ADFS<имя_объекта>`, чтобы получить информацию о конкретном командлете. На рис. 10.9 приведен пример запроса справочной информации по добавлению доверительного отношения с поставщиком утверждений в AD FS:

```
Get-Help Add-ADFSClaimsProviderTrust
```

Рис. 10.9. Использование PowerShell для получения справочной информации по определенному командлету AD FS

Полезно выделить время на изучение и применение Windows PowerShell на регулярной основе для выполнения практически всех административных задач, которые простираются далеко за пределы AD FS. Автоматизация задач может существенно повысить эффективность.

Добавление доверенной проверяющей стороны

Давайте возвратимся к нашей конфигурации AD FS. Сейчас необходимо добавить доверенную проверяющую сторону. Такое доверительное отношение может существовать между локальными приложениями, партнерскими организациями или облачными службами. Мастер добавления доверительного отношения для проверяющей стороны (Add Relying Party Trust Wizard) помогает установить доверительное отношение между службой федерации и проверяющими сторонами, такими как другая служба федерации, приложение или служба, которая потребляет утверждения от службы федерации вашей организации. Служба федерации выдает маркеры безопасности, используемые проверяющими сторонами для принятия решений по аутентификации.

В данном примере доверительное отношение будет создаваться с применением метаданных федерации. Поскольку партнерская организация не обязательно оказывается под рукой, чтобы поделиться своими метаданными федерации, мы создадим доверительное отношение AD FS с собственной организацией. Развертывать подобную топологию в производственной среде нет особого смысла, но она хорошо подойдет для целей демонстрации или тестирования возможностей и функциональности самой технологии. В производственной среде вы будете выполнять те же самые шаги, просто используя метаданные федерации от партнера, например, Office 365.

Ниже описаны шаги по созданию доверительного отношения.

1. В окне диспетчера серверов выберите в меню Tools (Сервис) пункт AD FS Management (Управление AD FS).
2. На экране AD FS Overview (Обзор AD FS) щелкните на ссылке Add a trusted relying party (Добавить доверенную проверяющую сторону) или выберите аналогичный пункт в раскрывающемся меню Actions (Действия). Запустится мастер Add Relying Party Trust Wizard.
3. Просмотрите информацию на экране Welcome (Добро пожаловать).

   Мастер предоставляет краткое описание работы доверительных отношений для проверяющих сторон.
4. Щелкните на кнопке Next (Далее) для перехода на экран Select Data Source (Выбор источника данных).

   Источник данных можно выбирать тремя способами.

   - Вы можете ввести сетевой путь для доступа к данным федерации, опубликованным в Интернете или в локальной сети.
   - Вы можете проследовать к файлу метаданных федерации.
   - Вы можете вручную ввести данные о проверяющей стороне.
5. Так как метаданные федерации являются локальными, введите непосредственный путь к метаданным федерации, предоставив URL (рис. 10.10), и добавьте **`/FederationMetadata/2007-06/FederationMetadata.xml`** к имени FQDN сервера, на котором размещены данные.
6. Щелкните на кнопке Next, чтобы перейти на экран Specify Display Name (Указание отображаемого имени).

   Здесь можно изменить стандартное отображаемое имя и указать любые примечания о проверяющей стороне.

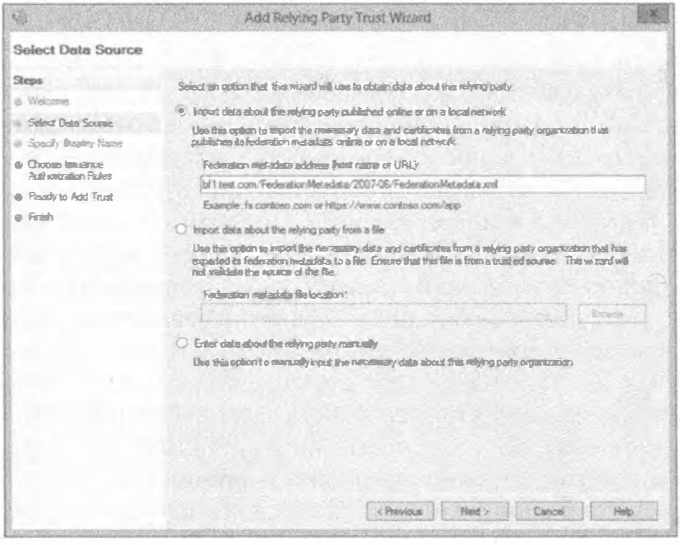


Рис. 10.10. Выбор источника данных с применением мастера Add Relying Party Trust Wizard

7. Щелкните на кнопке Next для перехода на экран Choose Issuance Authorization Rules (Выбор правил выдачи авторизации).

   Эти правила определяют, разрешено ли пользователю получать утверждения от проверяющей стороны. Вы можете либо разрешить, либо запретить всем пользователям доступ к этой проверяющей стороне.

8. В целях тестирования разрешите доступ всем пользователям.

   В производственной среде при необходимости доступ пользователей к приложению или службе можно запретить.

9. Щелкните на кнопке Next, чтобы перейти на экран Ready to Add Trust (Готовность к добавлению доверительного отношения). Внимательно просмотрите сведения на всех вкладках.

   Как показано на рис. 10.11, в добавлении доверительного отношения участвует большой объем информации.

10. Щелкните на кнопке Next, чтобы установить сконфигурированное доверительное отношение и отобразить финальный экран Finish (Завершение) мастера.

    В случае успешного завершения на этом экране будет отображаться заранее отмеченный флажок, предназначенный для открытия диалогового окна Edit Claim Rules (Редактирование правил для утверждений) для данной проверяющей стороны после закрытия мастера.

11. Если вы хотите изменить или добавить любые дополнительные правил для утверждений, оставьте стандартный выбор и закройте мастер; в противном случае снимите отметку с флажка и щелкните на кнопке Close (Закрыть).

Возвратившись обратно в оснастку AD FS Management, вы увидите, что доверительное отношение для проверяющей стороны было добавлено к списку доверительных отношений.

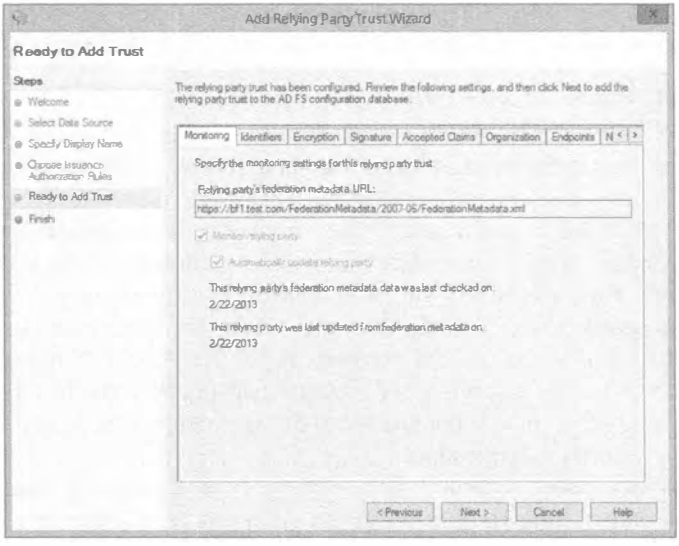


Рис. 10.11. Экран Ready to Add Trust

Итак, вы успешно развернули AD FS на новом сервере федерации. Проверить функционирование служб AD FS на сервере можно с помощью программы Event Viewer (Просмотр событий), как показано на рис. 10.12.

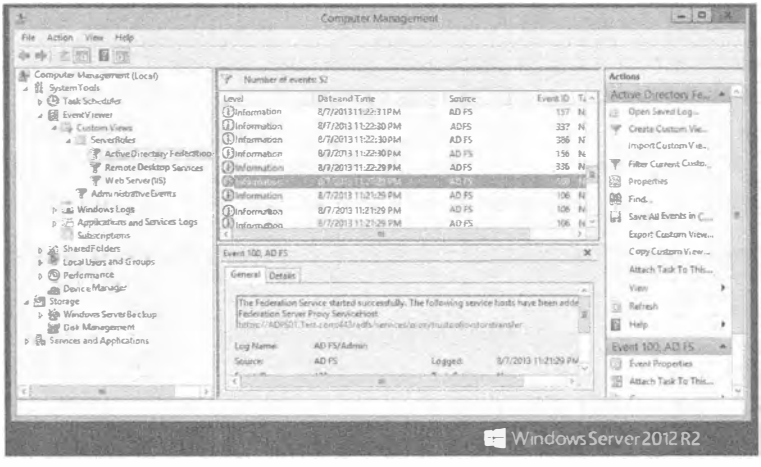


Рис. 10.12. Проверка факта установки и работоспособности служб AD FS с использованием Event Viewer

Дополнительные опции конфигурации для AD FS

Теперь, когда ваш сервер является полнофункциональным сервером федерации, можно ознакомиться с дополнительными задачами управления, доступными благодаря AD FS. Применяя оснастку AD FS Management, вы можете создавать дополнительные сертификаты для маркеров, добавлять новые серверы федерации и прокси-серверы федерации (внутрь фермы серверов федерации), настраивать мониторинг

производительности и выполнять множество других задач. Давайте внимательнее взглянем на некоторые из этих опций.

Добавление сертификата для подписи маркера или для шифрования маркера

Сертификаты являются очень важным фрагментом головоломки AD FS. Чтобы безопасно передавать информацию между серверами федерации, службы AD FS требуют использования и сертификата для подписи маркера, и сертификата для шифрования маркера. Такие сертификаты имеют цифровую подпись посредством секретного ключа. Когда партнер учетной записи выдает маркер безопасности для удостоверения пользователя, партнер ресурса проверяет аутентичность этого маркера. Если отправленная информация соответствует полученной информации, пользователю предоставляется доступ к желаемым ресурсам. Подобный тип проверки безопасности с шифрованием и расшифровкой предотвращает получение доступа к среде AD FS со стороны взломщиков.

Как упоминалось ранее в этой главе, в среде рекомендуется иметь доступными дополнительные сертификаты для подписи маркера и для шифрования маркера. Они предназначены для случаев, когда текущие сертификаты устаревают или возникает подозрение, что безопасность этих сертификатов была скомпрометирована. Если такая ситуация возникнет, вам придется перейти на новый сертификат. Ниже перечислены шаги по добавлению дополнительного сертификата для маркера с применением оснастки AD FS.

1. В окне диспетчера серверов выберите в меню Tools (Сервис) пункт AD FS Management (Управление AD FS).
2. В дереве консоли дважды щелкните на папке Service (Служба) и затем щелкните на папке Certificates (Сертификаты).
3. Выберите либо ссылку Add Token-Signing Certificate (Добавить сертификат для подписи маркера), либо ссылку Add Token-Decrypting Certificate (Добавить сертификат для шифрования маркера), как показано на рис. 10.13.

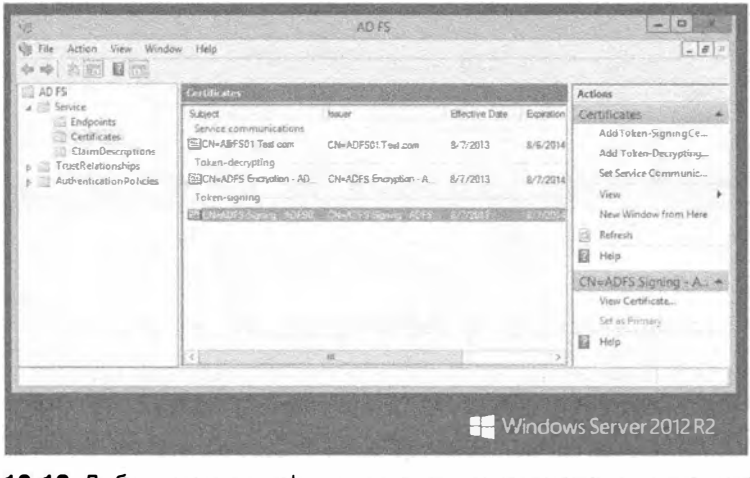


Рис. 10.13. Добавление сертификата для маркера с помощью оснастки AD FS

4. В диалоговом окне Browse for Certificate File (Обзор файла сертификата) перейдите в папку с файлом сертификата, который нужно добавить, выберите его и щелкните на кнопке Open (Открыть).

Настройка мониторинга производительности AD FS

Еще одним великолепным средством, автоматически включенным с AD FS, является возможность конфигурирования монитора производительности (Performance Monitor). Этот инструмент позволяет проводить активный мониторинг производительности инфраструктуры AD FS. По мере необходимости вы можете создавать и планировать создание отчетов для надлежащего управления средой. Очень важно внимательно следить за тем, насколько хорошо AD FS функционирует внутри предприятия. Службы AD FS поступают с двумя собственными наборами счетчиков производительности, которые отслеживают все транзакции аутентификации и выдачи маркеров, используемые AD FS. Настройка мониторинга производительности для AD FS осуществляется с помощью следующих шагов.

1. Запустите монитор производительности, либо выбрав в меню Tools (Сервис) пункт Performance Monitor (Монитор производительности) в окне диспетчера серверов, либо щелкнув на плитке Task Manager (Диспетчер задач) на экране Start (Пуск) и перейдя на соответствующую вкладку.
2. В дереве консоли разверните узел Data Collector Sets (Группы сборщиков данных), щелкните правой кнопкой мыши на элементе User Defined (Определенные пользователем) и выберите в контекстном меню пункт New⇨Data Collector Set (Создать⇨Группа сборщиков данных).

   Откроется мастер новой группы сборщиков данных (New Data Collector Set Wizard), как показано на рис. 10.14.
3. Назначьте новой группе сборщиков данных имя наподобие `AD FS Performance`, выберите переключатель Create manually (Advanced) (Создать вручную (для опытных)) и щелкните на кнопке Next (Далее). Открывшийся экран позволяет выбрать тип журналов данных для применения с AD FS. Оставьте выбранным переключатель Create data logs (Создать журналы данных) и отметьте флажки возле каждой доступной опции. В качестве альтернативы вместо создания журналов данных этот экран позволяет выбрать и создать оповещения счетчиков производительности.

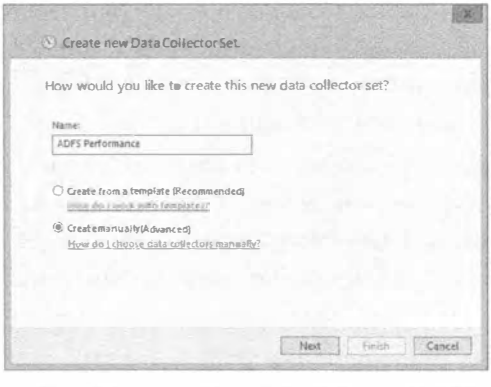


Рис. 10.14. Мастер New Data Collector Set Wizard

4. Щелкните на кнопке Next для перехода на экран Performance Counters (Счетчики производительности).
5. Щелкните на кнопке Add (Добавить), чтобы отобразить все доступные счетчики, которые можно выбрать.
6. Выберите счетчики AD FS и добавьте их в список Added counters (Добавленные счетчики), как показано на рис. 10.15.

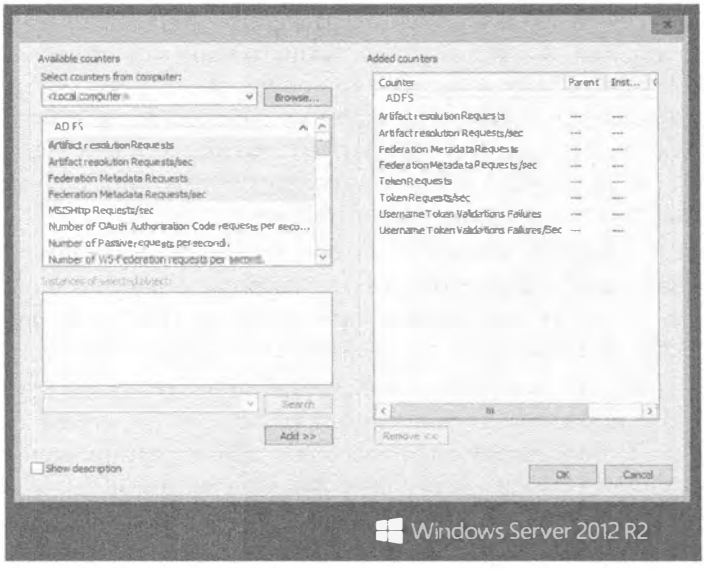


Рис. 10.15. Добавление счетчиков производительности AD FS

7. После добавления всех необходимых счетчиков производительности щелкните на кнопке OK.
8. Щелкните на кнопке Next, чтобы перейти на экран Event Trace Providers (Поставщики трассировки событий).
9. Щелкните на кнопке Add для обзора поставщиков событий и выберите для добавления AD FS и AD FS Tracing (Трассировка AD FS). Щелкните на кнопке OK.
10. Щелкните на кнопке Next, чтобы добавить ключи реестра для мониторинга.

    Это необязательная задача; мониторинг каких-либо ключей реестра производится только при желании.
11. Для продолжения щелкните на кнопке Next.

    Выдается запрос местоположения для сохранения данных.
12. Примите стандартное местоположение или выполните обзор и выберите другое местоположение для хранения данных.
13. Щелкните на кнопке Next, чтобы перейти на финальный экран мастера.

    Выдается запрос на подтверждение создания новой группы сборщиков данных.
14. Оставьте все опции без изменений и щелкните на кнопке Finish (Готово), завершив мастер.

Возвратившись в монитор производительности, вы увидите, что новая группа сборщиков данных была успешно добавлена и отображается в дереве консоли под узлом User Defined. Щелкните правой кнопкой мыши на группе сборщиков данных AD FS Performance и выберите в контекстном меню пункт Start (Начать), чтобы начать сбор данных. Вы заметите, что новый отчет AD FS генерируется под узлом Reports (Отчеты) в дереве консоли (рис. 10.16). Этот отчет можно использовать для отслеживания производительности инфраструктуры AD FS.

Рис. 10.16. Генерация отчета AD FS с применением монитора производительности

В табл. 10.1 приведены более подробные описания доступных счетчиков производительности AD FS. В ней объясняется назначение каждого счетчика и указывается, какие серверы его поддерживают. Эта информация также доступна по ссылке `http://technet.microsoft.com/en-us/library/ff627833(v=WS.10).aspx`.

Таблица 10.1. Счетчики производительности AD FS

Счетчик	Описание	Где может использоваться
Artifact Resolution Requests (Запросов распознавания артефактов)	Отслеживает количество запросов к конечной точке распознавания артефактов, отправленных серверу федерации	Серверы федерации
Artifact Resolution Requests/sec (Запросов распознавания артефактов/с)	Отслеживает количество запросов к конечной точке распознавания артефактов, отправленных серверу федерации, в секунду	Серверы федерации
Federation Metadata Requests (Запросов метаданных федерации)	Отслеживает количество входящих запросов метаданных федерации, отправленных серверу федерации	Серверы федерации
Federation Metadata Requests/sec (Запросов метаданных федерации/с)	Отслеживает количество входящих запросов метаданных федерации, отправленных серверу федерации, в секунду	Серверы федерации
Token Requests (Запросов маркеров)	Отслеживает количество запросов маркеров, которые были отправлены серверу федерации, включая запросы маркеров SSOAuth	Серверы федерации

Окончание табл. 10.1

Счетчик	Описание	Где может использоваться
Token Requests/sec (Запросов маркеров/с)	Отслеживает количество запросов маркеров, которые были отправлены серверу федерации, включая запросы маркеров SSOAuth, в секунду	Серверы федерации
Proxy MEX Requests (Запросов MEX прокси)	Отслеживает количество входящих запросов WS-Metadata Exchange (MEX), которые были отправлены прокси-серверу федерации	Прокси-серверы федерации
Proxy MEX Requests/sec (Запросов MEX прокси/с)	Отслеживает количество входящих запросов WS-Metadata Exchange (MEX), которые были отправлены прокси-серверу федерации, в секунду	Прокси-серверы федерации
Proxy Requests (Запросов прокси)	Отслеживает количество входящих запросов, отправленных прокси-серверу федерации запросов	Прокси-серверы федерации
Proxy Requests/sec (Запросов прокси/с)	Отслеживает количество запросов входящих запросов, отправленных прокси-серверу федерации запросов, в секунду	Прокси-серверы федерации

Добавление дополнительного сервера к ферме серверов федерации

В зависимости от организационных целей и выбранной топологии может понадобиться добавление дополнительных серверов к ферме серверов федерации. Размещение этих серверов зависит от того, как вы планируете использовать доступ SSO внутри организации. Если вы хотите SSO в рамках корпоративной сети, то могли бы логически поместить новый сервер в том же месте, что и остальные. Если же планируется применять возможности SSO с партнерской организацией в проекте с федеративным веб-доступом SSO, то придется разместить сервер федерации также и в партнерской организации.

В приведенном ниже примере показано, как добавить дополнительный сервер к ферме. Сервер должен удовлетворять нескольким требованиям, прежде чем его можно будет добавить. Он должен быть присоединен к домену в лесе Active Directory, иметь установленные роли и компоненты AD FS, а также обязательные сертификаты AD FS, установленные локально.

1. На сервере, который необходимо добавить, запустите задачу Post-deployment Configuration (Конфигурация постразвертывания) через флаг Notifications (Уведомления) в диспетчере серверов сразу после установки роли AD FS, как делали это при создании первого сервера федерации внутри фермы ранее в главе. Вы заметите, что мастер добавления дополнительного сервера к ферме очень похож на мастер создания первого сервера федерации, но имеет несколько отличий.
2. На этот раз на экране Welcome (Добро пожаловать) выберите переключатель Add a federation server to an existing federation service (Добавить сервер федерации в существующую службу федерации). Обратите внимание, что остальные экраны мастера конфигурации в списке слева изменились (рис. 10.17).

Рис. 10.17. Добавление сервера федерации в существующую службу федерации

3. Щелкните на кнопке Next (Далее) для перехода на экран Connect to AD DS (Подключение к AD DS). Точно так же, как при создании первого сервера федерации, для конфигурирования службы федерации на втором сервере внутри фермы требуются административные учетные данные.
4. Щелкните на кнопке Next. Вы заметите, что экран Specify Farm (Указание фермы) отличается от процесса конфигурирования первого сервера федерации. Поскольку мы уже создали ферму, сертификат SSL и выделенную учетную запись службы, когда занимались первым сервером, понадобится лишь указать конфигурацию для сервера федерации. Так как на первом сервере федерации мы использовали базу данных WID, оставьте стандартный выбор и введите имя первого сервера федерации, на котором находится база WID.
5. Щелкните на кнопке Next, чтобы перейти на экран Specify Certificate (Указание сертификата). Удостоверьтесь, что присоединяете тот же самый сертификат SSL, который применялся на первом сервере федерации внутри фермы.
6. Щелкните на кнопке Next. На появившемся экране Specify Service Account (Указание учетной записи службы) щелкните на кнопке Select (Выбрать) для обзора Active Directory и укажите выделенную учетную запись службы, созданную во время конфигурирования первого сервера федерации.
7. Остальные экраны мастера конфигурации аналогичны таким экранам при конфигурировании первого сервера федерации. Внимательно просмотрите произведенный выбор, перейдите на экран Pre-requisite Checks (Проверка предварительных условий) и установите службу. По пути отслеживайте любые предупреждения и сообщения об ошибках.
8. После успешного завершения установки осталось только проверить работоспособность сервера. Вспомните рис. 10.12. Запустите программу Event Viewer

на новом сервере федерации, чтобы удостовериться в корректном функционировании службы. Особое внимание обращайте на событие AD FS с идентификатором 100.

Верификация функциональности сервера федерации

Проверка журналов событий AD FS в Event Viewer — не единственный способ тестирования и верификации работоспособности AD FS на сервере федерации. В качестве альтернативы можете открыть окно браузера на клиентской машине внутри того же самого леса и ввести DNS-имя хоста сервера федерации с добавкой в конце `/adfs/fs/federationserverservice.asmx`. Например, вы могли бы ввести `https://bf1.test.com/adfs/fs/federationserverservice.asmx`. Клиенту может быть выдано сообщение о том, что имеется проблема с сертификатом безопасности этого веб-сайта. Щелкните на Continue to this website (Продолжить с этим веб-сайтом) и должен отобразиться XML-документ с описанием службы. Если доступ запрещен или не удается отобразить веб-страницу, значит, службы IIS функционируют некорректно и не обслуживают страницы, как должны. Ошибки AD FS также отображаются в Event Viewer с указанием направления в их устранении.

Добавление на сервер роли прокси-сервера федерации

Прокси AD FS представляют собой серверы федерации, которые находятся снаружи корпоративной сети. Главная цель прокси-сервера — разрешить удаленный доступ внутренним пользователям к ферме серверов из внешнего источника, такого как Интернет, не раскрывая внешнему миру существующую инфраструктуру AD FS. Когда удаленный пользователь запрашивает доступ в корпоративную сеть, прокси-сервер AD FS использует аутентификацию с помощью форм для выяснения у пользователя его имени и пароля.

К серверу предъявляется несколько требований, которые следует иметь в виду при развертывании на нем прокси-сервера федерации.

- Во внутренней корпоративной сети должен быть в наличии сервер федерации, с которым будет производиться взаимодействие.
- Прокси-сервер должен иметь доверенный сертификат SSL с именем субъекта, совпадающим с именем службы федерации.
- Понадобится сконфигурировать соответствующие записи DNS.

Шаги по добавлению роли прокси-сервера федерации похожи на шаги конфигурирования нового сервера федерации, которые приводились ранее в этой главе.

1. Запустите диспетчер серверов и на вкладке Dashboard (Управляющая панель) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты) или выберите пункт Add Roles and Features в раскрывающемся меню Manage (Управление).
2. Пройдите по экранам мастера, выбрав подходящий тип установки и опции сервера.
3. Добравшись до экрана Select server roles (Выбор серверных ролей), выберите роль Federation Service Proxy (Прокси службы федерации), как показано на рис. 10.18.

Не забывайте, что роли Federation Service Proxy и Federation Service не могут быть установлены на одном сервере.

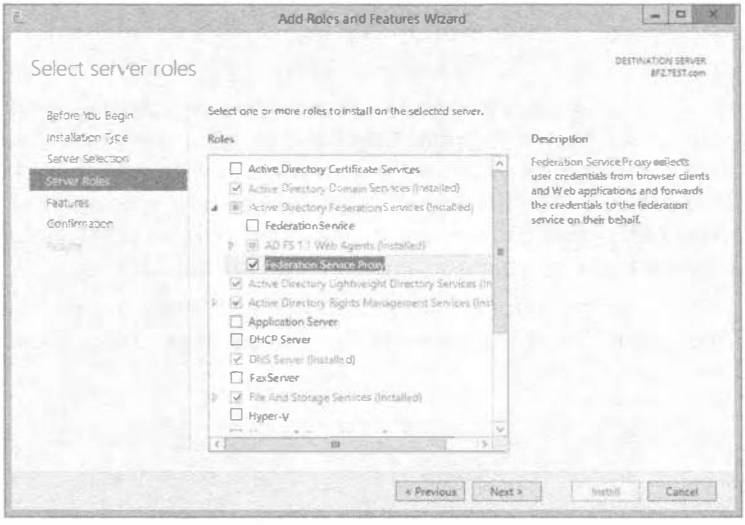


Рис. 10.18. Установка на сервере роли Federation Service Proxy

4. Если вы нуждаетесь или просто хотите добавить дополнительные компоненты на сервер, сделайте это на экране Select features (Выбор компонентов) мастера.
5. Продолжайте продвигаться вплоть до экрана Results (Результаты), чтобы завершить установку роли Federation Server Proxy.

Автоматизация конфигурирования клиентов с использованием групповой политики

Существуют дополнительные изменения в конфигурации, которые должны быть внесены для того, чтобы позволить клиентским компьютерам свободно взаимодействовать с приложениями федерации. Любой клиентский компьютер, желающий иметь доступ SSO к приложениям и службам, должен располагать установленным локально доверенным сертификатом SSL, а настройки браузера для каждого профиля пользователя должны быть сконфигурированы на доверие к серверу федерации.

Как вы и можете себе представить, ручное конфигурирование каждой индивидуальной машины и профиля пользователя в крупной среде окажется утомительной и длительной задачей. К счастью, вы можете воспользоваться групповой политикой и затолкнуть настройки и сертификаты на клиентские компьютеры. Выполните описанные ниже шаги по конфигурированию групповой политики для распределения сертификатов. Обратите внимание, что при этом требуются учетные данные администратора домена или предприятия.

1. Запустите на контроллере домена диспетчер серверов и выберите в меню Tools (Сервис) пункт Group Policy Management (Управление групповой политикой).
2. Найдите существующий объект групповой политики или создайте новый, который будет содержать настройки сертификата.

3. Удостоверьтесь в том, что объект GPO ассоциирован с доменом, сайтом или организационной единицей, где находятся соответствующие учетные записи пользователей и компьютеров.
4. Щелкните правой кнопкой мыши на этом объекте GPO и выберите в контекстном меню пункт Edit (Редактирование).
5. В дереве консоли раскройте папку Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies (Конфигурация компьютера \ Политики \ Настройки Windows \ Настройки безопасности \ Политики открытых ключей), щелкните правой кнопкой мыши на элементе Trusted Root Certification Authorities (Доверенные корневые центры сертификации) и выберите в контекстном меню пункт Import (Импортировать).
6. На экране Welcome (Добро пожаловать) мастера импорта сертификатов (Certificate Import Wizard) щелкните на кнопке Next (Далее), как показано на рис. 10.19.

Рис. 10.19. Мастер Certificate Import Wizard

7. На экране File to Import (Файл для импорта) введите путь к соответствующим файлам сертификатов (например, `\\bf1\c$\bf1.cer`) и щелкните на кнопке Next.
8. На экране Certificate Store (Хранилище сертификатов) выберите переключатель Place all certificates in the following store (Поместить все сертификаты в следующее хранилище) и щелкните на кнопке Next.
9. На экране Completing the Certificate Import Wizard (Завершение мастера импорта сертификатов) удостоверьтесь в корректности всей предоставленной ранее информации и щелкните на кнопке Finish (Готово).
10. Можете повторить эти шаги, чтобы добавить дополнительные сертификаты для каждого сервера федерации, который находится внутри фермы серверов федерации.

Резюме

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?

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?

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?

Глава 11

Введение в общее хранилище и кластеризацию

Общее хранилище и кластеризация в Windows Server 2012 R2 предоставляют, вероятно, наиболее важную функциональность, которая требуется любой инфраструктуре крупного предприятия или центра данных. Гарантирование того, что ресурсы вроде приложений, служб, файлов и папок доставляются с обеспечением высокой готовности (high availability — HA), централизации и масштабируемости, должно быть первостепенной целью каждого IT-администратора и консультанта. Использование общего хранилища и кластеризации предоставляет организациям возможность масштабировать хранилище по требованию, создавать централизованные местоположения для ресурсов и делать их высоко доступными для бизнес-деятельности.

Концепции общего хранилища и кластеризации не являются новыми или эксклюзивными для Windows Server 2012 R2, но обретение четкого понимания каждой концепции позволит уверенно развертывать расширенные предложения HA, которые поступают в готовом виде вместе с операционной системой. В этой главе вы изучите следующие темы:

- использование опций хранилища, доступных для кластеризации;
- применение кворума для помощи в кластеризации;
- построение кластеров хостов и гостей.

Основы общего хранилища

В наиболее базовой форме общее хранилище предоставляет центральное местоположение внутри IT-инфраструктуры организации, предназначенное для размещения специального набора файлов или приложений, так что многочисленные

пользователи могут иметь к ним одновременный доступ. В этой технологии могут быть задействованы самые разнообразные устройства хранения, примерами которых являются сети хранения данных (storage area network — SAN), сетевое хранилище (Network Attached Storage — NAS) и последовательно присоединенные устройства SCSI (Serial Attached SCSI — SAS). В зависимости от существующих требований (и бюджета), вы по своему усмотрению развертываете те или иные опции. В конечном счете, при объединении посредством кластеризации все эти опции преследуют одну и ту же цель — позволить пользователям продолжать работу с их приложениями и файлами в случае выхода сервера из строя. Рассмотрим простой пример с сотрудником отдела кадров по имени Сара. Она должна убедиться в наличии местоположения для безопасного хранения критически важных документов, связанных с кадрами, которые могут содержать номера карточек социального страхования. При правильно спроектированном и реализованном решении общего хранилища Сара может поместить эти файлы в совместно используемое местоположение, которое подвергается шифрованию и резервному копированию, и потенциально могла бы иметь права на управление настройками безопасности. Другие сотрудники с соответствующими правами для этого местоположения имеют доступ к своим файлам, и Саре не придется беспокоиться об открытии совместного доступа к файлам на ее собственной рабочей станции или о риске утратить файлы в результате аварии.

Хранилище и возможность предоставления к нему управляемого доступа являются наиболее распространенными требованиями в любой организации. Доступно множество опций хранения. Прежде чем приступить к рассмотрению опций, доступных в Windows Server 2012 R2, давайте ознакомимся с базовыми компонентами:

- iSCSI SAN
- Fiber Channel SAN
- Корпуса SAS
- SMB 3.0 Server 2012

Благодаря развитию средств, касающихся хранилища, в Windows Server 2012 R2 вы можете начать пользоваться этими компонентами в имеющейся инфраструктуре. Ниже приведен краткий обзор указанных технологий.

Сеть хранения данных

Сеть хранения данных — это подключенная к сети сущность, выделенная специально для хранения. Технология SAN является просто базовой инфраструктурой, и каждое конкретное решение SAN представляет хранилище собственным уникальным способом. В действительности речь идет о хранилище на уровне блоков, которое доступно ресурсам через сеть. SAN обычно выглядит как крупное устройство с многочисленными жесткими дисками, которые вы разделяете и форматируете для представления серверам и компьютерам в сети.

Вдобавок SAN не обязательно должна быть традиционной сетью; например, она может быть волоконно-оптическим каналом (Fiber Channel). В случае волоконно-оптического канала применяется тот же самый базовый принцип: это устройство, заполненное дисками, но сеть основана на оптоволокне. В большинстве организаций сети хранения данных имеет сетевой коммутатор, специально выделенный и оптимизированный для SAN. Сеть передачи данных, с которой взаимодействует

SAN, обычно называют *фабрикой хранилищ*. Главная цель SAN — разрешить различным типам серверов, приложений и пользователей из множества мест иметь доступ к пулу хранения, который может быть доступен из любого устройства, связанного с этой фабрикой хранилищ. Часть фабрики хранилищ является хост-адаптером шины (host bus adapter — HBA), представляющим собой сетевую интерфейсную плату (network interface card — NIC), которая соединяет фабрику хранилищ с ресурсами в сети, нуждающимися в доступе к хранилищу.

Многие организации и IT-профессионалы уверены, что SAN предоставляет им гибкость развертывания и повторного развертывания серверов и хранилища в намного более динамической манере. Серверы могут загружаться напрямую из SAN, что предоставляет им операционную систему и конфигурации в крупном местоположении с высокой готовностью. Если физический сервер утрачивает работоспособность, его место может занять новый сервер, а операционная система и связанные диски могут быть направлены на новый сервер намного быстрее, чем в случае перестройки и восстановления с ленты.

Мы рекомендуем уделить некоторое время на более глубокие исследования этих тем, и если в вашей организации имеется SAN, то вы должны начать с чтения сопутствующих руководств по развертыванию и администрированию.

iSCSI

Интерфейс малых компьютерных систем, основанный на TCP/IP (Internet Small Computer System Interface — iSCSI), существует на протяжении многих лет, и он применялся в качестве способа коммуникации компьютеров или серверов с дисковыми устройствами или другими устройствами хранения, такими как библиотеки лент. С развитием SCSI развивалась также сетевая инфраструктура, соединяющая серверы и компьютеры. Гигабитные сети стали намного более распространенным явлением, что обеспечивает подключение к хранилищам с широкой полосой пропускания. Протокол iSCSI используется для упрощения передачи данных по сети TCP/IP (Ethernet). Протокол iSCSI позволяет предоставлять дисковые устройства, расположенные в SAN, через существующую сеть вашим серверам.

Инициатор iSCSI (iSCSI Initiator) от Microsoft является программным компонентом, который встроен во все операционные системы Windows Server, начиная с Windows Server 2008, и также включен в Windows 7 и Windows 8. Инициатор iSCSI делает возможными подключения устройств Windows для утилизации этой технологии.

Как и с другими технологиями хранения, о которых здесь пойдет речь, мы не собираемся вдаваться в самые мелкие детали, касающиеся всех доступных опций масштабирования и производительности. Цель этой главы — предоставить введение в эти области.

Волоконно-оптический канал

Волоконно-оптический канал (Fiber Channel — FC) является еще одним высокоскоростным сетевым каналом, работающим через медную витую пару или оптоволоконный кабель. Подключение к серверам и хранилищу поддерживается через хост-адаптер шины (HBA) с применением протокола, похожего на TCP, который называется протоколом волоконно-оптического канала (Fiber Channel Protocol — FCP).

Адаптеры HBA взаимодействуют в группе зон со специальными мировыми именами, которые по существу действуют подобно IP-адресам. Подключение Fiber Channel к устройствам и хранилищу производится через оптоволоконный коммутатор и управляется в зонах, которые выделены специальным сетевым интерфейсам. Это давно было самым быстрым типом подключаемости к сетевым хранилищам, доступным для организаций, но он далеко не дешев!

Корпуса SAS

Последовательно присоединенные устройства SCSI (SAS) — это метод доступа к устройствам, которые используют последовательное подключение по локально соединенным кабелям. В отличие от iSCSI и FC, решения корпусов SAS не располагают сетевой подключаемостью. Технология SAS поддерживает ранние технологии SCSI, в том числе принтеры, сканеры и другие периферийные устройства. Корпуса SAS представляют собой большие устройства, подобные SAN, которые имеют множество дисков, сконфигурированных с применением различных уровней RAID для обеспечения избыточности на случай отказа диска.

RAID

Избыточный массив независимых дисков (Redundant Array of Independent Disks — RAID) состоит из множества дисков, сгруппированных вместе. Этот массив позволяет настраивать отказоустойчивые диски и масштабировать их для достижения высокого уровня производительности. Существует много типов RAID, которые предлагают разнообразные методы поддержки производительности и обхода отказа. Технологии RAID являются основой внутренней работы iSCSI, SAS и корпусов Fiber Channel SAN. По следующей ссылке вы найдете подробные сведения по типам RAID и ситуациям, в которых они используются: `http://technet.microsoft.com/en-us/library/cc786889(v=WS.10).aspx`.

SMB 3.0

Блок сообщений сервера (Server Message Block — SMB) — это протокол, специально разработанный для общих файловых ресурсов и масштабирования этих ресурсов или серверов. Он функционирует поверх TCP/IP, но может использовать другие сетевые протоколы. SMB применяется для доступа к пользовательским данным и приложениям в ресурсах, которые существуют на удаленном сервере. Для настройки SMB должны быть удовлетворены специфические требования.

- Требуется кластер с обходом отказа Windows Server 2012/2012 R2, имеющий минимум два узла.
- Должна быть возможность создания общих файловых ресурсов со свойством Continuous Availability (Постоянная доступность); по умолчанию так и есть.
- Общие файловые ресурсы должны находиться на томах CSV.
- На клиентских компьютерах, получающих доступ к этим ресурсам, должна быть установлена ОС Windows 8 или последующей версии.
- На серверах, использующих или обращающихся к этим ресурсам, должна быть установлена ОС Windows Server 2012 или выше.

На серверах кластера с обходом отказа, на которых функционирует ОС Windows Server 2012/2012 R2, дополнительные компоненты или роли устанавливать не нужно. Протокол SMB 3.0 включен по умолчанию. Ниже перечислены новые возможности SMB, доступные в Windows Server 2012/2012 R2.

- **SMB Transparent Failover (Прозрачный обход отказа SMB).** Эта возможность позволяет прозрачно подключать клиентов к другому узлу гладким образом, чтобы работа приложений и хранилища не прерывалась.
- **SMB Scale Out (Масштабирование SMB).** Применяя общие тома кластера (Cluster Shared Volume — CSV), вы создаете общий диск, который все узлы в кластере используют через прямой ввод-вывод, чтобы эффективнее расходовать полосу пропускания сети и нагрузку на файловых серверах. Это оптимизирует производительность и в то же время обеспечивает улучшенный доступ клиентам.
- **SMB Direct (Прямой доступ SMB).** Эта возможность задействует сетевые интерфейсные платы, которые поддерживают функции RDMA (Remote Direct Memory Access — дистанционный прямой доступ в память), и позволяет разгрузить центральный процессор и обеспечить более высокие скорости передачи данных с минимальной задержкой.

Новых возможностей SMB появилось совсем немного. Существует множество других компонентов, таких как специфичные для SMB командлеты PowerShell, шифрование и счетчики производительности.

Более подробную информацию по SMB и набору новых возможностей можно найти по ссылке `http://technet.microsoft.com/en-us/library/hh831795.aspx`.

Службы файлов и хранилища Windows Server 2012 R2

Роль File and Storage Services (Службы файлов и хранилища) в Windows Server, показанная на рис. 11.1, предоставляет все службы и функции, необходимые для управления и создания файловых серверов и хранилища разных типов в Windows Server.

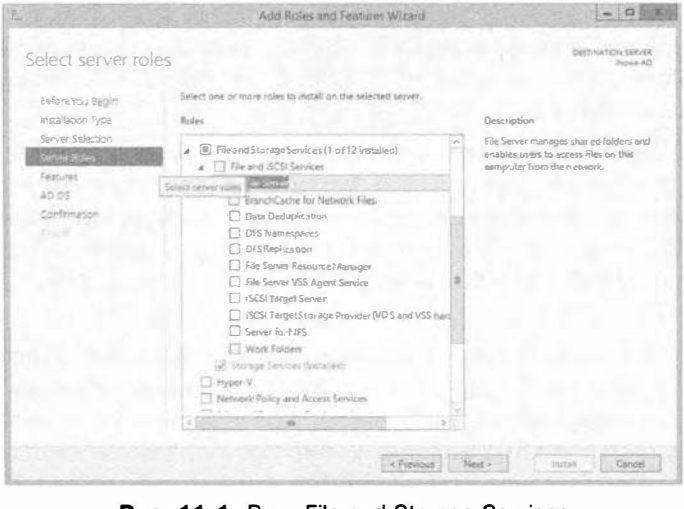


Рис. 11.1. Роль File and Storage Services

Как видите, компонент Storage Services (Службы хранилища) устанавливается по умолчанию и не может быть удален. Другие компоненты при необходимости могут быть установлены либо удалены.

Компонент File and iSCSI Services (Службы файлов и iSCSI) этой роли предоставляет множество других компонентов, которые помогают управлять общими файлами, размером диска, репликацией и офисами филиалов. В следующем списке представлен обзор этих компонентов с указанием возможностей, которые они предлагают для файлов и хранилища в Windows Server 2012 R2.

- **File Server (Файловый сервер).** Этот компонент позволяет управлять общими ресурсами и предоставляет пользователям возможность доступа к файлам на конкретном сервере в сети организации.
- **BranchCache for Network Files (BranchCache для сетевых файлов).** Этот компонент позволяет серверам BranchCache иметь сетевые файловые службы.
- **Data Deduplication (Дедупликация данных).** Эта служба помогает управлять и экономить дисковое пространство, анализируя содержимое тома и удостоверяясь в существовании только одной версии каждого файла. Продолжая приведенный ранее пример с Сарой и ее файлами из отдела кадров, предположим, что Меттью, коллега Сары в отделе кадров, сохранил копию файла в каком-то другом месте, подумав о том, что она недоступна. Служба Data Deduplication обеспечивает существование только одной версии конкретного файла, но делает доступными ссылки на него, так что Меттью сможет найти свой файл.
- **DFS Namespaces (Пространства имен DFS).** Распределенная файловая система (Distributed File System — DFS) позволяет настроить группу общих папок, которые могли бы располагаться на других серверах в организации, но выглядеть как имеющие одно имя. Вот пример:
  - сервер 1 имеет общую папку по имени `\\Server1\Files`;
  - сервер 2 имеет общую папку по имени `\\Server2\Stuff`.

С помощью DFS Namespaces можно было бы определить их как `\\Bigfirm\Shared`.

- **DFS Replication (Репликация DFS).** Этот компонент позволяет синхронизировать общие папки по сети WAN. Он не требует DFS Namespaces, но может применяться совместно.
- **File Server Resource Manager (Диспетчер ресурсов файлового сервера).** Диспетчер ресурсов файлового сервера (File Server Resource Manager — FSRM) — это инструмент для управления и мониторинга производительности, который предоставит более детальные отчеты о том, что происходит с хранилищем. Посредством FSRM можно также строить файловые политики, квоты и классификации.
- **File Server VSS Agent Service (Служба агента VSS файлового сервера).** Эту службу можно использовать для копирования приложений и данных, хранящихся на конкретном сервере, на котором установлена роль File and Storage Services, с применением службы теневого копирования томов (Volume Shadow Copy Service — VSS). За дополнительными сведениями о службе VSS обращайтесь по ссылке `http://tinyurl.com/c11whatisvss`.

- **iSCSI Target Server (Целевой сервер iSCSI).** Это предоставляет инструменты и связанные службы для управления серверами iSCSI.
- **iSCSI Target Storage Provider (VDS and VSS Hardware Providers) (Поставщик целевого хранилища iSCSI (поставщики оборудования VDS и VSS)).** Работает подобно службе File Server VSS Agent Service, но специфичен для серверов, которые используют цели iSCSI и службу виртуальных дисков (Virtual Disk Service — VDS).
- **Server for NFS (Сервер для NFS).** Вы можете включить сетевую файловую систему (Network File System — NFS), которая применяется в компьютерах с Unix/Linux, так что общие ресурсы из установки Windows Server 2012 R2 будут видимыми таким клиентам.
- **Work Folders (Рабочие папки).** Этот новый компонент Windows Server 2012 R2 предоставляет простой способ управления файлами, которые существуют на множестве рабочих станций и персональных устройств. Рабочая папка будет действовать в качестве хоста и синхронизировать файлы пользователей с этим местоположением, так что пользователи могут получать доступ к своим файлам изнутри или снаружи сети. Отличие от компонента File Server или DFS Namespaces в том, что файлы размещены на клиентах. Снова возвратившись к примеру с Сарой и Меттью из отдела кадров, отметим, что они могли бы использовать Work Folders для обеспечения синхронизации и обновления файлов, хранящихся в определенных местоположениях на их рабочих станциях, с файловым сервером. Если они работают над проектом вместе, но находятся в разных местах, нужные файлы будут всегда доступны и синхронизированы.

Все эти компоненты можно установить через управляющую панель диспетчера серверов, которая предоставляет детальные сведения о каждом компоненте и любые предварительные условия. В следующем разделе мы определим кластер и поможем построить высоко доступные службы при участии кластеризации с обходом отказа.

Кластеризация

В наиболее базовой форме *кластер* — это два или большее количество серверов (физических или виртуальных), сконфигурированных как логический объект и единственная сущность, которая управляет общими ресурсами и представляет их конечным пользователям. Серверы, являющиеся членами кластера, называются *узлами*. Тремя самыми распространенными типами кластеров в Windows Server 2012 R2 являются кластеры файловых серверов, кластеры SQL и кластеры Hyper-V.

Двухузловой кластер, например, можно было бы сконфигурировать с узлами (физическими либо виртуальными), множеством сетевых интерфейсных плат и каким-то решением общего хранилища наподобие iSCSI, SAN или напрямую присоединенных дисков.

Цель кластеризации заключается в том, чтобы разрешить определенной группе узлов работать вместе, пользуясь общей мощностью высоко доступных ресурсов. Это обеспечит вашим конечным пользователям высокую готовность в отношении рабочих нагрузок, которые им нужны.

Кластеризация предоставляет следующие преимущества.

- Возможность сохранения работоспособности в случае отказа или отключения узла.
- Возможность перезапуска виртуальной машины или сохранения работоспособности при отказе какой-то виртуальной машины.
- Нулевое время простоя для любых исправлений или обслуживания узлов кластера.
- Возможность переноса и рассредоточения нагрузки серверов (такого как гостевые виртуальные машины).

Опции масштабируемости выходят далеко за рамки двух хост-серверов и могут быть расширены вплоть до 64 узлов на кластер, даже с поддержкой разнесенных географических местоположений. Сложности географически распределенных кластеров для доступности и восстановления не являются темой этого раздела, но они станут более важными, как только вы начнете понимать возможности кластеризации.

Кластеры обычно используются в сценариях с высокой емкостью, высокой видимостью и устойчивостью к отказам. Вы проектируете размер и тип кластера на основе определенных потребностей службы или бизнес-деятельности, а также на базе ресурсов, которые должны быть размещены. При любом сценарии всегда думайте о кластеризации как о решении, предназначенном для увеличения доступности ваших служб, приложений и компонентов конечным пользователям.

В течение многих лет Windows Server росла как операционная система, и требования по созданию кластера всегда были ключом к успешной реализации кластера. В следующем примере мы рассмотрим эти требования.

Требования кластеризации

Мы посвятим некоторое время исследованиям требований к настройке кластера и ознакомлением с несколькими рекомендуемыми подходами. Но перед тем как приступить к изучению специфики оборудования, прочитайте статью "Проверка оборудования для отказоустойчивого кластера", доступную по ссылке `http://technet.microsoft.com/ru-ru/library/jj134244.aspx`.

> **Информация о проверке для Windows Server 2012 R2**
>
> На момент написания этой книги информация о проверке для Windows Server 2012 R2 не была опубликована. Требования, указанные в статье "Проверка оборудования для отказоустойчивого кластера", применимы и продолжат поддерживаться.

Ниже перечислены эти требования.

- **Серверы.** Наша бригада экспертов, обладатели звания MVP и специалисты из Microsoft рекомендуют использовать набор оборудования, который содержит одинаковые или похожие элементы и конфигурацию.
- **Сеть.** Всегда следует применять несколько сетевых интерфейсных плат. Кроме того, если кластеры используют iSCSI, вы должны разделять трафик сети и

трафик нормальных коммуникаций либо за счет применения физически разного сетевого оборудования, либо путем логического сегментирования трафика, используя виртуальные сети (VLAN) на коммутаторах.

- **Хранилище.** Если в кластере задействовано хранилище Serial Attached SCSI или Fiber Channel, то все элементы должны быть идентичны, включая драйверы HBA и прошитого ПО (firmware). Вы не должны применять множество версий прошитого ПО или драйверов, даже если производитель их поддерживает.
- **Общее хранилище.** Общее хранилище представляет собой обязательное требование. В Windows Server 2012 (и Windows Server 2012 R2) можно использовать общее хранилище, являющееся локальным через SAS на сервере, наряду с общими файловыми ресурсами SMB 3.0 для всех потребностей кластера.
- **Пространства хранения.** Если вы планируете применять Serial Attached SCSI, то в Windows Server 2012 и Windows Server 2012 R2 поддерживаются пространства хранения (Storage Spaces). Пространства хранения обсуждаются в главе 12, но в отношении пространств хранения и кластеров можно указать несколько базовых требований.
  - Необходимо иметь минимум три физических дисковых устройства SAS.
  - Устройства должны обладать емкостью минимум 4 Гбайт.
  - Устройства не могут быть загрузочными дисками; они должны быть выделены в качестве пула хранения.
  - При конфигурировании пространств хранения кластеры поддерживают только простые или зеркальные типы.

Функциональность кластеризации

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.

Со времен версии Windows Server 2008 R2 в кластеризацию были внесены многие усовершенствования. На кластеризацию оказывают влияние улучшения операционной системы, но ее средства остались на прежних местах и обладают теми же возможностями, что и в предшествующих версиях, с крупным усовершенствованием, таким как масштабируемость кластеров. В Windows Server 2012 и Windows Server 2012 R2 предлагается увеличенная масштабируемость в рамках компонента Hyper-V Failover Clustering (Кластеризация с обходом отказа Hyper-V), который теперь поддерживает вплоть до 64 узлов и 8 000 виртуальных машин на кластер.

Кроме того, в Microsoft представили концепцию *постоянной доступности*. Она включает объединение сетевых интерфейсных плат, поддержку обновления с учетом кластера (Cluster-Aware Updating) и масштабируемые файловые серверы (Scale-Out File Server — SOFS). Постоянная доступность — это сквозной мониторинг с вариантами его проведения вверх и вниз внутри целого стека кластеров.

- **Обновления с учетом кластера.** Cluster-Aware Updating — это служба, поддерживаемая заново сконструированными службами обновления Windows Server Update Services (дополнительные сведения ищите в главе 31 тома 2). Данный компонент переместит рабочую нагрузку или виртуальные машины в другой узел кластера, обработает обновление (при необходимости инициируя перезагрузку), после чего возвратит рабочую нагрузку обратно и продолжит со следующим узлом кластера.
- **Использование виртуальных дисков Hyper-V как открытого хранилища.** Вероятно, одной из лучших особенностей Windows Server 2012 и Windows Server 2012 R2 считается возможность употребления виртуальных дисков Hyper-V (только в формате VHDX) в качестве открытого хранилища для гостевой кластеризации, что значительно расширяет масштабируемость и доступность внутри виртуальной инфраструктуры, а также позволяет строить масштабируемые файловые серверы. Наиболее важно то, что появляется возможность применения файлов VHDX для кластеризации без SAN.

Правильно реализованное решение кластеризации с обходом отказа доведет до максимума продуктивность бизнес-деятельности и отточит уровни обслуживания. Отказоустойчивым центром данных является такой центр, который располагает пулами ресурсов для вычислительной мощности, хранилищем и сетевыми ресурсами. При построении среды кластеризации с обходом отказа с помощью Windows Server 2012 R2 вы начинаете с физического уровня, т.е. с сети.

На рис. 11.2 показан отдельный сервер с двумя физическими платами NIC и множеством виртуальных адаптеров.

Благодаря постоянной доступности, вы получаете не только более высокую надежность, но также улучшенные показатели производительности. При таком подходе вы объединяете множество подключений для увеличения полосы пропускания, доступной операционной системе, и обеспечения отказоустойчивости, если отказывает порт NIC, отключается кабель или перестает работать физическая плата.

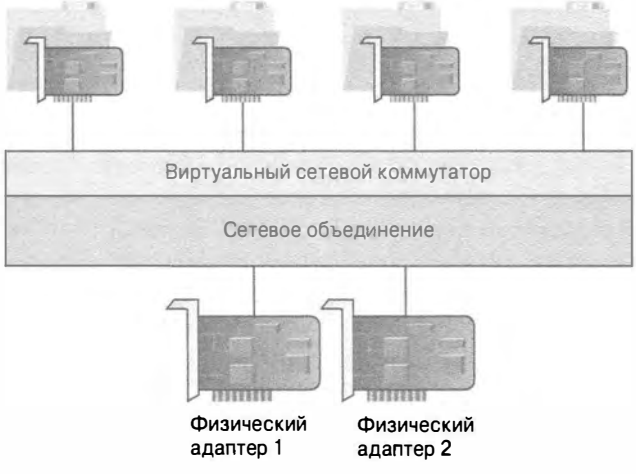


Рис. 11.2. Физические и виртуальные адаптеры

Общие тома кластера

Общие тома кластера (Cluster Shared Volume — CSV) являются компонентом кластеризации с обходом отказа и впервые были введены в Windows Server 2008 R2. Тома CSV проектировались специально для виртуализации. Их базовое применение было связано с упрощением хранилища для виртуальных машин. Если вы не используете том CSV с серверами Hyper-V, то доступ к вашему диску возможен только со стороны одного узла в каждый момент времени. Конфигурирование тома CSV позволяет применять обычный общий диск, упрощает задачи управления хранилищем для Hyper-V и допускает существование множества файлов VHD. Вы также можете минимизировать время простоя и утери подключения с помощью обнаружения отказа и восстановления посредством дополнительных путей подключения между узлами в кластере (через SAN).

Проектное решение тома CSV упрощает хранилище, так что несколько виртуальных машин могут получать доступ к одному и тому же диску одновременно, что очевидно не требует большого количества дисковых устройств. Вместе с этой моделью вы получите и другие возможности; когда вы делаете живой перенос виртуальной машины, общие тома создают множество подключений между узлами кластера и общим диском. Таким образом, если подключение утрачивается, перенос может быть продолжен через другое подключение. Чтобы задействовать тома CSV, вам придется использовать только разделы NTFS; какие-то другие специальные настройки или конфигурации не потребуются.

В Windows Server 2012 тома CSV позволяют нескольким узлам иметь доступ по чтению/записи к тому же самому диску. Вы получаете преимущество в виде возможности быстрого перемещения любого тома из одного узла внутри кластера в другой узел внутри этого кластера. Средства монтирования и размонтирования тома существенно улучшились, что способствует упрощению процедуры управления большим количеством дисков в кластерах. В Windows Server 2012 также были внесены значительные изменения в расширенные возможности, такие как тома BitLocker, устранение поддержки зависимостей от внешней аутентификации для пространств хранения и крупные усовершенствования в проверке функциональности между Hyper-V и CSV, которые увеличивают производительность. В версии Windows Server 2012 отсутствует автоматическая ребалансировка назначения узлов для дисков, но в Windows Server 2012 R2 владение тома CSV балансируется между всеми узлами. Ранее всеми дисками мог владеть один или два узла в, скажем, 12-узловом кластере, но в Windows Server 2012 R2 диски равномерно распределяются между 12 узлами. Если какой-нибудь из узлов теряет работоспособность, кластер автоматически запускает процесс ребалансировки размещения дисков. За счет перемещения из единственного узла координатора в распределенный узел поддержка масштабируемых файловых серверов намного более эффективна, а риск отказа значительно снижается.

В Windows Server 2012 R2 тома CSV имеют лучшую диагностику и способность к взаимодействию, чем в предшествующих версиях. Вы можете просматривать тома CSV на поузловой основе, чтобы выяснить, настроено ли перенаправление операций ввода-вывода и причина этого перенаправления. Версия Windows Server 2012 R2 располагает новым командлетом PowerShell под названием `Get-ClusterSharedVolumeState`.

В плане способности к взаимодействию в Windows Server 2012 R2 добавлена поддержка следующих средств:

- отказоустойчивая файловая система (Resilient File System — ReFS);
- дедупликация данных;
- равноправные пространства хранения и многоуровневые пространства хранения.

Рост и принятие виртуализации в организациях всех размеров показывает, что способ применения кластеризации в наши дни разительно изменился, если сравнивать с тем, как обстояли дела даже пять лет назад. Многие центры данных в настоящее время строят кластеры крупных размеров. В Microsoft усердно трудятся над повышением отказоустойчивости томов CSV, а также над расширением сферы их использования за пределы одних лишь виртуальных машин, распространяя CSV на масштабируемые файловые серверы (SOFS), особенно на общие файлы VHDX. Масштабируемые файловые серверы обсуждаются в главе 13. Основные изменения в томах CSV с момента Windows Server 2008 R2 расширяют перечень возможных случаев их применения, а также сценарии и опции хранилища для ваших кластеров.

Кластеры и виртуализация

В этом разделе внимание будет сосредоточено на усовершенствованиях в Windows Server 2012 R2. Так как между выпусками Windows Server 2012 и Windows Server 2012 R2 прошел всего один год, мы будем трактовать их как один выпуск. Средства, специфичные для Windows Server 2012 R2, будут отмечены особо. Первым делом, давайте взглянем на сами новые средства и то, какие великолепные опции получили гостевые кластеры (кластеры виртуальных машин).

- **Общий виртуальный жесткий диск.** Одним из новых средств является общий виртуальный жесткий диск (virtual hard disk — VHD) для гостевых кластеров, который предоставляет среде Hyper-V возможность использования файла `.vhdx` в качестве решения общего хранилища.
- **Очистка виртуальной машины при ее завершении.** Очистка виртуальной машины при ее завершении позволяет хосту Hyper-V запускать очистку конкретного узла и переносить все виртуальные машины на новый хост. Это также происходит, если виртуальная машина завершается во время бездействия.
- **Мониторинг работоспособности сети виртуальных машин.** Мониторинг работоспособности сети виртуальных машин позволяет выполнять живой перенос виртуальных машин, если в виртуальной сети произошло отключение. К дополнительным новым средствам относятся такие вещи, как управляющая панель кластера и определение работоспособности узлов, которые были помещены в эту управляющую панель.
- **Живые переносы.** До выхода Windows Server 2012 для проведения живого переноса нужно было иметь решение общего хранилища в месте, которое применялось для живого переноса без каких-либо простоев. Версия Windows Server 2012 позволяет перемещать виртуальные машины из хоста на хост с кластером или без него, и благодаря добавлению общих файловых ресурсов SMB 3.0, настроенные для этого файлы не обязаны находиться в SAN. Живые переносы можно делать из виртуальных машин, которые расположены на локальных дисках, присоединенных к серверу.

Одним из наиболее важных факторов, который необходимо понимать в кластеризации, является *кворум* — что он делает, для чего нужен, и какие усовершенствования были сделаны в Windows Server 2012 R2, улучшающие отказоустойчивость кворума. В следующем разделе мы объясним сущность кворума, так что вы получите более глубокое понимание его использования в кластеризации.

Понятие кворумов

Согласно толковым словарям, 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. Лучший способ начать сбор технических потребностей для вашего кластера — понять, что такое кворум и для чего он используется.

Кворум существовал примерно с момента появления кластеризации и был одним из основных компонентов, а также своего рода невоспетым героем. В каждой модификации Windows Server в кворум вносились усовершенствования, в итоге приведя нас к ситуации, когда мы теперь имеем дело с чрезвычайно развитыми возможностями кворума в версии Windows Server 2012. *Кворум — это настройка в обходе отказа, определяющая количество отказов, которые кластер может иметь или удерживать, сохраняя доступность своих служб в онлайновом режиме.* Как только порог кворума превышен, кластер переходит в отключенный режим.

Кластер вовсе не подсчитывает количество узлов и ресурсов, поэтому он не просматривает текущую емкость, чтобы принять решение о завершении служб. Думайте примерно так: пусть в кластере имеется сто узлов; это совершенно не означает, что после прекращения работоспособности пятидесяти из них кластер завершится, как только откажет пятьдесят первый узел. Кластер абсолютно не осведомлен о числе серверов или о том, какие ресурсы перегружены, а какие недогружены. Вместо этого ответственность кворума заключается в том, чтобы помочь предотвратить аномалию, называемую *расщеплением*, когда два сервера в кластере пытаются выполнить запись в один и тот же файл или получить право владения теми же ресурсами, потенциально разрушая их.

Работа кворума в этом качестве связана с недопущением проблемы и по существу принятием решения о том, что может ли кластер или же должен продолжать функционирование, остановив службу проблемного узла до тех пор, пока она не сможет нормально взаимодействовать с оставшимися кластерами. После решения проблемы кворум позволит ранее проблемному домену повторно присоединиться к кластерной группе и перезапустить все необходимые службы. Решения кворума принимаются посредством голосов; каждый узел в кластере имеет один голос, а в самом кластере может быть сконфигурирован свидетель. Свидетелем может быть общий файловый ресурс или диск (согласно рекомендациям бригады, занимающейся кластеризацией в Microsoft, вы должны всегда конфигурировать кластер с нечетным числом членов). Нечетное число узлов позволяет иметь четное количество голосов кворума, а дополняющий до нечетного числа ресурс может быть свидетелем для вывода узла из работы. Добавление такого дополнительного узла гарантирует, что если половина кластера выйдет из строя, то свидетель сохранит его в работоспособном состоянии.

Высоко доступное хранилище

Наличие высоко доступной виртуальной инфраструктуры является важным фактором успешности вашего плана HA. Соображения относительно опций хранилища и способа подключения хранилища к виртуальным машинам для обеспечения их непрерывного функционирования, когда оборудование отказывает, являются безоговорочными. Проектные соображения включают метод сохранения виртуальных машин и перечень видов компонентов, требуемых для предоставления преимуществ отказоустойчивости.

Ниже приведен список опций высоко доступного хранилища.

- **Оборудование.** Наиболее важным является оборудование для хранения, будь то SAN, iSCSI или JBOD (just a bunch of disks — просто группа дисков).
- **Электропитание.** Необходимо наличие стабильного электропитания и избыточных источников питания. Если вы можете предоставить вторичное электропитание, это превосходно.
- **Диски.** Хранилище HA должно быть в состоянии выдерживать дисковые отказы, продолжая удовлетворять вашим потребностям.
- **Оборудование сети хранения данных.** Создание высоко доступного аппаратного решения обычно предусматривает устранение всех одиночных точек отказа, включая компоненты сети хранения данных, такие как HBA или сетевые адаптеры.
- **Пространства хранения.** Это новое средство виртуализации хранилища, появившееся в Windows Server 2012, позволяет использовать присоединенные диски USB, Fiber Channel, iSCSI, SAS и SATA для создания виртуального диска, который может охватывать все упомянутые диски. Когда вы создаете такие виртуальные диски в Windows Server 2012 R2, для защиты применяется зеркальное отображение или контроль по четности, что позволяет справиться с дисковым сбоем без потери данных. Важно понимать, что лучше всего это достигается за счет распространения создаваемых пулов хранения на разнородные типы дисков.
- **Многопутевой ввод-вывод.** Многопутевой ввод-вывод (Multipath Input/Output — MPIO) — это средство Windows, которое позволяет сделать хранилище Fiber Channel и iSCSI доступным через множество путей по очереди для клиента вроде Hyper-V, чтобы обеспечить при доступе высокую готовность. Располагая множеством путей, MPIO рассматривает оба местоположения хранения как единственное устройство и естественным образом поддерживает обход отказа. MPIO выполняет всю необходимую работу; если что-то переходит в отключенный режим, MPIO обработает немедленное перенаправление на другое подключение.
- **Сетевое объединение и отказоустойчивость.** Если вы ищете способ подключения хостов Hyper-V к хранилищу, настоятельно рекомендуется настраивать хост-серверы с несколькими сетевыми интерфейсными платами и путями. Вы всегда стремитесь обеспечить избыточность посредством сетевого объединения на любом кластеризованном ресурсе, и применение SMB/SMB Multichannel предоставит наилучшую доступную полосу пропускания.

Пространства хранения

Пространства хранения (Storage Spaces) считаются одним из удобных новых средств Windows Server 2012 и Windows Server 2012 R2. Главное их преимущество в том, что они предоставляют возможность управления группой дисков как единым виртуальным дисковым устройством. Тип виртуального диска предписывает то, каким образом данные записываются на физические диски.

В настоящее время на выбор доступны три типа виртуальных дисков.

- **Простой.** Как вытекает из названия, это простой набор с чередованием без контроля по четности. Считайте такой тип близким к RAID 0. Простая топология не предоставляет избыточности, поэтому любой дисковый отказ может вызвать проблемы с доступом к данным. Это тип используется главным образом для увеличения пропускной способности и доведения до максимума емкости.
- **С зеркальным отображением.** Это конфигурация RAID 1, которая увеличивает надежность за счет применения двух дисков (например) и позволяет одному диску отказывать, не приводя к прерыванию доступа. Крупным недостатком является лишение дискового пространства, поскольку один из дисков используется в качестве копии (зеркала) другого диска.
- **С контролем по четности.** Похоже на конфигурацию RAID 5; это набор с чередованием данных, разнесенный по дискам, с распределенным контролем по четности. За счет чередования данных и информации на нескольких дисках повышается надежность. Как и в случае RAID 5, понадобятся минимум три диска.

Если вы не знакомы с дисковыми массивами RAID, рекомендуется почитать следующую статью, в которой описаны основы RAID и уровни RAID: `http://ru.wikipedia.org/wiki/RAID`.

С пространствами хранения связаны три базовых компонента.

- **Физические диски.** Если для своих пулов хранения вы задействуете физические диски, то ниже перечислены требования к ним:
  - минимум один физический диск;
  - два физических диска для создания отказоустойчивого виртуального диска с зеркальным отображением;
  - три физических диска для обеспечения отказоустойчивого зеркального отображения с контролем по четности;
  - пять физических дисков для обеспечения трехстороннего зеркального отображения;
  - все жесткие диски должны быть пустыми (неформатированными);
  - поддерживаемыми типами дисков являются iSCSI, SATA, SAS, SCSI и USB.
- **Пул хранения.** Пул хранения состоит из одного или более физических дисков, которые используются для создания виртуального диска. Неформатированный пустой диск может быть добавлен в пул хранения в любое время.
- **Виртуальные диски.** С точки зрения приложения или пользователя виртуальные диски рассматриваются как то же самое, что и физические диски. Преимущество виртуальных дисков в намного большей гибкости, и они обладают отказоустойчивостью физических дисков со встроенным зеркальным отображением.

Пространства хранения предлагают различные типы настройки (provisioning), которые определяют, сколько пространства используется и как распределять виртуальные диски. Вы можете определять тип производительности и то, что вы готовы применять для его достижения. В повышение или снижение производительности вовлечены многие проектные факторы, такие как скорость, размер и тип диска. Наличие хорошего плана и проекта увеличит производительность системы.

Тип настройки определяется способом распределения пространства для диска и выбранным типа производительности.

- **Thin provisioning (Тонкая настройка).** Тонкая настройка позволяет выделить больше пространства, в то время как использовать только такой объем, который необходим для файлов. Она обеспечивает гибкость, но снижает производительность, т.к. хранилище должно перемещаться и подтягивать дисковое пространство из пула, когда его размер увеличивается.
- **Fixed provisioning (Фиксированная настройка).** Фиксированная настройка резервирует целевое пространство. Например, если вы определяете 40 Гбайт, то это будет максимальный размер, который получит виртуальный диск. Он не может быть большим, чем дисковое пространство пула. Расширить фиксированный размер можно добавлением дополнительных дисков к пулу хранения, и вы заметите влияние на производительность, когда после добавления дисков вы начнете расширять ранее определенный диск. Потребуется небольшое время, чтобы ресурс сделал все необходимое.

Кластеризация внутри виртуальных машин

Когда вы разрабатываете свою стратегию кластеризации для принтеров, открытых файловых ресурсов или Hyper-V, то предоставляете инфраструктуре решение высокой готовности, которое может расти и в которое можно переместить критически важные системы. Для поддержки Windows Server 2012 R2 и гостевой кластеризации вы добавляете следующий уровень HA и увеличиваете скорость восстановления после отказа системы. Высокая готовность требуется не всегда только оборудованием; во многих случаях проблема порождается программным обеспечением, произрастающая из утечек памяти, обновлений ПО либо изменений конфигурации. При запуске приложений, осведомленных о кластерах, как виртуальной рабочей нагрузки, время обхода отказа и интеграция со многими новыми рабочими нагрузками с постоянной доступностью становятся более привлекательными, поскольку взаимодействие потребителей не прерывается.

Чтобы понять рабочую нагрузку, поддающуюся этому типу кластеризации, вы должны запомнить следующее золотое правило: если рабочая нагрузка задумана для кластеризации или ее рекомендуется кластеризировать в целях обеспечения HA или восстановления в аварийных ситуациях (disaster recovery — DR), она может работать в гостевом кластере. В Microsoft сделали рабочие нагрузки Windows Server 2012 и Windows Server 2012 R2 осведомленными о таком виртуальном гостевом кластере, в перечисленных ниже областях:

- постоянно доступные общие файловые ресурсы;
- сервер DHCP;
- SQL Server 2012;

- Exchange Server;
- SharePoint;
- общие файловые ресурсы (стандартное совместное использование файлов);
- службы печати.

Для применения этой технологии вы задействуете модель, включенную в Windows Server 2012 R2: общий файл VHDX. В Windows Server 2012 был введен формат VHDX, который решает потребности хранилища, защиты данных и производительности на дисках большого объема. Когда вы создаете виртуальные гостевые кластеры, то присоединяете файл VHDX к контроллеру SCSI для виртуальной машины, включая совместное использование для создания подключения и представляя файл VHDX как устройство SAS. Таким образом, вы получаете возможность построения инфраструктуры, которая необязательно требует iSCSI, Fibre Channel SAN или хранилища на уровне блоков, но при этом использовать SMB 3.0.

Теперь, когда вы понимаете некоторые базовые строительные блоки, можете вооружиться знаниями возможностей открытого хранилища и кластеризации Windows Server 2012 R2 и заняться настройкой кластера в следующем разделе.

Настройка кластера

В этом разделе мы пройдемся по базовым шагам настройки кластера на основе хостов. В качестве примера мы создадим двухузловой кластер и сконфигурируем его для открытых файловых ресурсов. Классификация открытых файловых ресурсов является великолепной отправной точкой для введения в управление кластером. Требования очень просты. Мы возьмем базовую потребность любого предприятия и немедленно обеспечим высокую готовность.

Для успешного освоения настройки вы должны проработать все последующие разделы.

Конфигурация кластера

Испытательная среда, которую мы собираемся применять для этого примера, довольно проста. Мы имеем два сервера, на которых функционирует Windows Server 2012 R2. Ниже описаны характеристики этих серверов.

Сервер 1 = `Cluster1`

- Локальное хранилище = устройство `C:\` объемом 30 Гбайт
- IP-адрес NIC #1 (основная): 192.168.1.17
- IP-адрес NIC #2 (второстепенная): 192.1681.18

Сервер 2 = `Cluster2`

- Локальное хранилище = устройство `C:\` объемом 30 Гбайт
- IP-адрес NIC #1 (основная): 192.168.1.19
- IP-адрес NIC #2 (второстепенная): 192.1681.20

Кластер для данного примера называется `DemoCluster` и имеет IP-адрес 192.168.1.21.

Для исследования базовых опций кластеризации мы собираемся сосредоточить внимание на кластеризации файловых служб, но уделим больше времени пошаговому прохождению процесса настройки кластера из двух узлов.

При подготовке к построению похожего примера кластера шаги должны быть довольно прямолинейны, и, будем надеяться, что вы уловите ценность настройки и использования кластерных служб для вашей организации. Что касается кворума, обсуждавшегося ранее, для него создан открытый ресурс на отдельном сервере; как уже упоминалось, в качестве кворума может быть задействован открытый файловый ресурс. В этом примере открытый ресурс будет расположен на контроллере домена Active Directory, `BF1`. Открытый ресурс `\\BF1\#Cluster` будет применяться для свидетеля.

Оба сервера имеют по две физических платы NIC. В идеальном случае внутри производственной среды вы предусмотрели бы минимум три NIC, а по возможности даже шесть. Вы должны разделять три типа сетевых потребностей. При наличии пяти и более доступных плат NIC, вы можете объединить две платы NIC для основной службы. Вспомните, что для каждой используемой платы NIC вы должны всегда применять статический IP-адрес. С кластеризацией поддерживается протокол DHCP, но он не идеален или не советуется в большинстве сценариев. В следующем списке приведена типичная конфигурация ролей для плат NIC.

- Роль 1 для NIC: управление кластером и хранилище — не устанавливайте стандартный шлюз.
- Роль 2 для NIC: трафик клиентов (для доступа к виртуальным машинам или приложениям):
  - необходим стандартный шлюз;
  - необходим DNS-сервер.

После того, как платы NIC настроены и вы готовы двигаться дальше, следующий шаг предусматривает назначение хостам имен (выбирайте для серверов имена, описывающие кластеры) и присоединение их к домену Active Directory. Как было указано ранее, серверы, используемые в этом примере, называются `Cluster1` и `Cluster2`.

После присоединения серверов к домену Active Directory понадобится проверить, что на каждом узле кластера установлены службы Remote Desktop (Удаленный рабочий стол) и Remote Management (Дистанционное управление), и поскольку вы собираетесь создавать кластер файлового сервера, требуется роль File Server (Файловый сервер).

Хранилище

Прежде чем мы настроим сам кластер, давайте кратко пересмотрим опции хранилища для кластеров. Вам доступно несколько опций на выбор, и с учетом того, что это является требованием, необходимо определить, какой тип хранилища вы хотите применить. Ниже перечислены типовые опции для общего хранилища:

- iSCSI SAN
- Fibre Channel SAN
- корпуса SAS
- общие папки SMB 3.0 в Windows Server 2012

Мы обсуждали эти компоненты ранее в главе. Одно из больших преимуществ опций хранилища в Windows Server 2012 R2 связано с тем, что поддерживаются все

решения хранилищ, используемые в наши дни, поэтому вы можете задействовать оборудование, которое у вас уже имеется. Вам не придется изменять инфраструктуру хранения. В Windows Server 2012 R2 предоставляется опция построения хранилища с помощью SMB 3.0, если вы не инвестировали средства в специфичное решение хранилища. Как обсуждалось ранее в этой главе, служба SMB 3.0 впервые была представлена в Windows Server 2012 с учетом масштабируемых файловых серверов и Hyper-V, и это стало началом того, что сейчас считается постоянной доступностью. Почитать о службе SMB 3.0 и ознакомиться со способами ее развертывания внутри организации можно по ссылке `http://tinyurl.com/c11SMB30`.

Добавление в кластер первого узла

Первым делом понадобится установить компонент Failover Clustering (Кластеризации с обходом отказа), и сделать это можно двумя способами. Как неоднократно упоминалось в этой книге, для установки указанного компонента можно применить PowerShell. Сведения по установке любых компонентов Windows с помощью PowerShell находятся по ссылке `http://tinyurl.com/c11ClusterInstall`. Для Failover Clustering введите в административной консоли PowerShell следующую команду:

```
Install-WindowsFeature -Name Failover-Clustering
```

Если инструменты администрирования еще не установлены, можете поместить в конец команды переключатель `-IncludeManagmentTools`.

В этом примере мы собираемся добавить с помощью диспетчера серверов роль File Server и компонент Failover Clustering. Следуйте указаниям мастера; поскольку мастер довольно прямолинеен и при добавлении компонента не задает каких-либо вопросов, происходит переход прямо к конфигурированию вашего кластера. Если вам нужна помощь в добавлении ролей и компонентов, обратитесь в главу 7.

После установки компонента Failover Clustering он появится в разделе Apps (Приложения) экрана Start (Пуск), как показано на рис. 11.3.

Рис. 11.3. Раздел Apps экрана `Start`

Дважды щелкните на элементе Failover Cluster Manager (Диспетчер кластеров с обходом отказа). На рис. 11.4 видно, что все основные компоненты, которые необходимы для создания, проверки и управления вашим кластером, собраны в одном окне.

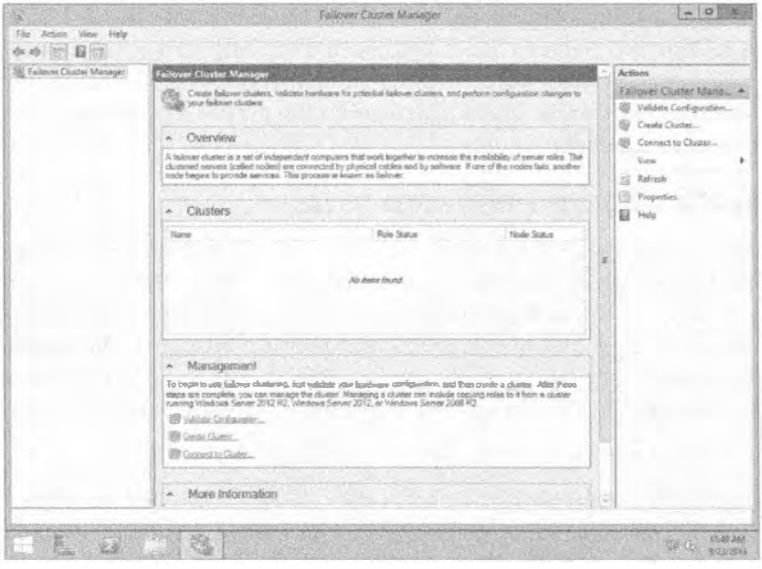


Рис. 11.4. Окно Failover Cluster Manager

Посвятите некоторое время исследованию этой консоли; раскройте раздел More Information (Больше информации) и найдите в веб базовые темы, которые обновлены в консоли. Так как веб-ссылки в консоли часто обновляются, вы обнаружите здесь любые важные изменения или обновления. Исследование консоли диспетчера кластеров очень важно, если вы сталкиваетесь с ней впервые.

Следующая задача предусматривает создание нового кластера; это делается с помощью следующих шагов.

1. Выберите пункт Create Cluster (Создать кластер) в меню Actions (Действия) или щелкните правой кнопкой мыши на Failover Cluster Manager в столбце слева и выберите в контекстном меню пункт Create Cluster, как показано на рис. 11.5.

   Появится экран Before You Begin (Прежде чем начать) и предоставит вам основы, необходимые для завершения этого процесса.

2. Щелкните на кнопке Next (Далее).

   Теперь необходимо ввести имя сервера, который должен быть частью этого кластера.

3. Введите `Cluster1` в качестве имени сервера (рис. 11.6) или можете щелкнуть на кнопке Browse (Обзор) и выбрать желаемый сервер.

4. Щелкните на кнопке Next.

   Когда вы выберете сервер, появится экран, предлагающий запустить проверку с целью выяснения, удовлетворяет ли этот сервер всем требованиям.

Рис. 11.5. Выбор пункта Create Cluster

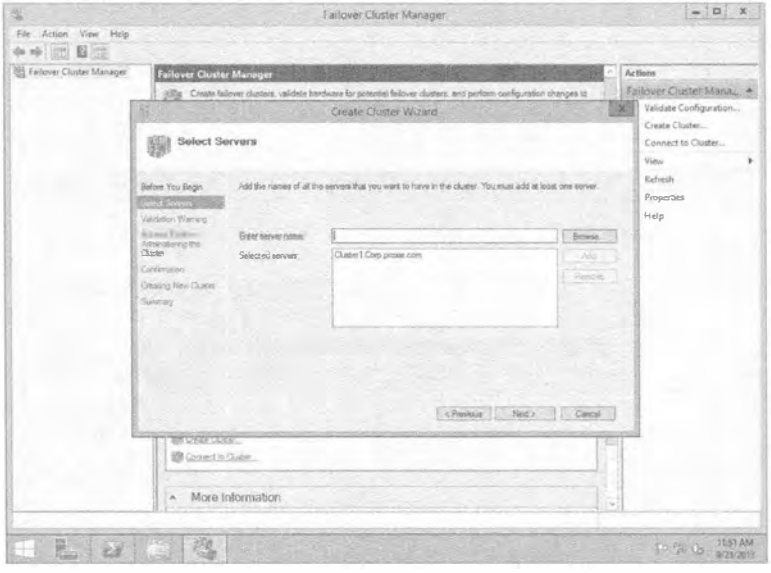


Рис. 11.6. Добавление сервера к кластеру

5. Вы можете выбрать вариант No (Нет), но всегда рекомендуется выбрать Yes (Да), чтобы запустить процедуру проверки. Процесс проверки кластера проведет вас по нескольким шагам, начиная с экрана Before You Begin.

   Следующим отобразится экран Testing options (Опции тестирования), предлагающий перечень тестов, которые вы хотите запустить в отношении этого кластера. По умолчанию выбран прогон всех тестов, что рекомендуется делать как минимум для первого узла в кластере.

6. Щелкните на кнопке Next, чтобы принять стандартный выбор.
7. Подтвердите информацию о том, какой сервер тестировать, и щелкните на кнопке Next для запуска процесса проверки.
   На рис. 11.7 показано окно мастера проверки конфигурации (Validate a Configuration Wizard) с длинным списком компонентов, требуемых для получения успешно функционирующего кластера.
8. После того, как проверка завершена, просмотрите экран Summary (Сводка) мастера (рис. 11.8).

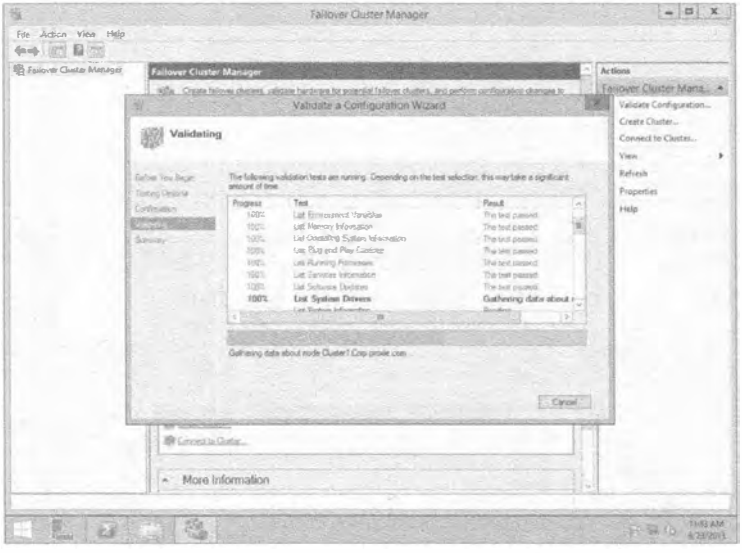


Рис. 11.7. Мастер Validate a Configuration Wizard

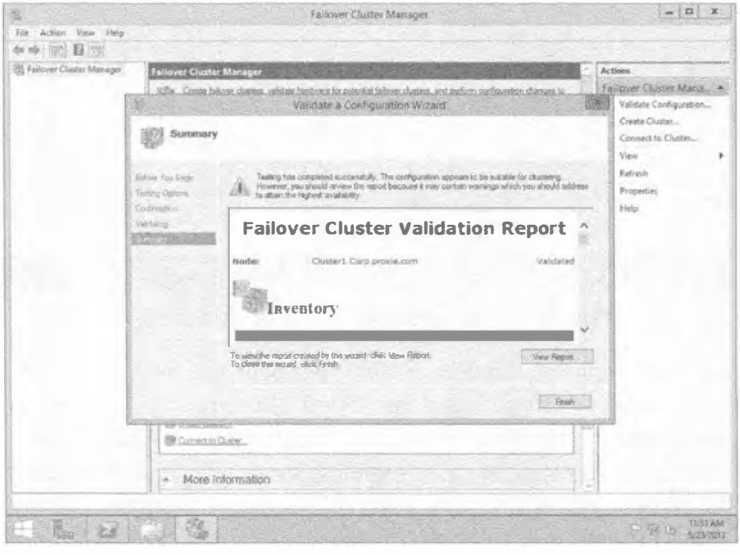


Рис. 11.8. Отчет о проверке

9. Дополнительно можете щелкнуть на кнопке View Report (Просмотреть отчет), чтобы открыть веб-форму, которая позволяет дальнейший анализ элементов отчета.

   На рис. 11.9 представлен экран Inventory (Опись) отчета. Как видите, элементы в столбце Name (Имя) являются гиперссылками, которые предоставят детальные сведения об элементах отчета.

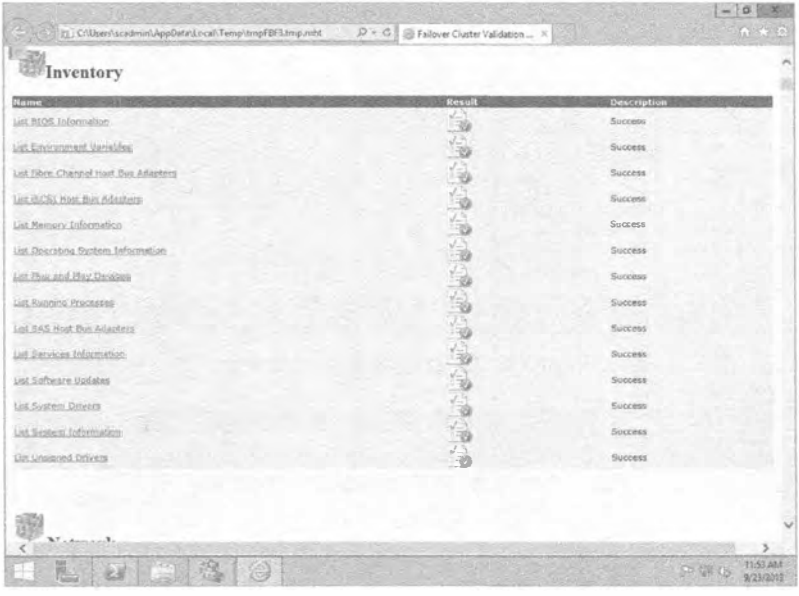


Рис. 11.9. Экран Inventory отчета о проверке

10. После добавления сервера, предназначенного для помещения в кластер, и прохождения процесса проверки необходимо предоставить кластеру имя и IP-адрес. Как показано на рис. 11.10, мы используем имя `DemoCluster`. Имя кластера будет применяться для подключения к нему и администрирования кластера и узлов, на которые ссылается этот центральный IP-адрес.
11. Подтвердите добавление, и мастер добавит совершенно новый кластер.
12. После появления экрана Summary щелкните на кнопке Finish (Готово). В окне диспетчера Failover Cluster Manager отобразится вновь созданный кластер с одним узлом (рис. 11.11).
13. Раскройте папку DemoCluster в левой части экрана и выберите папку Nodes (Узлы).

    На рис. 11.12 видно, что сервер `Cluster1` добавлен в качестве узла и является доступным.
14. Чтобы добавить роль к кластеру, щелкните на ссылке Configure Role (Конфигурировать роль) на экране Summary of Cluster (Сводка по кластеру), как показано на рис. 11.13. Откроется мастер высокой готовности (High Availability Wizard).

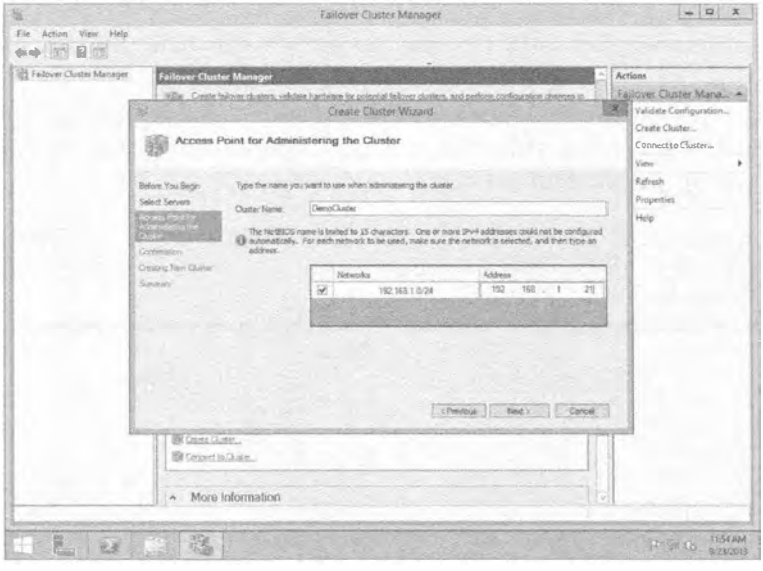


Рис. 11.10. Ввод имени кластера

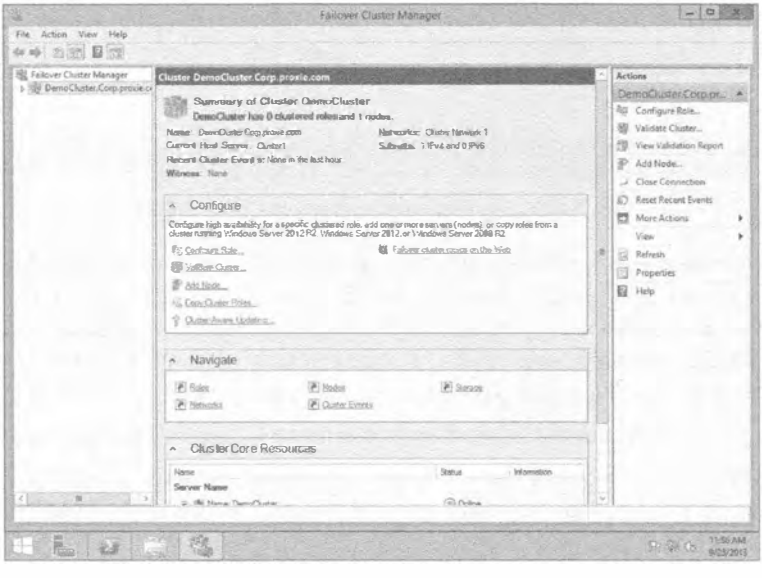


Рис. 11.11. Созданный кластер

Опции для ролей

Каждая из выбиваемых ролей будет требовать различные опции, и обладать собственным набором предварительных условий. Если вы собираетесь исследовать разнообразные рабочие нагрузки, рекомендуем ознакомиться с информацией по ссылке `http://blogs.msdn.com/b/clustering/`. Это основной сайт бригады, занимающейся кластеризацией в Microsoft, и нем содержится масса ресурсов по каждому типу кластерной рабочей нагрузки, который вам может понадобиться настраивать.

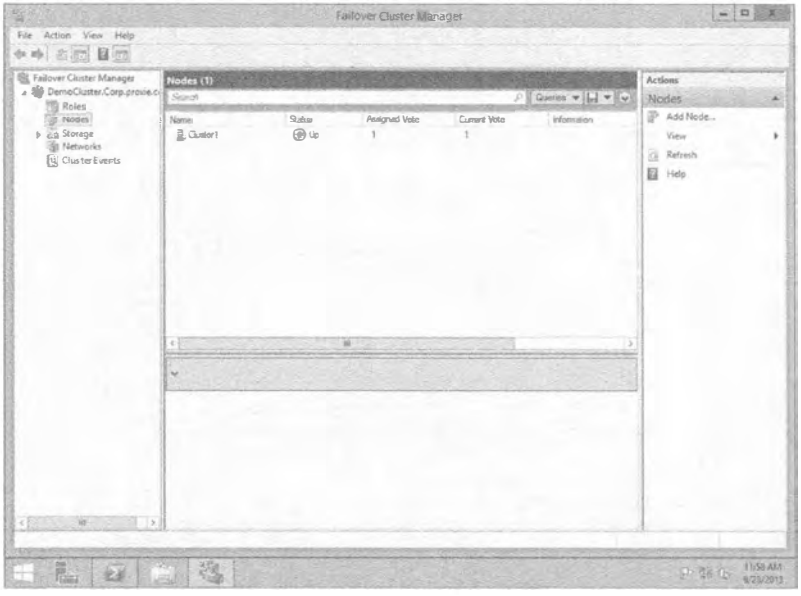


Рис. 11.12. Просмотр добавленных узлов

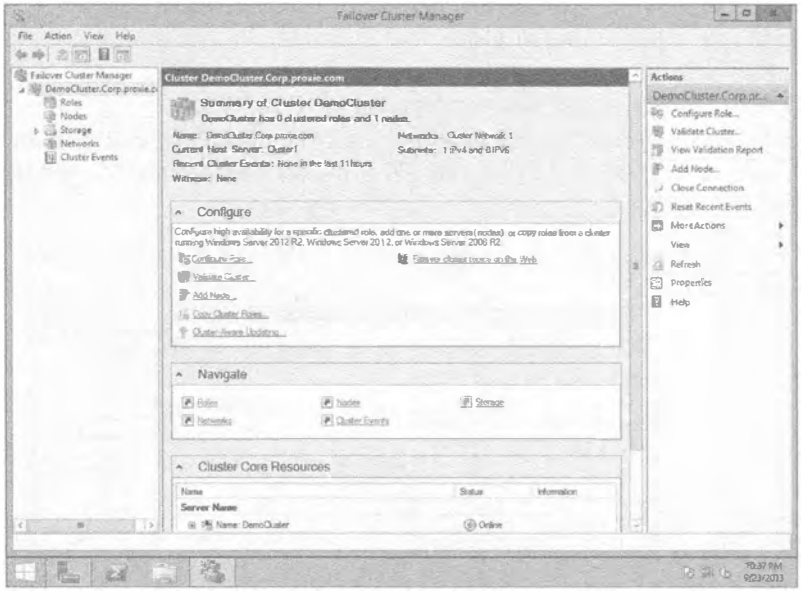


Рис. 11.13. Запуск мастера High Availability Wizard

15. Щелкните на кнопке Next, чтобы пропустить экран Before You Begin, после чего можете выбрать определенную роль для обеспечения высокой готовности.
16. В мастере высокой готовности (High Availability Wizard) выберите в списке роль File Server (Файловый сервер), как показано на рис. 11.14, и щелкните на кнопке Next.

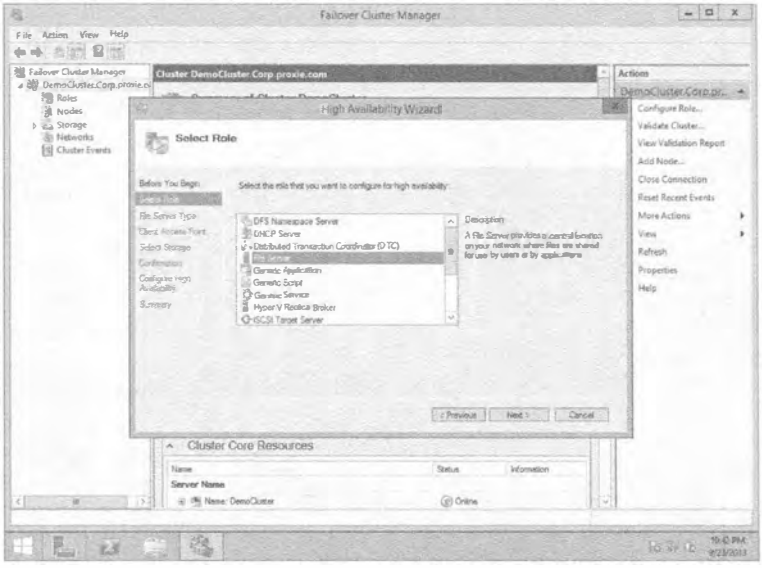


Рис. 11.14. Выбор роли

17. Укажите тип файлового сервера, который необходимо построить. На экране File Server Type (Тип файлового сервера), приведенном на рис. 11.15, видно, что доступны следующие опции:
    - File Server for general use (Файловый сервер для общего пользования) — для базовых открытых файловых ресурсов SMB и NFS;
    - Scale-Out File Server for application data (Масштабируемый файловый сервер для данных приложений) — для DFS и файловых серверов, охватывающих несколько узлов.

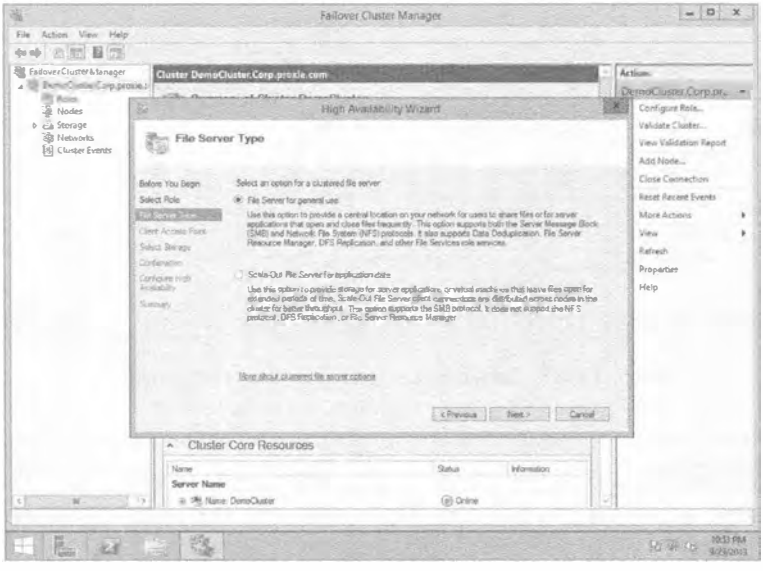


Рис. 11.15. Экран File Server Type

Следующие несколько шагов похожи на настройку кластера. Вы начнете с указания имени, которое клиенты будут применять для доступа к этому файловому кластеру. В этом примере мы будем использовать `DemoFile`.

18. Введите IP-адрес, с которым хотите ассоциировать файловый сервер. В этом примере мы будем применять 192.1681.22.
19. Выберите хранилище, используемое для кластера, щелкните на кнопке Next и подтвердите настроенную конфигурацию.

    После прохождения оставшихся экранов и просмотра сводки высоко доступный файловый сервер появится в папке Roles (Роли) в окне диспетчера кластеров с обходом отказа (рис. 11.16).

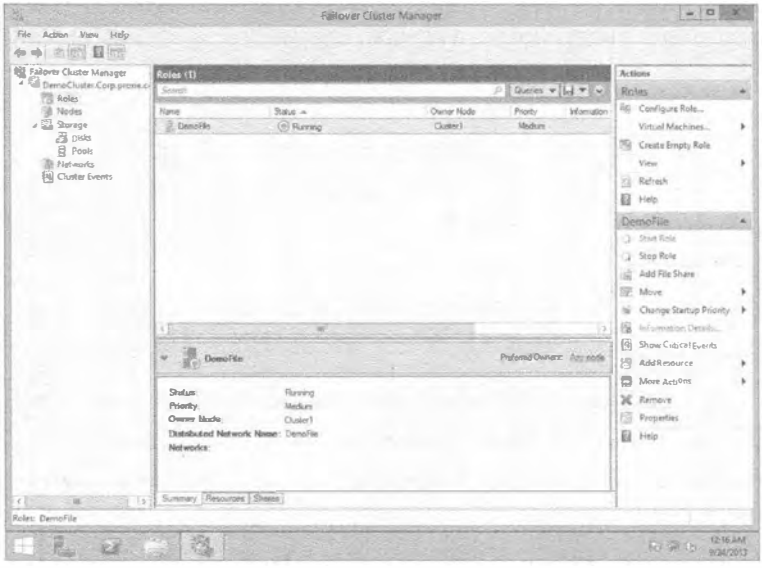


Рис. 11.16. Кластеризованная роль File Server

Добавление в кластер второго узла

Многие администраторы сразу переходят к добавлению второго узла в кластер, пропуская этап проверки работоспособности первого узла. Тем не менее, необходимо удостовериться в том, что первый узел функционирует, выполнив перечисленные ниже действия.

1. Взгляните на сервер `Cluster1` и проверьте, не отображаются ли для него какие-то сообщения об ошибках или значок с восклицательным знаком красного цвета.
2. Проверьте работоспособность хранилища и возможность подтверждения подключений к серверам.
3. Проверьте работоспособность сети и активность всех подключений.
4. Повторно запустите проверочные тесты и получите отчет для пересмотра всех опций.

Могут присутствовать некоторые предупреждения, и вы должны выделить время на оценку каждого из них и удостовериться в отсутствии потенциального влияния на добавление второго узла (или нескольких) к данному кластеру. Каждое сообщение об ошибке или предупреждение внутри отчета сопровождается ссылками и более подробной информацией, поэтому вы успешно позаботитесь о любой возникшей проблеме.

А теперь относительно добавления дополнительного узла к кластеру: важная часть, которая может показаться очевидной, заключается в том, что вы предоставляете службам хоста возможность обхода отказа. Конечно, захватывающе получить свой первый функционирующий кластер, но без дополнительных узлов это просто одинокая служба, выполняющаяся на сервере. Добавление второго узла лучше всего начинать в консоли Failover Cluster Management; для этого в разделе Configure (Конфигурирование) предусмотрена ссылка Add Node (Добавить узел), как показано на рис. 11.17.

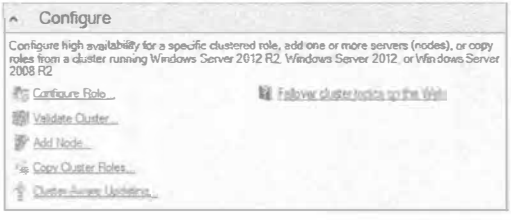


Рис. 11.17. Ссылка Add Node

1. Щелкните на ссылке Add Node (Добавить узел), чтобы запустить мастер.
2. Введите имя сервера; в этом примере им является **`Cluster2`**.

   Будет снова запрошено о необходимости запуска процесса проверки, который приведет к открытию мастера проверки.
3. По крайней мере, для двух первых узлов в кластере вы должны выбирать Run all tests (Запустить все тесты).

   После завершения процесса проверки вы получите еще один отчет о проверке, подобный показанному на рис. 11.9.
4. Удостоверьтесь, что все находится в приемлемом состоянии, и закончите добавление дополнительного узла.
5. Наконец, просмотрите папку Failover Cluster Manager\DemoCluster\Nodes (Диспетчер кластеров с обходом отказа \ `DemoCluster` \ Узлы), чтобы увидеть два добавленных узла.

   Как показано на рис. 11.18, оба узла имеют состояние Up (Работает).

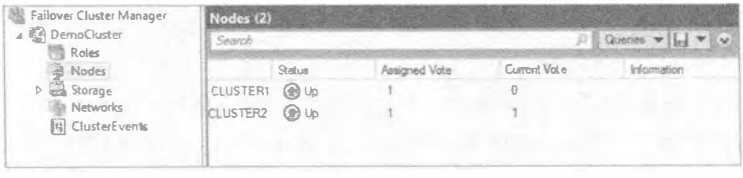


Рис. 11.18. Состояние узлов кластера

Имея оба узла в работающем состоянии, теперь кластер может обеспечивать обход отказа для любой рабочей нагрузки, которую вы хотите поддерживать.

На рис. 11.18 вы могли заметить рядом со столбцом Status (Состояние) два других столбца:

- Assigned Vote (Назначенный голос)
- Current Vote (Текущий голос)

В Windows Server 2012 R2 предоставляется опция конфигурации расширенного кворума, когда вы можете добавлять или отнимать голоса кворума для каждого узла. Изначально всем узлам назначены голоса. Чтобы содействовать решениям по восстановлению в аварийных ситуациях, может понадобиться отнять голоса у определенных узлов. Наиболее распространенной является ситуация, когда имеется географический кластер и нужно удалить голоса у сайта восстановления; если вы планируете делать это, почитайте руководство относительно соображений кворума для DR от Microsoft, которое доступно по ссылке `http://tinyurl.com/c11ClusterDR`.

Настройка инфраструктуры кластера обычно не сложна, хотя это может зависеть от существующих потребностей и служб, которые вы хотите предоставлять посредством кластера. Чем больше служб, узлов и сайтов вы добавляете, тем более сложным становится настройка, но она того стоит. Хосты кластера и гостевые возможности сделают все ресурсы вашей организации высоко доступными, масштабируемыми и восстанавливаемыми в случае отказа сайта.

В следующем разделе мы рассмотрим гостевую кластеризацию, объясним причины, по которым она может понадобиться, и покажем, каким образом в Windows Server 2012 R2 все сделано даже лучше, чем было.

Настройка гостевого кластера

Как ранее уже несколько раз упоминалось, гостевая кластеризация означает расширение кластерных служб внутрь уровня виртуальных машин. Идея в том, чтобы позволить виртуальным машинам иметь внутри себя опции высокой готовности, так что вы можете получить приложение или службу HA, которая расположена наверху кластеризированного набора хостов. В настоящее время вы переходите в исключительно высоко доступный центр данных, обеспечивая всем приложениям физическую или виртуальную постоянную доступность.

Что можно кластеризировать в виртуальных гостях? Все, что угодно, поддерживаемое кластеризацией. Вы можете включить все основные службы и обычные рабочие нагрузки Windows Server, такие как перечисленные ниже:

- Открытые файловые ресурсы и службы, включая DFS
- DHCP Server
- SQL Server
- Exchange Server
- SharePoint
- Internet Information Server

В Windows Server 2008 R2 гостевые кластеры поддерживали стандартное определение работоспособности операционной системы и приложений, а также опции

мобильности приложений. В тот момент не было поддержки для мобильности виртуальных машин, поэтому в случае отказа виртуальную машину приходилось перемешать на другой хост и активизировать. В Windows Server 2012 совершены значительные шаги в сторону восстановления, так что теперь возможно восстановление HA на гостевом уровне. При необходимости кластеризованная служба перезагрузит виртуальные машины, и на уровне хостов, когда требуется восстановление, виртуальная машина перейдет на другой узел.

По существу служба проверки работоспособности ролей (Role Health Service) будет обнаруживать отказ и автоматически проводить восстановление путем перемешения роли этой виртуальной машины на другую виртуальную машину, чтобы позволить операционной системе или приложениям обновиться. Теперь имеется возможность подключения виртуальных машин к хранилищу разных типов, т.е. вы можете подключаться к SAN для получения открытого хранилища через Fiber Channel посредством виртуальных оптоволоконных адаптеров.

Как только служба проверки работоспособности перейдет внутрь фаз мониторинга, она примет первый отказ, и приложения будут перемешены в другой узел. Второй или третий отказ приведут к прекращению работы хоста кластера и перезапуску виртуальной машины. Конфигурирование такого поведения очень просто и требует открытия списка свойств кластеризованной службы, установки второго и третьего отказов и настройки мониторов работоспособности приложений посредством кластеризованной службы.

Настройка гостевого кластера похожа на настройку кластера на основе хостов в том, что компоненты имеют те же самые требования за исключением того, что они могут быть виртуальными. Ниже приведены некоторые соображения по этому поводу.

1. Постройте минимум две виртуальных машины.
2. Создайте два виртуальных сетевых коммутатора, основываясь на имеюшихся требованиях.

   Если необходим доступ к дополнительным ресурсам, понадобится создать дополнительные сети, которые являются специфическими внешними виртуальными коммутаторами.
3. Подключите к виртуальным машинам связанное решение хранилиша, такое как виртуальное хранилище Fiber Channel, iSCSI или SMB.
4. Установите Windows Server 2012 R2 на своей виртуальной машине.
5. Установите компонент Failover Clustering на каждой виртуальной машине в данном кластере.
6. Подключите сеть и хранилище к виртуальным машинам.
7. Запустите мастер проверки конфигурации кластера (Validate Cluster Configuration Wizard) и удостоверьтесь, что получен положительный отчет.

Конфигурирование гостевых кластеров по существу аналогично конфигурированию кластера хостов; необходимо сконфигурировать все те же настройки за исключением роли Hyper-V, поскольку здесь все являются гостями Hyper-V. Если после этого введения в общее хранилище и кластеризацию вы чувствуете себя более осведомленным, настоятельно рекомендуем заглянуть в блог Clustering and High-

Availability (Кластеризация и высокая готовность) в TechNet, который доступен по ссылке `http://blogs.msdn.com/b/clustering/`.

Резюме

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?

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?

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?

Глава 12

Хранилище Windows 2012 R2: пространства хранения, возможности SAN и улучшенные инструменты

Администраторы, которые имели возможность поработать какое-то время с пространствами хранения (Storage Spaces) в Windows Server 2012, наверняка по достоинству оценят изменения, внесенные в Windows Server 2012 R2. Но прежде чем приступить к их обсуждению, давайте ознакомимся с краткой сводкой по Storage Spaces, предназначенной для тех, кто не еще не имел дела с этим средством.

Средство Storage Spaces было представлено в Windows Server 2012 как встроенный компонент. Вспомните, что это не RAID, но кое-что новое, что было спроектировано для полноценного корпоративного использования. Базовая функция Storage Spaces заключается в том, чтобы дать возможность взять просто группу дисков (just a bunch of disks — JBOD) и сконфигурировать их в пуле. Отсюда вы можете создавать виртуальные диски (действительное пространство хранения) и тома с устойчивостью к отказам разнообразных уровней. Такой тип конфигурации обеспечивает высокую гибкость.

Представьте себе отсутствие обязательства инвестировать в крупную дорогостоящую сеть хранения данных (storage area network — SAN) или в специальное обучение, которое администраторы должны были бы пройти, чтобы конфигурировать и обслуживать эту сеть. Основной целью Storage Spaces является предоставление рентабельного решения для хранилища с непрерывным доступом к данным. Пространства хранения и пулы спроектированы с возможностью увеличения по запросу.

Ниже приведен список лишь некоторых возможностей в Storage Spaces, входящих в состав Windows Server 2012:

- оперативная настройка;
- устойчивость к отказам (зеркальное отображение и контроль по четности);
- интеллектуальное исправление ошибок;
- поддержка множества владельцев;
- интеграция с CSV для возможности обработки масштабированных сценариев.

В этой главе вы изучите следующие темы:

- создание пула хранения на виртуальном диске;
- создание дополнительного хранилища на виртуальном диске;
- применение приемов дедупликации для сокрашения размера файлов.

Что нового в хранилище Windows Server 2012 R2?

Поскольку эта книга посвящена Windows Server 2012 R2, мы покажем, что нового появилось в хранилище. Разработчики из Microsoft включили в Storage Spaces технологию, которую ранее можно было встретить только в дорогостоящих массивах хранения. Эта технология подробно рассматривается в последующих разделах.

Многоуровневые пространства хранения

В современном мире хранилищ существует несколько классификаций дисков, в том числе последовательная расширенная технология подключения (Serial Advance Technology Attachment — SATA), последовательно присоединенное SCSI-устройство (Serial Attached SCSI — SAS), твердотельный накопитель (Solid State Drive — SSD) и оптоволоконный канал (Fibre Channel). Выбор правильного типа хранилища для работы очень важен. Например, если вам необходим файловый сервер, то SSD не является удачным выбором. Накопители SSD были спроектированы для обеспечения высокой скорости, но не емкости, и в связи с тем, что файловые серверы обычно нуждаются в емкости, а не скорости, в этом случае намного лучше может подойти диск SATA, который проектировался для большей емкости, нежели скорости.

В Windows Server 2012 R2 можно иметь максимум два уровня хранения, в сущности, быстрый уровень и медленный уровень. На быстром уровне автоматически используется SSD, а на медленном — SATA. По-настоящему хорошо здесь то, что администратор не должен решать заранее, где размещать данные. Службы управления уровнями хранения (Storage Tiers Management Service) автоматически проанализирует данные на дисках в срезах по 1 Мбайт. Она имеет две категории для назначения: горячие точки (hot spot) и холодные точки (cold spot). Горячие точки — это области данных, доступ к которым производится часто; здесь выдвигается предположение о том, что поскольку это активные данные, они являются своего рода "горячей темой". Холодные точки представляют собой противоположность: данные, доступ к которым осуществляется нечасто. После анализа горячие точки будут переведены на уровень SSD, а любые идентифицированные холодные точки будут назначены уровню SATA.

По умолчанию анализ происходит ежедневно в 1:00, но вы можете сконфигурировать это по своему усмотрению (рис. 12.1). Но если файл нуждается в нахождении на быстром уровне все время, администратор может "закрепить" такой файл на этом уровне.

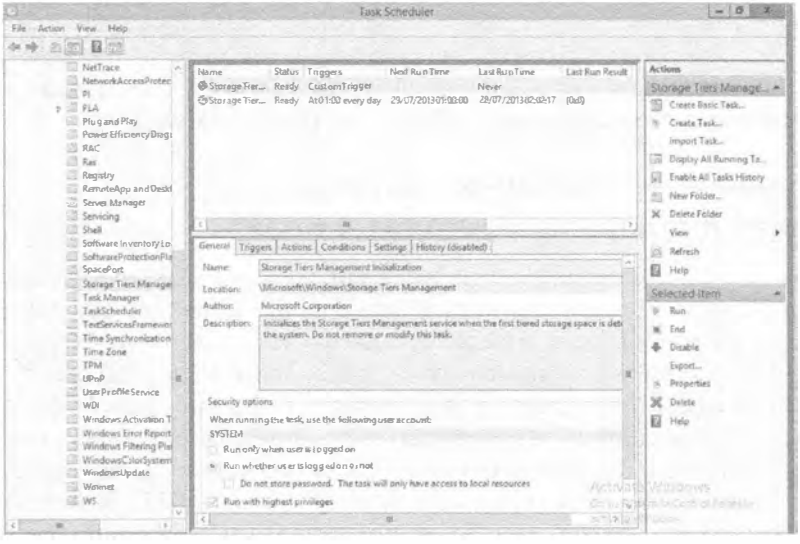


Рис. 12.1. Служба Storage Tiers Management в планировщике задач

Кеш с обратной записью

Под *кешем с обратной записью* понимается способ записи данных на диск. Данные сначала записываются в кеш, и будут храниться в нем до тех пор, пока их не потребуется перезаписать; в этот момент они сбрасываются на диск и фиксируются. В общем случае запись и хранение данных в кеше обеспечивает лучшую производительность и рассматривается как еще один тип памяти. Если приложение записывает в кеш, оно может быстро освободить свой обработчик ввода-вывода и возвратиться к выполнению других задач. Определенным рабочим нагрузкам традиционно не нравится кеширование с обратной записью, потому что когда приложение записывает данные, они должны быть записаны на диск во избежание разрушения. Например, Hyper-V требует сквозной записи. Многоуровневое хранилище может применяться в сочетании с виртуальным диском (в этом случае не с файлом VHD/VHDX, имеющим отношение к Hyper-V и виртуальным машинам, а виртуальным диском с точки зрения Storage Spaces), чтобы поглощать любые выбросы в операциях записи. Быстрый уровень затем может использоваться для преодоления выброса и разрешения Hyper-V применять кеширование с обратной записью.

Распараллеленное восстановление

В случае отказа диска в традиционном массиве RAID, при наличии *горячего резерва* (диск, который может немедленно принять работу отказавшего диска в массиве RAID), этот горячий резерв вступает в игру и массив RAID начнет воссоздание данных на отказавшем диске. Во время воссоздания влияние на производительность

дисковой подсистемы неизбежно, т.к. все данные записываются на единственный диск. Процесс распараллеленного восстановления в Storage Spaces несколько отличается. Если диск отказывает, оставшиеся работоспособные диски, которые имеют подходящую емкость, получают права владения данными, сохраненными на отказавшем диске, и будут обслуживать запросы от пользователей по всем доступным накопителям. Поскольку теперь помощь оказывают все диски, влияние на производительность отсутствует. Процесс восстановления может задействовать горячий резерв или же администратор может заменить отказавший диск новым, который в фоновом режиме постепенно возвратится в пространство хранения.

Низкоуровневое усовершенствование: встроенная поддержка секторов 4 Кбайт

Первоначально жесткие диски использовали формат 512 байтов на сектор, и это налагало ограничения на размер и производительность хранилища. Учитывая постоянно растущие потребности в емкости и скорости, назрела необходимость в изменениях, и в течение всего нескольких лет стандартом стали диски с секторами 4 Кбайт. Тем не менее, программное обеспечение (такое как утилиты файловой системы, операционные системы и механизмы баз данных) не обязательно быстро подхватили это изменение. Большинство производителей устройств поставляли диски с секторами 4 Кбайт, но в целях совместимости эмулировали 512-байтовые секторы. Очевидно, это сопровождается некоторыми накладными расходами, поскольку сектор 4 Кбайт целиком считывается в память, модифицируется и затем записывается обратно. Так как происходит определенная степень манипулирования, имеется также влияние на производительность, которое в данном случае вполне приемлемо.

Благодаря встроенной поддержке секторов 4 Кбайт, индустрия хранения данных больше не эмулирует 512-байтовые секторы, а это значит, что влияние на производительность устранено.

В следующем списке перечислены некоторые приложения и сценарии, которые становятся доступными при поддержке секторов 4 Кбайт:

- возможность установки Windows на диск с секторами 4 Кбайт и загрузки с него без необходимости в эмуляции (собственный диск 4 Кбайт);
- новый файловый формат VHDX;
- полная поддержка Hyper-V;
- резервное копирование Windows;
- полная поддержка со стороны файловой системы New Technology File System (NTFS);
- полная поддержка со стороны новой файловой системы ReFS (Resilient File System — отказоустойчивая файловая система);
- полная поддержка со стороны Storage Spaces;
- полная поддержка со стороны средства Windows Defender (Защитник Windows);
- поддержка входящих приложений.

Поддержка UEFI BIOS позволяет работать с дисками GPT

Главные загрузочные записи (master boot record — MBR) — это специальные области, расположенные в начале разделенного пространства на диске. Они содержат информацию о внутренней структуре разделов и связанный загрузочный код, который позволяет операционной системе запуститься. Запись MBR хранит свой адрес блока в 32-битном формате. Первоначально диск с 512-байтовыми секторами и адресом блока в 32 бита был ограничен объемом 2 Тбайт. Вполне очевидно, что это больше не является приемлемым. Таким образом, индустрия двигается в сторону секторов 4 Кбайт, и теперь диски обладают максимальной емкостью 16 Тбайт. Все выглядит так, как будто мы достигли цели, но с учетом современной инфраструктуры мы можем иметь дело с петабайтами данных, поэтому терабайты вряд ли справятся с этим.

Таблица разделов GUID (GUID Partition Table — GPT) предоставляет 64-битную структуру адресации. На диске с 512-байтовыми секторами можно иметь 9,4 Збайт (9 444 732 965 739 290 426 880) данных. В настоящее время GPT поддерживает максимальный размер диска и раздела, равный 8 Збайт.

Если вы приготовились преобразовать свои диски в GPT, то вы совершенно правы! Но будьте осторожны; не все операционные системы поддерживают загрузку из разделов GPT, используя стандартную систему BIOS. Ознакомьтесь с материалом по следующей ссылке:

```
http://ru.wikipedia.org/wiki/Таблица_разделов_GUID
```

Унифицированный расширяемый интерфейс прошивки (Unified Extensible Firmware Interface — UEFI) спроектирован как прямая замена унаследованной системы BIOS. По существу он делает ту же самую работу, но добавляет такую функциональность, как диагностика и восстановление компьютеров с развернутыми операционными системами. Интерфейс UEFI разработан для поддержки загрузки из разделов GPT, и Windows Server 2012 R2 полностью поддерживает UEFI BIOS.

Утилита CHKDSK стала более интеллектуальной

На протяжении многих лет утилита CHKDSK была одним из главных инструментов. Она входила в состав многочисленных поколений DOS и Windows, и замечательно видеть этот инструмент модернизированным.

Одной из крупнейших проблем, с которыми сталкивалась утилита CHKDSK до ее модернизации, была ее прямая связь с количеством файлов внутри тома. Большее число файлов требовало большего времени на ее выполнение. Еще одна причинявшая постоянное беспокойство сложность заключалась в том, что когда CHKDSK обнаруживала проблему, она обычно размонтировала том, повторно все сканировала, обнаруживала проблему снова и только затем ее исправляла. Несложно представить, что на крупных томах это занимало длительное время, а при современной культуре постоянной готовности простой попросту неприемлем.

Код инструмента CHKDSK был модернизирован, и модель работоспособности NTFS также была перепроектирована. Мы обсудим эти модернизации далее, но они, в сущности, были обусловлены тем, что утилита CHKDSK с прежними возможностями больше не была нужна.

Онлайновое самолечение

Хотя эта возможность файловой системы NTFS существовала со времен Windows Vista, количество проблем, которые она способна обнаружить и исправить, значительно увеличилось. В свою очередь, это снизило фактическую потребность в CHKDSK, поскольку большинство проблем удавалось решить с помощью онлайнового самолечения. Поддерживая самолечение, том не обязан переходить в отключенное состояние.

Онлайновая верификация

В Windows Server 2012 действительное повреждение можно подтвердить. Иногда ошибки возникают из-за проблем с памятью, но это не обязательно означает повреждение диска. Теперь, благодаря онлайновой верификации, вы можете активизировать проверку. Для выполнения этой проверки драйвер файловой системы запускает новую службу под названием Spot Verifier (Точечный верификатор), как показано на рис. 12.2. Она функционирует в фоновом режиме и не оказывает влияния на производительность системы.

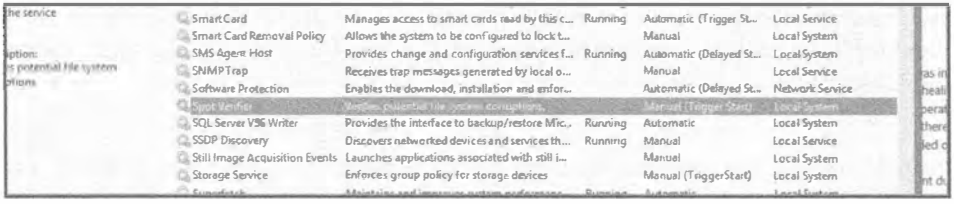


Рис. 12.2. Служба Spot Verifier

Онлайновая идентификация и ведение журналов

После обнаружения реальной проблемы запускается онлайновое сканирование файловой системы. Это сканирование рассчитано на выполнение в сочетании с операционной системой и будет запускаться только во время простоя системы или в период ее низкой загрузки. Найденная проблема фиксируется в журнале для последующего автономного исправления.

Точное и быстрое исправление

Поскольку в журнале была зафиксирована информация о местах возникновения проблем, вам не придется заново сканировать всю файловую систему в начале автономного процесса. По существу это означает, что когда вы переведете том в автономный режим для исправления ошибок, такой процесс займет секунды, а не потенциально часы. Быстрое исправление называется Spotfix. Если вы применяете общие тома кластера (Cluster Shared Volume — CSV), никакого простоя не будет, и тома оказываются постоянно готовыми.

Благодаря этим новым усовершенствованиям, исполняющая среда CHKDSK больше не зависит от количества файлов, а только от числа повреждений данных. Учитывая возможность исправления настолько многих проблем в онлайновом режиме (при постоянно онлайновом томе CSV), утилита CHKDSK становится менее востребованной. На рис. 12.3 показаны новые опции, которые доступны в CHKDSK.

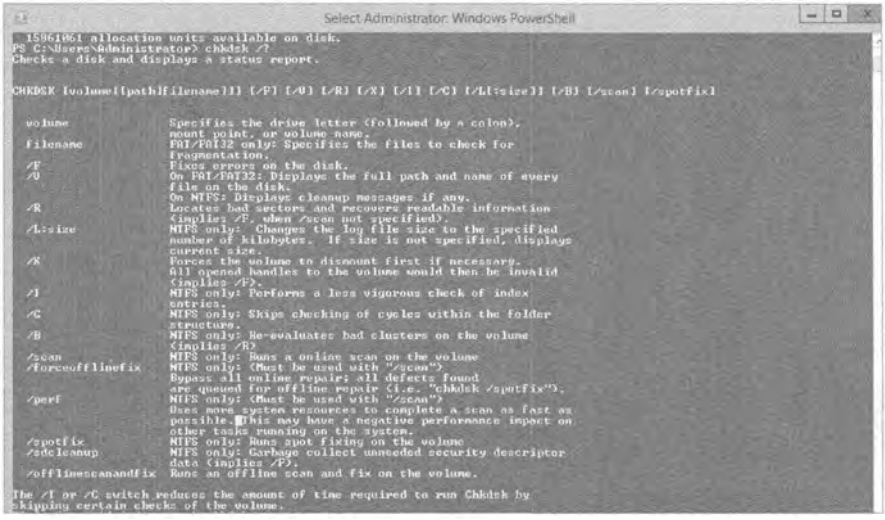


Рис. 12.3. Новые опции CHKDSK

Новыми опциями являются /scan, /forceofflinefix, /perf, /spotfix, /sdcleanup и /offlinescanandfix. Как видите, они напрямую относятся к описанной ранее новой модели работоспособности.

В этот момент мы должны подчеркнуть, что еще одной целью модернизации CHKDSK была необходимость сделать так, чтобы пользователи оставались информированными о любом повреждении. Частично причина заключалась в том, чтобы прекратить интенсивные запуски CHKDSK для верификации файловой системы со стороны пользователей и администраторов; теперь в этом просто нет нужды. Система использует центр действий (Action Center), включенный в Windows, чтобы уведомлять пользователя или администратора о разрушении данных в файловой системе и рекомендовать какое-то действие. На рис. 12.4 представлены результаты примера онлайнового сканирования.

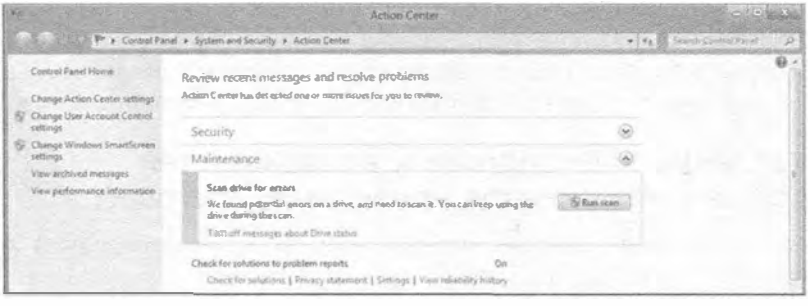


Рис. 12.4. Сообщение об онлайновом сканировании в Action Center

На рис. 12.5 видно, что если проблема не может быть устранена в онлайновом режиме, то Action Center предложит перезапустить компьютер, чтобы исправить ее автономно.

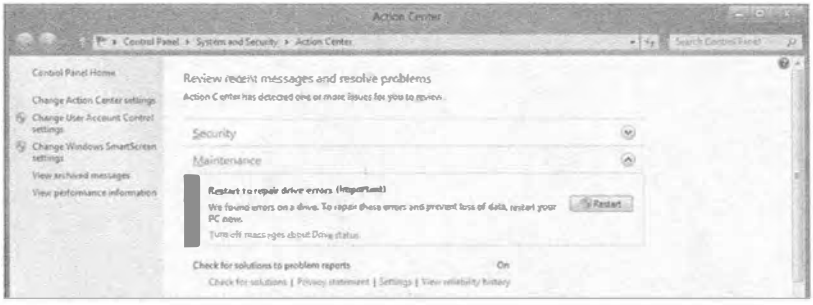


Рис. 12.5. Сообщение об автономном сканировании в Action Center

Пространства хранения в Windows Server 2012 R2

Концепция пространств хранения (Storage Spaces) в Windows Server 2012 R2 по существу совпадает с той, которая была воплощена в Windows Server 2012 и обсуждалась в начале этой главы. Исключениями являются упомянутые ранее новые средства, которые сейчас будут рассмотрены более подробно.

Повторное использование технологии из облачных служб Microsoft

В Microsoft запускают множество облачных служб. Наверняка вы слышали о Windows Azure или Office 365. Представьте себе все уроки, которые в Microsoft извлекли во время развертывания, настройки и выполнения ежедневных операций в этих средах. Также подумайте о том, что если бы Microsoft пришлось приобрести многомиллионные сети хранения, чтобы справиться с постоянно растущей потребностью в наличии хранилища в облачных средах, то насколько они были бы урезанными в контексте облачной среды.

Все накопленные знания разработчики из Microsoft применяют к выпускаемым новым технологиям, в том числе и к Storage Spaces. Они нуждались в рентабельном способе увеличения хранилища и поддержке основных возможностей, присущих сетям хранения данных, вот почему и появилась технология Storage Spaces. По мере развития облачных служб вы будете наблюдать улучшения в Storage Spaces наподобие тех, что вы видели между выпусками Windows Server 2012 и Windows Server 2012 R2.

Предоставление SAN-подобных возможностей посредством инструментов управления Microsoft

Одной из по-настоящему интересных особенностей технологий компании Microsoft является знакомый интерфейс, предлагаемый для управления ее программными продуктами. Обычно доступны два варианта: графический пользовательский интерфейс и PowerShell.

Применение графического пользовательского интерфейса

Несмотря на то что консоль управления Microsoft (Microsoft Management Console — MMC) — традиционная консоль для большинства оснасток управле-

ния — по-прежнему существует, большая часть средств внутри Windows Server 2012 R2 управляется через диспетчер серверов (Server Manager), окно которого показано на рис. 12.6. Область Storage Pools (Пулы хранения) по умолчанию включена на всех системах и может быть найдена в виде подкомпонента роли File and Storage Services (Службы файлов и хранилища).

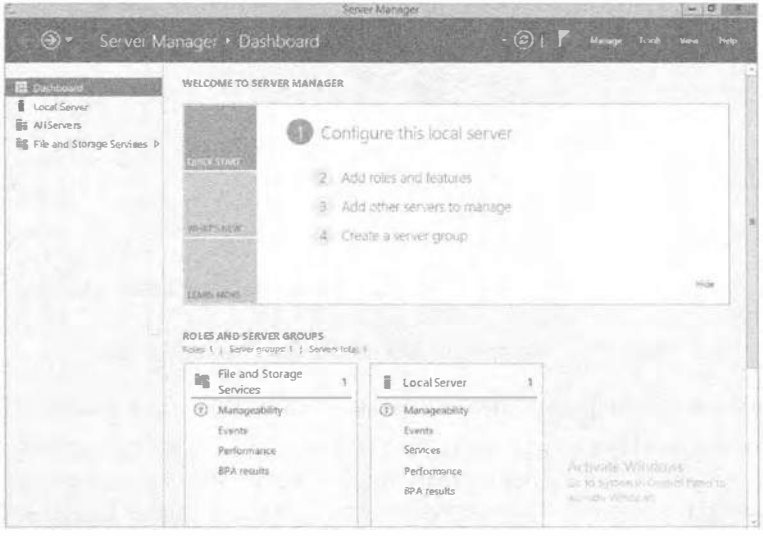


Рис. 12.6. Роль File and Storage Services в диспетчере серверов

Выбрав элемент меню File and Storage Services, вы увидите все связанные с ним опции, в том числе и Storage Pools (рис. 12.7). Щелчок на Storage Pools приводит к отображению основной конфигурации (рис. 12.8).

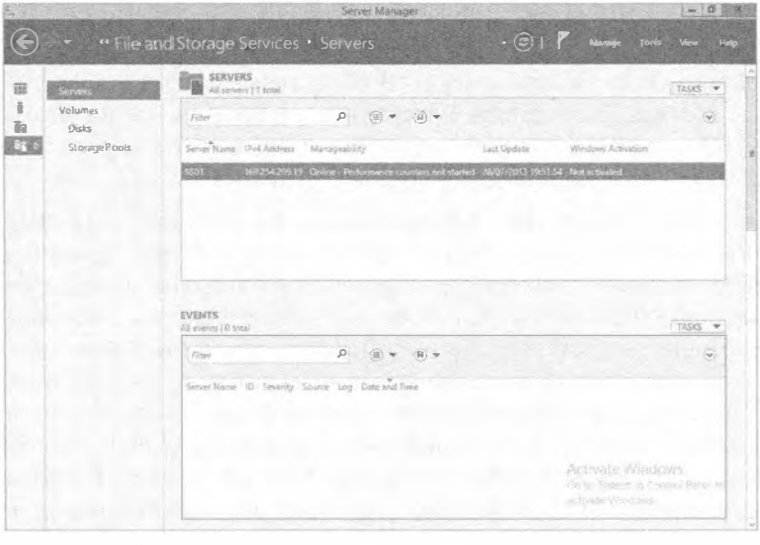


Рис. 12.7. Опции File and Storage Services

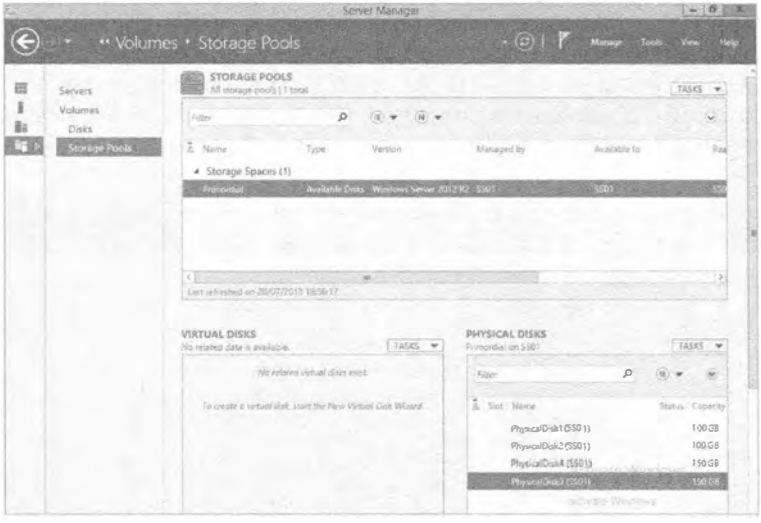


Рис. 12.8. Конфигурация компонента Storage Pools

Окно с основной конфигурацией делится на три главных области.

- **Storage Pools (Пулы хранения).** Эта область содержит раздел под названием Storage Spaces (Пространства хранения), в котором перечислено пространство Primordial (Первичное). По умолчанию все диски, которые не назначены другому пулу, назначаются пулу Primordial. Поработав с пространствами хранения, вы заметите, что пул Primordial перестанет отображаться после того, как все диски окажутся назначенными.

  Как видите, пока что другие назначенные или сконфигурированные пулы отсутствуют. В правом верхнем углу этой области, в раскрывающемся меню Tasks (Задачи), имеется опция для создания нового пула хранения. Мы этим займемся далее в главе, так что пока не думайте о ней. На пуле Primordial можно щелкнуть правой кнопкой мыши и просмотреть его свойства.

- **Virtual Disks (Виртуальные диски).** В области Virtual Disks представлены тома, которые вы будете создавать внутри пула хранения. Вспомните, что это не файл VHD или VHDX. Внутри пула Primordial создать виртуальный диск невозможно; сначала должен быть создан пул хранения.

- **Physical Disks (Физические диски).** Физические диски — это диски, которые доступны пространствам хранения для назначения пулам хранения. В каждый момент времени диск может быть назначен только одному пулу. Если вы щелкнете правой кнопкой мыши на диске в этом списке, то в открывшемся контекстном меню вы получите опцию переключения (включения/выключения) индикатора устройства (переключение индикаторов устройств помогает при выяснении, какие диски работают в массиве физического хранилища); это будет работать, только если используемое хранилище является совместимым со службами корпусов SCSI (SCSI Enclosure Services — SES). Службы SES также функционируют, когда устройство терпит отказ, и взаимодействуют с компонентом Storage Spaces, чтобы уведомить администратора о том, что произошло.

Использование PowerShell

Как уже упоминалось, для быстрой настройки Storage Spaces можно применять командлеты PowerShell. Некоторые администраторы при обслуживании серверов предпочитают работать в среде командной строки. Лично нам нравится смешанный подход.

В Windows Server 2012 R2 имеется новый модуль PowerShell по имени `Storage`, который содержит все командлеты PowerShell, необходимые для работы с компонентом Storage Spaces.

В Windows Server 2012 и последующих версиях модуль PowerShell автоматически импортируется, когда вы пытаетесь вызвать командлет, который является частью этого модуля. Чтобы просмотреть командлеты, доступные в модуле `Storage`, откройте окно PowerShell с повышенными полномочиями и введите **`get-command -module Storage`**. В Windows Server 2012 R2 доступны 102 командлета, правда, не все они относятся к пулу хранения.

К счастью, вы уже знакомы с PowerShell и понимаете его структуру "глагол/существительное". Если вы определяете, какие командлеты имеют отношение к тому, что было показано на рис. 12.8, это значит, что вы ищете командлеты, связанные с физическими дисками, виртуальными дисками и пулами хранения. Чтобы упростить идентификацию командлетов для каждого аспекта, введите **`get-command *StoragePool* |where {$_.modulename -eq "Storage"}`** и проанализируйте результат. На рис. 12.9 показан ожидаемый вывод; каждый командлет имеет собственный набор опций, которые можно просмотреть с помощью команды **`get-help имя_командлета`**.

```
PS C:\Users\Administrator> get-command *StoragePool* |where {$_.modulename -eq "Storage"}

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Function        Get-StoragePool                                    Storage
Function        New-StoragePool                                    Storage
Function        Remove-StoragePool                                 Storage
Function        Set-StoragePool                                    Storage
Function        Update-StoragePool                                 Storage
```

Рис. 12.9. Командлеты из модуля `Storage`

Мы не собираемся вдаваться здесь в особые подробности, но продемонстрируем вывод из пары командлетов. Например, введите **`get-storagepool`** и изучите вывод. Теперь введите **`get-storagepool |fl *`** и обратите внимание на разницу. `FL` — это псевдоним PowerShell для `Format-List`, а опция `*` определяет, какие свойства необходимо отобразить, в данном случае — все свойства. Вывод показан на рис. 12.10. Повторите такие же команды для командлетов `get-physicaldisk` и `get-virtualdisk` и просмотрите их вывод.

Создание пространства хранения

Storages Spaces является исключительно мощным компонентом, и, как упоминалось ранее, пространства хранения привносят множество преимуществ в организацию. Их также легко конфигурировать. Никакого специализированного обучения для этого не требуется.

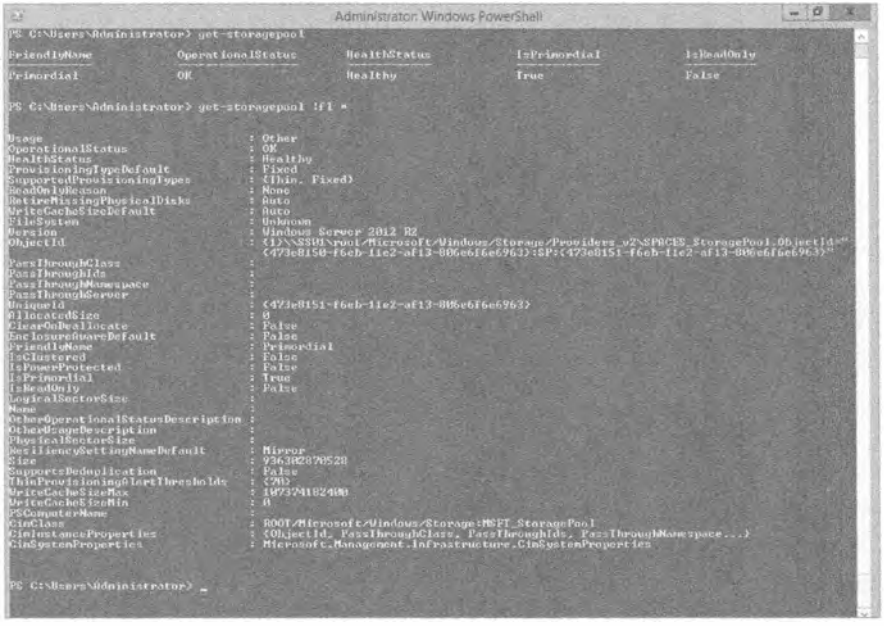


Рис. 12.10. Пример вывода из командлета `get-storagepool`

На следующих нескольких страницах мы обсудим процесс создания пространства хранения и покажем, насколько в действительности это легко делается. Общий процесс выглядит следующим образом.

1. Получение свободных физических дисков.
2. Создание пулов хранения.
3. Создание виртуальных дисков.

Мы продемонстрируем создание пула хранения с помощью графического пользовательского интерфейса и PowerShell. Однако сначала необходимо кратко представить испытательную среду. Мы имеем одиночный сервер с несколькими физическими дисками, двумя дисками SAS по 100 Гбайт, двумя дисками SAS по 150 Гбайт и одним диском SATA объемом 300 Гбайт.

Создание пула

При создании пула хранения вы должны решить, какие физические диски назначить этому пулу. Важно думать в терминах того, какой пул будет использоваться, и, с учетом наличия теперь средства многоуровневого хранения, какой тип дисков должен стать частью пула. Чтобы создать пул, выполните перечисленные ниже шаги.

1. Откройте диспетчер серверов и выберите в меню File (Файл) пункт Storage Services (Службы хранения).
2. Выберите элемент Storage Pools (Пулы хранения).
3. Щелкните правой кнопкой мыши на пуле Primordial и выберите в контекстном меню пункт New Storage Pool (Создать пул хранения), как показано на рис. 12.11. Откроется мастер создания пула хранения (New Storage Pool Wizard).

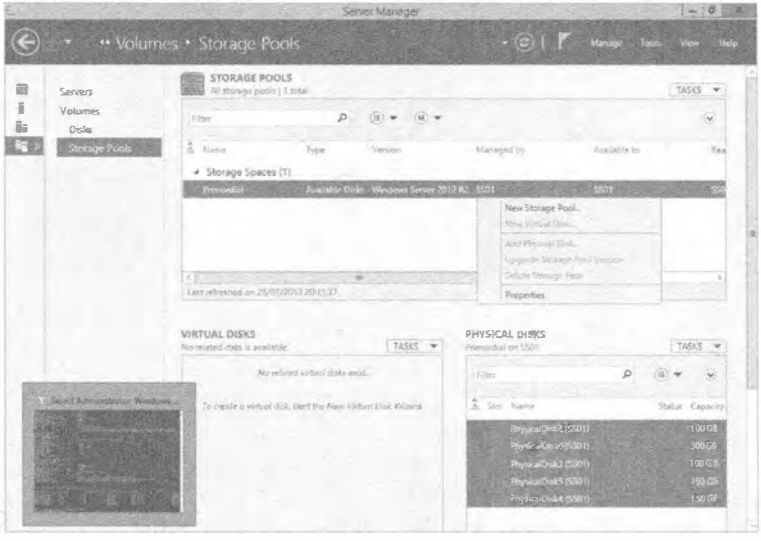


Рис. 12.11. Создание нового пула хранения

4. Щелкните на кнопке Next (Далее), чтобы пропустить экран приветствия.
5. На экране Storage Pool Name (Имя пула хранения), приведенном на рис. 12.12, вы должны назначить пулу хранения имя; в данном случае **Test**. При желании можно добавить описание.
   В нижней половине окна вы увидите, что для доступного дискового пула применяется пул Primordial. Далее потребуется выбрать физические диски в пуле.
6. В этом примере выберите все диски (рис. 12.13).

   Обратите внимание на возможность выбора дисков ATA и SAS. На рис. 12.14 представлены опции Allocation (Выделение): Automatic (Автоматическое), Hot Spare (Горячая замена) или Manual (Ручное).

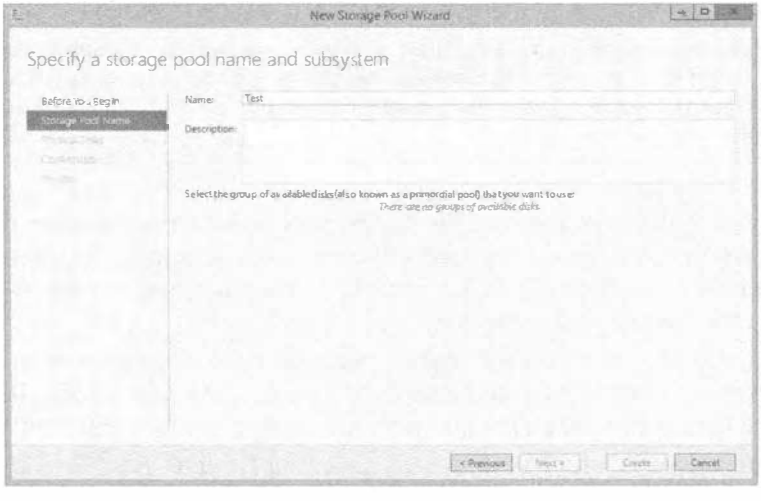


Рис. 12.12. Именование пула хранения

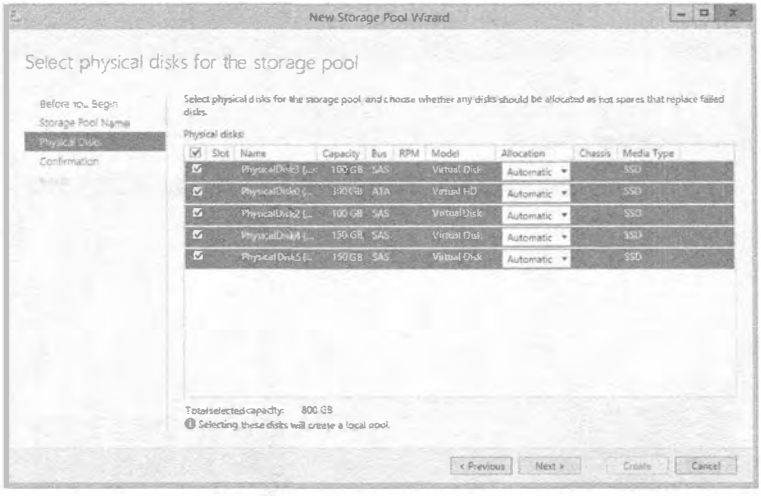


Рис. 12.13. Выбор дисков для пула хранения

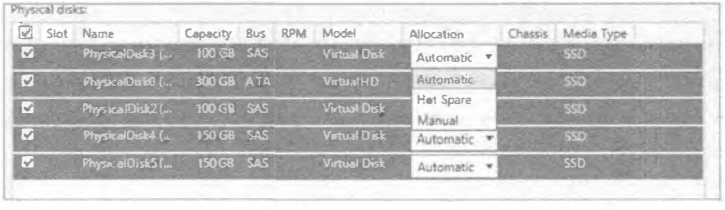


Рис. 12.14. Опции выделения дисков

7. В данном примере используется выделение Automatic. Для продолжения щелкните на кнопке Next.

Смешивание дисков, выделяемых вручную и автоматически

При выделении дисков вы можете иметь в пуле множество горячих замен, но не должны смешивать диски, выделяемые вручную и автоматически. Выбор опции Automatic на этом экране будет автоматически балансировать пул между горячими заменами и полезной емкостью.

Назначив опцию выделения диска, вы не сможете изменить ее с ручного на автоматическое внутри графического пользовательского интерфейса, но можете сделать это в PowerShell. На рис. 12.15 показан пример идентификации и изменения типа выделения диска.

8. Наконец, как и со всеми мастерами, вы получаете шанс пересмотреть выбранные опции, прежде чем фиксировать изменение (рис. 12.16). Щелкните на кнопке Create (Создать), когда будете удовлетворены выбранными вариантами.

   Появится экран с индикатором хода работ, на котором после создания пула будет отображено состояние Completed (Завершено), как показано на рис. 12.17.

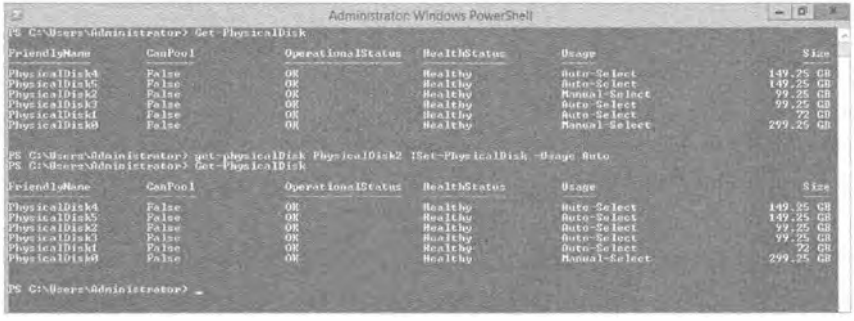


Рис. 12.15. Изменение типа выделения диска в PowerShell

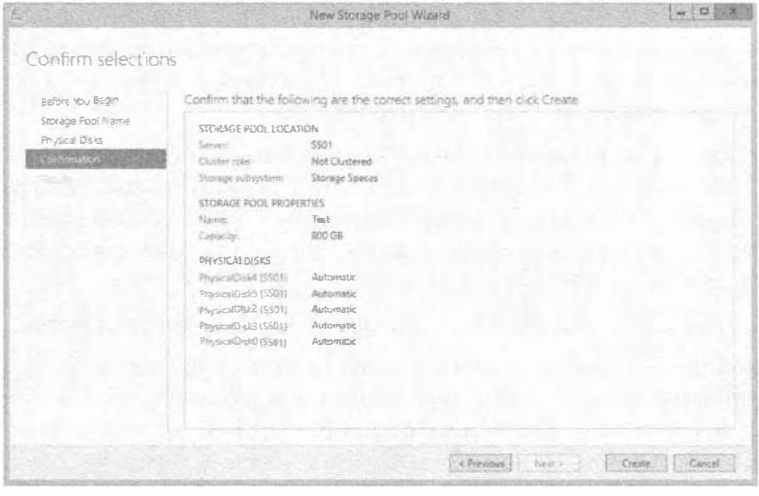


Рис. 12.16. Пересмотр опций конфигурации перед созданием пула

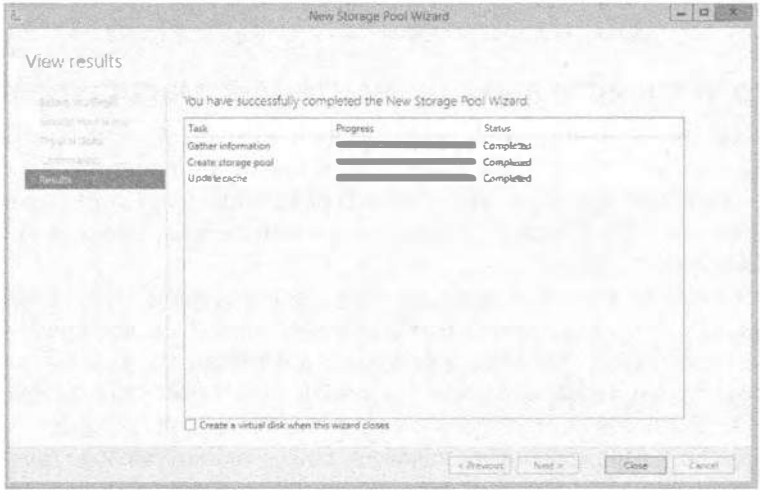


Рис. 12.17. Пул хранения успешно создан

Поздравляем, вы создали свой первый пул!

Ограничения пулов хранения

Как и со всеми технологиями, пулам хранения присущи некоторые ограничения, и хотя эта технология является мощной, она, безусловно, не может быть оптимальной абсолютно во всех ситуациях. Имея это в виду, давайте взглянет на ее ограничения.

- Жесткий диск должен иметь объем 10 Гбайт или больше.
- В пространстве хранения невозможно развернуть загрузочную систему.
- Любые диски, предназначенные для добавления в пул хранения, не должны быть разбиты на разделы или сформатированы. Все данные на таких дисках будут утрачены.
- В случае использования контроля по четности требуются три диска, при двухстороннем зеркальном отображении — два диска, а при трехстороннем зеркальном отображении — три и более дисков.
- Все диски в пуле должны иметь одинаковый размер сектора (4 Кбайт/512e или 512). 512e, или 512 Emulation (эмуляция 512-байтового сектора), позволяет производителям выпускать диски с секторами 4 Кбайт и обеспечивать совместимость с программным обеспечением, которое не модернизировано для восприятия секторов 4 Кбайт.
- Диски Fibre Channel и iSCSI в пуле хранения не поддерживаются.
- Все хранилище должно быть совместимо с драйвером `storport.sys`. Для проверки этого применяется список совместимости оборудования Microsoft (Microsoft Hardware Compatibility List), доступный по следующему URL: `http://www.microsoft.com/ru-ru/windows/compatibility/compatcenter/home`. (Если ваше оборудование находится в этом списке совместимости, то оно будет работать с драйвером `storport.sys`.)
- Если виртуальный диск должен использоваться в кластере с обходом отказа, на таком виртуальном диске должна быть развернута файловая система NTFS.

Просмотр устройств в инструменте Disk Management

В сущности, пул хранения представляет собой логический контейнер для дисков. Например, в нашей демонстрационной среде имеется несколько дисков, готовых для назначения в пул хранения. На экране Disk Management (Управление дисками), показанном на рис. 12.18, можно видеть все перечисленные ранее физические диски до их назначения в пул.

После добавления дисков в пул хранения мы обновляем Disk Management. Как видно на рис. 12.19, они перестали отображаться. Диск 1 по-прежнему остался, т.к. он является диском операционной системы, поэтому он должен быть всегда, и вы никогда не будете иметь возможность включить его в пространство хранения. Куда делись диски? Вспомните, что пул хранения является контейнером. Чтобы снова увидеть тома в Disk Management, понадобится создать виртуальные диски.

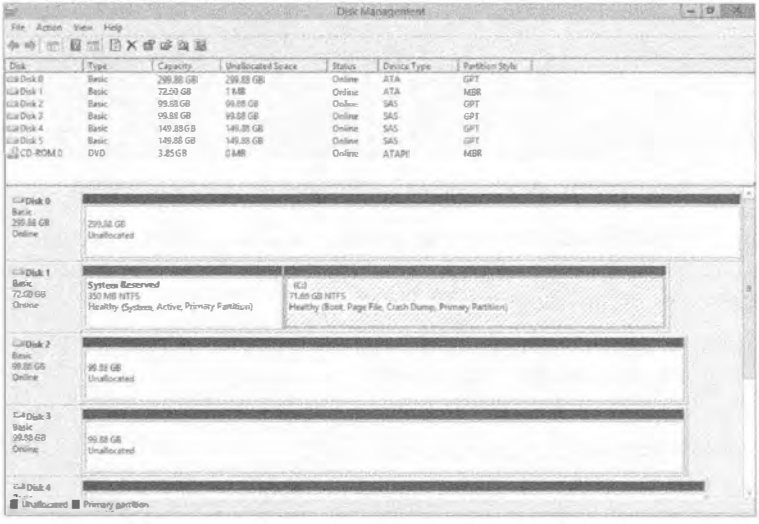


Рис. 12.18. Невыделенные диски в инструменте Disk Management

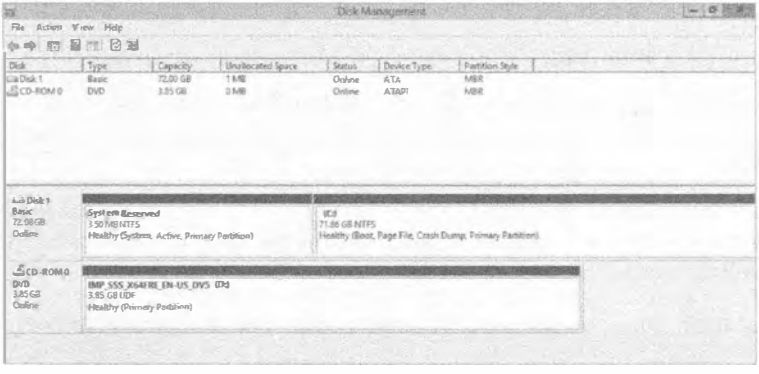


Рис. 12.19. После добавления в пул хранения диски больше не отображаются в Disk Management

Работа с пулом хранения в PowerShell

Ранее мы упоминали, что все задачи, выполняемые в графическом пользовательском интерфейсе, могут быть сделаны посредством PowerShell. Сейчас мы покажем, как создать пул хранения с применением PowerShell.

1. Сначала необходимо найти доступные диски. Воспользуйтесь командлетом `Get-PhysicalDisk` для получения списка всех дисков в системе. На рис. 12.20 показан результат для рассматриваемого примера.
2. Взгляните на свойство `CanPool`. Когда его значение равно `True`, этот диск может быть помещен в пул хранения.
3. Отфильтруйте физические диски, которые можно помещать в пул, и сохраните результаты в переменной для дальнейшего применения с помощью следующего синтаксиса:

```
$drivestopool = (Get-physicaldisk |where {$_.CanPool -eq $True})
```

Рис. 12.20. Отображение доступных физических дисков

4. Идентифицируйте подсистему хранения, с которой имеете дело, и снова сохраните результат в переменной, но в этом случае вы заинтересованы только в свойстве `FriendlyName` (рис. 12.21).

   Используйте приведенный ниже синтаксис для захвата значения свойства `FriendlyName` подсистемы хранения:

   ```
   $storagesystem = (get-storagesubsystem).friendlyname
   ```

   Теперь можно создать пул хранения.

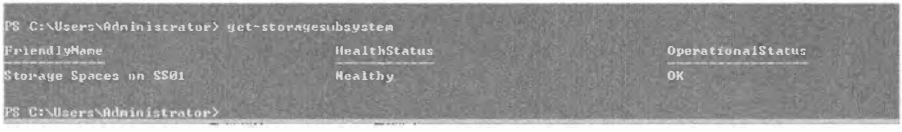


Рис. 12.21. Командлет `Get-StorageSubsystem`

5. Используйте следующий синтаксис для создания пула:

   ```
   New-storagepool -friendlyname TestPool -StorageSubSystemFriendlyName
   $storagesystem -physicaldisks $drivestopool
   ```

   Дружественное имя для пула (указываемое в `-friendlyname`) может быть любой желаемой строкой. Показанный синтаксис создаст пул по имени `TestPool` и добавит в него диски (рис. 12.22).

Рис. 12.22. Вывод в PowerShell при создании нового пула хранения

6. Теперь примените командлет `Get-StoragePool` для получения более подробной информации о пуле:

   ```
   Get-StoragePool TestPool |fl *
   ```

   Пример вывода можно видеть на рис. 12.23; обратите внимание на объем деталей, которые предоставляет PowerShell по сравнению с графическим пользовательским интерфейсом.

Выделение пространства пула под виртуальный диск

С самого начала этой главы мы прояснили, что когда ссылаемся на виртуальный диск в связи с пространством хранения, то не имеем в виду файл VHDX для виртуальной машины. На самом деле, до тех пор, пока вы не поместите виртуальную машину в пространство хранения или не используете ее в качестве целевого хранилища iSCSI, вы нигде не увидите файла VHD.

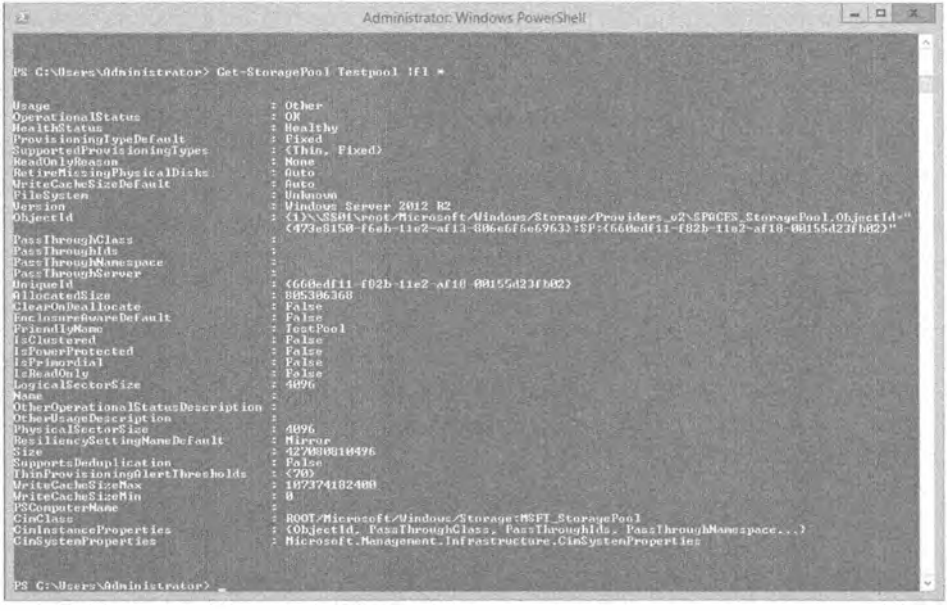


Рис. 12.23. Вывод из командлета `Get-StoragePool`

Виртуальные диски — это диски, которые выделяются из пула хранения. Ранее мы создавали пул для физических дисков и показали, что с точки зрения инструмента Disk Management все диски исчезали, поскольку они стали принадлежать пулу хранения. Для того чтобы использовать какое-то пространство, содержащееся внутри пула хранения, вы должны создать виртуальный диск. Он не связан напрямую с физическим диском в пуле хранения, но является представителем порции пространства, выделяемого из пула хранения. То, каким образом эта порция обретает существование, зависит опций, которые мы обсудим далее.

Одной из замечательных характеристик виртуализации в целом является возможность максимизации использования оборудования. Например, ранее многие организации имели по одному серверу на роль, что было расточительством, но теперь на одном сервере можно удерживать несколько ролей, которые полностью изолированы друг от друга. Надеемся, что на этом этапе вы уже знакомы с виртуализацией. Похожая концепция существует в пулах хранения и виртуальных дисках.

Как было указано, пулы хранения — это по существу логические контейнеры для набора физических дисков, которые вы хотите объединить. Виртуальные диски будут представлены серверу для применения в качестве тома. При наличии трех физических дисков по 500 Гбайт, скомбинированных в пул хранения, имеется потенциально 1,5 Тбайт пространства (рис. 12.24).

Рис. 12.24. Выделение пула хранения

Довольно неплохо. (Мы пока не принимаем во внимание избыточность, т.к. это будет объясняться позже.) Теперь системный администратор получает запрос от бригады, занимающейся новым приложением, которым

требуется 2 Тбайт пространства. Тем не менее, когда системный администратор пересматривает прогнозируемый рост, он понимает, что 2 Тбайт не нужны авансом, что хорошо, поскольку в бюджете не предусмотрены расходы на приобретение дополнительных дисков. Знакомая история? Вопрос в том, как разрешить проблему.

Одним из первых выборов, которые вы делаете при создании виртуальных дисков, касается типа настройки — фиксированной или тонкой.

- **Fixed provisioning (Фиксированная настройка).** При фиксированной настройке, если вы запрашиваете 2 Тбайт, то для настройки должно быть доступно 2 Тбайт емкости.
- **Thin provisioning (Тонкая настройка).** Диски с тонкой настройкой используют только то, что нужно в данный момент. Это замечательно! В предыдущем примере бригада, занимающаяся приложением, считает, что у них есть запрошенная емкость 2 Тбайт, но в действительности задействовано только доля от 2 Тбайт (рис. 12.25).

Фиксированная настройка
Емкость 1 Тбайт
Требуется 1 Тбайт
Используется 1 Тбайт

Тонкая настройка
Емкость 1 Тбайт
Требуется 1 Тбайт
Используется 200 Гбайт

Рис. 12.25. Диски с фиксированной или тонкой настройкой

Управление дисками с тонкой настройкой

Диски с тонкой настройкой могут приводить к невосполнимому распределению ресурсов и должны управляться. Понадобится создать оповещения, чтобы обеспечить мониторинг свободного пространства, остающегося в пуле и на виртуальном диске. Меньше всего хотелось бы получить перебой в работе из-за перегрузки ресурсов. При корректном применении диски с тонкой настройкой могут помочь системным администраторам уменьшить стоимость хранения, но по-прежнему удовлетворять нуждам потребителей.

Определение компоновки диска

Далее необходимо принять решение относительно компоновки виртуального диска. Доступны три вида компоновки с разной отказоустойчивостью.

- **Simple (Простая).** При такой компоновке данные разделяются на полосы по всем дискам в пуле. Эта компоновка не является отказоустойчивой. В случае сбоя диска все данные теряются.

- **Mirror (Зеркальное отображение).** Зеркальное отображение данных дублирует их на разных дисках; это дает максимальную отказоустойчивость, но оказывает значительное влияние на объем пространства, которое потенциально может использоваться. Чтобы защититься от одиночного дискового отказа, понадобится иметь в пуле хранения, по меньшей мере, два физических диска; для обработки двух дисковых отказов физических дисков должно быть минимум пять.
- **Parity (Контроль по четности).** Контроль по четности по существу записывает данные в полосы на всех дисках, но также производит запись информации о четности, что позволяет восстанавливать данные в случае отказа диска. Это обеспечивает великолепную отказоустойчивость и производительность. Для обработки одиночного дискового отказа понадобится, по меньшей мере, три физических диска.

На рис. 12.26 показано визуальное представление различных компоновок, доступных для применения. Части, помеченные как "Полоса данных (простая компоновка)", говорят о том, что данные записываются по всем дискам. В случае частей, помеченных как "Зеркало", если данные записываются на один диск в 4-дисковом зеркале, то они будут записываться также и на второй диск. Наконец, в частях, которые помечены как "Контроль данных по четности", данные записываются по всем дискам и сопровождаются информацией о четности, что позволит проводить восстановление при отказе.

Рис. 12.26. Компоновки виртуальных дисков

Создание виртуального диска в графическом пользовательском интерфейсе

Следующий шаг заключается в создании виртуального диска. Все виртуальные диски проще всего создавать внутри консоли Storage Pools (Пулы хранения) диспетчера серверов (рис. 12.27).

1. В области Virtual Disks (Виртуальные диски), находящейся в левой нижней части окна консоли, выберите в раскрывающемся меню Tasks (Задачи) пункт New Virtual Disk (Создать виртуальный диск), как показано на рис. 12.28.
2. Щелкните на кнопке Next (Далее) на экране приветствия мастера создания виртуального диска (New Virtual Disk Wizard).

   Как показано на рис. 12.29, вы должны выбрать пул хранения, в котором необходимо создать виртуальный диск. В рассматриваемом примере мы собираемся использовать пул `TestPool`.

3. Выберите пул хранения и щелкните на кнопке Next.

   Виртуальному диску понадобится назначить имя. Можно также ввести описание, для чего предназначен этот виртуальный диск.

4. В данном примере мы назвали диск `File_Vdisk`, как показано на рис. 12.30, и указали в описании, что он применяется для файлового хранилища.

   Следующий шаг связан с выбором компоновки хранения (рис. 12.31). Доступны три варианта: Simple (Простая), Mirror (Зеркальное отображение) и Parity (Контроль по четности).

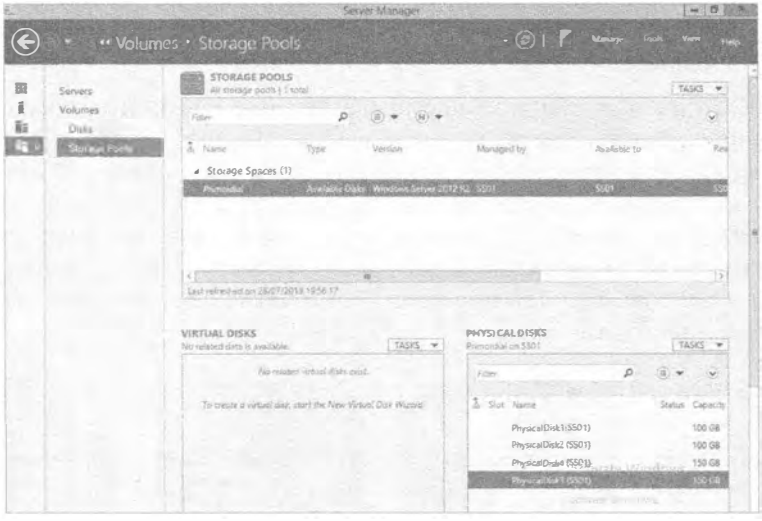


Рис. 12.27. Консоль Storage Pools

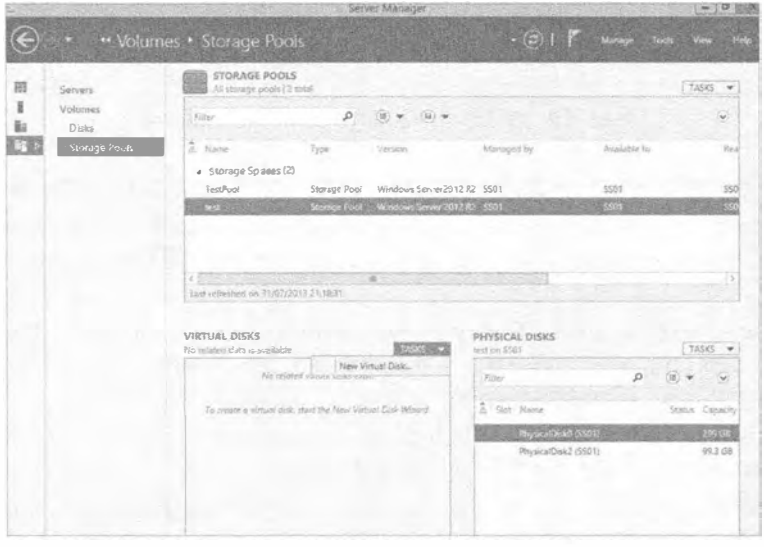


Рис. 12.28. Создание нового виртуального диска

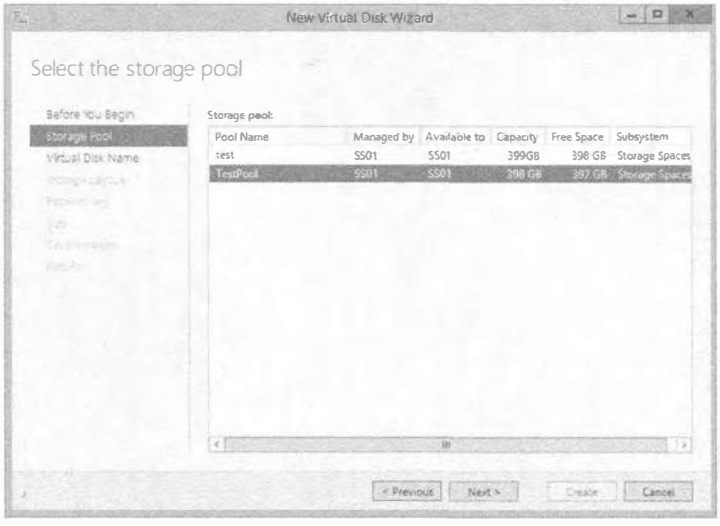


Рис. 12.29. Выбор пула хранения для создания виртуального диска

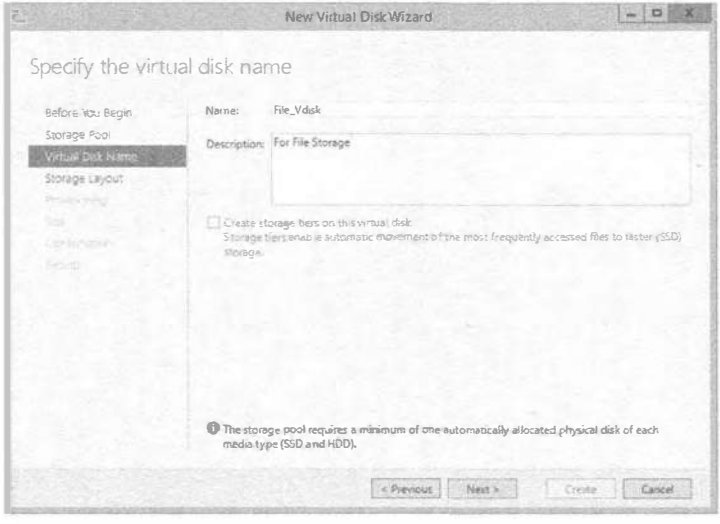


Рис. 12.30. Ввод имени и описания для виртуального диска

5. Для этого примера выберите Simple и щелкните на кнопке Next.

   Теперь необходимо выбрать тип настройки. Как показано на рис. 12.32, доступны два варианта: Thin (Тонкая) и Fixed (Фиксированная).

6. Для рассматриваемого примера выберите тип настройки Thin, т.к. требуется максимизировать пространство в пуле хранения.

   Сейчас нужно принять решение относительно размера виртуального диска. Поскольку для него выбрана тонкая настройка, теоретически можно ввести любое значение.

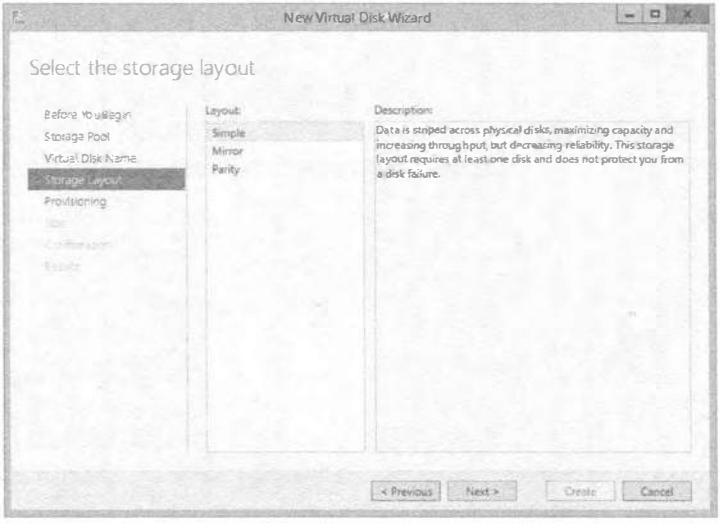


Рис. 12.31. Выбор компоновки хранения для виртуального диска

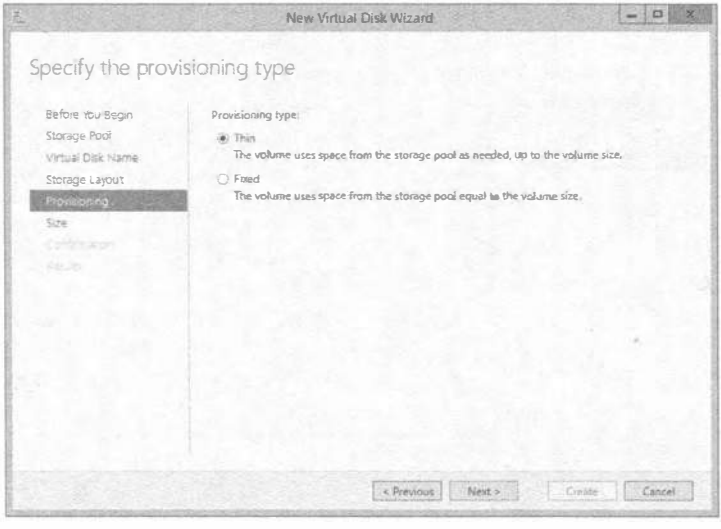


Рис. 12.32. Выбор типа настройки для виртуального диска

7. Пул хранения имеет емкость около 400 Гбайт, поэтому мы назначим виртуальному диску 500 Гбайт (рис. 12.33). Для продолжения щелкните на кнопке Next.
8. Наконец, просмотрите произведенный выбор и подтвердите его, щелкнув на кнопке Create (Создать).
9. Просмотрите информацию на экране Results (Результаты) и удостоверьтесь, что все завершено (рис. 12.34). Щелкните на кнопке Close (Закрыть), чтобы закрыть окно мастера.

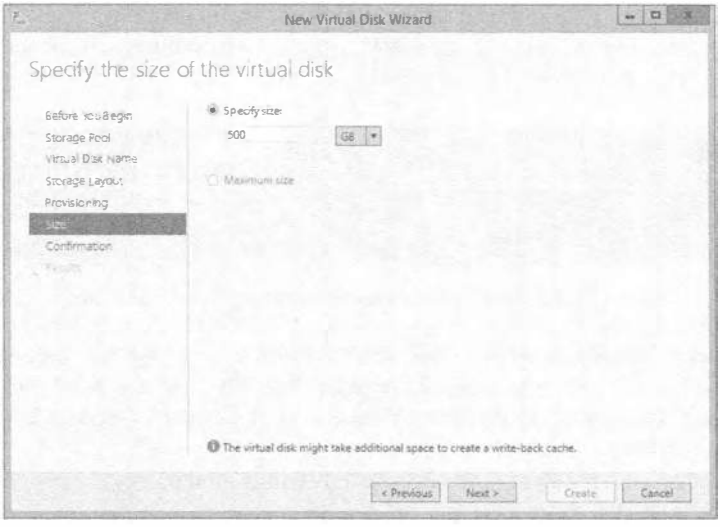


Рис. 12.33. Установка размера виртуального диска

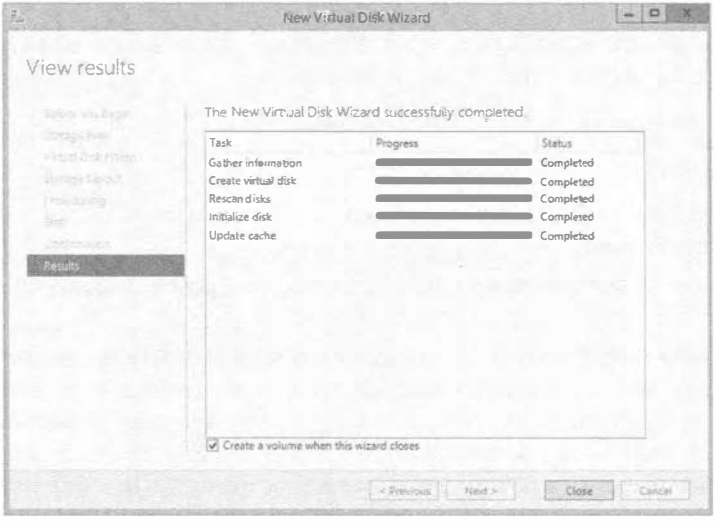


Рис. 12.34. Экран Results мастера после создания нового виртуального диска

Дополнительное упражнение

Загляните сейчас в инструмент Disk Management, и вы увидите, *что* неожиданно появилось!

Создание виртуального диска в PowerShell

Первым делом, давайте воспользуемся PowerShell для просмотра виртуального диска, который был создан в предыдущем примере с применением графического пользовательского интерфейса.

На рис. 12.35 демонстрируется применение командлета Get-VirtualDisk для извлечения всей информации о созданных виртуальных дисках. Как видите, был создан только один виртуальный диск емкостью 500 Гбайт.

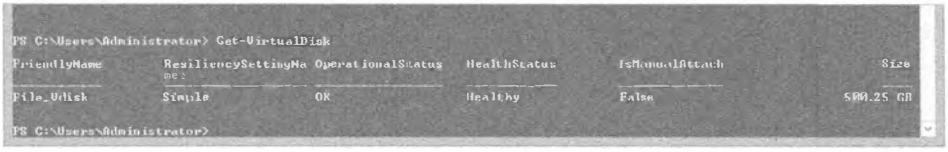


Рис. 12.35. Вывод из командлета Get-VirtualDisk

Чтобы создать новый виртуальный диск, необходимо воспользоваться командлетом New-VirtualDisk. Но прежде чем делать это, вы должны узнать дружественное имя пула хранения. Помните ли вы команду для получения дружественного имени пула хранения?

Имея дружественное имя, выполните следующие шаги.

1. С помощью показанного ниже синтаксиса сохраните дружественное имя пула хранения в переменной:

   ```
   $sp = (get-storagepool).friendlyname
   ```

   Следующий шаг заключается в создании виртуального диска, но сначала взгляните на полный синтаксис команды:

   ```
   New-VirtualDisk -StoragePoolFriendlyName $sp[1]
   -ResiliencySettingName Simple -Size 500GB -FriendlyName TestVdisk
   -ProvisioningType Thin -NumberofDataCopies 1 -NumberofColumns 2
   ```

   Как видите, на выбор доступно несколько больше опций. Далее приведены их краткие описания.

   - **ResiliencySettingName.** Эквивалент опций компоновки хранения Simple, Mirror, Parity.
   - **NumberofDataCopies.** Количество копий данных, которые необходимо хранить; эта опция напрямую связана с ResiliencySettingName. Если вы выбрали Simple, например, то NumberofDatacopies может быть только 1. В случае выбора Mirror значением NumberofDataCopies будет как минимум 2, в зависимости от объема дискового пространства, имеющегося в системе.
   - **NumberofColumns.** Прямо связано с количеством дисков, которые вы хотите использовать. Пул хранения может иметь сотни дисков, но вам может требоваться разделение на полосы, зеркальное отображение или применение контроля по четности, скажем, только для пяти дисков. Эта опция позволяет сделать выбор. Она также связана с ResiliencySettingName и NumberofDataCopies.

   Значения, установленные для NumberofDataCopies и NumberofColumns, относятся к выбранным опциям. Например, если необходимо зеркально отобразить данные, мы увеличиваем значение NumberofDataCopies, и если требуется охватить виртуальным диском несколько физических дисков, то мы увеличиваем NumberofColumns. В этом случае нужна только одна копия данных и запись данных на два диска.

2. С помощью опции `$sp[1]` мы выбираем один элемент из всех пулов хранения, захваченных командой `get-storagepool`. Например, при наличии пяти пулов хранения команда `get-storagepool` возвратит все пять, поэтому `$sp[1]` позволяет выбрать пул хранения с номером 2 из пяти захваченных. Счетчик начинается с 0, так что первый пул хранения можно извлечь как `$sp[0]`.

   В испытательной среде определено несколько пулов хранения. Если просто указать `$sp`, команда сообщит об ошибке, поскольку она попытается вставить (в этом случае) дружественные имена двух пулов хранения.

   На рис. 12.36 демонстрируется пример запуска только что разобранной команды.

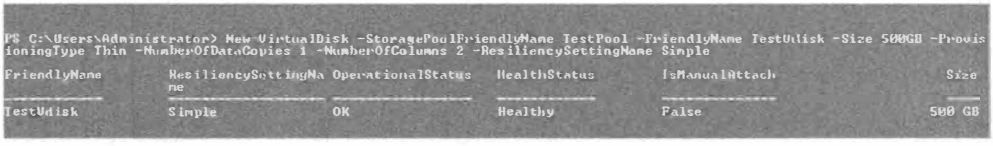


Рис. 12.36. Пример вывода команды создания виртуального диска в PowerShell

3. Запустите `get-virtualdisk` и просмотрите вывод, в котором должен присутствовать созданный диск.

И снова в качестве дополнительного упражнения просмотрите диск в инструменте Disk Management.

Тома из виртуальных дисков

Если вам когда-либо приходилось настраивать стандартный физический диск, создавать том и форматировать его, то вам должна быть хорошо знакома эта тема.

Создавать тома можно несколькими способами. Двумя наиболее известными способами являются инструмент Disk Management и утилита `Diskpart`, и при желании можно воспользоваться ими. Однако в рассматриваемом примере для демонстрации того, что все необходимое в отношении пространств хранения можно делать напрямую из пользовательского интерфейса Storage Pools (Пулы хранения), мы покажем, как создать здесь том.

На рис. 12.37 представлен пользовательский интерфейс Storage Pools, и в области Virtual Disks (Виртуальные диски) виден созданный ранее виртуальный диск `File_Vdisk`.

1. Щелкните правой кнопкой мыши на новом виртуальном диске и выберите в контекстном меню пункт New Volume (Создать том), как показано на рис. 12.38.
2. Щелкните на кнопке Next (Далее) на экране приветствия мастера создания тома (New Volume Wizard).
3. Выберите сервер `SS01` и диск Disk 6, `File_Vdisk` (рис. 12.39), затем щелкните на кнопке Next.

   Как и с нормальными дисками, один лишь факт, что полный диск может иметь емкость 500 Гбайт, вовсе не означает, что создаваемые тома обязаны быть по 500 Гбайт. Вы можете при желании создать несколько томов разных размеров. Они просто должны в сумме занимать до 500 Гбайт.

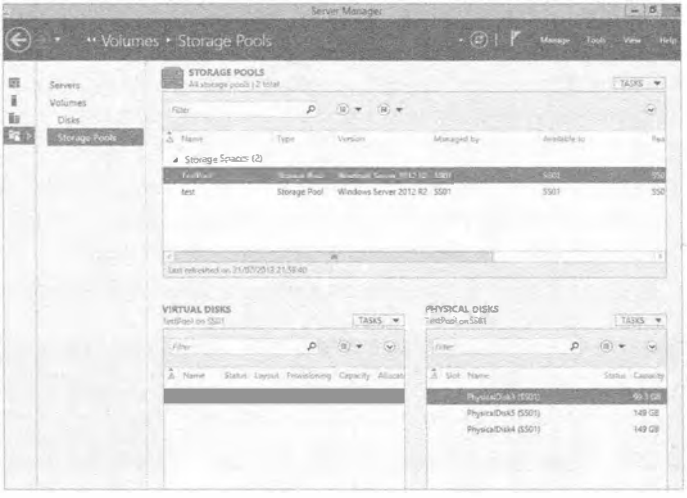


Рис. 12.37. Пользовательский интерфейс Storage Spaces с созданным ранее виртуальным диском

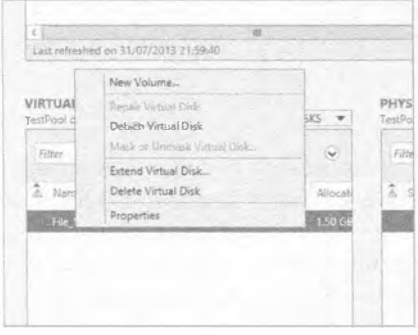


Рис. 12.38. Создание нового тома из виртуального диска

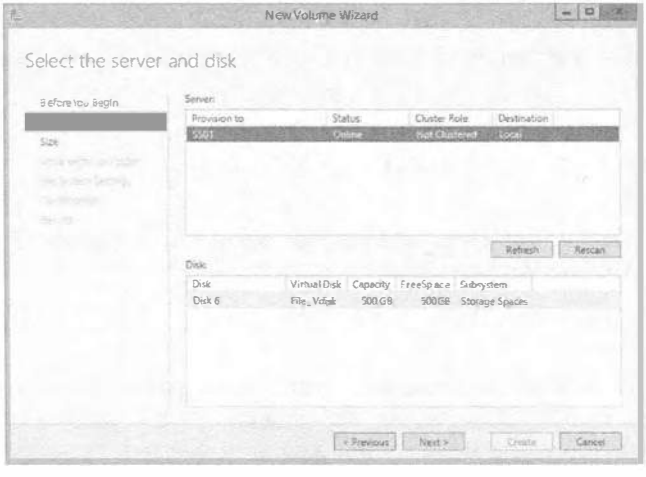


Рис. 12.39. Выбор сервера и виртуального диска

4. В этом примере мы оставляем стандартный размер 500 Гбайт с тонкой настройкой (рис. 12.40).

   Далее, как вы поступили бы с нормальным диском, выберите букву диска или папку, в которой необходимо смонтировать том.

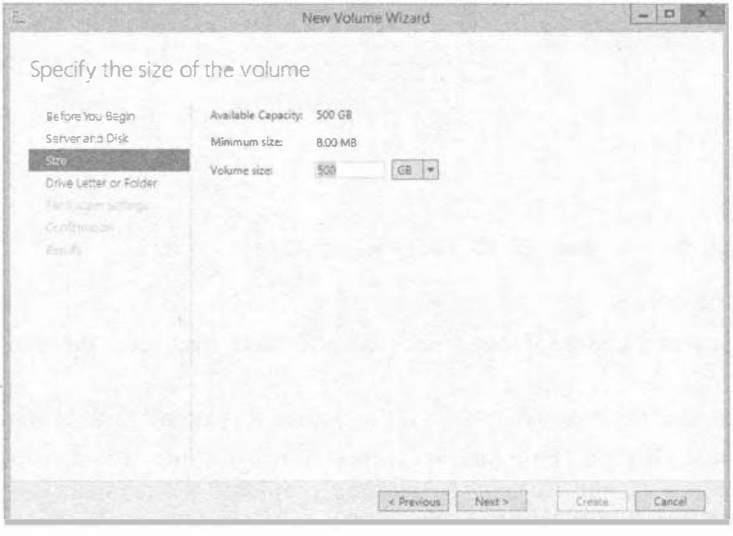


Рис. 12.40. Установка емкости для тома

5. В данном примере мы принимаем стандартную букву диска E, как показано на рис. 12.41.

   Теперь можно выбрать файловую систему. Обратите внимание, что выбирать можно только NTFS или ReFS (рис. 12.42).

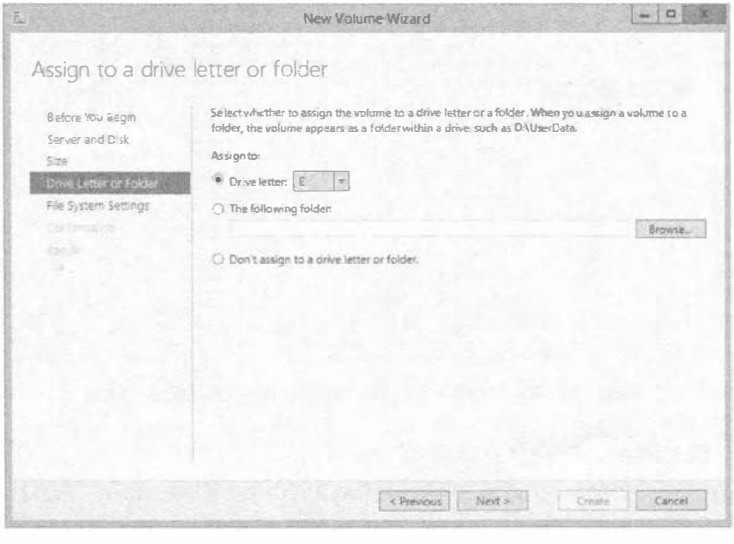


Рис. 12.41. Выбор буквы диска для тома

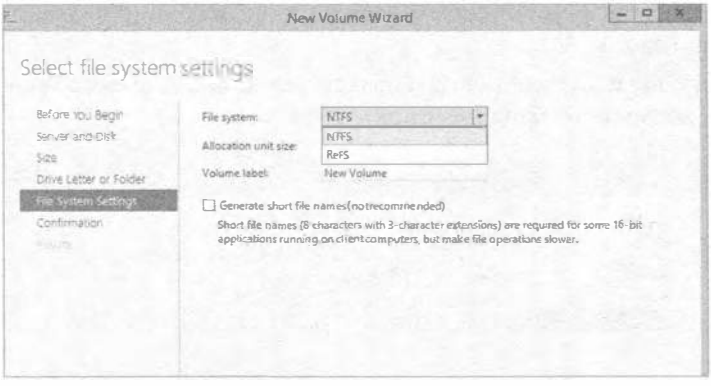


Рис. 12.42. Настройки файловой системы

6. Выберите NTFS.
7. В поле Volume Label (Метка тома) введите **`Test_Volume`** и щелкните на кнопке Next.
8. Подтвердите выбранные опции и щелкните на кнопке Create (Создать).
9. На экране Results (Результаты), показанном на рис. 12.43, удостоверьтесь в том, что все задачи имеют состояние Completed (Завершена), и щелкните на кнопке Close (Закрыть).
10. Откройте проводник Windows и обратите внимание на появление нового тома `E:`.

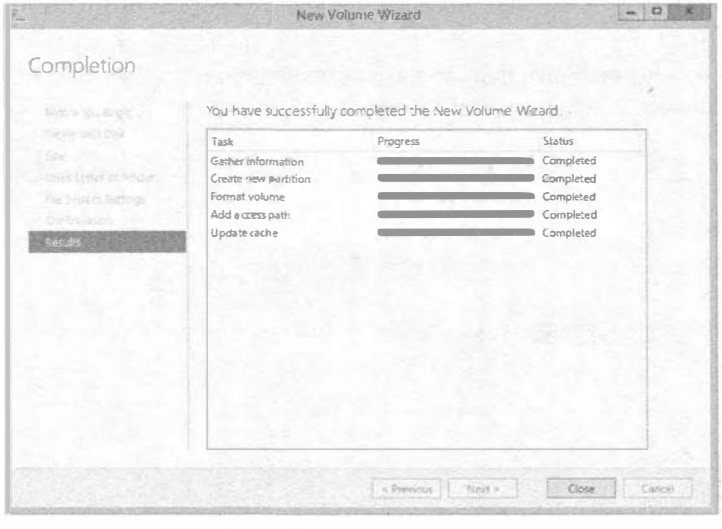


Рис. 12.43. Экран Results мастера создания тома

По умолчанию новые диски отключены

По умолчанию, когда вы добавляете физический диск либо VHD или даже новый виртуальный диск, он всегда будет в отключенном состоянии. Обычно это нормально, но в облачной среде необходимость перевода диска в онлайновое состояние

является дополнительным шагом, без которого можно было бы обойтись. В утилите командной строки `Diskpart` имеется возможность сконфигурировать опцию, чтобы виртуальный диск сразу после своего создания автоматически переходил в онлайновое состояние.

Чтобы установить состояние политики для дисков SAN в `Online All` (Все онлайновые), введите следующую команду в окне командной строки с повышенными полномочиями:

```
Diskpart "san policy=OnlineAll"
```

На рис. 12.44 приведен пример вывода утилиты `Diskpart` и установки политики SAN в `Online All`.

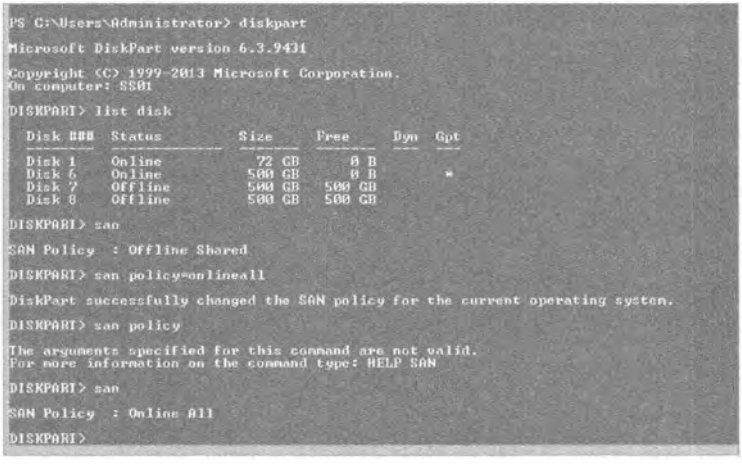


Рис. 12.44. Пример вывода утилиты `Diskpart` при установке политики SAN

Дополнительное упражнение

Используя ранее описанные шаги, создайте в пуле `TestPool` новый виртуальный диск. Перешел ли он в онлайновое состояние?

Перевод дисков в онлайновое состояние с помощью PowerShell

Как и все остальное, старые инструменты командной строки заменяются PowerShell. Можете ли вы угадать, какие командлеты применяются для выяснения, какие диски находятся в отключенном состоянии, и для их перевода в онлайновое состояние?

Для начала воспользуемся командлетом `get-disk` для получения информации о состоянии дисков. На рис. 12.45 показан пример вывода `get-disk`, где видно, что имеются два диска в отключенном состоянии.

1. Введите **`get-disk`** и нажмите <Enter>.
2. Можно было бы также отфильтровать только отключенные диски, введя следующую команду:

```
Get-disk |where {$_.operationalstatus -eq "Offline"}
```

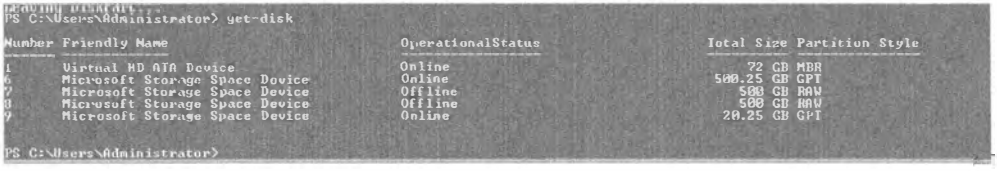


Рис. 12.45. Вывод командлета `get-disk`

3. Для перевода их в онлайновое состояние вы будете применять командлет `set-disk`.
4. Чтобы перевести все диски в онлайновое состояние за один раз, используя предыдущий синтаксис с фильтрацией отключенных дисков, вывод можно направить по конвейеру командлету `set-disk`.

   Ниже показан синтаксис, а на рис. 12.46 — результаты выполнения:

   ```
   Get-disk |where {$_.operationalstatus -eq "Offline"} |set-disk
   -isoffline $false
   ```

Рис. 12.46. Перевод всех дисков в онлайновое состояние с помощью PowerShell

Демонстрация настройки многоуровневого хранения с помощью PowerShell

Мы рассмотрели создание пула хранения, виртуального диска и томов для использования в среде. В начале главы упоминалось об уровнях хранения. Они могут предоставить огромные преимущества среде, поскольку позволяют разделять хранилище и обеспечивать возврат платежей на основе ресурсов, которые требуются конечным пользователям. По сути дела, если конечные пользователи требуют высокоскоростного хранилища, вы можете выделить его и выставлять соответствующие счета на оплату; в противном случае вы можете выделить для обслуживания их потребностей хранилище низкого уровня. Если ваша компания делает возврат платежей, то это пойдет на пользу всем конечным пользователям, т.к. пространства хранения будут автоматически перемещать данные с более частым доступом, на быстрый уровень хранения, а данные, к которым обращаются редко — на медленный уровень хранения.

Поскольку вы уже знакомы с консолью Storage Spaces (Пространства хранения), вы заметите, что внутри пользовательского интерфейса отсутствует место для конфигурирования пулов хранения. Это средство может быть сконфигурировано только через PowerShell.

Мы уже создали пул хранения по имени `TestPool`, так что давайте применять его в качестве дружественного имени.

Как уже говорилось, в Windows Server 2012 R2 можно создавать только два уровня хранения. Система распознает носители двух типов — твердотельный накопитель (Solid State Drive — SSD) и жесткий диск (Hard Disk Drive — HDD).

Запустив в испытательной среде командлет PowerShell под названием `get-physicaldisk`, мы получим вывод, показанный на рис. 12.47.

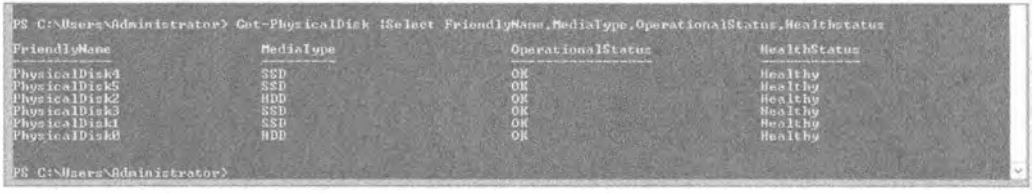


Рис. 12.47. Пример вывода командлета `get-physicaldisk` при создании уровней хранения

Создание пулов SSD и HDD

Вы видите, что в среде присутствуют устройства SSD и HDD. А теперь мы создадим уровни хранения. В рассматриваемом примере мы собираемся создать два уровня (что также является максимальным поддерживаемым количеством) и затем создадим виртуальный диск, который будет выделен по уровням. Далее мы разобьем диск на разделы и сформатируем.

Ниже показан синтаксис использования командлета `New-StorageTier` для создания пула SSD. Мы должны сохранить его в переменной для дальнейшего применения:

```
$ssdtier = new-storagetier -StoragePoolFriendlyName "TestPool"
-FriendlyName SSD_Tier -Mediatype SSD
```

Для создания уровня HHD используется следующий синтаксис:

```
$hddtier = new-storagetier -StoragePoolFriendlyName "TestPool"
-FriendlyName HDD_Tier -Mediatype HDD
```

Далее потребуется добавить виртуальный диск и привязать его к уровням хранения. Предугадывая вопрос, можно ли переназначить существующий виртуальный диск уровню хранения, ответим — нет, нельзя.

Имея это в виду, мы создадим новый виртуальный диск, который будет привязан к нашим уровням хранения. Вот какой синтаксис применяется:

```
New-VirtualDisk -StoragePoolFriendlyName TestPool -FriendlyName
Tiered_VDisk -StorageTiers @($ssdtier, $hddtier) -StorageTierSizes
@(10GB, 50GB) -ResiliencySettingName Simple
```

На рис. 12.48 показан вывод после успешного создания диска.

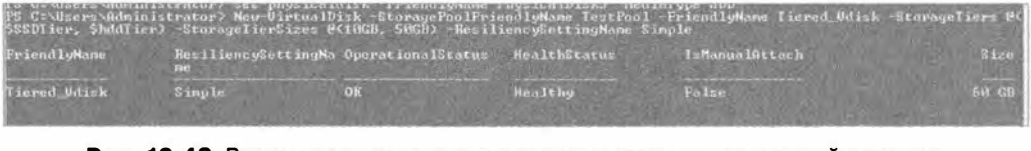


Рис. 12.48. Вывод после успешного создания диска внутри уровней хранения

Большинство опций должны выглядеть знакомыми по созданию виртуального диска ранее в главе. Тем не менее, есть две опции, которые связаны с созданием виртуального диска внутри уровня хранения.

- **`StorageTiers @($ssdtier, $hddtier)`**. Указывает используемые уровни. Это не хеш-таблица, так что будьте внимательны и не применяйте фигурные скобки. Мы сохранили уровни в отдельных переменных для простоты ссылки на них.
- **`StorageTierSizes @(10GB, 50GB)`**. Указывает размер каждого уровня и ссылается в порядке, установленном в опции `-StorageTier`. Как вы заметили на рис. 12.48, общий размер составляет 60 Гбайт, т.е. 10 Гбайт + 50 Гбайт.

Отсюда вам необходимо создать том, как это делалось ранее для хранения данных. Мы покажем быстрый трюк в PowerShell, которым можно воспользоваться для создания на диске тома 20 Гбайт и его форматирования в единственной строке. Ниже приведен синтаксис:

```
Get-VirtualDisk | Get-Disk | New-Partition -Size 20GB
-AssignDriveLetter | Format-Volume -Force -confirm:$false
```

Вывод команды представлен на рис. 12.49. Теперь вы можете перейти на диск по его букве и скопировать файл.

Рис. 12.49. Создание нового раздела и его форматирование в PowerShell

Выделите время на просмотр свойств только что созданного виртуального диска. На рис. 12.50 обратите внимание, каким образом разделилась емкость из-за того, что мы разнесли этот виртуальный диск по двум уровням.

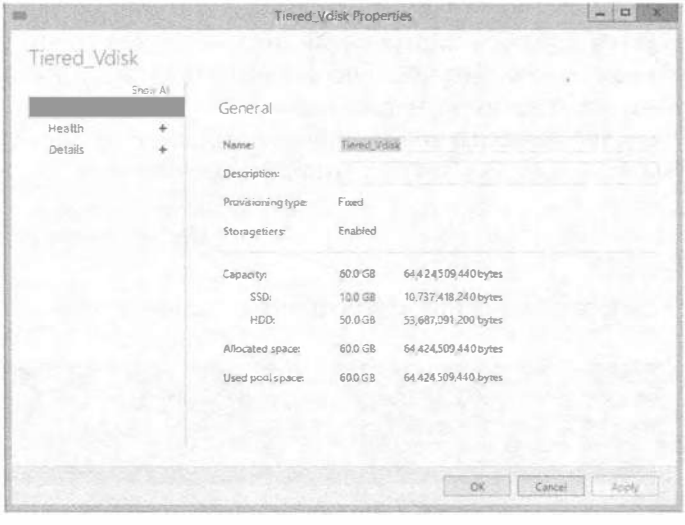


Рис. 12.50. Свойства многоуровневого виртуального диска

Использование кеша с обратной записью

А теперь мы покажем, как использовать одно из последних крупных средств технологии Storage Spaces в Windows Server 2012 R2 — кеша с обратной записью. Как и с уровнями хранения, его не получится включить через графический пользовательский интерфейс; это должно делаться в PowerShell. Вспомните, кеш с обратной записью может поспособствовать в ускорении работы приложений, т.к. запись в кеш является быстрой и не требует ожидания, пока хранилище зафиксирует запись.

Возьмите команду PowerShell, которая применялась для построения предыдущего уровня хранения, и модифицируйте имя и опции `StorageTierSizes`. Затем добавьте опцию `-WriteCacheSize` с настройкой размера; в данном случае необходим размер кеша с обратной записью, равный 2 Гбайт:

```
New-VirtualDisk -StoragePoolFriendlyName TestPool1 -FriendlyName
Tiered_VDisk -StorageTiers @($ssdtier, $hddtier) -StorageTierSizes @
(20GB, 70GB) -ResiliencySettingName Simple -WriteCacheSize 2GB
```

Итак, вы создали виртуальный диск, который будет использовать уровни хранения и имеет включенный кеш с обратной записью.

Оптимизация уровней хранения

Последний аспект, который мы обсуждали об уровнях хранения в начале этой главы, заключается в том, что каждую ночь в 1:00 запускается задание, повторно назначающее приоритеты хранилищу и перемещающее данные на быстрый уровень вместо медленного.

В планировщике задач выберите папку Task Scheduler Library\Microsoft\Windows\Storage Tiers Management (Библиотека планировщика задач \ Microsoft \ Windows \ Управление уровнями хранения). Планировщик задач отображает задачу под названием Storage Tiers Optimization (Оптимизация уровней хранения), показанный на рис. 12.51. При необходимости вы можете изменить задачу или запустить ее вручную.

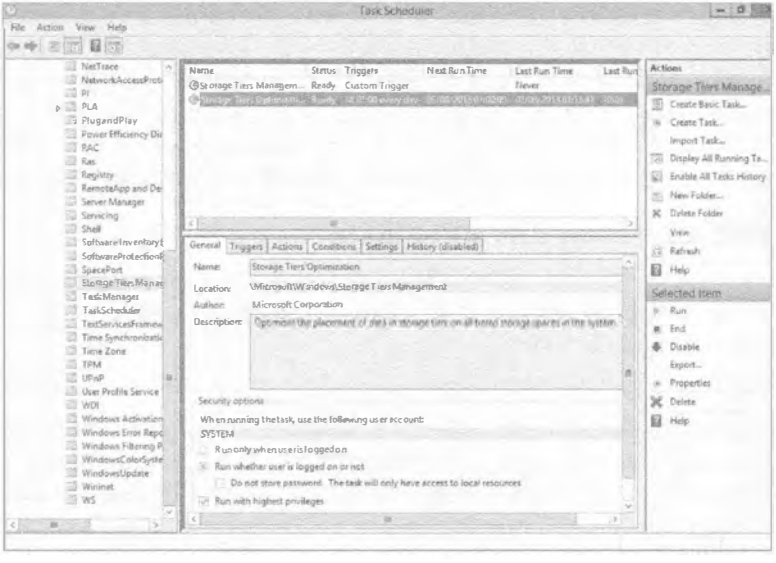


Рис. 12.51. Задача Storage Tiers Optimization

iSCSI в пространствах имен

Пространства имен чрезвычайно полезны для обеспечения масштабируемого и надежного хранилища. Подумайте о сумме, которую компании пришлось бы вложить для получения уже обрисованных возможностей. Что было бы действительно полезно сейчас — это объединение всей мощной технологии хранения с iSCSI, чтобы позволить удаленным системам (таким как файловые серверы, почтовые системы, кластеры виртуализации и т.п.) также получить выигрыш от этих средств.

iSCSI требует конфигурирования нескольких элементов, чтобы они предоставляли удаленным машинам номера логических устройств (logical unit number — LUN). Для начала мы объясним несколько элементов, образующих iSCSI с точки зрения хост-сервера и удаленного сервера, которые необходимо знать, чтобы понять рассматриваемый далее пример.

- **Целевой сервер iSCSI.** Позволяет инициаторам iSCSI создавать подключение к целевой службе, в свою очередь, представляющей диск VHD, который расположен на томе целевого сервера. Для операционной системы целевого сервера это выглядит как файл VHD. Вы можете сконфигурировать контроль доступа, чтобы соответствующим образом защитить диск.
- **Виртуальный диск iSCSI.** Виртуальный диск iSCSI в этом случае является действительным диском VHD, когда просматривается на целевом сервере, но с точки зрения клиента или инициатора он выглядит как диск, который может быть переведен в онлайновое или отключенное состояние и имеет созданные на нем тома.
- **Инициатор iSCSI.** Инициатор — это клиентское программное обеспечение, применяемое для подключения к целевому серверу и доступа к каким угодно виртуальным дискам iSCSI, которые были представлены и к которым авторизован доступ.

В наши дни эта технология является обычным явлением в большинстве компаний, и она позволяет создавать кластеры для бизнес-потребностей всех видов. Ранее нам приходилось использовать сервер Windows с целевым сервером iSCSI для создания кластера Hyper-V, предназначенного для функционирования в производственной сети. В следующем разделе мы разберем пример настройки целевой службы iSCSI, создания виртуального диска и его представления удаленной системе.

Добавление целевой службы iSCSI

По умолчанию целевая служба iSCSI не включена. Вы должны добавить ее с помощью PowerShell. Синтаксис для добавления компонента Windows под названием iSCSI Target Server выглядит так:

```
Add-windowsfeature FS-iSCSITarget-Server -IncludeManagementTools
```

После добавления компонента серверу может потребоваться перезагрузка, поэтому удостоверьтесь в том, что имеете возможность завершить установку.

Компонент iSCSI Target Server является частью роли File and Storage Services, а это значит, что его можно администрировать в консоли диспетчера серверов под узлом File and Storage Services, как показано на рис. 12.52.

Рис. 12.52. Управление целевым сервером iSCSI

Создание виртуального диска iSCSI

На рис. 12.52 видно, что есть две основных области: iSCSI Virtual Disks (Виртуальные диски iSCSI) и iSCSI Targets (Цели iSCSI). Как уже упоминалось, цель будет представлять виртуальные диски iSCSI, которые были созданы. (Не путайте их с виртуальными дисками в пространствах хранения. Они отличаются; виртуальные диски iSCSI на целевом сервере выглядят как файлы VHD.)

Чтобы продемонстрировать это, давайте создадим виртуальный диск iSCSI. В нашем примере мы будем использовать диск E, созданный ранее из многоуровневого пула хранения. Не беспокойтесь, если вы его не настроили; все, что вам необходимо — это диск и папка для сохранения файла VHD, который будет создан.

1. В центре области iSCSI Virtual Disks (Виртуальные диски iSCSI), показанной на рис. 12.52, щелкните на ссылке To create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard (Чтобы создать виртуальный диск iSCSI, запустите мастер создания виртуального диска iSCSI (New iSCSI Virtual Disk Wizard)).
2. Выберите целевой сервер в списке Server (Сервер) и том, где должен храниться виртуальный диск iSCSI. В данном примере диском будет `E:` (рис. 12.53).
3. Предоставьте виртуальному диску iSCSI описательное имя; например, если он предназначен для кластера Hyper-V, введите **`VMCluster_Vdisk`**. Обратите внимание на путь, отображающийся на экране iSCSI Virtual Disk Name (Имя виртуального диска iSCSI), который показан на рис. 12.54.
4. Укажите размер виртуального диска; в настоящем примере введите **`50 GB`**. Обратите внимание на опции; можно выбрать настройку всего пространства за один раз (Fixed (Фиксированный)), настройку динамически расширяемого диска (Dynamically Expanding (Динамическое расширение)) или применение разностного диска (Differencing (Разностный)). Если вы имели дело с Hyper-V, то опции должны быть вам хорошо знакомы.
5. В данном случае выберите Dynamically Expanding.

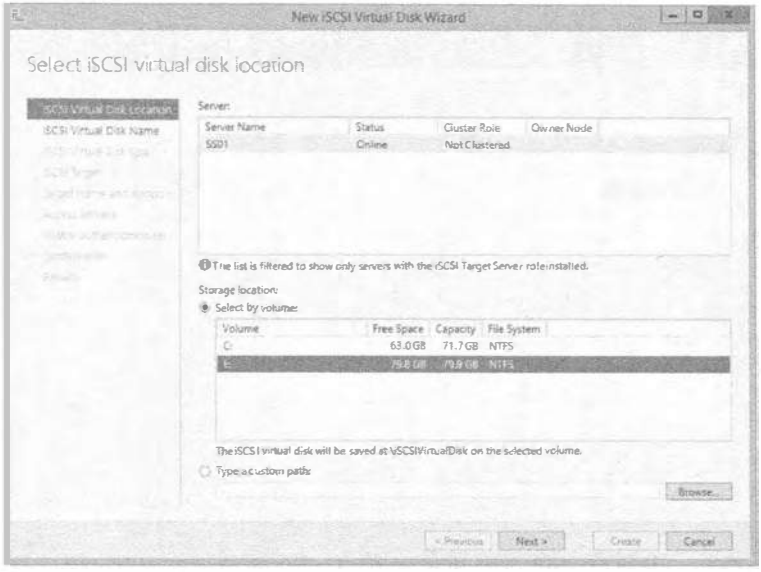


Рис. 12.53. Выбор сервера и тома для виртуального диска iSCSI

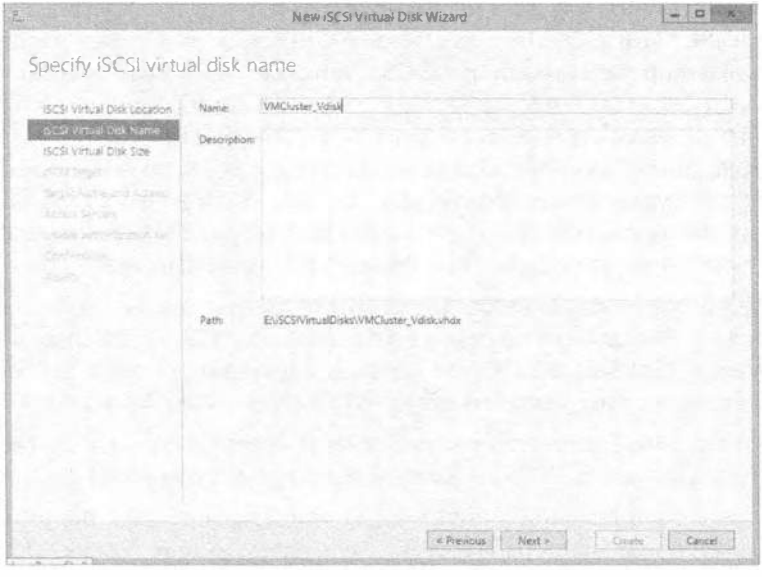


Рис. 12.54. Экран iSCSI Virtual Disk Name

Выбор между опциями Fixed и Dynamically Expanding

Полезно отметить, что вы должны соблюдать крайнюю осторожность, выбирая между опциями Fixed, Dynamically Expanding и Differencing. Выбор неподходящего типа диска окажет значительное влияние на производительность. В качестве эмпирического правила, если вы не уверены и не знаете тип рабочей нагрузки, который в конечном итоге будет использовать этот диск, выбирайте вариант Fixed.

6. Поскольку это новый сервер и пока что целевые серверы iSCSI отсутствуют, вы должны выбрать переключатель New iSCSI target (Новая цель iSCSI), как показано на рис. 12.55.
7. Укажите имя для цели iSCSI; в этом примере введите **`VMCluster_Target`** (рис. 12.56). Далее понадобится сконфигурировать доступ к созданному виртуальному диску iSCSI. Вы можете авторизовать специфичные инициаторы на основе их имен IQN или DNS, IP-адресов или MAC-адресов.

   IQN (iSCSI qualified name — определенное имя iSCSI) является автоматически сгенерированным именем. В серверах Microsoft оно всегда имеет формат `iqn.1991-06.com.microsoft:`*`имя_сервера`*.

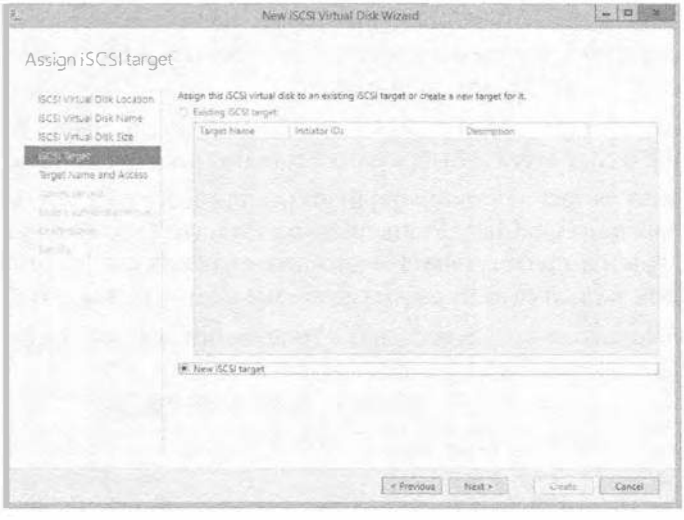


Рис. 12.55. Выбор переключателя New iSCSI target

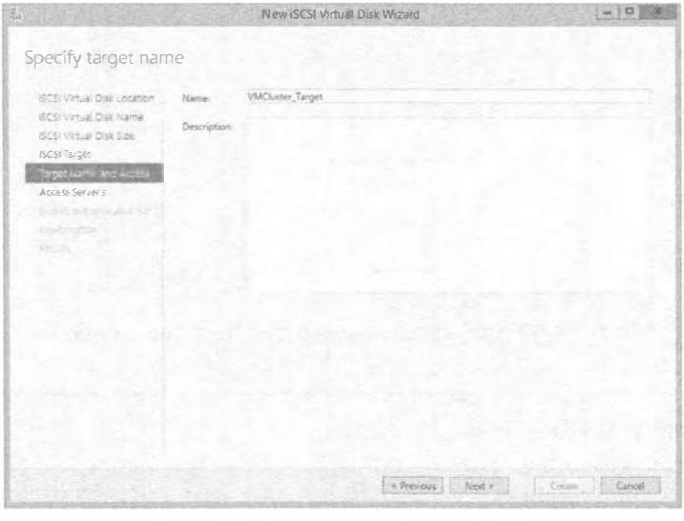


Рис. 12.56. Имя новой цели iSCSI

8. На экране Access Servers (Серверы доступа) мастера щелкните на кнопке Add (Добавить). Откроется диалоговое окно Add initiator ID (Добавление идентификатора инициатора), представленное на рис. 12.57.

   Если вы знакомы с технологией iSCSI, то заметите новую опцию для Windows Server 2012 и последующих версий. Когда определенное имя инициатора iSCSI не известно, его можно запросить у удаленного сервера. (IQN — это просто соглашение об именовании для iSCSI, которое соответствует формату имени машины; обычно оно следует такому формату: `iqn.1991-05.com.microsoft:server01.contoso.com`.)

   В прошлом при развертывании iSCSI мы отдавали предпочтение именам IQN, потому что они не меняются, если только не изменяется имя самой машины. Другие варианты, как было описано ранее, обладают возможностью легкого изменения в среде, и если вы представляете номера LUN удаленным машинам, то не хотите, чтобы это происходило.

9. Как показано на рис. 12.57, выберите переключатель Select from the initiator cache on the target server (Выбрать из кеша инициатора на целевом сервере).

   Далее можно запросить аутентификацию для номера LUN с применением CHAP (Challenge-Handshake Authentication Protocol (протокол аутентификации по методу "вызов-приветствие") — это протокол аутентификации для управления доступом к ресурсам). В рассматриваемом примере мы это проигнорируем.

10. Наконец, пересмотрите все настройки и щелкните на кнопке Create (Создать).

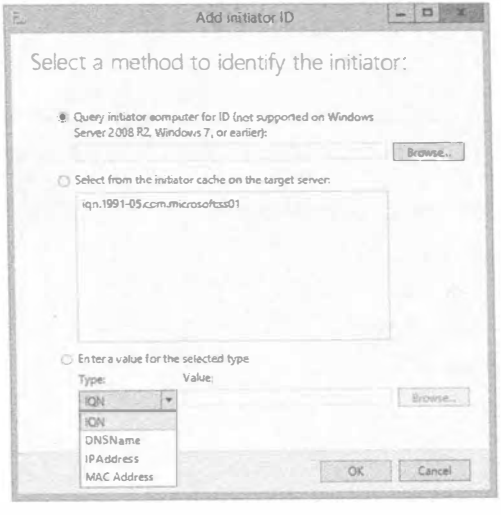


Рис. 12.57. Добавление идентификатора инициатора

Дополнительное упражнение

Воспользуйтесь командлетами iSCSI для просмотра целевого сервера iSCSI и развернутого виртуального диска. Для этого вам потребуются командлеты `Get-iSCSITargetServer` и `Get-iSCSIVirtualDisk`.

Хотите создать новый виртуальный диск для iSCSI в PowerShell и представить его цели? Ниже приведены примеры командлетов, которые можно применять.

1. Создайте виртуальный диск посредством командлета `New-iSCSIVirtualDisk`.

   Вот пример:

   ```
   New-IscsiVirtualDisk -path e:\newdisk.vhdx -SizeBytes 20GB
   -Computername SS01
   ```

2. Добавьте этот виртуальный диск к цели с помощью командлета `Add-IscsiVirtualDiskTargetMapping`.

   Вот пример:

   ```
   Add-IscsiVirtualDiskTargetMapping -TargetName VMcluster-Target
   -path e:\newdisk.vhdx
   ```

Дело сделано!

Подключение к виртуальному диску iSCSI со стороны клиента

Вы настроили целевой сервер iSCSI и новый виртуальный диск, но они не используются до тех пор, пока клиент не подключится к соответствующему номеру LUN. Вспомните, что если вы настроили списки доступа, то будете иметь возможность подключения к LUN только из указанной машины.

1. Выберите в меню Tools (Сервис) диспетчера серверов пункт iSCSI Initiator (Инициатор iSCSI), как показано на рис. 12.58.

   Откроется диалоговое окно iSCSI Initiator Properties (Свойства инициатора iSCSI).

2. Чтобы следовать нашему примеру, введите **`192.168.0.1`** в поле Target (Цель) и щелкните на кнопке Quick Connect (Быстро подключиться), как показано на рис. 12.59.

   Откроется диалоговое окно Quick Connect (Быстрое подключение), которое проверяет, что состоянием является Connected (Подключено). Это гарантирует видимость номера LUN и корректность настройки правил доступа (рис. 12.60). Для продолжения щелкните на кнопке Done (Готово).

Рис. 12.58. Нахождение инициатора iSCSI

Рис. 12.59. Диалоговое окно iSCSI Initiator Properties

Рис. 12.60. Успешное подключение к цели iSCSI

3. Перейдите на вкладку Volumes and Devices (Тома и устройства) и щелкните на кнопке Auto Configure (Сконфигурировать автоматически), как показано на рис. 12.61. Область Volume List (Список томов) автоматически заполнится томами, которые представляются клиенту.

Рис. 12.61. Вкладка Volumes and Devices

4. Наконец, в окне диспетчера серверов внутри узла File and Storage Services (Службы файлов и хранилища) щелкните на папке Volumes⇨Disks (Тома⇨Диски).

На рис. 12.62 видно, что появились два новых диска, для которых в столбце Bus Type (Тип шины) указано iSCSI. Теперь они готовы к форматированию и созданию стандартных томов.

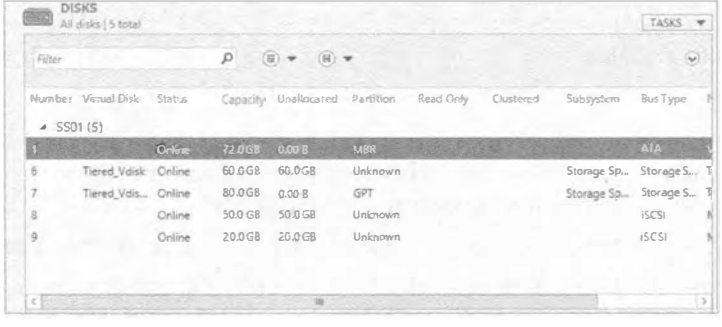


Рис. 12.62. Отображение добавленных дисков iSCSI

Общие ресурсы NFS

Сетевая файловая система (Network File System — NFS) позволяет совместно использовать файлы между сервером Windows и машинами с платформой Unix/Linux посредством протокола NFS Protocol. В Windows Server 2012 были внесены следующие усовершенствования.

- **Поддержка NFS версии 4.1.** Это включает упрощенный доступ через брандмауэры, протокол RPCSEC_GSS для расширенной безопасности, согласование безопасности клиентов и серверов, семантика файлов Windows и Unix, улучшенная поддержка для кластеризированных файловых серверов и дружественные к WAN составные процедуры.
- **Улучшенная производительность.** Никакой дополнительной настройки не требуется, т.к. за счет применения нового встроенного протокола RPC-XDR вы должны получить оптимальную производительность в готовом виде.
- **Более простое управление.** Задачи управления выполняются с помощью PowerShell и унифицированного графического пользовательского интерфейса в диспетчере серверов. Порт протокола RPC под номером 2049 упрощает конфигурирование брандмауэров. Еще одним усовершенствованием является улучшенное отображение удостоверений, к тому же появился новый поставщик WMIv2.
- **Усовершенствования, касающиеся высокой готовности NFSv3.** Теперь улучшены показатели времени обхода отказа с новыми настроенными путями обхода отказов для каждого физического дискового ресурса. Это ускоряет обход отказа для клиентов NFS.

Где используется общий ресурс NFS

Файловая система NFS применяется в средах, где существует требование наличия общих файловых ресурсов в среде со смесью операционных систем (таких как Windows и Unix/Linux). Благодаря усовершенствованиям в Windows Server 2012, вы теперь можете одновременно представлять общий ресурс с помощью NFS и SMB.

Обычное использование этого можно обнаружить в ряде гипервизоров от независимых разработчиков, в которых общие ресурсы Windows Server 2012 NFS применяются в качестве хранилищ данных для шаблонов и образов ISO.

Быстрая настройка общего ресурса NFS

Ниже мы покажем, как настроить общий ресурс NFS. Так как мы обычно спешим, давайте воспользуемся PowerShell. Добавьте службу NFS в Windows с помощью следующего синтаксиса:

```
Add-WindowsFeature FS-NFS-Service
```

В испытательной среде имеется каталог, к которому необходимо открыть совместное использование — `E:\shares`. Ниже описаны шаги, которые понадобится выполнить в графическом пользовательском интерфейсе.

1. Откройте диспетчер серверов и перейдите к роли File and Storage Services.
2. Щелкните на папке Shares (Общие ресурсы), т.к. мы собираемся работать с общими ресурсами. Появится область управления Shares (Общие ресурсы), как показано на рис. 12.63.

3. В области Shares выберите в раскрывающемся меню Tasks (Задачи) пункт New Share (Создать общий ресурс). Запустится мастер создания общего ресурса (New Share Wizard), окно которого представлено на рис. 12.64.
4. Выберите в списке File share profile (Профиль общего файлового ресурса) элемент NFS Share — Quick (Общий ресурс NFS — Быстрый).
5. Выберите свой сервер. В нашей испытательной среде им будет `SS01`.
6. На экране Share Location (Местоположение общего ресурса) выберите переключатель Type a custom path (Введите специальный путь) и введите путь к общему ресурсу. В нашей испытательной среде это `e:\shares` (рис. 12.65).

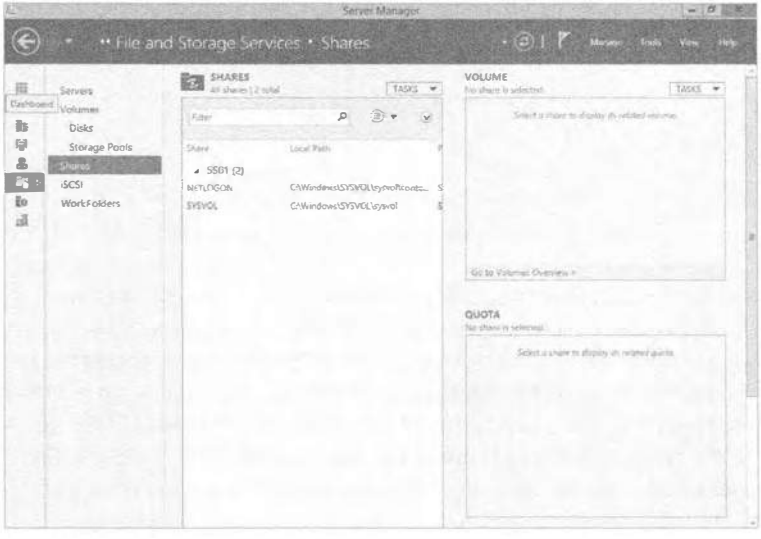


Рис. 12.63. Управление общими ресурсами в диспетчере серверов

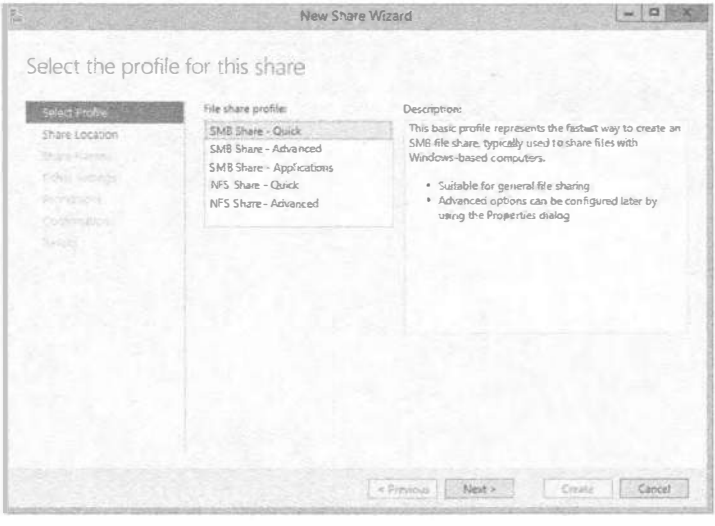


Рис. 12.64. Мастер New Share Wizard

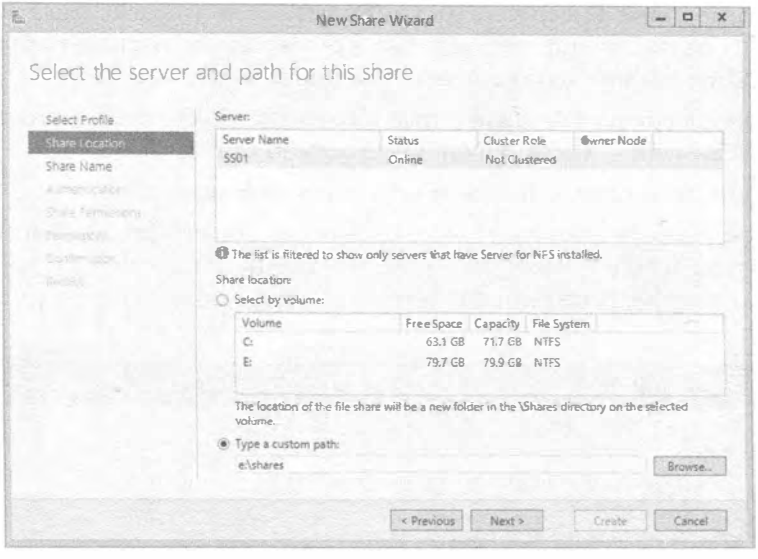


Рис. 12.65. Сервер и путь для общего ресурса

7. Введите имя общего ресурса. В нашей испытательной среде им будет `shares` (рис. 12.66). Выбор подходящего механизма аутентификации сильно зависит от среды, с которой вы интегрируетесь. В рассматриваемом случае мы не включали клиент Linux для аутентификации Kerberos, поскольку это автономный клиент. Как показано на рис. 12.67, мы отметили флажки No Server Authentication (AUTH_SYS) (Нет аутентификации на сервере (AUTH_SYS)) и Enable unmapped user access (Включить доступ неотображенных пользователей).

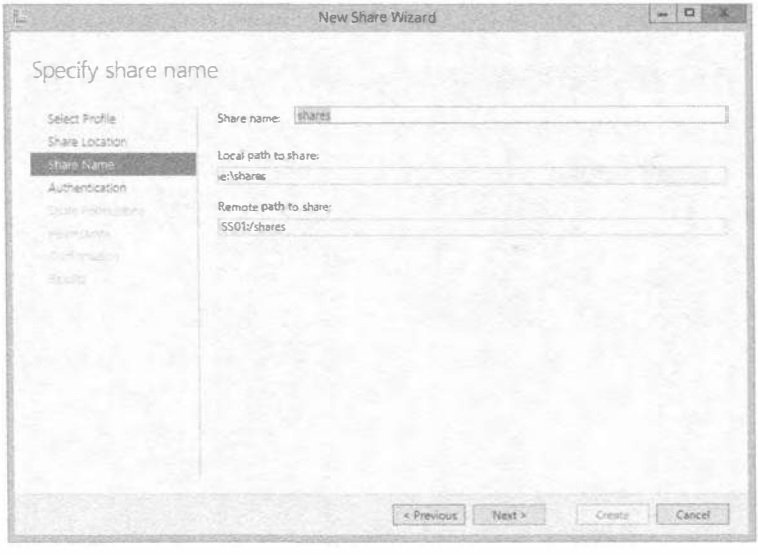


Рис. 12.66. Ввод имени общего ресурса

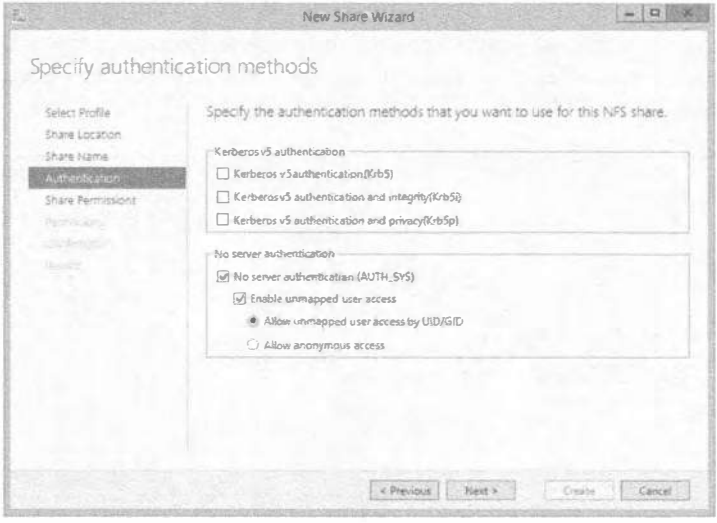


Рис. 12.67. Методы аутентификации

Дополнительно о хранилище

Бригада разработчиков, занимающаяся хранилищем в Microsoft, опубликовала цикл подробных статей, которые вы должны прочитать, если хотите получить дополнительные сведения о конфигурации и отображении удостоверений:

`http://blogs.technet.com/b/filecab/archive/2012/10/09/nfs-identitymapping-in-windows-server-2012.aspx`

8. На экране Share Permissions (Разрешения для общего ресурса) щелкните на кнопке Add (Добавить). В открывшемся диалоговом окне Add Permissions (Добавление разрешений) выберите переключатель All Machines (Все машины) и в списке Language encoding (Языковая кодировка) укажите ANSI. В списке Share permissions (Разрешения для общего ресурса) выберите Read / Write (Чтение / Запись), как показано на рис. 12.68.

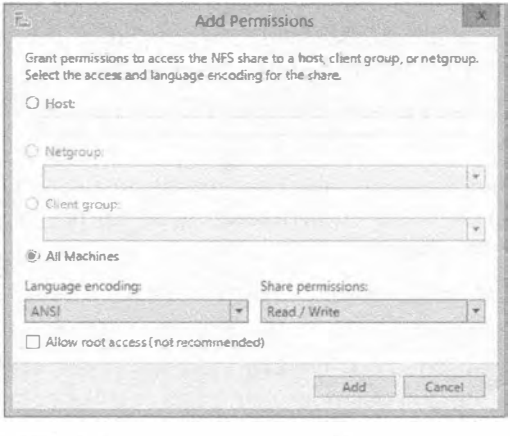


Рис. 12.68. Добавление разрешений для общего ресурса

9. На экране Specify permissions to control access (Указание разрешений для управления доступом) удостоверьтесь в том, что учетная запись Everyone (Все) существует и ей назначен уровень доступа Full Control (Полный доступ), как показано на рис. 12.69.

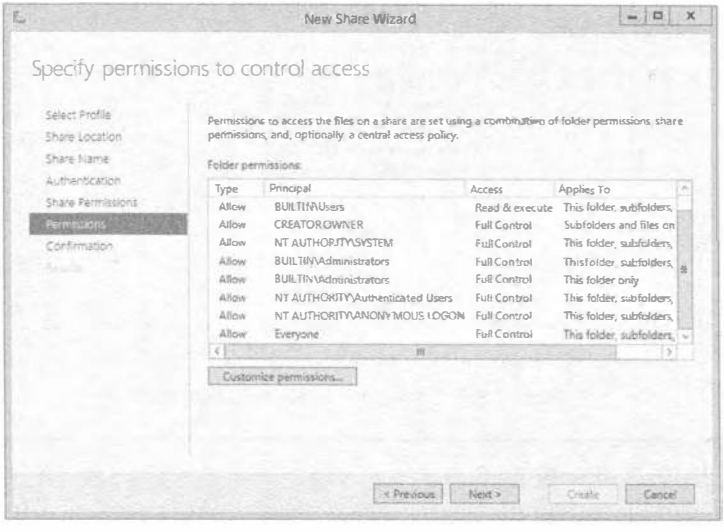


Рис. 12.69. Разрешения для управления доступом

10. Подтвердите выбранные установки и щелкните на кнопке Create (Создать), чтобы создать новый общий ресурс NFS.
11. Удостоверьтесь в успешном завершении создания и щелкните на кнопке Close (Закрыть).

Подключение к общему ресурсу NFS со стороны клиента

В нашей испытательной среде развернут дистрибутив Linux Mint. По умолчанию мы имеем возможность подключения к общему ресурсу, но при попытке обзора общего ресурса или создания на нем каталога возникают разнообразные ошибки. Наряду со многими другими дистрибутивами, Linux Mint требует установки пакета `nfs-common`, прежде чем можно будет читать из общего ресурса NFS. Для установки этого пакета выполните перечисленные далее шаги.

1. Введите в терминальном окне следующую команду:

   ```
   sudo apt-get install nfs-common
   ```

   Это установит необходимые элементы, чтобы позволить просматривать общий ресурс. Теперь вы можете смонтировать общий ресурс, ранее созданный на тестовом сервере Windows.

2. Введите в терминальном окне следующую команду:

   ```
   sudo mount -t nfs 192.168.0.1:/Shares /mnt/share
   ```

   Команда ничего не выводит; вместо этого вы должны перейти в каталог или указанную точку монтирования (`/mnt/share`). Ниже приведены объяснения этого синтаксиса.

- `sudo` — выполнение от имени суперпользователя (привилегированное выполнение определенных задач).
- `mount` — используется для монтирования различных типов файловых систем.
- `-t nfs` — для монтирования файловой системы NFS.
- `192.168.0.1:/Shares` — удаленный общий ресурс, который должен быть смонтирован.
- `/mnt/share` — локальная точка монтирования.

3. Перейдите к общему ресурсу, введя следующую команду:
   ```
   cd /mnt/share
   ```
4. Теперь просмотрите содержимое каталога с помощью такой команды:
   ```
   ls
   ```

На машине с Windows Server вы создали файл по имени `Readme.txt`. После ввода команды `ls` вы должны увидеть этот файл. Файл `Readme.txt` просто взят для примера; попробуйте поместить на общий ресурс в среде Windows Server собственные файлы и затем введите команду `ls` на клиентской машине Linux.

Дедупликация: диск и сеть

В Windows Server 2012 в качестве встроенного средства хранения появилась *дедупликация данных* (Data Deduplication). Дедупликация данных — это более эффективный способ хранения данных. С постоянно растущей потребностью в хранилище в облачных технологиях вы легко можете себе представить объем хранящихся дублированных файлов. Даже дома зачастую имеется несколько копий файлов ISO или виртуальных жестких дисков для хранилища USB и серверов. Каждый такой файл занимает 3–7 Гбайт. Из-за хранения множества копий и отсутствия продуманной библиотечной системы понапрасну расходуется много пространства хранения.

Это простой пример, но он поднимает другой вопрос: все файлы имеют похожие части и все они занимают место. Согласитесь, что было бы замечательно, если бы существовала возможность идентификации таких общих порций, создания единственной главной ссылки на диске и затем указания на нее из всех других файлов, которые имеют эту общую порцию? Дедупликация данных предоставляет эту возможность.

Дедупликация данных в Windows применяет концепцию под названием *хранилище фрагментов* (chunk store). Файл разделяется на фрагменты переменных размеров, обычно между 32 Кбайт и 128 Кбайт; в среднем фрагмент имеет размер около 64 Кбайт. Такие фрагменты сжимаются и помещаются в хранилище фрагментов. Каждый фрагмент хранится в контейнере фрагментов, который растет в размерах до 1 Гбайт, прежде чем будет создан новый контейнер. Просмотреть хранилище фрагментов и его контейнеры можно в корне тома, в папке по имени `System Volume Information` (Системная информация о томе). По умолчанию эта папка заблокирована для просмотра только от имени учетной записи `System` (Система), так что вы должны получить права владения ею и удостовериться, что у учетной записи `System` остается к ней полный доступ. Точка повторной обработки (reparse point) заменяет нормальный файл. При доступе к файлу точка повторной обработки показывает, где хранятся данные, и восстанавливает файл (рис. 12.70).

Рис. 12.70. Дедупликация данных в действии

Хотя компонент Data Deduplication по умолчанию не устанавливается, он спроектирован так, чтобы легко развертываться. Он также разработан с *нулевым* воздействием на пользователей; в сущности, пользователи даже ничего не заметят. Включить Data Deduplication на любом из основных томов данных можно с минимальным влиянием на производительность. Компонент спроектирован так, чтобы не пересекаться с файлами, которые являются новыми или в которые в текущий момент производится запись. Компонент будет ожидать и каждый час проверять, не появились ли файлы, пригодные для дедупликации. Вы можете изменить график этого процесса, приведя его в соответствие с нуждами компании.

Выяснение пригодности к дедупликации начинается с файлов, которые существуют более трех дней (эту настройку можно изменить), при этом из процесса всегда исключаются файлы с размером меньше 32 Кбайт, файлы с расширенными атрибутами или зашифрованные файлы. Если у вас есть другие файлы, которые вы не хотите подвергать процессу дедупликации, это также поддается конфигурированию.

Дедупликация происходит также в сетевом трафике. К отправляемому или получаемому трафику производится доступ с целью выяснения, может ли в отношении него быть проведена дедупликация, потенциально сокращая объем этого трафика. В отличие от дедупликации хранилища, график или тип данных для сетевой дедупликации изменять нельзя.

Тем не менее, есть несколько моментов, о которых следует знать перед тем, как продолжить. Дедупликация поддерживается только на томах NTFS, и ее невозможно выполнить на загрузочном или системном диске. В Windows Server 2012 она не может использоваться с томами CSV, живыми виртуальными машинами или базами данных SQL.

Так чего же нового версия Windows Server 2012 R2 привнесла в дедупликацию данных? Основное внимание было сосредоточено на разрешении дедупликации для живых виртуальных машин. Все верно; вы можете выполнять дедупликацию файлов VHD и VHDX, которыми пользуются живые виртуальные машины. Главным образом, вы можете применять ее в сценариях VDI (Virtual Desktop Infrastructure — инфраструктура виртуальных рабочих столов), с дальнейшей ориентацией на удаленное хранилище. Благодаря таким улучшениям, дедупликацию данных можно проводить в среде VDI. Также полезно отметить, что хотя она не поддерживается для других виртуализированных рабочих нагрузок, не существует каких-то специальных блокирующих средств, препятствующих ее включению. Как всегда, результаты не могут быть гарантированными.

Это удивительная технология, встроенная в Windows Server, которая обеспечит значительную экономию объема хранилища. Далее мы посмотрим, как ее конфигурировать.

Для начала понадобится добавить компонент Data Deduplication. Это можно сделать с помощью PowerShell. Синтаксис выглядит следующим образом:

```
Add-WindowsFeature FS-Data-Deduplication
```

Затем его можно конфигурировать через диспетчер серверов или PowerShell.

Конфигурирование дедупликации данных с помощью диспетчера серверов

Первым мы рассмотрим метод с диспетчером серверов.

1. Откройте диспетчер серверов, щелкните на File and Storage Services и выберите папку Volumes (Тома).
2. Щелкните правой кнопкой мыши на томе, для которого требуется сконфигурировать дедупликацию данных, и выберите в контекстном меню пункт Configure Data Deduplication (Конфигурировать дедупликацию данных), как показано на рис. 12.71.

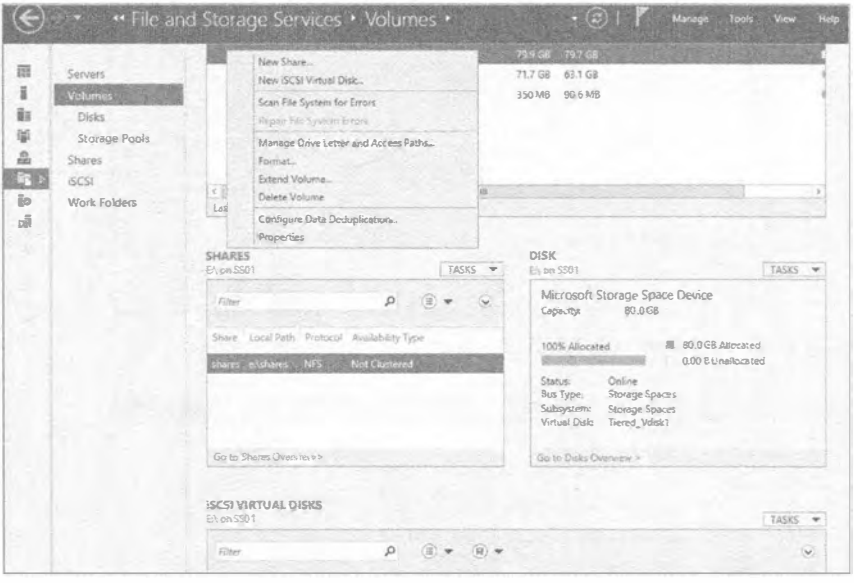


Рис. 12.71. Конфигурирование дедупликации данных

3. Выберите в раскрывающемся списке Data deduplication (Дедупликация данных) элемент General purpose file server (Файловый сервер общего назначения).

   Обратите внимание на еще один элемент, Virtual Desktop Infrastructure (VDI) server (Сервер инфраструктуры виртуальных рабочих столов (VDI)), показанный на рис. 12.72. Щелкните на кнопке OK.

   Далее необходимо решить, сколько должны просуществовать файлы, прежде чем они будут обработаны механизмом дедупликации. Это значит, что механизм не будет оказывать воздействие на вновь созданные файлы в течение указанного периода времени.

4. В нашем примере оставьте период в 3 дня.

   При желании позже это значение можно изменить (рис. 12.73).

   Кроме того, на этом экране можно выбрать любые файловые расширения, которые должны быть исключены из процесса дедупликации. Например, может быть нежелательно подвергать дедупликации базу данных SQL или Access. Чтобы указать в поле несколько расширений, разделяйте их запятыми. Например, если вы хотите исключить файлы баз данных SQL и файлы баз данных Active Directory (`ntds.dit`), то должны ввести в поле **`mdf,dit`**.

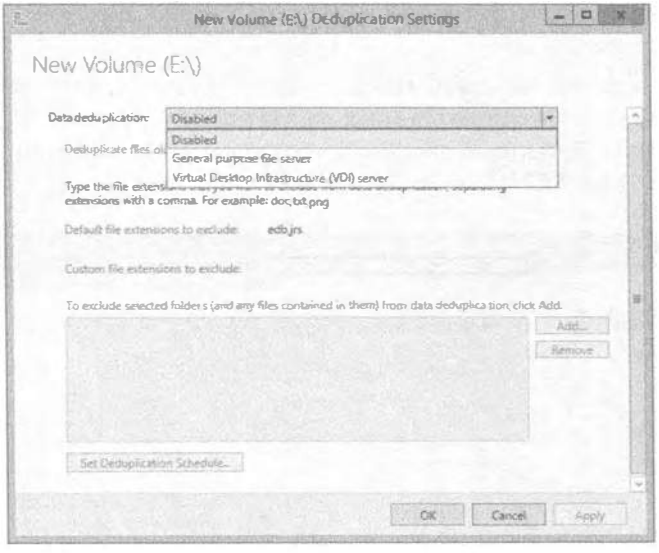


Рис. 12.72. Включение дедупликации данных

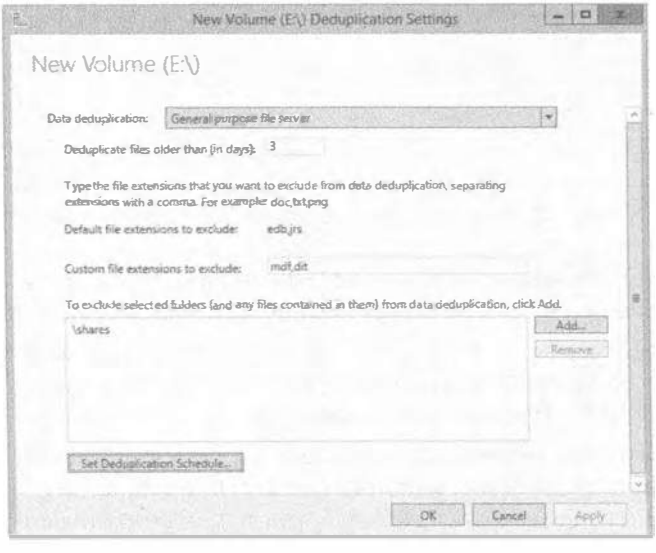


Рис. 12.73. Конфигурирование настроек дедупликации нового тома

5. Исключите файловые расширения, как показано на рис. 12.73.

   Исключение файла — это хорошо, но в организации могут существовать папки, которые являются очень чувствительными, и по этой причине не должны подвергаться дедупликации. Они могут иметь общие фрагменты, но вы не можете идти на риск повреждения диска на месте хранилища фрагментов, что потенциально могло бы затронуть информацию. Разумеется, это весьма маловероятный сценарий, но он просто демонстрирует возможность исключения папки с чувствительной информацией.

6. В этом случае мы исключим папку `E:\shares`, т.к. в ней ранее был создан общий ресурс NFS.

   Мы не на 100% уверены в том, что именно здесь будет храниться, поэтому не хотим брать на себя риск, не проведя дальнейшее исследование.

   В начале этой главы говорилось о том, что механизм дедупликации имеет фоновый процесс, который по умолчанию запускается каждый час. На рис. 12.73 видно, что есть также опция для изменения этого графика запуска.

7. Щелкните на кнопке Set Deduplication Schedule (Установить график дедупликации). Откроется диалоговое окно с набором флажков (рис. 12.74).

   По умолчанию флажок Enable background optimization (Включить оптимизацию фоновой обработки) отмечен, но можно также отметить флажок Enable throughput optimization (Включить оптимизацию пропускной способности), что инициирует задачу оптимизации при обработке больших объемов данных. В Microsoft утверждают, что пропускная способность дедупликации составляет приблизительно 2 Тбайт данных на том в 24-часовой период на единственном томе. Если томов несколько, работа на них может выполняться параллельно.

Рис. 12.74. Изменение графика дедупликации

8. В рассматриваемом примере оставьте график в том виде, как есть.

   Когда вы просмотрите том в диспетчере серверов, то обнаружите столбцы Deduplication Rate (Доля дедупликации), содержащий процентное значение, и Deduplication Savings (Экономия от дедупликации), содержащий значение в байтах (рис. 12.75).

Рис. 12.75. Просмотр сведений о дедупликации в диспетчере серверов

Конфигурирование дедупликации данных с помощью PowerShell

А теперь мы покажем, как работать с дедупликацией в PowerShell. На рис. 12.76 можно видеть доступные командлеты PowerShell.

```
PS C:\Users\Administrator> get-command -Module DeDuplication

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Function        Disable-DedupVolume                                DeDuplication
Function        Enable-DedupVolume                                 DeDuplication
Function        Expand-DedupFile                                   DeDuplication
Function        Get-DedupJob                                       DeDuplication
Function        Get-DedupMetadata                                  DeDuplication
Function        Get-DedupSchedule                                  DeDuplication
Function        Get-DedupStatus                                    DeDuplication
Function        Get-DedupVolume                                    DeDuplication
Function        Measure-DedupFileMetadata                          DeDuplication
Function        New-DedupSchedule                                  DeDuplication
Function        Remove-DedupSchedule                               DeDuplication
Function        Set-DedupSchedule                                  DeDuplication
Function        Set-DedupVolume                                    DeDuplication
Function        Start-DedupJob                                     DeDuplication
Function        Stop-DedupJob                                      DeDuplication
Function        Update-DedupStatus                                 DeDuplication

PS C:\Users\Administrator> _
```

Рис. 12.76. Командлеты PowerShell, предназначенные для дедупликации

1. Чтобы включить дедупликацию для тома, воспользуйтесь следующим синтаксисом:

   ```
   Enable-DedupVolume E:\
   ```

   Вывод показан на рис. 12.77.

   Теперь, когда известно, что дедупликация включена, вы хотите выяснить, какую экономию она обеспечивает.

Рис. 12.77. Вывод из командлета PowerShell, включающего дедупликацию

2. Запустите командлет `Get-DedupStatus` (рис. 12.78).

   На томах в нашей испытательной среде недостаточно много информации, чтобы провести дедупликацию, поэтому все значения на рис. 12.78 оказываются нулевыми, но это не просто так.

Рис. 12.78. Вывод из командлета `Get-DeDupStatus`

В конфигурации мы исключили `E:\shares`, т.к. мы не на 100% уверены в том, что именно здесь будет храниться, и поскольку это общий ресурс NFS для Linux, мы не хотим рисковать. (С практической точки зрения тип клиента не играет никакой роли; все прозрачно.) Внутрь `E:\shares` мы скопировали ISO-образ `Win2012R2_Preview`, имеющий размер около 4 Гбайт. Мы создали дополнительную папку `E:\TestData` и скопировали в нее два ISO-образа `Win2012R2_Preview` под разными именами, а также создали папку `Technical`, которая содержит документы с технической информацией (рис. 12.79).

Помните, что несмотря на копирование данных, мы должны подождать три дня, прежде чем они включатся в дедупликацию? Но мы не хотим ждать настолько долго, поэтому воспользуемся командлетом `Start-DedupJob`, чтобы ускорить процесс.

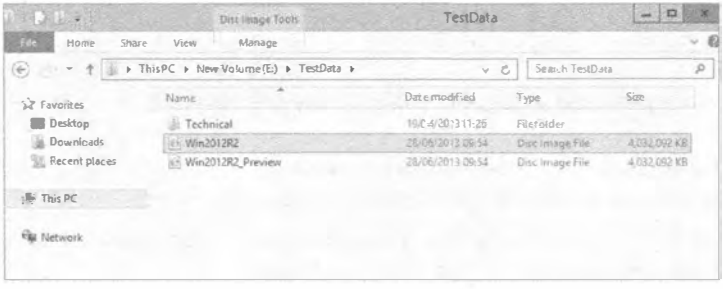


Рис. 12.79. Содержимое папки `E:\TestData`

3. Синтаксис командлета `Start-DedupJob` выглядит так:

   ```
   Start-DedupJob -Type Optimization -Volume E:
   ```

   Как показано на рис. 12.80, дедупликация была запущена по ручному графику и ее текущим состоянием является `Queued` (В очереди). При желании ее можно ускорить.

```
PS C:\Users\Administrator> start-dedupjob -type Optimization -Volume E:

Type         ScheduleType  StartTime  Progress  State   Volume
----         ------------  ---------  --------  -----   ------
Optimization Manual                   0 %       Queued  E:
```

Рис. 12.80. Вывод из командлета `Start-DedupJob`

4. В окне планировщика задач выберите папку Task Scheduler Library\Microsoft\Windows\Deduplication (Библиотека планировщика задач \ Microsoft \ Windows \ Дедупликация).

   На рис. 12.81 видны три задания (последние два из них мы объясним позже в этой главе):

   - `BackgroundOptimization`
   - `WeeklyGarbargeCollection`
   - `WeeklyScrubbing`

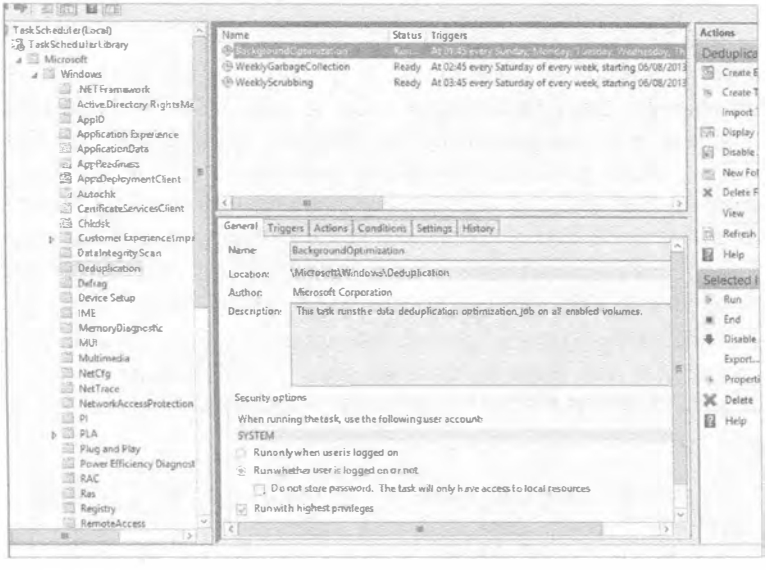


Рис. 12.81. Ручное инициирование задания `BackgroundOptimization`

5. Щелкните правой кнопкой мыши на задании `BackgroundOptimization`, возвратитесь в окно PowerShell и запустите командлет `Get-DedupJob`.

   Пример вывода показан на рис. 12.82. На рис. 12.83 видно, сколько уже было сэкономлено, и это процесс еще не завершен.

```
PS C:\Users\Administrator> Get-DedupJob

Type         ScheduleType  StartTime  Progress  State   Volume
----         ------------  ---------  --------  -----   ------
Optimization Scheduled                0 %       Queued  E:
Optimization Manual        05:35      14 %      Running E:

PS C:\Users\Administrator>
```

Рис. 12.82. Пример вывода из командлета `Get-DedupJob`

Рис. 12.83. Вывод из командлета `Get-DedupStatus` во время выполнения `Get-DedupJob`

6. Теперь сравните вывод на рис. 12.83 с выводом на рис. 12.84, когда командлет `Get-DedupJob` завершил работу.

   В нашей испытательной среде мы сэкономили 4,64 Гбайт, что великолепно, т.к. объем хранилища недостаточен.

Рис. 12.84. Вывод из командлета `Get-DedupStatus`, когда оптимизация завершена

7. Попробуйте запустить командлет `Get-DeDupVolume` для получения разного вывода.
8. В качестве дополнительного упражнения удалите папку `E:\Shares` из списка исключений и снова запустите задание оптимизации.

   Сколько пространства освободилось теперь?
9. Наконец, щелкните правой кнопкой мыши на папке `E:\TestData` и выберите в контекстном меню пункт Properties (Свойства).

   На рис. 12.85 показано диалоговое окно свойств папки `TestData` в нашей испытательной среде. Обратили внимание на разницу между значениями Size (Размер) и Size on disk (Размер на диске)?

   Итак, вы увидели дедупликацию в действии. Но куда делись данные?
10. Запустите командлет `Get-DedupMetadata`, чтобы просмотреть информацию о хранилище фрагментов, о котором шла речь в начале раздела. Вывод из командлета представлен на рис. 12.86.

Рис. 12.85. Свойства папки после проведения дедупликации

Как было показано на рис. 12.81, в планировщике задач имеются еще два задания, которые запускаются на еженедельной основе. Давайте посмотрим, что это за задания. Начнем с `GarbageCollection`.

```
PS E:\> Get-DedupMetadata

Volume                          : E:
VolumeId                        : \\?\Volume{e6b09afc-bb2d-4917-b6b7-6722f370af3a}\
StoreId                         : {361C0163-33CE-4845-A816-9E6357C2A32E}
DataChunkCount                  : 65472
DataContainerCount              : 47
DataChunkAverageSize            : 72.67 KB
DataChunkMedianSize             : 0 B
DataStoreUncompactedFreespace   : 0 B
StreamMapChunkCount             : 52
StreamMapContainerCount         : 1
StreamMapAverageDataChunkCount  :
StreamMapMedianDataChunkCount   :
StreamMapMaxDataChunkCount      :
HotspotChunkCount               : 0
HotspotContainerCount           : 0
HotspotMedianReferenceCount     :
CorruptionLogEntryCount         : 0
TotalChunkStoreSize             : 4.57 GB
```

Рис. 12.86. Вывод из командлета `Get-DedupMetadata`

По умолчанию задание `GarbageCollection` сконфигурировано на запуск еженедельно, но при необходимости его можно инициировать вручную. Задание `GarbageCollection` очищает хранилище фрагментов, удаляя неиспользуемые фрагменты, что освобождает дисковое пространство. Вы увидите, что это очень важное задание.

Чтобы вручную инициировать сборку мусора, запустите командлет `Start-DedupJob` следующим образом:

```
Start-DeDupjob -Type GarbageCollection -volume E:
```

Это поставит задание в очередь на выполнение во время простоя системы; в качестве альтернативы можно принудительно ускорить его выполнение в планировщике задач.

Дополнительное упражнение

Удалите все файлы ISO, которые были задействованы в примере, и очистите корзину. Запустите задание оптимизации, а затем и задание сборки мусора. После завершения этих заданий просмотрите размер хранилища фрагментов с применением командлета `Get-DedupMetadata`. Ниже показано, что размер хранилища фрагментов в результате уменьшился.

```
PS E:\> Get-DedupMetadata

Volume                          : E:
VolumeId                        : \\?\Volume{e6b09afc-bb2d-4917-b6b7-6722f370af3a}\
StoreId                         : {361C0163-33CE-4845-A816-9E6357C2A32E}
DataChunkCount                  : 19950
DataContainerCount              : 47
DataChunkAverageSize            : 75.5 KB
DataChunkMedianSize             : 0 B
DataStoreUncompactedFreespace   : 0 B
StreamMapChunkCount             : 44
StreamMapContainerCount         : 1
StreamMapAverageDataChunkCount  :
StreamMapMedianDataChunkCount   :
StreamMapMaxDataChunkCount      :
HotspotChunkCount               : 0
HotspotContainerCount           : 0
HotspotMedianReferenceCount     :
CorruptionLogEntryCount         : 0
TotalChunkStoreSize             : 1.44 GB
```

Проверка томов на предмет повреждений

Последним аспектом, относящимся к дедупликации, является проверка томов на предмет повреждений. Как несложно себе представить, чем больше общих данных обнаруживается в файлах, тем в большей степени будет расти хранилище фрагментов, и тем больше точек повторной обработки будет существовать на диске.

Предположим, что сектор диска, где располагается часть фрагмента, оказался поврежденным. Возникает риск потери сотен, а то и тысяч файлов. Хотя это редкое явление, особенно если вы дополнительно пользуетесь технологиями обеспечения отказоустойчивости, возможность его возникновения все же существует. Механизм дедупликации предлагает несколько специальных встроенных проверок, которые предотвращают такую ситуацию.

Например, дедупликация вводит избыточность для критически важных метаданных; она также предоставляет избыточность для фрагментов с самым частым обращением (если к фрагменту производится доступ более 100 раз, он становится горячей точкой). Дедупликация записывает в журнальный файл детали о любом повреждении, и позже за счет использования заданий очистки анализирует этот журнал и делает соответствующие исправления.

Исправления могут производиться с применением резервной копии при обращении к критически важным метаданным или горячей точке. Если дедупликация выполнялась в отношении пространства хранения с зеркальным отображением, то для исправления фрагмента она может использовать зеркальные данные.

Подобно заданиям оптимизации и сборки мусора, задания очистки запускаются по установленному графику, который можно настроить на более частое выполнение, чем по умолчанию один раз в неделю.

Запустить задание с помощью PowerShell можно следующим образом:

```
Start-DeDupJob -Type Scrubbing -Volume E:
```

Это инициирует задание верификации для диска `E:`, но проверяться будут только записи в журнальном файле повреждений.

Чтобы проверить целостность всего дедуплицированного тома, введите такую команду:

```
Start-DeDupJon -Type Scrubbing -Volume E: -full
```

Для просмотра результатов очистки запустите программу просмотра событий (Event Viewer). Весь вывод задания очистки хранится в узле Event Viewer\Applications and Services Logs\Microsoft\Windows\Deduplication\Scrubbing (Просмотр событий \ Журналы приложений и служб \ Microsoft \ Windows \ Дедупликация \ Очистка). Журнал очистки можно видеть на рис. 12.87.

Резюме

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?

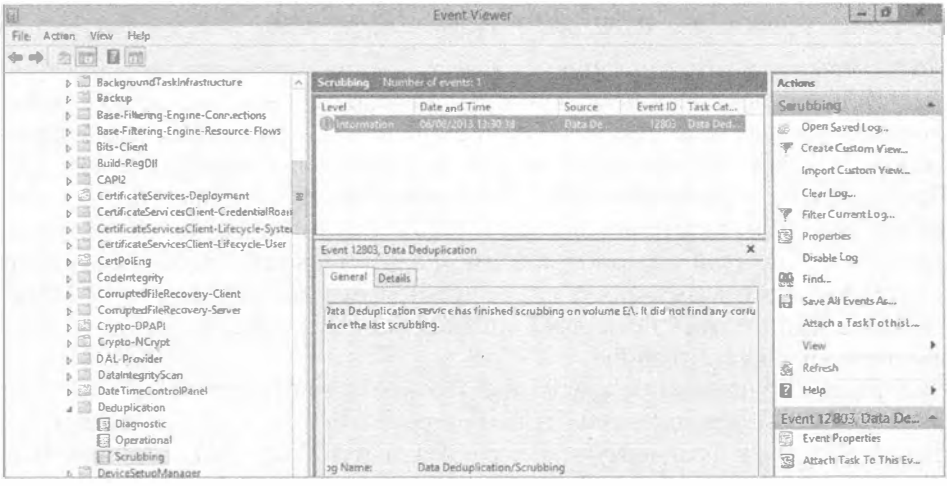


Рис. 12.87. Журнал очистки в программе просмотра событий

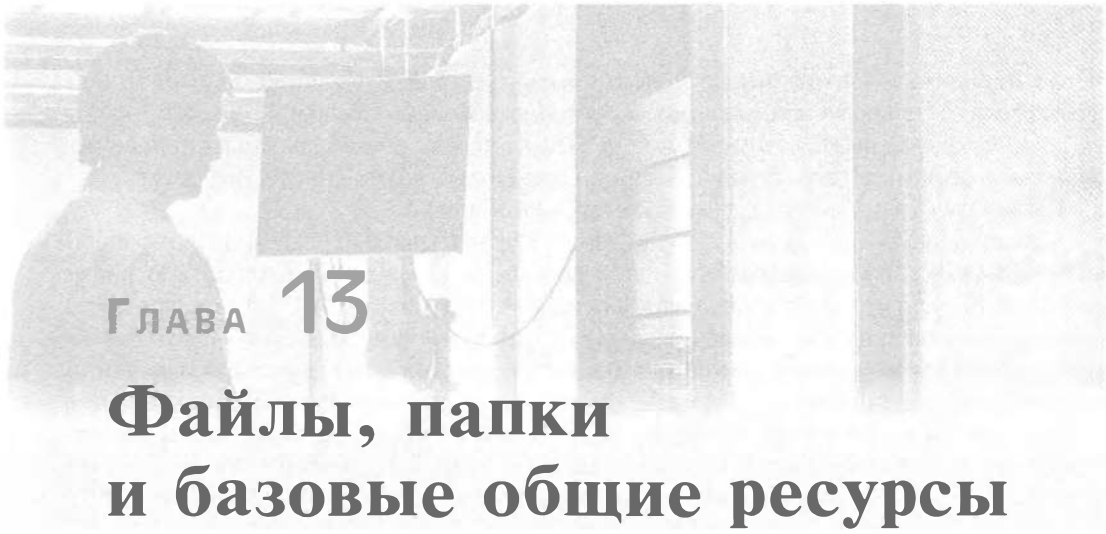
Контрольный вопрос. Создайте в испытательной среде пул хранения с тремя дисками, используя графический пользовательский интерфейс. Создайте виртуальный диск с размером в три раза больше общей полезной емкости диска. Сформатируйте его и подготовьте к работе.

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.

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.



Глава 13

Файлы, папки и базовые общие ресурсы

Одной из основных функций любого сервера является обслуживание ресурсов, таких как файлы и папки. В Windows Server 2012 R2 роли File Services (Службы файлов) и Storage Services (Службы хранилища) были объединены в одну роль под названием File and Storage Services (Службы файлов и хранилища). Эта роль устанавливается по умолчанию; однако любые дополнительные роли, которые обслуживают File and Storage Services, понадобится добавить посредством мастера в диспетчере серверов. Роль File Services включает службы роли наподобие диспетчера ресурсов файлового сервера (File Server Resource Manager — FSRM), службы для сетевой файловой системы (Network File System — NFS), обеспечивающие поддержку клиентов Unix, службу поиска в Windows (Windows Search) и службу BranchCache для удаленных офисов. Теперь, когда роль Storage Services доступна в сочетании с ролью File Services, в Windows Server 2012 R2 предлагается несколько новых и усовершенствованных ролей и компонентов, в том числе дедупликация (Deduplication), пространства хранения (Storage Spaces) и пулы хранения (Storage Pools), которые еще более улучшают эту версию Windows Server.

Когда вы планируете совместное использование файлов и папок, важно понимать не только то, как открыть общий доступ к данным, но также и то, как защитить их с помощью разрешений, включая разрешения файловой системы New Technology File System (NTFS) и общего доступа. Хотя оба набора разрешений применяются независимо, они обеспечивают накопительный эффект, предоставляя множество уровней расширенных параметров безопасности. Вы должны быть в состоянии быстро определить, какие окончательные разрешения имеет пользователь, который обращается к общему ресурсу через сеть. И если вы хотите защитить целые жесткие диски, то по-прежнему можете применять компонент BitLocker Drive Encryption (Шифрование диска BitLocker), чтобы шифровать их содержимое, как это делалось в Windows Server 2008 R2. Одной из наиболее заметных новых возможностей в шифровании дисков Windows Server 2012 R2 являются новые опции BitLocker

Drive Encryption. Теперь можно использовать опцию Encrypt used disk space only (Шифровать только использованное пространство диска). Больше не нужно ждать часами, пока завершится шифрование целого тома, в то время как занята только небольшая часть общего пространства на диске. Новые возможности BitLocker более подробно рассматриваются ближе к концу этой главы.

Лежащим в основе протоколом, который обрабатывает передачи файлов, является SMB (Server Message Block — блок сообщений сервера), который в Windows Server 2012 был модернизирован до версии 3.0. Протокол SMB 3.0 поддерживает много новых функций, которые превращают файловые общие ресурсы в фундамент для небольших и средних компаний. Этот стек протоколов обеспечивает ряд значительных преимуществ при передаче файлов по сети — при условии подключения к правильным видам клиентов. При подключении к унаследованным машинам по-прежнему будут применяться версии SMB 1.0 и SMB 2.0, со всеми присущими им проблемами. В настоящее время только Windows 8 и семейство Windows Server 2012 могут извлечь полную выгоду от новых функций SMB 3.0, которые будут обсуждаться в этой главе.

В этой главе вы изучите следующие темы:

- установка на сервере дополнительных ролей File and Storage Services;
- объединение разрешений общего доступа и NTFS;
- внедрение BitLocker Drive Encryption.

Роль File and Storage Services

Роль File and Storage Services комбинирует множество файловых технологий и технологий хранения, которые оказывают администраторам содействие в настройке файловых серверов для их организации. Стандартная установка сделает возможным базовое администрирование функциональности хранилища с применением диспетчера серверов или PowerShell, но для построения подходящего файлового сервера желательно установить роль File Server (Файловый сервер) наряду с другими важными ролями вроде File Server Resource Manager (Диспетчер ресурсов файлового сервера) и DFS Replication (Репликация DFS). Дело вовсе не в том, что файловая система DFS требуется все время — но она определенно может быть великолепным дополнением, когда необходима репликация для обеспечения доступности или репликация между географически разбросанными местоположениями. Важно иметь план и конечную цель для серверных ролей. Постарайтесь получить максимальную отдачу от первого прохода мастера за счет соответствующего планирования. Мы будем добавлять роли в следующем разделе.

Основной компонент любого сервера — его способность к совместному использованию файлов. На самом деле служба Server (Сервер) во всем семействе операционных систем Windows Server (включая Windows Server 2012 R2) обрабатывает базовые возможности сервера по общему доступу к файлам и печати. Но что именно это значит и почему оно настолько важно? По умолчанию одно лишь наличие функционирующего сервера вовсе не означает доступность любых ресурсов для пользователей. Прежде чем они смогут действительно работать с ресурсами, к этим ресурсам должен быть открыт общий доступ. Предположим, что на локальном диске `F` имеется папка под названием `Apps` с тремя подпапками (рис. 13.1).

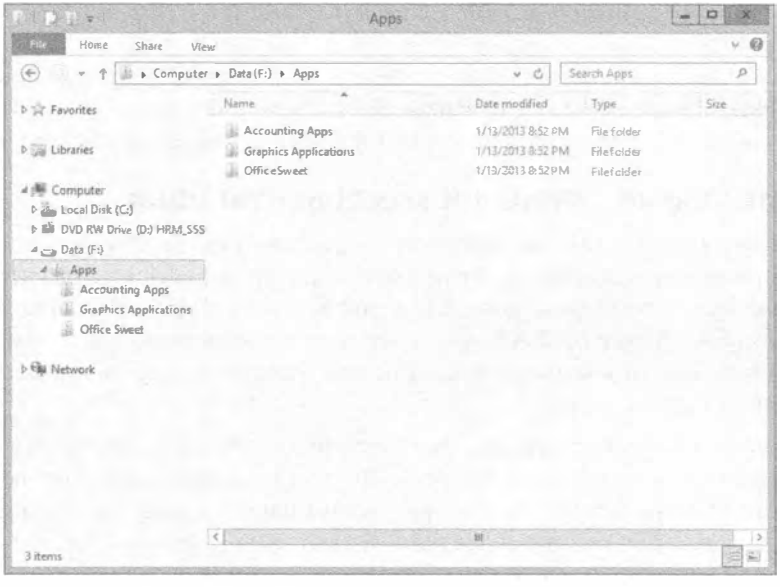


Рис. 13.1. Подпапки внутри папки `F:\Apps`

Когда вы открываете общий доступ к этой папке через сеть под именем `Apps`, вы разрешаете клиентам отображать новую букву диска на своих машинах на вашу папку `F:\Apps`. За счет такого отображения вы помещаете виртуальный указатель прямо на удаленный диск. Если вы отображаете диск `M` клиента на общий ресурс `Apps` сервера, то диск `M` будет выглядеть идентичным папке `F:\Apps` сервера, как показано на рис. 13.2.

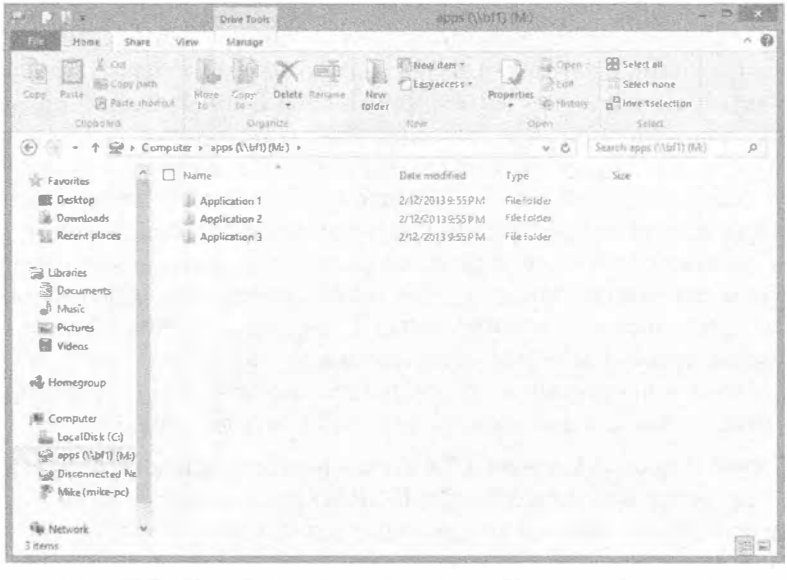


Рис. 13.2. Общий ресурс `BF1\Apps`, отображенный на диск `M`

Не беспокойтесь; позже в этой главе мы объясним, как создавать такой общий ресурс и подключаться к нему. Это все, что действительно нужно сделать. Совместное использование ресурсов означает, что вы позволяете пользователям обращаться к этим ресурсам из сети. Никакой реальной обработки со стороны сервера не производится; он просто раздает файлы и папки в том виде, как они есть.

Дополнительные службы и компоненты роли

Диспетчер серверов (Server Manager) — это одиночная консоль, включающая множество разделов, которые могут применяться для управления различными серверными ролями, в том числе ролью File and Storage Services. Роль File and Storage Services в Windows Server 2012 R2 позволяет делать намного больше, чем просто открывать общий доступ к папкам. Роль File and Storage Services включает несколько дополнительных служб роли.

- **File Server (Файловый сервер).** Это главная служба роли, требуемая для поддержки роли File and Storage Services. Данная роль предоставляет возможность создания и управления общими ресурсами наряду с разрешением пользователям открывать совместный доступ и обращаться к файлам, доступным в сети. Хорошей характеристикой службы роли File Server является то, что она автоматически добавляется при открытии общего доступа к какой-либо папке. Эта служба роли использует новый протокол SMB 3.0, который более подробно обсуждается ближе к концу главы.
- **Distributed File System (Распределенная файловая система).** Служба роли Distributed File System (DFS) включает роли DFS Replication (Репликация DFS) и DFS Namespaces (Пространства имен DFS) и более подробно раскрывается в главе 14.
- **Data Deduplication (Дедупликация данных).** Служба роли Data Deduplication (Dedup) позволяет сохранять больше дискового пространства за счет обнаружения и устранения дублирования внутри файлов данных. Вместо хранения множества копий идентичных файлов место занимает только одна копия, а все дубликаты ссылаются на нее. Основная идея Data Deduplication — сохранить больше данных внутри меньшего пространства, разделяя файлы на небольшие блоки, идентифицируя дубликаты и затем поддерживая единственную копию этих дубликатов. Дедупликация в Windows Server 2012 R2 теперь является основанной на блоках на уровне самой операционной системы; во многих решениях от поставщиков хранилищ применяется дедупликация, основанная на файлах, на уровне хранилища. Многие люди задаются вопросом, какую экономию дискового пространства они могут ожидать для разных типов файлов. В табл. 13.1 приведены некоторые впечатляющие показатели, полученные в результате тестирования в испытательной среде. Эти тесты могут быть до некоторой степени оптимизированы для достижения лучшей производительности.
- **File Server Resource Manager (Диспетчер ресурсов файлового сервера).** Служба роли File Server Resource Manager (FSRM) предоставляет развитый набор дополнительных инструментов, которые можно использовать для управления хранилищем данных на сервере, включая конфигурирование квот, определение политик блокировки файлов и генерация отчетов по хранилищу.

Таблица 13.1. Экономия хранилища, обеспечиваемая дедупликацией в испытательной среде

Тип файла	Экономия
Общие файлы	Экономия 50–60% пространства при включенной дедупликации
Документы	Экономия 30–50% пространства при включенной дедупликации
Библиотека приложения	Экономия 70–80% пространства при включенной дедупликации
Библиотека VHD	Экономия 80–95% пространства при включенной дедупликации

В разделе "Диспетчер ресурсов файлового сервера" далее в главе рассматриваются нововведения, привнесенные в FSRM версией Windows Server 2012 R2.

- **Network File System (Сетевая файловая система).** Эта служба позволяет предоставлять доступ к файлам из клиентских компьютеров Unix и других машин, которые могут взаимодействовать с применением Network File System (NFS). Операционная система Windows Server 2012 R2 проделала действительно долгий путь со времен Windows Server 2008, предложив в этой серверной редакции впечатляющее решение с кластеризированной реализацией. В Windows Server 2012 обеспечивается гладкий обход отказа для клиентов смешанного режима в кластеризированной среде. Признавая потребность в росте виртуализированного мира, в Microsoft спроектировали службу NFS специально для кластеризированных виртуальных сред, где непрерывность ввода-вывода поддерживается независимо от операции, выполняемой во время отказа. Теперь используется NFS версии 4.1, делая реализацию NFS самой надежной и простой для развертывания в рамках семейства Windows Server.

  В Windows Server 2012 R2 также появилось несколько новых командлетов PowerShell, предназначенных для NFS. Чтобы получить полный их список, запустите командлет `Get-Command -Module NFS`. Как вы увидите, доступны командлеты практически для любого действия, которое нужно выполнять с NFS. Для получения информации о синтаксисе или об отдельной команде применяйте любой из следующих командлетов:
  - `Get-Help <имя командлета> -Detailed`
  - `Get-Help <имя командлета> -Examples`
  - `Get-Help <имя командлета> -Full`
- **Storage Services (Службы хранилища).** В Windows Server 2012 R2 добавлены замечательные компоненты, входящие в состав Storage Services. Они теперь включают пространства хранения и пулы хранения. За счет объединения Storage Services с Data Deduplication в Windows Server 2012 R2 теперь можно не только предоставлять, но также и составлять конкуренцию службам, которые обычно требуют отдельной сети хранения данных.
- **File Server VSS Agent Service (Служба агента VSS файлового сервера).** Когда включена, эта служба роли позволяет выполнять теневое копирование приложений, которые хранят данные на вашем файловом сервере. Новый в Windows Server 2012 компонент VSS for SMB File Shares (VSS для файловых общих ресурсов SMB) позволяет строить резервные копии во время записи актуальных данных на общие ресурсы SMB. Предшествующие версии VSS разрешали работу теневого копирования только на локальных томах.

- **iSCSI Target Server (Целевой сервер iSCSI).** Эта служба роли представляет собой серверный компонент, который предлагает блочное хранилище другим серверам и приложениям в сети. Она содержит все инструменты управления, необходимые для целей iSCSI. Целевой сервер запускает цель iSCSI через сеть Ethernet без необходимости в развертывании какого-то дополнительного оборудования. Эта служба роли поддерживает неоднородное хранилище, что позволяет Windows Server совместно использовать его в смешанной программной среде, утилизируя разнообразные типы инициаторов iSCSI. Данной службой роли можно управлять с применением нового графического пользовательского интерфейса, интегрированного в диспетчер серверов, или новых командлетов Windows PowerShell, включенных в Windows Server 2012 R2.
- **BranchCache for Network Files (BranchCache для сетевых файлов).** Средство BranchCache может использоваться в среде с несколькими сайтами, чтобы позволить компьютерам в офисах филиалов кешировать общие загружаемые файлы. Компонент BranchCache должен быть включен на общей папке. Вы увидите, как это делается, в разделе "Использование автономных файлов / кеширования на стороне клиента" далее в главе.

> **Добавление роли File Server при открытии общего доступа к папке**
>
> Если вы просто применяете проводник Windows для открытия общего доступа к папке, то роль File Server добавляется автоматически. Вы не обязаны добавлять эту роль с использованием диспетчера серверов. Тем не менее, когда вы планируете задействовать любые дополнительные роли, то должны добавлять их с помощью мастера добавления ролей и компонентов (Add Roles and Features Wizard), доступного в диспетчере серверов.

Добавление ролей к роли File and Storage Services

Для добавления ролей к роли File and Storage Services выполните следующие шаги.

1. Запустите диспетчер серверов, щелкнув на значке Server Manager (Диспетчер серверов) в панели задач или на плитке Server Manager на экране Start (Пуск), как показано на рис. 13.3.
2. На вкладке Dashboard (Управляющая панель) щелкните на ссылке Add Roles and Features (Добавить роли и компоненты), как показано на рис. 13.4.
3. Мастер добавления ролей и компонентов (Add Roles and Features Wizard) проведет вас по остальным действиям процесса. Просмотрите информацию на экране Before you begin (Прежде чем начать) и щелкните на кнопке Next (Далее).
4. На экране Installation Type (Тип установки) по умолчанию выбран переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов). Второй переключатель, Remote Desktop Services installation (Установка служб удаленного стола), касается служб роли для развертывания VDI (Virtual Desktop Infrastructure — инфраструктура виртуальных рабочих столов). Оставьте выбор по умолчанию и щелкните на кнопке Next.

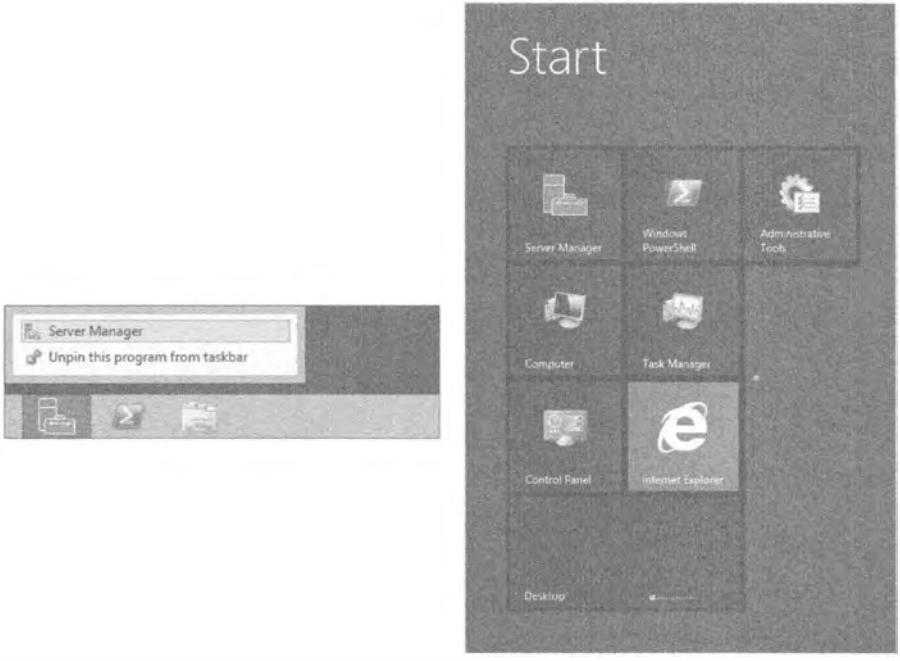


Рис. 13.3. Запуск диспетчера серверов из панели задач или экрана Start

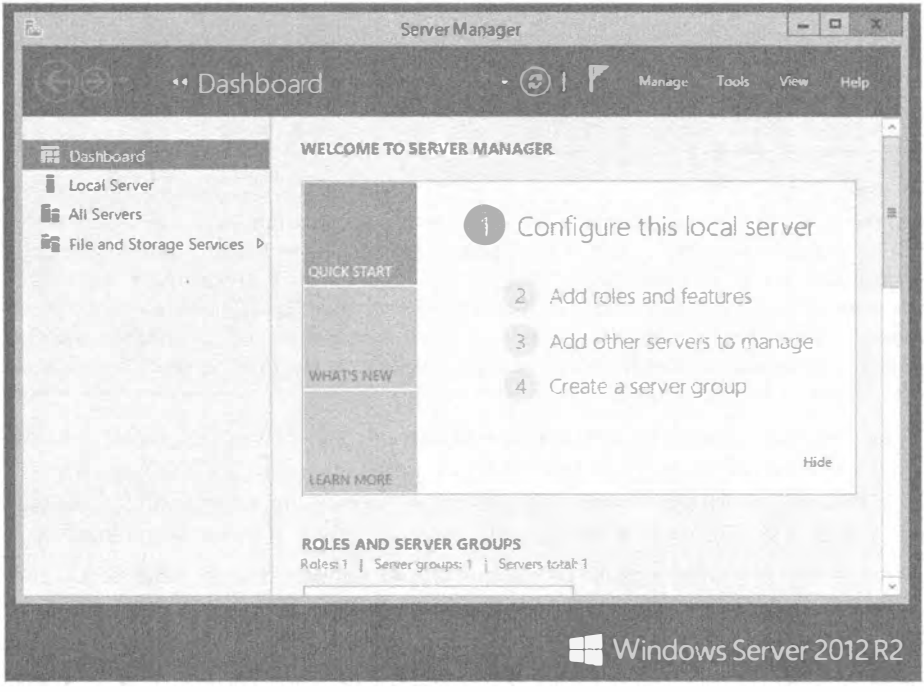


Рис. 13.4. Запуск мастера Add Roles and Features Wizard

5. На экране Server Selection (Выбор сервера) выберите сервер, к которому необходимо добавить службы роли, и щелкните на кнопке Next.
6. На экране Server Roles (Серверные роли) выберите следующие службы роли (рис. 13.5): File Server, File Server Resource Manager и BranchCache for Network Files. Щелкните на кнопке Next.

   Теперь, когда службы роли выбраны, наступило время установить любые дополнительные компоненты, которые помогают в поддержке этих служб ролей. На выбор доступны многие полезные компоненты.

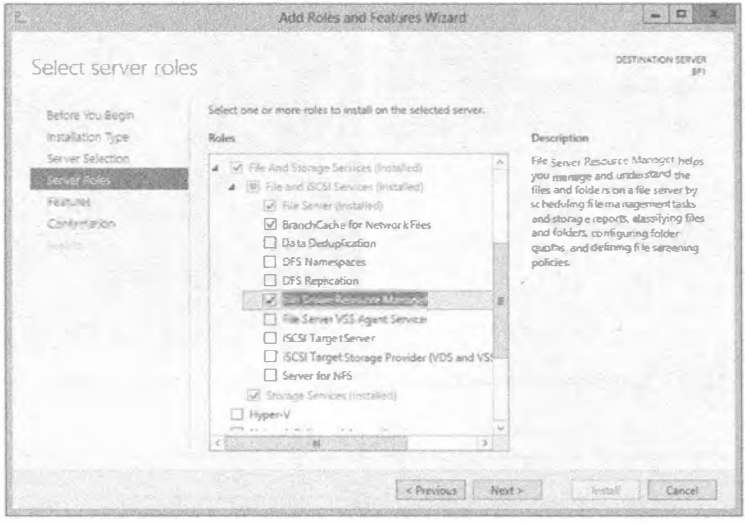


Рис. 13.5. Выбор служб ролей File and Storage Services

Роли или компоненты

Ролью считается крупная функция сервера, тогда как компонент — это пакет дополнения меньшего размера, который обычно предоставляет добавочную поддержку для основной роли. Основные роли могут включать Active Directory, DNS и DHCP. Компоненты, подобные PowerShell, Windows Server Backup (Резервное копирование Windows Server) и Remote Assistance (Дистанционный помощник), обеспечивают дополнительную функциональность, помогая эффективнее управлять серверными ролями.

7. Для примера давайте установим компоненты BitLocker Drive Encryption, BranchCache и Enhanced Storage (Расширенное хранилище). Вы заметите, что выбор BitLocker Drive Encryption приводит к автоматическому выбору для установки также и компонента Enhanced Storage (рис. 13.6). Щелкните на кнопке Next.
8. Просмотрите информацию на экране Confirmation (Подтверждение), удостоверившись в том, что ничего не упустили из виду.

   Мастер аккуратно отображает все выбранные роли, компоненты и поддерживающие их инструменты. На этом экране присутствует несколько дополнительных опций, которые вы можете счесть полезными: Restart the destination server automatically if required (При необходимости автоматически перезапускать целе-

вой сервер), Export configuration settings (Экспортировать настройки конфигурации) и Specify an alternate source path (Указать альтернативный исходный путь).

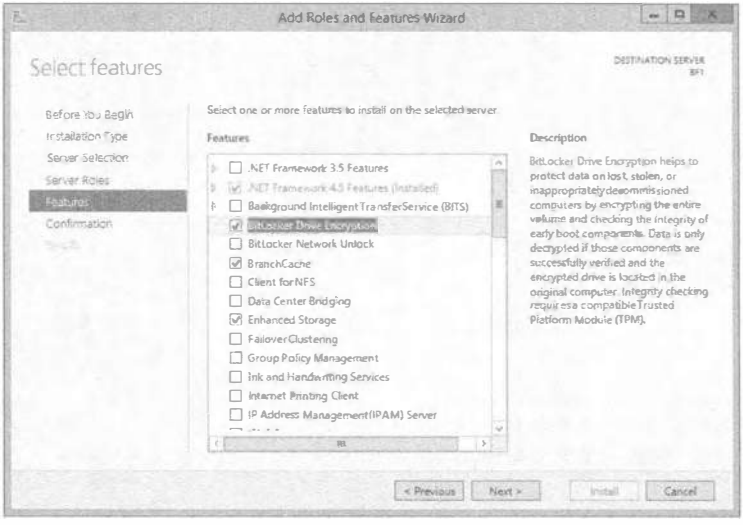


Рис. 13.6. Выбор дополнительных компонентов для служб роли

9. Щелкните на кнопке Install (Установить).

   Финальным экраном мастера является Results (Результаты). Здесь отобразится индикатор хода работ по установке. Если вы хотите закрыть этот экран и выйти, задача будет выполняться в фоновом режиме. Вы всегда можете просмотреть детальные сведения о задаче в панели задач, щелкнув на значке Notifications (Уведомления).

10. После успешной установки перезагрузите сервер вручную, или если вы отметили флажок Restart the destination server automatically if required на экране Confirmation, то сервер перезагрузится по завершении процесса установки.

Теперь диспетчер серверов включает все роли и компоненты, которые были установлены во время выполнения упражнения. Открыв диспетчер серверов и перейдя на вкладку Dashboard, вы можете просмотреть и воспользоваться установленными ролями и компонентами, щелкая на инструментах и выбирая желаемые ресурсы. Компоненты File Server Resource Manager показаны на рис. 13.7.

Создание общих ресурсов

Процесс создания общих ресурсов в этой редакции сервера претерпел ряд интересных изменений. Похоже, что практически все имеет мастер, проводящий нас по задачам и действиям. Существует множество разных способов создания общих ресурсов, которые обсуждаются в данной книге повсеместно. В этом разделе мы сосредоточим внимание на создании общих ресурсов с помощью диспетчера серверов. Независимо от применяемого метода, на компьютере, где создаются общие ресурсы, вы должны иметь права пользователя `Administrator` (Администратор) или `Power User` (Опытный пользователь).

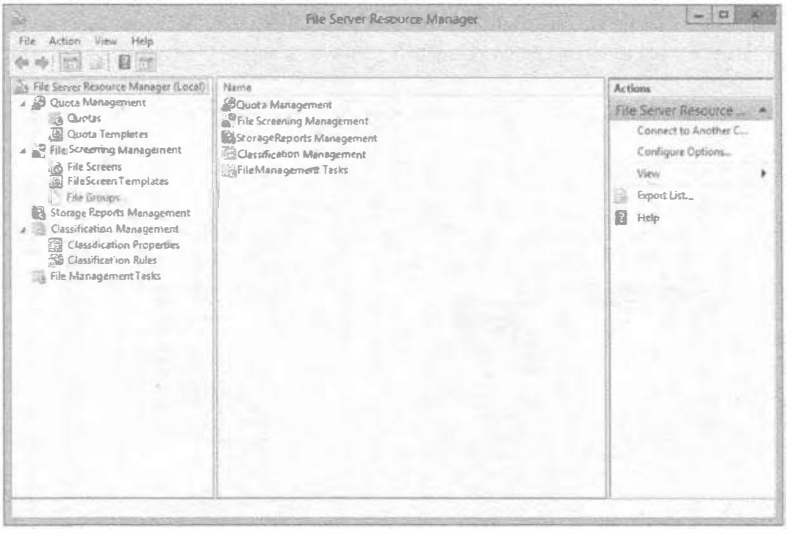


Рис. 13.7. Инструменты File Server Resource Manager

После создания общий ресурс можно опубликовать в Active Directory, чтобы упростить пользователям его нахождение. В этом разделе вы научитесь создавать общие ресурсы с использованием диспетчера серверов и публиковать их в Active Directory.

Создание общих ресурсов с помощью диспетчера серверов

Добавлять общие ресурсы в диспетчере серверов относительно просто. На вкладке Shares (Общие ресурсы) для роли File and Storage Services доступен мастер создания общего ресурса (New Share Wizard), который помогает выполнить эту задачу.

1. Запустите диспетчер серверов, если это еще не сделано, щелкнув на значке Server Manager (Диспетчер серверов) в панели задач или на плитке Server Manager на экране Start (Пуск).
2. Выберите роль File and Storage Services и затем вкладку Shares (Общие ресурсы).
3. Щелкните правой кнопкой мыши на области местоположения общей папки и выберите в контекстном меню пункт New Share (Создать общий ресурс). Можно также выбрать пункт New Share в раскрывающемся меню Tasks (Задачи). В любом случае запустится мастер создания общего ресурса, как показано на рис. 13.8.

   На первом экране мастера, Select Profile (Выбор профиля), предоставляется возможность выбрать профиль протокола для применения при создании общего ресурса. Доступны два крупных варианта и несколько подвариантов. Вы можете создать либо общий ресурс SMB, либо общий ресурс NFS. В целом можно отметить следующее:

   - общие ресурсы SMB используются для операционных систем Windows;
   - общие ресурсы NFS применяются для взаимодействия с машинами на основе Unix.

Протоколы SMB и NFS имеют варианты профиля общего ресурса Quick (Быстрый) и Advanced (Расширенный). Профиль Advanced имеет несколько дополнительных опций конфигурации, среди которых включение квот. Позже всегда можно добавить дополнительные компоненты, используя диспетчер серверов. Если вы решите включить квоты, то вам сначала потребуется построить новый шаблон квот или отредактировать существующий такой шаблон. Для SMB предусмотрен еще один шаблон профиля под названием SMB Share — Applications (Общий ресурс SMB — Приложения). Этот профиль создает общий файловый ресурс SMB с дополнительными настройками, применяемыми в виртуальной среде.

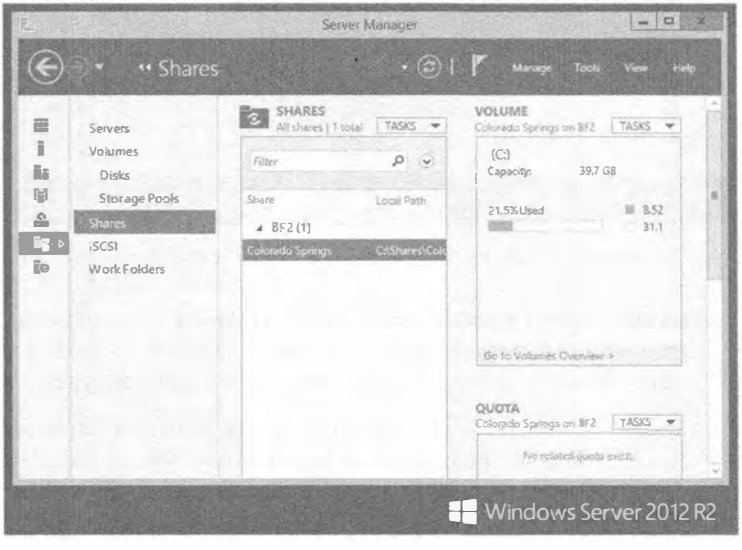


Рис. 13.8. Создание общего ресурса с использованием диспетчера серверов

4. Для целей этого упражнения выберите профиль SMB Share — Quick (Общий ресурс SMB — Быстрый), как показано на рис. 13.9, и щелкните на кнопке Next (Далее).

NFS для клиентов Unix

Вариант NFS не пригоден к употреблению, если на сервер не была добавлена роль Services for Network File System (Службы для сетевой файловой системы). Если позже вы решите добавить поддержку для клиентов Unix, то всегда сможете добавить упомянутую службу. После этого варианты NFS станут доступными в мастере New Share Wizard.

5. На экране Share Location (Местоположение общего ресурса) выберите сервер, на котором будет размещен общий ресурс, и укажите том на сервере, который будет служить местоположением общего ресурса.

   Обратите внимание, что общий ресурс можно создавать только на сервере с установленной ролью File Services Resource Manager.

6. Щелкните на кнопке Next.

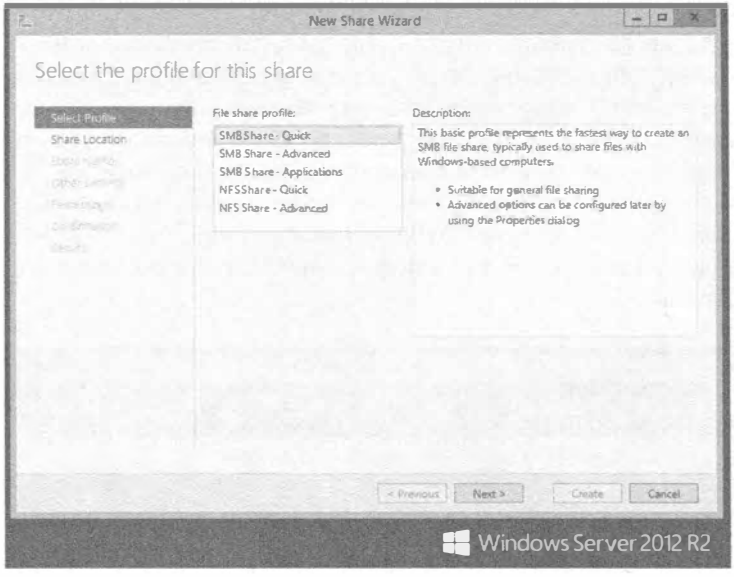


Рис. 13.9. Выбор профиля общего ресурса

На экране Share Name (Имя общего ресурса) можно определить имя общего ресурса и предоставить его описание. При этом отображаются локальный и удаленный сетевые пути, необходимые для достижения ресурса.

7. Примите эту информацию к сведению, т.к. вам понадобится сообщить указанные сетевые пути своим пользователям для доступа к общему ресурсу. На рис. 13.10 приведен пример именования общего ресурса. Щелкните на кнопке Next. На экране Other Settings (Другие настройки) предлагаются четыре дополнительных настройки, помогающие сделать общий ресурс более надежным.
   - Опция Enable access-based enumeration (Включить перечисление на основе доступа) будет автоматически скрывать папку от пользователя, который не имеет разрешения читать папку.
   - Опция Allow caching (Разрешить кеширование) предоставляет автономным пользователям доступ к общим данным, когда они работают в автономном режиме.
   - Поскольку вы установили компонент BranchCache в предыдущем упражнении, то теперь можете выбрать опцию Enable BranchCache on the file share (Включить BranchCache на этом общем ресурсе).
   - Последняя опция на этом экране, Encrypt data access (Шифровать доступ к данным), защищает удаленный доступ к файлам из общего ресурса.

   Если вы еще не включили шифрование на сервере, сделайте это прямо сейчас, отметив этот флажок. В случае если он недоступен или уже отмечен, значит, на данном сервере шифрование включено.
8. Сделайте нужный выбор и щелкните на кнопке Next.

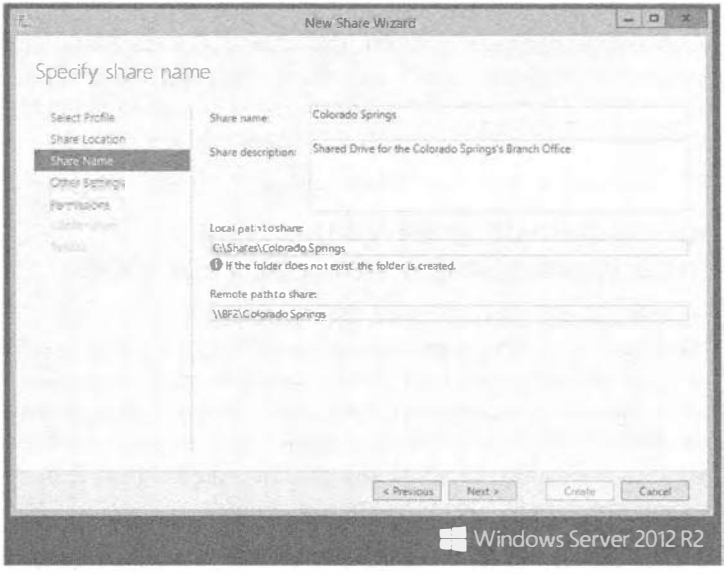


Рис. 13.10. Именование общего ресурса

9. Экран Permissions (Разрешения) предоставляет возможность при желании изменить разрешения NTFS. Разрешения NTFS будут раскрыты позже в этой главе, а пока щелкните на кнопке Next, чтобы принять стандартные разрешения NTFS.
10. На экране Confirmation (Подтверждение) представлена сводка по всем выбранным настройкам для создания нового общего ресурса. Внимательно просмотрите их, внесите любые необходимые изменения и щелкните на кнопке Create (Создать). Экран Confirmation показан на рис. 13.11.

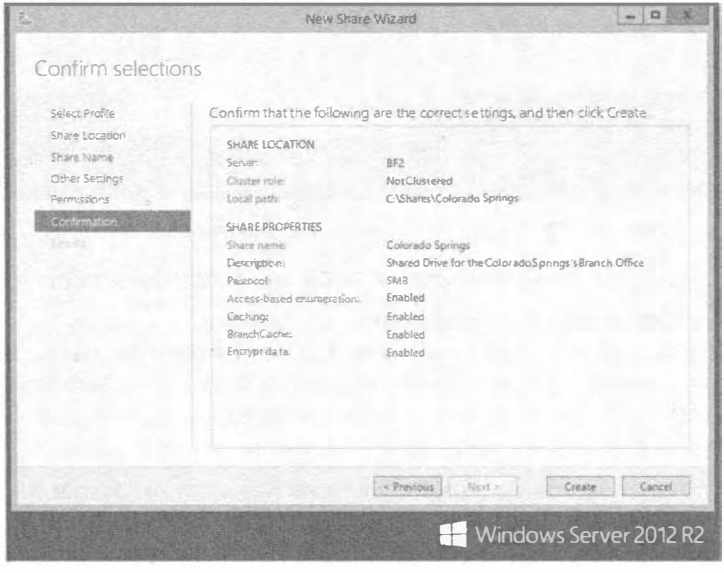


Рис. 13.11. Экран Confirmation

Последним экраном этого мастера является Results (Результаты). Отобразятся два индикатора хода работ: один для задачи Create SMB Share (Создание общего ресурса SMB) и еще один для задачи Set SMB Permissions (Установка разрешений SMB). После того как состоянием обеих задач станет Completed (Завершена), общий ресурс построен и готов к использованию.

11. Щелкните на кнопке Close (Закрыть), чтобы завершить работу мастера.

Создание общих ресурсов на удаленных компьютерах с помощью диспетчера серверов

Предыдущую процедуру можно также выполнить для создания общих ресурсов на удаленных компьютерах с применением диспетчера серверов. Подобно предшествующим редакциям сервера, диспетчер серверов способен выполнять задачи управления на удаленных компьютерах. На компьютерах, функционирующих под управлением Windows Server 2012, компонент Remote Management по умолчанию установлен и включен. На рис. 13.12 видны различные опции, которые диспетчер серверов предлагает, когда был добавлен другой сервер.

Рис. 13.12. Задачи управления на удаленном сервере

Управление сервером Windows Server 2008 из Windows Server 2012 R2

Для того чтобы полностью управлять серверами, на которых выполняется Windows Server 2008 или Windows Server 2008 R2, потребуется провести несколько обновлений. Для начала установите .NET Framework 4.0 и затем Windows Management Framework 3.0. После этого необходимо удостовериться в корректной конфигурации удаленного компьютера, что можно сделать путем ввода трех команд.

1. Введите показанную ниже команду в окне командной строки на компьютере, который вы желаете администрировать дистанционным образом. Эта команда включит прослушиватель WinRM:

```
winrm qc
```

2. После выдачи запроса введите **Y** и нажмите <Enter>.
3. Удостоверьтесь, что на удаленном компьютере функционирует служба виртуальных дисков (Virtual Disk Service). Это можно сделать с помощью следующих команд:

```
sc config vds start= auto
net start vds
```

Пример из практики

Установка лимита пользователей

Вы можете сконфигурировать количество пользователей, которые могут одновременно подключаться к общему ресурсу, путем настройки опции User limit (Лимит пользователей) в диалоговом окне свойств общего ресурса. Чтобы установить лимит пользователей, откройте папку Administrative Tools (Администрирование), дважды щелкните на значке Computer Management (Управление компьютером), разверните узел Shared Folders (Общие папки), выберите папку Shares (Общие ресурсы), щелкните правой кнопкой мыши на общем ресурсе, для которого хотите установить лимит пользователей, и выберите в контекстном меню пункт Properties (Свойства). Ниже показан экранный снимок с настройкой лимита пользователей для общего ресурса.

В качестве примера, если приложение лицензировано для 100 параллельных пользователей, вы можете сконфигурировать общий ресурс на сервере для поддержки этого лимита, несмотря на то, что в сети может быть 200 пользователей. Просто выберите переключатель Allow this number of users (Разрешить это количество пользователей) и укажите в поле рядом соответствующее число (по умолчанию оно равно 1). По мере того, как пользователи подключаются к общему ресурсу, их число приближается к лимиту пользователей. При отключении от общего ресурса их количество уменьшается. Такой тип принудительного применения лицензий может быть удобен для снижения затрат на лицензирование.

Однако будьте осторожны в отношении лицензирования. Не у всех приложений имеется режим параллельных лицензий, хотя может существовать режим клиентских лицензий. В режиме клиентских лицензий производитель не заботится о том, сколько пользователей получают доступ к приложению в любой момент времени; играет роль только количество людей, в целом установивших приложение. В таких случаях лимит пользователей никак вас не защитит.

Необходимо также помнить о том, что этот лимит параллельно подключаемых пользователей основан на целом общем ресурсе. Он не может быть определен для каждой папки внутри общего ресурса. Например, у вас может быть два приложения на одном общем ресурсе. Приложение 1 имеет лимит в 100 пользователей, а для приложения 2 лимит не предусмотрен. По невнимательности вы можете ограничить доступ к приложению 2, когда для общего ресурса устанавливается лимит подключений в 100 пользователей. Простое решение заключается в использовании разных общих ресурсов в случае, когда требуются разные лимиты.

Наконец, вы должны принять во внимание, каким образом пользователи подключаются к общему ресурсу для взаимодействия с приложениями, прежде чем ограничивать их на базе параллелизма. Если все пользователи подключаются к общему ресурсу при входе в систему (как с отображенным диском), и не отключаются вплоть до выхода из системы, то лимит параллелизма может в первую очередь расходоваться на вошедших в систему пользователей, достигая в итоге предела в 100 человек, хотя в действительности работать с приложением могла только небольшая группа пользователей. Если подключения осуществляются только при использовании приложения, то лимит пользователей будет работать довольно хорошо.

Следите за пробелами в команде sc

Команда `sc config` применяется для изменения конфигурации службы. По умолчанию служба виртуальных дисков (Virtual Disk Service — VDS) не запускается, поэтому вы будете использовать эту команду для автоматического запуска VDS на сервере. Служба VDS необходима для получения доступа к возможностям дистанционного управления. Чтобы получить дополнительные сведения об опциях и функциях команды `sc`, откройте окно командной строки и введите `sc config?`. Команда конфигурирования сервера (server config — `sc`) очень привередлива в отношении пробелов. Показанная ниже команда содержит пробел после символа =, и она будет работать:

```
sc config vds start= auto
```

С другой стороны, следующая команда работать откажется из-за пропущенного пробела:

```
sc config vds start=auto
```

4. **Создайте исключение брандмауэра для группы `Remote Volume Management` (Управление удаленными томами) с помощью приведенной далее команды. В книге команда разнесена на две строки, но на самом деле она должна вводиться в одной строке.**

```
netsh advfirewall firewall set rule~CA
group="Remote Volume Management" new enable=yes
```

Если команда была введена корректно, в выводе отобразится строка `Updated 3 rules` (Обновлены 3 правила).

После того как удаленный компьютер сконфигурирован, вы можете открыть диспетчер серверов на своем локальном компьютере и выбрать в меню Manage

(Управление) пункт Add Servers (Добавить серверы). Существуют три способа нахождения и добавления новых машин в локальном диспетчере серверов. Сервер можно добавить методом поиска в Active Directory и выбора компьютера, присоединенного к домену. Кроме того, сервер можно добавить, введя на вкладке DNS имя компьютера или его IP-адрес. И, наконец, вкладка Import (Импорт) позволяет напрямую запросить сетевой путь к желаемой машине или просмотреть местоположения в сети для обнаружения нужного ресурса. Воспользовавшись одним из перечисленных методов, найдите машину для управления и щелкните на кнопке OK. Через короткое время диспетчер серверов подключится к удаленному компьютеру. После этого вы сможете просматривать и управлять удаленным компьютером на вкладке All Servers (Все серверы) в диспетчере серверов. Просто щелкните правой кнопкой мыши на подключенном удаленном компьютере, и в контекстном меню отобразится список функций управления (рис. 13.13).

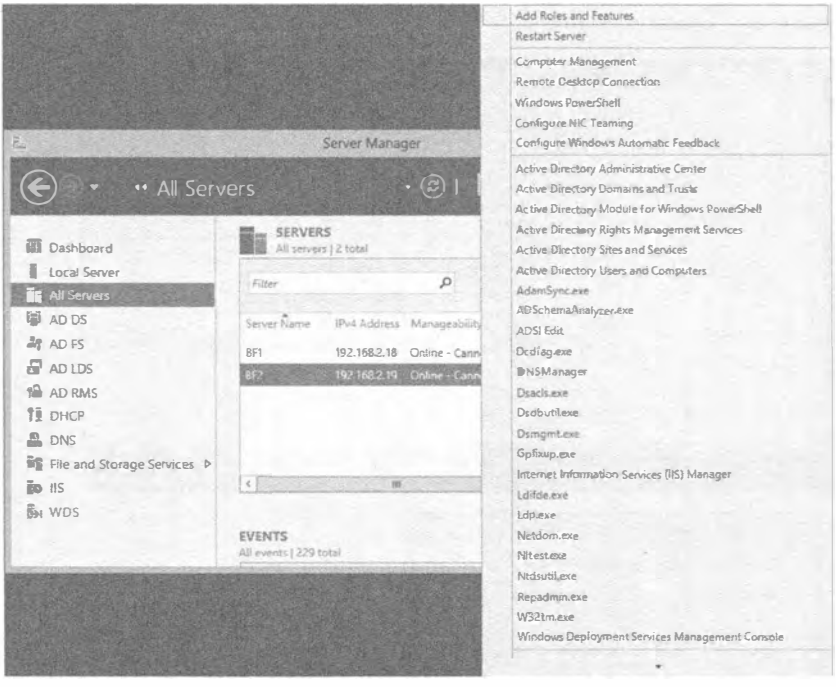


Рис. 13.13. Управление удаленным компьютером

Публикация общих ресурсов в Active Directory

Одной из великолепных особенностей среды Active Directory является возможность объединения всех ресурсов предприятия в единый каталог, будь то принтеры, группы, пользователи, организационные единицы или что угодно из области ваших фантазий — точнее, возможность их обслуживания. Это касается и общих ресурсов. Главная причина публикации общего ресурса в Active Directory связана с тем, чтобы упростить пользователям его нахождение.

Публикация общего ресурса осуществляется в консоли управления Active Directory Users and Computers (Пользователи и компьютеры Active Directory).

Щелкните правой кнопкой мыши на необходимой организационной единице и выберите в контекстном меню пункт New⇨Shared Folder (Создать⇨Общая папка). Вам будет предложено указать имя для этой публикации общего ресурса и, конечно же, имя самого общего ресурса. Это все, что нужно было сделать — общий ресурс теперь опубликован в Active Directory. После публикации общего ресурса можете также добавить ключевые слова, чтобы упростить пользователям его нахождение.

1. Щелкните правой кнопкой мыши на объекте общей папки в консоли Active Directory Users and Computers.
2. Выберите в контекстном меню пункт Properties (Свойства) и открывшемся диалоговом окне щелкните на кнопке Keywords (Ключевые слова).
3. Добавьте любые желаемые ключевые слова, которые пользователи могут применять при поиске этого общего ресурса.

На рис. 13.14 демонстрируется добавление ключевых слов к опубликованному общему ресурсу Colorado Springs.

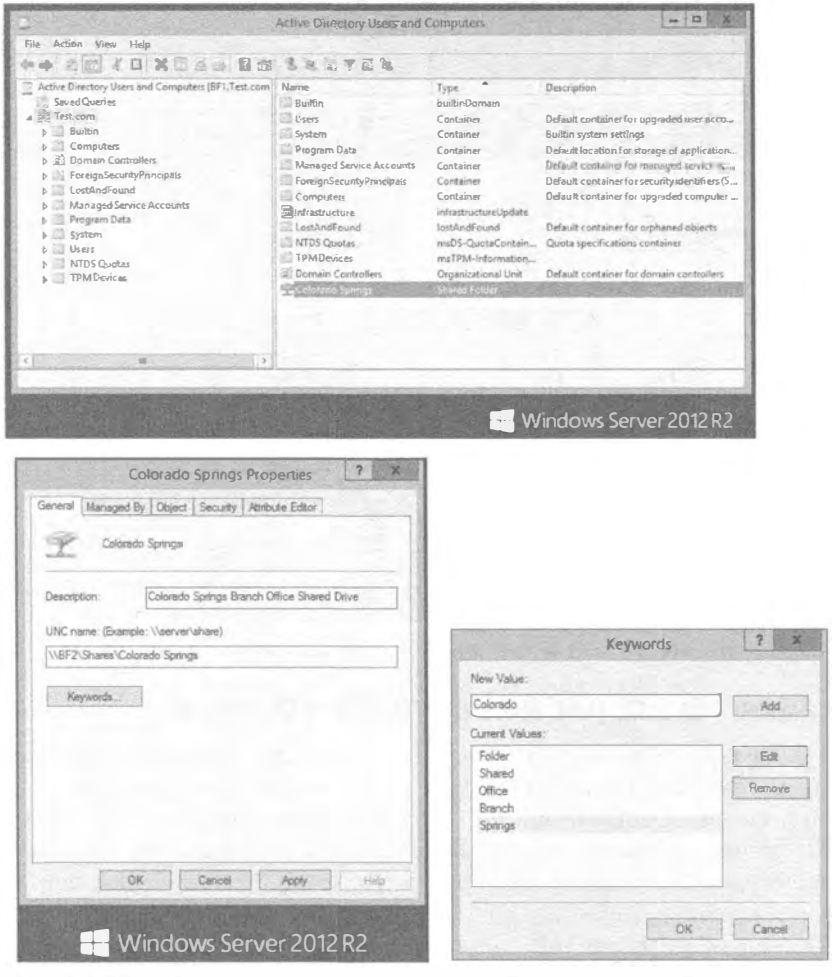


Рис. 13.14. Добавление ключевых слов к опубликованному общему ресурсу

После этого пользователи могут с помощью инструмента поиска в Active Directory искать по ключевым словам. На рис. 13.15 показан инструмент поиска в Active Directory с выбранным элементом Shared Folders (Общие папки) в раскрывающемся списке Find (Искать). Мы добавили ключевое слово `Colorado` и щелкнули на кнопке Find Now (Найти сейчас), что привело к нахождению нужного общего ресурса. Для доступа к общему ресурсу достаточно просто дважды щелкнуть на нем.

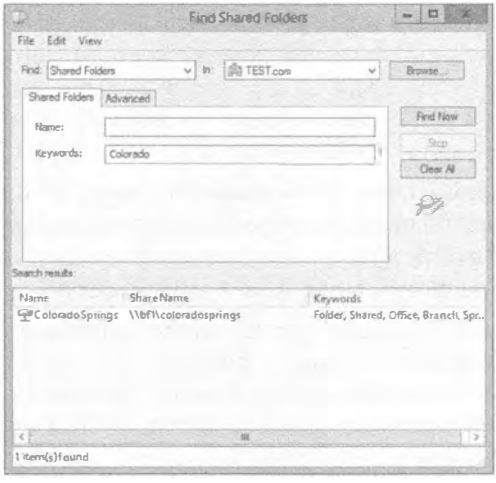


Рис. 13.15. Применение инструмента поиска в Active Directory для нахождения опубликованного общего ресурса

Управление разрешениями

Одним из крупных достоинств дисков, сформатированных с файловой системой NTFS, и общих ресурсов является возможность назначения разрешений и управления тем, кто может иметь доступ к различным файлам и папкам. В то время как в главе 14 будет подробно раскрыта внутренняя работа этих разрешений, в настоящей главе мы дадим базовое введение в разрешения NTFS и общего доступа. Вы заметите, что в этой редакции сервера в отношении разрешений изменилось не очень многое. По большей части просто появился новый способ для навигации и работы с теми же самыми функциями и инструментами, которые вы хорошо знаете по версии Windows Server 2008 R2.

Между разрешениями NTFS и разрешениями обшего доступа есть много сходства, о чем пойдет речь в этом разделе. Сходство включает то, как каждому разрешению может быть назначено действие Allow (Разрешить) или Deny (Запретить), каким образом разрешения накапливаются, как Deny получает приоритет и каким образом используется принцип неявного запрета.

Когда пользователь обращается к общему ресурсу, к которому применены разрешения NTFS и общего доступа, результирующее разрешение в общем случае называется *наименее ограничивающим разрешением*. Поскольку вас могут попросить решить проблему с невозможностью доступа к какому-то файлу или папке, вы должны знать, как вычислить результирующее разрешение, чему и посвящен материал данного раздела.

Разрешения NTFS

Разрешения NTFS применяются к любому файлу или папке на диске, который был сформатирован с файловой системой NTFS.

- **Read (Чтение).** Когда пользователю назначено разрешение Read, ему позволено просматривать содержимое, разрешения и атрибуты, ассоциированные с файлом или папкой.
- **Read & Execute (Чтение и выполнение).** Разрешение Read & Execute используется для предоставления пользователю возможности запуска файлов. Любые исполняемые файлы (такие как `.exe`, `.bat` и `.com`) — это файлы, которые можно запускать. Если пользователь имеет только разрешение Read, но не Read & Execute, файлы не могут быть запущены.
- **List Folder Contents (Список содержимого папки).** Разрешение List Folder Contents позволяет пользователю просматривать содержимое папки. Оно дает пользователю возможность увидеть, какие файлы существуют внутри папки, но без применения разрешений Read к этим файлам.
- **Write (Запись).** Если пользователю назначено разрешение Write для файла или папки, он может модифицировать содержимое этого файла или папки. Под этим понимается добавление в папку новых файлов или папок либо внесение изменений в существующие файлы или папки. Тем не менее, удалять файлы из папки не допускается.
- **Modify (Изменение).** Разрешение Modify включает все разрешения Read, Read & Execute и Change, а также возможность удаления файлов и папок.
- **Full Control (Полный доступ).** Разрешение Full Control представляет собой объединение всех доступных разрешений с дополнительной возможностью изменения разрешений и смены владельца файлов или папок.

Разрешения общего доступа

Разрешения общего доступа применяются к общим ресурсам, только когда к ним производится доступ через сеть. Разрешений общего доступа всего лишь три.

- **Read (Чтение).** Пользователи, которым выдано разрешение Read, могут читать файлы и папки внутри общего ресурса.
- **Change (Изменение).** Пользователи, которым выдано разрешение Change, могут читать, запускать, модифицировать и удалять файлы и папки внутри общего ресурса.
- **Full Control (Полный доступ).** Пользователи, которым выдано разрешение Full Control, могут делать все то же самое, что и пользователи с разрешением Change, а также вдобавок изменять разрешения для общего ресурса.

Сходные черты разрешений общего доступа и разрешений NTFS

Теперь, когда вы имеете базовое понимание в целом разрешений NTFS и обшего доступа, легче выявить сходные черты между ними. Все они перечислены ниже.

- Обоим типам разрешений может быть назначено действие Allow (Разрешить) или Deny (Запретить).
- Оба типа разрешений являются накопительными.
- В обоих типах разрешений приоритет имеет действие Deny.
- Оба типа разрешений поддерживают принцип неявного запрета.

Назначение действия Allow или Deny

Приступив к работе с разрешениями, вы заметите, что для каждого из перечисленных разрешений предусмотрены флажки Allow (Разрешить) или Deny (Запретить). Ниже приведен обзор того, как они работают.

- Если для разрешения отмечен флажок Allow в отношении пользователя или группы, то этот пользователь или группа имеют данное разрешение.
- Если для разрешения отмечен флажок Deny в отношении пользователя или группы, то этот пользователь или группа не имеют данного разрешения.
- Разрешения являются накопительными. Если пользователю назначено несколько разрешений Allow (таких как Allow Read и Allow Change), пользователь получает объединение назначенных разрешений.
- Если пользователю назначены разрешения и Allow, и Deny, то разрешения Deny имеют преимущество.

Если пользователю вообще не назначены какие-либо разрешения, он не имеет доступа к объекту. Это называется *неявным запретом*. Разрешения общего доступа и разрешения NTFS используют модель избирательного управления доступом (discretionary access control — DAC). Каждый объект имеет список избирательного управления доступом (discretionary access control list — DACL), состоящий из записей управления доступом (access control entry — ACE).

Каждая запись ACE идентифицирует пользователя или группу с ассоциированным идентификатором защиты (security identifier — SID) и разрешением Allow или Deny. Любой объект может иметь несколько записей ACE в своем списке DACL; другими словами, любой объект может иметь множество назначенных ему разрешений.

Идентификаторы защиты

Каждый пользователь и каждая группа уникально идентифицируются с помощью SID. Когда пользователь входит в систему, создается маркер, включающий SID пользователя и идентификаторы SID всех групп, членами которых пользователь является. Этот маркер применяется операционной системой для определения, должен ли пользователь иметь доступ. Идентификаторы SID в маркере сравниваются с идентификаторами SID из записей управления доступом в списке DACL, чтобы выяснить, возможен ли доступ.

Когда пользователь обращается к файлу, папке или общему ресурсу, операционная система сравнивает список DACL с учетной записью пользователя и его членством в группах. Если обнаруживается соответствие, пользователю предоставляется соответствующее разрешение.

Накопленные разрешения

Объектам могут назначаться множество разрешений. В качестве примера предположим, что имеется общий ресурс по имени `ProjectData`. Группе `Administrators` может быть предоставлено разрешение Full Control, какой-то группе — разрешение Change, а еще какой-то группе — разрешение Read. При назначении нескольких разрешений они накапливаются. Другими словами, если к пользователю применяется множество разрешений, то пользователь получает объединение всех этих разрешений.

Представим, что Салли состоит в группах `G_Sales` и `G_SalesAdmins`, и этим группам выданы следующие разрешения для общего ресурса `Sales`:

`G_Sales`	Разрешение Allow Change
`G_SalesAdmins`	Разрешение Allow Full Control

Поскольку Салли является членом обеих групп, ей предоставляются разрешения Change и Full Control; говоря по-другому, она получает объединение разрешений Change и Full Control.

Действие Deny имеет приоритет

Если к любому разрешению, назначенному пользователю, применены действия Allow и Deny, то Deny получает приоритет. В качестве примера предположим, что группе `G_Sales` выдано разрешение Full Control для общего ресурса, который содержит патентованную информацию. По ряду причин пользователь `Billy Joe Bob` (являющийся членом группы `G_Sales`) впал в немилость в компании. Вас попросили оставить его в группе `G_Sales`, чтобы он имел доступ к другим обшим ресурсам, но запретить ему доступ к общему ресурсу с патентованной информацией.

Рис. 13.16. Выбор специальных разрешений общего доступа

На рис. 13.16 показано, как вы можете поступить. Для начала разрешения общего доступа выданы персоналу из группы `G_Sales`, имеющей разрешение Full Control для этого общего ресурса. Чтобы полностью запретить пользователю `Billy Joe Bob` доступ к данным, его учетная запись была добавлена и ей назначено разрешение Deny Full Control. Другими словами, его учетная запись была явно запрещена.

Обратите внимание на возникший конфликт. Пользователю предоставляется доступ как члену группы `G_Sales` и запрещается доступ для его учетной записи. Конфликт разрешается в пользу Deny. Если подумать, то это имеет смысл. Когда вы предпринимаете дополнительные действия, необходимые для запрещения доступа, то не хотите, чтобы что-то его переопределило. Действие Deny имеет приоритет.

Неявный запрет

Существует также характеристика, известная как *неявный запрет*. Если разрешение не выдано явно, оно неявно запрещается.

Предположим, что есть общий ресурс по имени `ProjectData`, доступ к которому разрешен только группе `G_Sales`. Мария состоит в группе `G_HR` и не является членом группы `G_Sales`, так что она не имеет доступа к этому общему ресурсу. Поскольку доступ Марии не был предоставлен явно, для нее неявно доступ запрещен.

Сравните это со своей квартирой. Если вы никому не давали ключи от нее, то никто не сможет в нее попасть. Конечно, вам по-прежнему придется беспокоиться о бандитах и взломщиках, но с основной точки зрения отсутствие факта предоставления разрешений означает отсутствие доступа.

Модификация разрешений общего доступа и NTFS

Разрешения общего доступа и NTFS можно модифицировать с использованием диспетчера серверов, значка Computer Management (Управление компьютером) или проводника Windows. Шаги для каждого метода немного отличаются, но, в конечном счете, мы получим те же самые вкладки разрешений. Мы ограничимся обсуждением процедуры, предусматривающей применение диспетчера серверов.

Предположим, что вы создали общий ресурс и выдали разрешение Read группе `Everyone` (Все). Однако теперь вы хотите изменить разрешения так, чтобы пользователи в группе `G_Sales` имели разрешение Change, и никто из пользователей кроме администраторов не мог просматривать или использовать этот набор папок и файлов. Чтобы внести такие изменения, выполните следующие шаги.

1. Запустите диспетчер серверов и откройте узел File and Storage Services⇨Shares (Службы файлов и хранилища⇨Общие ресурсы).
2. Щелкните правой кнопкой мыши на общем ресурсе `Apps` и выберите в контекстном меню пункт Properties (Свойства).
3. Щелкните на кнопке Permissions (Разрешения) и затем на кнопке Customize Permissions (Изменить разрешения). Окно должно выглядеть примерно так, как показано на рис. 13.17.

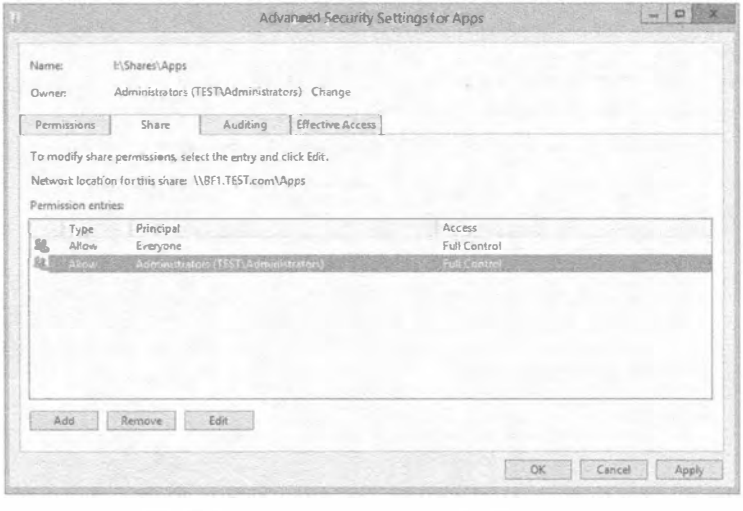


Рис. 13.17. Просмотр разрешений общего доступа

4. На вкладке Share (Общий доступ) щелкните на кнопке Add (Добавить). Затем выберите переключатель Select a principal (Выбрать участника) и введите имя группы, которой необходимо предоставить доступ к общему ресурсу (например, `G_Sales`), после чего щелкните на кнопке OK.
5. Поскольку вы не хотите, чтобы доступ получили абсолютно все, выберите группу `Everyone` и щелкните на кнопке Remove (Удалить). Щелкните на кнопке OK.
6. Щелкните на кнопке Apply (Применить) и перейдите с вкладки Share на вкладку Permissions (Разрешения).

   Обратите внимание, что на вкладке Permissions делегированы разрешения NTFS, а на вкладке Share делегированы разрешения Share. Смешивание этих разрешений будет рассматриваться в следующем разделе.
7. Находясь на вкладке Permissions, щелкните на кнопке Add и введите имя группы, которую нужно добавить (такое как `G_Sales`). Щелкните на кнопке OK, чтобы добавить группу.

   По умолчанию любому добавляемому пользователю или группе автоматически предоставляются разрешения Read, Read & Execute и List Folder Contents.
8. Выберите разрешение Allow Write для добавленной группы, удостоверьтесь, что также внесли изменения в файлы, и щелкните на кнопке OK.
9. Не забудьте также удалить группу `Everyone` из этого набора разрешений: выберите группу `Everyone` и щелкните на кнопке Remove.

   Разрешения общего доступа и разрешения NTFS управляются раздельно, но работают вместе для предоставления надлежащих разрешений. Окно будет выглядеть примерно так, как показано на рис. 13.18.
10. Щелкните на кнопках Apply и OK в диалоговом окне Advanced Security (Расширенная безопасность) для завершения установки разрешений.

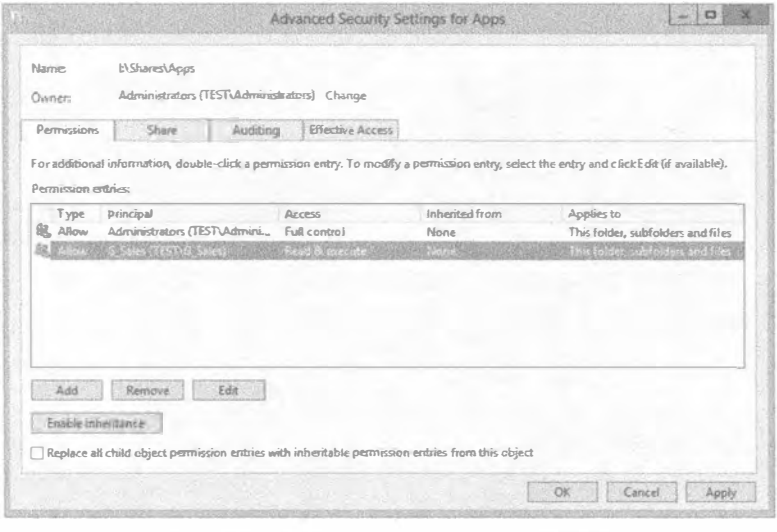


Рис. 13.18. Просмотр разрешений NTFS

11. Щелкните на кнопках Apply и OK на вкладке Permissions, чтобы завершить упражнение.

Объединение разрешений общего доступа и NTFS

Люди иногда находят сложным идентификацию разрешений, которые пользователь будет иметь, когда он обращается к файлу или папке через общий ресурс. Нам нравится сохранять процесс простым благодаря следующим трем шагам.

1. Определите накопленное разрешение NTFS.
2. Определите накопленное разрешение общего доступа.
3. Определите, какое из этих двух разрешений обеспечивает наименьший доступ (обычно оно называется наиболее ограничивающим разрешением).

Представим, что Салли состоит в группах `G_Sales` и `G_ITSalesAdmins`. Разрешения, назначенные для папки `SalesData` (совместно используемой как общий ресурс `SalesData`), описаны в табл. 13.2.

Таблица 13.2. Пример объединения разрешений общего доступа и NTFS

Группа	Разрешения NTFS	Разрешения общего доступа
`G_Sales`	Read, Read & Execute, List Folder Contents	Read
`G_ITSalesAdmins`	Full Control	Change

На шаге 1 вам необходимо определить накопленное разрешение NTFS. Салли имеет разрешения Read, Read & Execute и List Folder Contents как член группы `G_Sales`. Вдобавок она имеет разрешение Full Control, будучи членом группы `G_ITSalesAdmins`. Поскольку разрешение Full Control включает все другие разрешения, накопленным разрешением NTFS будет Full Control.

На шаге 2 вы должны определить накопленное разрешение общего доступа. Салли имеет разрешение Read как член группы `G_Sales`. Кроме того, у нее есть разрешение Change, поскольку она является членом группы `G_ITSalesAdmins`. Так как разрешение Change включает разрешения Read и Write, накопленным разрешением общего доступа оказывается Change.

Последний шаг предусматривает ответ на простой вопрос. Какое разрешение предоставляет наименьший доступ, т.е. является наиболее ограничивающим: Full Control или Change? Ответ — Change. Разрешение Change Салли и получит, когда обратится к общему ресурсу через сеть.

А как насчет сложного вопроса? Какое разрешение будет у Салли, когда она обратится к папке `SalesData` локально?

Ответ — Full Control. Вспомните, что разрешения общего доступа применяются только в случае, если пользователь обращается к общему ресурсу через сеть. При локальном доступе к папке применяются только разрешения NTFS.

Подключение к общим ресурсам

Теперь, когда у вас есть общие ресурсы, каким образом люди могут пользоваться ими? Предполагая наличие общего ресурса по имени `Apps` на сервере `BF1`, как кто-то, подключенный к сети, мог бы получить к нему доступ?

В основном вы подключаетесь к общему ресурсу, используя имя UNC (universal naming convention — универсальное соглашение по именованию) вида \\ИмяСервера\ИмяОбщегоРесурса. В качестве альтернативы можете нажать комбинацию клавиш <Windows+R> на рабочем столе, чтобы открыть диалоговое окно Run (Выполнить), и ввести в нем **\\ИмяСервера** (здесь указывается имя любого сервера, подключенного к сети) и следом обратную косую черту (рис. 13.19). Еще один способ открытия диалогового окна Run в Windows Server 2012 предусматривает переход на экран Start (Пуск), ввод **Run** и нажатие <Enter>. На рис. 13.19 мы применяем **\\BF2** для подключения к серверу по имени BF2.

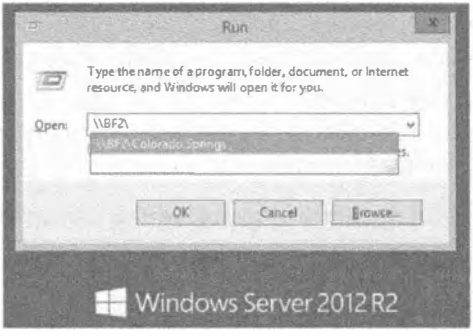


Рис. 13.19. Поиск общих ресурсов

После подключения операционная система извлекает список доступных общих ресурсов. На этом сервере в текущий момент существуют четыре общих ресурса, причем все они не являются скрытыми. В главе 14 будет показано, как сделать доступными дополнительные скрытые общие ресурсы. Вы могли бы ввести **Apps** в конце \\BF1\, получив запись вида **\\BF1\Apps**, или просто выбрать общий ресурс Apps в раскрывающемся списке на рис. 13.19 и щелкнуть на кнопке OK, чтобы подключиться к нему.

Помимо меню поиска, для подключения к общему ресурсу доступны и другие методы.

- **Отображение диска.** Вы можете отобразить букву диска на общий ресурс в сети. Например, пользователям может быть необходим доступ к общему ресурсу при каждой загрузке системы. Щелкните правой кнопкой мыши либо на узле Computer (Компьютер), либо на узле Network (Сеть) в проводнике Windows и выберите в контекстном меню пункт Map Network Drive (Подключить сетевой диск). Уделите время на то, чтобы оценить новый внешний вид пользовательского интерфейса Windows Server 2012 R2. При открытом окне проводника Windows выберите узел Computer и затем опцию Computer в верхней панели действий. Отобразится новая лента, похожая на те, которые вы знаете по программам вроде Microsoft Word. В этой ленте доступно много новых опций, в числе которых Map a Network Drive (Подключить сетевой диск). На рис. 13.20 показано диалоговое окно Map Network Drive (Подключение сетевого диска). При отмеченном флажке Reconnect at sign-in (Восстанавливать при входе в систему) пользователь всегда будет иметь диск Z, отображенный на общий ресурс, после загрузки системы.

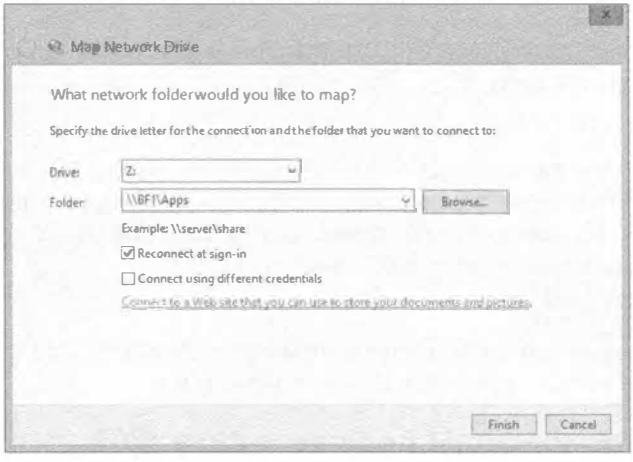


Рис. 13.20. Отображение общего ресурса на букву диска

- **Поиск в Active Directory.** Если клиент является членом домена, то в окне Network (Сеть) появится опция Search Active Directory (Поиск в Active Directory). Чтобы открыть окно Network в Windows Server 2012 R2, выберите на экране Start (Пуск) плитку Network (Сеть).
- **Использование `net use`.** Вы можете применять команду `net use` в командной строке. Базовый синтаксис выглядит следующим образом:

  ```
  net use буква_диска \\имя_сервера\имя_общего_ресурса
  ```

  Например, чтобы присоединить общий ресурс `Apps` на сервере `BF1` и затем иметь возможность ссылаться на этот общий ресурс как на диск `Z`, можно воспользоваться такой командой:

  ```
  net use Z: \\BF1\apps
  ```

  Если позже вы захотите удалить это отображение, понадобится ввести следующую команду:

  ```
  net use Z: /delete
  ```

Конфликт между наборами учетных данных

Иногда при попытке подключения к общему ресурсу возникает ошибка с сообщением следующего вида: "набор учетных данных конфликтует с существующим набором учетных данных для этого общего ресурса".

Вот что происходит. Вы уже пытались получить доступ к этому общему ресурсу и по какой-то причине потерпели неудачу — возможно, неправильно ввели пароль. Сервер, на котором находится общий ресурс, подготовил информацию о том, что вы — недобросовестный клиент, и он больше ничего не желает слышать о вас. Вам нужно заставить сервер забыть о вас, чтобы вы могли начать все сначала. Это делается с помощью опции `/d`.

Предположим, что вы уже пробовали обратиться к общему ресурсу `\\BF1\Apps`, и попытка завершилась неудачей. Может быть, вы *действительно* подключились к общему ресурсу, но без разрешений. (Мы знаем, что это не имеет смысла, но так случается.) Чтобы выяснить, к каким общим ресурсам вы подключены, необходи-

мо ввести просто **net use**. Скорее всего, вы увидите \\BF1\Apps в списке. Вы должны отключиться от сервера BF1, чтобы впоследствии начать заново. Для этого введите следующую команду:

```
net use \\BF1\apps /d
```

Затем введите еще раз команду net use, удостоверившись, что все эти подключения очищены; может оказаться, что у вас есть *множество* соединений с определенным сервером. В редких случаях требуется отключиться от *всех* общих файловых ресурсов, для чего используется такая команда:

```
net use * /d
```

После закрытия всех подключений попробуйте подключиться к общему ресурсу с помощью команды net use еще раз, и все заработает.

Использование команды net use в сети WAN

Мы подошли к одной из наиболее сложных областей сетевой работы: подключению к ресурсам через большие расстояния со многими неизвестными. Если вам приходилось когда-либо иметь дело с удаленными на большие расстояния вычислениями, то вы знаете, что полагаться на них нельзя. Однако в арсенале команды net use появился новый небольшой набор функций, который позволяет прояснить множество "неизвестных" в общей картине.

Вместо того чтобы рассчитывать на выяснение подходящего сервера распознавания имен, обращения к этому серверу и получения точного и надежного преобразования по неточному и ненадежному сетевому каналу, вы теперь можете отобразить нужный ресурс прямо на диск своего сервера через IP-адрес ресурса. Конечно, вы должны знать этот IP-адрес, но такой подход довольно безопасен в плане отказов. В нашем случае мы работаем из нескольких местоположений, соединенных посредством каналов WAN с ретрансляцией кадров. Сеть не всегда способна хорошо преобразовывать имена серверов в IP-адреса, поэтому команда net use \\BF1 обычно сообщает о невозможности *найти* \\BF1. Но даже если она *работает*, распознавание имен — преобразование имени вроде BF1 в сетевой адрес — занимает время.

Если вам известен IP-адрес сервера, с которым вы пытаетесь взаимодействовать, то указывайте его вместо имени этого сервера. Зная, что IP-адресом сервера BF1 является 134.81.12.4, вы можете ввести такую команду:

```
net use \\134.81.12.4\apps
```

И поскольку потенциально вы можете подключаться из другой сети, понадобится добавить информацию /user:. Неплохо также указать /persistent:no, чтобы ваша система не тратила до пяти минут на попытки восстановления этого подключения при следующей загрузке. Таким образом, например, если сервер BF1 является членом домена под названием BigFirm.com, и вы располагаете учетной записью в домене BigFirm.com по имени boss, то вы можете удостовериться в том, что BF1 знает, кто вы такой, и позволит войти в систему:

```
net use \\134.81.12.4\apps /user:bigfirm.com\boss /persistent:no
```

Хотя существует много удобных методов подключения к общим ресурсам с применением различных графических пользовательских интерфейсов, не упускайте из виду команду net use. Вы наверняка сочтете ее полезной.

Распространенные общие ресурсы

В Windows Server имеется несколько заранее созданных и распространенных общих ресурсов. Большинство из них являются скрытыми. Если вы знаете эти общие ресурсы, то сможете подключиться к любому из них, используя путь UNC.

- **C$, D$ и т.д.** Все устройства, включая устройство для чтения CD-ROM, имеют скрытые общие ресурсы для своего корня. Общие ресурсы такого рода называются *административными общими ресурсами*. Вы не можете изменять разрешения или свойства этих общих ресурсов, разве что конфигурировать их для средства автономных файлов (Offline Files), о котором пойдет речь в конце главы. Подключаться к административным общим ресурсам могут только члены групп `Administrators` (Администраторы) и `Backup Operators` (Операторы резервного копирования), и вы не можете отменить совместный доступ для административных общих ресурсов, не модифицировав реестр или не остановив службу `Server` (что прекратит совместный доступ для всех обших ресурсов). Такие общие ресурсы пригодятся администраторам сервера, которые решают много задач управления дистанционно. Отображение диска на общий ресурс `C$` эквивалентно нахождению в каталоге `C:\` на сервере.

- **ADMIN$.** Общий ресурс `ADMIN$` — это еще один административный общий ресурс, который отображается на местоположение операционной системы. Например, если операционная система установлена в `D:\Windows`, то общий ресурс `ADMIN$` будет отображен на `D:\Windows`.

- **PRINT$.** Всякий раз, когда вы создаете совместно используемый принтер, система помещает его драйверы в этот общий ресурс. В результате при подключении клиентов к общему принтеру драйверы легко загружаются.

- **IPC$.** Общий ресурс `IPC$` является, пожалуй, одним из наиболее широко применяемых общих ресурсов в межсерверных коммуникациях, хотя вы редко будете взаимодействовать с ним напрямую. Когда вы пытаетесь получить доступ к общим ресурсам на других компьютерах (для чтения журналов событий, например), система использует *именованные каналы*. Именованный канал — это фрагмент памяти, служащий коммуникационным каналом между двумя процессами, будь они локальными или удаленными, и общий ресурс `IPC$` применяется этими именованными каналами.

- **NETLOGON.** Общий ресурс `NETLOGON` используется в сочетании с обработкой запросов входа со стороны пользователей. После успешного входа пользователи получают любую информацию профиля или сценарий, который должен для них выполниться. Таким сценарием часто является пакетный файл. Например, у нас имеется общий пакетный файл, который мы хотим запускать для всех пользователей каждый раз, когда они входят в систему. Это позволяет обеспечить выполнение всеми клиентами стандартного набора команд, подобных копированию обновленной информации о сети, отображению стандартных сетевых дисков и т.п. Такие пакетные файлы, сценарии и профили находятся внутри общего ресурса `NETLOGON`. Общий ресурс `NETLOGON` требуется на всех контроллерах домена.

- **SYSVOL.** Общий ресурс SYSVOL применяется для хранения информации групповой политики и сценариев, к которым обращаются клиенты по сети. Вы всегда будете видеть общие ресурсы SYSVOL на контроллерах домена, но они могут реплицироваться на серверы-члены.

Диспетчер ресурсов файлового сервера

Диспетчер ресурсов файлового сервера (File Server Resource Manager — FSRM) является важным дополнением, которое может конфигурироваться с помощью роли File and Storage Services (Службы файлов и хранилища). Он включает несколько дополнительных возможностей, упрощающих управление файловым сервером:

- создание и управление политиками квот;
- создание и управление политиками блокировки файлов;
- просмотр отчетов.

Эти приемы рассматриваются в последующих разделах.

Создание политик квот

Файловая система NTFS давно включала средства управления квотами, но благодаря FSRM, они были значительно усовершенствованы. Выражаясь кратко, квоты позволяют отслеживать и ограничивать пространство, которое пользователи могут потреблять на томе или в папке.

> **Сравнение мониторинга использования хранилища и политик квот**
>
> Хотя для мониторинга использования хранилища применяется та же самая технология, что и в политиках квот, доступных в файловой системе NTFS, в ней имеется тонкое отличие от политик квот. Мониторинг хранилища отслеживает том целиком и по умолчанию сконфигурирован на уведомление о ситуации, когда на диске заполняется 85% его емкости. Политики квот можно конфигурировать на отдельных папках, что дает возможность точной настройки того, что именно отслеживается.

При создании квот есть возможность установки лимитов, при которых выдается предупреждение, установки лимитов принудительного применения, предоставления уведомлений о достижении лимитов по электронной почте или через записи в журнале событий и даже выполнения команд в ответ на достижение любого лимита. Квоты могут быть установлены для любого общего ресурса на сервере или для любого заданного пути.

Квоты могут оказаться очень удобными для мониторинга хранилища на файловых серверах. Например, в вашем распоряжении может находиться файловый сервер с хранилищем в 2 Тбайт. Вы можете считать, что имеете более чем достаточно пространства, но если какие-то пользователи создают и редактируют аудио- и видео-файлы, то 2 Тбайт свободного пространства могут очень скоро сойти на нет. Политика квоты может помочь в ограничении пользователей определенным объемом. С другой стороны, эти аудио- и видео-файлы могут быть неотъемлемой частью вашей бизнес-деятельности, поэтому ограничивать пространство хранения

нежелательно. В таком случае лучше обеспечить информирование о том, что занятое пространство хранилища достигло определенного порога. Вместо действительного ограничения хранилища вы можете просто отслеживать его использование с помощью политики квоты.

На первый взгляд, политики квот очень просты для понимания и реализации. Тем не менее, они могут стать довольно сложными при практическом применении.

Шаблоны квот

В состав диспетчера FSRM включено несколько шаблонов квот, которые можно легко применять в том виде, как они есть, или же модифицировать для удовлетворения существующих нужд. Можно даже создавать собственные шаблоны. На рис. 13.21 показано диалоговое окно Configure Quota (Конфигурирование квоты) со стандартными шаблонами.

Рис. 13.21. Просмотр доступных шаблонов квот

Так как вы уже уловили идею о том, как работают квоты, по информации в этом диалоговом окне вы сможете понять, что будет делать та или иная квота. Важной частью информации является тип квоты: жесткая или мягкая. *Жесткая* квота будет принудительно применять лимит и предотвращать его превышение пользователями. *Мягкая* квота используется только для мониторинга; она выдаст уведомление, но не будет принудительно применять лимит.

Шаблон 200 MB Limit with 50 MB Extension (Лимит 200 Мбайт с расширением 50 Мбайт) представляет собой великолепный пример реагирования на достижение лимита квоты. Чтобы просмотреть или отредактировать свойства шаблона, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Edit Template Properties (Редактировать свойства шаблона).

На рис. 13.22 показаны свойства шаблона во время редактирования. Слева можно видеть базовый шаблон. Обратите внимание на нижнюю часть диалогового окна, где

сконфигурированы три порога для уведомлений: 85%, 95% и 100%. Предупреждение о достижении порога в 85% только отправляется по электронной почте, предупреждение о пороге в 95% отправляется по электронной почте и фиксируется как событие в журнале, а предупреждение о пороге в 100% дополнительно инициирует выполнение команды.

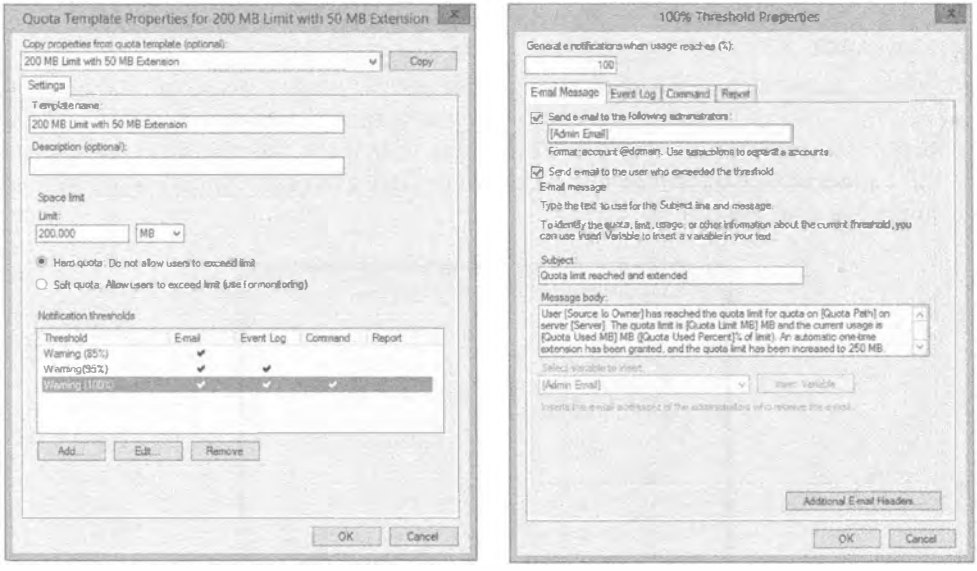


Рис. 13.22. Просмотр шаблона квоты

Диалоговое окно справа на рис. 13.22 открывается в результате выбора элемента Warning (100%) (Предупреждение (100%)) в списке Notification thresholds (Пороги для уведомлений) и щелчка на кнопке Edit (Редактировать). Для модификации квоты применяется инструмент командной строки `dirquota.exe`. В частности, он изменяет лимит квоты с 200 Мбайт на 250 Мбайт. Команды, которые вы здесь помещаете, ограничиваются разве что вашей фантазией. При необходимости вы также устанавливаете контекст безопасности команды в зависимости от разрешений, которые требуются команде для выполнения.

Помимо выполнения команды, доступны другие реакции на достижение порога: отправка сообщения электронной почты, регистрация события в журнале и создание отчета.

Вкладка E-mail Message

Вкладка E-mail Message (Сообщение электронной почты) позволяет конфигурировать почтовый ответ, отправляемый при достижении порога. Если вы хотите отправить сообщение администратору, просто добавьте на этой вкладке адрес электронной почты администратора (или группу рассылки администратора) в формате `учетная_запись@домен`, например, `ITAdmins@bigfirm.com`. Можете также сконфигурировать отправку сообщения пользователю, который превысил порог, отметив для этого флажок Send e-mail to the user who exceeded the threshold (Отправить сообщение электронной почты пользователю, превысившему порог). Для поиска адреса электронной почты пользователя диспетчер FSRM использует Active Directory.

Шаблоны включают заранее настроенную строку темы и тело сообщения, причем и там, и там присутствуют переменные. На рис. 13.23 видно, что тело сообщения содержит множество переменных: `Source Io Owner` (Исходный владелец операций ввода-вывода), `Quota Path` (Путь для квоты), `Server` (Сервер) и т.д. Если вы щелкнете внутри строки темы или тела сообщения, раскрывающийся список переменных сразу же станет доступным. При выборе любой переменной ниже списка отображается краткое объяснение того, что она собой представляет. Например, увидев поначалу `[Source Io Owner]`, не вполне ясно, что такое `Io`, но после выбора этой переменной в раскрывающемся списке становится понятно, что `Io` означает I/O, т.е. ввод-вывод.

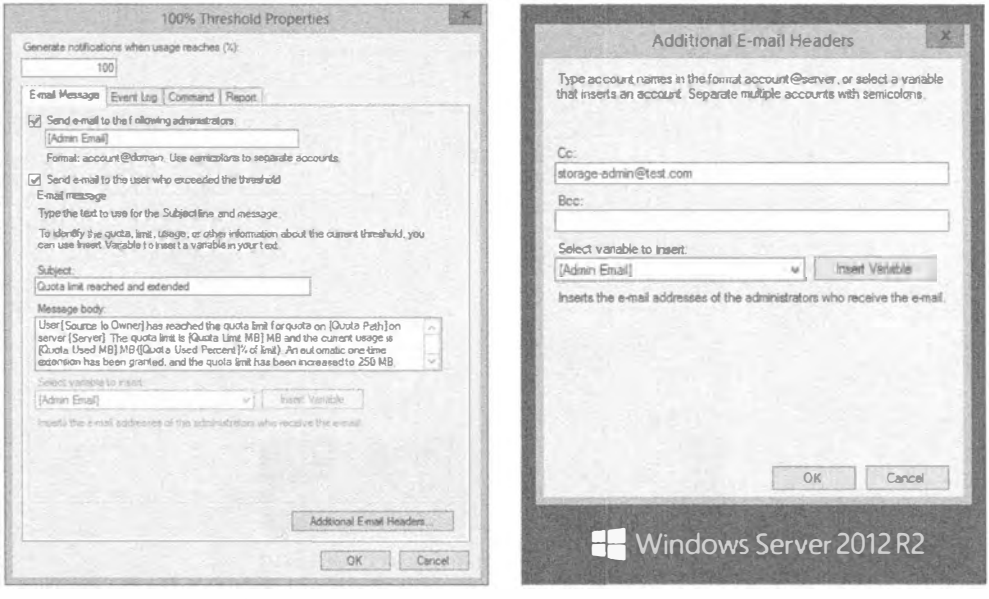


Рис. 13.23. Просмотр вкладки E-mail Message

Щелкнув на кнопке Additional E-mail Headers (Дополнительные почтовые заголовки), вы можете добавить в сообщение электронной почты дополнительные заголовки, которые показаны справа на рис. 13.23. Они также включают переменные, которые можно выбирать в раскрывающемся списке Select variable to insert (Выберите переменную для вставки) и щелкать на кнопке Insert Variable (Вставить переменную).

Сервер SMTP должен быть сконфигурирован

Для отправки сообщений электронной почты диспетчером FSRM его потребуется сконфигурировать с именем или IP-адресом сервера SMTP, который буде принимать эти сообщения. Это делается в диалоговом окне параметров диспетчера FSRM, которое рассматривается далее в главе.

Вкладка Event Log

При желании вы можете сконфигурировать регистрацию событий в журнале событий приложений. Для этого достаточно перейти на вкладку Event Log (Журнал событий) и отметить флажок Send warning to event log (Отправить предупреждение в журнал событий), как показано на рис. 13.24. Любые отправляемые события попадут в журнал событий приложений.

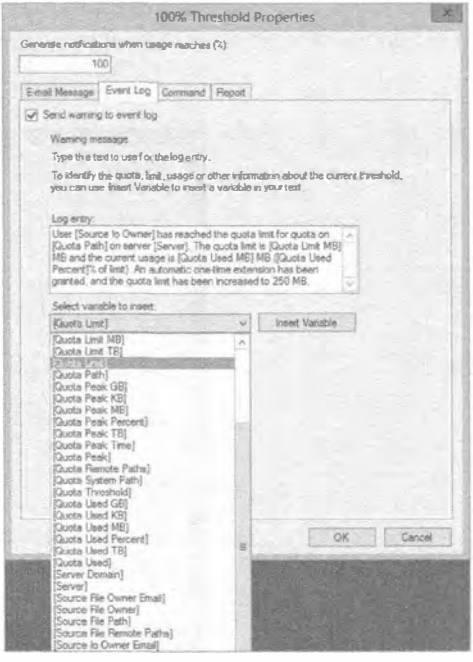


Рис. 13.24. Просмотр вкладки Event Log

Точно так же, как вы могли добавлять переменные в сообщения электронной почты, вы можете добавлять их в журнальные записи. На рис. 13.24 раскрыт список переменных, чтобы продемонстрировать доступные для добавления переменные. Переменных намного больше, чем удалось показать на этом рисунке.

Вкладка Report

Вкладка Report (Отчет) позволяет манипулировать порогами для уведомлений. Здесь вы можете настроить отчеты, которые генерируются в ответ на достижение порога и автоматически отправляются по электронной почте администраторам и/или пользователю. Отчеты могут также создаваться по запросу, как вы увидите позже в этой главе.

Создание квоты

Теперь, когда вы понимаете основы, создать и применить квоту довольно просто. В Windows Server 2012 R2 доступно несколько способов конфигурирования квот на разных уровнях общих ресурсов и папок. Если вы уже создали общий ресурс и шаблоны квот, то можете легко сконфигурировать квоту, щелкнув правой кноп-

кой мыши на общем ресурсе на вкладке Shares (Общие ресурсы) в окне диспетчера серверов для роли File and Storage Services и выбрав в контекстном меню пункт Configure Quota (Сконфигурировать квоту). Корректировка свойств и создание шаблонов квот делается прямо в диспетчере FSRM, доступном через меню Tools (Сервис) диспетчера серверов.

Предположим, что вы хотите отслеживать объем данных, которые хранятся в папке по имени `Graphics` в системе. В частности, вам нужно знать, приблизился ли объем используемого хранилища к 500 Мбайт. Если этот лимит достигнут, вы хотите отправить пользователю отчет, который позволит ему выяснить, какие файлы дублируются, какие файлы являются самыми крупными, а какие файлы давно не использовались.

Для создания такой квоты понадобится выполнить следующие шаги.

1. Запустите диспетчер серверов и выберите в меню Tools (Сервис) пункт File Server Resource Manager (Диспетчер ресурсов файлового сервера).
2. Разверните узел Quota Management (Управление квотами), щелкните правой кнопкой мыши на папке Quotas (Квоты) и выберите в контекстном меню Create Quota (Создать квоту).
3. Введите в текстовом поле Quota Path (Путь для квоты) путь к папке, которую вы хотите отслеживать.

   Например, вы могли бы ввести **`I:\Finance`**. В качестве альтернативы можете щелкнуть на кнопке Browse (Обзор) и проследовать на нужный путь. Здесь на выбор доступна возможность применить эту новую квоту только к выбранной папке или распространить действие шаблона квоты на все существующие и новые подпапки внутри папки `Graphics`.

   Следующий выбор в этом окне позволяет определить свойства квоты.
4. Для целей данного упражнения выберите шаблон 200 MB Limit Reports to User (Лимит 200 Мбайт с выдачей отчета пользователю). Позже мы отредактируем свойства этой квоты.
5. Просмотрите сводку по свойствам квоты и щелкните на кнопке Create (Создать).

   Новая квота отобразится, позволив дальнейшую модификацию ее свойств.
6. Щелкните правой кнопкой мыши на новой квоте и выберите в контекстном меню пункт Edit Quota Properties (Редактировать свойства квоты).

   В диалоговом окне Quota Properties (Свойства квоты) предоставьте описание новой квоты.
7. Затем вручную скорректируйте значение в поле Space limit (Лимит пространства) на 500 Мбайт и оставьте без изменений выбранный по умолчанию переключатель Hard quota (Жесткая квота). Теперь можете отредактировать пороги для уведомлений (в списке Notification thresholds (Пороги для уведомлений)), как показано в левой части рис. 13.25.
8. Выберите в списке Notification thresholds элемент Warning (100%) (Предупреждение (100%)) и щелкните на кнопке Edit (Редактировать).

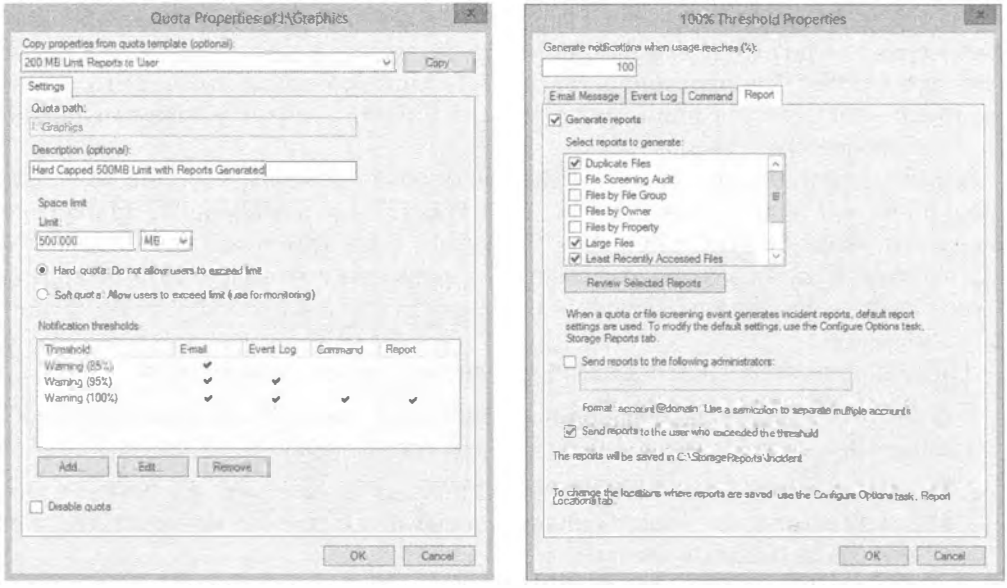


Рис. 13.25. Просмотр вкладки Report диалогового окна свойств новой квоты

9. Просмотрите информацию на вкладках E-mail Message (Сообщение электронной почты), Event Log (Журнал сообщений) и Command (Команда).

   Если появляется предупреждение о том, что сервер SMTP не сконфигурирован, ознакомьтесь с ним и для продолжения щелкните на кнопке Yes (Да); вы можете сконфигурировать сервер SMTP позже. Обратите внимание на возможность изменения данных на любой из этих вкладок.

10. Перейдите на вкладку Report, которая должна выглядеть примерно так, как показано справа на рис. 13.25.

    Обратите внимание, что отчеты уже сконфигурированы. Флажок Generate reports (Генерировать отчеты) отмечен, и для генерации указаны три отчета: Duplicate Files (Дублированные файлы), Large Files (Большие файлы) и Least Recently Accessed Files (Файлы с наиболее давним доступом). Вдобавок квота сконфигурирована на отправку отчетов пользователю, который превысил порог (отмечен флажок Send reports to the user, who exceeded the threshold (Отправлять отчеты пользователю, превысившему порог)).

11. Щелкните на кнопке OK, чтобы закрыть диалоговое окно 100% Threshold Properties (Свойства порога 100%).

12. Щелкните на кнопке OK, чтобы закрыть диалоговое окно Quota Properties.

Создание политик блокировки файлов

Фильтры блокировки файлов используется для фильтрации файлов, чтобы гарантировать, что файлы определенных типов не сохраняются на сервере. Предположим, после внедрения политики квоты и ознакомления с рядом отчетов вы обнаруживаете, что диск F почти полон, т.к. один из пользователей сохранил на сервере несколько гигабайтов резервных копий файлов MP3.

Хотя замечательно, что пользователь создает резервные копии своих файлов, вас может не устраивать тот факт, что он задействует для этого ваш сервер. Кроме того, вы можете решить, что на вашем сервере вообще никто не должен хранить файлы MP3 или любые другие аудио- либо видео-файлы.

Вы можете создать фильтр блокировки файлов, которая будет блокировать сохранение пользователями определенных типов файлов и генерировать уведомления, когда кто-то попытается записать блокируемые файлы на сервер. Фильтры блокировки файлов могут быть созданы на целых томах или конкретных папках, и точно так же, как квоты имеют шаблоны, фильтры блокировки файлов также могут иметь шаблоны. На рис. 13.26 показано окно диспетчера серверов с отображаемыми шаблонами блокировки файлов.

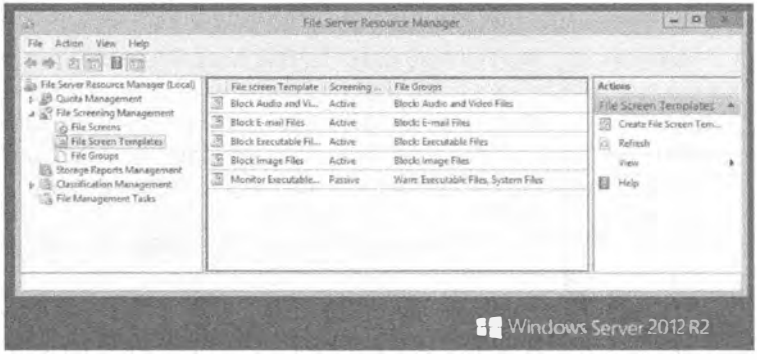


Рис. 13.26. Просмотр шаблонов блокировки файлов

Обратите внимание, что в шаблонах идентифицировано несколько хорошо известных типов групп файлов, таких как аудио- и видео-файлы и файлы изображений. Конкретные расширения этих типов файлов идентифицированы в узле File Groups (Группы файлов). Например, аудио- и видео-файлы включают расширения `.mp1`, `.mp2`, `.mp3`, `.mp4` и `.mpeg` — причем это далеко не полный перечень.

Когда вы создаете фильтр блокировки файлов, то просто выбираете одну из групп файлов. Это будет удовлетворять вашим потребностям большую часть времени, но если вы хотите добавить типы файлов либо исключить определенные типы файлов из политики, то можете соответствующим образом модифицировать содержимое.

Представьте, что в вашей компании недавно узнали, что многие пользователи хранят на сервере файлы Outlook с расширением `.pst`, которые имеют размеры свыше 1 Гбайт и поглощают пространство хранилища. В компании заявили, что пользователи не могут хранить файлы электронной почты на файловом сервере. Чтобы обеспечить применение этого правила, выполните описанные ниже шаги.

1. Запустите диспетчер серверов и перейдите к узлу File Screen Templates (Шаблоны блокировки файлов).
2. Щелкните правой кнопкой мыши на шаблоне Block E-mail Files (Блокировать файлы электронной почты) и выберите в контекстном меню пункт Create File Screen from Template (Создать фильтр блокировки файлов из шаблона).
3. В текстовом поле File Screen Path (Путь для фильтра блокировки) введите имя тома, на котором необходимо организовать блокировку файлов (такое как **`F:\`**).

Поскольку был выбран шаблон Block E-mail Files, свойства фильтра блокировки файлов уже установлены. Это свойства можно было бы изменить или при желании даже определить специальные свойства. Оставьте выбор по умолчанию и просмотрите сводку в нижней части окна.

4. Щелкните на кнопке Create (Создать).
5. Выберите узел File Screens (Фильтры блокировки файлов), находящийся выше узла File Screen Templates (Шаблоны блокировки файлов) в дереве диспетчера FSRM.
6. Щелкните правой кнопкой мыши на только что созданном фильтре блокировки файлов и выберите в контекстном меню пункт Edit File Screen Properties (Редактировать свойства фильтра блокировки файлов). Диалоговое окно должно выглядеть подобным показанному на рис. 13.27.

   Обратите внимание, что вы можете выбрать либо переключатель Active screening (Активная блокировка), либо переключатель Passive screening (Пассивная блокировка). Поскольку вы хотите конкретно блокировать сохранение пользователями файлов на сервере, оставьте выбранным переключатель Active screening. Пассивная блокировка используется для мониторинга.

Рис. 13.27. Просмотри свойств фильтра блокировки файлов

7. Просмотрите информацию на вкладках E-mail Message (Сообщение электронной почты), Event Log (Журнал сообщений), Command (Команда) и Report (Отчет).

   Если появляется предупреждение о том, что сервер SMTP не сконфигурирован, ознакомьтесь с ним и для продолжения щелкните на кнопке Yes (Да). Вы заметите, что эти вкладки очень похожи на те, что применялись при настройке квот. Изменилось только содержимое уведомления.

8. После просмотра вкладок щелкните на кнопке OK.

Генерация отчетов

Доступно несколько разных отчетов. Отчеты можно генерировать как часть любой политики квоты или политики блокировки файлов. Можно также настроить генерацию отчетов по графику или генерировать их по требованию.

К счастью, отчеты удобно именованы, поэтому основное их содержимое легко определить по одному лишь имени. Доступны следующие отчеты: Duplicate Files (Дублированные файлы), File Screening Audit (Аудит блокировки файлов), Files by File Group (Файлы по файловым группам), Files by Owner (Файлы по владельцам), Files by Property (Файлы по свойствам), Large Files (Большие файлы), Least Recently Accessed Files (Файлы с наиболее давним доступом), Most Recently Accessed Files (Файлы с наименее давним доступом) и Quota Usage (Показатели использования квоты). Кроме того, отчеты можно сохранять в разных форматах, таких как DHTML, HTML, XML, CSV и текстовый. Для доступа к отчетам выполните следующие шаги.

1. Запустите диспетчер серверов. Щелкните правой кнопкой мыши на узле Storage Reports Management (Управление отчетами по хранилищу) в окне диспетчера ресурсов файлового сервера (File Server Resource Manager) и выберите в контекстном меню пункт Generate Reports Now (Сгенерировать отчеты сейчас).

   На вкладке Settings (Настройки) вы можете выбрать столько отчетов, сколько нужно, но в случае выбора их всех запаситесь терпением; для крупных томов генерация всех отчетов займет довольно ощутимое время. Некоторые отчеты имеют дополнительные параметры, допускающие модификацию. Например, если вы выбрали отчет Quota Usage, то можете щелкнуть на кнопке Edit Parameters (Редактировать параметры) и изменить минимальный показатель использования квоты, который будет включен в отчет.

2. Выберите отчеты, подлежащие генерации, и отметьте флажки возле форматов, в которых хотите получить эти отчеты. Диалоговое окно будет выглядеть примерно так, как показано на рис. 13.28.

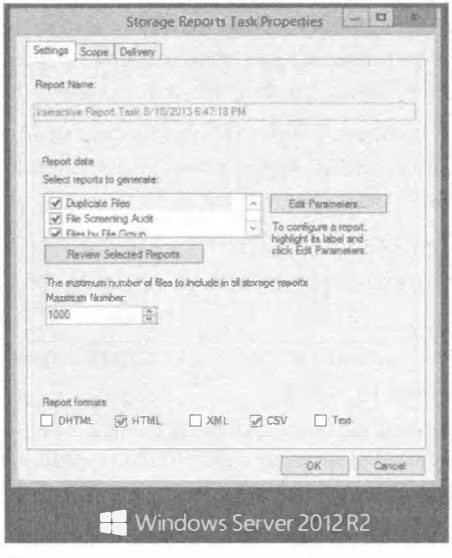


Рис. 13.28. Выбор типов и форматов для генерируемых отчетов

3. Перейдите на вкладку Scope (Область действия).

   На этой вкладке необходимо выбрать тип данных, которые будут накапливаться в отчетах.

4. Сделайте выбор типов файлов и щелкните на кнопке Add (Добавить).

   Откроется диалоговое окно, в котором можно перейти к нужным папкам и добавить их для формирования отчетов.

5. Выберите папки и щелкните на кнопке OK.

   Последней вкладкой диалогового окна Storage Reports Task Properties (Свойства задачи генерации отчетов по хранилищу) является Delivery (Доставка). Отчеты можно отправить по электронной почте администратору.

6. Просто отметьте флажок и укажите адрес электронной почты лица, которому должны быть отправлены отчеты.

   Это особенно удобно для отчетов, генерируемых по графику. Например, можно генерировать все отчеты в воскресенье и обеспечить их отправку по электронной почте в понедельник утром для просмотра.

7. В диалоговом окне Generate Storage Reports (Генерация отчетов по хранилищу) выберите переключатель Generate Reports in the Background (Генерировать отчеты в фоновом режиме) и щелкните на кнопке OK.

   В результате будет создана задача генерации отчетов, которая удалится после своего завершения. По умолчанию в диалоговом окне выбран переключатель Wait for the reports to generate and then display them (Ожидать генерации отчетов и затем отобразить их). Вы можете отслеживать выполнение задачи, а после ее завершения отчеты отобразятся. Стандартным местоположением для локального сохранения отчетов на сервере является `\\c$\StorageReports\Interactive`. В зависимости от объема данных в отчетах выполнение может потребовать нескольких минут.

8. Пока задача генерации отчетов выполняется, щелкните правой кнопкой мыши на узле Storage Reports Management и выберите в контекстном меню пункт Schedule a New Report Task (Запланировать новую задачу генерации отчетов).

9. На вкладке Settings назначьте новой запланированной задаче генерации отчетов подходящее имя, укажите виды отчетов, подлежащие генерации, и выберите форматы этих отчетов.

10. Перейдите на вкладку Scope.

    Здесь необходимо выбрать тип данных и папки, для которых будут формироваться отчеты.

11. На вкладке Delivery отметьте флажок и укажите адрес электронной почты для еженедельной отправки отчетов.

    Для любых уведомлений по электронной почте, предоставляемых FSRM, потребуется соответствующим образом сконфигурированный сервер SMTP.

12. По умолчанию на вкладке Schedule (График) выбран переключатель Weekly (Еженедельно), отмечен флажок Sunday (Воскресенье), а в поле Run at (Запускать в) указано 5:00:00 утра (рис. 13.29).

Рис. 13.29. Планирование генерации отчетов

13. Щелкните на кнопке OK, чтобы принять график.

    Новый график теперь отображается в окне FSRM с раскрытым узлом Storage Reports Management. При наличии сконфигурированного сервера SMTP, щелкните правой кнопкой мыши на задаче и запустите ее, чтобы протестировать выполненную работу.

Отслеживайте потребление дискового пространства отчетами

Если вы создаете график генерации отчетов, который будет создавать файлы отчетов в вашей системе, то должны отслеживать объем пространства, занимаемого отчетами. При наихудшем сценарии график генерации отчетов сформирован, и отчеты регулярно создаются, постоянно потребляя дисковое пространство. Чтобы снизить это влияние на функционирование сервера, можно изменить стандартное местоположение отчетов, модифицировав настройки на вкладке Report Locations (Местоположения для отчетов) в окне параметров File Server Resource Manager.

К этому моменту созданная ранее задача генерации отчетов должна завершиться.

14. Перейдите к отчетам, расположенным в папке `%systemdrive%\StorageReports\Interactive`, используя для этого проводник Windows.
15. Дважды щелкните на сгенерированных HTML-файлах, чтобы просмотреть доступную в них информацию. Дважды щелкните на текстовых файлах, чтобы взглянуть, как отображается информация внутри них.

Как видите, диспетчер FSRM предлагает развитые возможности построения отчетов.

Параметры File Server Resource Manager

Для модификации доступно множество параметров FSRM. Параметры на вкладке Email Notifications (Уведомления по электронной почте) должны быть сконфигурированы, прежде чем вы сможете пользоваться любыми почтовыми возможностями сервера. Чтобы открыть диалоговое окно настройки параметров, щелкните правой кнопкой мыши на элементе File Server Resource Manager (Диспетчер ресурсов файлового сервера) внутри диспетчера серверов и выберите в контекстном меню пункт Configure Options (Конфигурировать параметры). Откроется диалоговое окно свойств с семью вкладками.

- **Email Notifications (Уведомления по электронной почте).** Если вы хотите использовать уведомления по электронной почте, то должны ввести имя или IP-адрес сервера SMTP, который будет принимать почтовые отправления от вашего сервера. На этой вкладке вы также вводите стандартный адрес электронной почты для получателя-администратора и стандартный адрес From (От). Чтобы удостовериться в корректности сконфигурированных настроек, можно отправить тестовое сообщение электронной почты.
- **Notification Limits (Лимиты для уведомлений).** После того, как порог (такой как потребление 85% пространства на диске) достигнут, он остается актуальным до тех пор, пока не будет предпринято какое-то действие. Вместо того чтобы досаждать пользователю уведомлениями каждые 30 секунд, вы можете установить лимиты времени в минутах для таких уведомлений. По умолчанию для каждой реакции на достижение порога — уведомлению по электронной почте, записи в журнал событий и генерации отчетов — отводится 60 минут.
- **Storage Reports (Отчеты по хранилищу).** Многие отчеты имеют параметры, которые можно модифицировать. Каждый параметр, допускающий изменение, имеет стандартное начальное значение, которое может быть установлено на этой вкладке.
- **Report Locations (Местоположения для отчетов).** Отчеты сохраняются в стандартных местоположениях на системном диске (которым обычно является `c:\`). Внутри папки `%systemdrive%\StorageReports` создаются три подпапки: `Incident` (для уведомлений), `Scheduled` (для запланированных задач генерации отчетов) и `Interactive` (для отчетов, генерируемых по требованию). На этой вкладке можно изменить стандартные местоположения для любых отчетов.
- **File Screen Audit (Аудит блокировки файлов).** На этой вкладке присутствует единственный флажок Record file screening activity in an auditing database (Записывать действия по блокировке файлов в базу данных аудита). Если он отмечен, действия блокировки будут фиксироваться в базе данных с целью дальнейшего изучения с помощью отчета по аудиту блокировки файлов.
- **Automatic Classification (Автоматическая классификация).** Файлами можно управлять на основе свойств классификации и создаваемых вами правил, а не на базе того, где эти файлы находятся в дереве каталогов. Если вы используете управление классификацией (это делают немногие), можете на данной вкладке создать расписание для применения правил классификации и генерации отчетов. Дополнительные сведения о классификации файлов приведены в следующей статье TechNet: `http://technet.microsoft.com/library/dd758765.aspx`.

- **Access-Denied Assistance (Помощь при запрете доступа).** Появившаяся в версии Windows Server 2012 вкладка Access-Denied Assistance позволяет настраивать собственное сообщение об ошибке запрета доступа, которое отображается пользователю, не имеющему подходящих разрешений для доступа к определенной папке или файлу. Кроме того, можно предоставить пользователям возможность запрашивать помощь прямо из сообщения об ошибке, щелкая на гиперссылке. Это очень удобная функция.

Хотя NTFS — великолепная файловая система, включающая такие дополнительные средства, как квоты NTFS, вы можете получить намного больше возможностей за счет использования диспетчера FSRM. Если вы управляете файловым сервером, полезно ознакомиться с этими дополнительными средствами.

Протокол SMB 3.0

Блок сообщений сервера (Server Message Block — SMB) — это сетевой протокол уровня приложений, который применяется в основном для предоставления общего доступа к файлам, принтерам, портам и коммуникациям между машинами в сети. На протокол SMB обычно ссылаются как на общую файловую систему для Интернета (Common Internet File System — CIFS). Этот протокол используется главным образом с операционными системами Windows и служит основой для реализации распределенной файловой системы (Distributed File System) от Microsoft.

В текущей редакции сервера протокол SMB 3.0 несколько изменился. Многие новые функции делают этот протокол надежной и высокопроизводительной альтернативой применению устройств Fibre Channel и iSCSI. Давайте рассмотрим некоторые новые возможности.

- **Обход отказа транспорта SMB.** Эта возможность позволяет администраторам проводить обслуживание на кластеризированных компьютерах без необходимости в каком-либо простое. В случае обхода отказа в кластере клиенты SMB 3.0 будут автоматически подключены к другой кластеризированной машине, не теряя доступ к общим файловым ресурсам, которые они использовали. Кластеризированные машины файловых серверов устраняют единую точку отказа, когда имеется только один файловый сервер или некластеризированная среда.
- **Масштабирование SMB.** Клиенты SMB больше не ограничены полосой пропускания одиночного узла кластера. Кластеризированные машины балансируют нагрузку между собой с применением своих собранных вместе ресурсов. Не каждый сервер в кластере файловых серверов является активным узлом, обслуживающим содержимое для клиентов. Масштабируемые общие файловые ресурсы SMB всегда сконфигурированы с набором свойств Continuously Available (Постоянная готовность).
- **Многоканальность SMB.** Данная возможность позволяет файловым серверам использовать несколько сетевых подключений одновременно, что значительно увеличивает полосу пропускания, т.к. можно передавать больше данных через множество высокоскоростных сетевых адаптеров в одно и то же время. Это также означает наличие нового уровня отказоустойчивости в сети. Применяя несколько подключений одновременно, клиенты продолжат бесперебойную работу в случае утери какого-то одного подключения. Еще одним преиму-

ществом многоканальности SMB является автоматическое обнаружение. Это средство будет обнаруживать наличие доступных сетевых путей и динамически добавлять подключения по мере надобности.

- **Протокол SMB Direct.** Протокол SMB Direct — это новый транспортный протокол для SMB 3.0, который разрешает прямую передачу данных между серверами с минимальным участием центрального процессора и низкой задержкой, когда имеются сетевые адаптеры с поддержкой RDMA (remote direct memory access — удаленный прямой доступ в память). Сетевой файловый сервер становится способным к размещению локального хранилища для приложений, подобных Microsoft SQL Server 2012 и Microsoft Hyper-V.
- **Командлеты Windows PowerShell и объекты WMI для SMB.** Крупным преимуществом в Windows Server 2012 является то, что все управляющие командлеты PowerShell теперь включены в состав операционной системы. Новые командлеты SMB позволяют администраторам управлять и отслеживать файловые серверы и общие файловые ресурсы. Вы можете также написать сценарии для автоматизации общих задач администрирования файлового сервера. Благодаря новым объектам WMI, разработчики извлекают выгоду из возможности создания автоматизированных решений для конфигурирования и мониторинга файлового сервера.
- **Шифрование SMB.** Эта новая функция позволяет шифровать данные на ходу на основе файлов или общих ресурсов. Она защитит передаваемые данные от перехвата или подделки без протокола IPsec или любого дополнительного выделенного оборудования. Шифрование SMB также очень удобно, когда удаленные пользователи пытаются получить доступ к данным из незащищенных сетей. Оно обеспечит защиту данных при их передаче из ресурсов корпоративной сети в незащищенную удаленную сеть пользователя. Ранее в главе мы включали шифрование SMB путем отметки соответствующего флажка на экране Other Settings (Другие настройки) мастера создания общего ресурса (New Share Wizard) при выполнении упражнения по созданию новых общих ресурсов. Эту функцию можно также включить прямо в диспетчере серверов, не прибегая к помощи мастера.
- **Аренда каталогов SMB.** Данная функция использует BranchCache для предоставления более быстрого доступа к документам через сети WAN, которым присуща высокая задержка. Аренда каталогов сокращает количество полных циклов коммуникации между клиентом и сервером через WAN. Клиент кеширует метаданные каталогов и файлов в согласованной манере на более длительные периоды времени. Когда информация изменяется, сервер уведомляет клиента и инициирует синхронизацию, которая обновит кеш клиента. Эта функция спроектирована для работы с домашними папками пользователей и опубликованными общими ресурсами.

Спецификация протокола SMB 3.0

Хотя здесь были подчеркнуты некоторые важные возможности SMB 3.0, мы определенно не раскрыли абсолютно все. Если вы желаете ознакомиться с полной спецификацией протокола, проследуйте по ссылке `http://support.microsoft.com/kb/2709568`.

Совместимость с версиями SMB 2.0 и SMB 1.0

Для обеспечения обратной совместимости новейшие операционные системы поддерживают версии протокола SMB 2.0 и SMB 1.0. Чтобы получить полную отдачу от функций, доступных в SMB 3.0, и на сервере, и на клиенте должна быть возможность применения SMB 3.0. В табл. 13.3 показаны версии операционных систем и поддерживаемые ими версии протокола SMB. Сопоставив серверную ОС в верхней строке с клиентской ОС в левом столбце таблицы, вы получите версию SMB, которая будет использоваться во время взаимодействия. Например, если вы выберете Windows Server 2008 R2 в верхней строке и Windows 7 в левом столбце, то на пересечении будет указано, что самой высокой поддерживаемой версией протокола является SMB 2.1.

Таблица 13.3. Версии операционных систем и поддержка протокола SMB

Клиентская/серверная операционная система	Windows 8 Windows Server 2012 R2	Windows 7 Windows Server 2008 R2	Windows Vista Windows Server 2008	Предшествующие версии Windows
Windows 8 Windows Server 2012 R2	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 Windows Server 2008 R2	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista Windows Server 2008	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
Предшествующие версии Windows	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

Версия SMB 3.0 применяется всякий раз, когда это возможно для клиентов, которые ее поддерживают. Поскольку SMB 3.0 не поддерживается другими операционными системами (такими как Windows 7 или Windows Server 2008), более новые клиенты могут использовать старые версии протокола при взаимодействии с унаследованными машинами. Хорошая новость в том, что все это делается автоматически. Вам не придется предпринимать какие-то действия по конфигурированию, чтобы задействовать SMB 3.0 либо переключиться обратно на SMB 2.0 или SMB 1.0 для унаследованных клиентов. Вот что автоматически происходит в отношении SMB:

- если оба клиента поддерживают SMB 3.0, то SMB 3.0 будет применяться автоматически;
- если один из клиентов не поддерживает SMB 3.0 (например, Windows 7), то для этого сеанса будет использоваться версия SMB, поддерживаемая этой ОС (SMB 2.1 в данном примере).

Вероятно, вы уже слышали о маркетинговых кампаниях "Вместе лучше" ("Better Together"), проводимых Microsoft. Это не просто маркетинг ради маркетинга. Протокол SMB является одним из примеров, где вы по-настоящему получите более высокую производительность, сочетая вместе новые технологии. В сети с серверами Windows Server 2012 R2, но с рабочими столами Windows 7 версия протокола SMB 3.0 применяться не сможет. Если это занятая сеть, то разница окажется заметной.

Безопасность SMB

В этой редакции сервера в реализацию SMB 3.0 было внесено несколько улучшений, касающихся безопасности. Протокол SMB 3.0 получил новый алгоритм для подписи SMB под названием AES-CMAC. Алгоритм CMAC (Cipher-based Message Authentication Code — код аутентификации сообщений, основанный на шифре) базируется на блочном шифре с симметричным ключом (AES (Advanced Encryption Standard — расширенный стандарт шифрования)), тогда как алгоритм HMAC, используемый в SMB 2.0, основан на хеш-функции (SHA (Secure Hash Algorithm — алгоритм безопасного хеширования)). Стандарт AES был спецификацией, официально принятой правительством США в 2002 году, и одобрен Агентством национальной безопасности для шифрования совершенно секретной информации.

Алгоритм AES-CMAC обеспечивает более строгую гарантию целостности данных, чем контрольная сумма или код обнаружения ошибок. Алгоритм CMAC предназначен для обнаружения преднамеренных, неавторизованных изменений данных, а также случайных изменений. Верификация с помощью кода обнаружения ошибок или контрольной суммы позволяет выявить только случайные изменения данных.

Алгоритм HMAC SHA-256, применяемый в SMB 2.0, поддерживает целостность данных — гарантию того, что данные не были модифицированы. Хотя SMB 1.0 также обеспечивает целостность данных, безопасность в HMAC SHA-256 выше, а в AES-CMAC — еще выше.

Хеш — это просто число, созданное путем выполнения алгоритма хеширования над пакетом, сообщением или файлом. До тех пор пока пакет остается тем же самым (не изменяется), алгоритм хеширования будет всегда давать один и тот же хеш (одинаковое число). В общем, хеш обеспечивает целостность данных для пакетов, сообщений или файлов, следуя описанным ниже шагам.

1. Создание пакета.
2. Вычисление хеша для пакета.
3. Отправка пакета и хеша получателю.
4. Получатель вычисляет хеш полученного пакета и сравнивает его с полученным хешем.
   - Если хеши совпадают, целостность данных соблюдена.
   - Если хеши отличаются, целостность данных утеряна. Это может произойти из-за того, что атакующий изменил данные, или просто потому, что биты во время транспортировки потерялись.

Тем не менее, если атакующий может модифицировать данные в пути, то почему бы ему не изменить также и хеш во время передачи? Чтобы воспрепятствовать этому, хеш шифруется с помощью ключа сеанса, известного только клиенту и серверу. Такой процесс называется *цифровым подписанием* пакета в SMB 1.0 и SMB 2.0. Он выглядит следующим образом.

1. Создание пакета.
2. Вычисление хеша для пакета.
3. Шифрование хеша помощью ключа сеанса (или общего ключа).
4. Отправка пакета с зашифрованным хешем.

5. Получатель расшифровывает зашифрованный хеш.
6. Получатель вычисляет хеш полученного пакета.
7. Получатель сравнивает два хеша, чтобы выяснить, не утеряна ли целостность данных.

Включение цифрового подписания для пакетов SMB 1.0 может снизить производительность на 10–15%. Хотя вы по-прежнему столкнетесь с падением производительности в SMB 2.0, она не настолько значительна. Одна из основных причин связана с упрощением SMB 2.0, в результате чего меньше пакетов отправляется и меньше пакетов нуждается в подписании.

Внедрение BitLocker

Шифрование дисков BitLocker (BitLocker Drive Encryption) — это технология, предназначенная для обеспечения защиты целых дисковых накопителей. Более новой технологией является BitLocker To Go, которая появилась в Windows 7 и позволяет шифровать флэш-накопители USB. Здесь мы сосредоточим внимание на использовании BitLocker Drive Encryption для защиты дисков в Windows Server 2012.

Основное предназначение BitLocker заключается в шифровании данных на жестких дисках, чтобы в случае их похищения или утери данные были недоступными. Это часто применяется на ноутбуках и серверах, расположенных в местах со слабой физической защитой. Ноутбуки легко украсть — люди часто оставляют их в конференц-залах на время обеда или забывают их на стульях, откуда они быстро исчезают.

Подобным же образом серверы, находящиеся в удаленных офисах, часто слабо защищены физически — во всяком случае, слабее, чем в головном офисе. Возможно, главная серверная комната очень хорошо физически защищена, но сервер в удаленном офисе может скрываться за дверцами шкафа, которые легко открыть ломиком или даже кредитной карточкой.

BitLocker усиливает физическую защиту

BitLocker усиливает физическую защиту, но не может противостоять всем возможным атакам. Вредоносное программное обеспечение, такое как руткиты, может организовать в системе слабые места, которые сделают возможным доступ к данным, если компьютер впоследствии будет похищен.

Кроме того, если дисковые устройства на выведенном из эксплуатации сервере не очищены, они могут содержать данные, делиться которыми нежелательно. BitLocker защитит эти данные от несанкционированного использования.

На первый взгляд, может показаться, что данные на этих дисках защищены посредством разрешений. Однако атакующий может настроить домен и поместить свою учетную запись в группу `Enterprise Admins` (Администраторы предприятия). Имея физический доступ к серверу, он затем может изъять дисковое устройство из сервера, установить его на свой сервер и легко получить права владения над всеми файлами. После этого он будет владеть всеми вашими данными. Тем не менее, если файлы зашифрованы, атакующему будет намного труднее получить доступ к данным — мы не решаемся утверждать о полной невозможности доступа, но сам факт шифрования вполне может отпугнуть большинство атакующих.

Что нового в BitLocker

В Microsoft добавили к BitLocker несколько впечатляющих новых функций в версиях Windows 8 и Windows Server 2012. Теперь средство BitLocker может быть настроено перед установкой, и тогда шифрование понадобится только для используемого дискового пространства. Это сэкономит массу времени на обеих сторонах установки. Одним из недостатков первоначального выпуска BitLocker было длительное время, затрачиваемое на шифрование диска. Очень приятно видеть значительный рост производительности в данной редакции BitLocker. Ниже перечислены новые возможности и функции последнего выпуска.

- **Настройка BitLocker.** За счет применения среды предустановки Windows (Windows Preinstallation Environment — WinPE) администраторы теперь могут включить BitLocker перед развертыванием операционной системы.
- **Шифрование только используемого дискового пространства.** Эта функция позволяет выполнять шифрование гораздо быстрее за счет того, что ему подвергается только используемое дисковое пространство. Доступны два метода шифрования: Full Volume Encryption (Шифрование полного тома) и Used Disk Space Only (Только используемое дисковое пространство).
- **Возможность изменения PIN-кода и пароля стандартными пользователями.** Для конфигурирования BitLocker по-прежнему требуются административные привилегии, но теперь стандартным пользователям предоставлена возможность изменять PIN-код или пароль для тома операционной системы либо тома фиксированных данных по умолчанию.
- **Защита Network Unlock.** В Windows Server 2012 R2 появилась новая опция защиты BitLocker для томов операционной системы — Network Unlock. Машины домена, присоединенные к доверенной проводной сети, могут иметь разблокированный системный том сразу после загрузки системы. Это очень удобно в случае утери PIN-кода.
- **Поддержка зашифрованных жестких дисков для Windows.** Версии Windows 8 и Windows Server 2012 теперь содержат поддержку BitLocker для зашифрованных жестких дисков. BitLocker будет поддерживать заранее зашифрованные жесткие диски Windows от производителя.
- **Шифрование для кластеризированных общих томов.** Шифрование томов BitLocker поддерживается для кластеров с обходом отказа, которые функционируют под управлением Windows Server 2012 R2. В среде Active Directory, работающей на функциональном уровне домена Windows Server 2012, традиционные кластеризированные диски и кластеризированные общие тома могут применять шифрование на уровне томов, предоставляемое BitLocker. Каждый узел выполняет расшифровку, используя учетную запись компьютера, которая называется объектом имени кластера (cluster name object — CNO). Это делает возможной физическую защиту развертывания за пределами защищенного центра данных и помогает удовлетворять требованиям соответствия для шифрования на уровне томов.

Требования к оборудованию

Для обеспечения наилучшей защиты оборудование должно включать криптопроцессор Trusted Platform Module (TPM) версии 1.2, представляющий собой встроенный в компьютер аппаратный компонент, который обычно находится на материнской плате.

Если в системе имеется TPM 1.2 и средство BitLocker включено, система будет выполнять проверку целостности во время загрузки. Если она обнаруживает изменения в оборудовании, указывающие на то, что жесткий диск находится на другом компьютере, устройство блокируется и пребывает в таком состоянии до тех пор, пока не будет вручную разблокировано с применением ключа восстановления.

Тем не менее, на многих компьютерах TPM 1.2 отсутствует. Существуют альтернативы, которыми можно воспользоваться для шифрования дисков с помощью BitLocker.

- **Пароль.** Средство BitLocker может шифровать диск, а для его разблокирования применяется пароль.
- **Смарт-карта.** Средство BitLocker может шифровать диск, а для его разблокирования используется смарт-карта с PIN-кодом.

Вариант TPM, пароля или смарт-карты выбирается при включении BitLocker на конкретном диске. На рис. 13.30 система не имеет TPM, так что присутствуют только опции пароля и смарт-карты.

Также возможно выбрать опцию автоматического разблокирования диска при доступе из того же самого компьютера. Это требует, чтобы диск, на котором находится Windows, был также защищен посредством BitLocker. При таком использовании шифрование будет видимым только при переносе диска на другой компьютер (или в случае изменения оборудования на текущем компьютере, достаточного для того, чтобы средство BitLocker посчитало, что диск был перемещен).

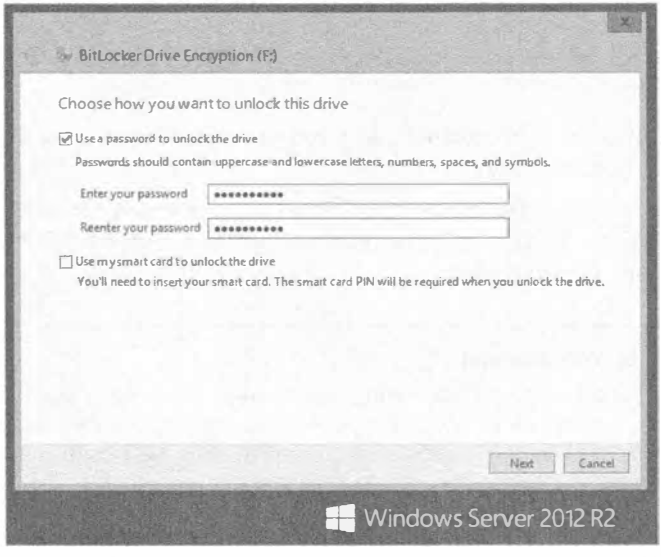


Рис. 13.30. Разблокирование диска, защищенного с помощью BitLocker

Средство BitLocker может быть внедрено в разделах без шифрования всего диска. Например, если система имеет единственный физический жесткий диск, разбитый на два раздела (C и D), вы можете заблокировать диск D с помощью BitLocker, не блокируя диск C.

Ключ восстановления

Ключ восстановления BitLocker может применяться, если TPM обнаруживает, что диск был перемещен на другой компьютер. Как только криптопроцессор TPM определяет факт переноса (либо изменения оборудования), он блокирует диск до тех пор, пока он не будет разблокирован с использованием ключа восстановления.

BitLocker поддерживает механизм восстановления на случай, если пароль забыл или смарт-карты утеряна. В Microsoft рекомендуют сохранить ключ восстановления в Active Directory Domain Services, записать его в файл, распечатать его или хранить в надежном месте. Мастер BitLocker предоставляет три опции:

- сохранить ключ восстановления на флэш-накопитель USB;
- сохранить ключ восстановления в файл;
- распечатать ключ восстановления.

Этот ключ должен быть защищен на уровне, сопоставимом с данными, хранящимися на диске. Другими словами, если на вашем диске имеются секретные патентованные данные, то защищайте ключ восстановления подобно тому, как защищаете эти данные.

Включение BitLocker

По умолчанию средство BitLocker не включено. Перед тем как BitLocker можно будет включить, вы должны добавить компонент BitLocker Drive Encryption (Шифрование диска BitLocker). Вспомните упражнение по добавлению ролей в начале этой главы: мы уже включили роль BitLocker. При желании освежить память можете возвратиться и просмотреть упражнение еще раз. В перечисленных ниже шагах предполагается, что в системе отсутствует TPM 1.2, а роль BitLocker уже установлена на сервере.

1. Откройте панель управления и щелкните на значке System and Security (Система и безопасность).

   В центре системы и безопасности (System and Security Center) вы должны увидеть компонент BitLocker Drive Encryption. Если он отсутствует, значит, этот компонент не был добавлен.

Поиск в панели управления

В панели управления имеется одна изящная функция, которая очень полезна, но на нее часто не обращают внимания. В правом верхнем углу окна расположено поле поиска. В нем можно вводить любой поисковый термин (такой как BitLocker или User), и в окне будут отображаться только подходящие значки. Поиск в панели управления доступен также в Windows Vista, Windows 7, Windows 8 и Windows Server 2008. Аналогичная функция поиска не помешала бы и в групповой политике.

2. Щелкните на значке BitLocker Drive Encryption (Шифрование диска BitLocker). Диалоговое окно будет выглядеть примерно так, как показано на рис. 13.31.

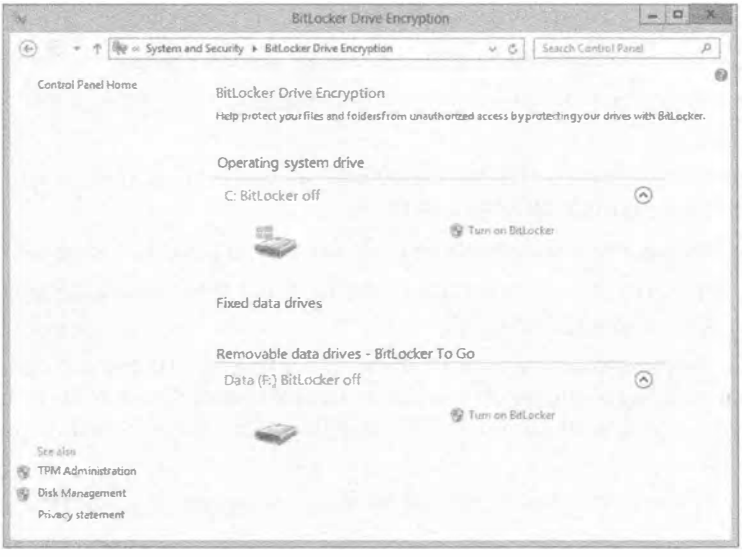


Рис. 13.31. Включение шифрования диска BitLocker

3. Щелкните на ссылке Turn on BitLocker (Включить BitLocker).

   Откроется начальный экран BitLocker Drive Encryption (Шифрование диска BitLocker), который позволяет выбрать способ разблокирования этого диска. При отсутствии TPM доступны две опции: Use a password to unlock the drive (Использовать пароль для снятия блокировки диска) и Use a smart card to unlock the drive (Использовать смарт-карту для снятия блокировки диска).

4. Отметьте флажок Use a password to unlock the drive и введите пароль в двух полях. В качестве альтернативы, если у вас есть смарт-карта и система поддерживает работу со смарт-картами, можете отметить флажок Use a smart card to unlock the drive.

5. Щелкните на кнопке Next (Далее).

6. Выберите Save the recovery key to a file (Сохранить ключ восстановления в файле). Укажите местоположение для файла на своем компьютере и щелкните на кнопке Save (Сохранить).

   В идеальном случае этот файл должен быть сохранен на отдельном устройстве (таком как флэш-накопитель USB). При попытке сохранить файл на том же физическом диске отобразится диалоговое окно с предупреждением, но вы можете щелкнуть в нем на кнопке Yes (Да), чтобы продолжить.

7. Щелкните на кнопке Next.

   На следующем экране можно указать объем дискового пространства, подлежащего шифрованию. Здесь можно выбрать новую опцию Encrypt disk space only (Шифровать только используемое пространство на диске).

Если вы выберете Encrypt entire drive (Шифровать весь диск), то в зависимости от размера диска процесс может занять продолжительное время. Мы заметили, что шифрование 1 Гбайт требует около 30 секунд, так что при объеме диска 500 Гбайт у вас появится возможность сделать перерыв.

8. Оставьте все без изменений и щелкните на кнопке Next.

   На следующем экране понадобится подтвердить свои намерения зашифровать этот диск.

9. По готовности щелкните на кнопке Start encrypting (Начать шифрование). Отобразится индикатор хода работ.

10. Дождитесь завершения процесса и щелкните на кнопке Close (Закрыть).

    После перезагрузки системы диск оказывается помеченным как зашифрованный и не будет доступен.

11. Вы можете разблокировать этот диск, щелкнув на его значке правой кнопкой мыши и выбрав в контекстном меню пункт Unlock Drive (Снять блокировку с диска), как показано на рис. 13.32. Введите указанный ранее пароль и разблокируйте диск.

    После разблокирования диска вы можете обращаться к данным обычным образом.

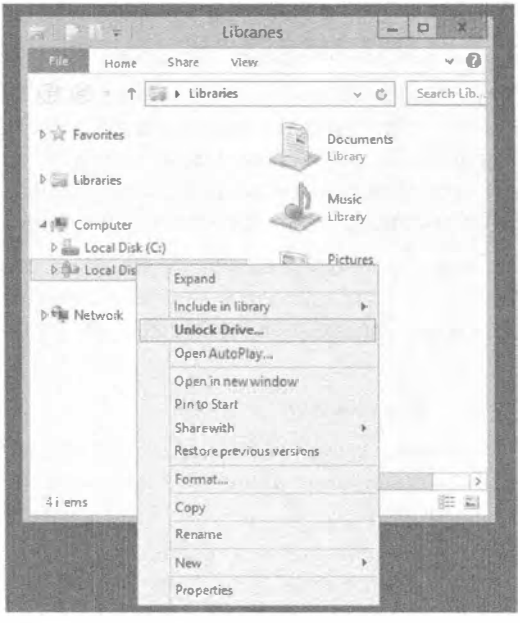


Рис. 13.32. Снятие блокировки с зашифрованного диска

12. Щелкните правой кнопкой мыши на значке диска и выберите в контекстном меню пункт Manage BitLocker (Управлять BitLocker).

    Это предоставит возможность изменить пароль и манипулировать другими опциями для диска.

BitLocker To Go

BitLocker To Go — великолепная возможность, которой легко пользоваться после того, как на сервер добавлен соответствующий компонент.

1. Откройте окно BitLocker Drive Encryption через панель управления.
2. Вставьте флэш-накопитель USB и щелкните для него на ссылке Turn On BitLocker (Включить BitLocker).
3. Введите пароль, сохраните ключ восстановления и затем щелкните на кнопке Start encrypting (Начать шифрование).

Если флэш-накопитель переносится на другой компьютер, он перестает читаться.

Однако вы можете вставить флэш-накопитель в другой компьютер и ввести пароль, когда он будет запрошен, после чего вы получите доступ ко всем своим данным. Хотя это лучше всего работает в Windows 8 или Windows Server 2012 R2, вы можете получить доступ к своим данным и на других системах, таких как Windows 7, запустив программу `BitLockerToGo.exe` для расшифровки и копирования данных.

Многие организации предпринимают дополнительные меры, чтобы защитить "данные в состоянии покоя", и BitLocker To Go вполне удовлетворяет таким потребностям. Мы ожидаем широкого применения этого средства в ближайшем будущем.

Использование автономных файлов / кеширования на стороне клиента

При наличии в вашей сетевой среде пользователей с ноутбуками вам наверняка понравится средство Offline Files (Автономные файлы) или Client-Side Caching (Кеширование на стороне клиента); в Microsoft применяют эти названия взаимозаменяемо. На самом деле оно будет привлекательным практически для всех, кто использует сеть. Средство Offline Files предоставляет три основных преимущества: оно позволяет сети выглядеть более быстрой для своих пользователей, сглаживает "затормаживания" сети и упрощает задачу синхронизации файлов на ноутбуках с файлами на сервере.

Как работает Offline Files

Средство Offline Files включено на общих ресурсах, расположенных на сервере. Оно автоматически кеширует файлы, к которым производится доступ, сохраняя кешированные копии в папке на локальном жестком диске (папка вполне ожидаемо называется `Offline Files`). Эти кешированные копии затем применяются для ускорения доступа в сеть (или кажущегося доступа в сеть), поскольку последующий доступ к файлу может быть обработан с использованием кешированной копии, а не путем передачи его содержимого через сеть.

Это очень удобно для пользователей, находящихся в пути. Средство Offline Files позволяет кешированным копиям файлов действовать в качестве временной замены сети, если та отсутствует (что нередко бывает у мобильных пользователей) или работает крайне неустойчиво.

В Offline Files применяется механизм кеширования со сквозной записью; когда вы записываете файл, он передается в целевое местоположение внутри сети для сохранения, а также кешируется на локальном жестком диске. И когда вы хотите об-

ратиться к файлу, кешированному в Offline Files, средство Offline Files *предпочтет* предоставить вам кешированную копию (что быстрее), но сначала проверит, не изменился ли этот файл на сервере, сравнивая даты, время и размеры его копий на сервере и в кеше. Если они остались одинаковыми, средство Offline Files без проблем выдаст файл из кеша; в противном случае Offline Files извлечет копию файла из сети, обеспечив актуальность данных.

Средство Offline Files увеличивает шансы наличия в кеше новейших копий файлов, выполняя фоновую синхронизацию несколькими способами, которые определяются пользователем. Эта синхронизация почти незаметна для пользователя, который просто работает с общим ресурсом по сети.

Нам нравится средство Offline Files по следующим причинам.

- **Средство Always Offline Mode (Всегда автономный режим).** Это новое настраиваемое средство в Windows 8 и Windows Server 2012 предоставляет пользователям возможность более быстрого доступа к файлам и меньшего расходования полосы пропускания за счет работы всегда в автономном режиме. В отличие от предшествующих редакций, в которых осуществлялось переключение из онлайнового режима в автономный в зависимости от наличия соединения с сетью, средство Always Offline Mode обеспечивает пребывание в автономном режиме даже при высокоскоростном подключении к сети. Операционная система Windows будет автоматически обновлять файлы путем их синхронизации с кешем Offline Files. Это новое средство способствует более высокой производительности дисков. Средство Always Offline Mode требует, чтобы компьютер был присоединен к домену и установленного компонента Group Policy Management (Управление групповой политикой).
- **Более быстрый доступ.** Из-за того, что часто используемые кешированные файлы будут располагаться на локальном жестком диске в папке `Offline Files`, вы немедленно заметите увеличение скорости реакции сети. Открытие файла, который выглядит как находящийся в сети, но в действительности хранится в папке на локальном диске, дает очевидные и значительные улучшения времени отклика, поскольку требуется лишь небольшая активность со стороны сети либо она вовсе отсутствует.
- **Сокращенный сетевой трафик.** Так как кешированные файлы не нуждаются в повторной передаче по локальной сети, сетевой трафик сокращается. Наличие часто используемых файлов в локальной папке кеша также решает проблему, когда необходим файл из сервера, а доступ в сеть отсутствует. Если вы пытаетесь обратиться к файлу на сервере, который не отвечает (или вы физически не подключены к сети), средство Offline Files перейдет в "автономный" режим. В этом режиме Offline Files просматривает кеш Offline Files и если находит в нем копию требуемого файла, то предоставляет ее вам, как будто бы сервер функционирует и соединен с рабочей станцией.
- **Автоматическая синхронизация.** Если вам когда-либо приходилось находиться в командировке, то вы знаете две наихудших вещи, которые могут произойти при поездке с ноутбуком: когда внезапно обнаруживается, что вы забыли один или два важных файла, или досаждают переживания по поводу того, что по возвращении нужно не забыть скопировать измененные вами файлы об-

ратно на сетевые серверы. Средство Offline Files значительно уменьшает шанс возникновения первой из двух проблем, потому что можно сконфигурировать автоматическое копирование часто используемых файлов в локальную папку кеша сети. Автоматизация процесса синхронизации ноутбука с серверами существенно снижает объем работ при выполнении второй задачи.

BranchCache

Технология BranchCache предназначена для оптимизации доступности данных в офисах филиалов, которые подключаются через медленные каналы WAN. Средство BranchCache, когда оно включено, позволяет данным кешироваться на компьютерах в офисе филиала и применяться другими компьютерами в этом офисе.

Предположим, что компания имеет головной офис, находящийся в Колорадо-Спрингс, и офис филиала, расположенный в Тампе и соединенный медленным каналом связи. Когда пользователям из Тампы необходим доступ к данным, открытым на сервере в Колорадо-Спрингс, им приходится подключаться через канал WAN, даже если они просто открыли и сразу же закрыли файл.

Благодаря BranchCache, файлы могут кешироваться на каком-то компьютере в удаленном офисе после первого обращения к ним. Пользователи, которым нужен файл, впоследствии могут получать доступ к его локально кешированной копии. BranchCache по-прежнему проверяет актуальность кешированной версии файла, но короткая проверка метки времени по каналу связи происходит намного быстрее, чем повторная загрузка всего содержимого файла.

Средство BranchCache поддерживает два режима.

- **Режим размещенного кеша (Hosted Cache).** Данные размещаются на одном или большем числе серверов в удаленном офисе с установленной операционной системой Windows Server 2008 R2 или более новой версии, такой как Windows Server 2012 R2.
- **Режим распределенного кеша (Distributed Cache).** Данные размещаются на компьютерах в офисе филиала. Необходимость в сервере отсутствует, но данные могут кешироваться только на компьютерах с Windows 7 и Windows 8. Более старые версии клиентских операционных систем для размещения кеша непригодны.

Средство BranchCache поддерживается на серверах Windows Server 2008 R2, Windows Server 2012 и Windows Server 2012 R2, а также на клиентах Windows Vista, Windows 7 и Windows 8. Включить BranchCache на серверах, предшествующих Windows Server 2008 R2, или на клиентах с версией ОС, более ранней, чем Windows Vista, не удастся. В режиме Distributed Cache данные будут кешироваться только на компьютерах Windows 7 и Windows 8, но компьютеры с Windows Vista по-прежнему будут иметь доступ к данным, кешированным с помощью BranchCache, несмотря на то, что машины с Windows Vista не могут выступать в качестве хостов. Прежде чем средство BranchCache может быть включено, оно должно быть добавлено как служба роли внутри роли File and Storage Services.

В групповой политике (Group Policy) предусмотрено несколько настроек, которые можно использовать для включения и управления BranchCache. Эти настройки находятся в узле Computer Configuration\Policies\Administrative Templates\Network\BranchCache (Конфигурация компьютера \ Политики \ Административные шаблоны \ Сеть \ BranchCache) групповой политики.

Включение средства Offline Files на сервере

Средство Offline Files включается на сервере относительно легко. Доступны два способа включения кеширования общего ресурса. Это можно сделать на экране Other Settings (Другие настройки) мастера создания общего ресурса (New Share Wizard) при создании нового общего ресурса, а если общий ресурс уже создан, то можно изменить его свойства.

1. Запустите диспетчер серверов и перейдите на вкладку Shares (Общие ресурсы) для роли File and Storage Services, где вы увидите все общие ресурсы, которые в настоящее время открыты в сети.
2. Щелкните правой кнопкой мыши на любом общем ресурсе и выберите в контекстном меню пункт Properties (Свойства).
3. Щелкните на кнопке Settings (Настройки) и в открывшемся диалоговом окне перейдите на вкладку Caching (Кеширование).

Диалоговое окно будет выглядеть подобно показанному на рис. 13.33. Здесь вы можете включить кеширование общего ресурса и средство BranchCache, если оно еще не было включено.

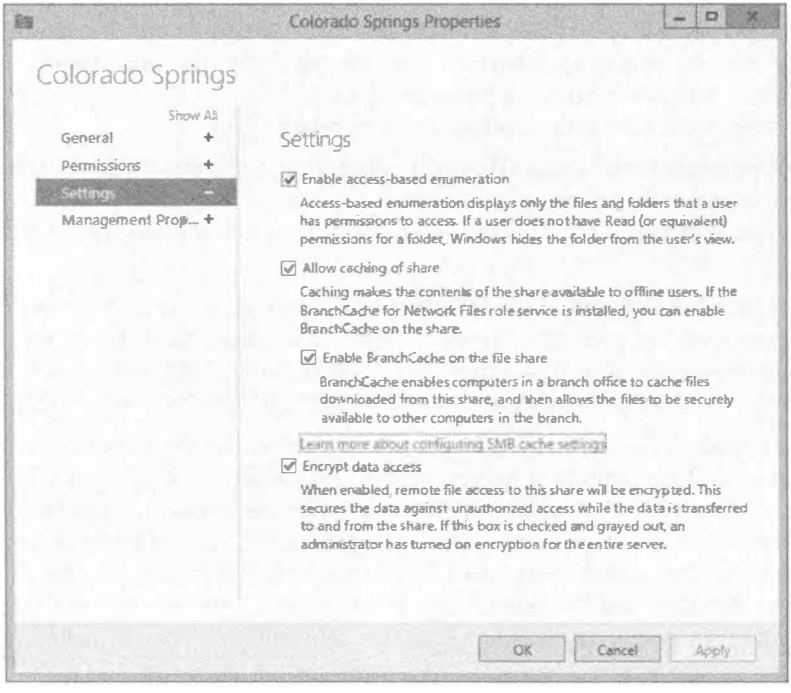


Рис. 13.33. Просмотр настроек Offline Files

Хотя в этом разделе объяснялось средство Offline Files, и было показано, каким образом его конфигурировать на сервере, его необходимо сконфигурировать также на стороне клиента. В разных клиентских операционных системах (Windows XP, Windows Vista, Windows 7 и Windows 8) это делается по-разному.

Ниже приведены ссылки, по которым доступны описания для различных клиентов.

Windows XP:

```
http://support.microsoft.com/kb/307853
```

Windows Vista:

```
http://windows.microsoft.com/en-US/windows-vista/Working-with-network-files-when-you-are-offline
```

Windows 7:

```
http://www.windows7update.com/Windows7-Offline-Files.html
```

Window 8:

```
http://technet.microsoft.com/en-us/library/hh848267
```

Резюме

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?

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?

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?

Глава 14

Создание и управление общими папками

Возможно, вы еще помните те времена, когда данные, которыми вы хотели поделиться с коллегами, помещались на флоппи-диски. Потребность в общем доступе к файлам и папкам является одной из самых важных причин, по которым были разработаны серверные технологии. В операционной системе Microsoft Windows Server 2012 R2 были предложены новые и усовершенствованные пути организации общего доступа к файлам с помощью служб, подобных NFS (Network File System — сетевая файловая система), которые предоставляют решение общего доступа к файлам для предприятий, располагающих смесью разнообразных операционных систем. Благодаря NFS, вы можете открывать общий доступ к файлам не только для других серверов Windows, но также и для клиентов Unix, Linux и Mac OS, если они присутствуют в вашей организации. В этой главе мы погрузимся в NFS и посмотрим, что появилось нового, а что изменилось в текущей редакции сервера.

В Windows Server 2012 R2 также модернизированы технологии распределенной файловой системы (Distributed File System — DFS), которые продолжают предлагать дружественную к WAN репликацию для упрощения доступа к географически разбросанным файлам и папкам. Общий доступ к файлам и папкам по сети можно предоставлять на основе их группирования. Эта функция упрощает сложный процесс, который был утомительным и затратным по времени в ранних выпусках Windows Server.

В настоящей главе мы поможем вам разобраться в DFS и затем в NFS, предоставив пошаговые руководства по применению этой захватывающей функциональности. Вы узнаете, что собой представляют указанные функции, как они работают и каким образом извлечь из них максимальную пользу.

В этой главе вы изучите следующие темы:

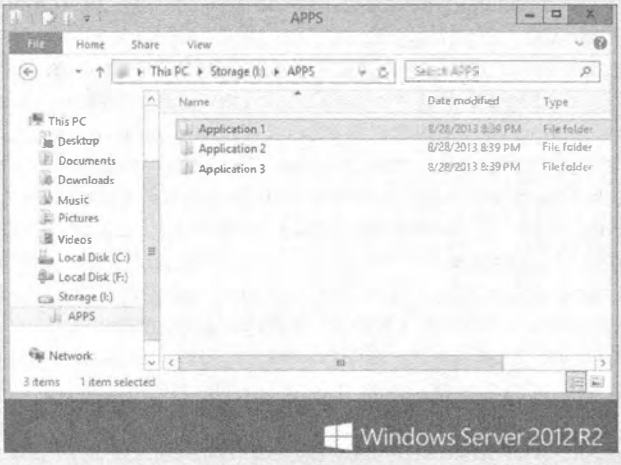
- добавление на сервер роли File and Storage Services (Службы файлов и хранилища);
- добавление общей папки, используя NFS;
- добавление корня DFS.

Создание общих папок

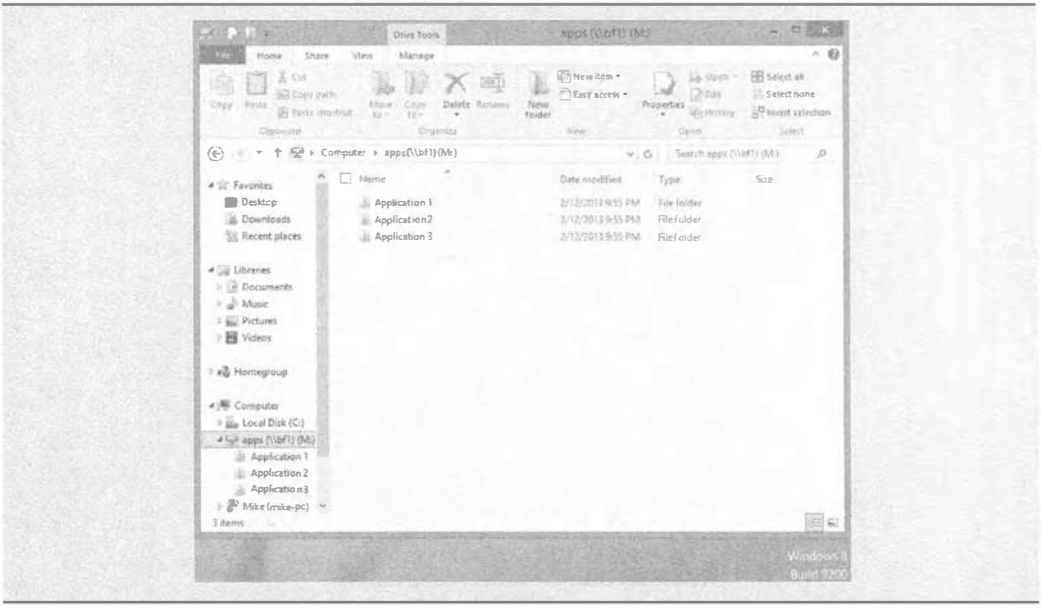
Чтобы иметь возможность создать общую папку, вы должны располагать подходящими правами. Для этого вы должны быть либо администратором, либо опытным пользователем. Создавать общие ресурсы можно двумя способами: либо в проводнике Windows, находясь на сервере, либо в диспетчере серверов на сервере или дистанционно.

Некоторые основы общего доступа к файлам

Одним из основных компонентов любого сервера является возможность общего доступа к файлам. В действительности возможность организации общего доступа к файловым и принтерным ресурсам поддерживается службой Server (Сервер), которая входит в состав каждого члена семейства Windows NT, включая Windows Server 2012 R2. Но что именно она собой представляет и почему настолько важна? По умолчанию один лишь факт наличия функционирующего сервера совершенно не означает доступность каких-либо ресурсов пользователям. Чтобы пользователи на самом деле смогли обращаться к ресурсам на сервере, вы должны открыть общий доступ к этим ресурсам. Предположим, что у вас на локальном диске `I` имеется папка `APPS` с тремя подпапками приложений, как показано ниже:



Когда вы открываете общий доступ к этой папке из сети под именем `APPS`, вы позволяете клиентам отображать на вашу папку `I:\APPS` новые буквы дисков на своих машинах. За счет отображения диска создается виртуальный указатель непосредственно на место подключения. Если вы отобразите диск `M` клиента на общий ресурс `APPS` сервера, то диск `M` будет выглядеть идентично папке `I:\APPS` сервера, что видно на следующем экранном снимке:



Создание общих ресурсов в проводнике Windows

Давайте возвратимся к открытию общего доступа к папке `APPS`. Если вы находитесь непосредственно на сервере, то для создания общего ресурса и управления всеми его свойствами можете применять проводник Windows. Итак, вы хотите сделать папку `I:\APPS` доступной в сети под именем `APPS`.

В окне проводника Windows щелкните правой кнопкой мыши на папке `APPS` и выберите в контекстном меню пункт Sharing and Security (Общий доступ и безопасность). Откроется диалоговое окно свойств для папки `APPS`. Перейдите на вкладку Sharing (Общий доступ). Чтобы открыть общий доступ к папке, можно щелкнуть на кнопке Share (Общий доступ) или на кнопке Advanced Sharing (Расширенная настройка общего доступа), как показано на рис. 14.1.

1. Итак, есть две кнопки для открытия общего доступа: Share и Advanced Sharing. Щелкните на кнопке Advanced Sharing, чтобы воспользоваться дополнительными возможностями, предлагаемыми мастером. Первым делом понадобится отметить флажок Share this folder (Открыть общий доступ к этой папке).
2. После открытия общего доступа ресурсу необходимо назначить имя. Это очень важный шаг, поскольку под данным именем пользователи будут подключаться к общему ресурсу. Укажите имя **APPS**.
3. После именования общего ресурса станет доступной область Comments (Примечание), позволяя предоставить описание общего ресурса. Здесь также можно установить лимит пользователей, что поможет управлять доступом к общему ресурсу. Введите описание общего ресурса, укажите реалистичное число для максимального количества одновременных подключений и затем щелкните на кнопке Permissions (Разрешения), чтобы открыть следующее диалоговое окно.

Рис. 14.1. Свойства общего ресурса `APPS`

4. Группе `Everyone` (Все) автоматически предоставляется разрешение Read (Чтение) для нового общего ресурса. Щелкните на кнопке Add (Добавить); откроется диалоговое окно поиска, в котором можно разрешить доступ к общему ресурсу другим пользователям и группам. Всегда сначала добавляйте пользователя или группу административного уровня и затем выдавайте этому объекту разрешение Full Control (Полный доступ). Это гарантирует, что администратор в любой момент сможет управлять и поддерживать общий ресурс. Рекомендуется предоставлять разрешение Full Control только администраторам. Вы же не хотите, чтобы кто угодно мог назначать и отзывать разрешения по собственному желанию. Только вообразите, насколько быстро все пойдет наперекосяк, когда пользователь удалит разрешения для группы администраторов и возьмет под контроль ваш общий ресурс! Поскольку это общий ресурс `APPS`, который должны читать все, оставьте группу `Everyone` с разрешением Read. Для продолжения щелкните на кнопках Apply (Применить) и OK.
5. Последней опцией в окне Advanced Sharing (Расширенная настройка общего доступа) является кнопка Caching (Кеширование). Она позволяет выбрать дополнительные настройки автономного режима, например, включить BranchCache — великолепное средство, которое обсуждалось в предыдущей главе. Просмотрите доступные варианты, сделайте необходимый выбор и щелкните на кнопке OK. Для получения дополнительной информации о кешировании можете щелкнуть на гиперссылке Configure Offline Availability for a Shared Folder (Настройка доступа к общей папке вне сети) в нижней части диалогового окна.
6. Просмотрите все выбранные настройки общего доступа к папке и затем щелкните на кнопках Apply и OK, чтобы завершить открытие общего доступа. Общий ресурс `APPS` стал доступным через сеть.

Теперь, когда папка APPS открыта для общего доступа пользователям, вы можете перейти к этому общему ресурсу в проводнике Windows. Существует множество путей для просмотра общих дисков и папок. В следующем разделе мы покажем, как просматривать общие ресурсы с помощью консоли Computer Management (Управление компьютером).

Установка лимитов пользователей

Вы можете сконфигурировать количество пользователей, которые могут одновременно подключаться к общему ресурсу, путем настройки опции User limit (Лимит пользователей) в диалоговом окне свойств общего ресурса. Если приложение внутри общего ресурса лицензировано для 100 параллельных пользователей, вы можете сконфигурировать общий ресурс на сервере для поддержки этого лимита, несмотря на то, что в сети может быть 200 пользователей. По мере того, как пользователи подключаются к общему ресурсу, их число приближается к лимиту пользователей. При отключении от общего ресурса их количество уменьшается. Это означает возможность установки лимита для общего ресурса, который не превышает существующие ограничения лицензирования, что поможет сохранить соответствие лицензионным соглашениям.

Однако будьте осторожны в отношении лицензирования. Не у всех приложений имеется режим параллельных лицензий, хотя может существовать режим клиентских лицензий. В режиме клиентских лицензий производитель не заботится о том, сколько пользователей получают доступ к приложению в любой момент времени; играет роль только количество людей, в целом установивших приложение. В таких случаях лимит пользователей никак вас не защитит.

Наконец, вы должны принять во внимание, каким образом пользователи подключаются к общему ресурсу для взаимодействия с приложениями, прежде чем ограничивать их на базе параллелизма. Если все пользователи подключаются к общему ресурсу при входе в систему и не отключаются вплоть до выхода из системы, то лимит параллелизма может в первую очередь расходоваться на вошедших в систему пользователей, достигая в итоге предела в 100 человек, хотя в действительности работать с приложением могла только небольшая группа пользователей. Если подключения осуществляются только при использовании приложения, то лимит пользователей будет работать довольно хорошо.

Удаленное создание общих ресурсов с помощью консоли управления компьютером

В Windows Server 2012 R2 были внесены замечательные усовершенствования в способ применения диспетчера серверов. Из единственного сервера управления можно создавать и управлять общими ресурсами на множестве серверов, при кладывая лишь небольшие усилия. До тех пор, пока удаленный сервер находится в онлайновом режиме и доступен через сеть, нет никаких причин входить в его систему непосредственно на месте. Давайте посмотрим, как использовать новый интерфейс диспетчера серверов для подключения к удаленному серверу и создания на нем нового общего ресурса.

1. Запустите диспетчер серверов, щелкните на элементе All Servers (Все серверы) и щелкните правой кнопкой мыши на сервере, которым необходимо управлять дистанционным образом.

В контекстном меню отобразится новый набор пунктов, одним из которых является Computer Management (Управление компьютером), как показано на рис. 14.2.

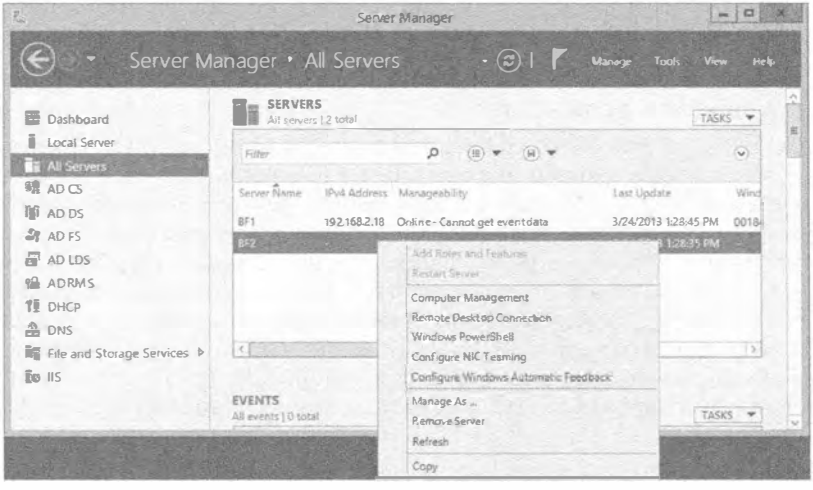


Рис. 14.2. Применение диспетчера серверов для подключения к другому серверу

Инструмент Computer Management

Консоль Computer Management (Управление компьютером) находится в программной группе Administrative Tools (Администрирование). С помощью этого инструмента вы можете, помимо прочего, создавать и управлять общими ресурсами локально или же дистанционно. Если в проводнике Windows щелкнуть правой кнопкой мыши на папке, которая не является локальной на вашей машине, в контекстном меню не появится пункт для открытия общего доступа. Если же вы собираетесь создать общий ресурс, используя консоль Computer Management на своей локальной машине, то для этого все готово. Чтобы управлять общим ресурсом на удаленном сервере, к этому серверу сначала необходимо подключиться.

2. Выберите пункт Computer Management, после чего диспетчер серверов автоматически подключится к удаленному серверу.
3. Выберите папку Computer Management\System Tools\Shared Folders\ Shares (Управление компьютером \ Системные инструменты \ Общие папки \ Общие ресурсы), как показано на рис. 14.3.
4. Теперь можете либо выбрать в меню Actions (Действия) пункт New Share (Новый общий ресурс),

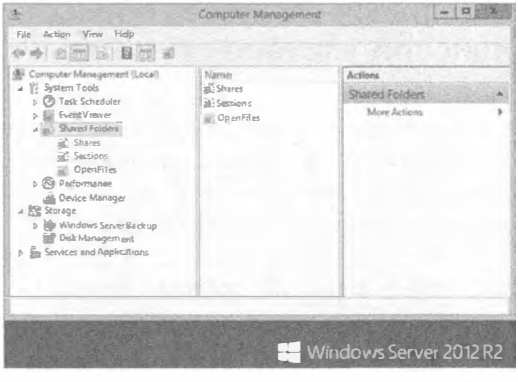


Рис. 14.3. Общие папки в консоли Computer Management

либо щелкнуть правой кнопкой мыши в окне со списком общих ресурсов и выбрать в контекстном меню пункт New Share.

5. На начальном экране мастера создания общей папки (Create A Shared Folder Wizard) щелкните на кнопке Next (Далее); появится экран, представленный на рис. 14.4. Удостоверьтесь в корректности информации в поле Computer name (Имя компьютера), чтобы общий ресурс был создан на нужном компьютере. Чтобы создать общий ресурс, вы можете просмотреть исходные диски и папки или же создать новую папку на лету, просто введя полное имя диска и папки в поле Folder path (Путь к папке).
6. Для этого примера создайте новую папку по имени **`Graphics`** и откройте к ней общий доступ как к **`I:\Graphics`**.
7. Завершив ввод пути к папке, щелкните на кнопке Next.
8. Появится экран, показанный на рис. 14.5. Введите здесь имя, которое должно быть назначено этому общему ресурсу, и его краткое описание.
9. Для продолжения щелкните на кнопке Next.

   На следующем экране (рис. 14.6) будут определяться разрешения общего доступа, для чего предоставляются четыре переключателя.

   - **All Users Have Read-Only Access (Все пользователи имеют доступ только для чтения).** Эта опция позволяет группе `Everyone` иметь доступ только для чтения к содержимому папки. Она является стандартной настройкой в Windows Server 2012 и хорошо демонстрирует повышенное внимание, уделяемое компанией Microsoft безопасности на протяжении последних нескольких лет. В предшествующих редакциях сервера по умолчанию группа `Everyone` имела полный доступ (Full Control), включая анонимных пользователей, пришедших из сети! С момента выхода версии Windows Server 2008 при создании общего ресурса вам не придется начинать с широко открытых дверей. Вы начинаете с закрытой двери и открываете ее согласно своим спецификациям, когда вам будет удобно.

Рис. 14.4. Указание местоположения в мастере Create A Shared Folder Wizard

Рис. 14.5. Назначение общему ресурсу имени и описания

- **Administrators Have Full Access; Other Users Have Read-Only Access (Администраторы имеют полный доступ; остальные пользователи имеют доступ только для чтения).** Эта опция обеспечивает пользователям возможность просмотра данных и запуска программ, но не позволяет им изменять или удалять что-либо внутри общего ресурса. Однако администраторы обладают всеми правами для управления данными.
- **Administrators Have Full Access; Other Users Have No Access (Администраторы имеют полный доступ; остальные пользователи не имеют доступа).** Эта опция позволяет пользователям делать все кроме удаления файлов или папок, изменения разрешений либо получения прав владения файлами.
- **Customize Permissions (Настроить разрешения).** Эта опция позволяет определять разрешения на основе конкретных пользователей или групп.

Сохраняйте общие ресурсы защищенными

При определении подходящих разрешений общего доступа необходимо принимать во внимание несколько очень важных аспектов, связанных с безопасностью. Разрешение Full Control должно предоставляться только администраторам, а пользователи должны иметь только те права, которые соответствуют их служебным обязанностям. Это обеспечивает организации две серьезных вещи: гарантирует, что никто кроме IT-персонала корпорации не сможет управлять, изменять или удалять разрешения общего доступа и объекты, и также ограничивает количество высокопривилегированных учетных записей в сети, которые могут стать причиной появления брешей в безопасности. Если ваши пользователи только читают и записывают в общий сетевой ресурс и одна из их учетных записей окажется скомпрометированной, то, во всяком случае, посредством этой учетной записи не удастся нанести значительный ущерб, подобный удалению целого общего ресурса.

10. После настройки разрешений для общего ресурса щелкните на кнопке Next, чтобы перейти на финальный экран мастера Create A Shared Folder Wizard, на котором отображаются результаты и предоставляется возможность запустить мастер снова для создания еще одной общей папки (рис. 14.7).

Рис. 14.6. Управление доступом к общему ресурсу в мастере Create A Shared Folder Wizard

Рис. 14.7. На финальном экране мастера показана сводка по созданному общему ресурсу

Более развитый подход предполагает применение Windows PowerShell для создания общих файловых ресурсов SMB. Преимущество командлетов SMB в том, что в Windows Server 2012 R2 они доступны по умолчанию.

1. Откройте окно Windows PowerShell из панели задач от имени учетной записи администратора.
2. Запустите следующую команду, чтобы создать новый общий файловый ресурс:
   ```
   PS C:\> New-SmbShare -Name ИмяОбщегоРесурса -Path C:\ЛокальнаяПапка
   ```
3. Запустите следующую команду, чтобы получить список существующих общих ресурсов, в котором будет присутствовать только что созданный ресурс:
   ```
   PS C:\> Get-SmbShare
   ```
4. Наконец, введите следующую команду, чтобы удалить только что созданный общий ресурс:
   ```
   PS C:\> Remove-SmbShare -Name ИмяОбщегоРесурса
   ```

Управление разрешениями

Разрешения общего доступа применяются, когда пользователь обращается к файлу или папке через сеть, но они не принимаются во внимание, если пользователь получает доступ к данным ресурсам локально, как это было бы при его нахождении непосредственно за компьютером либо при использовании ресурсов на терминальном сервере. В противоположность этому, разрешения NTFS применяются независимо от того, каким образом пользователь обращается к тем же ресурсам, то ли он подключается к ним дистанционно, то ли входит в них из консоли. Итак, когда доступ к файлам осуществляется локально, применяются только разрешения NTFS. При дистанционном обращении к тем же самым файлам применяется объединение разрешений общего доступа и NTFS с вычислением наиболее ограничивающего разрешения из этих двух типов. Дополнительную информацию о файловой системе NTFS можно найти в главе 13.

Создание разрешений общего доступа

Разрешения общего доступа являются, пожалуй, простейшей формой управления доступом, с которой вы будете иметь дело в Windows Server. Вспомните, что разрешения общего доступа оказывают воздействие, только когда вы пытаетесь обратиться к ресурсу через сеть. Считайте разрешения общего доступа разновидностью пропуска в охраняемое здание. Когда вы подходите к входной двери и предъявляете свое удостоверение, охранник просматривает вашу фамилию и выдает пропуск, который указывает уровень доступа к внутренним помещениям. Если на пропуске написано "доступ уровня 1", он позволит зайти в любую комнату с уровнем 1, но никуда больше. Если вы попытаетесь, оказавшись внутри, зайти в комнату с требуемым уровнем доступа 2, пропуск не сработает. Определяя разрешения общего доступа, вы безопасно управляете уровнем доступа для каждого лица у входной двери.

Однако имейте в виду, что упомянутая входная дверь — или разрешение уровня общего ресурса — это не полная картина. Разрешение уровня общего ресурса представляет только *максимальный* уровень доступа, который вы получите внутри. Если вы располагаете разрешением Read на общем ресурсе, то самое большее, что вы смо-

жете делать после дистанционного подключения к нему — это чтение. Подобным образом, разрешение Change позволит в лучшем случает вносить изменения. Если вы хотите иметь полный контроль над *всем* внутри общего ресурса, вам понадобится разрешение Full Control *на* общем ресурсе. Но поймите, что когда мы говорим о том, что разрешение общего доступа — это *максимальный* уровень доступа, который вы получите внутри общего ресурса, то имеем в виду возможность наличия дополнительного ограничения внутри за счет применения разрешений уровня файлов (или NTFS). Вы можете располагать полным доступом на общем ресурсе, но объект внутри него может иметь разрешения NTFS, которые позволяют только читать его.

Определение разрешений общего доступа

Чтобы определить разрешения общего доступа, выполните следующие действия в консоли Computer Management.

1. Щелкните правой кнопкой мыши на имени общего ресурса, который вы хотите защитить, и выберите в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом окне свойств перейдите на вкладку Share Permissions (Разрешения общего доступа).

   Вы можете попасть в это место из проводника Windows, щелкнув правой кнопкой мыши на локальной общей папке, выбрав в контекстном меню пункт Sharing and Security (Общий доступ и безопасность) и затем в открывшемся диалоговом окне шелкнув на кнопке Permissions (Разрешения). Оба метода приводят к той же самой вкладке диалогового окна, которая показана на рис. 14.8.

Рис. 14.8. Вкладка Share Permissions

Отсутствие полного доступа у группы Everyone

Обратите внимание на то, что группа Everyone по умолчанию имеет разрешение Read, что является великолепным шагом вперед в мире Windows в плане безопасности. Вплоть до версии Windows Server 2003 группа Everyone по умолчанию получала доступ Full Control. Еще одно удобное свойство в Windows Server 2012 связано с тем, что группа Everyone больше не добавляется к папке при открытии к ней общего доступа.

В этом диалоговом окне вы видите область Group or user names (Имена групп или пользователей) со списком пользователей и групп, назначенных общему ресурсу; для выбранного пользователя или группы в области, расположенной ниже, отображаются разрешения на этом открытом ресурсе. Разным пользователям и группам можно назначать разные уровни разрешений. На уровне общего доступа имеются три типа разрешений, описанные в табл. 14.1.

Таблица 14.1. Типы разрешений

Разрешение	Уровень доступа
Full Control (Полный доступ)	Группа, которой назначено это разрешение, может выполнять любые функции над всеми файлами и папками внутри общего ресурса
Change (Изменение)	Группа, которой назначено это разрешение, может читать и запускать, а также изменять и удалять файлы и папки внутри общего ресурса
Read (Чтение)	Группа, которой назначено это разрешение, может читать и запускать файлы и папки, но не модифицировать или удалять что-либо внутри общего ресурса

Пример на рис. 14.8 демонстрирует доступ Read для группы `Everyone`. Хотя вы не видите здесь учетную запись `Administrator` с какими-то специальными правами, учтите, что локальные администраторы всегда имеют доступ Full Control на общих ресурсах компьютера. Если вы хотите изменить разрешения, предоставив доступ Full Control всем сетевым администраторам, то должны добавить их группу и назначить ей эти права.

2. Щелкните на кнопке Add (Добавить), чтобы открыть диалоговое окно Select Users, Computers, Service Accounts, or Groups (Выбор пользователей, компьютеров, учетных записей служб или групп), представленное на рис. 14.9.

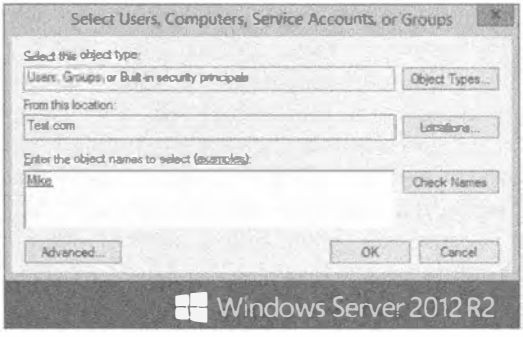


Рис. 14.9. Диалоговое окно Select Users, Computers, Service Accounts, or Groups

3. Либо введите имя пользователя или группы, подлежащей добавлению, либо щелкните на кнопке Advanced (Дополнительно), что приведет к отображению другого диалогового окна Select Users, Computers, Service Accounts, or Groups (рис. 14.10), которое позволяет производить поиск в каталоге.

   Можете либо воспользоваться функциями поиска в Active Directory на вкладке Common Queries (Общие запросы), чтобы сузить выбор, либо щелкнуть на кнопке Find Now (Найти сейчас), что обеспечит перечисление всех пользователей и групп в каталоге.

4. Найдите желаемую группу (`Domain Administrators` (Администраторы домена) в настоящем примере) и щелкните на кнопке OK и затем еще раз на кнопке OK. Произойдет возврат обратно на вкладку Share Permissions с отображением и выделением добавленной группы `Domain Administrators`.

5. Отметьте флажок Allow (Разрешить) для разрешения Full Control.

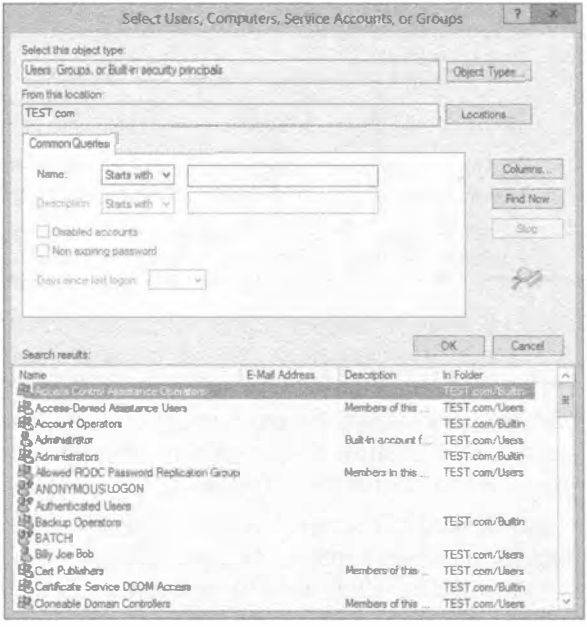


Рис. 14.10. Перечисление всех пользователей и групп по щелчку на кнопке Find Now

Опять-таки, имейте в виду, что разрешения уровня общего ресурса — это как раз то, что вы сначала фильтруете для пользователей, обращающихся к файлам через сеть. Независимо от разрешений, получаемых на уровне общего ресурса, это будет наивысший уровень разрешений, который вы можете получить для файлов и папок (как вы помните, применяется наиболее ограничивающий из них). Если вы имеете права Read на общем ресурсе, но права Full Control на файле, то общий ресурс не позволит вам делать что-то кроме чтения.

Действия Allow и Deny

Отмечая флажок Allow (Разрешить) для разрешения Full Control, назначенного группе `Domain Administrators` в предыдущем примере, вы наверняка заметили, что для каждого перечисленного разрешения предусмотрен также флажок Deny (Запретить). Разрешения общего доступа являются, наверное, простейшим набором разрешений, с которыми вы будете иметь дело, поэтому они хорошо подходят для объяснения действий Allow и Deny. Вот как они работают.

- Администратор общего ресурса, файла, учетной записи пользователя или чего-то еще может изменить разрешения на своем объекте. (На самом деле, это почти полное определение администратора.)

  Существует несколько видов разрешений — Full Control, Change или Read в случае общих ресурсов. Для любого из них администратор может отметить флажок Allow или Deny либо же решить снять отметку с *обоих* флажков, оставив пользователя без Allow или Deny на этом разрешении.

- Если пользователь не имеет разрешения (другими словами, флажки Allow и Deny не отмечены), то он не получит доступ к объекту.

- Если для разрешения отмечен флажок Allow, пользователь может применить разрешение, а если флажок Deny, то нет. Мы знаем, что это очевидно, но давайте посмотрим, как это проявляется в более сложных ситуациях.

Разрешения для файлов и каталогов

Теперь, когда вы хорошо понимаете опции разрешений уровня общих ресурсов, можно более детально рассмотреть наборы разрешений для файлов и каталогов. Эти наборы разрешений, которые обычно называют разрешениями NTFS, позволяют назначать особые разрешения папкам и файлам внутри общего ресурса. Такие дополнительные разрешения делают возможным ограничение доступа вплоть до уровней папок и файлов общего каталога.

Рекомендуется содержать в актуальном состоянии документацию по разрешениям, которыми вы управляете внутри общего ресурса. Всякий раз, когда вы вносите изменения в разрешения для файлов и папок, фиксируйте эти изменения в документации для будущей ссылки и для использования в качестве руководства при устранении проблем с разрешениями, которые возникают в среде. Особые обстоятельства могут потребовать блокировки папок и файлов с ограничением работы с ними только определенными группами доступа или пользователями. Попытка удержать в памяти все особые разрешения на папках и файлах в крупной среде может превратиться в настоящий кошмар. Качественная и ясная документация является настоятельной необходимостью, особенно в случае утери наборов настроенных, не унаследованных разрешений, примененных к папкам и файлам, которые должны быть восстановлены из-за повреждения или удаления. Документируйте абсолютно все.

Типы разрешений

Прежде чем назначать разрешения файлам и папкам, вы должны хорошо разобраться в том, что собой представляют эти разрешения и как они работают. Имеются два разных уровня разрешений.

Чтобы увидеть высший уровень, перейдите в любую папку NTFS, щелкните на ее имени правой кнопкой мыши, выберите в контекстном меню пункт Properties (Свойства) и в открывшемся диалоговом окне свойств папки щелкните на вкладке Security (Безопасность). Вкладка Security будет похожа на показанную на рис. 14.11.

Разрешения, которые вы видите на рис. 14.11, фактически образованы из разрешений более низкого уровня. Например, высокоуровневое разрешение List Folder Contents (Список содержимого папки) заключает в себе пять разрешений более низкого уровня: Traverse Folder/Execute File (Траверс папки / Выполнение файла),

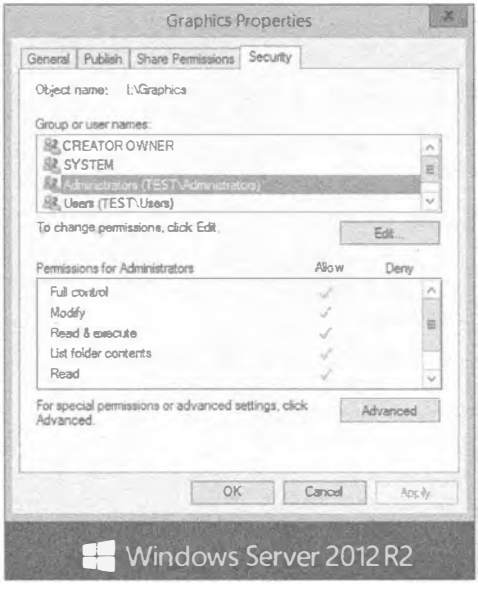


Рис. 14.11. Высокоуровневые разрешения NTFS

List Folder/Read Data (Список папки / Чтение данных), Read Attributes (Чтение атрибутов), Read Extended Attributes (Чтение расширенных атрибутов) и Read Permissions (Чтение разрешений). Можете думать о них, как о "молекулярных" и "атомарных" разрешениях. Существует 13 атомарных разрешений для NTFS. (Другие виды объектов Active Directory, такие как организационные единицы, *могут* иметь дочерние объекты, поскольку внутри организационной единицы допускается создавать пользователей и другие организационные единицы.) Все типы объектов AD совместно используют один и тот же набор атомарных разрешений, даже если они не имеют к ним никакого отношения — попробуйте предоставить кому-то возможность создания дочерних объектов для объекта групповой политики; польза от этого будет примерно такой же, как поручение работнику кирпичного завода возможности установки половой принадлежности кирпичей.

В табл. 14.2 показано, как группы атомарных разрешений в левом столбце образуют молекулярные разрешения.

Таблица 14.2. Атомарные и молекулярные разрешения

Атомарное разрешение	Write (Запись)	Read (Чтение)	List Folder Contents (Список содержимого папки)	Read & Execute (Чтение и выполнение)	Modify (Изменение)	Full Control (Полный доступ)
Traverse Folder/ Execute File (Траверс папки / Выполнение файла)			X	X	X	X
List Folder/Read Data (Список папки / Чтение данных)		X	X	X	X	X
Read Attributes (Чтение атрибутов)		X	X	X	X	X
Read Extended Attributes (Чтение расширенных атрибутов)		X	X	X	X	X
Create Files/Write Data (Создание файлов / Запись данных)	X				X	X
Create Folders/ Append Data (Создание папок / Добавление данных)	X				X	X
Write Attributes (Запись атрибутов)	X				X	X
Write Extended Attributes (Запись расширенных атрибутов)	X				X	X

Окончание табл. 14.2

Атомарное разрешение	Write (Запись)	Read (Чтение)	List Folder Contents (Список содержимого папки)	Read & Execute (Чтение и выполнение)	Modify (Изменение)	Full Control (Полный доступ)
Delete Subfolders and Files (Удаление подпапок и файлов)						X
Delete (Удаление)					X	X
Read Permissions (Чтение разрешений)	X	X	X	X	X	X
Change Permissions (Изменение разрешений)						X
Take Ownership (Получение права владения)						X

Атомарные разрешения

Мы начнем с атомарного уровня. Такие разрешения являются строительными блоками для формирования разрешений, о которых мы обычно говорим — Read, Modify и Full Control. Возможно, вы никогда не увидите атомарные разрешения, и тем более не будете ссылаться на них как на самих по себе.

- **Traverse Folder/Execute File (Траверс папки / Выполнение файла).** Разрешение Traverse Folder позволяет обойти все блокировки на более высоких уровнях и по существу обеспечить себе права уровня 4. Подобно Execute File, это полезное разрешение, однако оно ничего не делает в отношении файлов. Вот что происходит: когда файловая система NTFS проверяет разрешение, она извлекает 13 битов. При просмотре первого бита она выясняет, это файл или папка. Если объект является файлом, то первый бит интерпретируется как разрешение Execute File. Если же это папка, то первый бит трактуется как разрешение Traverse Folder. Вы увидите аналогичное поведение, хотя и в менее экстремальной форме, в ряде других разрешений.
- **List Folder/Read Data (Список папки / Чтение данных).** Разрешение List Folder позволяет просматривать имена файлов и подпапок внутри папки. Разрешение Read Data дает возможность просматривать содержимое файла. Это атомарное право является основным компонентом разрешения Read.

Подумайте о разделении между указанными двумя атомарными разрешениями. Действительно ли между ними есть много отличий? Да, но вероятно это ненадолго. Помните те дни, когда мы называли все файлами и каталогами? Теперь обычными стали термины файл и *папка*. Сейчас мы начинаем привыкать к еще одному термину, вступившему в игру: *объект*. Внутри файловой системы на машине объектами является все — и файлы, и папки. Это атомарное разрешение можно было бы перефразировать как *чтение объекта*. Независимо от того, к чему оно применяется — к файлу или к папке, — оно дает право исследовать содержимое объекта.

- **Read Attributes (Чтение атрибутов).** Базовые атрибуты — это свойства файла, такие как Read-Only (Только чтение), Hidden (Скрытый), System (Системный) и Archive (Архивный). Атомарное разрешение Read Attributes позволяет просматривать такие атрибуты.
- **Read Extended Attributes (Чтение расширенных атрибутов).** Определенные программы поддерживают для своих типов файлов дополнительные атрибуты. Например, если в вашей системе установлена программа Microsoft Word, и вы просмотрите атрибуты файла DOC, то увидите все виды атрибутов: Author (Автор), Subject (Тема), Title (Название) и т.д. Они называются расширенными атрибутами и варьируются от программы к программе. Атомарное разрешение Read Extended Attributes позволяет просматривать эти атрибуты.
- **Create Files/Write Data (Создание файлов / Запись данных).** Атомарное разрешение Create Files позволяет помешать новые файлы в папку. Разрешение Write Data дает возможность перезаписывать существующие данные внутри файла. Это атомарное разрешение не позволяет добавлять данные в существующий файл.
- **Create Folders/Append Data (Создание папок / Добавление данных).** Разрешение Create Folders дает возможность создавать подпапки внутри папок. Разрешение Append Data позволяет добавлять данные в конец существующего файла, но не изменять данные внутри этого файла.
- **Write Attributes (Запись атрибутов).** Это разрешение позволяет изменять базовые атрибуты файла.
- **Write Extended Attributes (Запись расширенных атрибутов).** Это разрешение позволяет изменять расширенные атрибуты файла.
- **Delete Subfolders and Files (Удаление подпапок и файлов).** Это довольно странное разрешение. Только подумайте: располагая этим разрешением, вы можете удалять подпапки и файлы, *даже если не имеете разрешения Delete на этих подпапках и файлах*. Как такое могло стать возможным? Если, забежав вперед, вы почитаете о следующем атомарном разрешении, Delete, то увидите, что оно позволяет удалять файл или папку. В чем разница? Представляйте ситуацию следующим образом: если вы находитесь в файле или папке, то разрешение Delete позволяет удалить этот файл или папку. Но предположим, что вы находитесь в папке и хотите удалить ее *содержимое*. Атомарное разрешение Delete Subfolders and Files дает вам такое право. Разница между Delete и Delete Subfolders and Files весьма расплывчата. Одно из них позволяет удалить конкретный объект, а другое — удалить *содержимое* этого объекта. Если вы располагаете правом удаления содержимого папки, то не хотите терять это право только потому, что один объект внутри папки не желает выдавать вам разрешение. В конце концов, это ваша папка, и вы вольны делать с ней все, что хотите.
- **Delete (Удаление).** На этот раз все просто и понятно. Разрешение Delete позволяет удалить объект. Или все не так просто и понятно? Если вы имеете только атомарное разрешение Delete на удаление папки, но не атомарное разрешение Delete Subfolders and Files на удаление подпапок и файлов, и если к одному файлу внутри папки доступ отсутствует, то сможете ли вы удалить эту папку? Нет. Удалить папку не удастся до тех пор, пока она не будет пустой, а это значит, что вам потребуется удалить упомянутый файл. Но вы не можете уда-

лить этот файл, не имея либо прав Delete для самого файла, либо прав Delete Subfolders and Files для родительской папки данного файла.

- **Read Permissions (Чтение разрешений).** Атомарное разрешение Read Permissions позволяет просматривать все разрешения NTFS, ассоциированные с файлом или папкой, но не изменять их.
- **Change Permissions (Изменение разрешений).** Это атомарное разрешение позволяет изменять разрешения, назначенные файлу или папке.
- **Take Ownership (Получение права владения).** Мы поговорим более подробно о том, что представляет собой право владения и что оно делает, позже в главе, но это атомарное разрешение позволяет получить права владения файлом. Будучи владельцем, вы имеете неотъемлемое право изменять разрешения. По умолчанию администраторы всегда могут получать права владения каким-либо файлом или папкой.

Молекулярные разрешения

Глубокое понимание работы атомарных разрешений, а также понимание того, как они образуют молекулярные разрешения (см. табл. 14.2), обеспечивает исключительное осознание сути и функционирования этих молекулярных разрешений. В настоящем разделе мы постараемся лучше прояснить объединение атомарных разрешений, но во время чтения вам придется периодически возвращаться к табл. 14.2. Приведенная здесь информация сформирует прочную основу, которая поможет управлять разрешениями в будущем.

- **Read (Чтение).** Разрешение Read является наиболее базовыми правами. Оно позволяет просматривать содержимое, разрешения и атрибуты, ассоциированные с объектом. Если объект представляет собой файл, вы можете просматривать файл, что включает возможность запуска этого файла, если он оказывается исполняемой программой. Если объект является папкой, разрешение Read позволяет просматривать ее содержимое.

  А теперь рассмотрим сложную часть, касающуюся чтения папки. Предположим, что у вас имеется папка, которой вы назначили разрешение Read. Эта папка содержит подпапку, к которой вы запретили любой доступ, в том числе и чтение. Логично было бы предположить, что вы сможете вообще увидеть эту подпапку. Однако подпапка, прежде чем вы обратитесь к ее собственным атрибутам, является *частью* исходной папки. Поскольку вы можете читать содержимое исходной папки, то сможете увидеть, что подпапка существует. Если же вы попытаетесь перейти в эту подпапку, тогда — и только тогда — вы получите сообщение о запрете доступа.
- **Write (Запись).** Разрешение Write, как бы просто оно не выглядело, таит в себе ловушку. Для начала, разрешение Write на папке позволяет создавать новый файл или подпапку внутри этой папки. А что можно сказать о разрешении Write на файле? Означает ли оно возможность изменения файла? Подумайте, что происходит, когда вы *изменяете* файл. Для изменения файла вы обычно должны иметь возможность открыть файл или прочитать файл. Чтобы изменить файл, разрешение Write должно сопровождаться разрешением Read. Хотя существует одна лазейка: если вы просто добавляете данные в файл, без необходимости в

его открытии, то достаточно одного лишь разрешения Write. Тем не менее, если программист написал приложение, открывающее файл в режиме только для записи, содержимое файла затем усекается без его чтения, после чего происходит запись в файл, и все это не предполагает чтение файла; таким образом, файл можно было бы изменить, не прибегая к процессу чтения вообще.

- **Read & Execute (Чтение и выполнение).** Разрешение Read & Execute идентично разрешению Read, но предоставляет дополнительную атомарную привилегию обхода папки.
- **Modify (Изменение).** Выражаясь просто, разрешение Modify является объединением разрешений Read & Execute и Write с предоставлением дополнительной роскоши в виде разрешения Delete. Даже располагая возможностью изменения файла, вы никогда не сможете удалить его. При выборе разрешений для файлов и папок вы заметите, что если выбрали только разрешение Modify, то разрешения Read, Read & Execute и Write выбираются автоматически.
- **Full Control (Полный доступ).** Разрешение Full Control — это комбинация всех ранее упомянутых разрешений с возможностями изменения разрешений и получения права владения объектами, к которым оно применено. Разрешение Full Control также позволяет удалять подпапки и файлы, даже когда эти подпапки и файлы специально не разрешают их удалять.
- **List Folder Contents (Список содержимого папки).** Разрешение List Folder Contents применяется аналогично разрешению Read & Execute, но предназначено только для папок. Разрешение List Folder Contents позволяет просматривать содержимое папок. Что более важно, разрешение List Folder Contents *наследуется* только папками, и оно видно, только когда просматриваются свойства безопасности папок. Это разрешение позволяет взглянуть, какие файлы существуют в папке (подобно Read), но не будет применять к этим файлам разрешение Read & Execute. По сравнению с этим, если вы применили к папке разрешение Read & Execute, то будете располагать теми же возможностями просмотра папок и их содержимого, но также сможете распространять права Read & Execute на файлы внутри этих папок.
- **Special Permissions (Особые разрешения).** Особые разрешения — это просто настроенная группа атомарных прав, которую вы можете создавать, когда ни одно из рассмотренных выше стандартных молекулярных разрешений не подходит в вашей конкретной ситуации. Хотя может показаться, что возможность Special Permissions было нововведением версии Windows Server 2003, на самом деле оно существовало в Windows 2000 Server. Просто это средство не было видимым как молекулярное разрешение. В Windows 2000 Server отсутствовал какой-нибудь способ сообщить о том, что папка имеет настроенные атомарные разрешения, если только вы не заглядывали на вкладку Advanced (Дополнительно) диалогового окна свойств безопасности. В Windows Server 2012 это можно сделать, посмотрев на флажки Allow/Deny для возможности Special Permissions, чтобы понять, были ли модифицированы записи управления доступом (access control entry — ACE). Если флажки затенены, тогда по щелчку на кнопке Advanced (Дополнительно) вы можете просмотреть и отредактировать изменения в записях ACE.

Унаследованные разрешения

Начиная с ранних редакций Windows Server, существовало средство, которое называется *унаследованными разрешениями*. В настоящее время вполне вероятно, что вы уже привыкли пользоваться этим великолепным средством. Если для файла или папки установлено наследование разрешений, то сам по себе файл или папка в действительности не имеет разрешений; просто применяются разрешения родительской папки. Если родительская папка также наследует разрешения, вы продолжаете подниматься вверх по цепочке каталогов, пока не столкнетесь с папкой, которой назначены жесткие разрешения. Не стоит и говорить, что корневой каталог не может наследовать разрешения.

Например, предположим, что у вас есть папка по имени `APPS`, содержащая три подпапки и файлы. Все подпапки и файлы допускают наследуемые разрешения. Если вы назначите папке `APPS` разрешение Read & Execute для пользователей, то все подпапки и файлы автоматически отразят это новое разрешение. Что если вы хотите настроить разрешения для первой подпапки, предоставив пользователям дополнительную возможность записи? Щелкните на этой папке правой кнопкой мыши, выберите в контекстном меню пункт Properties (Свойства) и в открывшемся диалоговом окне свойств перейдите на вкладку Security (Безопасность), чтобы просмотреть разрешения, назначенные папке. Если флажки для чего-нибудь, отличного от Special Permissions, затенены, вы можете утверждать, что папка наследует разрешения у своей родительской папки. Здесь вам понадобится перейти на вкладку Advanced (Дополнительно), чтобы увидеть опцию Allow inheritable permissions from parent to propagate to this object and all child objects (Позволить наследуемым разрешениям от родителя распространяться на этот объект и все его дочерние объекты). Эта опция показывает, наследует ли объект разрешения, и позволяет указать, допускается ли наследование.

Назначение разрешений файлам и папкам

После того как вы поняли, что собой представляют различные разрешения, назначить их файлам и папкам будет парой пустяков. Откройте проводник Windows и выполните следующие шаги.

1. Найдите файл или папку, которой хотите назначить права, щелкните на ее имени правой кнопкой мыши, выберите в контекстном меню пункт Properties (Свойства) и в открывшемся диалоговом окне перейдите на вкладку Security (Безопасность). Взгляните на рис. 14.12. В верхней части окна показаны группы и пользователи, которым назначены разрешения, а в нижней части — разрешения, назначенные выбранному пользователю или группе. В этом примере вы начина-

Рис. 14.12. Вкладка Security диалогового окна свойств папки `APPS`

ете с папки APPS. В идеальном случае, т.к. папка предназначена для приложений, вы хотите, чтобы все пользователи имели разрешение Read & Execute и не могли изменять, добавлять или удалять что-либо. Также вы хотите оставить администраторам полный доступ, чтобы они имели возможность обслуживать данные. Кроме того, есть группа администраторов базы данных, которым необходимо предоставить права Modify. Поскольку для групп Users (Пользователи) и Administrators (Администраторы) по умолчанию уже присутствуют записи, вы начнете с добавления группы Database Managers (Администраторы базы данных) и выдачи ей прав Modify.

2. Щелкните на кнопке Edit (Редактировать) и затем на кнопке Add (Добавить), в результате чего откроется диалоговое окно Select Users, Computers, Service Accounts, or Groups (Выбор пользователей, компьютеров, учетных записей служб или групп), которое было показано на рис. 14.9.

   Здесь вы можете ввести имя пользователя или группы, щелкнуть на кнопке Advanced (Дополнительно) и затем на кнопке Find Now (Найти сейчас), либо настроить запрос вручную, подготовив список учетных записей домена.

3. Так как вы знаете имя группы, которую нужно добавить в этом примере (Database Managers), просто введите его в диалоговом окне Select Users, Computers, Service Accounts, or Groups и щелкните на кнопке Check Names (Проверить имена). Выполнится перекрестная проверка на совпадение вручную введенной записи со списком имен.

4. Как только имя отобразится подчеркнутым, щелкните на кнопке OK, чтобы возвратиться на вкладку Security диалогового свойств папки APPS.

   После добавления группы Database Managers диалоговое окно должно выглядеть подобным приведенному на рис. 14.13.

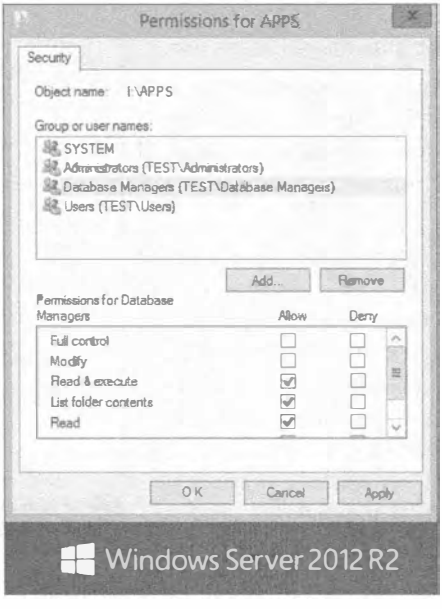


Рис. 14.13. Добавление группы Database Managers

Более быстрое добавление пользователей и групп

Используя метод из предыдущего примера, можно добавлять сразу множество пользователей и групп. Когда вы набираете имена вручную, просто введите первое имя, щелкните на кнопке Check Names и начинайте набирать следующее имя. Если вы ввели неполное имя до щелчка на кнопке Check Names, вам будет предоставлено ближайшее соответствие введенной записи. Если вы решили применять интерфейс поиска в Active Directory, то можете выбрать несколько учетных записей. Для этого щелкните на первой записи и затем, удерживая нажатой клавишу <Ctrl>, щелкайте на дополнительных записях.

Теперь все, что осталось — назначить корректное разрешение, которым является право Modify.

5. Выделите группу `Database Managers` и отметьте флажок Allow (Разрешить) для Modify.

   Вкладка Security должна выглядеть примерно так, как показано на рис. 14.14.

   Поскольку группы `Users` и `Administrators` были добавлены по умолчанию, когда вы создавали общий ресурс, давайте посмотрим на стандартные разрешения, примененные к ним, чтобы выяснить, необходимы ли какие-нибудь корректировки.

6. Щелкните на группе `Users`; вы увидите диалоговое окно, представленное на рис. 14.15.

Рис. 14.14. Применение разрешения Modify

Рис. 14.15. Стандартные разрешения для группы `Users`

Предостережение относительно уровней разрешений

Вы должны быть осмотрительны при выборе некоторых уровней разрешений. Выбор Read & Execute включает все права Read, поэтому Read выбирается автоматически. С другой стороны, если вы хотите очистить Read & Execute, снятие отметки с флажка Allow для Read & Execute не приводит к автоматическому снятию отметки с такого флажка для Read.

На рис. 14.15 видно, что группа `Users` уже имеет ряд стандартных разрешений, в числе которых Read & Execute, List Folder Contents и Read. Вы также заметите, что эти разрешения унаследованы, потому что флажки в столбце Allow затенены. Тем не менее, как вы можете помнить, затенение записи Special Permissions не означает, что разрешения являются унаследованными (хотя они и могут быть таковыми). Затенение здесь указывает лишь на то, что имеются дополнительные записи разрешений, которые можно просмотреть в этом конкретном диалоговом окне.

7. Щелкните на кнопке Advanced (Дополнительно), чтобы получить диалоговое окно Advanced Security Settings for APPS (Расширенные настройки безопасности для `APPS`). Взглянув на рис. 14.16, вы увидите намного более сложную версию записей разрешений по сравнению с той, что была показана на рис. 14.15. Правда, не совсем понятно, почему разработчики из Microsoft решили сначала отображать своего рода оглавление по разрешениям, а не предоставлять сразу подробную информацию.

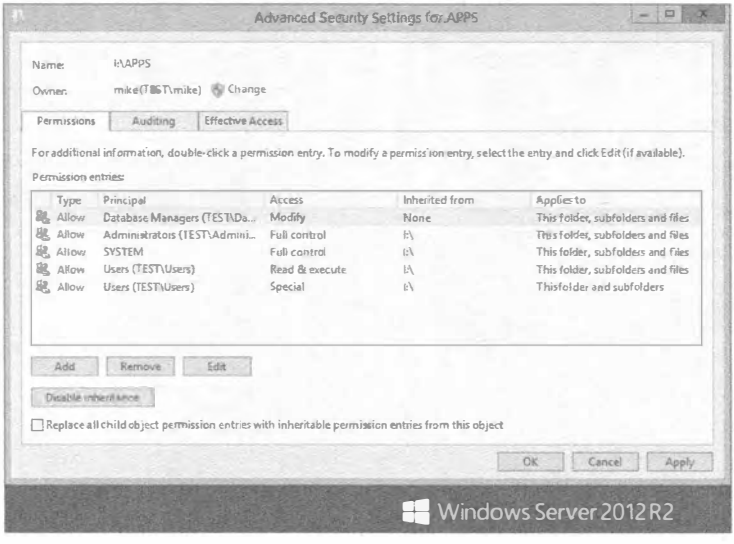


Рис. 14.16. Диалоговое окно Advanced Security Settings for APPS

В списке Permission entries (Записи безопасности) перечислены выбранные группы и пользователи с описанием их прав. В этом диалоговом окне вы можете отключать наследование, щелкая на кнопке Disable inheritance (Отключить наследование), а также по-прежнему добавлять и удалять записи, щелкая на кнопках Add (Добавить) и Remove (Удалить). Так в чем же разница? В этом окне вы получаете больше деталей.

Прежде всего, вы заметите, что одна запись в предшествующем окне разрешений может стать здесь двумя и более детализированными записями, позволяя четко видеть, какие есть права и откуда они унаследованы, и созданы ли записи для данного ресурса специально вручную. Например, обратите внимание, что группа Users имеет две записи, которые обе унаследованы от тома. Кроме того, в столбце Applies to (Применяется к) четко видно, откуда происходят разрешения. Разумеется, наличие всех этих деталей значительно помогает при поиске и устранении неполадок, т.к. вся необходимая информация собрана в одном месте (точнее, почти вся).

У вас есть возможность приспособить свои расширенные разрешения к атомарному уровню, выбрав запись и щелкнув на кнопке Edit (Редактировать). Однако будьте осторожны. При таком большом количестве разрешений, поступающих из множества разных мест (и здесь мы даже не учитывали разрешения общего доступа!), этот процесс легко может привнести путаницу в процедуру устранения неполадок. Пытайтесь максимально упрощать свои ресурсы и пользователей, по томам, по группам или по машинам, и вы существенно облегчите себе жизнь, имея дело с разрешениями.

Чтобы посмотреть, какие права имеет группа Users, и удостовериться в том, что она получит корректный доступ к папке APPS, выполните следующие шаги.

1. Выберите запись для группы Users с разрешением Read & Execute.
2. Щелкните на кнопке View (Просмотреть) в диалоговом окне Advanced Security Settings for APPS (Расширенные настройки безопасности для APPS).
3. Щелкните на кнопке Show advanced permissions (Показать расширенные разрешения) и обратите внимание, что опции здесь затенены.

Если вы повторите те же самые шаги для группы Database Managers, то заметите, что теперь вместо кнопки View (Просмотреть) отображается кнопка Edit (Редактировать). Почему для группы Database Managers разрешения не затенены? Причина в том, что наследование применяется к группе Users, но не к группе Database Managers. Если вы хотите редактировать разрешения для Users здесь, то вам придется разорвать наследование и повторно добавить эту группу. На рис. 14.17 показаны атомарные разрешения для группы Users.

На основании точной информации выясняется, что конечным разрешением является Read & Execute. Ни больше и ни меньше; эти пять атомарных разрешений образуют разрешение Read & Execute. Считайте, что это закон.

Наследование разрешений

Вы могли заметить, что раскрывающийся список Applies to (Применяется к) тоже не доступен для записи группы Users. Это еще один результат наследования. Наследование удобно трактовать как указание свыше. Такие разрешения будут применяться к данной папке, подпапкам и файлам, если только вы не отключите наследование и не создадите собственные специальные разрешения. Или же вы могли бы перейти прямо к источнику, поскольку, будучи администратором, вы устанавливаете правила, когда дело доходит до наследования. Открывая диалоговое окно свойств для тома и редактируя записи для группы Users, вы можете удалить или модифицировать разрешения; затем вы можете точно указать, где они должны применяться повсюду на томе, используя кнопку Apply Onto (Применить на).

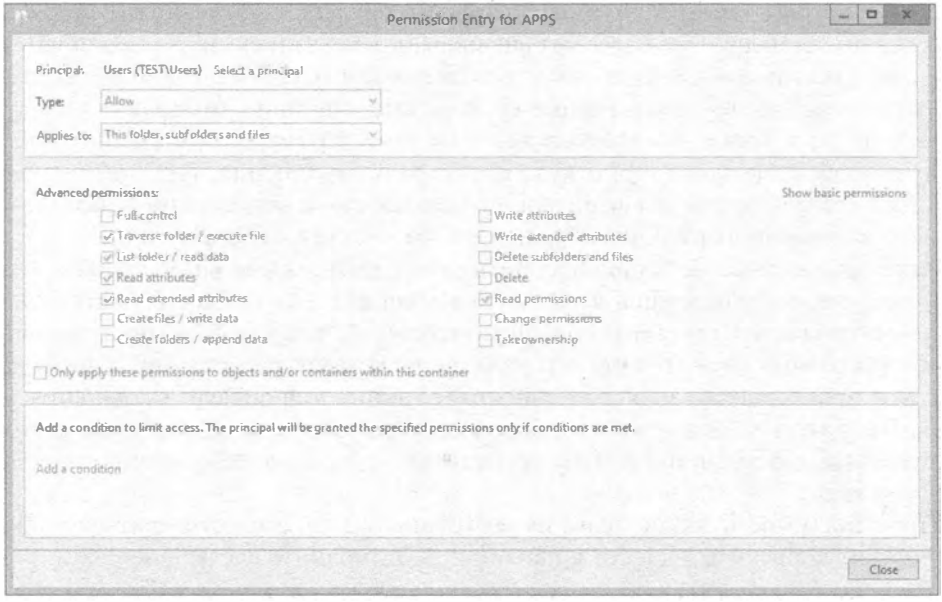


Рис. 14.17. Просмотр и редактирование атомарных разрешений предоставляет максимальную информацию

Обратите внимание на наличие двух записей для группы `Users`. Стандартные разрешения в Windows Server 2012 являются более защищенными, чем в предшествующих редакциях сервера. Вспомните, что в Windows 2000 Server группа `Everyone` имела разрешение Full Control для *чего угодно*!

Давайте исследуем атомарные разрешения для другой записи группы `Users`.

1. Если вы по-прежнему видите диалоговое окно, показанное на рис. 14.17, щелкните на кнопке Close (Закрыть) — вам не нужно изменять запись Read & Execute, т.к. это именно то, что требуется для папки `APPS`.

2. Возвратившись в диалоговое окно Advanced Security Settings for APPS (Расширенные настройки безопасности для `APPS`), щелкните на другой записи для группы `Users` и затем щелкните на кнопке Edit (Редактировать). Откроется диалоговое окно, представленное на рис. 14.18.

Стандартные разрешения для группы `Users` включают возможность создания файлов и папок на томе, а также возможность записи и добавления данных в файлы, содержащиеся внутри этого тома — конечно, если вы специально не запретите такую возможность любым конкретным ресурсам на томе. Таким образом, вы имеете здесь набор разрешений, находящийся между двумя обсуждаемыми ранее группами атомарных разрешений. Первый набор атомарных разрешений, который вы видели для группы `Users`, образует молекулярное разрешение Read & Execute. Если вы добавили эти два атомарных разрешения, то молекулярное разрешение попадет куда-то между Read & Execute и Modify. Вполне понятно, что разрешение Modify также включает права Write Attributes, Write Extended Attributes и Delete Subfolders and Files.

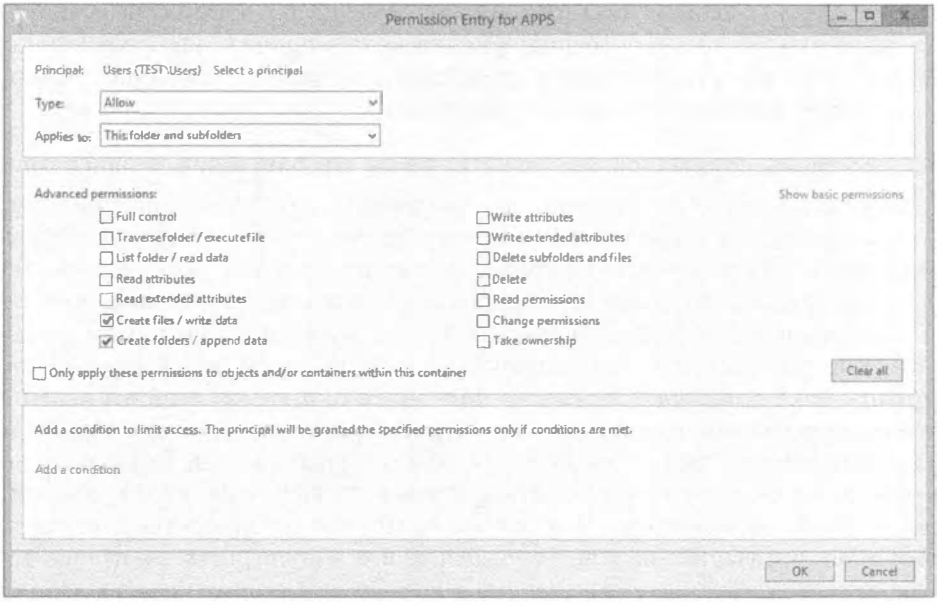


Рис. 14.18. Редактирование специальных разрешений для группы `Users`

По двум причинам проще использовать действие Deny.

- Во-первых, вам не придется беспокоиться об остальных разрешениях, унаследованных от тома, часть из которых понадобится сохранить. Когда вы удаляете наследование, вам предоставляется право копировать существующие унаследованные разрешения и затем редактировать их по своему усмотрению.
- Во-вторых, удаляя наследование, вы устраняете возможность вывода разрешений из тома в глобальную область действия, что является довольно удобным средством. Как упоминалось ранее, если вы можете упростить разрешения, выполняя работу в глобальной области действия, то сохраните немало времени и усилий.

Чтобы отключить для группы `Users` возможность создания файлов или папок либо записи или добавления данных в папку `APPS`, просто отметьте флажки Deny (Запретить) для обеих записей атомарных разрешений (рис. 14.19) и щелкните на кнопке OK.

Рис. 14.19. Имеется недостаточно информации для определения *полной* истории разрешений на основе первоначального диалогового окна разрешений

Удаление группы или пользователя

Чтобы удалить запись для группы или пользователя, просто щелкните на кнопке

Remove (Удалить) в любом диалоговом окне свойств, которые были рассмотрены ранее. Если пользователь или группа присутствует по причине наследования, кнопка Remove будет недоступной, и вам придется отключить наследование, щелкнув на кнопке Disable inheritance (Отключить наследование).

Использование детализированного интерфейса для получения полной истории

Взгляните на рис. 14.19. Помните это диалоговое окно? Мы напомним вам кое-что, о чем говорилось ранее касательно интерфейсов, применяемых для управления разрешениями NTFS: это окно не предоставляет достаточного объема информации, из-за чего возникают затруднения. Если вы решили отключить наследование, чтобы избавиться разрешения Write для группы `Users`, и для этого щелкнули на кнопке Remove (Удалить) в данном диалоговом окне, то тем самым вы удалили *обе* записи для группы `Users`, которые видели на рис. 14.16. К тому же, если вы используете это окно для добавления учетной записи пользователя или группы, то будете иметь возможность отметки только флажков для молекулярных разрешений, которые здесь видны — вы не сможете точно указать, где эти разрешения должны применяться с использованием наследования. Чтобы сделать это, вам пришлось бы перейти в диалоговое окно, показанное на рис. 14.16. Лучше всего пропустить это излишнее диалоговое окно и перейти непосредственно к детализированному представлению. Это позволит получить полную историю с самого начала.

Конфликтующие разрешения

Разрешения можно назначать файлам, а также папкам. Точно так же, как разрешения общего доступа могут вступать в противоречие с разрешениями для файлов и папок, разрешения для файлов могут конфликтовать с разрешениями для папок. В конфликтах на уровне общего доступа преимущество получают разрешения общего доступа; если же в противоречие вступают разрешения для файлов и папок, то предпочтение отдается разрешениям для файлов. Разрешения общего доступа устанавливают максимально допустимый доступ, так что если разрешением общего доступа является Read, а разрешением NTFS — Write, то результатом окажется разрешение Read. Если вы назначите папке права только для чтения, но какому-то файлу внутри этой папки — права на изменение, то все равно будете иметь возможность изменять этот файл.

Множество разрешений

А теперь поговорим о еще одной проблеме. Вы предоставили группе `Administrators` полный контроль над папкой `APPS`, а группа `Everyone` имеет только разрешение Read & Execute. Вот где разрешения снова вступают в конфликт. Группа `Everyone` содержит пользователей, не так ли? Даже администраторы являются пользователями. Хм. Как же это работает? Дело в том, что при наличии нескольких разрешений преимущество получит *наименее ограничивающее* разрешение при условии, что в игру не вовлечены разрешения общего доступа. Предположим, что у вас есть администратор Боб. Он входит в состав группы `Users`, которая имеет права доступа только для чтения к какому-то файлу. Боб также является членом группы `Administrators`, имеющей полный доступ. В таком случае Боб получит полный доступ, т.к. это разрешение наименее ограничивающее.

Разрешения Deny

Ранее мы говорили о разрешениях Deny в связи с общими ресурсами и кратко рассматривали последствия наследования разрешений в отношении к действиям Allow и Deny. То же самое применимо к разрешениям файлов и папок, но чуть более сложным способом из-за большего количества параметров безопасности. Подумайте о файле электронной таблицы с назначением премий внутри корпорации, который вы пытаетесь защитить. Вы хотите, чтобы все видели этот файл, но изменять его содержимое могли только менеджеры. Это имеет смысл: предоставьте группе `Employees` (Сотрудники) права на чтение, а группе `Managers` (Менеджеры) — полный доступ. Предположим, что где-то по пути какой-то руководитель низшего звена попадает в обе группы. По одним меркам эта персона должна быть частью группы `Managers`, тогда как по другим — входить в состав группы `Employees`. Если вы оставите только что описанные разрешения, данный руководитель получит лучшее из двух миров в отношении файла электронной таблицы — полный доступ. По этой причине вы принимаете решение о том, что члены группы `Employees` не должны явно иметь полный доступ. И как теперь поступить?

Все довольно просто: запретите это чрезмерное разрешение. Вам потребуется определить, какие разрешения *не* должны иметь сотрудники, и отметить для этих разрешений флажки в столбце Deny (Запретить); таким методом вы можете гарантировать, что сотрудники будут располагать только правами Read. Чтобы сделать это, выполните следующие шаги.

1. Щелкните на имени файла правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства).
2. В открывшемся диалоговом окне свойств перейдите на вкладку Security (Безопасность) и щелкните на кнопке Advanced (Дополнительно). (Вспомнили интерфейс, представленный на рис. 14.15?)
3. Выделите запись для группы `Employees` (Сотрудники) и щелкните на кнопке Edit (Редактировать), что позволит модифицировать атомарные разрешения для файла электронной таблицы.
4. В раскрывающемся списке Type (Тип) выберите элемент Deny (Запретить) и затем щелкните на ссылке Show advanced permissions (Показать расширенные разрешения).
5. Отметьте флажки для разрешений, как показано на рис. 14.20.

   Вы должны отдельно отметить флажки для каждого разрешения. Однако если вы отметите флажок Full Control (Полный доступ), то отметятся все остальные флажки, т.к. Full Control включает все разрешения. В этом примере нас интересует включение разрешения Read и отключение разрешения Write.
6. Щелкните на кнопке OK, чтобы новые разрешения вступили в силу.

Вы получите предупреждение, сообщающее о том, что разрешения Deny переопределят разрешения Allow. Теперь в сценарии с несколькими разрешениями преимущества получают разрешения Deny, и даже с учетом того, что упомянутый ранее руководитель имеет членство в обеих группах `Managers` и `Employees`, его права будут ограничены посредством Deny.

Рис. 14.20. Разрешения Deny

В диалоговом окне Advanced Security Settings обратите внимание на наличие двух записей для группы `Employees`: одна для разрешения Deny и одна для разрешения Allow. Они больше не объединяются в единое целое, как вы привыкли видеть в выпусках Windows Server, предшествующих Windows Server 2008.

Действующие разрешения

Что будет конечным результатом всех этих разрешений, если одни из них наследуются, другие — нет, некоторые применяются к пользователям, а некоторые — к группам? Кто и что сможет делать с теми или иными файлами? Как выяснить, каким будет результат всех имеющихся разрешений для любой группы, пользователя или объекта? В состав Windows Server 2012 включен инструмент, который позволяет вычислить действующий доступ для любого отдельного пользователя или группы на заданном объекте. Взгляните на диалоговое окно, представленное на рис. 14.21. И снова это диалоговое окно расширенных настроек безопасности для папки `APPS`, которое к настоящему времени вы должны хорошо знать. Вспомните, что администраторы имеют разрешение Full Control, администраторы базы данных — разрешение Modify, а пользователи — разрешение Read & Execute.

Чтобы увидеть, как в точности работают все эти разрешения, перейдите на вкладку Effective Access (Действующий доступ), которая показана на рис. 14.22. В выпуске Windows Server 2012 R2 эта вкладка порядком изменилась. Новая вкладка Effective Access теперь позволяет легко просматривать уровень доступа пользователя или группы к любым локальным или присоединенным к домену машинам или группам. Вы можете выбрать локального или сетевого пользователя, включить в запрос членство в группах этого пользователя и просмотреть действующий доступ в отношении другой группы или сервера. В следующем примере можно видеть действующие разрешения для группы `Database Managers` на тестовом сервере `BF1`. Действующим доступом является Modify, как было установлено в предшествующих упражнениях.

Рис. 14.21. Расширенные разрешения для папки APPS

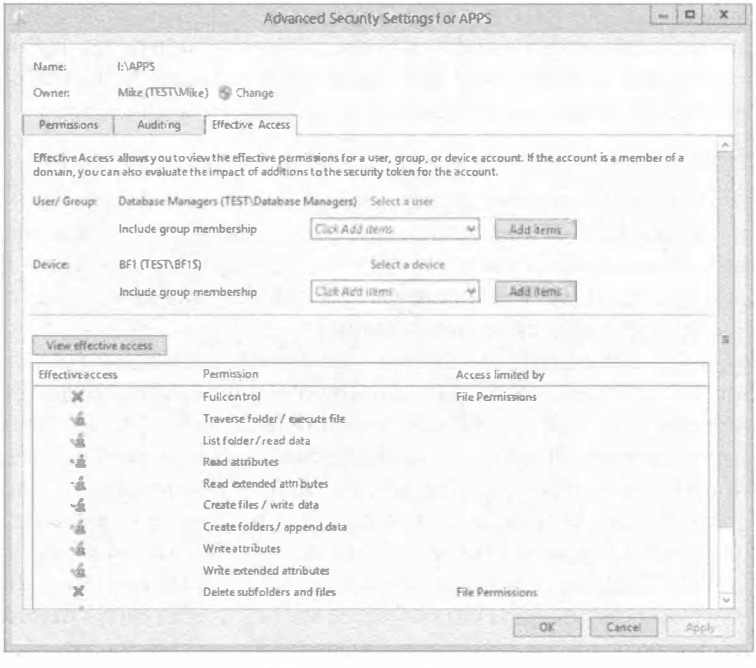


Рис. 14.22. Вкладка Effective Access

Конечно, для просмотра разрешений на любом проверяемом ресурсе необходимо располагать соответствующими правами, и *существуют* ограничения в плане факторов, которые используются для определения действующего доступа. Например, вы можете не иметь возможности просмотра разрешений для каждого пользователя

или группы. Рассмотрим локальную группу Users на сервере по имени Storage, на котором находится общий ресурс APPS. Из-за того, что этот сервер является членом домена Active Directory, глобальная группа под названием Domain Users (Пользователи домена) автоматически вкладывается внутрь локальной группы Users. Чтобы просмотреть действующие разрешения на локальной группе Users, понадобится выполнить перечисленные ниже действия на вкладке Effective Access диалогового окна Advanced Security Settings for APPS (Расширенные настройки безопасности для APPS).

1. Щелкните на ссылке Select a user (Выбрать пользователя) или Select a device (Выбрать устройство) и затем щелкните на кнопке Location (Местоположение).
2. Выберите локальное местоположение по имени Storage (в отличие от каталога).

Поскольку группа Domain Users вложена в локальную группу Users, пользователи домена имеют те же самые права для папки за исключением существования любого другого набора разрешений, который конфликтовал бы с ними. Но когда вы попытаетесь получить действующие разрешения для группы Domain Users с помощью этого инструмента, обнаружится отсутствие доступа, т.к. данный инструмент не умеет вычислять действующие разрешения для групп домена, вложенных в локальные группы.

Безусловно, это ограничивает эффективность инструмента, но вы по-прежнему можете применять его при вычислении множества записей ACE для пользователя или группы, как было продемонстрировано в предыдущем примере.

Право владения

В процессе назначения и отзыва разрешений вы обязательно столкнетесь с проблемой, когда никто, включая администраторов, не может получить доступ к файлу. И вы не можете изменить разрешения файла, потому что для этого необходимы определенные разрешения. Ситуация зачастую оказывается действительно трудной. К счастью, помочь здесь может право владения.

Каждый объект имеет атрибут, который называется *владелец* (owner). Владелец полностью отделен от разрешений. Для *каждого* объекта всегда будет существовать *некоторый* владелец. Но чем это может помочь? Дело в том, что владелец объекта обладает специальной привилегией — возможностью назначения разрешений.

Получение права владения файлом или папкой — относительно простая задача при условии, что учетная запись, используемая для изменения права владения, имеет полный доступ на желаемом ресурсе. Возвратившись обратно к рис. 14.16, вы заметите поле Owner (Владелец), расположенное ниже поля Name (Имя). Вы также обнаружите рядом ссылку Change (Изменить); если она недоступна, значит, вы вошли с учетной записью, которая не имеет привилегии на изменение права владения. По щелчку на ссылке Change откроется диалоговое окно Select User (Выбор пользователя), позволяющее назначить право владения другому пользователю или группе.

На корпоративном общем ресурсе в производственной среде имеет смысл обеспечить права владения всеми его файлами и папками для учетной записи с повышенными полномочиями, контролируемой персоналом из IT-отдела, или точнее — учетной записи службы уровня хранилища. Наиболее интенсивно такая

конфигурация применяется для целей резервного копирования и восстановления. Некоторые файловые системы не позволяют восстанавливать файлы, для которых отсутствуют разрешения на это действие. Представьте себе попытку восстановления общего ресурса, на котором пользователи сделали себя владельцами папок и файлов, удалив весь остальной доступ. Такие папки или файлы окажутся невосстановимыми никем кроме своего владельца. Это укрепляет хорошую стратегию поддержания строгих и управляемых разрешений повсеместно в среде из одного контролируемого централизованного места.

Работа со скрытыми общими ресурсами

После открытия общего доступа к папке из сети она становится видимой сообществу пользователей. Но что, если вы не хотите, чтобы общий ресурс могли видеть абсолютно все? Например, мы создали на сервере общий ресурс с исходными дистрибутивами, чтобы всякий раз, когда мы находимся на рабочей станции пользователя, была возможность устанавливать любые приложения без необходимости в захватывании с собой компакт-дисков. На самом деле это сделано для удобства, но в то же время мы не хотим, чтобы пользователи могли заходить на данный общий ресурс и устанавливать любые приложения, которые им попадутся на глаза. Несомненно, мы могли бы ограничить общий ресурс, предоставив разрешения на доступ к нему только себе, но это также требует определенных усилий. Мы вовсе не хотим выходить из системы пользователя и заходить под своей учетной записью при каждом выполнении установки, особенно когда задействуются профили пользователей. В такой ситуации может помочь создание скрытых общих ресурсов. Мы хотим, чтобы общий ресурс существовал и был доступным, но просто не так легко обнаруживался. Хотя это и не полностью защищенное решение, оно является сдерживающим фактором против чрезмерно любопытных пользователей.

Чтобы создать скрытый обший ресурс, откройте общий доступ к папке обычным образом, но добавьте в конец имени нового общего ресурса знак доллара. Вот и все. Теперь, когда сервер регистрирует информацию для списка доступных ресурсов, он просто не будет включать в него этот скрытый общий ресурс.

Давайте посмотрим, как создать общий ресурс по имени `INSTALL$`, который соответствует папке `I:\Install`.

1. Создайте общий ресурс, как это делается обычно, но назовите его **`INSTALL$`**, а не `INSTALL` (рис. 14.23).
2. Выберите разрешения, чтобы позволить доступ только администраторам (рис. 14.24).

   Теперь из клиентских рабочих станций вы не увидите общего ресурса `INSTALL$` в списке доступных ресурсов, но по-прежнему сможете вручную отображать диск на ресурс `INSTALL$` с целью дальнейшего подключения к нему.
3. Выберите имя общего ресурса в консоли Computer Management (Управление компьютером), как показано на рис. 14.25.

Хотя скрытый общий ресурс не будет отображаться в списке доступных ресурсов внутри проводника Windows, он будет видимым через консоль Computer Management. Это помогает помнить о том, какие скрытые общие ресурсы были созданы.

Рис. 14.23. Создание скрытого общего ресурса

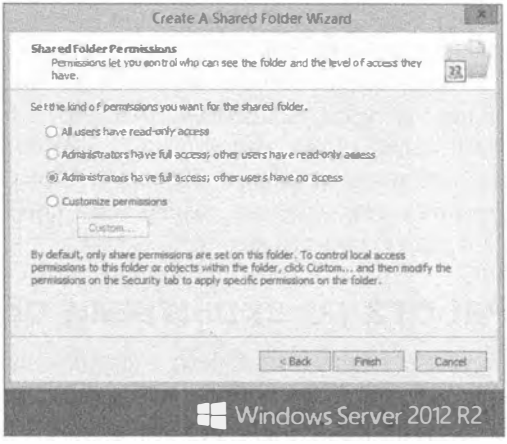


Рис. 14.24. Установка разрешений для администраторов на скрытом общем ресурсе

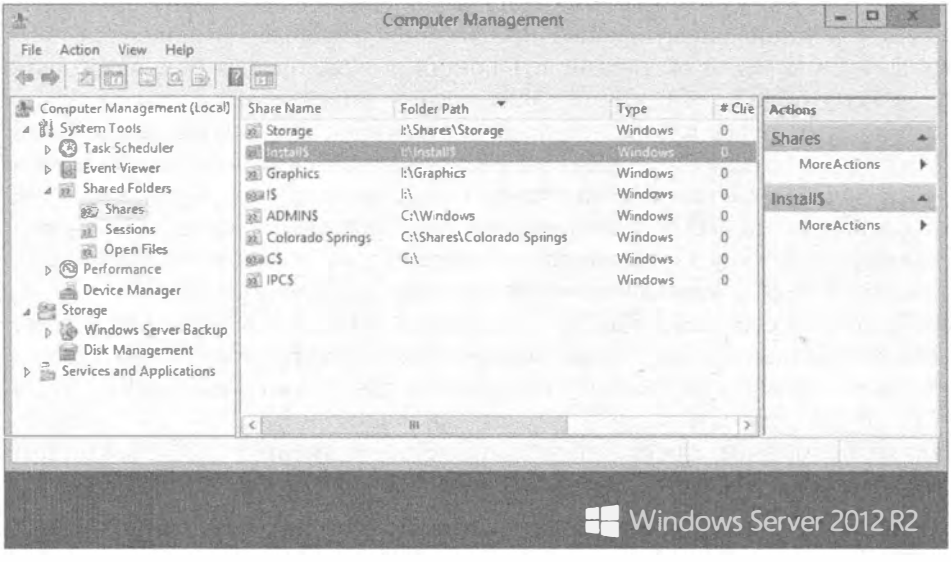


Рис. 14.25. Отображение диска на скрытый общий ресурс

Исследование распределенной файловой системы

Что собой представляет распределенная файловая система (Distributed File System — DFS)? Благодаря DFS вы можете создавать единственный общий ресурс, который заключает в себе каждый ресурс, основанный на файловом общем ресурсе, внутри сети. Думайте о нем, как о доме для всех общих файловых ресурсов в сети со страницей "ссылок", указывающих клиентам на отдельный сервер или серверы, где действительно размещены эти общие ресурсы. Вы можете иметь общие ресурсы, которые охватывают целый мир. Сгруппируйте всех их вместе под одним пространством

имен и откройте пользовательской базе общий доступ к этому пространству имен, чтобы сделать возможным дружественный к пользователям, централизованный метод общего доступа к ресурсам. Продвигаясь на шаг дальше, файловая система DFS может реплицировать изменения в общие ресурсы на любых серверах, которые являются членами группы репликации, сохраняя все эти серверы в актуальном состоянии.

В Windows Server 2012 применяются две технологии.

- **DFS Namespaces (Пространства имен DFS).** Компонент DFS Namespaces предоставляет возможность группировать общие папки, находящиеся на разных сайтах и серверах, в одно или несколько логически структурированных пространств имен. Пространство имен затем представляется пользователю в виде единой общей папки, состоящей из множества подпапок, как если бы все они располагались в локальном каталоге. Это великолепная функциональность, которая делает возможным централизованный метод управления и использования общих ресурсов на большом числе физически отдельных серверов или местоположений сайтов. Такая структура повышает готовность и автоматически подключает пользователей к общим папкам внутри того же самого сайта Active Directory Domain Services, когда они доступны, вместо их маршрутизации по каналам WAN.
- **DFS Replication (Репликация DFS).** Компонент DFS Replication — это эффективный механизм репликации с несколькими хозяевами, который можно применять для поддержания папок в синхронизированном состоянии между серверами через сетевые подключения с ограниченной пропускной способностью. Репликация DFS может происходить среди множества сайтов и серверов, находящихся внутри одного и того же леса. Компонент DFS Replication использует удаленное разностное сжатие (remote differential compression — RDC) для определения и репликации только изменившихся блоков данных файла. Компонент DFS Replication работает рука об руку с новыми средствами дедупликации данных (Data Deduplication), предлагаемыми в Windows Server 2012 R2. Будучи интегрированным с той же самой технологией хранилища уровня блоков, компонент DFS Replication поддерживает репликацию папок и файлов, расположенных на томах, для которых включена дедупликация. Применение дедупликации для снижения требований к хранилищу в файловой системе NTFS не оказывает никакого неблагоприятного влияния на репликацию DFS.

Прежде чем можно будет пользоваться этими средствами, на сервер понадобится добавить новые роли — DFS Namespaces и DFS Replication. Добавьте их с помощью мастера добавления ролей и компонентов (Add Roles and Features Wizard) в диспетчере серверов (рис. 14.26).

Существует несколько дополнительных требований, которые необходимо принять во внимание до запуска DFS. Чтобы можно было успешно развернуть DFS Replication в имеющейся среде, серверы должны быть сконфигурированы так, как описано ниже.

- Все серверы, которые вы хотите сделать членами группы репликации, должны иметь установленную роль DFS Replication.
- Вы должны удостовериться, что применяемое антивирусное программное обеспечение совместимо с DFS Replication.

- Все серверы-члены должны находиться внутри одного и того же леса. Компонент DFS Replication хорошо работает между доменами, но пока что не поддерживает репликацию между лесами.
- Удостоверьтесь в том, что схема AD DS актуальна и соответствует всем подходящим дополнениям схемы в данной редакции сервера. В Windows Server 2012 R2 такая актуальность соблюдена.
- Учтите, что компонент DFS Replication не поддерживает файловые системы FAT и Resilient File System (ReFS), а также не работает с данными, которые хранятся на кластеризированных общих томах. Чтобы репликация между серверами поддерживалась, данные должны находиться в файловой системе NTFS.

Рис. 14.26. Добавление ролей DFS Namespaces и DFS Replication

Альтернативой использованию мастера Add Roles and Features Wizard может быть применение Windows PowerShell для добавления ролей и компонентов. Ниже приведены примеры использования PowerShell для добавления к серверу ролей DFS Namespaces и DFS Replication, а также создания пространства имен DFS.

1. Откройте окно Windows PowerShell через панель задач от имени учетной записи администратора.
2. Запустите следующие команды для установки на сервере роли DFS:

```
PS C:\> Import-Module ServerManager
PS C:\> Add-WindowsFeature FS-DFS
PS C:\> Import-Module DFS
```

3. Запустите следующую команду для создания отдельного пространства имен DFS:

```
PS C:\> New-DfsnRoot -TargetPath "\\Test-FS\Software" -Type Standalone
-EnableSiteCosting -Path "\\Test\Software"
```

4. Чтобы просмотреть доступные новые командлеты PowerShell в Windows Server 2012 R2, предназначенные для DFS, выполните такую команду:

```
PS C:\> Get-Command -Module DFS
```

Терминология, связанная с DFS

Прежде чем двигаться дальше, необходимо освоить терминологию, связанную с DFS. Как и в случае Active Directory, здесь в игру вступает целый новый набор концепций.

Вы начинаете с *корня* (root). Его можно приблизительно трактовать как общий ресурс, который будет видимым для сети. В нашем примере корнем является `APPS`. Внутри сайта можно иметь много корней, и в Windows Server 2012 один сервер может содержать более одного корня подобно тому, как это было в Windows Server 2008. Корень открывается для общего доступа из сети и в действительности функционирует подобно любому другому общему ресурсу. Внутри общей папки можно иметь дополнительные файлы и папки.

Под корнем вы добавляете *ссылки DFS* (DFS link). Ссылка — это другой общий ресурс где-то в сети, который помещен под корень. Термин *ссылка* является частью бесконечного смещения терминологии. В этом случае, похоже, мы сместились в сторону терминологии Интернета. Представляйте корень DFS как домашнюю веб-страницу, содержащую ничего кроме имени и множества ссылок на другие веб-страницы. Ссылки внутри иерархии DFS подобны гиперссылкам на веб-странице, которые автоматически направляют в новое местоположение. Вы, как пользователь, не обязаны знать, куда ведут эти ссылки, до тех пор, пока вы получаете искомую веб-страницу. После нахождения домашней страницы (корня DFS) посредством этих гиперссылок (ссылок DFS) вы будете направлены на любой желаемый веб-сайт (общий ресурс).

Цель (target) или *реплика* (replica) может направляться либо на корень, либо на ссылку. При наличии в сети двух идентичных общих ресурсов, обычно находящихся на разных серверах, их можно сгруппировать вместе внутри одной и той же ссылки в виде *целей DFS*. Вы также можете реплицировать целый корень — т.е. оглавление — в качестве *члена реплики корня*. После того как цели сконфигурированы для репликации, служба репликации файлов (File Replication Service) поддерживает содержимое корней в синхронизированном состоянии.

Выбор между автономной и доменной файловой системой DFS

Перед тем, как приступать к созданию системы DFS, вы должны решить, какой вид файловой системы DFS вам необходим. Это решение главным образом будет основано на том, имеется ли Active Directory. Большое отличие будет касаться корня DFS. В файловой системе DFS, основанной на Active Directory или на домене, сам корень может иметь реплики. Другими словами, единая точка отказа — корень — рассредоточивается по Active Directory. Если используются реплики корня, то при наличии, скажем, 27 серверов, размещающих Active Directory, вы будете иметь 27 мест, где будет находиться информация DFS. Надо заметить, что это не вся информация, но ее вполне достаточно для указания клиентам на одну из реплик корня DFS. Благодаря этому, до тех пор, пока служба Active Directory функционирует и доступна, доступной будет также и файловая система DFS. Кроме того, будучи интегрированными в Active Directory, реплики ссылок могут быть сконфигурированы для применения автоматической репликации.

Пример из практики

DFS и вы

Мы начали эту главу с совета насчет того, что вы должны взглянуть или начать пользоваться файловой системой DFS. Ладно, позвольте нам поведать короткую историю о том, как однажды сервер прекратил свое существование. Просто почитайте и осознайте, почему применение DFS может сберечь критически важные файлы и сократить время, требуемое для восстановления файлов и/или папок.

Как-то раз несколько лет назад один из авторов этой книги в завершение рабочего дня исследовал журналы событий на своих серверах. Казалось, что все было в порядке, поэтому он поехал в направлении к дому, до которого было около 45 миль. Когда до дома оставалось минут 15, он получил на пейджер сообщение от лица, занимающегося поддержкой во второй половине дня, которое гласило, что главный сервер на одной из площадок прекратил работу и не удается войти в систему или увидеть его с помощью команды `ping`. Опасаясь худшего, автор развернул машину обратно лишь для того, чтобы по прибытии увидеть, что производственная деятельность продолжается и ничего не требуется предпринимать. Критически важные файлы, необходимые для работы в ту ночь, были позаимствованы из другого сервера.

На следующий день сервер был восстановлен (как оказалось, причиной была проблема с материнской платой) и компания не подверглась простою. Время, которое потребовалось бы для восстановления из резервной копии, вдвое бы превышало среднее время для восстановления (mean time to restore — MTTR) и стоило бы миллионов долларов производственных потерь. Эта цена включала бы людей, которые не смогли работать на предприятии из-за отсутствия данных. Если вы хотите сохранить данные в деле, освойте, как следует, функционирование файловой системы DFS.

При автоматической репликации служба репликации файлов (File Replication Service) принимает на себя задачу синхронизации содержимого реплицированных файлов, обеспечивая наличие во всех репликах одной и той же информации. Можно с уверенностью утверждать, что если вы имеете домен Active Directory, то должны выбрать файловую систему DFS, основанную на домене.

Но у файловой системы DFS, основанной на домене, есть действительно интересная особенность. Если вы размещаете DFS в домене Active Directory под названием `test.com`, то помимо того, что пользователи не обязаны знать, на каком сервере находится конкретный общий ресурс, они даже не нуждаются в информации о том, на каком сервере располагается сама файловая система DFS. Вместо отображения диска на `\\имя_сервера\имя_DFS` пользователи могли бы отображать диск на `\\test.com\имя_DFS`. Теперь, используя ту же самую логику, которую клиент применял для нахождения доступного контроллера домена Active Directory, клиент может искать хост DFS. Если один хост отказал, клиент просто обращается к другому хосту.

Файловая система DFS, основанная на домене, автоматически публикует свою топологию в Active Directory. Это означает, что действительная иерархия DFS — корни, ссылки и цели — публикуется в Active Directory, так что все контроллеры домена будут знать, где находится DFS, как она выглядит и каким образом перейти к ней. Это вовсе *не* значит, что каждый контроллер домена является сервером реплик корня DFS.

Если вы добрались до этого места, то вероятно не располагаете Active Directory, чтобы публикация стала возможной. А как насчет сетей, не основанных на AD? Большинство компаний перешли на Active Directory. Большинство из них установили местами, по меньшей мере, несколько серверов-членов. Для тех компаний, которые не прошли через процесс миграции, технология DFS предлагает расширение базового файлового сервера, которое позволяет предприятию выйти за пределы физических границ и перейти в более дружественное к пользователю и управляемое состояние.

Автономная файловая система DFS является крупным шагом вперед в направлении мира файловых общих ресурсов из предшествующих версий Windows Server, не требуя предварительного развертывания Active Directory. В автономной файловой системе DFS вы не получите высокой отказоустойчивости самого корня, автоматической репликации и опубликования DFS в Active Directory. Но вы все равно получите в свое распоряжение остальные удобства, такие как объединение всех сетевых общих ресурсов в единое пространство имен и в конечном итоге устранение зависимости от имен физических серверов и местоположений, когда пользователи начнут обращаться к своим ресурсам. Чуть позже мы обсудим, как извлечь пользу от привносимых DFS преимуществ в практической среде с или без Active Directory, но сначала давайте посмотрим, как все это построить.

Предположим, что в сети имеется следующий набор общих ресурсов.

Путь UNC	Отображение у пользователей	Описание ресурса
\\DC1\APPS	G:	Все общие приложения
\\RESOURCE1\APPS	G:	Те же приложения, что и в \\DC1\APPS
\\STORAGE\SALES	S:	Корпоративные данные о продажах
\\STORAGE2\USERS	H:	Все пользовательские каталоги
\\STORAGE\FINANCE	Q:	Корпоративные данные о финансах
\\RESOURCE2\APP2	P:	Смешанные приложения

Это может вызвать настоящую головную боль у пользователей (не говоря уже об администраторах), которым придется помнить, куда необходимо переходить для подключения ко всем перечисленным ресурсам. Ресурсы размешены на пяти разных серверах. Вдобавок, если клиенту нужно получит доступ одновременно к ресурсам APPS, SALES, USERS и FINANCE, ему потребуется сделать четыре разных подключения. Да, четыре подключения звучит не так уж устрашающе, но мы имели дело с крупными сетями, где клиентам попросту не хватало доступных букв дисков для отображения на очередной общий ресурс; каждая буква от A до Z была на что-то отображена. Вам также придется помнить, какие клиенты подключаются к \\DC1\APPS, а какие — к \\RESOURCE1\APPS, которые представляют собой идентичные общие ресурсы, размещенные на двух разных серверах. Опять-таки, это не является большой проблемой в данном конкретном примере, но при наличии, скажем, 50 серверов, содержащих тот же самый набор APPS, их отслеживание станет настоящим кошмаром.

Преимущества DFS

Как вы, вероятно, уже поняли, файловая система DFS наиболее выгодна на крупных предприятиях, и ее развертывание в небольших сетях может не стоить приложенных усилий.

А теперь давайте рассмотрим этот же сценарий, но в DFS. Вы будете иметь один корень DFS (под названием `Corp`) с перечисленными внутри него всеми корпоративными общими ресурсами.

Создание корня DFS

В качестве типа корня DFS можно выбрать доменный корень или автономный корень. Доменный корень опубликует себя в Active Directory, в то время как автономный корень — нет. Это фундаментальное отличие является решающим фактором того, какой объем функциональности вы получите. Имейте в виду, что доменный корень DFS должен располагаться на контроллере домена, поэтому предполагается наличие Active Directory. Одно из наиболее важных преимуществ возможности публикации в Active Directory заключается в том, что доменные корни могут иметь реплики, а реплика корня позволяет хранить этот корень на любом контроллере домена, что значительно повышает отказоустойчивость. Поскольку корни требуют для реплик такого уровня наличие среды Active Directory, автономные корни не могут иметь реплики. В следующем упражнении мы будем использовать тестовый сервер `BF1` в качестве сервера пространства имен, и выберем эту опцию на соответствующем этапе.

Начнем с открытия окна DFS Management (Управление DFS), показанного на рис. 14.27, чтобы приступить к работе с функциями DFS, которые мы вскоре опишем.

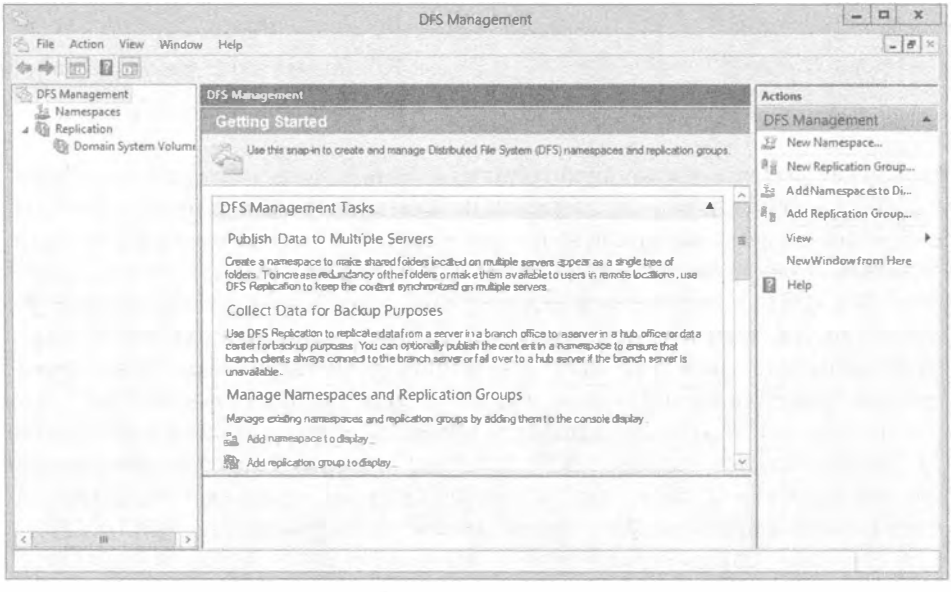


Рис. 14.27. Окно DFS Management

Создать новое пространство имен в окне DFS Management можно двумя путями. Можно выбрать в меню Action (Действие) пункт New Namespace (Создать пространство имен) или же можно щелкнуть правой кнопкой мыши на элементе Namespaces (Пространства имен) и выбрать в контекстном меню такой же пункт. В результате запустится мастер создания пространства имен (New Namespace Wizard), который проведет вас через весь процесс.

1. Щелкнув на кнопке Browse (Обзор), найдите нужный сервер или введите его имя напрямую (рис. 14.28).

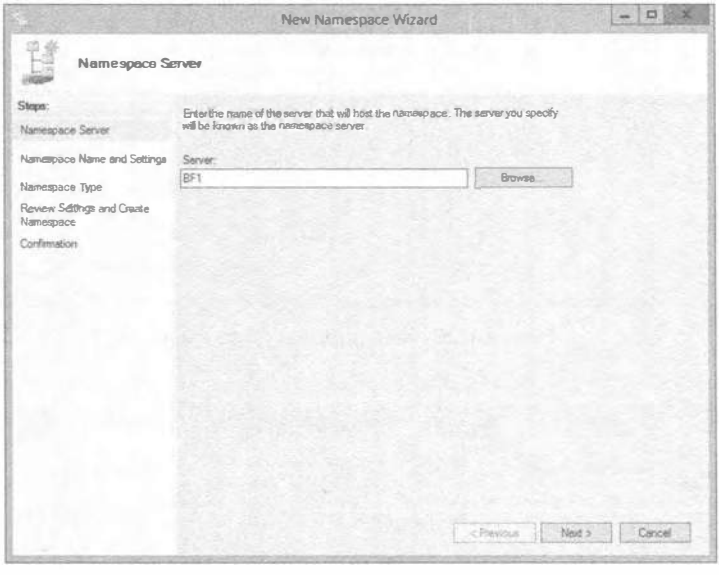


Рис. 14.28. Новый сервер пространства имен

Использование мастеров

Мы рекомендуем пользоваться мастерами до тех пор, пока вы не освоитесь с процессом; эта рекомендация справедлива для всех редакций Windows Server 2012.

2. Назначьте имя пространству имен, как показано на рис. 14.29. Это имя будет появляться после имени сервера, и вдобавок применяться в качестве имени для коллекции файлов и папок, добавленных в пространство имен.

   Теперь необходимо указать тип создаваемого пространства имен. На выбор доступно пространство имен, основанное на домене, и автономное пространство имен. Пространство имен, основанное на домене, допускает хранение на одном и более серверов пространств имен. Автономное пространство имен предполагает его размещение на единственном сервере пространств имен.

3. В данном примере выберите на экране Namespace Type (Тип пространство имен) автономное пространство имен (рис. 14.30). Позже вы сможете добавить в него файлы и папки.

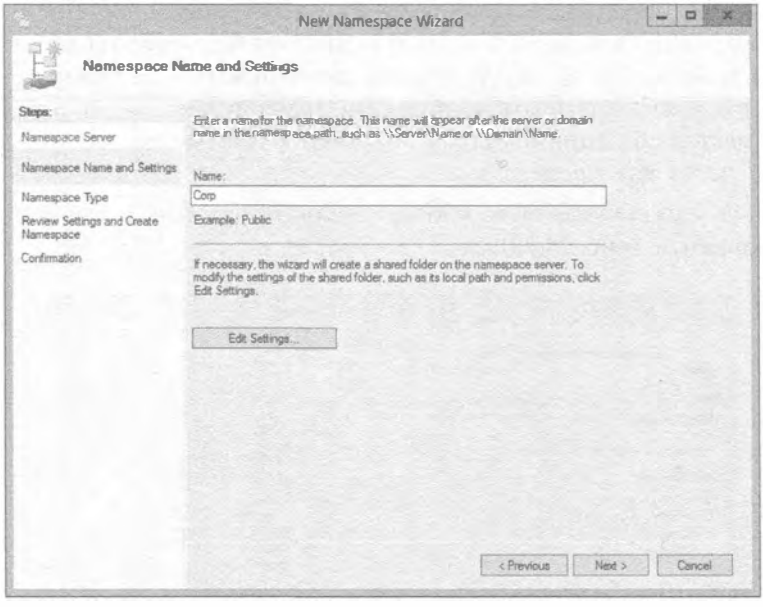


Рис. 14.29. Имя пространства имен

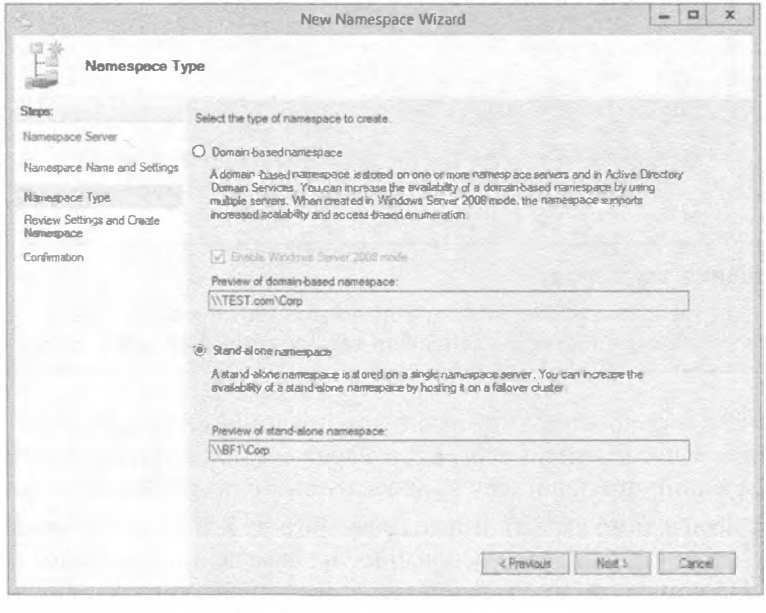


Рис. 14.30. Экран Namespace Type

На последнем экране, Review Settings and Create Namespace (Просмотр настроек и создание пространства имен), отображаются все настройки, которые необходимо подтвердить, чтобы пространство имен было создано (рис. 14.31).

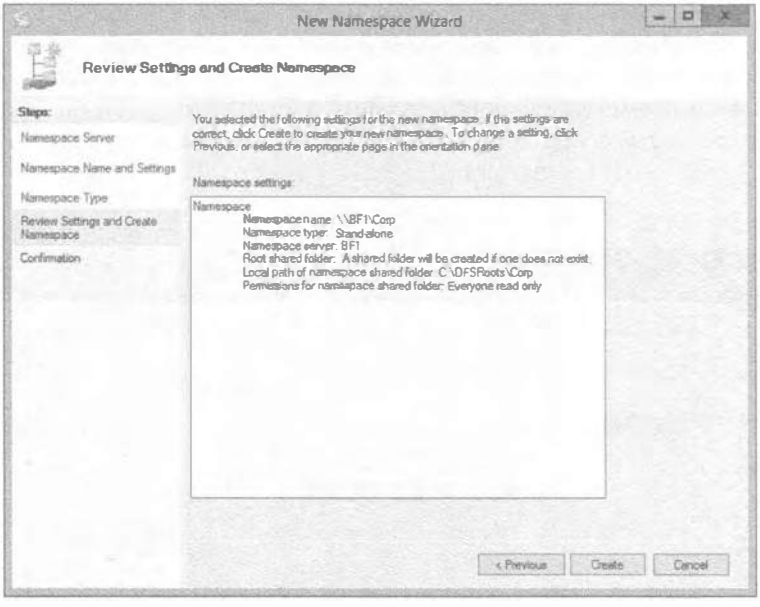


Рис. 14.31. Экран Review Settings and Create Namespace

4. Если настройки выбраны правильно, щелкните на кнопке Create (Создать), чтобы создать пространство имен. Отобразится экран Confirmation (Подтверждение), приведенный на рис. 14.32.

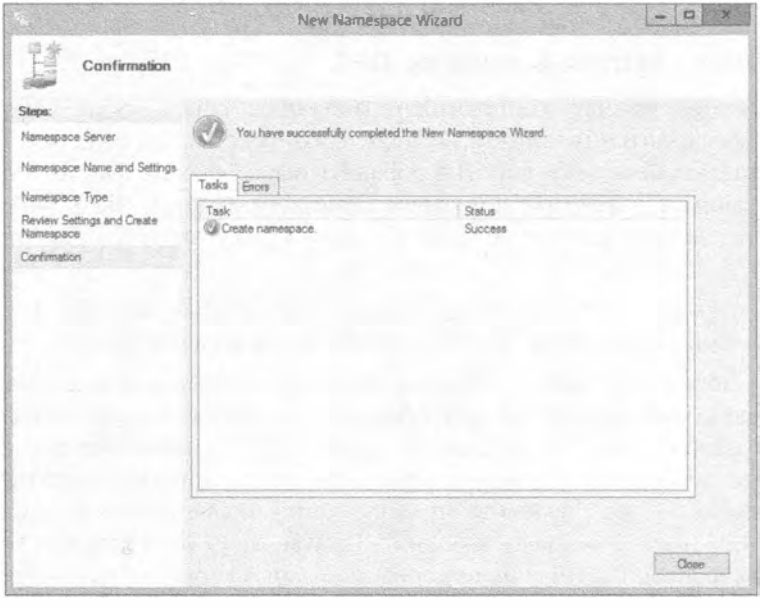


Рис. 14.32. Экран Confirmation

Процесс создания пространства имен может занять некоторое время; однако, после его завершения вы уже довольно далеко продвинулись в решении задачи сбора файлов и папок в одном логически общем месте внутри серверной среды с единственным именем, упрощающим к нему доступ. В области Shares (Общие ресурсы) окна диспетчера серверов вы увидите созданную папку `Corp` с локальным путем `c:\DFSRoots\Corp` (рис. 14.33).

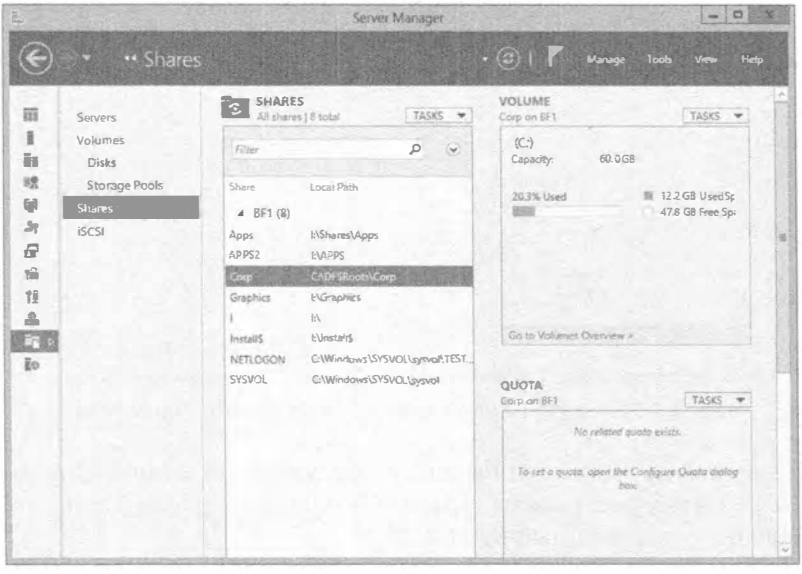


Рис. 14.33. Путь к корню DFS

Добавление ссылок в корень DFS

Внутрь одного общего корня можно добавлять ссылки или файлы и папки. Для этого понадобится щелкнуть на пункте контекстного меню Add Folder Target (Добавить конечный объект папки) и добавить все желаемые файлы и папки. Итак, давайте создадим новую папку и добавим в нее конечные файлы и папки.

В качестве демонстрации создадим новую папку внутри пространства имен `Corp`.

1. Находясь в консоли DFS Management, щелкните на пункте New Folder (Создать папку) в области Actions (Действия) справа и назначьте ей имя.
2. Теперь добавьте конечные объекты папок. Для этого щелкните на новой папке правой кнопкой мыши и выберите в контекстном меню пункт Add Folder Target (Добавить конечный объект папки). В открывшемся диалоговом окне Add Folder Target (Добавление конечного объекта папки) щелкните на кнопке Browse (Обзор), укажите нужную папку и щелкните на кнопке OK. На рис. 14.34 показано диалоговое окно Browse for Shared Folders (Просмотр открытых папок). В случае использования разных серверов их имена будут изменяться после \\; тем не менее, в этом примере мы имеем дело только с одним сервером, т.к. выбрали автономный режим. Если применяется режим, основанный на домене, мы указали бы только один конечный объект папки.

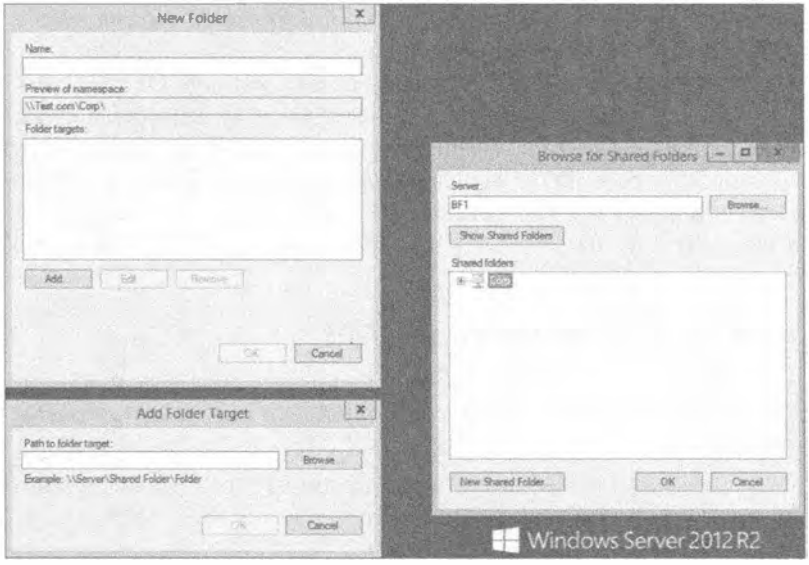


Рис. 14.34. Диалоговое окно Browse for Shared Folders

3. Щелкните на кнопке OK. Поскольку для новой папки еще не создана группа репликации, сделайте это сейчас.

Однако учтите, что DFS не является новым типом файлового сервера. В определенном смысле это вообще не файловый сервер — напротив, это метод размещения своего рода "оглавления" для группы существующих общих файловых ресурсов и указание клиентам на этот источник информации, когда они нуждаются в подключении к общему ресурсу, на который есть ссылка в данном оглавлении. Файловая система DFS вовсе *не* создает самостоятельно общие файловые ресурсы; сначала вы должны создать все общие файловые ресурсы на различных серверах и только *затем* использовать DFS для привнесения в них определенного порядка. Чтобы подчеркнуть этот момент, вот еще один факт о DFS: общие файловые ресурсы не обязательно должны быть общими файловыми ресурсами Windows NT, Windows Server 2003 или Windows Server 2008. При наличии на компьютере клиентского программного обеспечения для Unix NFS, Banyan VINES и Novell NetWare вы могли бы создать "общий ресурс" DFS, указывающий только на тома NFS, VINES и NetWare! Файловая система NFS будет рассматриваться следующей, но прежде нужно закончить с DFS.

Но не значит ли это, что новый корень DFS, т.е. "оглавление", образует новую единую точку отказа? Если один сервер, на котором находится корень — место, куда все пользователи обращаются за своими ресурсами — перестанет функционировать, то и пользователи утратят возможность работы, не так ли? Не обязательно. В сочетании с Active Directory корни DFS можно сделать отказоустойчивыми. Вместо размещения реального, физического корня на одном сервере он может быть сохранен в среде Active Directory, поддерживаемой всеми контроллерами домена. После этого, если один из серверов, содержащих корень — в Active Directory — потерпит отказ, пользователи будут автоматически направлены в другое местоположение для извлечения информации корня безо всякой заминки.

Мы еще раз подчеркиваем функцию DFS. *Отказоустойчивость DFS* не означает резервное копирование данных в общих файловых ресурсах. Она лишь означает резервное копирование "оглавления", предлагаемого корнем DFS. Если компьютер, на котором размещен корень DFS, перестанет работать (приносим свои извинения за постоянное акцентирование внимания на этом моменте, но вполне реально, что машина, хранящая корень DFS, *не содержит ни единого байта из общих файлов*, а только указатели на серверы, где размещены такие файлы), то найдется другой компьютер, который возьмет на себя роль "сервера оглавления" или, выражаясь языком Windows Server 2012, корня DFS.

Конфигурирование репликации DFS

Можете ли вы как-то защитить общие файловые ресурсы и их данные путем внедрения определенного вида отказоустойчивости? Да, это можно сделать с помощью репликации.

1. Откройте консоль DFS Management и щелкните на узле Replication (Репликация) внутри узла Namespaces (Пространства имен), как показано на рис. 14.35.

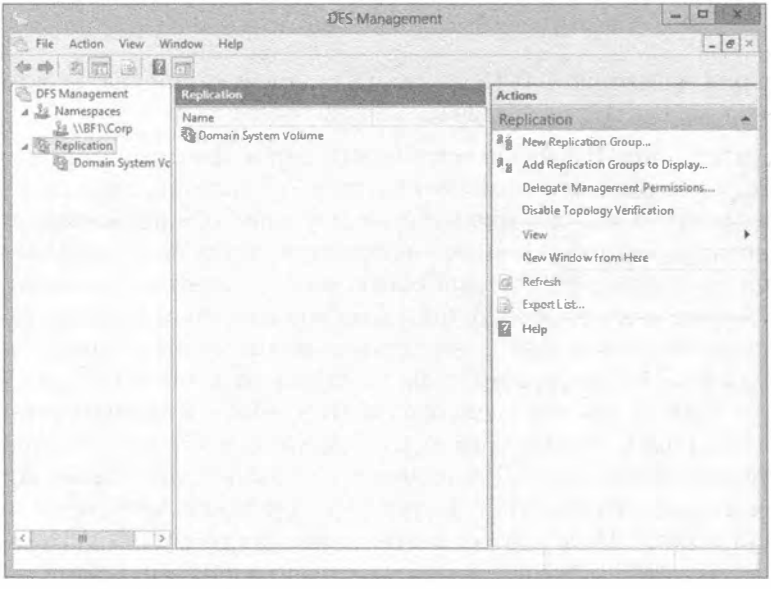


Рис. 14.35. Область Replication консоли DFS Management

2. В области Actions (Действия) щелкните на пункте New Replication Group (Создать группу репликации). Одной из замечательных особенностей Windows Server 2012, которую мы пока специально не отмечали, является применение мастеров и их внешний вид. Открыв окно мастера, обратите внимание, что все шаги четко перечислены в колонке слева. Это помогает планировать действия, поскольку вы знаете, чего ожидать следующим — больше не бывает так, что после щелчка на кнопке OK или Next (Далее) обнаруживается нечто совершенно неожиданное. Кроме того, эти шаги снабжены гораздо лучшими пояснениями, чем в предшествующих версиях сервера.

Как бы то ни было, давайте возвратимся к работе. На первом экране мастера создания группы репликации (New Replication Group Wizard) доступны два переключателя — Multipurpose replication group (Многоцелевая группа репликации) и Replication group for data collection (Группа репликации для сбора данных). Если вы используете пространство имен, основанное на домене, или автономное пространство имен, то должны оставить без изменений переключатель, выбранный по умолчанию, т.е. Multipurpose replication group. Если же вы хотите реплицировать данные для их резервного копирования или "собирать" данные, скажем, на сервере концентратора, то выберите переключатель Replication group for data collection.

3. Оставьте выбранным переключатель Multipurpose replication group.
4. На экране Name and Domain (Имя и домен) необходимо назначить имя группе репликации. Укажите в качестве имени `CorpRep` (рис. 14.36).

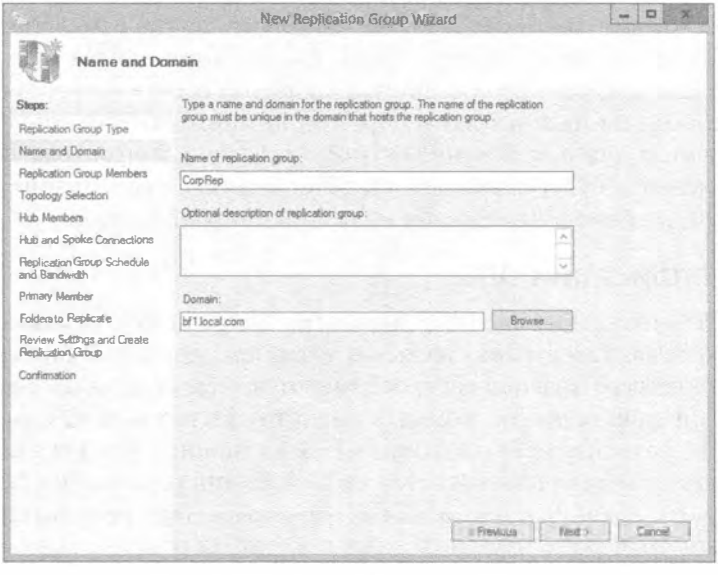


Рис. 14.36. Экран Name and Domain

5. Далее понадобится добавить серверы, которые будут членами группы репликации. Выбор серверов должен быть обдуманным, потому что вы увеличиваете объем данных, циркулирующих между такими серверами.

Ожидание репликации

Изменения конфигурации не применяются немедленно ко всем членам. Новая конфигурация должна быть реплицирована на все контроллеры домена, и каждый член группы репликации должен опросить ближайший к нему контроллер домена, чтобы получить эти изменения. Сколько времени потребует данные действия, зависит от задержки репликации AD DS и длительности интервала опроса (60 минут) в каждом члене. Чтобы обеспечить немедленный опрос изменений конфигурации, откройте окно командной строки и введите следующую команду на каждом компьютере, являющемся членом группы репликации: `dfsrdiag.exe pollad`.

6. Продолжите работу в мастере и сделайте выбор для топологии, сервера концентратора, целевой папки на сервере концентратора и реплицируемых папок, расписания и полосы пропускания группы репликации.
7. Просмотрите все настройки и щелкните на кнопке Create (Создать), чтобы создать группу репликации.

Используя службу репликации DFS (DFS Replication Service — DFSR), файловая система DFS может поддерживать все копии реплицированных целевых объектов в синхронизированном друг с другом состоянии. Если по ссылке у вас есть полностью динамические данные (под *динамическими* мы понимаем любые данные, которые изменяются по мере доступа к ним пользователями, например, документы Word, электронные таблицы, базы данных или что-то еще, что требует для изменения взаимодействия с пользователями), то вполне вероятно, что они не должны реплицироваться. Предположим, что Джейн и Боб редактируют один и тот же документ, но делают это в разных копиях на двух отдельных общих ресурсах. Джейн вносит свои изменения и закрывает документ, а затем Боб вносит другие изменения и сохраняет свою версию. Кто выиграет? Выиграет Боб, т.к. он сохранил документ последним. После сохранения документ реплицируется на другой общий ресурс, перезаписывая изменения, сделанные Джейн. Таким образом, помните, что если пользователь редактирует документ, получая к нему доступ по ссылке, которая ведет к реплике, то внесенные изменения будут перезаписаны при следующей репликации. Соблюдайте осторожность при применении ссылок на реплики и репликации.

Понятие репликации DFS

Сама по себе репликация проста. В автономной версии DFS репликация является ручной, и одна ссылка на реплику является хозяином. Другими словами, изменения от конкретного сервера-хозяина распространяются всем остальным сервера реплик. Если физический общий ресурс, который вы хотите удерживать в синхронизированном состоянии, находится внутри тома NTFS на машине Windows Server 2012, то репликация автоматически основывается на расписании репликации Active Directory и используется репликация с несколькими хозяевами. При репликации с несколькими хозяевами вы можете изменять файлы по любой одной ссылке на реплику, а изменения будут автоматически копироваться на другие члены. Действительно, в автоматической репликации нет такого понятия, как хозяин, после проведения начальной репликации. Первой репликации будет нужен хозяин, чтобы гарантировать, что все общие ресурсы имеют одну и ту же стартовую точку. Тем не менее, советуют не смешивать автоматическую и ручную репликацию внутри одного набора реплик.

Отсутствующая ссылка

Теперь, когда раскрыт процесс репликации, мы должны обратить внимание на то, что Active Directory и DFS реплицируются в одно и то же время. Они не совпадают, но дублируют метод своего выполнения. Однажды мы имели проблемы с репликацией и обнаружили, что после того, как скорректировали процесс репликации Active Directory, репликация FRS, или DFS в этом случае, также восстановила работоспособность. Если это не исправляет репликацию DFS, то придется провести более детальный поиск и устранение неполадок.

Управление репликацией DFS

После конфигурирования DFS потребуется пройти через несколько шагов для надлежащего управления корнями, ссылками и клиентами, которые к ним подключены. Настроив группы репликации, можете приступать к внесению необходимых изменений.

Редактирование расписания и полосы пропускания для репликации

Выполните описанные ниже задачи, чтобы внести изменения в расписание и полосу пропускания для группы репликации.

Чтобы отредактировать расписание и полосу пропускания для группы репликации, выполните следующие шаги.

1. Находясь внутри узла Replication (Репликация) дерева консоли, щелкните правой кнопкой мыши на группе репликации, расписание которой необходимо отредактировать, и выберите в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом окне щелкните на кнопке Edit Schedule (Редактировать расписание).
2. В диалоговом окне Edit Schedule (Редактирование расписания) укажите, когда репликация должна происходить, а также установите максимальный объем полосы пропускания, который она может потреблять.

Чтобы отредактировать расписание и полосу пропускания для конкретного подключения, выполните следующие шаги.

1. Находясь внутри узла Replication (Репликация) дерева консоли, выберите соответствующую группу репликации.
2. Выберите папку Connections (Подключения), щелкните правой кнопкой мыши на подключении, которое необходимо отредактировать, и выберите в контекстном меню пункт Properties (Свойства).
3. В открывшемся диалоговом окне свойств подключения перейдите на вкладку Schedule (Расписание), выберите Custom connection schedule (Специальное расписание для подключения) и щелкните на кнопке Edit Schedule (Редактировать расписание).
4. В диалоговом окне Edit Schedule (Редактирование расписания) укажите, когда репликация должна происходить, а также установите максимальный объем полосы пропускания, который она может потреблять.

Включение и отключение репликации

Временами возникает необходимость во включении и отключении групп репликации.

Чтобы отключить или включить репликацию для конкретного подключения, выполните следующие шаги.

1. Запустите диспетчер серверов и выберите в меню Tools (Сервис) пункт DFS Management (Управление DFS).
2. Находясь внутри узла Replication (Репликация) дерева консоли, выберите группу репликации, содержащую подключение, которое вы хотите отредактировать.

Реплицировать или не реплицировать

Если вы обновляете свою сеть и хотите управлять полосой пропускания, то может понадобиться отключить репликацию. Всякий раз, когда мы модернизируем серверы или сетевые устройства, мы отключаем репликацию и изменяем время репликации Active Directory. Вряд ли вы захотите создать себе проблемы, если после добавления оборудования серверы попытаются провести репликацию и потерпят неудачу. Это не только переполнит журналы ошибок, но также быстро приведет к возникновению проблем. При внесении изменений в архитектуру сети самое лучшее, что можно сделать — отключить репликацию.

3. Щелкните на папке Connections (Подключения).
4. Выполните одно из указанных ниже действий.
   - Чтобы отключить репликацию для подключения, щелкните правой кнопкой мыши на подключении и выберите из контекстного меню пункт Disable (Отключить).
   - Чтобы включить репликацию для подключения, щелкните правой кнопкой мыши на подключении и выберите из контекстного меню пункт Enable (Включить).

Поддержка подключений

В Microsoft не поддерживают однонаправленные подключения для репликации DFS. Создание однонаправленного подключения для репликации может вызвать множество проблем, в числе которых ошибки топологии проверки работоспособности, проблемы со ступенчатыми изменениями, а также проблемы с базой данных репликации DFS. Чтобы создать однонаправленное подключение, вместо этого сделайте реплицируемую папку на соответствующем члене группы репликации доступной только для чтения.

Включение и отключение репликации на конкретном члене

Иногда может понадобиться включить или отключить репликацию для конкретных членов группы репликации. На повестке дня должно стоять особое внимание. После включения ранее отключенный член должен выполнить начальную репликацию реплицируемой папки. Начальная репликация приводит к передаче около 1 Кбайт данных для каждого файла или папки в реплицируемой папке, и любые модифицированные или новые файлы, появившиеся в члене группы репликации, будут перемещены на нем в папку `DfsrPrivate\PreExisting` и впоследствии заменены авторитетными файлами из другого члена. Если все члены отключены, тогда главным членом становится первый включенный член, что может оказаться не тем, что требуется.

Общий доступ или публикация

Изменения членства не применяются немедленно. Изменения членства должны реплицироваться на все контроллеры домена, и членам группы репликации понадобится опрашивать ближайший контроллер домена, чтобы получить изменения. Количество времени, сколько это может занять, зависит от задержки репликации AD DS и короткого интервала опроса (пять минут) на члене.

Общий доступ или публикация реплицированной папки

После того как мастер New Replication Group Wizard завершен, может понадобиться открыть общий доступ или опубликовать реплицированную папку. Для этого папка должна быть добавлена в существующее или новое пространство имен.

Чтобы открыть общий доступ к реплицированной папке без ее публикации в пространстве DFS, выполните следующие шаги.

1. Запустите диспетчер серверов и выберите в меню Tools (Сервис) пункт DFS Management (Управление DFS).
2. Находясь внутри узла Replication (Репликация) дерева консоли, щелкните на группе репликации, содержащей реплицированную папку, к которой вы хотите открыть общий доступ.
3. На вкладке Replicated Folders (Реплицированные папки) панели деталей щелкните правой кнопкой мыши на реплицированной папке, к которой вы хотите открыть общий доступ, и выберите в контекстном меню пункт Share and Publish in Namespace (Открыть общий доступ и опубликовать в пространстве имен).
4. В мастере открытия общего доступа и публикации реплицированной папки (Share and Publish Replicated Folder Wizard) выберите переключатель Share the replicated folder (Открыть общий доступ к реплицированной папке) и затем следуйте всем указаниями мастера.

Чтобы открыть общий доступ к реплицированной папке и опубликовать ее в пространстве DFS, выполните следующие шаги.

1. Запустите диспетчер серверов и выберите в меню Tools (Сервис) пункт DFS Management (Управление DFS).
2. Находясь внутри узла Replication (Репликация) дерева консоли, щелкните на группе репликации, содержащей реплицированную папку, к которой вы хотите открыть общий доступ.
3. На вкладке Replicated Folders (Реплицированные папки) панели деталей щелкните правой кнопкой мыши на реплицированной папке, к которой вы хотите открыть общий доступ, и выберите в контекстном меню пункт Share and Publish in Namespace (Открыть общий доступ и опубликовать в пространстве имен).
4. В мастере открытия общего доступа и публикации реплицированной папки (Share and Publish Replicated Folder Wizard) выберите переключатель Share and publish the replicated folder in a namespace (Открыть общий доступ и опубликовать реплицированную папку в пространстве имен) и затем следуйте всем указаниями мастера.

Проверка требований безопасности

Для выполнения этой процедуры вы должны удовлетворить требования безопасности для управления репликацией и пространствами имен DFS. Если общий доступ к папкам открывается с помощью мастера Share and Publish Replicated Folder Wizard, то вы должны иметь членство в локальной группе `Administrators` на серверах, где открывается общий доступ к каждой папке.

Случаи практического использования

Перед тем, как приступать к настройке корня, созданию ссылок и реорганизации методов доступа пользователей к своим ресурсам, давайте кратко рассмотрим несколько случаев, когда DFS действительно повышает ценность сети. Помните, что речь не идет о работе с какими-то новыми средствами, а только о том, чтобы упростить жизнь, повысить эффективность и увеличить продуктивность.

Объединенные ресурсы предприятия

Пример DFS, с которым мы работали в этой главе, является хорошей демонстрацией объединения ресурсов предприятия. Вы можете взять все общие ресурсы сети и поместить их в один логический общий ресурс. Тогда вместо того, чтобы помнить, на каком логическом диске находится тот или иной ресурс, необходимо знать только папку. Важно также то, что настройка DFS в действительности не оказывает никакого влияния на конфигурацию сети. Вы можете строить и экспериментировать с конфигурациями DFS целый день в производственной среде, и никто даже не заподозрит о ее существовании. Все старые общие ресурсы сети останутся на своих местах, данные не будут затронуты, а пользователи не увидят ничего отличающегося. Как только новая конфигурация DFS станет готовой, наступит трудная часть процесса — изменение у пользователей отображений дисков с одного диска для одного общего ресурса на один диск для всех общих ресурсов. Не стоит недооценивать такую задачу. Это больше, чем просто отображение новой буквы диска на корень DFS. Все приложения должны будут знать, что они больше не находятся на диске `X`, например, а вместо этого располагаются на диске `Y`.

Управление жизненным циклом

Хорошая новость заключается в том, что с DFS вы в последний раз будете иметь дело с изменением отображений дисков. Когда возникнет потребность переместить данные из одного сервера на другой, чтобы вывести из эксплуатации старый сервер и ввести вместо него новый, вам не придется заниматься резервным копированием данных, очисткой сервера, построением нового сервера с тем же именем и восстановлением данных с целью воссоздания прежней физической машины. С помощью DFS вы можете установить новый сервер и сконфигурировать его как отключенную ссылку на реплику для общего ресурса, который вы хотите "переместить". Убедившись, что все данные были успешно перемещены, переведите новый сервер в онлайновый режим и отключите старый сервер. Пользователи даже не узнают, что они уже попадают на новый сервер. Файловая система DFS обрабатывает все безо всяких усилий.

Исследование сетевой файловой системы

Мы рассмотрели DFS, так что теперь вам известно, насколько удобным может быть указание на единственное логическое местоположение для нахождения множества файлов и папок. Теперь вы можете разговаривать с животными — или открывать общий доступ к файлам для всяких липовых операционных систем. Конечно, это шутка — вам нужна возможность общего доступа к файлам в рамках всей организации, и если в ней присутствуют машины с другими операционными системами, то в Windows Server 2012 предлагается для этого соответствующий инструмент. Данный раздел будет иметь несколько технический характер, и вы должны учитывать, что мо-

жете в этом не нуждаться; тем не менее, если вы все же испытываете потребность в такой работе, то должны следовать приведенным здесь указаниям. При добавлении роли File and Storage Services к серверу понадобится выбрать NFS. Вы должны были сделать это в предыдущем разделе, посвященном DFS. В противном случае возвратитесь к роли File and Storage Services и добавьте компонент NFS, отметив связанный с ним флажок. Итак, мы начнем обсуждение с того, что собой представляет файловая система NFS, и что может предоставить Windows Server 2012 в этом отношении.

Сетевая файловая система (Network File System — NFS) является решением общего доступа к файлам для организаций, которые имеют смешанные среды машин с Windows и Unix/Linux. Файловая система NFS дает возможность открывать общий доступ к файлам между указанными разными платформами при функционирующей операционной системе Windows Server 2012. Службы NFS в Windows Server 2012 включают следующие возможности и усовершенствования.

- **Поиск в Active Directory.** Вы имеете возможность применять Windows Active Directory для доступа к файлам. Расширение схемы Identity Management for Unix (Управление удостоверениями для Unix) для Active Directory содержит поля идентификатора пользователя Unix (Unix user identifier — UID) и идентификатора группы (group identifier — GID). Это позволяет службам Server for NFS (Сервер для NFS) и Client for NFS (Клиент для NFS) просматривать отображения учетных записей пользователей Windows на Unix прямо из служб домена Active Directory (Active Directory Domain Services). Компонент Identity Management for Unix упрощает управление отображением учетных записей пользователей Windows на Unix в Active Directory Domain Services.
- **Улучшенная производительность сервера.** Службы для NFS включают драйвер фильтра файлов, который значительно сокращает общие задержки при доступе к файлам на сервере.
- **Поддержка специальных устройств Unix.** Службы для NFS поддерживают специальные устройства Unix (`mknod`).
- **Расширенная поддержка Unix.** Службы для NFS поддерживают следующие версии Unix: Sun Microsystems Solaris версии 9, Red Hat Linux версии 9, IBM AIX версии 5L 5.2 и Hewlett Packard HP-UX версии 11i. Однако более новые версии, несомненно, будут поддерживаться в будущем.

Вы можете пользоваться инструментами командной строки, но в Windows Server 2012 доступна также консоль Services for Network File System (Службы для сетевой файловой системы), окно которой показано на рис. 14.37. Инструменты командной строки будут демонстрироваться далее в этой главе.

Один из наиболее распространенных сценариев, который создает необходимость в применении NFS, предусматривает открытие доступа пользователям в среде Windows к системе планирования ресурсов предприятия (enterprise resource planning — ERP), основанной на Unix. Находясь в системе ERP, пользователи могут создавать отчеты и/или экспортировать финансовые данные в Microsoft Excel для дальнейшего анализа. Файловая система NFS позволяет обращаться к этим файлам, по-прежнему находясь в среде Windows, что сокращает потребность в наличии специальных технических навыков и снижает временные затраты на экспорт файлов с использованием сценария Unix и последующий их импорт в определенное приложе-

ние Windows. Может также возникнуть ситуация, когда у вас имеется система Unix, которая применяется для хранения файлов в какой-то сети хранения данных (storage area network — SAN). Запуск служб NFS на машине Windows Server 2012 позволяет пользователям в организации получать доступ к сохраненным там файлам безо всяких накладных расходов, связанных со сценариями на стороне Unix.

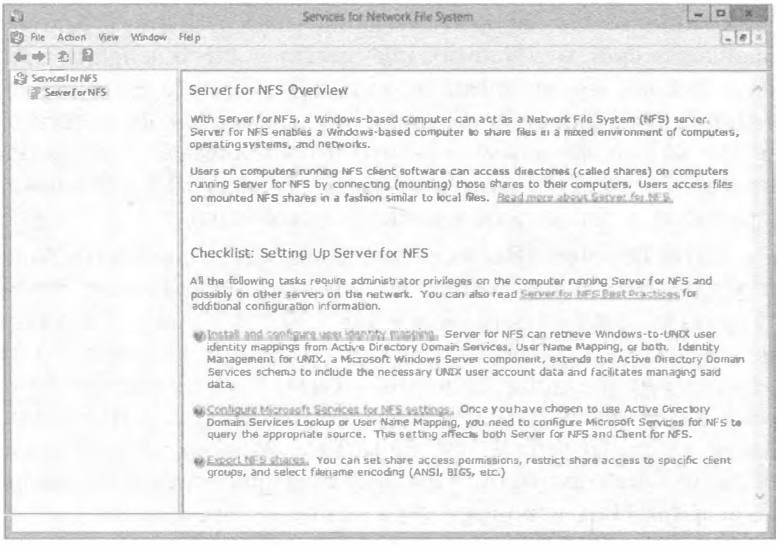


Рис. 14.37. Консоль Services for the Network File System

Компоненты служб NFS

Доступны следующие два компонента служб NFS.

- **Server for NFS (Сервер для NFS).** Обычно компьютер, основанный на Unix, не может обращаться к файлам, расположенным на компьютере, основанном на Windows. Тем не менее, компьютер, на котором функционирует Windows Server 2012 R2 и компонент Server for NFS, может действовать в качестве файлового сервера для компьютеров с Windows и Unix.
- **Client for NFS (Клиент для NFS).** Обычно компьютер, основанный на Windows, не может обращаться к файлам, находящимся на компьютере, основанном на Unix. Тем не менее, компьютер, на котором функционирует Windows Server 2012 R2 и компонент Client for NFS, может получать доступ к файлам, которые хранятся на сервере NFS, основанном на Unix.

Службы NFS в Windows Server 2012 R2 также имеют инструменты администрирования, которые можно использовать для управления NFS; эти функции администрирования находятся в оснастке консоли управления Microsoft (Microsoft Management Console — MMC), обсуждаемой повсеместно в настоящей книге.

Перед применением NFS должны быть удовлетворены предварительные условия и сделаны определенные допущения. Вы должны обладать базовым пониманием сред Windows и Unix, располагать знанием безопасности файлов и уметь администрировать Windows Server 2012 R2. Еще одним требованием является хорошее понимание того, в чем нуждаются пользователи.

Меры предосторожности, касающиеся NFS

До установки служб NFS вы должны удалить любые ранее установленные компоненты NFS, такие как компоненты NFS, которые были включены в состав Services for Unix. Мы рекомендуем создать резервную копию или внести запись в конфигурацию, прежде чем удалять компоненты NFS, чтобы можно было восстановить эту конфигурацию Services for NFS.

По умолчанию компонент Server for NFS поддерживает клиентские компьютеры Unix, использующие NFS версии 2 или 3. Однако это можно переопределить и сконфигурировать Server for NFS на разрешение доступа только клиентам с NFS версии 2. За инструкциями обращайтесь в раздел "Configuring Server for NFS" ("Конфигурирование Server for NFS") в справке по службам NFS. Компонент Client for NFS поддерживает обе версии NFS, и это настройке не подлежит.

Вам понадобится собрать список пользователей, групп и компьютеров, которые будут применяться. Прежде чем развернуть NFS и заявить о своих талантах, начните с тестового идентификатора на серверах Windows и Unix. Первым делом создайте учетные записи пользователей на обоих серверах и затем установите компонент Server for NFS, выполнив следующие шаги.

1. Запустите диспетчер серверов и выберите в меню Manage (Управление) пункт Add Roles and Features (Добавить роли и компоненты).
2. Откроется окно мастера добавления ролей и компонентов (Add Roles and Features Wizard). На экране Installation Type (Тип установки) оставьте выбранным переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) и щелкните на кнопке Next (Далее).
3. На экране Server Selection (Выбор сервера) выберите сервер для установки роли и щелкните на кнопке Next.
4. Отыщите роль Server for NFS (Сервер для NFS), развернув узел File and Storage Services (Службы файлов и хранилища) и раскрыв папку File and iSCSI Services (Службы файлов и iSCSI), после чего отметьте для нее флажок. Для продолжения щелкните на кнопке Next.
5. Выберите любые дополнительные компоненты, которые хотите добавить к серверу в настоящий момент. Обратите внимание, что на этом же экране можно было бы добавить компонент Client for NFS, но в данном упражнении мы устанавливаем только Server for NFS. Щелкните на кнопке Next, чтобы перейти на экран Confirmation (Подтверждение).
6. Просмотрите роли и компоненты, которые будут установлены, и щелкните на кнопке Install (Установить).
7. Когда установка завершится, будет отображен экран Results (Результаты). Щелкните на кнопке Close (Закрыть).

Теперь необходимо сконфигурировать аутентификацию NFS и создать общую папку NFS. Удостоверьтесь, что для этого используется Windows Server 2012 со всеми актуальными обновлениями безопасности. Теперь, когда компонент Server for NFS установлен, вы получаете новую вкладку под названием NFS Sharing (Общий доступ NFS) в диалоговом окне свойств папки.

Выполните перечисленные ниже шаги, чтобы создать общую папку NFS.

1. Создайте на компьютере с функционирующей ролью Server for NFS папку, которая будет использоваться в качестве общей папки NFS.
2. Щелкните правой кнопкой мыши на созданной папке и выберите в контекстном меню пункт Properties (Свойства).
3. В открывшемся диалоговом окне свойств перейдите на вкладку NFS Sharing (Общий доступ NFS) и щелкните на кнопке Manage NFS Sharing (Управлять общим доступом NFS).
4. В диалоговом окне NFS Advanced Sharing (Расширенный общий доступ NFS) отметьте флажок Share this folder (Открыть общий доступ к этой папке). По умолчанию имя общего ресурса совпадает с именем папки. Если вы хотите разрешить анонимный доступ, отметьте флажок Allow anonymous access (Разрешить анонимный доступ).
5. Щелкните на кнопке Permissions (Разрешения), в открывшемся диалоговом окне щелкните на кнопке Add (Добавить) и затем выполните одно из следующих действий.
   - В списке Names (Имена) щелкните на клиентах и группах, которые хотите добавить, и щелкните на кнопке Add (Добавить).
   - В области Add Names (Добавить имена) введите имена клиентов и групп, которые хотите добавить, разделяя имена в списке точками с запятой (;).
6. В списке Type of Access (Тип доступа) щелкните на типе доступа, который хотите предоставить выбранным клиентам и группам.
7. Отметьте флажок Allow Root Access (Разрешить доступ пользователю `root`), если хотите, чтобы пользователь, идентифицированный как `root`, имел доступ не как анонимный пользователь. По умолчанию идентификатор пользователя `root` принудительно устанавливается в идентификатор анонимного пользователя.
8. В списке Encoding (Кодирование) щелкните на типе кодирования имен каталогов и файлов, который должен применяться для выбранных клиентов и групп. Соблюдайте здесь согласованность!
9. Два раза щелкните на кнопке OK и затем щелкните на кнопке Apply (Применить) и OK.

Важной особенностью Windows Server 2012 R2 является возможность использования PowerShell для выполнения тех же самых задач, которые только что делались с помощью пользовательского интерфейса. Давайте посмотрим, как применять PowerShell для установки роли NFS на сервере и для создания общего файлового ресурса NFS.

1. Откройте окно Windows PowerShell через панель задач от имени учетной записи администратора.
2. Запустите следующие команды, чтобы установить роль NFS на сервере:

```
PS C:\> Import-Module ServerManager
PS C:\> Add-WindowsFeature FS-NFS-Services
PS C:\> Import-Module NFS
```

3. Запустите приведенную ниже команду, чтобы создать новый общий файловый ресурс NFS:

```
PS C:\> New-NfsShare -Name "NFSshare01" -Path "C:\shares\NFSshare01"
```

4. Для просмотра всех новых командлетов PowerShell, относящихся к NFS, которые доступны в Windows Server 2012 R2, выполните следующую команду:

```
PS C:\> Get-Command -Module NFS
```

Установка стандартных разрешений

Теперь вы будете применять ряд стандартных разрешений к создаваемым файлам и папкам и затем внесете небольшие изменения в настройки брандмауэра на сервере, который используется для NFS. Помните, что этот сервер должен находиться за основными брандмауэрами организации и быть защищенным. Для функционирования NFS вам понадобится открыть все перечисленные ниже порты.

Службы для компонента NFS	Для чего открывается порт	Протокол	Порт
User Name Mapping (Отображение имен пользователей) и Server for NFS (Сервер для NFS)	Portmapper (Средство отображения портов)	TCP, UDP	111
Server for NFS (Сервер для NFS)	Network Status Manager (Диспетчер состояния сети)	TCP, UDP	1039
Server for NFS (Сервер для NFS)	Network Lock Manager (Диспетчер блокировок сети)	TCP, UDP	1047
Server for NFS (Сервер для NFS)	NFS Mount (Монтирование NFS)	TCP, UDP	1048
Server for NFS (Сервер для NFS)	Network File System (Сетевая файловая система)	TCP, UDP	2049

Требования к портам

В зависимости от имеющихся требований, может понадобиться открыть порты TCP (Transmission Control Protocol — протокол управления передачей), порты UDP (User Datagram Protocol — протокол дейтаграмм пользователя) либо те и другие. В целях тестирования мы рекомендуем открыть транспорт TCP и UDP для всех протоколов.

Чтобы открыть порты в брандмауэре, выполните следующие шаги.

1. Находясь в системе компьютера, на котором запущена служба User Name Mapping или Server for NFS, нажмите комбинацию клавиш <Windows+R>. В окне Run (Выполнить) введите **`firewall.cpl`** и щелкните на кнопке OK.
2. Перейдите на вкладку Exceptions (Исключения) и щелкните на кнопке Add Port (Добавить порт).
3. В поле Name (Имя) введите имя открываемого порта, как упоминалось выше во врезке "Установка стандартных разрешений".
4. В поле Port number (Номер порта) введите соответствующий номер порта.
5. Выберите переключатель TCP или UDP и щелкните на кнопке OK.

6. Повторите шаги 2–5 для каждого открываемого порта и по завершении щелкните на кнопке OK.

Затем потребуется добавить программу `mapsvc.exe` в список исключений брандмауэра.

> **Меры предосторожности, касающиеся брандмауэра**
>
> Перед внесением изменений в настройки брандмауэра удостоверьтесь, что файловый сервер, применяемый для NFS, хорошо защищен и находится за основными производственными брандмауэрами. Эти указания предполагают, что вы никогда не будете вносить такие изменения на пограничном сервере внутри демилитаризованной зоны (DMZ).

1. Находясь в системе компьютера, на котором запущена служба User Name Mapping, нажмите комбинацию клавиш <Windows+R>. В окне Run (Выполнить) введите **`firewall.cpl`** и щелкните на кнопке OK.
2. Перейдите на вкладку Exceptions (Исключения) и щелкните на кнопке Add Program (Добавить программу).
3. Щелкните на кнопке Browse (Обзор), выберите файл `mapsvc.exe` и затем щелкните на кнопке Open (Открыть). По умолчанию этот файл находится в `%windir%\System32`.
4. В целях тестирования щелкните на кнопке Change scope (Изменить область действия), в открывшемся диалоговом окне выберите переключатель Any computer (Любой компьютер) и щелкните на кнопке OK.
5. Щелкните на кнопке OK еще два раза.

Процесс практически подошел к концу. Далее необходимо включить общий доступ к файлам и принтерам на компьютере, выполняющем службы NFS. Вероятно, вы уже знаете, как это сделать, раз уж дочитали до этого места, но ради завершенности ниже перечислены соответствующие шаги.

1. Находясь в системе компьютера, на котором запущены службы Services for NFS, нажмите комбинацию клавиш <Windows+R>. В окне Run (Выполнить) введите **`firewall.cpl`** и щелкните на кнопке OK.
2. Перейдите на вкладку Exceptions (Исключения), отметьте флажок File and Printer Sharing (Общий доступ к файлам и папкам) и щелкните на кнопке OK.
3. Повторите шаг 2 на каждом компьютере, выполняющем Services for NFS.

Перед тем, как предоставить результаты пользователям, вы наверняка захотите провести тестирование, убедившись в работоспособности всей функциональности. В следующей статье Microsoft TechNet описаны четыре теста, которые вы можете выполнить: `http://technet.microsoft.com/ru-ru/library/cc753302.aspx`.

Для конфигурирования брандмауэра можно также использовать утилиту командной строки `netsh`. На рис. 14.38 показан список доступных команд.

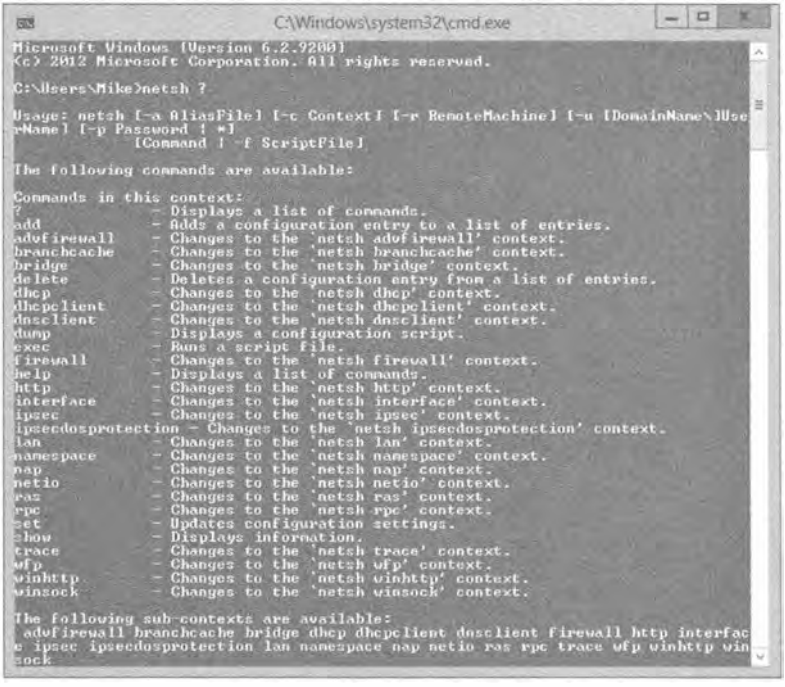


Рис. 14.38. Утилита командной строки `netsh`

Резюме

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.

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.

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`.

Глава 15

Динамическое управление доступом: общие файлы

Мы уверены, что по мере продвижения по материалу этой книги вы стали понимать обширное число функциональных средств, которые были включены в Windows Server 2012. Сейчас мы добрались до вероятно наиболее важного нового средства — динамического управления доступом (Dynamic Access Control). Эта новаторская функциональность основательно реорганизует работу администраторов файловых серверов!

Давайте начнем с короткого примера. Когда вы приступаете к работе в компании и получаете учетную запись пользователя на компьютере, то почти наверняка она будет членом стандартной группы по имени `Domain Users` (Пользователи домена). Поскольку вам требуется доступ к различным ресурсам, вы отправляете соответствующие формы запросов владельцам ресурсов, и вам предоставляется доступ, что обычно означает включение вашей учетной записи в группу доступа, которой уже выданы права на доступ к нужным ресурсам. (Например, если вас интересует доступ к финансовым данным, то общий ресурс `Finance` предоставит доступ для чтения и записи этих данных всем, кто входит в состав группы `Finance`.) По мере того, как вам будет требоваться доступ к растущему числу ресурсов, ваша учетная запись будет добавляться во все большее количество групп. С появлением новых ресурсов создаются новые группы, предназначенные для управления доступом к ним.

Подумайте о том, насколько много файловых серверов развернуто по всему миру в наши дни, и какое огромное число групп создано для управления доступом к таким общим ресурсам. Затем добавьте ко всему этому объем усилий по администрированию, направленных не только на создание, но также и на последующее их обслуживание. Именно так сегодня выглядит реальность для администраторов файловых серверов.

Позвольте нам представить динамическое управление доступом (Dynamic Access Control — DAC). Это в полном смысле слова средство нового поколения, предназначенное для защиты информации, которая должна быть безопасной, и управле-

ния доступом к ресурсам, к которым должны иметь доступ только авторизованный персонал.

Вообразите себе ситуацию, когда не особо технически подкованный финансовый директор крупной корпорации решает занести зарплаты всех начальников отделов в электронную таблицу Excel и не защищает этот файл паролем или не помешает в зашищенную папку. Недовольный работник завладеет этим документом и опубликует его всему миру. В результате в неудобное положение будет поставлена не только компания, но также и сам финансовый директор!

А теперь представьте себе мир, в котором финансовый директор совершает ту же самую глупость, но данные автоматически зашищаются, поскольку они содержат ключевые слова, которые инициируют процесс, классифицирующий данные как конфиденциальные, с возможностью доступа к ним только членам определенных групп. Тогда все было бы просто замечательно! Это и есть одна из новаторских возможностей DAC. Будем надеяться, теперь вы уловили общую картину того, что будет подробно рассмотрено, и чем вы научитесь пользоваться.

Основной момент, который вы должны запомнить: DAC не является единственным фрагментом технологии. Это решение файлового сервера. В нем собраны вместе условные выражения (например, входит ли данный пользователь в состав какой-то группы, или должен ли компьютер, из которого происходит обращение к файлу, быть присоединенным к домену), классификация файлов (такая как высокая важность для бизнес-деятельности и т.п.), а также центральные политики доступа (Central Access Policies) (централизованно управляющие всеми политиками авторизации), и с помощью Kerberos проверяет "утверждения", поступающие от пользователей. В свою очередь, эти технологии объединяются для формирования DAC и позволяют создавать центрально управляемую руководящую политику среди файловых серверов.

В этой главе вы изучите следующие темы:

- защита данных с использованием условий;
- создание нового типа утверждения и свойства ресурса;
- защита сотен серверов;
- классификация и защита данных без знания того, что они собой представляют.

Новый метод защиты общих файловых ресурсов

Мы предполагаем, что если вы читаете эту главу, то знакомы с основами обших файловых ресурсов, т.е. знаете, как их создавать и как ими управлять. Если это не так, остановитесь! Сначала вы должны возвратиться к главе 13, в которой приведены подробные объяснения. Если же вы владеете соответствующими знаниями и готовы продолжить, то вперед!

Давайте сразу приступим к делу и рассмотрим разрешения общего доступа, показанные на рис. 15.1.

Как видите, крупных изменений здесь нет. Реальная мошь при защите общих файловых ресурсов кроется в свойствах безопасности на вкладке Security (Безопасность), представленной на рис. 15.2.

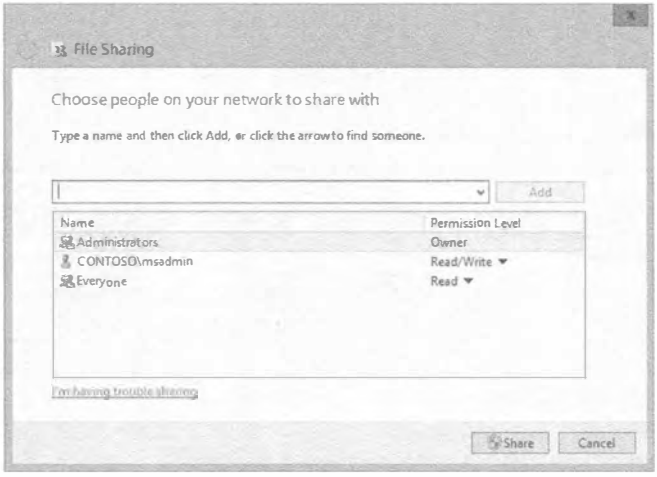


Рис. 15.1. Разрешения общего доступа к файлам в Windows Server 2012

Рис. 15.2. Вкладка Security диалогового окна свойств общего файлового ресурса

На этой вкладке Security разрешения NTFS принудительно применяются не только к папке, но также и к файлам. Однако, как вы наверняка заметили, она не выглядит сильно отличающейся от предшествующих версий Windows Server.

Поскольку это определенно дополнительное средство, оно вполне разумно доступно по щелчку на кнопке Advanced (Дополнительно), расположенной в нижней части вкладки Security (см. рис. 15.2).

На рис. 15.3 показано диалоговое окно Advanced Security Settings (Расширенные настройки безопасности) для общего файлового ресурса, и именно здесь мы можем начать конфигурирование основных аспектов DAC.

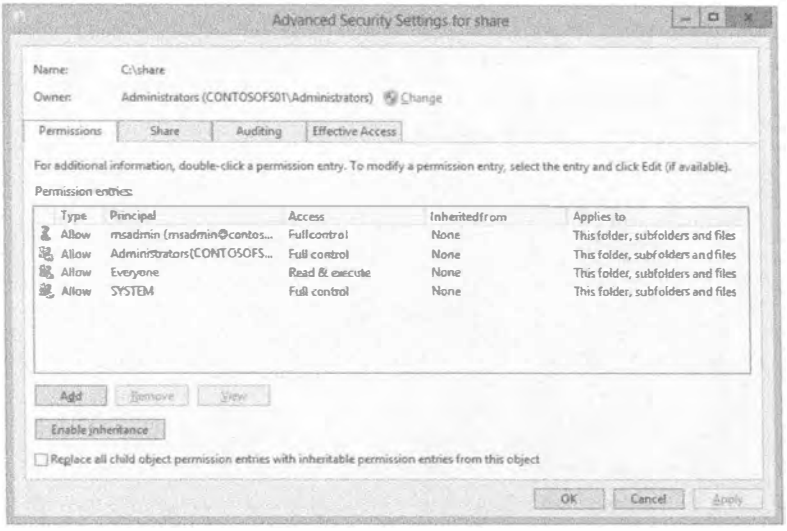


Рис. 15.3. Диалоговое окно Advanced Security Settings для общего файлового ресурса

В этом примере мы имеем дело с единственной папкой по имени `share`. Для нее открыт общий доступ только для чтения всем пользователям посредством разрешений общего доступа и доступ только для чтения через разрешения NTFS; вдобавок мы также предоставили администраторам полный доступ (Full Control). Тем не менее, на рис. 15.3 можно заметить, что участник `Everyone` (Все) имеет доступ Read & Execute (Чтение и выполнение). Теперь вы видите, что диалоговое окно Advanced Security Settings предлагает более детализированное управление, но это все еще не DAC.

Щелкните на кнопке Add (Добавить) в диалоговом окне Advanced Security Settings и откроется диалоговое окно Permission Entry for share (Запись разрешения для `share`), приведенное на рис. 15.4.

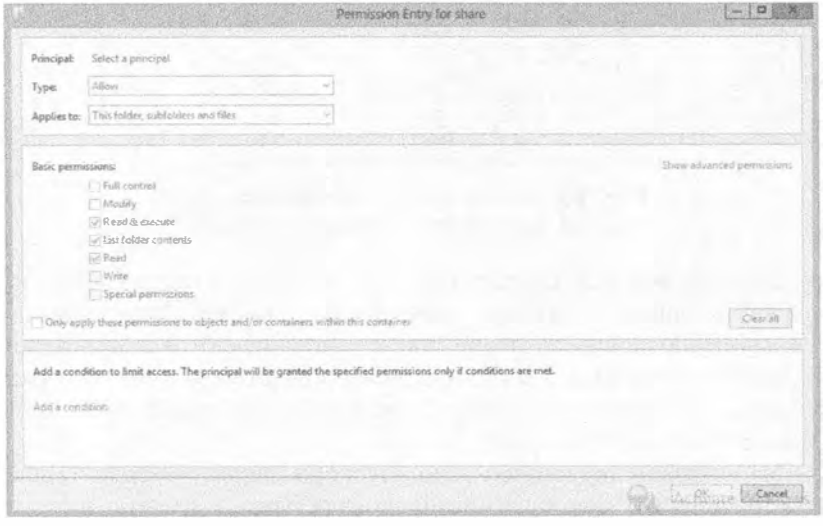


Рис. 15.4. Диалоговое окно Permission Entry for share

Первым делом вы должны выбрать участника. Участником может быть, например, учетная запись пользователя или группа, которой вы хотите назначить привилегии. До тех пор, пока не будет выбран участник, все элементы остаются затененными.

Как видите, довольно много опций выглядит знакомо по предыдущим версиям Windows Server. Однако теперь имеется новый раздел, где можно добавить условие. Вот здесь и начинается функциональность DAC: условные выражения.

После щелчка на ссылке Add a condition (Добавить условие) появляется возможность создать условие (рис. 15.5).

Рис. 15.5. Добавление условия

Первым условием является выбор между устройством и пользователем. Теперь вы можете защищать данные не только на уровне учетной записи пользователя, но также и на уровне устройства, из которого производится доступ к ресурсу. Вы можете разрешать доступ к ресурсам из корпоративного устройства, но не из домашнего ноутбука. Это позволит гарантировать безопасность данных, т.к. вы контролируете корпоративные ноутбуки и настольные компьютеры.

В примере на рис. 15.6 мы выдали пользователю по имени John McCabe (`johm@contoso.ie`) разрешения Read & Execute, List Folder Contents и Read, а также добавили условие предоставления ему доступа к общему ресурсу с компьютера, являющегося частью группы `Domain Computers` (Компьютеры домена).

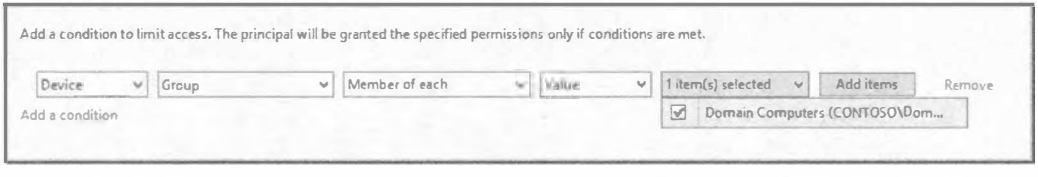


Рис. 15.6. Добавление условия в диалоговом окне Permission Entry for share

Возвратившись в диалоговое окно Advanced Security Settings, вы увидите, что добавлен новый участник с заполненным столбцом Condition (Условие), как показано на рис. 15.7. Для участника John McCabe (`johm@contoso.ie`) можно добавить дополнительные условия и применить к ним булевскую логику And (И) либо Or (Или). Операция And требует истинности всех условий. Например, можно было бы предусмотреть условие, что устройство должно входить в состав группы `Domain Computers`, и условие, что пользователь должен быть членом группы `IT Admins`. Если оба условия не удовлетворены, доступ не предоставляется. В случае Or, если одно из условий соблюдается, то доступ будет выдан. На рис. 15.8 приведен пример объединения условий с помощью And.

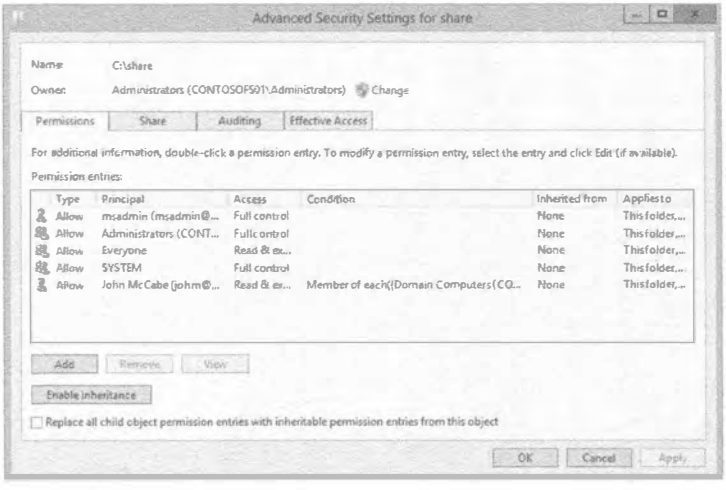


Рис. 15.7. Диалоговое окно Advanced Security Settings с заполненным столбцом Condition для пользователя по имени John McCabe (`johm@contoso.ie`)

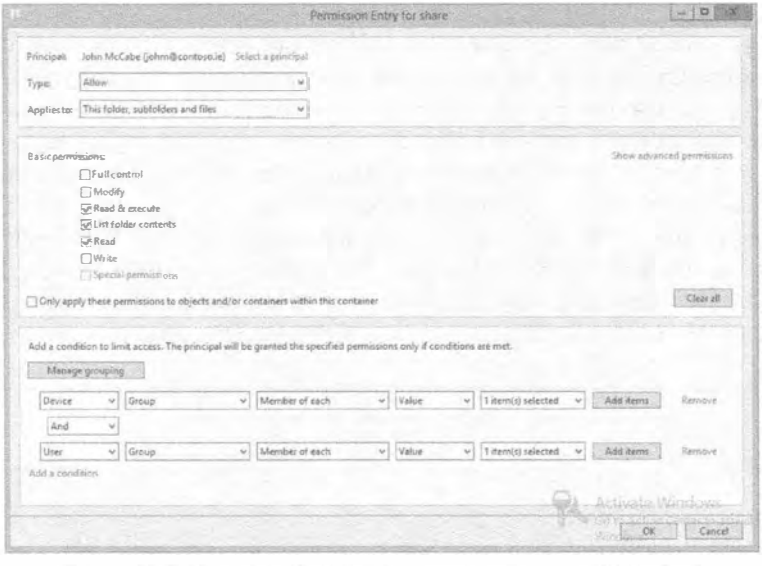


Рис. 15.8. Пример объединения условий с помощью And

Управление доступом с использованием групп и атрибутов пользователя в Active Directory

Как было показано в предыдущем разделе, мы можем выбрать участника (вспомните, что участником может быть пользователь или группа) и назначить условие, после чего на основе этого условия доступ будет разрешен или запрещен. Это возвращает нас к старой проблеме администрирования групп.

Подумайте о следующем. Насколько часто внутри крупной или даже мелкой организации очищаются группы в Active Directory, и как часто происходить доступ к привилегиям существующей пользовательской базы, чтобы удостовериться в том, что они по-прежнему допустимы? Должен ли кто-то действительно быть частью группы `IT Admins` (Администраторы IT-отдела) теперь, когда он стал водителем грузовика? Что, если теперь вы могли бы, например, изменить поле `Department` (Отдел) внутри учетной записи пользователя в Active Directory, и это привело бы к изменению разрешений доступа?

В Active Directory хранится большой объем информации с различными метками для идентификации данных, которые называются атрибутами. Например, когда вы создаете четную запись пользователя, то наиболее базовой информацией, которую вы вводите, будет имя и фамилия лица. Эта информация сохраняется в атрибуте внутри Active Directory. Такие атрибуты могут быть пересмотрены и отредактированы (но будьте осторожны, чтобы не внести путаницу). На рис. 15.9 представлен пример некоторых атрибутов; в данном случае мы просматриваем атрибуты для пользователя по имени David McCormick. Удобным атрибутом, который можно применять для защиты информации, является `Department` (Отдел). На рис. 15.9 видно, что наш пользователь входит в состав группы `IT`. Мы знаем, что группа `IT` содержит много конфиденциальных сведений, и мы определенно не хотим, чтобы имена пользователей и пароли или важная информация о сети попала в нехорошие руки.

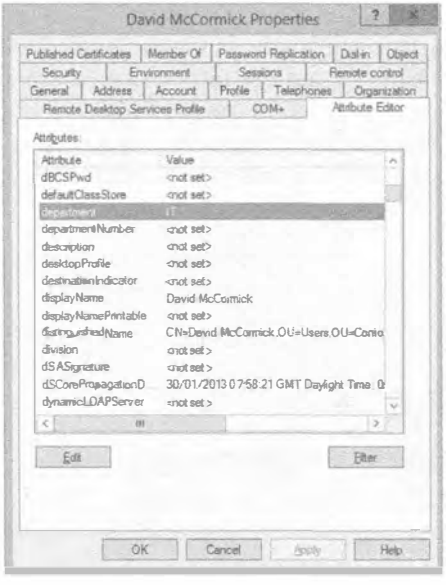


Рис. 15.9. Атрибут `Department`

Если вы просмотрите все атрибуты, доступные для пользователя, то заметите, что их список очень длинный. На деле только несколько полей могут оказаться полезными при управлении доступом к данным. Примерами могут служить `EmployeeType` (вы можете не разрешать сотрудникам, работающим не на полную ставку, доступ к определенными типам данных), `Company` (вы не хотите, чтобы персонал из дочерней компании имел доступ к данным компании Contoso) и `PhysicalDeliveryOfficeName` (может быть нежелательно, чтобы сотрудники из офиса в Лондоне получали доступ к данным офиса в Нью-Йорке).

Не ограничивайтесь только упомянутыми вариантами; вы можете подыскать собственные атрибуты. Если желаемый атрибут не существует, можете создать его и затем пользоваться. Очевидно, что такой прием не для робкого десятка, однако он иллюстрирует, насколько гибким может быть DAC.

На рис. 15.5 применялись только атрибуты `User` и `Device`. Теперь у нас есть новая опция под названием `Resource` (Ресурс), как показано на рис. 15.10.

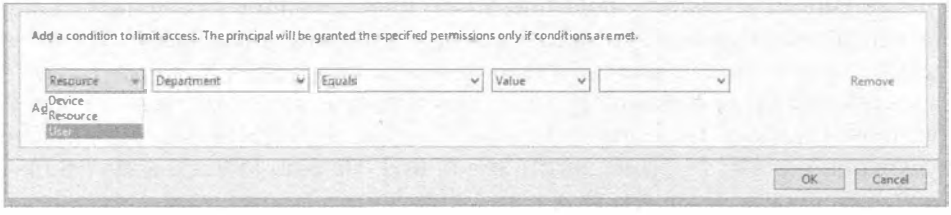


Рис. 15.10. Опция `Resource` в диалоговом окне Permission Entry for share

Опция `Resource` предоставляет опубликованные вами типы утверждений (по существу атрибуты, которые вы публикуете для представления утверждений авторизации, чтобы получить доступ к ресурсам). В этом примере после выбора `Resource` отображается опция `Department`. Пока что не переживайте по поводу того, как она здесь появилась; мы объясним это далее в главе.

Существуют те же самые логические условия Equals (Равно) или Not Equals (Не равно), но теперь последнее поле опций автоматически снабжается списком общих отделов, в котором можно делать выбор (рис. 15.11).

Этот список не извлекается из сводного списка всех пользователей в Active Directory. Это стандартный список, предоставляемый DAC, когда вы публикуете атрибут как тип утверждения; при необходимости можете его модифицировать.

Рис. 15.11. Потенциальные значения для выбранного атрибута `Department`

Но не будем забегать вперед. Чтобы средство DAC работало, вы должны создать решение, и важно понять концепции, прежде чем приступать к конфигурированию решения.

Защита данных посредством атрибутов машины

В последние годы многие компании преследовала мания реализовать политику BYOD (bring-your-own-device — принеси свое собственное устройство). Для сотрудников стало обычным явлением приобретать за свои деньги современные устройства, которые удовлетворяли их персональным нуждам и также позволяли получать доступ к данным в корпоративной сети. Устройства включали планшеты и ноутбуки и в редких случаях домашние настольные компьютеры. С точки зрения IT-администратора запрос вами строгого управления доступом к информации может оказаться утомительным. Вы могли заметить проблему: поскольку предприятие не является владельцем устройства, оно не так много может предпринять действий по управлению безопасностью этого устройства. Крупная задача заключается в том, как обеспечить работу таких устройств в среде, но ограничить их только информацией, которая не относится к конфиденциальной.

Еще раз взгляните на рис. 15.5; вы увидите, что имеется опция `Device`. Она позволяет решить, должен ли компьютер быть по умолчанию частью какой-то группы, и разрешен ли ему доступ к ресурсу. Предположим, что вы создали четыре группы: первая из них объединяет настольные компьютеры, вторая — ноутбуки, третья — машины из финансового отдела, а четвертая — машины из конструкторского отдела. Далее вы могли бы создать правило, требующее, чтобы только настольные компьютеры и ноутбуки, которые являются также частью финансового отдела, имели доступ ко всей информации, содержащейся внутри общего ресурса `Finance`. Таким образом, вы можете зашифровать машины финансового отдела (настольные или ноутбуки), так что если пользователь скопирует данные из центрального общего ресурса, эта информация будет защищена. Пример хоть и прост, но он демонстрирует, насколько большой контроль может быть предпринят для защиты информации вашей компании.

Централизованное управление разрешениями с использованием шаблонов

Теперь вы располагаете мощным инструментом для управления доступом к ресурсам, но если вам придется делать все вручную, то очевидно это займет немалое время. Подобно большинству современных задач в области IT, лучше всего обеспечить централизацию. Можете ли вы себе представить наличие всей мощи средства DAC, но необходимость его внедрения на каждом файловом сервере внутри среды?

В Windows Server 2012 имеется утилита управления под названием ADAC (Active Directory Administrative Center — Административный центр Active Directory). Запустить эту утилиту можно через меню Tools (Сервис) диспетчера серверов.

После запуска ADAC в разделе навигации слева вы увидите элемент Dynamic Access Control (Динамическое управление доступом). По щелчку на элементе Dynamic Access Control станет доступной область, где вы будете централизованно конфигурировать правила DAC для среды. На рис. 15.12 показано окно Active Directory Administrative Center (Административный центр Active Directory).

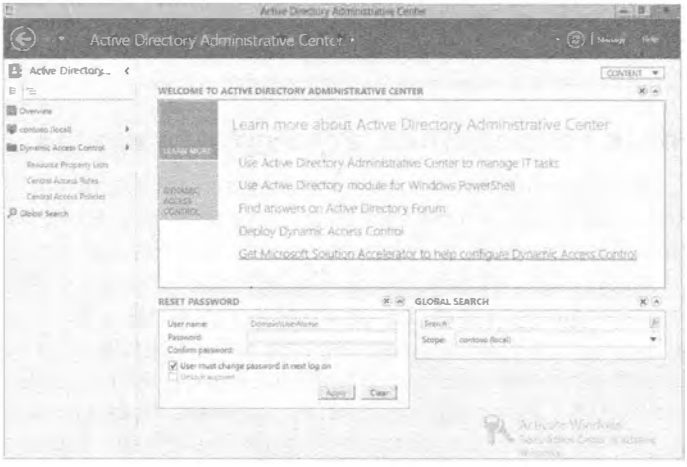


Рис. 15.12. Динамическое управление доступом в ADAC

Ниже приведены пояснения всех элементов, отображаемых под основным элементом Dynamic Access Control. По мере продвижения далее они станут важными.

- **Central Access Policies (Центральные политики доступа).** Центральная политика доступа означает именно то, о чем говорит ее название. Это центральное место для хранения политик доступа, которые необходимо конфигурировать. Ее настройка придает душевное спокойствие, гарантируя развертывание конфигурации на всех файловых серверах в среде.
- **Central Access Rules (Центральные правила доступа).** Центральные правила доступа — это правила о том, как вы хотите защищать информацию. Распространенным примером может служить предоставление доступа на основе отдела. Центральные политики доступа используют эти правила, содействуя в применении стандарта по всей организации. На рис. 15.13 представлен экран DAC для центральных правил доступа.
- **Claim Types (Типы утверждений).** Типы утверждений основаны на атрибутах Active Directory. Для конфигурирования утверждений могут использоваться атрибуты, основанные на пользователях и устройствах. Типы утверждений в конечном итоге применяются в процессе авторизации с помощью Kerberos.
- **Resource Properties (Свойства ресурсов).** Свойства ресурсов позволяют использовать свойства, которые могут быть определены на файле или папке, чтобы помочь классифицировать информацию. Например, если поле `Department` на файле установлено в `HR`, эта информация может быть автоматически классифицирована как конфиденциальная. Данная информация может также применяться центральными правилами доступа для указания на корректный ресурс и разрешения.
- **Resource Property Lists (Списки свойств ресурсов).** Списки свойств ресурсов предоставляют возможность категоризации свойств ресурсов в более полезные контейнеры. Например, список свойств ресурсов мог бы ограничивать количество классификаций, отображаемых для выбранного ресурса, что упрощает отслеживание, когда вы не нуждаетесь во всех потенциальных ресурсах, которые были определены.

Позже в этой главе мы приведем примеры создания всех указанных элементов и соберем их все вместе.

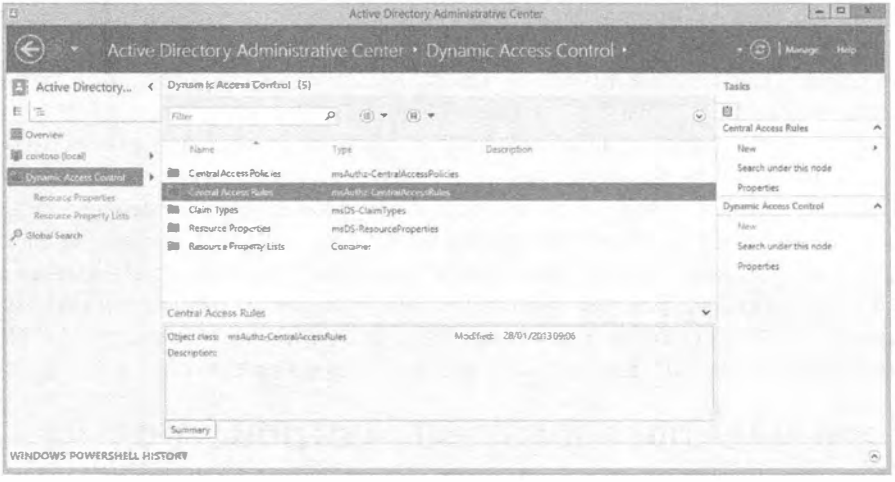


Рис. 15.13. Центральные правила доступа

Использование действующих разрешений для поиска и устранения неполадок в управлении доступом

Предположим, что в вашей компании применена центральная политика доступа к тестовому общему ресурсу на файловом сервере. Этот общий ресурс имеет несколько подпапок, имеющих простые имена, основанные на трех отделах: `Sales` (отдел продаж), `Accounts` (бухгалтерский отдел) и `Engineering` (конструкторский отдел). Администратор уже сконфигурировал политики для авторизации доступа к каждой подпапке только из отдела, которому она соответствует.

Администратор желает удостовериться в корректности работы политик. Для достижения этого вы можете использовать действующие разрешения, и вы можете также протестировать учетные записи индивидуальных пользователей без необходимости в получении их учетных данных и проверки наличия доступа.

Не беспокойтесь, если пока не полностью понимаете все это. Позже в данной главе мы покажем, как применять действующие разрешения и предоставим подходящие экранные снимки.

Автоматическая классификация файлов

К этому моменту вы уже знаете, какую значительную мощь может предложить динамическое управление доступом. Подумайте обо всей информации, содержащейся внутри файлов, которые размещены на общих сетевых ресурсах внутри компании, и затем попробуйте представить, как вы собираетесь защитить каждый из них.

Традиционно защита данных была ручным процессом, и хуже того, вы должны были удостовериться в том, что IT-администраторы и пользователи понимают, как правильно управлять своими документами.

Представьте себе, что кто-то поместил электронную таблицу Excel с платежной ведомостью в неположенное место, которое не имеет традиционных разрешений

для его защиты! Вообразите ситуацию, когда ваша компания располагает интеллектуальной собственностью, которая некорректно защищена! Наконец, подумайте о давлении со стороны руководства и попытки гарантировать безопасность данных.

В современных IT-инфраструктурах централизованное управление, где автоматизируется как можно большее число задач, должно быть минимальной основой в организации. Применение такого простого принципа классификации данных исключительно важно.

Вы можете это сделать с использованием свойств ресурсов, упоминаемых ранее в главе. Такие свойства ресурсов позволяют вручную устанавливать классификацию, но в случае комбинации этого с диспетчером ресурсов файлового сервера (File Server Resource Manager — FSRM) в Windows Server 2012 вы можете автоматически классифицировать документы. Если пользователь поместит документ не в то место внутри общего файлового ресурса, вы уверены в том, что какая-либо конфиденциальная информация не может быть доступна неавторизованным пользователям. Позже в этой главе мы продемонстрируем, каким образом добиться этого.

Игроки DAC: пользователь, устройство, ресурсы и утверждения

По мере продвижения в этой главе, мы затрагивали ключевых игроков в DAC, а также то, в чем заключается их работа. Прежде чем включать DAC и знакомиться с различными сценариями, мы приведем краткую сводку по этим игрокам и предоставим дополнительные сведения о них.

Пользователь

Начнем с пользователя. Как все мы знаем, пользователь — это обычно то, как мы идентифицируем себя, и он является основным методом авторизации. Предоставить доступ к ресурсам можно именно объекту пользователя. Тем не менее, учетные данные пользователей содержат громадный объем информации, которая при надлежащем заполнении позволит использовать эти поля (атрибуты) для предоставления дополнительной авторизации к ресурсам.

Устройство

Подобно пользователям, устройства также имеют большой объем информации, с которой можно работать. Вам всего лишь понадобится выбрать необходимые атрибуты. Хороший пример можно привести для конфиденциальной информации; чтобы предотвратить утечку данных, было бы замечательно иметь возможность ограничения доступа к этой информации устройствами, которые, как вы знаете, будут всегда физически расположены внутри офиса и подключены к корпоративной сети. Ограничить доступ к такой информации можно на основе местоположения. Для настольных компьютеров вы можете просто ввести **`Onsite`** в их поле `Location` (Местоположение), а для ноутбуков — **`Mobile`**.

Обычно для настольных компьютеров корпорации ограничивают доступ к сменным носителям и физически защищают сам системный блок. Поскольку ноутбук по своей природе является мобильным, защитить его физически очень трудно, и могут существовать уважительные причины для включения доступа к сменному носителю.

Пользователь может теперь обращаться к конфиденциальной информации, копировать ее на свои ноутбуки и затем копировать на устройство USB. Однако с помощью утверждения `Device` вы можете ограничить доступ к такой конфиденциальной информации по типу устройства, имеющегося у пользователя, даже если пользователь располагает полным доступом к ней. Если пользователь не применяет для доступа физически защищенное устройство, он не сможет обратиться к конфиденциальной информации, что предотвращает утечку данных.

Ресурсы

Ресурсы имеют ключевую важность. Если они не были определены, то их потребуется определить. Ресурсы помогают классифицировать данные на файловых серверах, и с ними можно взаимодействовать посредством инструмента FSRM, гарантируя, что это происходит автоматически. В результате решается крупная проблема того, как применить это задним числом к текущей среде. В Microsoft уже сделали немало работы по определению ресурсов внутри DAC, и по нашему мнению это лучшее, что мы видели до сих пор. Помните, что именно *вы* должны уделять время планированию своих ресурсов; в противном случае позже вы столкнетесь с большими проблемами.

Утверждения

Утверждение представляет собой информацию о сущности, полученную от доверенного источника. Это метод авторизации, который основан на атрибуте (обычно на устройства или на пользователе) и предназначен для обеспечения дополнительной безопасности ресурсов. Утверждением также может быть местоположение вашего офиса или отдела, равно как и любой другой атрибут, определенный для предоставления доступа к информации. Например, если ваш офис находится в Нью-Йорке, то вы можете иметь доступ к общему ресурсу `America`.

Утверждения бывают трех типов (т.к. мы уже обсудили утверждения о пользователе и об устройстве, здесь приводится только краткий обзор).

- **Утверждение о пользователе (user claim).** Утверждение о пользователе ассоциировано с атрибутами пользователя Active Directory, к примеру, с отделом или местоположением. Любой атрибут формально может стать частью модели утверждений о пользователях.
- **Утверждение об устройстве (device claim).** Подобно утверждению о пользователе, информация утверждения об устройстве берется из атрибутов, связанных с учетной записью компьютера в Active Directory. Например, для создания утверждения может использоваться местоположение или версия операционной системы.
- **Утверждение о преобразовании (transformation claim).** Утверждения о преобразовании предназначены для сценариев с пересечением границ лесов. Многие современные предприятия редко имеют только один лес, в котором бы они хранили и управляли всем необходимым. Этот тип утверждений помогает защищать данные в сценарии с несколькими лесами. Утверждение о преобразовании позволяет ограничить типы информации, видимой среде между лесами.

Например, в лесе `contoso.com` для создания утверждений применяется местоположение и отдел, но в лесе `litware.com` показывать отдел нежелательно; политика преобразования даст возможность скрыть отдел и оставить видимым только местоположение. Это также позволяет воспрепятствовать поступлению в среду ненужной информации утверждений. Таким образом, несмотря на то, что объект пользователя может включать идентификатор сотрудника, отдел и сведения о менеджере, вы можете быть заинтересованы только в идентификаторе сотрудника, поэтому заблокировать остальную информацию.

И снова здесь требуется соответствующее планирование. Вы должны определить, какие типы утверждений должны использоваться внутри организации, а также выяснить наличие доверительных отношений между лесами, и в случае, если применяется DAC, то какие политики преобразований должны быть предусмотрены.

- **Центральные правила доступа.** Эти правила объединяют ресурсы и только что описанные утверждения, чтобы позволить динамически управлять доступом к информации. Они будут введены в центральную политику доступа, которую вы определите позже, а она, в свою очередь, будет применяться к серверной базе, доступом к которой вы хотите управлять.

Теперь вы знаете основных игроков, и после того, как вы включите средство DAC и сконфигурируете его в своей среде, все станет на свои места.

Давайте приступим.

Включение DAC

В этом разделе главы предполагается наличие у вас сервера с установленной операционной системой Windows Server 2012. В нашей испытательной среде мы располагаем тремя серверами с Windows Server 2012 и клиентской машиной с Windows 8. Среди этих серверов сконфигурирован один контроллер домена и два файловых сервера. Также настроено несколько учетных записей с определенными атрибутами (к примеру, `Manager` (менеджер), `Location` (местоположение) и `Department` (отдел)), на основе которых позже можно создать утверждения.

Первым делом понадобится включить поддержку утверждений, комплексной аутентификации и защиты Kerberos в центре распределения Kerberos (Kerberos Distribution Center — KDC), где через групповую политику (Group Policy) будут генерироваться билеты аутентификации Kerberos.

1. На контроллере домена откройте консоль Group Policy Management (Управление групповой политикой), доступную в группе Administrative Tools (Администрирование), или, если вы предпочитаете пользоваться средством поиска в Windows Server 2012, то откройте меню Start (Пуск) и начните вводить **`Group Policy`**, в результате чего вы увидите этот инструмент.
2. Раскройте узел Group Policy Management (Управление групповой политикой).
3. Внутри узла Group Policy Management последовательно раскройте узлы Forest (Лес), Domains (Домены), ваш домен, Domain Controllers (Контроллеры домена) и найдите элемент Default Domain Controllers Policy (Стандартная политика контроллеров домена), как показано на рис. 15.14.

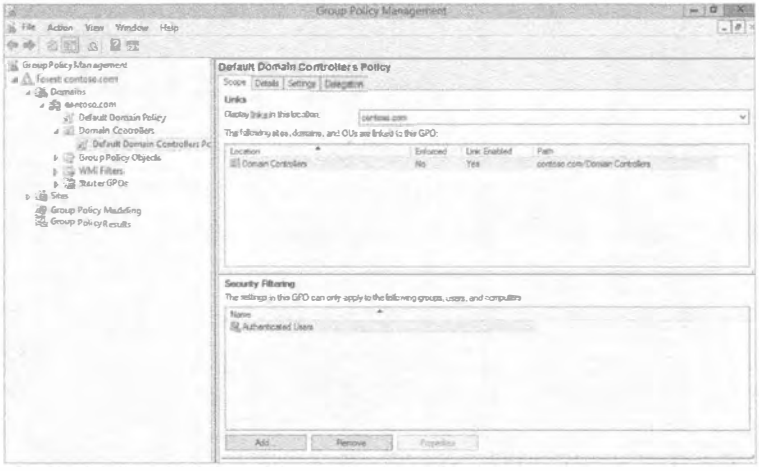


Рис. 15.14. Элемент Default Domain Controllers Policy в консоли Group Policy Management

4. Щелкните на элементе Default Domain Controllers Policy правой кнопкой мыши и выберите в контекстном меню пункт Edit (Редактировать). Откроется окно Group Policy Management Editor (Редактор управления групповой политикой), представленное на рис. 15.15.
5. В древовидной структуре слева перейдите к папке Computer Configuration⇨Policies⇨Administrative Templates⇨System (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система), как показано на рис. 15.16.

   Вам необходимо отредактировать политику KDC support for claims, compound authentication and Kerberos armoring (Поддержка KDC для утверждений, комплексной аутентификации и защиты Kerberos), расположенную в правой части окна. Дважды щелкните на этой политике, в результате чего откроется диалоговое окно редактора политики с опциями конфигурации (рис. 15.17).

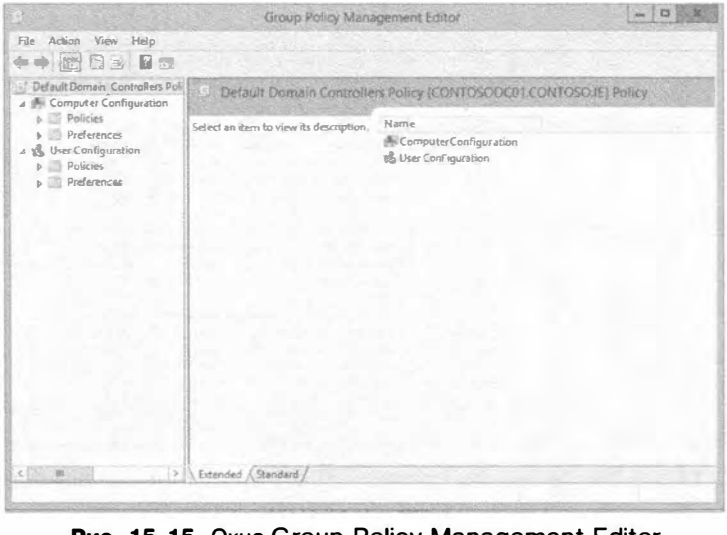


Рис. 15.15. Окно Group Policy Management Editor

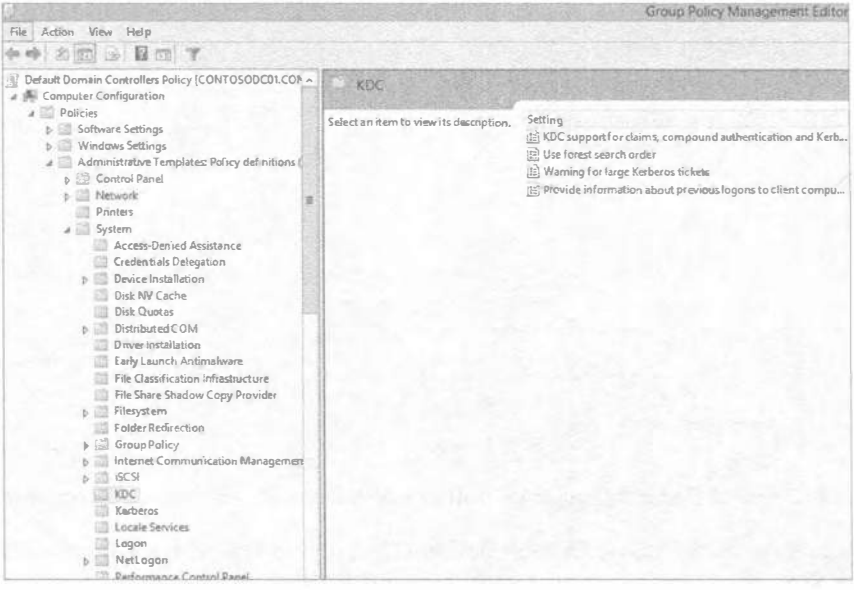


Рис. 15.16. Нахождение политики для редактирования с целью включения поддержки KDC

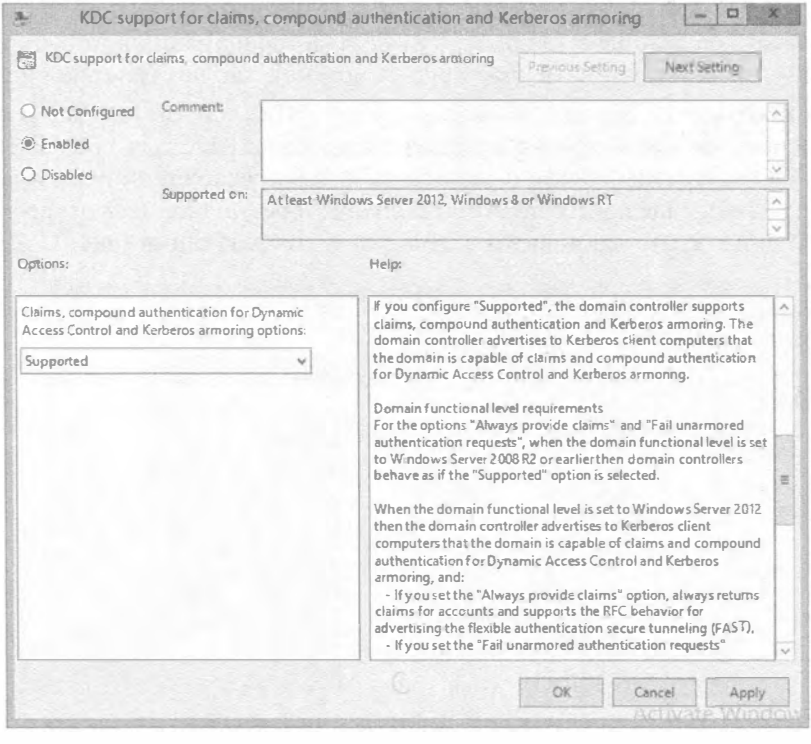


Рис. 15.17. Конфигурирование политики KDC support for claims, compound authentication and Kerberos armoring

6. Выберите переключатель Enabled (Включена); обратите внимание, что в раскрывающемся списке в области Options (Параметры) появился элемент Supported (Поддерживается). Щелкните на кнопке OK.

   В этом раскрывающемся списке доступны и другие элементы, которые описаны справа в области Help (Справка).

7. Посвятите некоторое время чтению сведений в области Help, после чего просто оставьте выбранным элемент Supported в раскрывающемся списке и щелкните на кнопке OK.

8. Закройте окно консоли Group Policy Management.

9. Откройте окно командной строки от имени учетной записи администратора и введите команду `gpupdate /force`, чтобы применить только что сконфигурированную политику, или подождите выполнения стандартной репликации и обновления групповой политики.

Ранее в этой главе речь шла об административном центре Active Directory (Active Directory Administrative Center). В нем как раз и будет конфигурироваться средство DAC.

Части политики доступа

Вы уже знаете, что для работы DAC необходимо сконфигурировать несколько компонентов: типы утверждений, ресурсы и центральные правила доступа. Мы также упоминали, что стремимся минимизировать накладные расходы, связанные с управлением. Именно здесь в игру вступают центральные политики доступа. Они собирают вместе все работы по конфигурированию для обеспечения легкого администрирования и управления доступом к информации в рамках существующей среды. Далее будет показано, как защищать файловые серверы, используя DAC централизованным образом, и как применять это повсеместно в организации. Новую технологию лучше всего изучать, непосредственно погрузившись в нее. Давайте построим простую политику доступа.

Создание политики динамического доступа

Откройте административный центр Active Directory и щелкните на элементе Dynamic Access Control (Динамическое управление доступом), как показано на рис. 15.18.

Если вы попытаетесь в этот момент создать центральную политику доступа, то не сможете сделать это. Как уже было сказано, сначала вы должны создать ресурсы, типы утверждений и центральные правила доступа.

Обратите внимание на разнообразные опции в центре окна. При щелчке на них меню Tasks (Задачи) в правой части окна изменяется в соответствии с выбранной опцией. Первым делом создадим новый тип утверждения.

1. Щелкните на элементе Claim Types (Типы утверждений) в центре окна и взгляните на меню Tasks, измененное согласно выбранной опции.

2. В меню Tasks под группой Claim Types выберите пункт New⇨Claim Type (Создать⇨Тип утверждения), как показано на рис. 15.19.

   Откроется диалоговое окно, позволяющее создать новый тип утверждения.

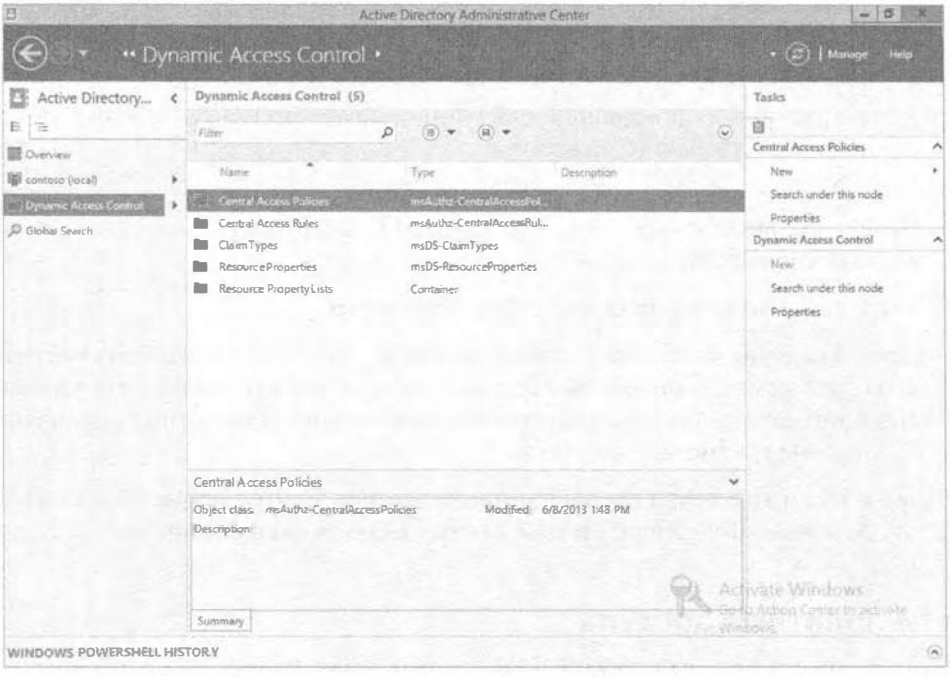


Рис. 15.18. Административный центр Active Directory

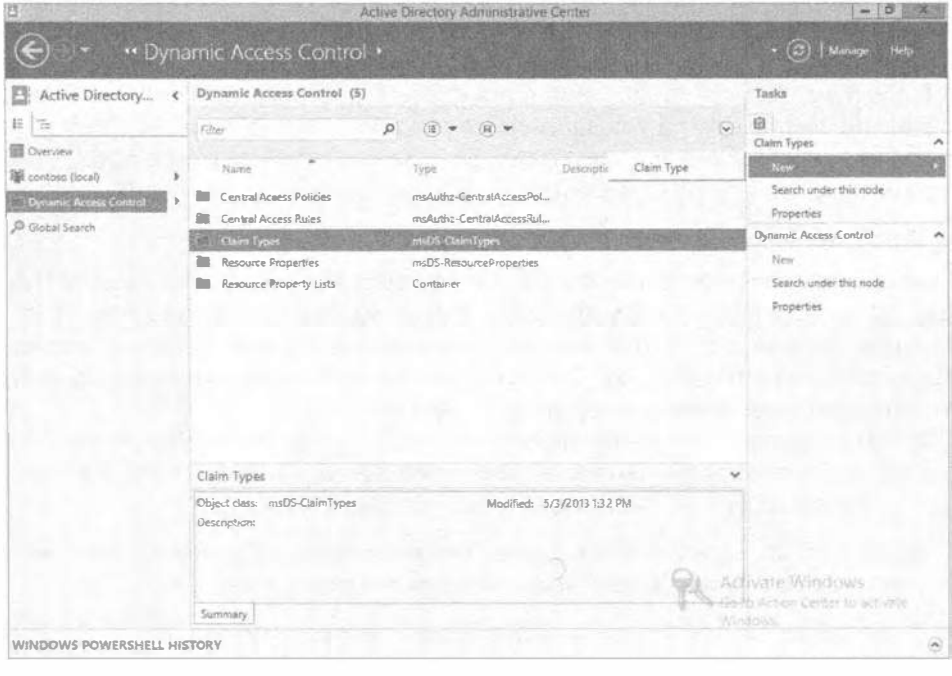


Рис. 15.19. Создание нового типа утверждения

3. Изучите доступные опции; вы увидите все атрибуты, которые потенциально могут участвовать при создании типа утверждения. Эти разные атрибуты предназначены для утверждений о пользователях и об устройствах.

   Например, найдите и выберите атрибут `dNSHostName`, и вы заметите, что он относится к утверждениям об устройствах, поскольку отмечен флажок Computer (Компьютер), что можно видеть на рис. 15.20.

Рис. 15.20. Отображение сведений об атрибуте `dNSHostName`

4. В списке Source Attribute (Исходный атрибут) выберите атрибут `department`.
5. Измените содержимое поля Display name (Отображаемое имя) справа в окне на **`department_Contoso`** (рис. 15.21).

Рис. 15.21. Изменение атрибута `department` для создания типа утверждения

6. Прокрутите содержимое окна до появления области Suggested Values (Предполагаемые значения); здесь будет указана информация, относящаяся к компании Contoso; например, в Microsoft уже сконфигурировали тип утверждения `Department` (Отдел), но не перечислили ни одного отдела.

   Мы создаем тип утверждения `Department` для компании Contoso, в которой есть четыре отдела: `Sales` (отдел продаж), `IT` (отдел информационных технологий), `Accounts` (бухгалтерский отдел) и `HR` (отдел кадров). Вы будете использовать их позже для управления доступом к демонстрационным общим ресурсам. Например, отделу `Sales` будет разрешен доступ только к данным `Sales`, отделу `HR` — только к данным `HR` и т.д.

7. Ниже текста When a user assigns a value to this claim type (Когда пользователь присваивает значение этому типу утверждения) выберите переключатель The following values are suggested (Предполагаются следующие значения), как показано на рис. 15.22.

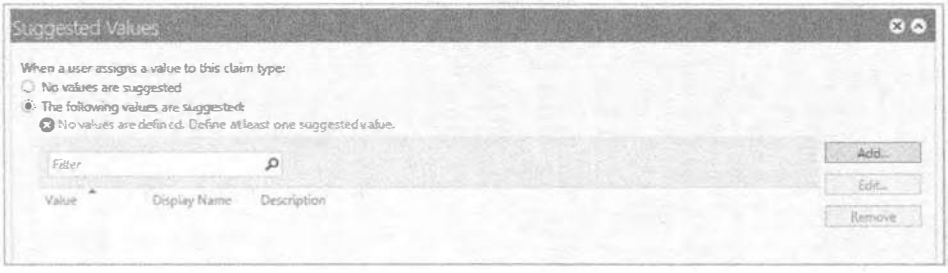


Рис. 15.22. Установка значений для типа утверждения

8. Щелкните на кнопке Add (Добавить); откроется диалоговое окно Add a suggested value (Добавление предполагаемого значения).

9. Введите **`Sales`** в полях Value (Значение) и Display name (Отображаемое имя) и щелкните на кнопке OK (рис. 15.23).

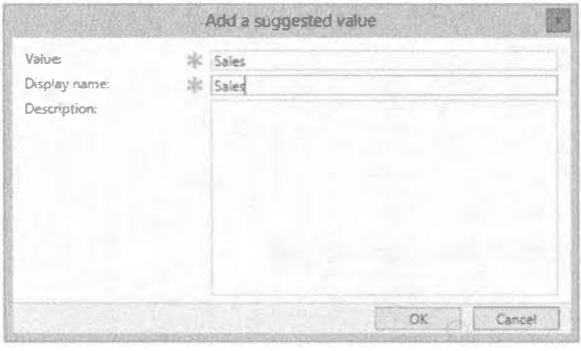


Рис. 15.23. Добавление предполагаемого значения

10. Повторите шаги 8 и 9 для отделов `IT`, `Accounts` и `HR`, после чего щелкните на кнопке OK.

    На этом процесс создания первого типа утверждения завершен.

А теперь необходимо создать свойство ресурса.

1. В окне, показанном на рис. 15.19, щелкните на элементе Resource Properties (Свойства ресурсов) и затем, подобно тому, как это делали ранее, выберите в меню Tasks (Задачи) пункт New⇨Resource Property (Создать⇨Свойство ресурса).

   Вы увидите две доступных опции: свойство ресурса и ссылочное свойство ресурса.

2. Так как мы уже создали тип утверждения, мы собираемся применять ссылочное свойство ресурса. Выбирайте свойство ресурса, если тип утверждения пока еще не создавался.

   В представленном на рис. 15.24 диалоговом окне Create Reference Resource Property (Создание ссылочного свойства ресурса) можно заметить созданный ранее тип утверждения. Поле Display name (Отображаемое имя) также заполнено, а в раскрывающемся списке Value type (Тип значения) для выбора доступны элементы Single-valued Choice (Однозначный выбор) и Multi-valued Choice (Многозначный выбор).

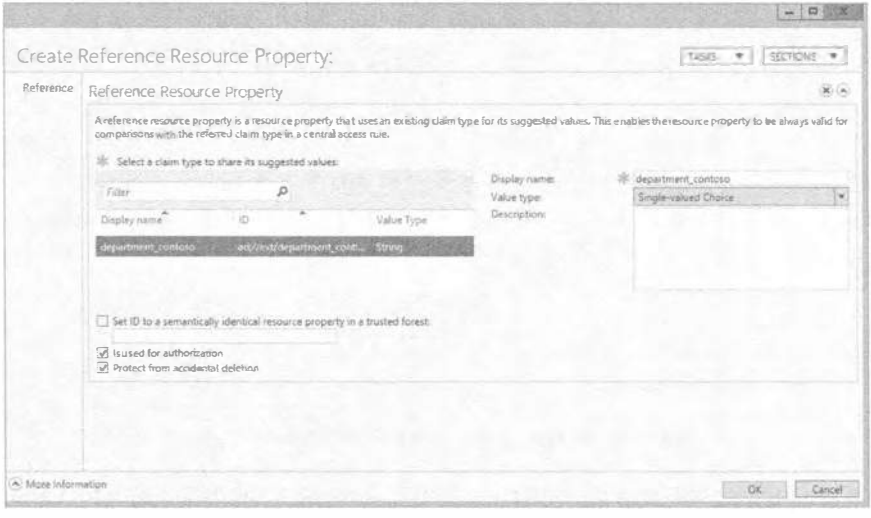


Рис. 15.24. Диалоговое окно Create Reference Resource Property

3. В данном случае выберите элемент Single-valued Choice, поскольку в большинстве компаний "официально" предполагается, что сотрудник работает только в одном отделе.

   Из-за того, что в конечном итоге это свойство будет задействовано в центральных правилах и политиках доступа, отметьте флажок Is used for authorization (Используется в авторизации).

4. По завершении щелкните на кнопке OK.

Побочная задача

В справочных целях сообщаем, что эта задача представляет собой процедуру создания свойства ресурса, для которого тип утверждения не существует, например,

если вы не хотите пользоваться свойствами ресурсов, предоставленными Microsoft, или они просто не удовлетворяют вашим нуждам. Еще одним примером может быть ситуация, когда вы создали в Active Directory специальный атрибут и хотите его применять в качестве типа утверждения.

После завершения предыдущего упражнения откроется диалоговое окно New Resource Property (Новое свойство ресурса). Выполните перечисленные ниже шаги.

1. На экране Dynamic Access Control (Динамическое управление доступом) административного центра Active Directory щелкните на элементе Resource Properties (Свойства ресурсов) и в меню Tasks (Задачи) выберите пункт New⇨Resource Property (Создать⇨Свойство ресурса).
2. В поле Display name (Отображаемое имя) введите **department_contoso_test**, а в раскрывающемся списке Value type (Тип значения) выберите вариант Single-valued Choice (Однозначный выбор). Для типа значения доступны разные варианты, которые должны планироваться заранее. Большинство компаний разрешают сотруднику одновременно числиться только в каком-то одном отделе, поэтому в данном случае вариант Single-valued Choice представляется наиболее подходящим (рис. 15.25).

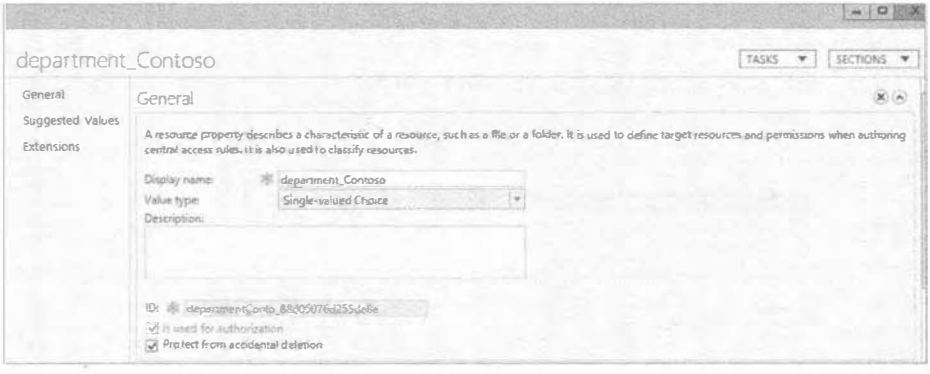


Рис. 15.25. Создание нового свойства ресурса

3. Просмотрите опции в раскрывающемся списке Value type; как видите, их довольно много.
4. Прокрутите содержимое окна до появления области Suggested Values (Предполагаемые значения) и добавьте предполагаемые значения, как делали это ранее при создании нового типа утверждения.
5. Щелкните на кнопке OK. Вы создали новое свойство ресурса.

В этот момент вы возвратитесь на экран Resource Properties (Свойства ресурсов), приведенный на рис. 15.26.

Как вы наверняка помните, мы указывали, что в Microsoft проделали немало работы, чтобы позволить компаниям быстро развертывать средство DAC. Часть общей цели заключалась в том, чтобы сделать средство DAC быстрым для развертывания, и хотя вы должны кое-что знать о том, какие правила/свойства/типы утверждений понадобится создать, в следующем руководстве вы увидите, что многое для вас уже сделано, и придется лишь произвести необходимый выбор.

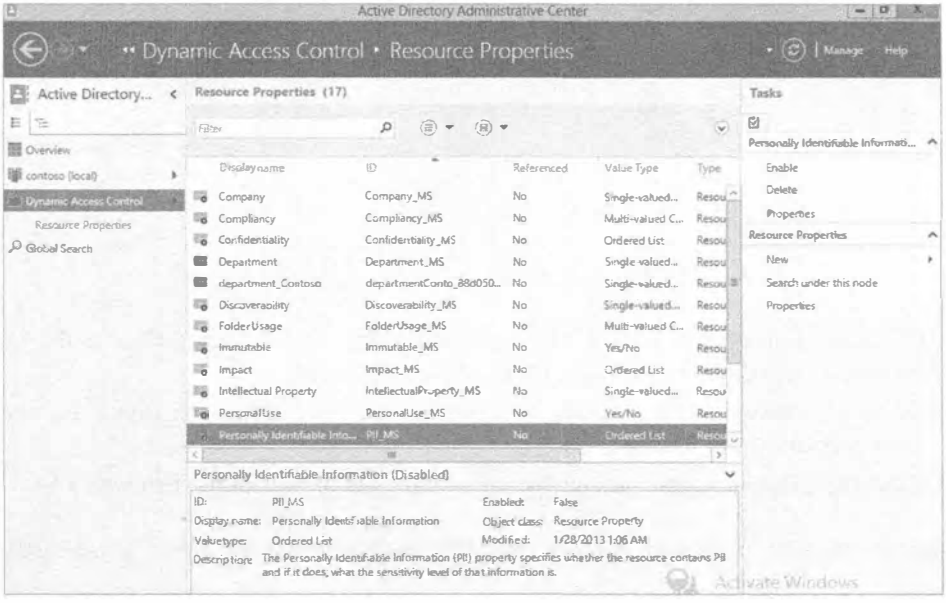


Рис. 15.26. Экран Resource Properties

1. Просмотрите список Resource Properties (Свойства ресурсов), чтобы увидеть, что сконфигурировано и чем можно было бы воспользоваться вместо создания новых свойств.

   Давайте проведем быструю проверку:

   - вы создали новый тип утверждения для отделов компании Contoso;
   - вы создали ссылочное свойство ресурса, основанное на утверждении `Department` для Contoso.

   Далее понадобится сконфигурировать список свойств ресурсов. Свойство ресурса *должно* быть частью какого-то списка свойств ресурсов. Список свойств ресурсов будет загружаться файловыми серверами. Как видно в главном окне Dynamic Access Control на рис. 15.27, список свойств ресурсов имеет тип Container (Контейнер).

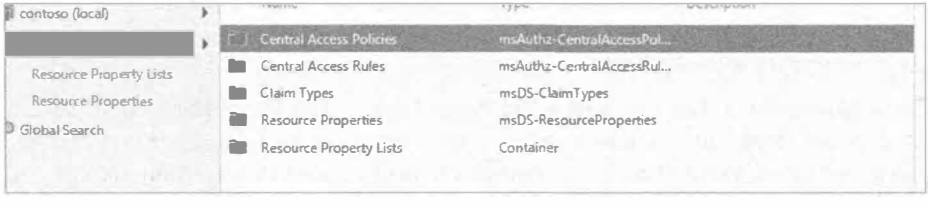


Рис. 15.27. Главное окно Dynamic Access Control

2. Дважды щелкните на элементе Resource Property Lists (Списки свойств ресурсов); откроется экран, показанный на рис. 15.28.

   Отображаемый глобальный список свойств ресурсов (Global Resource Property List) — это стандартный список, который получат все файловые серверы.

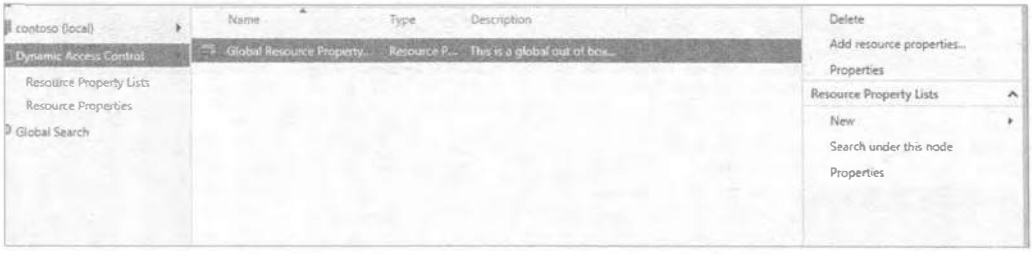


Рис. 15.28. Глобальный список свойств ресурсов

3. В информационных целях дважды щелкните на элементе Global Resource Property List (Глобальный список свойств ресурсов).

   Обратите внимание, что по умолчанию в этом списке присутствуют все свойства ресурсов (рис. 15.29).

   Давайте добавим свойство ресурса в список Global Resource Property List.

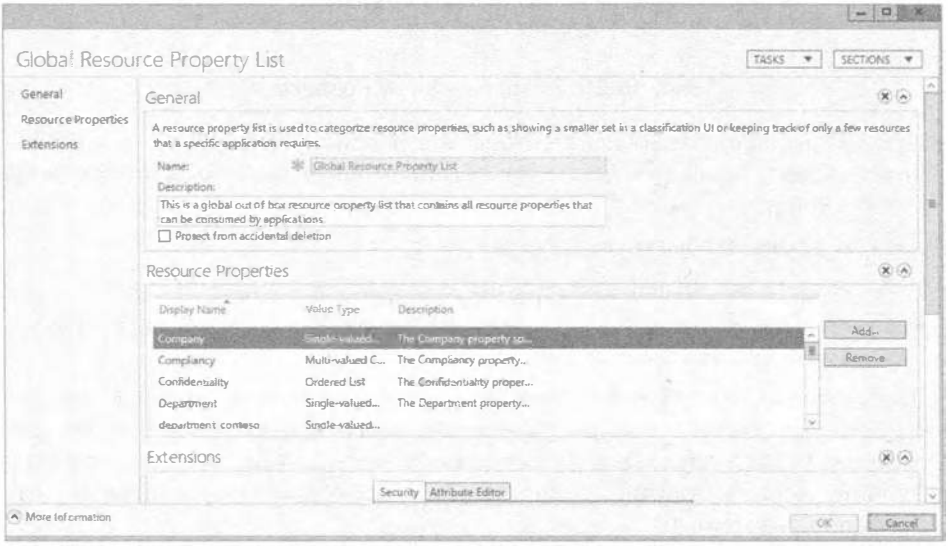


Рис. 15.29. Содержимое глобального списка свойств ресурсов

4. Щелкните на кнопке Add (Добавить).
5. В открывшемся диалоговом окне Select Resource Properties (Выбор свойств ресурсов) перейдите к свойству `department_contoso` и шелкните на кнопке со стрелками, указывающими вправо, чтобы добавить его (рис. 15.30).
6. Щелкните на кнопке OK, перейдите к списку свойств ресурсов и удостоверьтесь в том, что в нем присутствует только что добавленное свойство. Щелкните на кнопке OK в главном окне, чтобы закрыть его.

Вы создали новый тип утверждения, ссылочное свойство ресурса и добавили его в список Global Resource Property List.

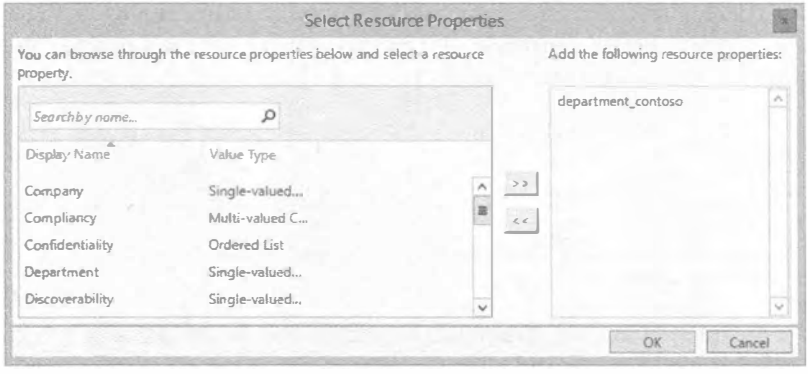


Рис. 15.30. Добавление нового свойства ресурса в список Global Resource Property List

Далее потребуется создать центральное правило доступа.

1. В главном окне Dynamic Access Control щелкните на элементе Central Access Rules (Центральные правила доступа) и выберите в меню Tasks (Задачи) пункт New⇨Central Access Rule (Создать⇨Центральное правило доступа).
2. В открывшемся диалоговом окне Create Central Access Rule (Создание центрального правила доступа) введите **`Contoso_Demo_rule`** в поле Name (Имя), как показано на рис. 15.31.

   В области Target Resources (Целевые ресурсы) при желании вы можете обеспечить большую избирательность в отношении ресурсов, доступом к которым вы управляете. В этом примере оставьте стандартный вариант All Resources (Все ресурсы), так что вы сможете настроить всем аутентифицированным пользователям доступ для чтения ко всем ресурсам.

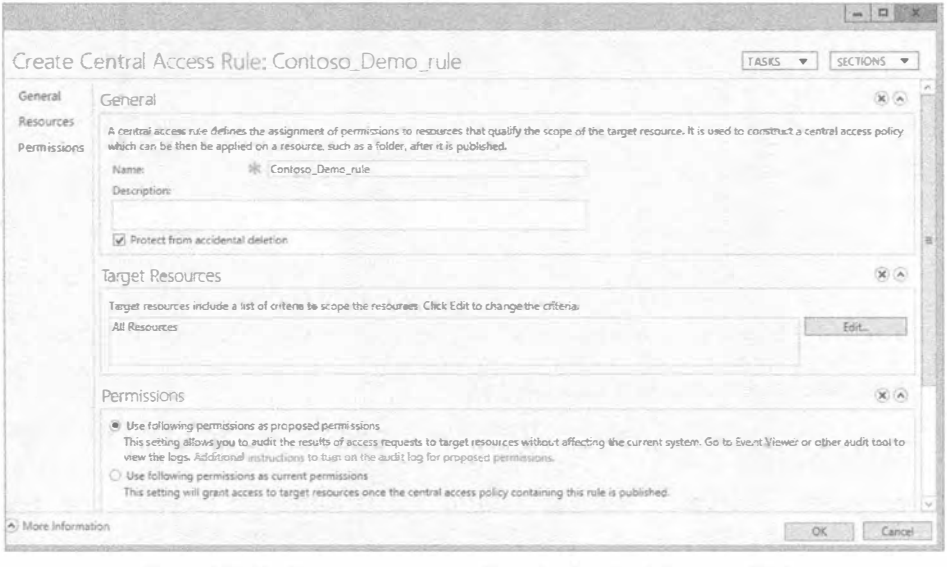


Рис. 15.31. Диалоговое окно Create Central Access Rule

3. В области Permissions (Разрешения) выберите переключатель Use following permissions as current permissions (Использовать следующие разрешения как текущие разрешения), как показано на рис. 15.32.

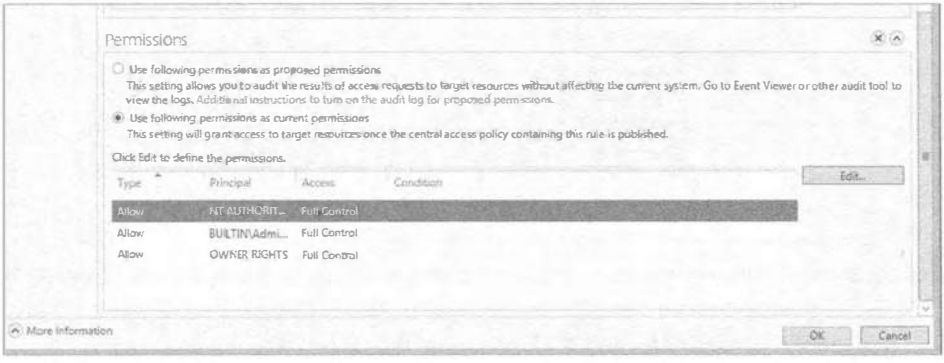


Рис. 15.32. Добавление разрешений для центрального правила доступа

4. Щелкните на кнопке Edit (Редактировать) в области Permissions.

   Откроется диалоговое окно Advanced Security Settings for Permissions (Расширенные настройки безопасности для разрешений), представленное на рис. 15.33.

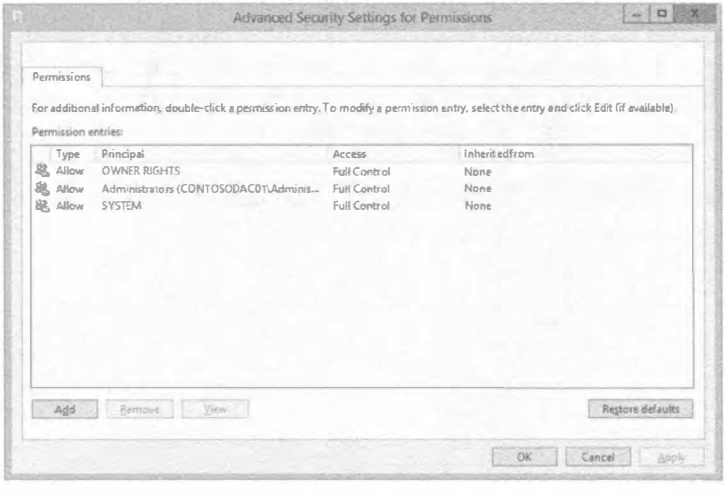


Рис. 15.33. Диалоговое окно Advanced Security Settings for Permissions

5. Щелкните на кнопке Add (Добавить).

   Откроется диалоговое окно Permission Entry for Permissions (Запись разрешения для разрешений).

6. Щелкните на ссылке Select a principal (Выбрать участника) и введите **`Authenticated Users`**; оставьте отмеченными флажки для разрешений Read (Чтение) и Read and Execute (Чтение и выполнение), как показано на рис. 15.34. Далее, как вы уже делали это ранее, необходимо добавить условия.

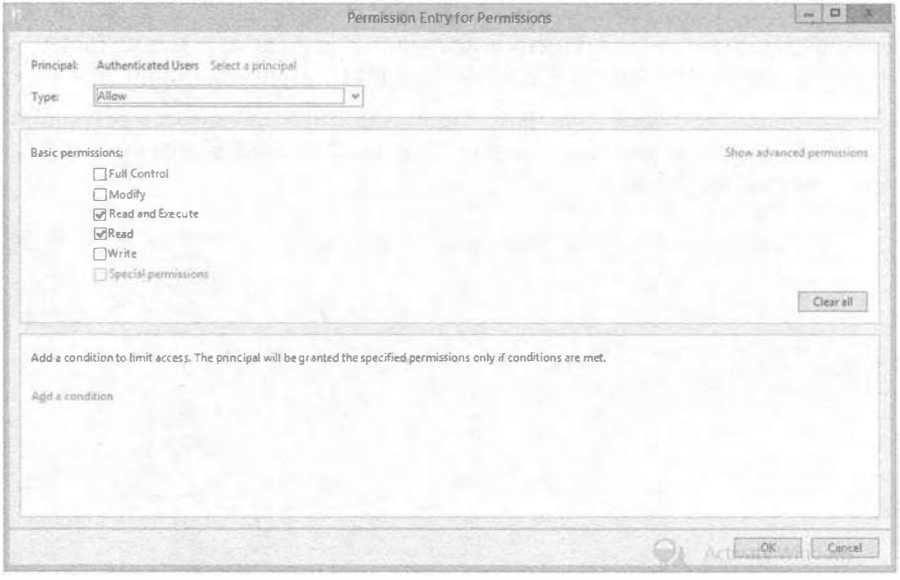


Рис. 15.34. Диалоговое окно Permission Entry for Permissions

7. Щелкните на ссылке Add a condition (Добавить условие).

   Отобразятся опции, предназначенные для конфигурирования.

8. В первом поле с раскрывающимся списком выберите вариант User (Пользователь), во втором поле — `department_contoso`, а в последнем поле — `Accounts` (бухгалтерский отдел).

   Обратите внимание, что раскрывающийся список в последнем поле содержит отделы, которые были созданы вами ранее.

9. Повторите шаг 8 для оставшихся отделов. Используйте условие And (И), что видно на рис. 15.35.

Рис. 15.35. Добавление условий в центральное правило доступа

10. Завершив добавление условий, щелкните на кнопке OK, и затем щелкните на OK еще два раза, чтобы закрыть все окна.

Великолепно! Вы близки к финишу и теперь должны создать центральную политику доступа, которая затем будет применяться для развертывания на файловых

1. В главном окне Dynamic Access Control щелкните на элементе Central Access Policies (Центральные политики доступа) и выберите в меню Tasks (Задачи) пункт New⇨Central Access Policy (Создать⇨Центральная политика доступа).
2. В открывшемся диалоговом окне Create Central Access Policy (Создание центральной политики доступа) введите **`Contoso Test CAP`** в поле Name (Имя), как показано на рис. 15.36.

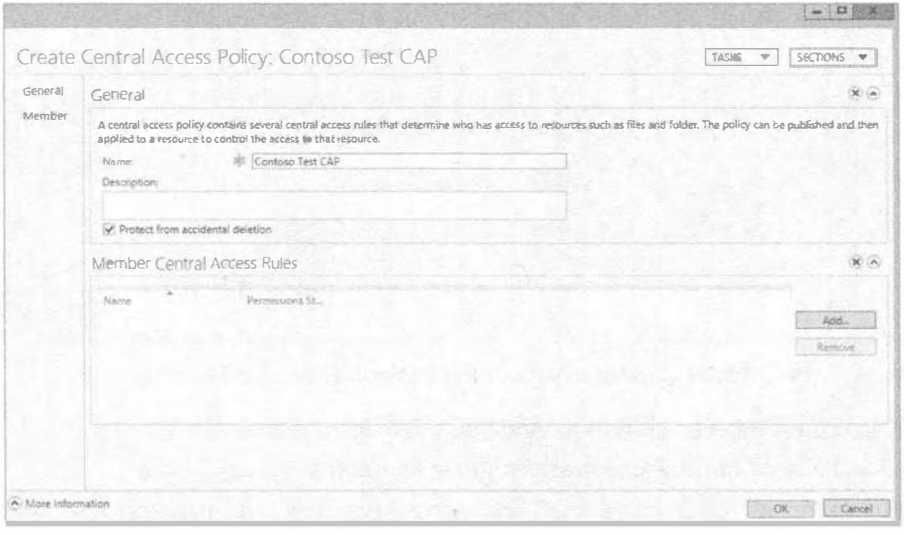


Рис. 15.36. Диалоговое окно Create Central Access Policy

3. Вам необходимо добавить правило, которое вы создали ранее, поэтому щелкните на кнопке Add (Добавить) возле области Member Central Access Rules (Центральные правила доступа, являющиеся членами). Откроется диалоговое окно Add Central Access Rules (Добавление центральных правил доступа).
4. Выберите правило `Contoso_Demo_rule`, щелкните на кнопке со стрелками, указывающими вправо, и затем щелкните на кнопке OK (рис. 15.37).
5. Щелкните на кнопке OK, чтобы завершить создание политики.

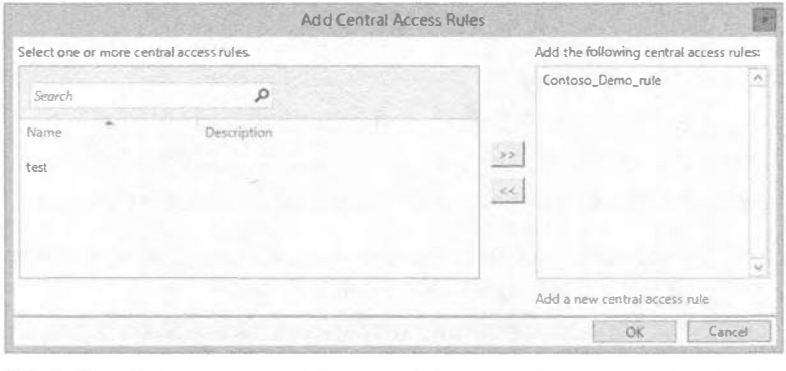


Рис. 15.37. Добавление центрального правила доступа в центральную политику доступа

Применение политик динамического управления доступом

Вы создали политику динамического управления доступом, но чтобы она была результативной, ее необходимо применить к серверам. Это делается через групповую политику (Group Policy). За счет развертывания групповой политики вы получаете удивительную гибкость, начиная с нацеливания на специфичные группы серверов и распространяя ее далее по мере необходимости.

В главе 9 вы должны были ознакомиться, что собой представляет групповая политика; если же нет, возвратитесь и прочитайте ее.

Вы должны воспользоваться консолью Group Policy Management (Управление групповой политикой) и создать в ней новую групповую политику для распространения центральной политики доступа. Эта консоль доступна через меню Tools (Сервис) диспетчера серверов.

В рассматриваемом примере консоль Group Policy Management необходимо открывать на контроллере домена. (Предполагается, что к этому моменту вы уже знакомы с данным инструментом.)

Мы собираемся создать групповую политику прямо под корневым уровнем домена `contoso.ie` и нацелить ее непосредственно на файловые серверы. Но прежде чем начать, ознакомьтесь со следующими рекомендациями.

- Создавайте необходимые группы для надлежащего нацеливания на файловые серверы.
- Создавайте организационные единицы в структурированной иерархической манере и назначайте групповую политику желаемой организационной единице, но никогда — корневому домену.

Итак, приступим.

1. Щелкните правой кнопкой мыши на домене `contoso.ie`, как показано на рис. 15.38, и выберите в контекстном меню пункт Create a GPO in this domain, and Link it here (Создать объект GPO в этом домене и связать его).

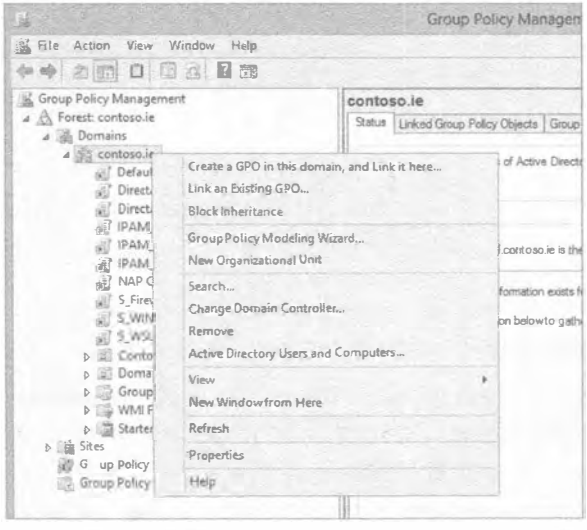


Рис. 15.38. Создание объекта GPO для развертывания центральной политики доступа

2. В открывшемся диалоговом окне New GPO (Новый объект GPO) назначьте имя создаваемому объекту GPO.

   В данном сценарии в качестве имени выбрано **CAP-Contoso-Demo**.

3. Щелкните на кнопке OK (рис. 15.39).

   Новый объект GPO должен теперь отображаться в списке под `contoso.ie`.

Рис. 15.39. Диалоговое окно New GPO

4. Щелкните на имени групповой политики, в области Security Filtering (Фильтрация безопасности) на вкладке Scope (Область действия) окна консоли Group Policy Management (рис. 15.40) выберите группу `Authenticated Users` (Аутентифицированные пользователи) и щелкните на кнопке Remove (Удалить).

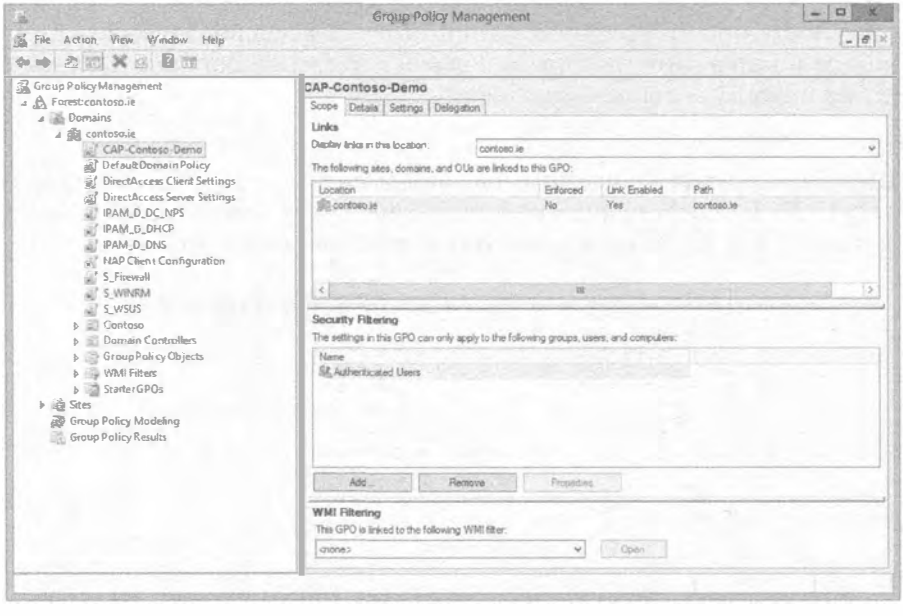


Рис. 15.40. Удаление группы `Authenticated Users`

5. В открывшемся диалоговом окне Do you want to remove this delegation privilege? (Хотите ли вы удалить эту делегированную привилегию?) щелкните на кнопке OK.

6. Щелкните на кнопке Add (Добавить).

   Откроется диалоговое окно Select User, Computer, or Group (Выбор пользователя, компьютера или группы).

7. Щелкните на кнопке Object Types (Типы объектов) и отметьте флажок Computer (Компьютер), т.к. по умолчанию он не отмечен, после чего щелкните на кнопке OK.
8. В поле Enter object name to select (Введите имя объекта для выбора) и введите имя файлового сервера, к которому хотите применить групповую политику.

   В этом примере мы используем **contosofs01**.
9. Щелкните на кнопке Check Names (Проверить имена), удостоверьтесь в том, что они распознаются, и щелкните на кнопке OK (рис. 15.41).

   В области Security Filtering вы увидите полное имя учетной записи компьютера; это просто означает, что политика будет применена только к этому компьютеру, хотя она располагается в корне домена (рис. 15.42).

   Далее вам понадобится отредактировать эту групповую политику.

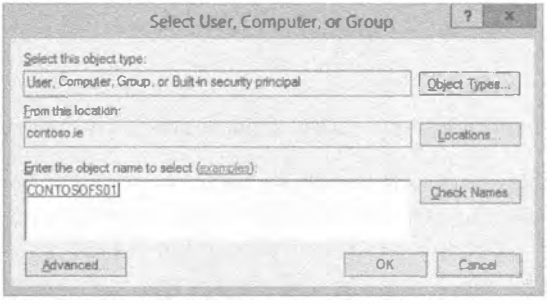


Рис. 15.41. Проверка в окне поиска, распознается ли имя

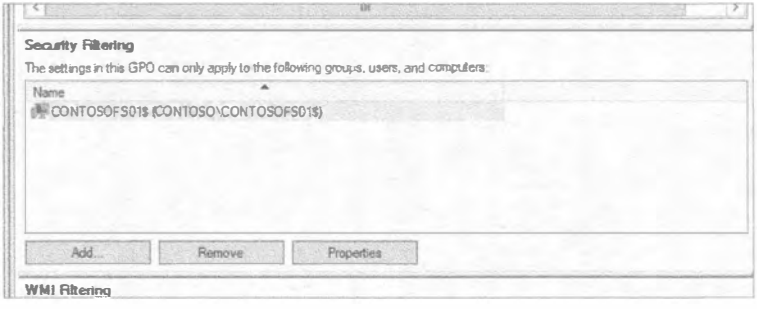


Рис. 15.42. Учетная запись компьютера, добавленная в область Security Filtering

10. Щелкните правой кнопкой мыши на групповой политике `CAP-Contoso-Demo` и выберите в контекстном меню пункт Edit (Редактировать).

    Откроется диалоговое окно Group Policy Management Editor (Редактор управления групповой политикой).
11. Перейдите к папке Computer Configuration⇨Policies⇨Windows Settings⇨Security Settings⇨File System⇨Central Access Policy (Конфигурация компьютера⇨Политики⇨Настройки Windows⇨Настройки безопасности⇨Файловая система⇨Центральная политика доступа), как показано на рис. 15.43.

    В настоящий момент конфигурировать нечего.

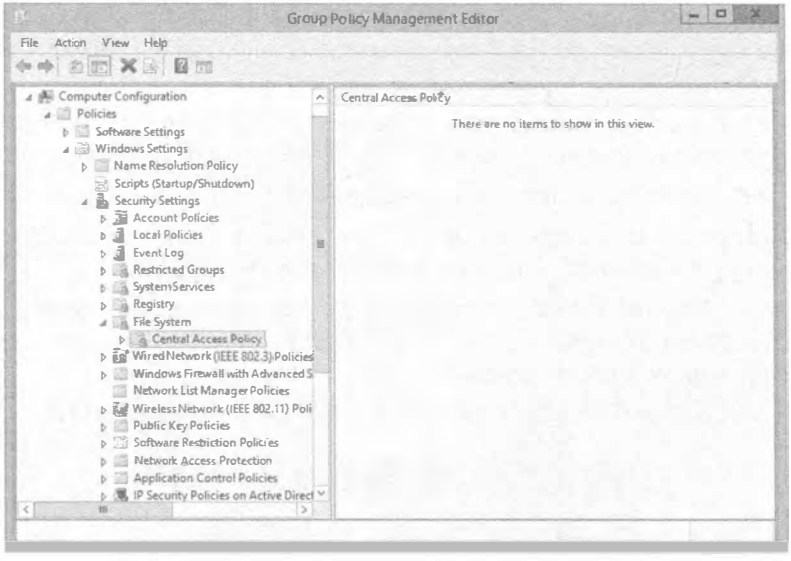


Рис. 15.43. Папка Central Access Policy в редакторе управления групповой политикой

12. Щелкните правой кнопкой мыши на папке Central Access Policy и выберите в контекстном меню пункт Manage Central Access Policies (Управлять центральной политикой доступа), как показано на рис. 15.44.

    Откроется диалоговое окно Central Access Policies Configuration (Конфигурация центральной политики доступа), в котором вы увидите сконфигурированные ранее центральные политики доступа.

Рис. 15.44. Диалоговое окно Central Access Policies Configuration

13. Выберите политику, которую вы хотите применить, и щелкните на кнопке Add (Добавить). В этом примере мы выбрали политику `Contoso Test CAP` (рис. 15.45).
14. Щелкните на кнопке OK.
15. Прокрутите содержимое окна Group Policy Management Editor вниз, чтобы увидеть папку Advanced Audit Policy Configuration⇨Audit Policies⇨Object Access (Расширенная конфигурация политики аудита⇨Политики аудита⇨Доступ к объектам), и дважды щелкните на подкатегории Audit Central Access Policy Staging (Установка аудита центральной политики доступа), как показано на рис. 15.46.

Рис. 15.45. Выбор центральных политик доступа для применения

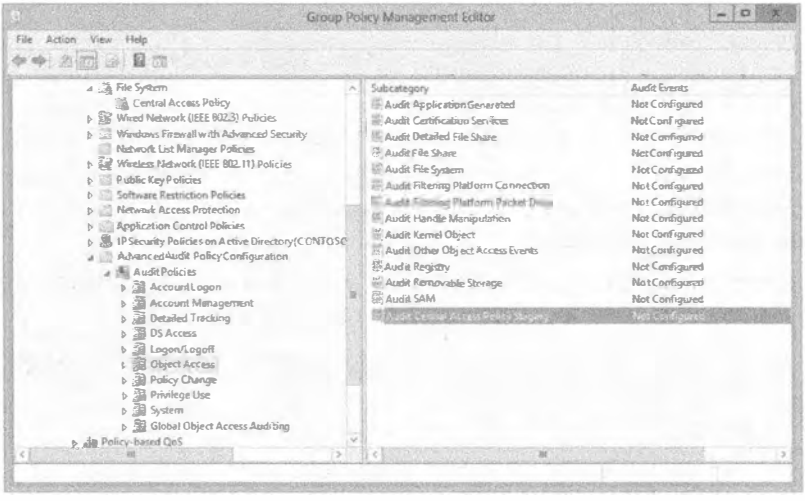


Рис. 15.46. Установка аудита центральной политики доступа

16. Отметьте все флажки в диалоговом окне Audit Central Access Policy Staging Properties (Свойства установки аудита центральной политики доступа), приведенном на рис. 15.47, и щелкните на кнопке OK. Закройте окно Group Policy Management Editor.

    Теперь нужно удостовериться в том, что политика применяется к файловому серверу.

17. Войдите в систему файлового сервера `ContosoFS01`, откройте окно командной строки от имени учетной записи администратора и введите команду **`gpupdate /force`**.

    Сконфигурированная политика будет применена.

18. Чтобы получить подтверждение о том, что политика была применена, взгляните на папку, для которой вы открыли общий доступ как `ContosoFS01`. В нашей демонстрационной среде мы открыли общий доступ к папке `C:\share` как `\\contosofs01\share`. На рис. 15.48 и 15.49 показана настройка правил для разрешений NTFS и разрешений общего доступа.

    Заметили ли вы новую вкладку Central Policy (Центральная политика)? По умолчанию никаких политик не применяется.

    После перехода на вкладку Central Policy вам понадобится щелкнуть на ссылке Change (Изменить) для получения доступа к раскрывающемуся списку, в котором вы обнаружите сконфигурированную ранее политику, примененную посредством групповой политики.

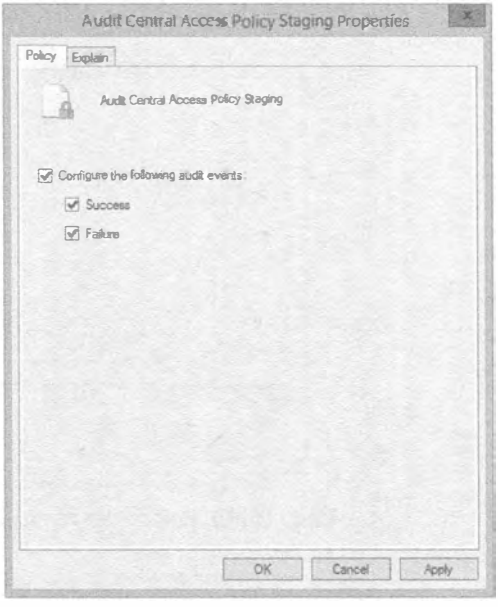


Рис. 15.47. Конфигурирование аудита

19. Выберите политику `Contoso Test CAP`, в результате чего отобразятся центральные правила доступа, которые вы сконфигурировали для разрешения/ограничения доступа к ресурсам.
20. Щелкните на кнопке со стрелкой вниз возле центрального правила доступа, и вы увидите опции, которые сконфигурировали ранее.

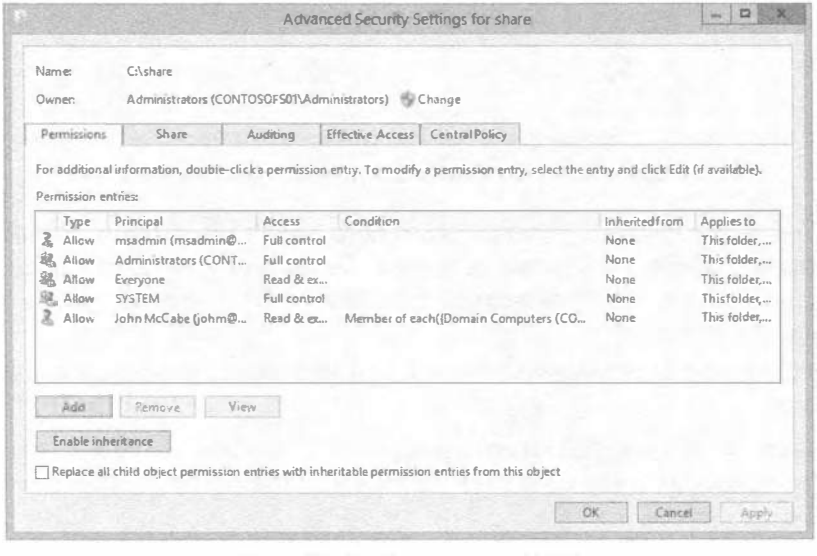


Рис. 15.48. Разрешения NTFS

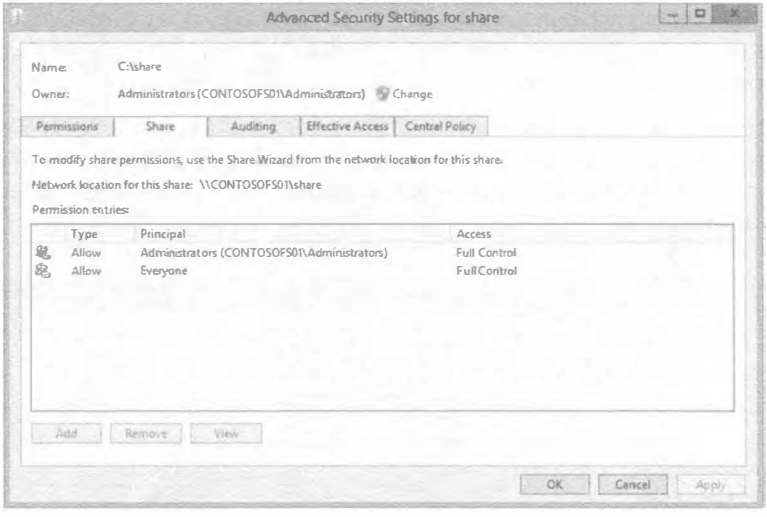


Рис. 15.49. Разрешения общего доступа

Тестирование новой политики

Итак, вы применили заранее сконфигурированную центральную политику доступа к общему ресурсу на файловом сервере. Взгляните на рис. 15.48 и 15.49 еще раз. Что касается разрешений NTFS, группе `Everyone` (Все) был предоставлен доступ по чтению к папке `C:\share`, а также общий доступ после того, как была применена центральная политика доступа. На самом деле ситуация не идеальна, но это распространенная проблема в большинстве сред.

С технической точки зрения любой должен иметь возможность доступа к этому общему ресурсу и извлечения содержащейся в нем ценной информации. Давайте проверим это.

1. В системе файлового сервера `Contosofs01` перейдите в место расположения общего ресурса.

   В этом примере наш общий ресурс находится в `C:\share`.

2. Щелкните правой кнопкой мыши на папке `C:\share` и выберите в контекстном меню пункт Properties (Свойства).

3. Перейдите на вкладку Security (Безопасность) и щелкните на кнопке Advanced (Дополнительно), чтобы открыть диалоговое окно Advanced Security Settings for share (Расширенные настройки безопасности для `share`), которое представлено на рис. 15.50.

4. Перейдите на вкладку Effective Access (Действующий доступ).

   Действующий доступ позволит протестировать разрешения центральную политику доступа, примененную к общему ресурсу для участника в форме пользователя или устройства. Например, центральная политика доступа, которую мы определили, содержит внутри одно правило, разрешающее доступ к этому общему ресурсу только персоналу из отдела `HR` или `Accounts`. В испытательной среде сконфигурированы два пользователя: Том (`Tom`), работающий в отделе `Accounts`, и Кен (`Ken`), занятый в отделе `IT`. Несмотря на то что разре-

шения NTFS и разрешения общего доступа позволяют подключаться группе Everyone, т.е. всем, центральная политика доступа это переопределит. Главный вопрос: так ли это на самом деле?

Попробуем выяснить. На вкладке Effective Access, приведенной на рис. 15.51, можно выбрать пользователя или устройство. В данном примере мы выбираем пользователя, поскольку настроенный ранее тип утверждения основан на отделе пользователя.

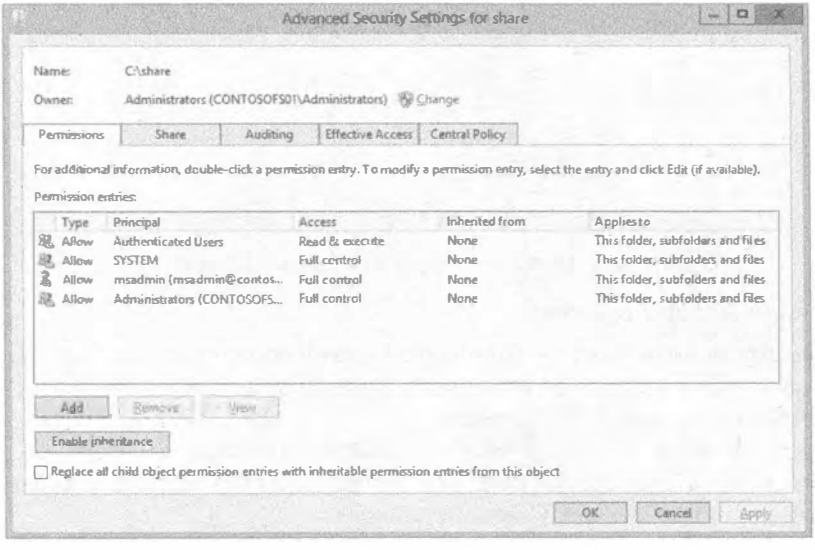


Рис. 15.50. Диалоговое окно Advanced Security Settings for share

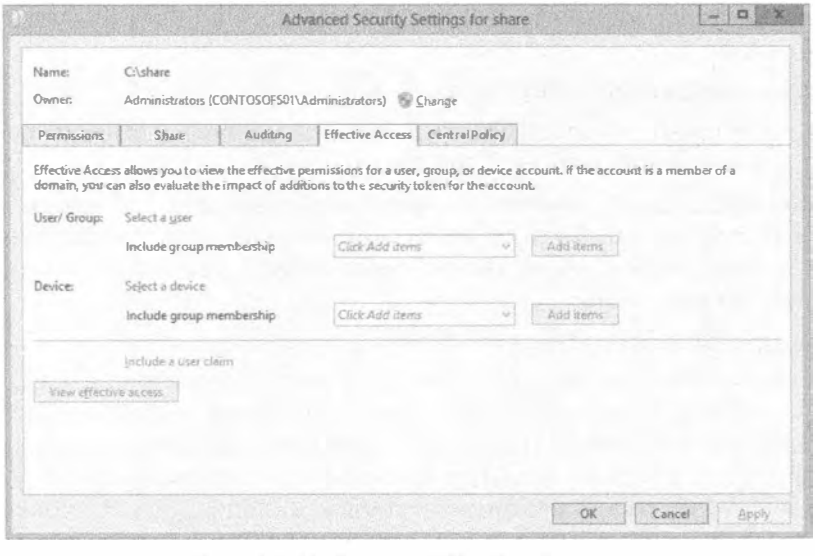


Рис. 15.51. Вкладка Effective Access

5. Щелкните на ссылке Select a user (Выбрать пользователя) и введите **Tom** в поле Search (Поиск); щелкните на кнопке Check Names (Проверить имена) и затем на кнопке OK. Вкладка Effective Access приобретает вид, показанный на рис. 15.52.

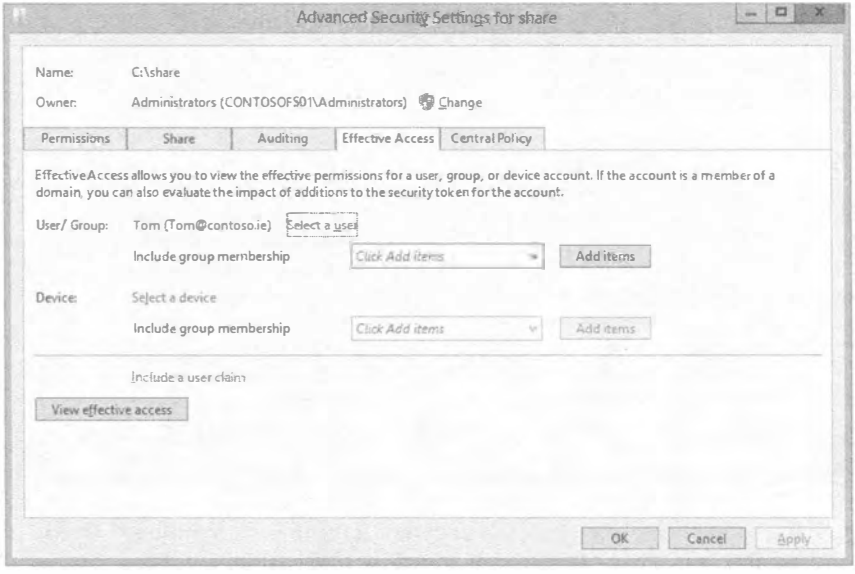


Рис. 15.52. Вкладка Effective Access после выбора пользователя

6. Щелкните на кнопке View effective access (Просмотреть действующий доступ) в нижней части вкладки.

   Мы ожидаем, что Том получит разрешение Read & Execute (Чтение и выполнение). На рис. 15.53 можно видеть результаты. Как и предполагалось, согласно сконфигурированной центральной политике доступа, том имеет разрешения Read (Чтение) и Read & Execute.

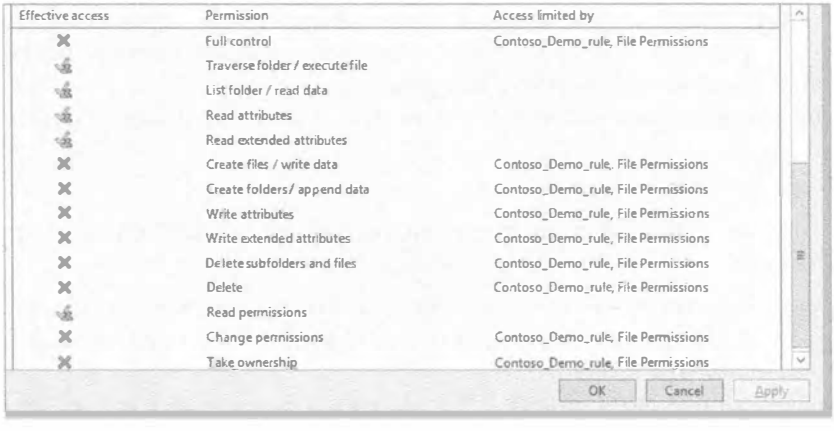


Рис. 15.53. Результаты вычисления действующего доступа для Тома

7. Повторите процесс для Кена.

   Вспомните, что Кен является сотрудником отдела IT, поэтому в соответствие с установленным правилом Кену должен быть запрещен доступ к этому общему ресурсу. Результаты для Кена приведены на рис. 15.54; как и ожидалось, доступ для него запрещен.

Effective access	Permission	Access limited by
✖	Full control	Contoso_Demo_rule, File Permissions
✖	Traverse folder / execute file	Contoso_Demo_rule
✖	List folder / read data	Contoso_Demo_rule
✖	Read attributes	Contoso_Demo_rule
✖	Read extended attributes	Contoso_Demo_rule
✖	Create files / write data	Contoso_Demo_rule, File Permissions
✖	Create folders / append data	Contoso_Demo_rule, File Permissions
✖	Write attributes	Contoso_Demo_rule, File Permissions
✖	Write extended attributes	Contoso_Demo_rule, File Permissions
✖	Delete subfolders and files	Contoso_Demo_rule, File Permissions
✖	Delete	Contoso_Demo_rule, File Permissions
✖	Read permissions	Contoso_Demo_rule
✖	Change permissions	Contoso_Demo_rule, File Permissions
✖	Take ownership	Contoso_Demo_rule, File Permissions

Рис. 15.54. Результаты вычисления действующего доступа для Кена

Попробуйте обратиться к общему ресурсу из клиента Windows, чтобы посмотреть, будет ли предоставлен доступ. В дополнение измените поле `Department` в Active Directory, после чего выйдите из системы и снова войдите, проверив наличие доступа.

Помощь в случае запрещения доступа

При ежедневной работе на крупном предприятии количество разрешений, добавляемых и удаляемых службой поддержки, может оказаться поразительно большим. Это интенсивная ручная работа, отнимающая немало времени. В Windows Server 2012 появилось средство помощи в случае запрещения доступа, призванное смягчить эту нагрузку. Данное средство перекладывает ответственность за управление доступом на владельца данных или требует от владельца данных, как минимум, предоставления службе поддержки значимой информации, которая позволила бы быстро обойти проблему с запретом доступа.

Помощь в случае запрещения доступа может быть сконфигурирована двумя путями:

- через групповую политику;
- посредством диспетчера ресурсов файлового сервера (FSRM) на индивидуальной основе.

Сначала мы покажем, как конфигурировать это средство через групповую политику. Позже в главе при рассмотрении классификации мы продемонстрируем его настройку в диспетчере FSRM.

Давайте создадим новый объект GPO для средства помощи в случае запрещения доступа, который будет применяться на уровне организации.

1. Находясь в системе машины (в данном случае на контроллере домена `ContosoDC01`), которая содержит консоль Group Policy Management, откройте этот инструмент и создайте новый объект групповой политики под названием **`Global-Access-Denied-Assistance`**.
2. Как и ранее, щелкните правой кнопкой мыши на только что созданном объекте GPO и выберите в контекстном меню пункт Edit (Редактировать). Откроется диалоговое окно Group Policy Management Editor (Редактор управления групповой политикой).
3. Перейдите к папке Computer Configuration⇨Policies⇨Administrative Templates⇨System⇨Access-Denied Assistance (Конфигурация компьютера⇨Политики⇨Административные шаблоны⇨Система⇨Помощь в случае запрещения доступа), как показано на рис. 15.55.
4. В правой части окна дважды щелкните на настройке Customize message for Access Denied errors (Настроить сообщение для ошибок запрещения доступа).

   Откроется окно Customize message for Access Denied errors (Настройка сообщения для ошибок запрещения доступа), представленное на рис. 15.56.
5. Выберите переключатель Enabled (Включена), чтобы сконфигурировать параметры этой новой политики.

   В области Options (Параметры) окна имеется пять разделов. В настоящем примере мы собираемся оставить настройки Add the following text to the end of the email (Добавить следующий текст в конец сообщения электронной почты) и Email recipients (Получатели сообщения электронной почты) в состоянии, установленном по умолчанию, но модифицируем настройки Display the following message to users who are denied access (Отображать следующее сообщение пользователям, которым запрещен доступ) и Enable users to request assistance (Разрешить пользователям запрашивать помощь).

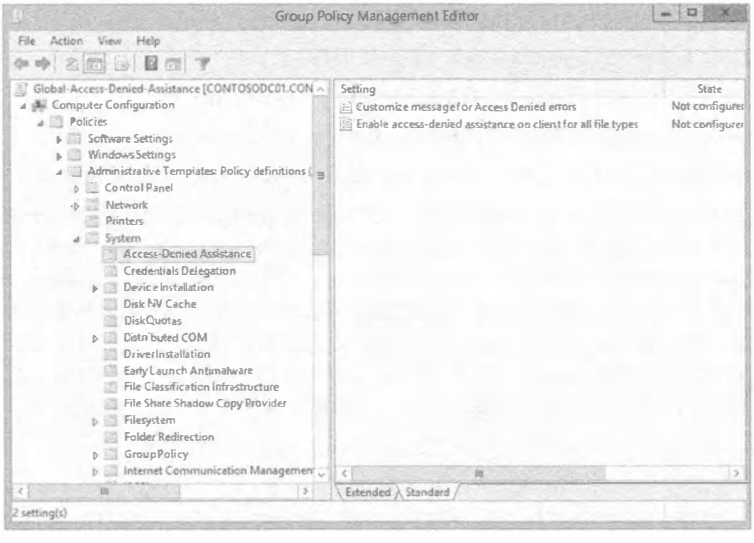


Рис. 15.55. Диалоговое окно Group Policy Management Editor с выбранной папкой Access-Denied Assistance

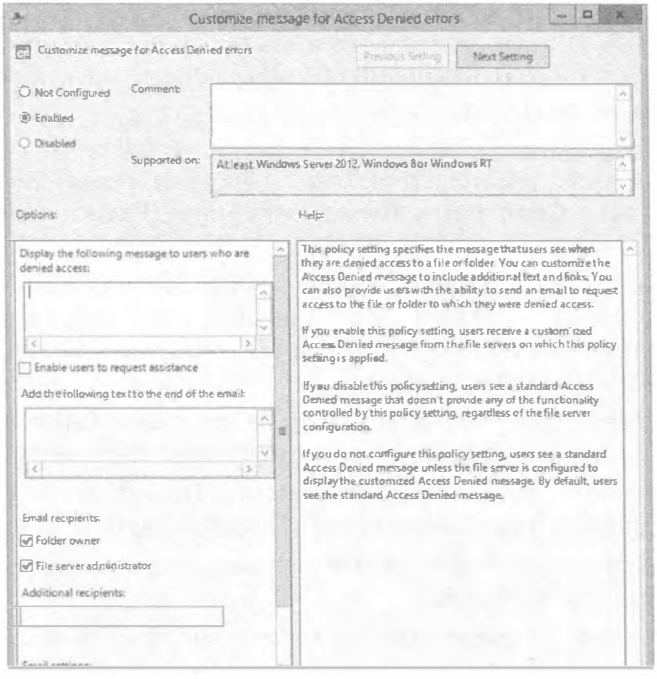


Рис. 15.56. Окно Customize message for Access Denied errors

6. Отметьте флажок Enable users to request assistance и затем добавьте сообщение, которое будет отображаться пользователю в случае запрета доступа.

   В области Display the following message to users who are denied access имеется возможность использовать предварительно определенные макросы, генерируя по-настоящему информативное сообщение для пользователя. В настоящее время доступны четыре макроса:

   - [Original File Path] (исходный путь к файлу);
   - [Original File Path Folder] (исходный путь к папке);
   - [Admin Email] (адрес электронной почты администратора);
   - [Data Owner Email] (адрес электронной почты владельца данных).

   Вот пример сообщения: Access is denied to [Original File Path]. Please contact [Data Owner Email] or click request assistance and provide business justification to access resources (Доступ к [Original File Path] запрещен. Пожалуйста, свяжитесь с [Data Owner Email] или щелкните на ссылке для запроса помощи и предоставления обоснований доступа к ресурсам). Понятно, что это всего лишь пример, но мы уже имеем две точки контакта и можем предоставить полный путь к файлу, содействуя устранению проблем у пользователей.
7. Завершив создание сообщения, щелкните на кнопке OK.
8. В окне Group Policy Management Editor дважды щелкните на настройке Enable access-denied assistance on client for all file types (Включить помощь в случае запрещения доступа на стороне клиента для всех типов файлов) и включите ее.
9. По завершении щелкните на кнопке OK.

10. Обновите политику на файловом сервере и на клиенте, выполнив команду **gpupdate /force** в окне командной строки, открытом от имени учетной записи администратора.
11. Проверьте на клиентской машине существование указанного ниже ключа реестра, удостоверившись в корректном применении политики.

    Должен существовать ключ `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer` и быть в наличии новое значение типа `DWORD` по имени `EnableShellExecuteFilestreamCheck`, установленное в `1`.

    Теперь попробуйте подключиться к общему ресурсу от имени учетной записи пользователя, не имеющего доступа (в данном случае Кена); будет получено более информативное сообщение и предоставлена возможность запроса помощи (рис. 15.57). Обратите внимание, что макрос [Data Owner Email] был заменен адресом электронной почты владельца папки, а конечному пользователю выдано дружественное в плане восприятия сообщение.

Рис. 15.57. Специальное сообщение о запрете доступа

12. Щелкните на ссылке Request Assistance (Запросить помощь). Откроется диалоговое окно Request Assistance (Запрос помощи), представленное на рис. 15.58.

    В сообщение включено имя пользователя и название общего ресурса, к которому он пытался получить доступ. Пользователю предлагается обосновать необходимость открытия ему доступа к ресурсу.
13. Щелкните на кнопке Send message (Отправить сообщение), чтобы отправить сообщение.

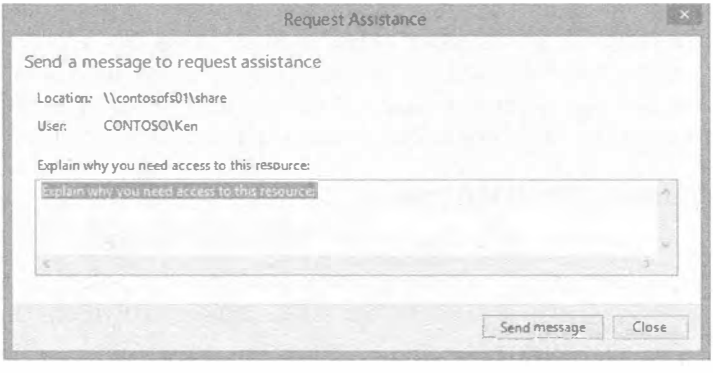


Рис. 15.58. Диалоговое окно Request Assistance

Настройка почтовых параметров

Чтобы можно было отправлять сообщения, в диспетчере FSRM должны быть сконфигурированы почтовые параметры. К тому же вы должны иметь в домене допустимый сервер SMTP, который может ретранслировать сообщения.

Утверждения — использование различных атрибутов

Мы рассмотрели базовый пример защиты данных с применением поля `Department`. А теперь мы продвинемся на шаг вперед и защитим данные на основе местоположения офиса и занимаемой должности. В этом примере мы собираемся задействовать двух пользователей из предыдущего примера, Тома и Кена. Они оба инженеры, но Том работает в офисе в Эмпайр-стейт-билдинг (Empire State Building), а Кен — в офисе в Крайслер-билдинг (Chrysler Building).

На общем ресурсе `ContosoFS01` созданы две подпапки: `Accounts` и `Engineering`. Предыдущая центральная политика доступа была применена к подпапке `Accounts`, чтобы ограничить доступ к ней только персоналу из отделов `Accounts` и `HR`. Для этого использовалась операция Or (Или), так что если пользователь работал в отделе `Accounts` или `HR`, он получал доступ к ресурсу. В данном случае мы хотим обеспечить доступ к ресурсу `Engineering` только для инженеров и (посредством операции And (И)) только для тех из них, которые работают в офисе внутри Эмпайр-стейт-билдинг. Давайте займемся этим. Прежде всего, мы резюмируем шаги, которые придется выполнить.

1. Создание типа утверждения для должности и офиса.
2. Создание свойства ресурса, основанного на типах утверждений.
3. Добавление свойства ресурса в список свойств ресурсов.
4. Создание правила доступа, используя ранее созданные свойства ресурсов.
5. Создание новой политики доступа и ее развертывание на файловых серверах.
6. Применение новой политики доступа к подпапке `Engineering`.
7. Проверка с помощью действующего доступа.

Настоятельно рекомендуется опробовать эти действия до того, как перейти непосредственно к проработке сценария. Нужна пошаговая демонстрация? Без проблем. Поскольку мы предоставили экранные снимки в предыдущем примере, мы здесь не будем их повторять, чтобы обеспечить вам небольшое испытание. Согласно перечисленным выше шагам, создадим для начала два новых утверждения.

Шаг 1: создание утверждения

Выполните следующие действия, чтобы создать утверждение.

1. Откройте административный центр Active Directory и в левой части окна щелкните на элементе Dynamic Access Control (Динамическое управление доступом).
2. Щелкните на элементе Claim Types (Типы утверждений) и выберите в меню Tasks (Задачи) пункт New⇨Claim Type (Создать⇨Тип утверждения).

3. В поле поиска над списком Source Attribute (Исходный атрибут) введите `title`.
4. Прокрутите содержимое окна до появления области Suggested Values (Предполагаемые значения) и выберите переключатель The following values are suggested (Предполагаются следующие значения).
5. Щелкните на кнопке Add (Добавить) и в открывшемся диалоговом окне введите значения из следующей таблицы:

Value (Значение)	Display name (Отображаемое имя)
`Engineer`	`Engineer` (Инженер)
`Accountant`	`Accountant` (Бухгалтер)
`Reception`	`Reception` (Секретарь)
`Director`	`Director` (Начальник отдела)

6. По завершении щелкните на кнопке OK.

Теперь с помощью тех же самых действий создайте новый тип утверждения для строений, в которых находятся офисы:

- `Empire State Building` (Эмпайр-стейт-билдинг)
- `Chrysler Building` (Крайслер-билдинг)

Часто бывает так, что отображаемое поле в учетной записи пользователя Active Directory не соответствует ожидаемому атрибуту буквально. Например, на рис. 15.59 показано поле `Office` (Офис). Однако в Active Directory нет атрибута, который имел бы название `Office`.

Рис. 15.59. Поле `Office` внутри свойств учетной записи пользователя Active Directory

Действительным атрибутом Active Directory для поля `Office` является `physicalDeliveryOfficeName` (рис. 15.60).

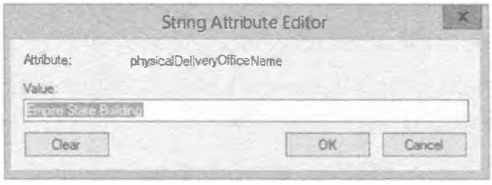


Рис. 15.60. Действительный атрибут Active Directory для поля `Office`

Шаг 2: создание свойства ресурса

Выполните следующие действия, чтобы создать свойство ресурса.

1. В главном окне Dynamic Access Control щелкните на элементе Resource Properties (Свойства ресурсов) и выберите в меню Tasks (Задачи) пункт New⇨Resource Property (Создать⇨Свойство ресурса).

   Вы увидите две доступных опции: свойство ресурса и ссылочное свойство ресурса. Помните, в чем разница между ними? Ссылочные свойства ресурсов предназначены для типов утверждений, которые уже сконфигурированы.

2. В диалоговом окне Create Reference Resource Property (Создание ссылочного свойства ресурса) выберите `physicalDeliveryOfficeName`, установите в качестве типа значения Single-valued Choice (Однозначный выбор) и щелкните на кнопке OK.

3. Повторите действия для должности.

Шаг 3: добавление в список свойств ресурсов

Этот шаг является в какой-то мере иллюзией, потому что `title` и `physicalDeliverOfficeName` уже известны как атрибуты. Вы увидите, что они присутствуют в глобальном списке свойств ресурсов (Global Resource Property List). Удостоверьтесь в этом до создания правил.

Шаг 4: создание центрального правила доступа

Выполните следующие действия, чтобы создать центральное правило доступа.

1. В главном окне Dynamic Access Control щелкните на элементе Central Access Rules (Центральные правила доступа) и выберите в меню Tasks (Задачи) пункт New⇨Central Access Rule (Создать⇨Центральное правило доступа).

2. Введите **`Contoso-Title-Office-Secure`** в качестве имени правила.

   Оставьте целевые ресурсы в том виде, как есть, поскольку вы хотите применять это правило ко всем ресурсам, которые укажете позже.

3. В области Permissions (Разрешения) щелкните на кнопке Edit (Редактировать) и затем на кнопке Add (Добавить).

4. Щелкните на ссылке Select a principal (Выбрать участника) и введите **`Authenticated Users`**.

5. Щелкните на кнопке Check Names (Проверить имена), а затем на кнопке OK.

6. В области Basic Permissions (Базовые разрешения) отметьте для данного примера флажок Full Control (Полный доступ).
7. Добавьте условия, как показано на рис. 15.61, и щелкните на кнопке OK.

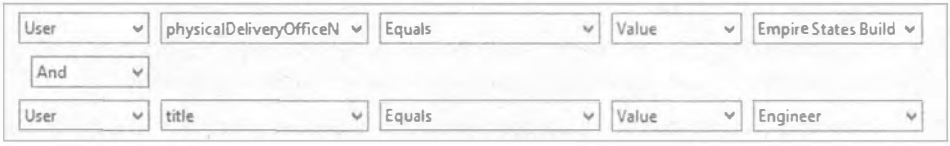


Рис. 15.61. Условия защиты

8. Щелкните на кнопке OK, чтобы закрыть диалоговое окно Advanced Security Settings for Permissions (Расширенные настройки безопасности для разрешений), и затем еще раз на кнопке OK, чтобы завершить создание центрального правила доступа.

Шаг 5: создание центральной политики доступа и ее развертывание через групповую политику

Выполните следующие действия, чтобы создать центральную политику доступа.

1. В главном окне Dynamic Access Control щелкните на элементе Central Access Policies (Центральные политики доступа) и выберите в меню Tasks (Задачи) пункт New⇨Central Access Policy (Создать⇨Центральная политика доступа).
2. В открывшемся диалоговом окне введите **`Contoso Secure By Title/Office`** в поле Name (Имя).
3. В области Central Access Rules (Центральные правила доступа) щелкните на кнопке Add (Добавить) и выберите созданное ранее правило.
4. Щелкните на кнопке OK, чтобы завершить создание политики.
5. Перейдите на машину, в которой имеется консоль Group Policy Management (Управление групповой политикой).
6. Откройте консоль Group Policy Management. Щелкните правой кнопкой мыши на созданной ранее групповой политике `CAP-Contoso-Demo` и выберите в контекстном меню пункт Edit (Редактировать).
7. Перейдите к папке Computer Configuration⇨Policies⇨Windows Settings⇨Security Settings⇨File System (Конфигурация компьютера⇨Политики⇨Настройки Windows⇨Настройки безопасности⇨Файловая система).
8. Щелкните правой кнопкой мыши на центральной политике доступа и выберите в контекстном меню пункт Manage Central Access Policies (Управлять центральными политиками доступа).
9. Добавьте новую политику, щелкните на кнопке OK и закройте окно консоли Group Policy Management.
10. Выполните на файловом сервере команду **`gpupdate /force`**, чтобы применить новую политику.

Шаг 6: применение политики к папке Engineering

Выполните следующие действия, чтобы применить политику к папке Engineering.

1. Перейдите к общему ресурсу, щелкните на его имени правой кнопкой мыши и выберите в контекстном меню пункт Properties (Свойства).
2. В открывшемся диалоговом окне свойств перейдите на вкладку Security (Безопасность) и щелкните на кнопке Advanced (Дополнительно).
3. Щелкните на центральной политике доступа в диалоговом окне Advanced Security Settings for Engineering (Расширенные настройки безопасности для Engineering).
4. Щелкните на кнопке Change (Изменить) и выберите политику Contoso Secure By Title/Office.
5. Просмотрите правила, удостоверившись в их корректности.

Не закрывайте это диалоговое окно!

Шаг 7: проверка с помощью действующего доступа

Выполните следующие действия, чтобы провести проверку с помощью действующего доступа.

1. Перейдите на вкладку Effective Access (Действующий доступ).
2. Щелкните на ссылке Select a user (Выбрать пользователя) и введите **Tom** в поле Search (Поиск).
3. Щелкните на кнопке Check Names (Проверить имена) и затем на кнопке OK.
4. Щелкните на кнопке View effective access (Просмотреть действующий доступ).

   Поскольку пользователь Tom является инженером, работающим в офисе в Эмпайр-стейт-билдинг, он должен получить полный доступ к папке Engineering.
5. Повторите эти действия для пользователя Ken.

   Хотя пользователь Ken — инженер, однако он работает не в офисе в Эмпайр-стейт-билдинг, поэтому он не должен получить доступ к этой папке.

> **Важно! Разрешения NTFS — наименее привилегированные правила**
>
> Если к этому времени вы еще не заметили, центральные политики доступа работают с разрешениями безопасности NTFS. Во всех случаях преимущество получает наименьшая привилегия. Например, если вы предоставили разрешение Full Control (Полный доступ) посредством центральной политики доступа, а максимальным разрешением NTFS для пользователя является Read-Only (Только чтение), вы увидите на вкладке Effective Access результирующие права Read-Only!

Разрешения устанавливаются путем объединения с помощью операции "И" центральных политик доступа и разрешений NTFS. Проверьте это самостоятельно.

Классификация

Первым делом мы кратко поясним, что понимается под *классификацией*. Мы уверены, что вы знакомы с фильмами об армии, и наверняка замечали в них демонстрацию какого-нибудь файла с большой печатью, гласящей "Совершенно секретно". Так просто, да? По существу вы обсуждаете с людьми содержимое файла. На современном предприятии документы могут классифицироваться на основе их важности для компании. Например, в больнице информация о пациентах является крайне конфиденциальной, поэтому она может быть классифицирована с помощью признака "Конфиденциальная". Распространенная область действия состоит из трех классификаций.

- **Высокое влияние на бизнес-деятельность.** Информация, которая может значительно навредить репутации или основной бизнес-деятельности компании вплоть до ее закрытия или начала уголовного расследования.
- **Среднее влияние на бизнес-деятельность.** Информация, которая может вызвать большие затруднения или причинить вред будущему компании.
- **Низкое влияние на бизнес-деятельность.** Информация, которая обычно доступна или не имеет конфиденциальный характер.

Крайне важно уяснить потребность в классификации документов внутри предприятия. Выражаясь просто: действительно ли вы хотите, чтобы произошла утечка информации за пределы компании, в которой, например, раскрываются секреты коммерческой деятельности, вызывая непоправимый ущерб всей компании?

Классификация документов предоставляет компаниям шанс предотвратить такой тип утечки данных. К примеру, посредством службы управления правами (Rights Management Service — RMS), входящей в состав Windows Server, можно обнаруживать, что документ является совершенно секретным, используя разнообразные правила, и затем его содержимое может быть зашифровано или заблокировано от просмотра неавторизованным персоналом.

Как вы можете себе представить, крупной проблемой является то, каким образом классифицировать все существующие документы внутри предприятия. Скорее всего, ранее не было привычки помещать такую информацию в свойства файла при сохранении документа. Если на предприятии желают модифицировать классификацию в своих документах, это будет затратной работой с точки зрения как времени, так и финансов. В Windows Server 2012 у вас имеется возможность автоматической классификации документов, так что вы можете при необходимости защищать их содержимое с помощью RMS или блокировать к ним доступ посредством динамического управления доступом. Интересно отметить, что классификация файлов была доступна, начиная с версии Windows Server 2008.

Классификация документа

Документ допускается классифицировать вручную. В испытательной среде у нас есть файл `Finance.rtf`, хранящийся в папке `C:\share\accounts`.

1. Щелкните правой кнопкой мыши на имени этого файла (в данном случае `Finance.rtf`) и выберите в контекстном меню пункт Properties (Свойства).

   Откроется диалоговое окно Finance Properties (Свойства `Finance`) с пятью вкладками (рис. 15.62).

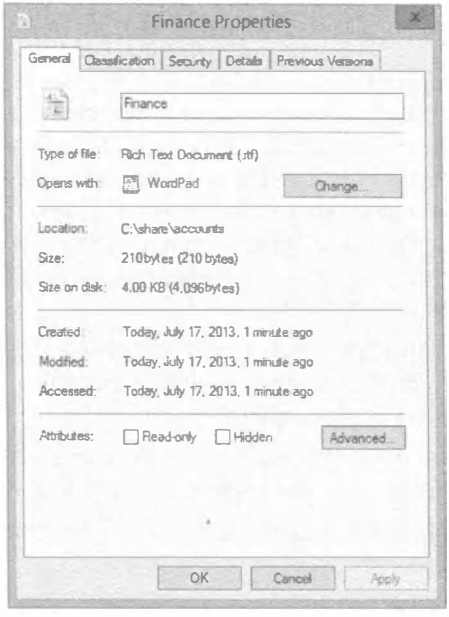


Рис. 15.62. Диалоговое окно Finance Properties

Рис. 15.63. Вкладка Classification

2. Перейдя на вкладку Classification (Классификация), вы заметите, что определенные сведения уже заполнены (рис. 15.63). Можете ли вы сказать что-нибудь об этих данных? Это свойства ресурсов, которые мы опубликовали ранее в этой главе через динамическое управление доступом.
3. Щелкните на `department_contoso` и выберите `Accounts`.

   Поздравляем! Вы только что классифицировали свой первый документ.

Как уже упоминалось, такой подход может оказаться утомительным, если это придется делать для всех существующих документов. В Windows Server 2012 имеется инструмент под названием File Server Resource Manager (Диспетчер ресурсов файлового сервера), который по умолчанию не устанавливается; он доступен через меню Tools (Сервис) диспетчера серверов.

Давайте кратко рассмотрим диспетчер ресурсов файлового сервера для Windows Server 2012. В меню Tools диспетчера серверов выберите пункт File Server Resource Manager (Диспетчер ресурсов файлового сервера); откроется окно консоли MMC, как показано на рис. 15.64.

В левой части видны элементы Quota Management (Управление квотами), File Screening Management (Управление блокировкой файлов), Storage Reports Management (Управление отчетами по хранилищу), Classification Management (Управление классификацией) и File Management Tasks (Задачи управления файлами). В данном случае нас интересует элемент Classification Management. Щелкните на стрелке рядом с ним, чтобы отобразить две дополнительных опции:

- Classification Properties (Свойства классификации)
- Classification Rules (Правила классификации)

Рис. 15.64. Оснастка File Server Resource Manager консоли MMC

Свойства классификации

Свойства классификации могут быть унаследованы через динамическое управление доступом или установлены локально. Вы можете конфигурировать варианты использования Authorization (Авторизация), File Classification (Классификация файлов) и Folder Management (Управление папками). Здесь также можно конфигурировать Access-Denied Assistance (Помощь в случае запрещения доступа), но только для локального файлового сервера.

Обратите внимание, что в этой консоли вы не можете модифицировать элементы с областью действия Global (Глобальная), поскольку они унаследованы из DAC.

Правила классификации

Правила классификации позволяют настраивать условия, которые будут автоматически классифицировать документы. В нашем примере мы собираемся исследовать этот аспект более глубоко. С помощью нескольких шагов, приведенных далее, мы покажем, как создавать подходящие правила, которые позволяют классифицировать документы и папки. Мы проведем вас через все требуемые действия и продемонстрируем функционирование автоматической классификации.

Для автоматической классификации документов вам понадобится создать правило классификации. Прежде всего, чтобы содействовать последующему конфигурированию и объяснению некоторых элементов, необходимо отобразить папки с применением свойства Folder Usage (Использование папок).

1. Находясь в оснастке File Server Resource Manager (Диспетчер ресурсов файлового сервера) консоли MMC, щелкните на элементе Classification Properties (Свойства классификации).
2. Дважды щелкните на свойстве Folder Usage (Использование папок), как показано на рис. 15.65.

   Откроется диалоговое окно Edit Local Classification Property (Редактирование локального свойства классификации).

3. Прокрутите список в самый низ, щелкните на пустом поле и введите **Accounts**.

4. Повторите шаг 3, но на этот раз введите **Engineering**, и по завершении щелкните на кнопке OK (рис. 15.66).

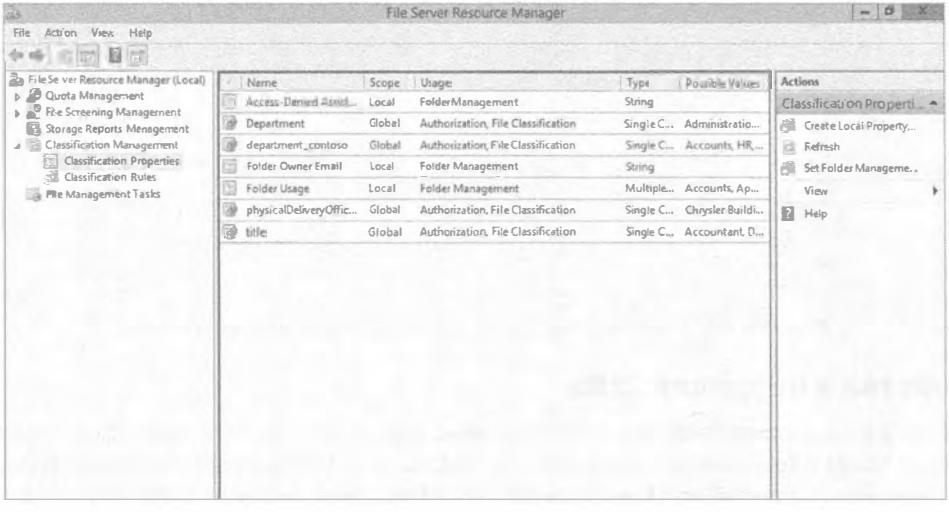


Рис. 15.65. Отображение свойства Folder Usage в оснастке File Server Resource Manager

Рис. 15.66. Добавление значений к свойству Folder Usage

А теперь давайте сконфигурируем наши папки.

1. Выберите в меню Actions (Действия), расположенном в правой части окна консоли MMC, пункт Set Folder Management (Установить управление папками).

   Откроется диалоговое окно Set Folder Management Properties (Свойства установки управления папками).

2. В поле со списком Property (Свойство) выберите элемент Folder Usage (Использование папок), как показано на рис. 15.67.

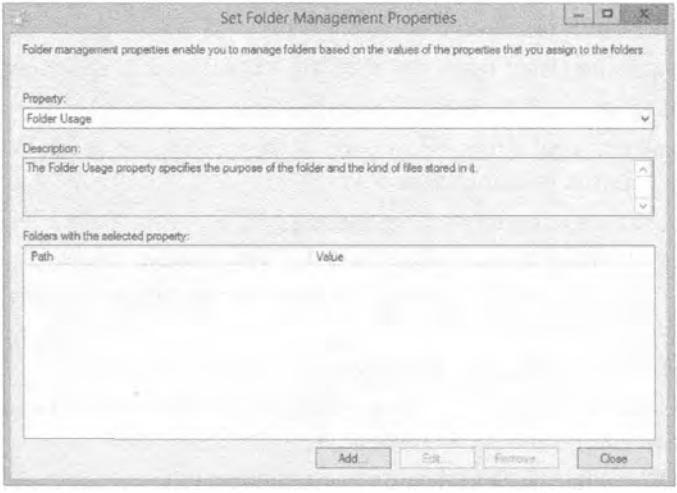


Рис. 15.67. Диалоговое окно Set Folder Management Properties

3. Щелкните на кнопке Add (Добавить), проследуйте по пути к папке `Accounts` и отметьте флажок Accounts, что проиллюстрировано на рис. 15.68. Щелкните на кнопке OK.
4. Повторите шаг 3 для папки `Engineering` (рис. 15.69).
5. Щелкните на кнопке Close (Закрыть).

Рис. 15.68. Добавление значения к папке `Accounts`

Рис. 15.69. Добавление значения к папке `Engineering`

Проделанная работа окажет содействие позже, при создании правил классификации, т.к. только что ратифицированные свойства будут доступны для выбора во время построения правила.

1. Щелкните на элементе Classification Rules (Правила классификации) в левой части окна консоли MMC.
2. Выберите в меню Actions (Действия), расположенном в правой части окна консоли MMC, пункт Create Classification Rule (Создать правило классификации).

   Откроется диалоговое окно Create Classification Rule (Создание правила классификации), представленное на рис. 15.70.
3. В поле Rule name (Имя правила) введите `File Classification`.
4. Перейдите на вкладку Scope (Область действия).

   Именно здесь в игру вступает та работа, которая была ранее выполнена в отношении свойства Folder Usage.
5. Отметьте флажки Accounts и Engineering.

   На рис. 15.71 обратите внимание на то, что список The following folders are included in this scope (Следующие папки включены в эту область действия) автоматически заполнен.
6. Далее перейдите на вкладку Classification (Классификация).

   На вкладке Classification первое, что следует выбрать — это метод классификации. По умолчанию таких методов три.

   - **Content Classifier (Классификатор содержимого).** Позволяет настраивать шаблоны, при обнаружении которых внутри файла происходит автоматическая классификация документа.

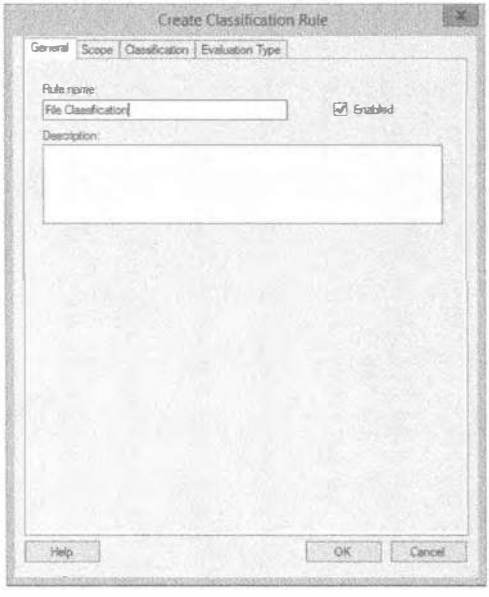


Рис. 15.70. Диалоговое окно Create Classification Rule

Рис. 15.71. Вкладка Scope

- **Folder Classifier (Классификатор папок).** Автоматически классифицирует все папки с указанным значением.
- **Windows PowerShell Classifier (Классификатор Windows PowerShell).** Позволяет написать собственный агент обнаружения на PowerShell и затем выполнять его. Является исключительно мощным методом для опытных пользователей.

7. В этом упражнении выберите вариант Content Classifier.
8. В поле со списком Property (Свойство) выберите `department_contoso` и укажите `Accounts` в качестве значения (рис. 15.72).
9. Щелкните на кнопке Configure (Конфигурировать) в области Parameters (Параметры).

   Откроется диалоговое окно Classification Parameters (Параметры классификации), показанное на рис. 15.73. В раскрывающемся списке Expression Type (Тип выражения) доступны три элемента:

   - Regular expression (Регулярное выражение)
   - String (case-sensitive) (Строка (чувствительная к регистру символов))
   - String (Строка)

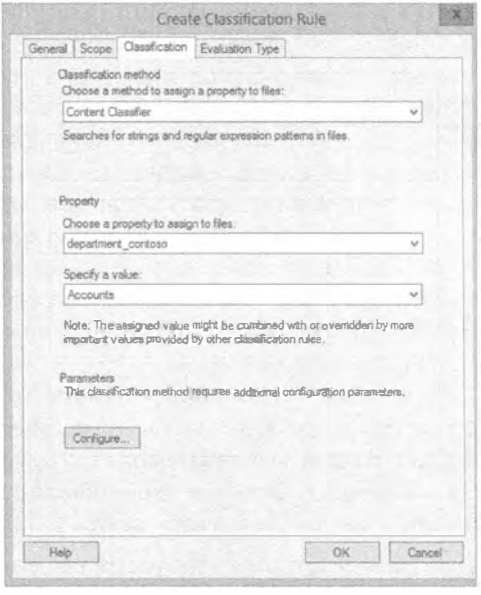


Рис. 15.72. Конфигурирование классификации

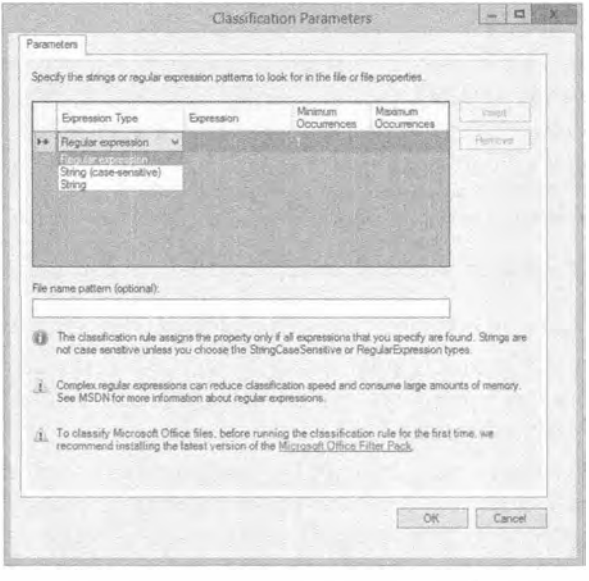


Рис. 15.73. Диалоговое окно Classification Parameters

Все это объясняется в следующих двух разделах.

Типы выражений

Регулярные выражения применяются для идентификации шаблонов внутри данных, подобно функции поиска в Notepad, когда вы нажимаете <F3>, вводите искомую строку и функция пытается ее найти. Регулярные выражения выполняют аналогичное действие. Традиционно они используются в мире программирования или телефонии для обнаружения шаблонов в данных или манипулирования телефонными номерами. Например, можно создать регулярное выражение для распознавания номера кредитной карты.

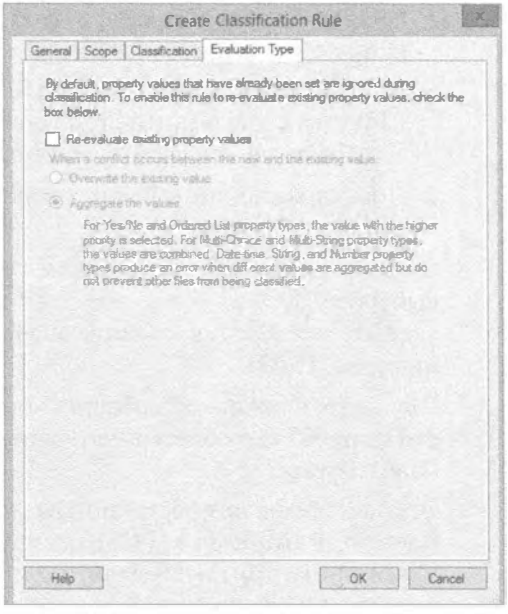


Рис. 15.74. Вкладка Evaluation Type

Далее мы предоставим краткое руководство по регулярным выражениям. Но для начала мы продемонстрируем, как обнаружить простой строковый шаблон `Finance` и как после его обнаружения внутри документа соответствующим образом его классифицировать.

1. Для целей этого примера выберите вариант String (Строка) в поле со списком Expression Type (Тип выражения) внутри диалогового окна Classification Parameters (Параметры классификации), т.к. мы собираемся обнаруживать строковый шаблон внутри документа.
2. В поле Expression (Выражение) введите **`Finance`** и щелкните на кнопке OK.

> **Создание нескольких правил**
>
> Можно иметь сразу множество параметров оценки разных типов. Однако оцениваемый файл должен соответствовать всем указанным критериям, и оценка производится только один раз для каждого файла во время выполнения. Если необходимо искать и сопоставлять с несколькими разными шаблонами, придется создать множество правил.

3. Перейдите на вкладку Evaluation Type (Тип оценки), представленную на рис. 15.74.

   Здесь имеется возможность повторной оценки существующих свойств и в случае возникновения конфликта либо перезаписывать предыдущее значение, либо объединять значения.
4. В данном случае отметьте флажок Re-evaluate existing property values (Повторно оценивать значения существующих свойств) и затем выберите переключатель Overwrite the existing value (Перезаписывать существующее значение).
5. Щелкните на кнопке OK.

Правило классификации готово. Осталось его либо запустить вручную, выделив правило и выбрав в меню Actions (Действия) пункт Run Classification Rule (Запустить правило классификации), либо подождать, пока его выполнит планировщик задач.

В случае запуска вручную отображается окно с запросом о том, выполнять задачу в фоновом режиме или ожидать ее завершения (рис. 15.75).

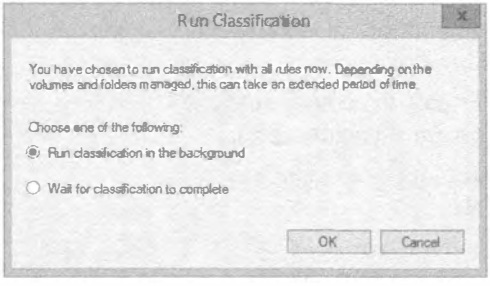


Рис. 15.75. Варианты выполнения классификации при запуске вручную

Мы оставляем выбранным переключатель Run classification in the background (Выполнить классификацию в фоновом режиме), что позволит планировщику задач выполнить задачу классификации на основе расписания. Однако сначала необходимо сконфигурировать параметры для автоматической классификации файлов.

1. В левой части оснастки File Server Resource Manager (Диспетчер ресурсов файлового сервера) консоли MMC перейдите в самый верх древовидного представления и выберите узел File Server Resource Manager (Local) (Диспетчер ресурсов файлового сервера (локальный)).
2. Щелкните на этом узле правой кнопкой мыши и выберите в контекстном меню пункт Configure Options (Сконфигурировать параметры), как показано на рис. 15.76.

Рис. 15.76. Выбор конфигурирования параметров для автоматической классификации файлов

3. В открывшемся диалоговом окне File Server Resource Manager Options (Параметры диспетчера ресурсов файлового сервера) перейдите на вкладку Automatic Classification (Автоматическая классификация).

   Как видите, по умолчанию автоматическая классификация отключена.

4. Отметьте флажок Enable fixed schedule (Включить фиксированное расписание).
5. В поле Run at (Выполнять в) укажите время `01:00:00 AM`.
6. Выберите переключатель Weekly (Еженедельно) и отметьте флажок Sunday (Воскресенье).
7. Отметьте флажок Allow continuous classification for new files (Разрешить непрерывную классификацию новых файлов) и оставьте остальные параметры без изменений (рис. 15.77).
8. Щелкните на кнопке OK.

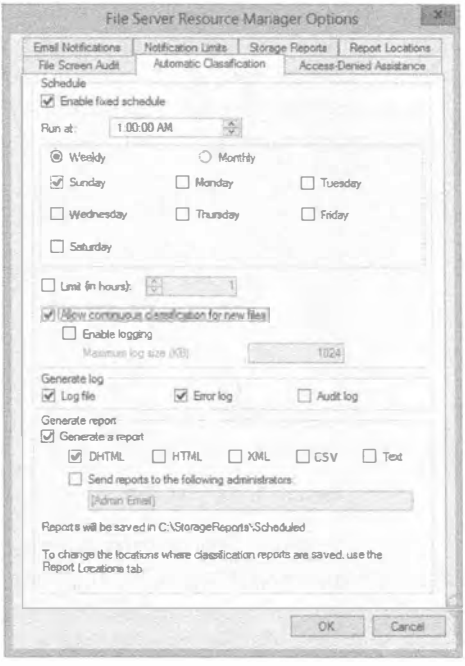


Рис. 15.77. Параметры автоматической классификации файлов по расписанию

Теперь можете удостовериться в том, что расписание было настроено в планировщике задач.

1. Откройте планировщик задач и перейдите к папке Task Scheduler Library⇨Microsoft⇨Windows⇨File Server Resource Manager (Библиотека планировщика задач⇨Microsoft⇨Windows⇨Диспетчер ресурсов файлового сервера).

   Здесь вы увидите новую задачу по имени `FciClassification` с параметрами, которые вы сконфигурировали.

2. Проверьте, под управлением чего эта задача выполняется — правильно, под управлением PowerShell.

Поскольку вы хотите запустить задачу сразу, не дожидаясь часа ночи в воскресенье, понадобится выполнить кучную классификацию, но не сейчас.

1. Сначала необходимо проверить документ, на котором будет тестироваться работа классификации. Откройте файл, который хотите использовать для тестирования. В нашей испытательной среде имеется единственный файл `Private Data.rtf` в папке `C:\share\accounts`. Его содержимое можно видеть на рис. 15.78. Вспомните, что правило классификации настроено на классификацию содержимого и поиск одного вхождения строки `Finance`. В результате документ должен быть классифицирован как относящийся к отделу `Accounts`.
2. Далее проверьте существующую классификацию документа, щелкнув на его имени правой кнопкой мыши и выбрав в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом меню свойств перейдите на вкладку Classification (Классификация).

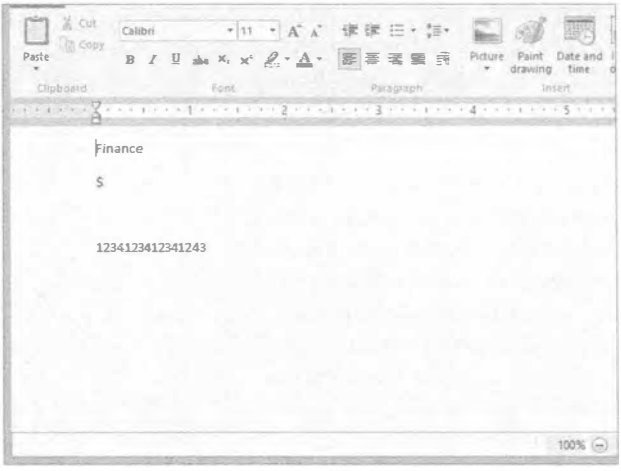


Рис. 15.78. Содержимое файла `Private Data.rtf`

На рис. 15.79 видно, что в настоящий момент классификация у файла отсутствует.

3. Возвратитесь в оснастку File Server Resource Manager и запустите правило классификации файлов. Для этого выделите необходимое правило и выберите в расположенном справа меню Actions (Действия) пункт Run Classification With All Rules now (Запустить классификацию со всеми правилами прямо сейчас). В появившемся диалоговом окне оставьте выбранным переключатель Run classification in the background (Выполнить классификацию в фоновом режиме) и щелкните на кнопке OK.

Рис. 15.79. Отсутствие классификации у файла `Private Data.rtf`

Рис. 15.80. Установка классификации файла `Private Data.rtf`

4. Подождите завершения процесса и снова проверьте классификацию файла. Как показано на рис. 15.80, классификация `department_contoso` была установлена в `Accounts`.

Чтобы удостовериться в том, что здесь не произошла какая-то ошибка и не была также включена папка `Engineering`, давайте проверим ее содержимое и классификацию файлов. В испытательной среде внутри папки `C:\share\engineering` содержится файл по имени `Engineer Scope.rtf`, и как можно заметить на рис. 15.81, даже после завершения всего процесса классификация у данного файла отсутствует. Почему? Да потому, что мы не устанавливали для него какие-либо правила.

Опробуйте разные комбинации и создайте новые правила самостоятельно, чтобы по-настоящему вникнуть в принципы классификации, рассмотренные до сих пор.

Рис. 15.81. Отсутствие классификации у файла `Engineer Scope.rtf`

Регулярные выражения

Ранее было обещана краткая демонстрация регулярных выражений. Это тот предмет, о котором вы должны спрашивать у опытных программистов или инженеров в отрасли телефонии, т.к. именно они являются специалистами в этой области и обычно способны конструировать исключительно сложные, но полезные выражения.

Кроме того, поищите в Интернете ссылки на учебные руководства по регулярным выражениям — там есть немало полезных справочников как на русском, так и на английском языке.

Как и большинство средств, регулярные выражения лучше изучать на их практическом применении. Поэтому давайте рассмотрим базовый пример. Предположим, что вы хотите распознавать номер кредитной карты. Первым делом вы должны посмотреть, какими характеристиками обладает номер кредитной карты, и проще всего начать с того, что он всегда содержит 12 цифр.

Чтобы обнаруживать комбинацию из 12 цифр с помощью регулярного выражения, понадобится следующий запрос:

```
"\d{12}"
```

Здесь `\d` означает “обнаруживать цифры”, а `{12}` — “в количестве 12 штук”.

Другой способ опознания записи с номером кредитной карты вида 1234-1234-1234-1234 выглядит так:

```
"\d{4}-\d{4}-\d{4}-\d{4}"
```

Как видите, все довольно просто. Будем надеяться, что в вашей среде имеется не так много комбинаций из 12 цифр, которые не являются номерами кредитных карт и окажутся ошибочно классифицированными посредством такого базового правила.

Однако мы можем внести ряд дополнительных уточнений. К примеру, пусть карты Visa начинаются с цифры 4, после которой следует комбинация из 11 других цифр. Как в этом случае будет выглядеть регулярное выражение? Вот так:

```
"\d[4]{11}"
```

Ниже приведен стандартный формат номера кредитной карты:

```
"{\d[4]{3}-\d{4}-\d{4}-{\d{4}"
```

А теперь рассмотрим другой пример. Компании чаще всего опасаются утечки интеллектуальной собственности и сведений о заработной плате. Полагаем, вы согласитесь с этим. По нашему мнению, эти фрагменты информации нуждаются в защите, так что давайте построим еще одно регулярное выражение. Мы также будем использовать данный пример позже при интеграции такого регулярного выражения с конфигурацией динамического управления доступом.

Но для начала, как могло бы выглядеть регулярное выражение для обнаружения слов *intellectual property* (интеллектуальная собственность)?

Оно может быть простым: `"intellectual.*property"`

А что вы думаете относительно регулярного выражения для слова *payroll* (платежная ведомость)?

Примите во внимание несколько дополнительных примеров наподобие слов *wages* (заработная плата) и *pensions* (пенсии).

Ниже перечислены ссылки на сведения о регулярных выражениях, которые могут оказаться полезными:

```
http://msdn.microsoft.com/en-us/library/ae5bf541(v=vs.80).aspx
http://www.solmetra.com/scripts/regex/index.php
http://www.regular-expressions.info/reference.html
http://www.cheatography.com/davechild/cheat-sheets/regular-expressions/
```

Способность обнаруживать шаблоны вроде этого и даже более сложные их вариации может обеспечить высокую гибкость при классификации данных внутри предприятия, что позволит автоматически защищать данные с помощью набора других инструментов, таких как Rights Management Server (Сервер управления правами).

Защита данных с использованием DAC и классификации файлов

В завершение этой главы давайте рассмотрим реалистичный пример, с которым вы можете столкнуться на своем рабочем месте. Большинство современных компаний в какой-то момент начинают иметь дело с номерами кредитных карт. При этом ответственность за обеспечение безопасности таких данных возложена на саму компанию. В реальном мире номера кредитных карт хранятся в зашифрованных базах данных, но в нашем примере компания Contoso хранит их в документе Word.

Мы должны защитить не только компанию, но также и информацию, чтобы не произошла ее утечка. Мы не хотим, чтобы инженеры могли войти на общий ресурс и скопировать файл с номерами кредитных карт. Это может повлечь за собой пагубные последствия.

С учетом всего сказанного, ниже представлен список того, что мы собираемся предпринять.

- Создать файл RTF, содержащий внутри номер кредитной карты.
- Создать файл RTF, содержащий внутри слово *payroll*.
- Создать файл RTF, содержащий внутри слова *Intellectual Property*.
- Создать правило классификации для обнаружения указанных фрагментов с применением регулярных выражений и строки в содержимом.
- Создать центральную политику доступа, которая будет использовать классификацию файлов для защиты ресурса.

Итак, за работу. Для начала создадим три необходимых документа.

1. В системе файлового сервера (в этом примере `ContosoFS01`) перейдите в папку `C:\share\accounts`.
2. Щелкните правой кнопкой мыши на имени папки и выберите в контекстном меню пункт New⇨Rich Text Document (Создать⇨Документ RTF), как показано на рис. 15.82.

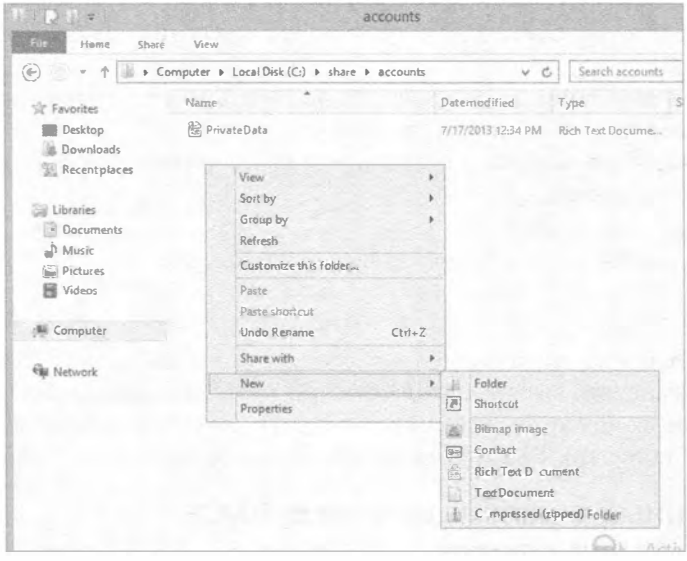


Рис. 15.82. Создание документа RTF

3. Введите **`File1`** в качестве его имени.

   Мы специально используем обобщенное имя, которое не отражает характер содержимого.
4. Дважды щелкните на имени `File1`, чтобы открыть файл, и введите номер, состоящий из 12 цифр.
5. Сохраните и закройте файл.
6. Повторите описанную процедуру для файлов с именами **`File2`** и **`File3`**.
7. Внутрь файла `File2` поместите произвольные слова и включите слово *payroll*, а внутрь файла `File3` — произвольные слова и слова *Intellectual Property*.
8. Сохраните все файлы.

9. Быстрый тест: проверьте классификацию каждого документа и удостоверьтесь в том, что ничего не установлено.

Далее создадим правила классификации для автоматической классификации этих документов.

1. В системе файлового сервера `ContosoFS01` откройте оснастку File Server Resource Manager (Диспетчер ресурсов файлового сервера) консоли MMC.

   Необходимо создать три новых правила, т.к. мы ищем разные шаблоны, которые не обязательно в полном составе будут присутствовать в одном файле.
2. Щелкните на элементе Classification Rules (Правила классификации) и в меню Actions (Действия), расположенном справа, выберите пункт Create Classification Rule (Создать правило классификации).
3. На вкладке General (Общие) в области Rule Name (Имя правила) введите **`Auto Classify For Credit Cards`**.
4. Перейдите на вкладку Scope (Область действия) и щелкните на `Accounts`.

   Обратите внимание, что общий ресурс `Accounts` заполнился автоматически.

   Быстрый тест: как сюда попали папки, включенные в область действия `Accounts`?
5. Перейдите на вкладку Classification (Классификация).
6. В качестве метода классификации выберите Content Classifier (Классификатор содержимого).
7. В поле со списком Property (Свойство) выберите свойство для назначения файлам.
8. Выберите `department_contoso`, а в поле Specify a value (Указать значение) укажите `Accounts`.
9. Щелкните на кнопке Configure (Конфигурировать) в области Parameters (Параметры).

   Быстрый тест: как выглядит регулярное выражение для обнаружения номера из 12 цифр? Подумайте о шаблоне для сопоставления.
10. Завершив ввод параметров, щелкните на кнопке OK.
11. Перейдите на вкладку Evaluation Type (Тип оценки), отметьте флажок Re-evaluate existing property values (Повторно оценивать значения существующих свойств) и затем выберите переключатель Overwrite the existing value (Перезаписывать существующее значение).
12. Щелкните на кнопке OK.
13. Описанным методом создайте еще два правила, в которых используется следующая информация:

Имя правила	Что ищет	Тип выражения	Минимальное количество вхождений
`Auto Classify Payroll`	`Payroll`	String (Строка)	1
`Auto Classify`	`Intellectual Property`	Regular Expression (Регулярное выражение)	1

14. После создания всех правил запустите классификацию вручную и дождитесь ее завершения.
15. Удостоверьтесь в работоспособности правил и корректности классификации документов.

Итак, правила классификации файлов определены и работают. Теперь нужно построить политику, чтобы к этим типам документов имел доступ только персонал из отдела `Accounts` или `HR`.

Но сначала нужно подготовиться. Чтобы все прошло успешно, необходимо удалить все центральные политики доступа, которые уже были применены к папке `C:\share\accounts`.

1. Щелкните правой кнопкой мыши на имени папки и выберите в контекстном меню пункт Properties (Свойства). В открывшемся диалоговом окне свойств папки перейдите на вкладку Security (Безопасность) и щелкните на кнопке Advanced (Дополнительно). В диалоговом окне Advanced Security Settings (Расширенные настройки безопасности) перейдите на вкладку Central Policy (Центральная политика), щелкните на ссылке Change (Изменить), в раскрывающемся списке выберите элемент No Central Policy Applied (Нет примененной центральной политики) и щелкните на кнопке OK.
2. Войдите в систему на клиентской машине от имени учетной записи пользователя, не относящегося к отделу `Accounts` (в нашем примере это `Ken`) и удостоверьтесь в наличии возможности просмотра папки `Accounts` и доступа к файлам.
3. Если после удаления центральной политики вы не можете получить доступ к файлам, проверьте разрешения и при необходимости назначьте для папки подходящие разрешения, такие как Full Control (Полный доступ) группе `Domain Users` (Пользователи домена).

Теперь понадобится защитить данные с помощью новой центральной политики доступа.

1. В главном окне Dynamic Access Control административного центра Active Directory щелкните на элементе Central Access Rules (Центральные правила доступа).
2. Выберите в меню Tasks (Задачи) справа пункт New⇨Central Access Rule (Создать⇨Центральное правило доступа).
3. В открывшемся диалоговом окне Create Central Access Rule (Создание центрального правила доступа) введите **`Securing Auto Classified Accounts Data`** в поле Name (Имя).
4. Ранее область Target Resources (Целевые ресурсы) оставалась незатронутой, но теперь щелкните в ней на кнопке Edit (Редактировать).

   Целевые ресурсы будут работать вместе с классификацией файла для его защиты. Экран, показанный на рис. 15.83, очень похож на другие экраны, основанные на условиях, с которыми вы имели дело в предшествующих упражнениях.
5. Приведите все в соответствие с рис. 15.83 и щелкните на кнопке OK. Теперь мы нацелены на все файлы, которые были классифицированы для `Accounts`.

Рис. 15.83. Установка целевых ресурсов

Далее потребуется установить разрешения; полный доступ к документам должен иметь только персонал из отделов `HR` и `Accounts`.

1. В области Permissions (Разрешения) выберите переключатель Use following permissions as current permissions (Использовать следующие разрешения как текущие разрешения), щелкните на кнопке Edit (Редактировать) и в открывшемся диалоговом окне Advanced Security Settings for Permissions (Расширенные настройки безопасности для разрешений) щелкните на кнопке Add (Добавить).
2. Откроется диалоговое окно Permission Entry for Permissions (Запись разрешения для разрешений). Щелкните на ссылке Select a principal (Выбрать участника), введите **`Authenticated Users`** и отметьте флажок Full Control (Полный доступ).
3. Приведите область условий в соответствие с рис. 15.84.

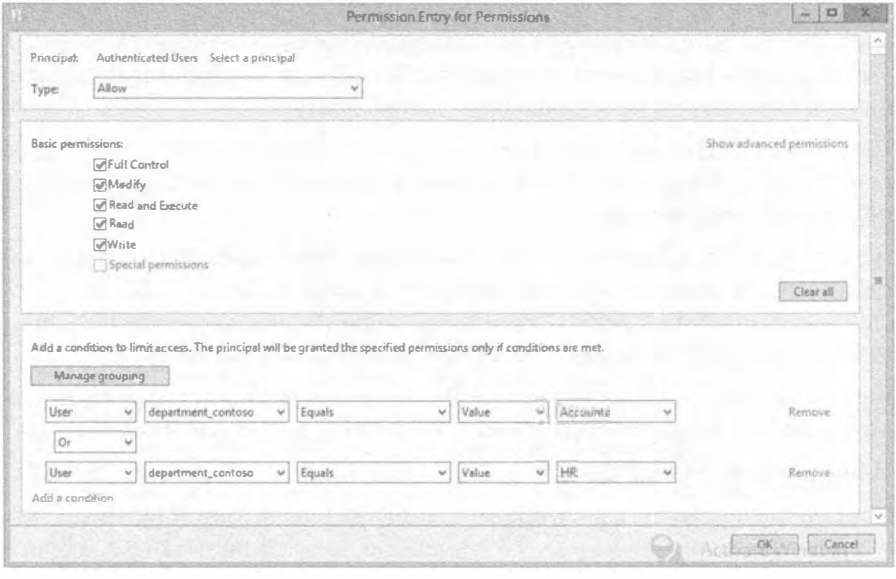


Рис. 15.84. Разрешения и условия

4. Щелкните на кнопке OK два раза, чтобы закрыть все диалоговые окна.
5. Щелкните на кнопке OK, чтобы закрыть диалоговое окно Create Central Access Rule.

Теперь необходимо создать центральную политику доступа, чтобы ее можно было впоследствии развернуть на файловых серверах.

1. В главном окне Dynamic Access Control административного центра Active Directory щелкните на элементе Central Access Policies (Центральные политики доступа).
2. Выберите в меню Tasks (Задачи) пункт New⇨Central Access Policy (Создать⇨Центральная политика доступа).
3. В открывшемся диалоговом окне Create Central Access Policy (Создание центральной политики доступа) введите **CAP-AutoClassify** в поле Name (Имя). Вам необходимо добавить правило, которое вы создали ранее, поэтому щелкните на кнопке Add (Добавить) возле области Member Central Access Rules (Центральные правила доступа, являющиеся членами). В открывшемся диалоговом окне Add Central Access Rules (Добавление центральных правил доступа) выберите правило `Securing Auto Classified Accounts Data` и щелкните на кнопке OK.
4. Щелкните на кнопке OK, чтобы завершить создание политики.
5. Откройте консоль Group Policy Management (Управление групповой политикой).
6. Найдите групповую политику `CAP-Contoso-Demo`, которая была создана ранее для развертывания центральных политик доступа на файловых серверах.
7. Щелкните на ней правой кнопкой мыши и выберите в контекстном меню пункт Edit (Редактировать).
8. Перейдите к папке Computer Configuration⇨Policies⇨Windows Settings⇨Security Settings⇨File System⇨Central Access Policy (Конфигурация компьютера⇨Политики⇨Настройки Windows⇨Настройки безопасности⇨Файловая система⇨Центральная политика доступа).
9. Щелкните правой кнопкой мыши на папке Central Access Policy и выберите в контекстном меню пункт Manage Central Access Policies (Управлять центральной политикой доступа).
10. В открывшемся диалоговом окне Central Access Policies Configuration (Конфигурация центральной политики доступа) выберите политику `CAP-AutoClassify`, щелкните на кнопке Add (Добавить) и закройте диалоговое окно Group Policy Management Editor (Редактор управления групповой политикой).
11. В системе файлового сервера откройте окно командной строки от имени учетной записи администратора и введите команду **gpupdate /force**.
12. Примените политику `CAP-AutoClassify` к папке `Accounts` из `C:\share`.
13. Войдите в систему на клиентской машине от имени учетной записи пользователя, не относящейся к отделу `HR` или `Accounts`, и попытайтесь обратиться к информации в папке `Accounts`. Можете ли вы ее видеть?

14. Если вы ее видите, попробуйте получить к ней доступ.

    Если вы ее не видите, значит, включена опция Enable access-based enumeration (Включить перечисление на основе доступа), и это скрывает файлы и папки, для которых вы не имеете разрешений.

15. Выйдите из системы и затем войдите от имени учетной записи пользователя из отдела `Accounts` или `HR`, чтобы увидеть разницу.

16. Создайте в папке `Accounts` новый файл RTF по имени `File5` и поместите внутрь него любую информацию, не защищаемую правилами классификации.

17. Теперь попробуйте получить доступ к документу `File5` с клиентской машины посредством учетной записи пользователя из отдела `Accounts` и учетной записи пользователя не из отдела `Accounts`.

    Видите, как все здорово!

Резюме

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?

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.

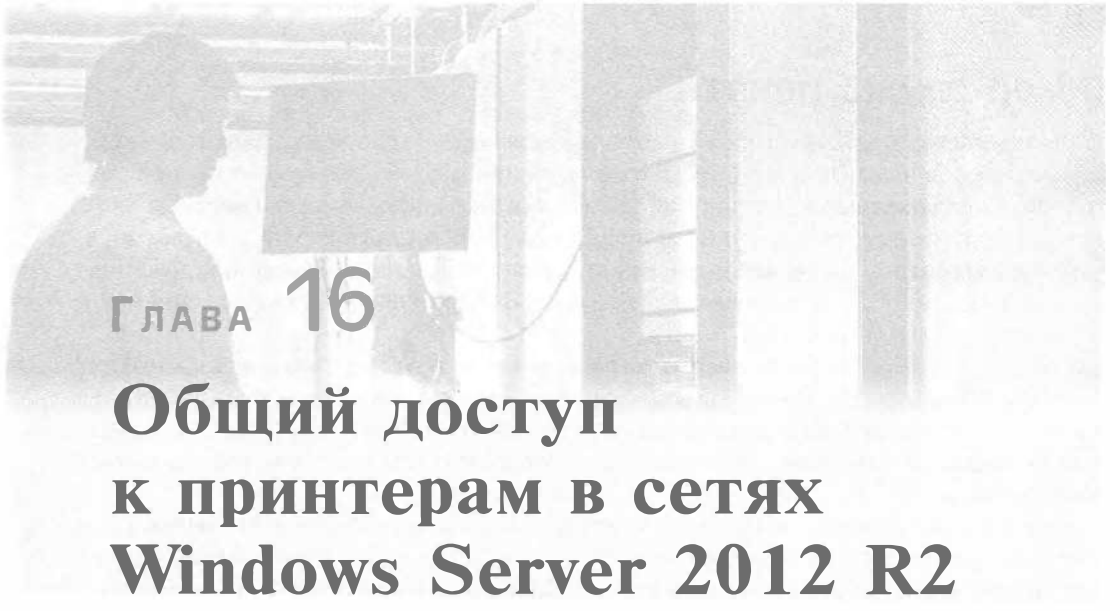
> *Контрольный вопрос.* Как обеспечить возможность доступа к данным, находящимся на ваших общих ресурсах, только сотрудникам из Ирландии? Что нужно сделать для того, чтобы можно было применять название страны в качестве маркера авторизации?

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?

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 зашишать 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?



Глава 16

Общий доступ к принтерам в сетях Windows Server 2012 R2

Если ваша компания располагает неограниченными средствами, то она может позволить себе приобрести устройство печати для каждого пользователя. Можете себе вообразить наличие такого устройства на каждом столе? Вот и мы не можем. Даже в лучшие времена успешные и прибыльные компании не были настолько расточительными.

Вместо этого компания часто определяет пропорцию между количеством устройств печати и числом пользователей, к примеру, один принтер на каждые 5, 10 или 20 сотрудников. В результате экономятся средства не только на самих устройствах печати, но также расходы на потребленную электроэнергию и обслуживание.

К тому же для большей эффективности обслуживания этих принтеров они часто устанавливаются на серверах печати. На одиночном сервере печати могут размещаться сотни принтеров.

В Windows Server 2012 R2 вы можете добавить роль Print and Document Services (Службы печати и документов), в которой предусмотрена консоль Print Management (Управление печатью). Это не только оптимизирует сервер для обслуживания заданий печати для конечных пользователей, но консоль Print Management также позволяет управлять многочисленными серверами печати из центрального местоположения.

В этой главе вы изучите следующие темы:

- добавление роли Print and Document Services;
- управление принтерами с использованием консоли Print Management;
- управление свойствами серверов печати;
- управление свойствами принтеров.

Обзор служб печати

Большинство пользователей уверено, что *принтер* — это такой сероватый ящик, находящийся в шаговой доступности от их рабочих мест, куда они помещают бумагу и получают напечатанные документы. Но все мы знаем, что в загадочном мире администрирования систем принтер представляет собой логический программный компонент, который является посредником между пользовательскими приложениями и собственно *устройством печати*. Все настройки конфигурации применяются к принтерам, а не к устройствам печати.

Пропорция между принтерами и устройствами печати не обязательно выглядит как один к одному. Вы можете иметь один принтер и одно устройство печати, два принтера для одиночного устройства печати или один принтер и несколько устройств печати. В ходе этой главы мы еще поговорим о том, *по какой причине* может понадобиться.

Когда вы отправляете документы принтеру, они становятся частью *очереди* принтера, т.е. группы документов, ожидающей печати. Документы ждут в очереди до тех пор, пока устройство печати не окажется свободным для принятия задания печати.

Большинство людей в вашей сети не будут иметь собственные устройства печати, установленные на их столах. Взамен пользователи обычно выполняют печать на принтере, доступном через сеть. Доступ к такому принтеру может осуществляться непосредственно через сеть или посредством сервера печати (чему уделено основное внимание в настоящей главе).

Взгляните на рис. 16.1, на котором иллюстрируются разные способы конфигурирования устройств печати в сети. Устройство печати 1 подключено напрямую к порту USB на компьютере Салли. Оно не считается сетевым принтером до тех пор, пока Салли не откроет к нему общий доступ. Тем не менее, даже если Салли откроет общий доступ, устройство печати будет сделано общим не сервером печати, а компьютером Салли. В таком контексте компьютер Салли действует в качестве сервера печати, даже если на ее компьютере просто функционирует Windows 7.

Устройство печати 2 напрямую подключено к серверу печати, который может открыть к нему общий доступ, так что это устройство считается сетевым принтером. Поскольку устройства печати 3 и 4 подключены непосредственно к сети, они также трактуются как сетевые принтеры.

Рис. 16.1. Устройства печати в сети

Устройства печати 3 и 4 должны иметь сетевые интерфейсные платы, которым могут быть назначены IP-адреса, чтобы обеспечить их доступность через сеть.

На рис. 16.1 не вполне ясно, обслуживаются ли устройства печати 3 и 4 сервером печати. Одно из них могло бы обслуживаться, а другое быть автономным сетевым принтером. Давайте предположим, что сервер печати сконфигурирован на обслуживание заданий для устройства печати 3. Все пользователи будут посылать свои задания серверу печати, который будет управлять очередью для устройства печати 3.

С другой стороны, представим, что сервер печати не настроен на обслуживание заданий для устройства печати 4. В таком случае пользователям понадобится конфигурировать это устройство печати индивидуально в каждой системе, и задания будут отправляться прямо устройству печати, а не серверу. При этом устройство печати 4 не пользуется многими преимуществами сервера печати, такими как автоматическая загрузка заданий печати, управление доступом к принтерам посредством разрешений или расписаний либо управление очередями, если только функциональность подобного рода не встроена в программное обеспечение устройства.

Основное внимание в этой главе сосредоточено на применении сервера Windows Server 2012 R2 в качестве сервера печати. Если устройства печати просто подключены к сети и не обслуживаются каким-нибудь принтером, они остаются сами по себе.

Процесс печати в Windows Server 2012 R2 несколько сложнее, чем он выглядит со стороны. Модель печати использует многочисленные компоненты для визуализации данных приложений при выводе графики, для помещения данных в принтер и для содействия принтеру в управлении множеством заданий печати. Некоторая изложенная далее информация о том, *как* работает печать, является довольно низкоуровневой, но она становится полезной при поиске и устранении неполадок.

Спулер печати

Компьютеры функционируют намного быстрее, чем устройства печати. Ничего удивительного. Тем не менее, несколько лет назад, когда задание отправлялось устройству печати, компьютер замедлялся до скорости этого устройства до тех пор, пока задание печати не было полностью завершено. В течение этого периода пользователь не мог делать что-то другое на компьютере.

Работа без сервера печати

Мы потратили немало времени на работу в организациях, в которых не применялись серверы печати. Вместо этого устройство печати подключалось напрямую к сети, и ему назначался IP-адрес, после чего каждый компьютер требовалось конфигурировать для использования такого устройства печати.

Один из значительных недостатков данного метода заключается в том, что у пользователей часто возникают проблемы с подключением к устройству печати и установкой корректного драйвера. Они должны знать IP-адрес для подключения к принтеру, но даже тогда может быть выбран ошибочный драйвер, давая в результате бесполезные распечатки. Пользователи обращаются в службу поддержки, и если специалисты из этой службы не знают, какой точно драйвер необходим, начинаются судорожные его поиски.

Когда применяется сервер печати, пользователям нужно просто указать путь UNC (universal naming convention — универсальное соглашение об именовании) принтера (*имяСервера**имяОбщегоРесурса*) при его добавлении. Затем сервер автоматически загрузит корректный драйвер. Например, принтер можно было бы сделать общим ресурсом по имени `Laser1` на сервере `BF1`, и для автоматической загрузки правильного драйвера для их операционных систем пользователям пришлось бы только подключиться к `\\BF1\Laser1`. Кроме того, если устройство печати перемещается в другую подсеть, вносить изменения в конфигурацию понадобится только на сервере, а не на каждом клиенте.

Компромиссом, на который приходится идти, является стоимость сервера печати и связанного с ним обслуживания. Тем не менее, поскольку на серверах можно легко совмещать несколько ролей, файловые серверы часто действуют также и в качестве серверов печати.

Можете не сомневаться, что такое положение вещей с замедлением компьютера из-за печати вызывало раздражение у многих пользователей, поэтому был разработан спулер печати. Теперь, когда пользователь отправляет задания печати, служба спулера принимает их и хранит в памяти или на жестком диске до тех пор, пока устройство печати не сможет принять эти задания. Если вы печатаете документ, то можете почти немедленно начать делать что-то еще, даже если процесс распечатывания документа занимает, скажем, 10 минут.

Когда пользователи печатают документы на принтере, обслуживаемом сервером печати, в действительности задействованы два спулера. Служба спулера на компьютере пользователя выполняет подкачку документа (обычно только в память) и затем отправляет задание серверу печати. После того, как сервер печати получает это задание, он также производит его подкачку. Так как сервер печати может работать над другими заданиями, он обычно будет хранить задания печати на жестком диске.

Стандартной папкой для подкачанных документов является `C:\Windows\System322\Spool\Printers`. Позже в главе будет показано, как это изменить.

Драйвер принтера

Драйверы принтеров — это программное обеспечение, которое позволяет операционной системе взаимодействовать с принтером и в конечном итоге отправлять задание печати в устройство печати. За последние годы драйверы принтеров были унифицированы, в результате чего работа с ними несколько упростилась. Вы будете сталкиваться с тремя основными драйверами печати:

Itanium	Тип 3 — пользовательский режим
x64	Тип 3 — пользовательский режим
x86	Тип 3 — пользовательский режим

Обратите внимание, что все драйверы обозначены как “Тип 3 — пользовательский режим”. Драйверы, существовавшие до выхода Windows 2000 Server, относились к драйверам типа 2 для режима ядра. Они взаимодействовали с ядром операционной системы и потенциально могли привести к краху системы, если что-то шло не так.

Драйверы типа 3 работают только в пользовательском режиме и изолированы от операционной системы. Itanium — это специальная 64-разрядная архитектура, применяемая в высокопроизводительных серверах, x64 обозначает 64-разрядную, а x86 — 32-разрядную архитектуру. Хорошая новость в том, что вы можете установить драйвер x86 типа 3 для пользовательского режима, и он будет работать в любой 32-разрядной операционной системе — во всяком случае, должен.

К счастью, вы можете загрузить все три драйвера печати на сервер Windows Server 2012 R2, и при подключении разных систем будет автоматически загружаться подходящий драйвер. Однако вы по-прежнему должны контролировать загрузку на сервер корректных драйверов. Другими словами, если вы поддерживаете 32-разрядных клиентов Windows XP и 64-разрядных клиентов Windows 7, понадобится обеспечить наличие драйверов x86 и x64.

С выпуском Windows Server 2012 R2 появились новые драйверы v4. Эти драйверы не являются совместимыми с операционными системами, предшествующими Windows 8 и Windows Server 2012 R2, но — барабанная дробь — можно выполнять печать в очередь v4 из сервера печати Windows Server 2012 R2, используя расширенный драйвер Point and Print Compatibility (Совместимость указания и печати).

Поскольку архитектура v4 поддерживает инфраструктуру классов драйверов для печати, пользователи могут устанавливать принтеры без необходимости в нахождении драйвера для конкретного принтера. Это решает проблемы безопасности и совместимости, обнаруженные в драйверах v3.

Поиск драйверов для принтеров

Поиск подходящих драйверов печати (особенно для новых операционных систем) часто является очень сложной задачей. В идеальном мире с выходом новой операционной системы каждая компания автоматически получала бы корректные драйверы, поэтому оборудование продолжало бы функционировать. Однако многие обстоятельства направлены против такого сценария. Компания может создать драйвер печати, который работает с предвыпускной версией ОС лишь для того, чтобы увидеть, что внесенные в последнюю минуту изменения в ОС привели в результате к утере работоспособности своего драйвера.

Разумеется, когда компания обнаруживает, что ее драйвер больше не функционирует, она корректирует и перепроектирует его, после чего выкладывает новый драйвер на своем веб-сайте, как только это становится возможным. Тем не менее, драйвер нуждается в тестировании и проверке корректности его работы, прежде чем он будет включен в состав операционной системы или доступен через службу обновления Windows Update.

Тем временем пользователи, которые провели модернизацию до нового выпуска ОС, обнаруживают, что они больше не могут распечатывать. Они пробуют получить обновления посредством службы Windows Update (которая включает только драйверы, прошедшие через длительный процесс обкатки и тестирования), но безуспешно. Знающим пользователям (и администраторы) известно, что в такой ситуации лучшим источником является веб-сайт производителя устройства печати. Они заходят на веб-сайт производителя, но он может как содержать, так и не содержать корректный драйвер, и часто пользователю (или администратору) приходится проходить через затяжной процесс проб и ошибок, пока он не найдет что-то работающее или откажется от дальнейших попыток. Это было весьма очевидным, когда вышла версия Windows Vista, вызвавшая массу нареканий в этом отношении со стороны пользователей.

Спецификация XPS

Спецификация XPS (XML Paper Specification — бумажная спецификация XML) основана на языке XML (Extensible Markup Language — расширяемый язык разметки) — отраслевом стандарте, который неуклонно проникал во многие текущие технологии, включая базы данных, веб-службы и теперь вот печать. Язык HTML (используемый при построении веб-страниц) основан на XML. Данные XML содержатся в простых текстовых документах, которые можно читать с помощью элементарных приложений наподобие Notepad (Блокнот) и применять для хранения значительных объемов данных и метаданных.

XPS в Интернете

В Microsoft взяли себе на вооружение XPS и опубликовали много материалов об использовании этой спецификации внутри своих продуктов. Домашняя страница XPS доступна по адресу `www.microsoft.com/whdc/xps/default.mspx`. Кроме того, движущей силой стандартизации XPS на множестве платформ выступает ассоциация ECMA International. С деталями заседаний и доступными документами можно ознакомиться по адресу `www.ecma-international.org/memento/TC46-M.htm`.

Метаданные применяются для описания данных. Например, метаданные внутри печатного документа могут использоваться для идентификации всех данных на страницах 1, 2 и т.д. Они также могли бы применяться для описания требуемого способа отображения данных, такого как стиль или размер шрифта.

В Microsoft построили формат документа XPS на основе спецификаций Open XML Markup Compatibility (Открытая совместимость разметки XML) и OPC (Open Packaging Conventions — Открытые соглашения об упаковке). Их представление заключается в достижении намного большей эффективности, совместимости с большим числом приложений и более высокого качества документов, когда используются драйверы принтеров XPSDrv.

Концептуально спецификация XPS похожа на формат PDF (Portable Document Format — формат переносимых документов), созданный компанией Adobe Systems для обмена документами. Бьемся об заклад, что вы уже открывали хотя бы несколько документов PDF во время своих путешествий, учитывая то, насколько широко они применяются в наши дни. Документ PDF удобен тем, что создающее его лицо может управлять внешним видом этого документа при печати. Сравните это с обычным документом Word, который при печати на разных принтерах может выглядеть по-разному.

Документы XPS можно создавать в Microsoft Office 2012, и к этим документам может быть открыт общий доступ в точности как к файлам PDF. Чтобы сохранить документ в формате XPS, выберите пункт меню Save As⇨XPS Document (Сохранить как⇨Документ XPS). Пользователи, располагающие средством просмотра XPS, могут просматривать эти документы, точно так же, как пользователи могут просматривать файлы PDF, имея подходящую версию программы Adobe Reader. В дополнение к сохранению файлов в формате XPS, документы могут быть транслированы в формат XPS, так что они могут использоваться драйверами принтеров XPSDrv.

XPSDrv: новая модель драйверов принтеров

Драйверы принтеров, созданные с применением в своих интересах нового формата XPS, называют драйверами принтеров XPSDrv. Эти драйверы обеспечивают более значительную гибкость, чем старые функции обработки графики GDI (Graphics Device Interface — интерфейс графических устройств), которые использовались до драйверов принтеров XPSDrv.

В драйверах принтеров XPSDrv применяется формат документов XPS для получения на принтерах улучшенного вывода WYSIWYG (what-you-see-is-what-you-get — принцип полного соответствия). Может использоваться больший диапазон цветов, и становится возможным другой графический вывод, такой как прозрачные области и градиенты.

Поскольку в драйверах принтеров XPSDrv применяется формат XPS, а он приводит к получению подкачанных файлов меньшего объема, чем формат GDI, сокращается общий размер подкачанных печатных файлов.

Интерфейс GDI

Интерфейс GDI является частью операционной системы, которая начинает процесс генерации визуального вывода, предназначенного как для экрана, так и для принтера. Исторически сложилось так, что GDI использовался для формирования вывода WYSIWYG, ориентированного на экран и печатную страницу. Чтобы построить экранный вывод, интерфейс GDI обращается к видеодрайверу, а для генерации печатного вывода взаимодействует с драйвером принтера, предоставляя ему необходимую информацию об устройстве печати и тип применяемых данных.

Хотя драйверы принтеров, основанные на GDI, заменяются драйверами принтеров XPSDrv, какое-то время вы еще можете встречать старые драйверы на основе GDI. А теперь, когда вы ознакомились с обзором служб печати, давайте перейдем к рассмотрению роли Print and Document Services (Службы печати и документов).

Установка роли Print and Document Services

Роль Print and Document Services добавляется к серверу, когда вы хотите, чтобы он стал сервером печати. При добавлении этой роли у вас появится возможность добавить несколько разных служб в зависимости от того, что именно должен делать сервер печати.

- **Print Server (Сервер печати).** Служба Print Server включает консоль Print Management (Управление печатью), которую вы будете использовать для выполнения большинства задач управления на своем сервере печати. Посредством этой оснастки можно управлять множеством принтеров и даже множеством северов печати. Это основная служба сервера печати и именно ей уделяется главное внимание в настоящей главе.
- **LPD Service (Служба LPD).** Если в вашей организации имеются компьютеры на базе Unix, которым требуется печатать на устройствах печати, обслуживаемых вашим сервером печати, можете добавить службу демона линейного принтера (Line Printer Daemon — LPD). Служба LPD позволит любым клиентам, пользующимся службой удаленного доступа к линейному принтеру (Line Printer Remote — LPR), печатать на общих принтерах вашего сервера печати.

- **Internet Printing (Печать через Интернет).** Протокол печати через Интернет (Internet Printing Protocol — IPP) позволяет клиентам, на которых установлен клиент Internet Printing, применять веб-браузер для подключения и выполнения печати на общих принтерах вашего сервера. Добавление этой службы также приводит к созданию веб-сайта, где пользователи могут управлять своими заданиями печати на сервере вместо использования консоли печати.
- **Distributed Scan Server (Распределенный сервер сканирования).** Служба Distributed Scan Server позволяет серверу получать отсканированные документы из сканеров в сети и направлять их в корректные местоположения. При добавлении этой службы также добавляется оснастка Scan Management (Управление сканированием).

Добавление роли Print and Document Services

Роль Print and Document Services довольно просто установить с применением диспетчера серверов. Единственный выбор, который вам понадобится сделать — какие конкретно службы добавить, а это зависит от того, что будут делать клиенты. Чтобы добавить роль Print and Document Services к серверу Windows Server 2012 R2, выполните следующие шаги.

1. Запустите диспетчер серверов через панель задач.
2. Щелкните на ссылке Add roles and features (Добавить роли и компоненты).
3. Просмотрите информацию на экране Before you begin (Прежде чем начать) и щелкните на кнопке Next (Далее).
4. 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.
5. Выберите сервер из пула серверов и щелкните на кнопке Next.
6. На экране Select Server Roles (Выбор серверных ролей) выберите роль Print and Document Services и щелкните на кнопке Next.
7. Откроется диалоговое окно с запросом на добавление компонента Role Administration Tools (Инструменты администрирования роли); щелкните на кнопке Add Features (Добавить компоненты), чтобы продолжить.
8. Можете пропустить остальные компоненты, щелкнув на кнопке Next.

   Вы должны попасть на экран со сводкой по роли Print and Document Services, показанный на рис. 16.2. Щелкните на кнопке Next.
9. На экране Role Services (Службы роли) службы Print Server (Сервер печати) будут выбраны по умолчанию; щелкните на кнопке Next, чтобы продолжить.
10. На экране Confirmation (Подтверждение) щелкните на кнопке Install (Установить).
11. Если все было сделано правильно, вы должны увидеть экран с индикатором хода работ по установке (рис. 16.3).
12. Когда установка завершится, щелкните на кнопке Close (Закрыть).

После добавления роли Print and Document Services вы можете получать доступ к службе Print Server в диспетчере серверов. Служба Print Server является централизованным источником для управления всеми задачами печати.

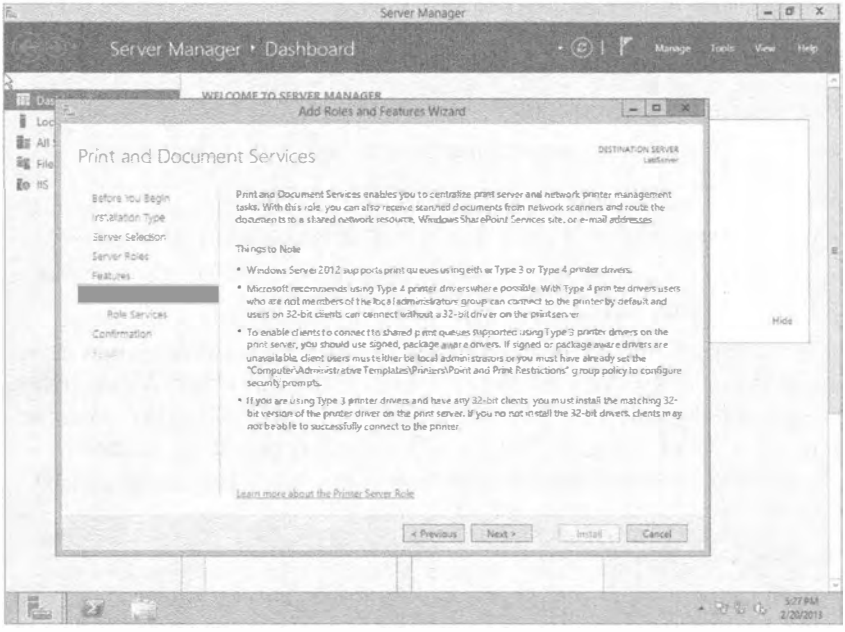


Рис. 16.2. Сводка по роли Print and Document Services

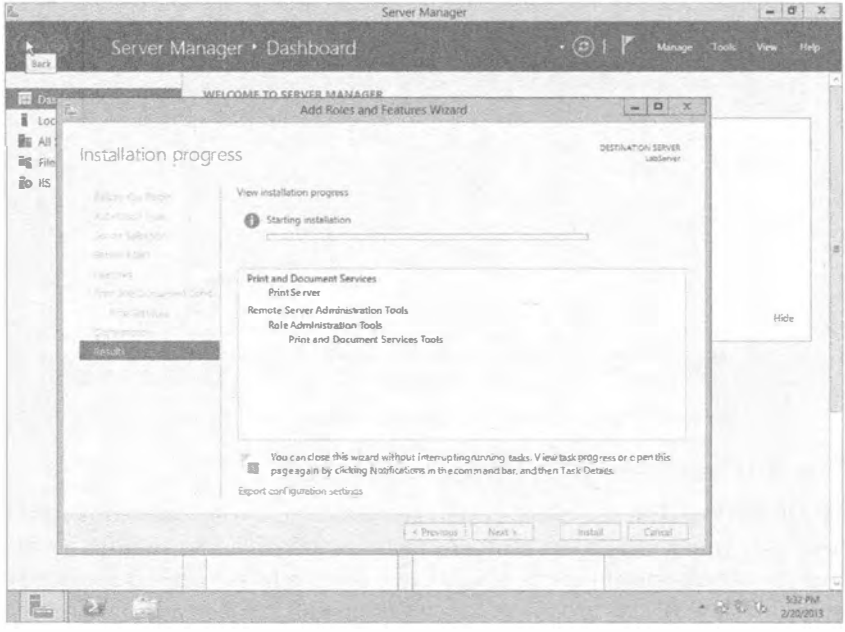


Рис. 16.3. Добавление службы Print Server

Работа в консоли управления печатью

Консоль управления печатью (Print Management console — PMC) является великолепным дополнением к интерфейсу операционной системы, в конечном счете, позволяющим выполнять *все*, что связано с печатью, в единственной консоли. Она дает возможность делать почти все, что угодно, с принтерами и другими серверами печати, включая следующие действия:

- добавление новых драйверов;
- просмотр принтеров с использованием специальных фильтров;
- управление настройками и драйверами принтеров;
- управление состоянием принтеров и настойка оповещений;
- подключение к удаленным серверам печати, так что все это можно выполнять для целого предприятия.

Добавив к серверу роль Print and Document Services, вы можете запускать консоль PMC, нажимая клавишу <Windows> и щелкая на кнопке стиля Metro под названием Print Management (Управление печатью). Консоль PMC выглядит подобно показанной на рис. 16.4. Открыть консоль PMC возможно также из диспетчера серверов, выбрав пункт меню Tools⇨Print Management (Сервис⇨Управление печатью).

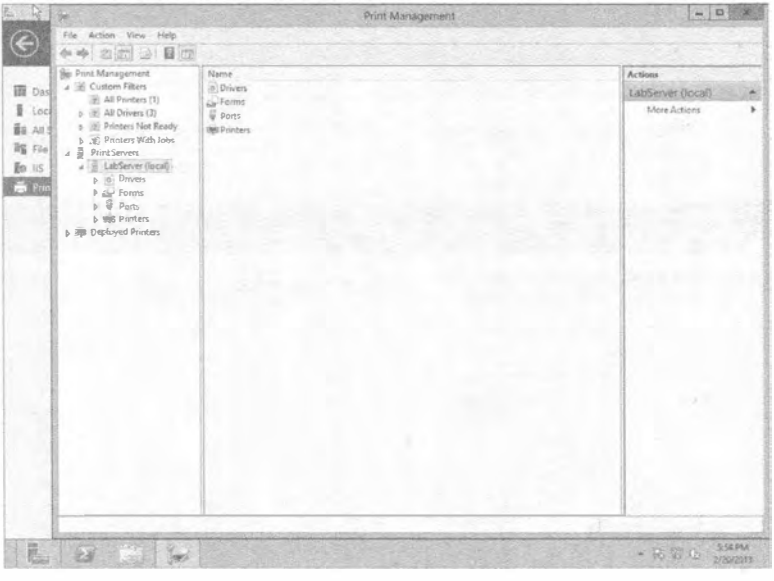


Рис. 16.4. Просмотр консоли управления печатью

Консоль PMC разделена на три главных области.

- **Custom Filters (Специальные фильтры).** Фильтры позволяют просматривать все принтеры, управляемые из этой консоли, не обращая внимания на то, к каким серверам печати они подключены. Если сервер печати обслуживает всего пять устройств печати, то это не составит большой проблемы. Тем не менее, при наличии сотен подключенных устройств печати возможность поиска среди

них с применением специальных фильтров намного упростит вашу работу. Как вы увидите далее в главе, инструмент поступает с несколькими стандартными фильтрами, но также можно создавать и собственные фильтры.

- **Print Servers (Серверы печати).** На рис. 16.4 добавлен один сервер печати (`LabServer`). Однако если в организации имеется много серверов печати, ими всеми можно управлять через единственную консоль PMC. Каждый сервер печати может располагать собственными драйверами, формами, портами и принтерами.
- **Deployed Printers (Развернутые принтеры).** Здесь перечислены принтеры, которые были развернуты с использованием групповой политики. Развертывание принтеров с помощью групповой политики рассматривается далее в этой главе.

Кроме того, внутри каждого сервера печати есть четыре основных узла. Эти узлы применяются для управления различными устройствами печати и принтерами, обслуживаемыми конкретным сервером печати.

- **Drivers (Драйверы).** Здесь можно добавлять драйверы, необходимые для принтеров. Драйверы бывают трех типов: Itanium для высокопроизводительных серверов, x64 для 64-разрядных систем и x86 для 32-разрядных систем.
- **Forms (Формы).** Формы на сервере отражают разнообразные печатные макеты, которые могут поддерживать установленные принтеры. Они определяют размер бумаги и поля печатной области. Большую часть времени большинство людей пользуются бумагой размера "письмо" (216×279 мм), и форма `Letter` (Письмо) определяет такой размер. Однако на выбор существует много других форм, к тому же можно создавать и собственную форму. Формы отображаются на основе серверов, а не принтеров.
- **Ports (Порты).** Порты служат для подключения к устройствам печати. Унаследованными являются последовательные порты (COM1–COM4), параллельные порты (LPT1–LPT3) и FILE (файл). Если вы подключите принтер USB, автоматически добавится порт USB. Новым портом стал XPSPort и он применяется для создания документов в формате Microsoft XPS. Можно также создавать стандартные порты TCP/IP, чтобы подключаться к любому сетевому принтеру, используя его IP-адрес.
- **Printers (Принтеры).** Когда вы добавляете принтер, он появляется в этой области. Вспомните, что принтер — это программный интерфейс, которым вы можете манипулировать на сервере печати, и он будет отправлять задания печати на устройство печати. В зависимости от существующих потребностей, вы можете иметь множество принтеров для любого устройства печати.

Добавление новых принтеров

Для добавления новых принтеров используется консоль PMC, и одна из хороших новостей состоит в том, что вы можете применять ее для автоматического обнаружения принтеров в той же подсети, где находится сервер печати. Щелкните правой кнопкой мыши на узле Printers (Принтеры) и выберите в контекстном меню пункт Add Printer (Добавить принтер); откроется окно мастера установки сетевого принтера (Network Printer Installation Wizard), представленное на рис. 16.5.

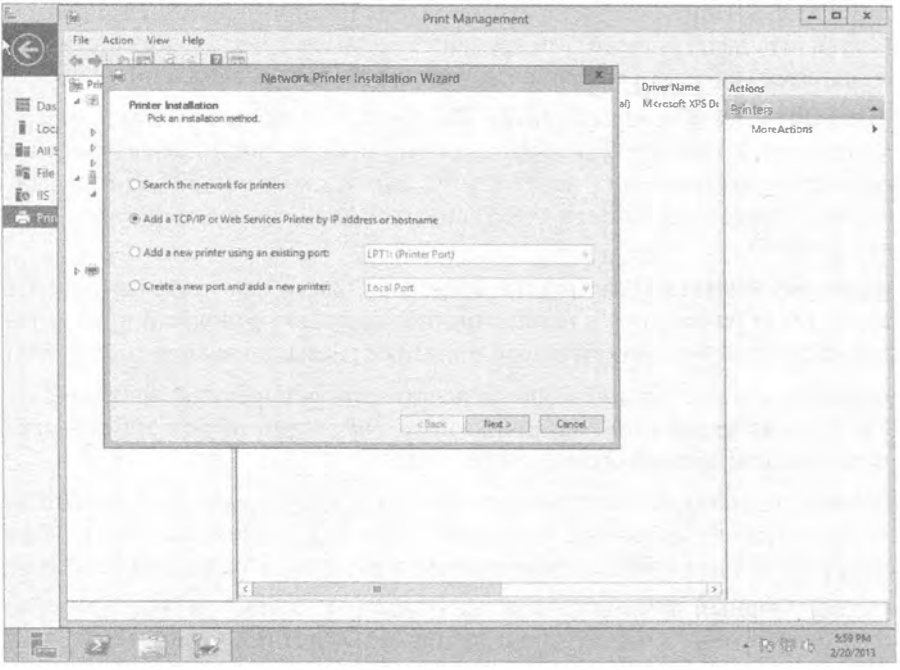


Рис. 16.5. Добавление нового сетевого принтера посредством мастера Network Printer Installation Wizard

В нем предлагаются четыре переключателя.

- **Search the Network for Printers (Искать принтеры в сети).** Данный метод позволяет консоли PMC обнаруживать принтеры автоматически. Он будет работать только с сетевыми принтерами в локальной подсети, но если дело обстоит именно так, то экономятся усилия с вашей стороны.
- **Add a TCP/IP or Web Services Printer by IP Address or Hostname (Добавить принтер TCP/IP или веб-служб по IP-адресу либо имени хоста).** Если принтер находится в отдельной подсети или сконфигурирован как принтер веб-служб (доступный через веб-сервер), используйте этот переключатель, чтобы вручную добавить IP-адрес либо имя хоста этого принтера. В случае указания имени хоста вы должны удостовериться в том, что оно распознается системой DNS или другим методом преобразования имен.
- **Add a New Printer Using an Existing Port (Добавить новый принтер, используя существующий порт).** Если порт уже существует, с помощью этого метода можно добавить принтер для имеющегося порта. Единственный принтер может иметь один порт, сконфигурированный для каждого устройства печати. Когда включена организация пула для принтера (эта процедура объясняется позже в главе), вы можете иметь несколько портов, сконфигурированных для одного принтера; каждый порт будет подключен к устройству печати. Также вы можете добавлять дополнительные принтеры для какого-то устройства печати, чтобы появилась возможность манипулирования разными свойствами, такими как разрешения или расписания принтера, что будет показано далее в главе.

- **Create a New Port and Add a New Printer (Создать новый порт и добавить новый принтер).** Данный метод позволяет создавать новые порты и добавлять к ним принтеры. Мастер не предоставляет столько вариантов, и вы можете достичь желаемого с применением других методов, поэтому вы можете никогда и не воспользоваться этим переключателем.

Принтеры, подключенные к порту USB сервера, не нуждаются в выполнении дополнительных действий. Просто подключите принтер к порту USB, и он будет автоматически распознан, а драйвер для него загружен. По умолчанию принтер не будет общим, но вы можете открыть диалоговое окно его свойств (рассматривается позже в этой главе) и открыть общий доступ на вкладке Sharing (Общий доступ).

Удаление принтера

Иногда возникает необходимость удалить принтер из сервера печати. Большую часть времени этот процесс исключительно прост: вы раскрываете узел Printers (Принтеры) в консоли PMC, щелкаете правой кнопкой мыши на принтере, который решили отправить в пресловутую большую сеть на небесах, и выбираете в контекстном меню пункт Delete (Удалить). Принтер должен немедленно исчезнуть.

Если принтер, который вы удалили, *не* исчез немедленно, вы можете получить ошибку. Удостоверьтесь в том, что он не находится в процессе печати документа. Даже если принтер никогда не работал (например, вы пытались настроить его и указали неправильный порт), он может по-прежнему ожидать заданий печати. (В действительности, это *особенно* реально, если принтер никогда не работал, но вы настаивали на его настройке, став причиной ошибок и будущего скорого провала.)

Проверьте очередь печати принтера, который пытаетесь удалить. Если в ней содержатся ожидающие задания печати, выберите пункт меню Printer⇨Cancel All Documents (Принтер⇨Отменить все документы) и после этого попробуйте удалить принтер. Перезагрузка сервера печати не очистит список находящихся в очереди задач — их придется отменить вручную.

Автоматическое обнаружение сетевых принтеров

Метод поиска принтера, инициируемый выбором переключателя Search the Network for Printers (Искать принтеры в сети), довольно хорош, но слегка обманчив. Он будет искать в локальной подсети, где расположен принтер, но если сеть содержит несколько подсетей, вся она просматриваться не будет. Другими словами, данный метод не умеет искать любые принтеры, которые доступны только через маршрутизатор.

Если в локальной подсети имеется сетевой принтер, для его установки вы можете выполнить перечисленные ниже шаги.

1. Откройте консоль Print Management (Управление печатью) и выберите свой сервер печати.
2. Щелкните правой кнопкой мыши на узле Printers (Принтеры) и выберите в контекстном меню пункт Add Printers (Добавить принтеры).
3. Выберите переключатель Search the Network for Printers (Искать принтеры в сети) и щелкните на кнопке Next (Далее).

   Это приведет к началу широковещательного поиска в подсети. Если в подсети имеются принтеры, вы их увидите (рис. 16.6).

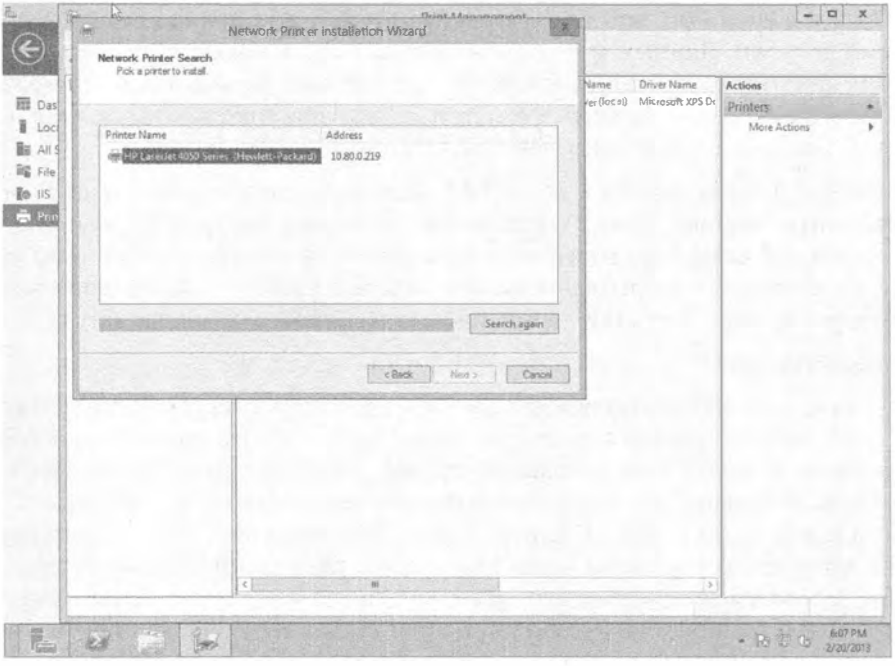


Рис. 16.6. Поиск принтеров в сети (и обнаружение одного)

Сеть должна быть сконфигурирована как частная

Если в центре управления сетями и общим доступом (Network and Sharing Center) ваша сеть настроена как открытая, вы не сможете автоматически обнаруживать сетевые принтеры. Вам придется изменить конфигурацию на частную сеть, указывая на то, что это домашняя или рабочая сеть.

4. После нахождения принтера выберите его и щелкните на кнопке Next.

   Хотя здесь это не видно, но автоматически создается стандартный порт TCP/IP с IP-адресом принтера. Вы не обязаны создавать порт как отдельный шаг.

5. Операционная система Windows попытается отыскать драйвер для принтера. Если ей это удастся, драйвер принтера будет выбран на экране Printer Driver (Драйвер принтера). Если драйвер не обнаружен, понадобится установить новый драйвер, выбрав переключатель Install a new driver (Установить новый драйвер) и щелкнув на кнопке Next.

6. Когда драйвер не был найден автоматически, доступны три варианта для поиска драйвера. Все они определены на экране, показанном на рис. 16.7.

   а. Выберите на экране производителя и модель принтера. Тем не менее, учитывая, что самой операционной системе Windows не удалось найти драйвер, вряд ли этот выбор окажется успешным.

   б. Если сервер имеет доступ в Интернет, щелкните на кнопке Windows Update (Обновление Windows), чтобы поискать драйвер там.

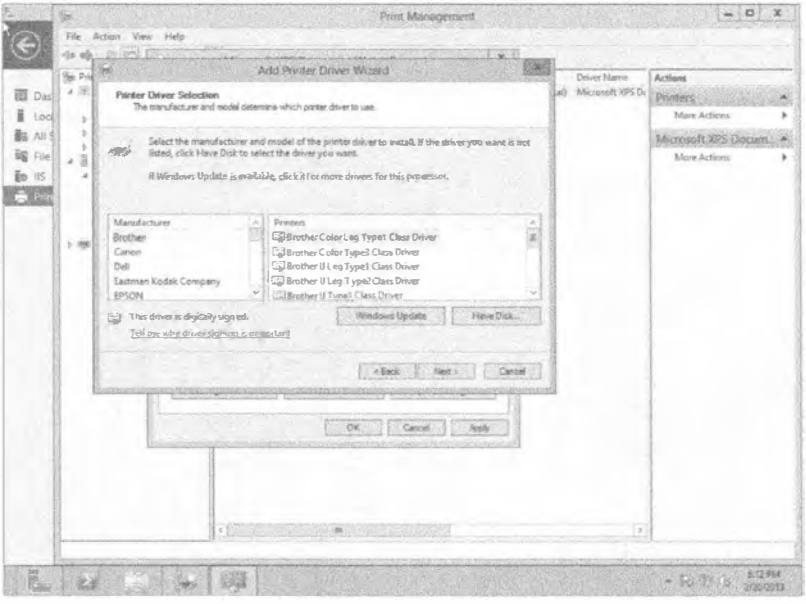


Рис. 16.7. Добавление драйвера принтера вручную

в. Щелкните на кнопке Have Disk (Имеется диск). Поскольку 64-разрядные драйверы пока еще не настолько широко распространены, может потребоваться зайти на веб-сайт производителя, загрузить 64-разрядную версию драйвера и распаковать ее в своей системе. После щелчка на кнопке Have Disk вы можете перейти в папку, где были распакованы файлы, выбрать нужный драйвер и щелкнуть на кнопке OK.

г. После выбора драйвера щелкните на кнопке Next.

7. После загрузки драйвера назначьте принтеру имя и откройте к нему общий доступ.

   К принтеру должен быть открыт общий доступ, чтобы пользователи могли подключаться к нему и отправлять свои задания печати. На рис. 16.8 показан экран Printer Name and Sharing Settings (Имя принтера и настройки общего доступа). Выбирайте такое имя, которое будет легко опознаваться персоналом, использующим принтер.

8. На экране Printer Found (Принтер найден) будут отображены выбранные детали. Щелкните на кнопке Next.

   Перед появлением завершающего экрана мастера система попытается установить драйвер и принтер. Если обнаружится несовместимость между драйвером и принтером, здесь отобразится сообщение об ошибке. Если все в порядке, вы увидите сообщение об успешном добавлении принтера (рис. 16.9).

9. Отметьте флажок Print test page (Печатать тестовую страницу) и щелкните на кнопке Finish (Готово).

   Печать тестовой страницы обеспечит окончательную проверку того, что все работает нормально.

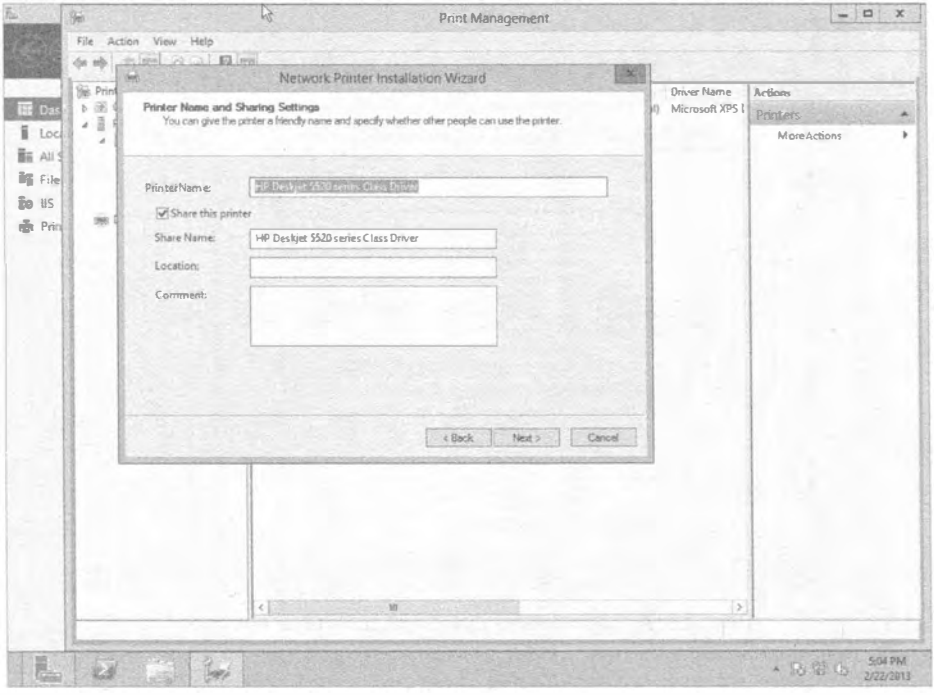


Рис. 16.8. Назначение имени и открытие общего доступа к принтеру

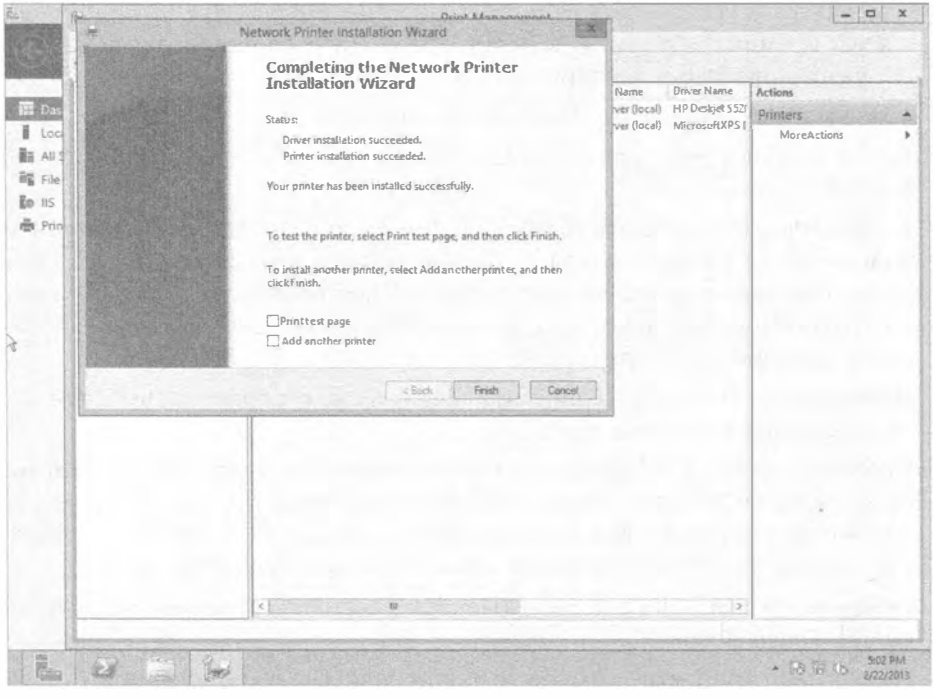


Рис. 16.9. Принтер успешно добавлен

Использовать (или не использовать) местоположения принтера

Хотя можно ввести "местоположения принтера" в мастере добавления принтера, чтобы позволить пользователям искать принтер по определенному признаку, средство Printer Locations (Местоположения принтера) также является довольно сложным в настройке, из-за чего оно обычно не применяется.

Когда средство Printer Locations полностью развернуто, оно позволяет пользователям искать принтеры, возвращая в результате принтер, который расположен ближе других. Например, если пользователь ищет принтер с двухсторонней печатью, а в организации имеется 25 таких принтеров, то будут предложены только те из них, которые находятся ближе всего к рабочему месту пользователя.

Формулировка "ближе всего к рабочему месту пользователя" в данном контексте означает нахождение в той же самой подсети.

Это требует организации и внедрения подсетей для физически близких устройств. Например, если организация располагает несколькими зданиями, эти здания имеют множество этажей, а этажи построены с рядом крыльев, то каждое крыло каждого этажа в каждом здании будет нуждаться в отдельной подсети. Если одна подсеть охватывает все этажи восточного крыла здания, средство Printer Locations не будет корректно работать, поскольку пользователь из первого этажа мог быть направлен к принтеру, находящемуся на третьем этаже, что многие сочли бы не самым "ближайшим местоположением".

В поле Location (Местоположения) экрана, показанного на рис. 16.8, должна быть указана точная информация. Во-первых, она должна вводиться с использованием служб и сайтов Active Directory (Active Directory Sites and Services) для добавления местоположения каждой подсети. Во-вторых, она должна быть введена как свойство для каждого принтера. Здесь учитывается также и правильность написания. Если местоположение подсети описано как "Здание 1, этаж 3, западное крыло", но для местоположения принтера указано "Здание1, этаж 3, западное крыло" (без пробела между "Здание" и "1"), то местоположения не будут совпадать и принтер не может быть найден.

Несмотря на то что идея, положенная в основу средства Printer Locations, выглядит неплохо, мы просто не видим, как ею эффективно воспользоваться. Тем не менее, по-прежнему можно ввести местоположение, и если пользователи знают, какое местоположение искать, они сумеют его найти.

Ручная установка новых принтеров

Если необходимо установить принтер, который не находится в вашей подсети, воспользуйтесь следующей процедурой.

1. Щелкните правой кнопкой мыши на узле Printers (Принтеры) в консоли PMC и выберите в контекстном меню пункт Add Printers (Добавить принтеры).
2. Выберите переключатель Add a TCP/IP or Web Services Printer by IP Address or Hostname (Добавить принтер TCP/IP или веб-служб по IP-адресу либо имени хоста) и щелкните на кнопке Next (Далее).
3. В поле со списком Type of device (Тип устройства) выберите TCP/IP Device (Устройство TCP/IP).
4. Введите IP-адрес принтера или, если система DNS сконфигурирована для преобразования имени принтера, можете ввести соответствующее имя принтера.

5. Удостоверьтесь, что флажок Auto detect the printer driver to use (Автоматически обнаруживать драйвер принтера для использования) отмечен (рис. 16.10). Щелкните на кнопке Next.

   После этого мастер будет действовать точно так же, как в случае процесса автоматического обнаружения. Сначала он попытается обнаружить порт TCP/IP. Затем он попробует найти драйвер. Если драйвер не был найден, выполните следующие шаги.

   а. Выберите переключатель Install a new driver (Установить новый драйвер).

   б. Щелкните на кнопке Next, перейдите к подходящему драйверу и щелкните на кнопке OK.

   в. Щелкните на кнопке Next.

6. После установки драйвера назначьте принтеру имя и откройте к нему общий доступ, указав имя общего ресурса.

7. Щелкните на кнопке Next, просмотрите все детали и снова щелкните на кнопке Next, чтобы установить драйвер и принтер.

Обратите внимание, что единственным отличием здесь был ручной ввод IP-адреса вместо того, чтобы позволить мастеру найти его в сети. В качестве напоминания: вы должны добавлять принтер вручную, если он находится в другой подсети.

Конфигурирование и просмотр настроек и ресурсов

Установка принтера является первым шагом, но одна лишь установка совершенно не гарантирует, что принтер будет иметь правильные драйверы или корректные формы, доступные пользователям.

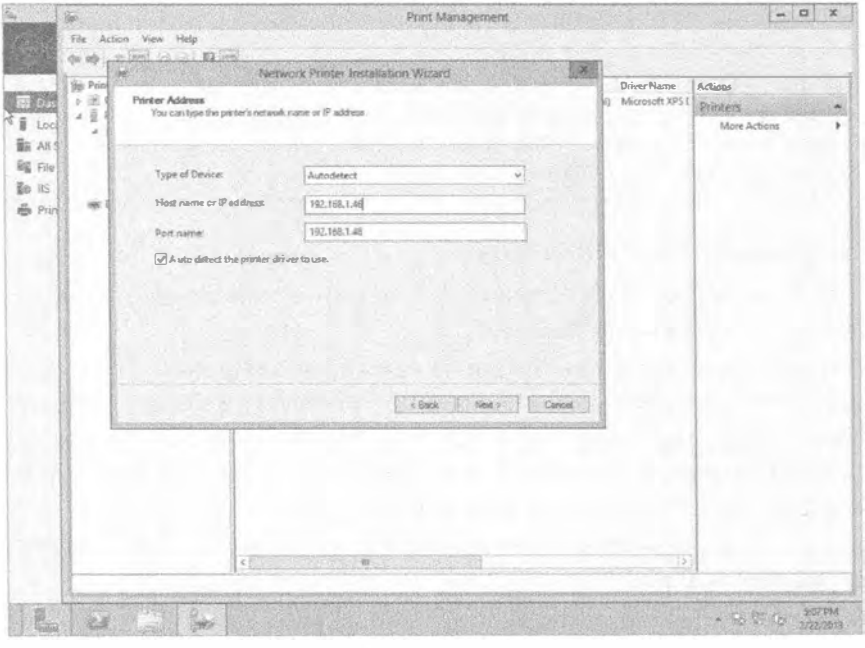


Рис. 16.10. Добавление IP-адреса принтера

В этом разделе мы покажем, как консоль PMC организует такие настройки, чтобы помочь вам просматривать и конфигурировать параметры сервера печати для драйверов, портов и доступных форм.

Управление драйверами принтера

Если вы хотите добавить принтер в систему Windows Server 2012 R2, на который пользователи смогут печатать, то для него понадобятся 64-разрядные драйверы, совместимые с сервером печати. Для использования общих принтеров конечными пользователями нужны также драйверы для их систем.

Например, если вы поддерживаете клиентов с 32-разрядными операционными системами, вам необходимо добавить к серверу печати подходящие для них драйверы. Вы можете просмотреть список всех драйверов, которые в текущий момент установлены на сервере, выбрав узел Drivers (Драйверы) в консоли PMC (рис. 16.11).

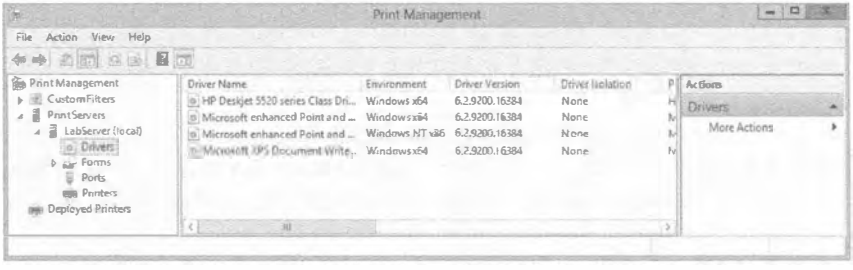


Рис. 16.11. Просмотр установленных драйверов

Обратите внимание, что драйверы принтеров основаны на архитектуре x64. Они непригодны для клиентов x86 (или 32-разрядных).

Изменение представления драйверов для принтеров

Представление драйверов для принтеров отображает много сведений о драйверах, но вы можете быть заинтересованы в большем объеме информации. При желании это представление можно изменить, чтобы вывести дополнительные сведения или убрать ненужную информацию. В качестве примера добавим URL веб-сайта изготовителя, чтобы идентифицировать источник для получения обновлений.

На рис. 16.12 показано диалоговое окно Add/Remove Columns (Добавление или удаление столбцов) для представления драйверов.

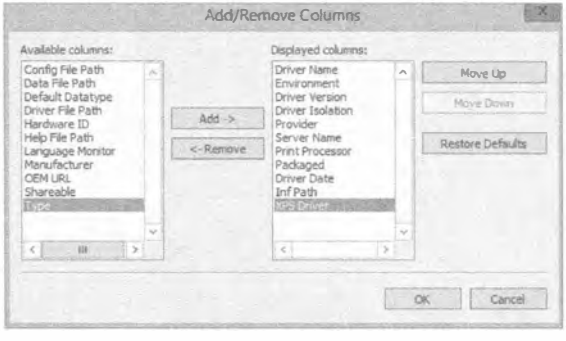


Рис. 16.12. Изменение представления с установленными драйверами

Чтобы открыть его, при выделенном узле Drivers (Драйверы) выберите пункт меню View⇨Add/Remove Columns (Вид⇨Добавить или удалить столбцы). Здесь можно выбрать любые элементы в списке Available columns (Доступные столбцы) и добавить их в список Displayed columns (Отображаемые столбцы), щелкнув на кнопке Add (Добавить). Аналогично, отображаемые столбцы можно удалить, выбрав их в списке Displayed columns и щелкнув на кнопке Remove (Удалить). На рис. 16.12 мы добавили к представлению столбец с URL веб-сайта для получения драйвера.

Установка новых драйверов для принтеров

Дополнительные драйверы для принтеров можно установить с применением узла Drivers или путем добавления драйвера к конкретному принтеру. Чтобы добавить драйвер к принтеру, используйте следующие шаги.

1. Откройте консоль Print Management (Управление печатью) и выберите свой сервер печати.
2. Перейдите в контейнер Printers (Принтеры). Щелкните правой кнопкой мыши на имени нужного принтера и выберите в контекстном меню пункт Properties (Свойства).
3. В открывшемся диалоговом окне свойств принтера перейдите на вкладку Sharing (Общий доступ) и щелкните на кнопке Additional Drivers (Дополнительные драйверы). Откроется диалоговое окно Additional Drivers (Дополнительные драйверы), приведенное на рис. 16.13.
4. Отметьте флажок в строке x86 Type 3 — User Mode (x86 Тип 3 — пользовательский режим) и щелкните на кнопке OK.
   Сервер начнет поиск совместимого драйвера во внутреннем хранилище драйверов. Если такой драйвер обнаруживается, он добавится. Если же нет, вам будет предложено перейти в местоположение драйвера.

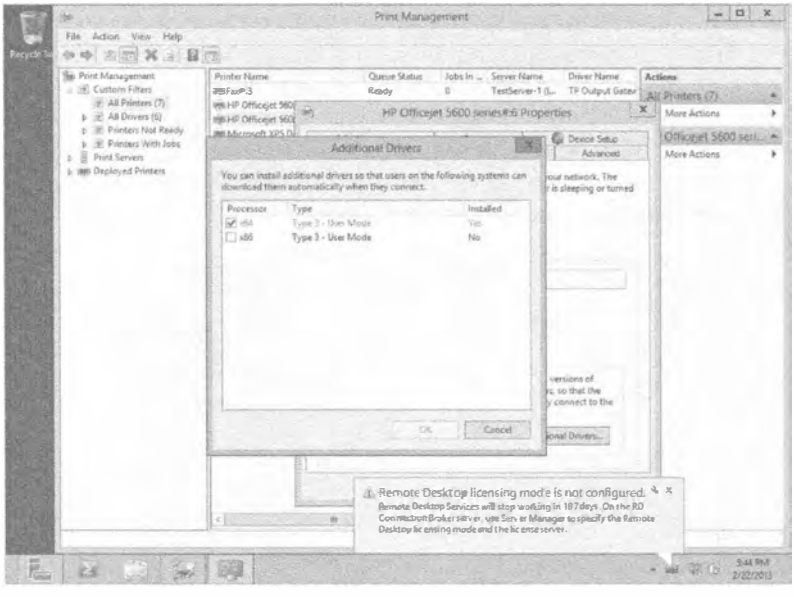


Рис. 16.13. Просмотр дополнительных драйверов, установленных для принтера

Когда драйвер в хранилище отсутствует, лучше всего его искать на веб-сайте производителя принтера, откуда его можно загрузить и распаковать в определенную папку.

5. Перейдите в соответствующее местоположение и щелкните на кнопке OK.

> **Хранилище драйверов**
>
> Все драйверы устройств (включая драйверы для принтеров в Windows Server 2012 R2) устанавливаются в защищенную папку, которая называется хранилищем драйверов. Вы можете думать о нем как об обычном магазине или торговом центре, где можно покупать товары (разумеется, кроме того факта, что операционная система не требует за это денег). Когда требуется драйвер, производится поиск в хранилище. Если драйвер обнаруживается в хранилище, он автоматически устанавливается. Если же его в хранилище нет, Windows может выполнить поиск в дополнительных местах (таких как Windows Update) и запросить у пользователя путь к файлу драйвера. В хранилище драйверов помещаются только подписанные драйверы, что делает его более защищенным.

6. Щелкните на кнопке Additional Drivers, чтобы удостовериться в добавлении драйвера. Пометка No (Нет) в столбце Installed (Установлен) изменится на Yes (Да).

Просмотр и редактирование настроек портов

Все порты сервера печати находятся в контейнере Ports (Порты). Здесь можно выяснить, какие принтеры к каким портам подключены или какие порты имеют присоединенные принтеры. Вдобавок вы можете просматривать или модифицировать свойства любого порта, просто щелкнув на нем правой кнопкой мыши и выбрав в контекстном меню пункт Configure Port (Конфигурировать порт). Диалоговое окно конфигурации порта показано на рис. 16.14.

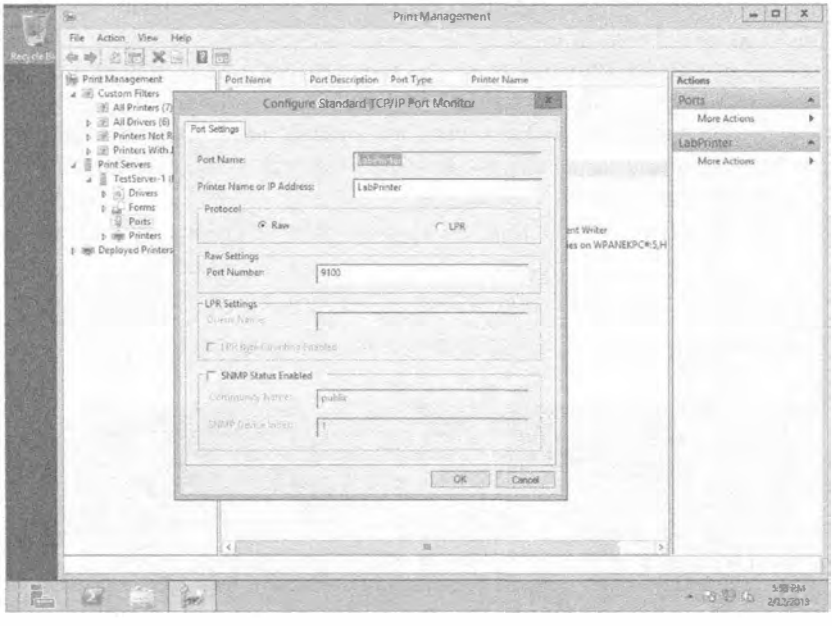


Рис. 16.14. Просмотр портов, доступных на сервере печати

При необходимости вы можете изменить IP-адрес принтера, использующего данный порт. Изменение этого IP-адреса может понадобиться, когда принтер перемещается в другую подсеть или ему назначается отличающийся IP-адрес по какой-то другой причине.

Для управления сетевыми устройствами часто применяется простой протокол сетевого управления (Simple Network Management Protocol — SNMP), и хотя стандартным именем сообщества является `Public` (Открытое), в производственной среде оно будет изменено. Если вы хотите, чтобы порты имели возможность взаимодействовать с системой управления SNMP, имя сообщества потребуется изменить для соответствия существующей среде.

Просмотр форм

Формы на сервере отражают разнообразные печатные макеты, которые могут поддерживать установленные принтеры. Формы отображаются для каждого сервера по отдельности. Другими словами, все формы на сервере печати доступны всем принтерам.

Щелчок правой кнопкой мыши на контейнере Forms (Формы) и выбор в контекстном меню пункта Manage Forms (Управлять формами) приведет к открытию диалогового окна свойств принтера с выбранной вкладкой Forms (Формы). Получить доступ к этой вкладке можно также через диалоговое окно свойств сервера печати. Здесь можно создать специальную форму, если возникает необходимость иметь специфичные поля или размеры печатной страницы.

Добавление роли Print Services к серверу версии Server Core

В Windows Server 2012 R2 поддерживается роль Print and Document Services для Server Core. Версия Server Core не имеет графического пользовательского интерфейса и требует управления из командной строки — во всяком случае, начальные задачи управления должны выполняться в командной строке.

Если на сервере функционирует Server Core и нужно сделать его сервером печати, добавив роль Print and Document Services, вы должны запустить PowerShell. В окне командной строки Server Core введите **`PowerShell`**. Обратите внимание, что после этого приглашение на ввод команды начинается с `PS`, указывая на то, что вы находитесь внутри приложения PowerShell.

Далее введите следующие две команды в командной строке PowerShell:

```
PS C:\Users\Administrator>ipmo ServerManager
PS C:\Users\Administrator>add-WindowsFeature Print-Server
```

Спустя момент вы увидите результаты установки (рис. 16.15).

Рис. 16.15. Установка сервера печати в Server Core с помощью PowerShell

Использование командлета Get-WindowsFeature для просмотра установленных ролей

Командлет Get-WindowsFeature позволяет получить сведения о конфигурации в установленной копии Server Core. Он также предоставляет корректное написание и синтаксис всех ролей, которые можно добавлять. Например, роль принтера идентифицируется как Print-Services.

В этот момент придется принять одно решение. Как вы хотите управлять ролью Print Services — в командной строке или посредством графического пользовательского интерфейса? В случае если вы предпочитаете управлять ею из графического пользовательского интерфейса (который более интуитивно понятен), необходимо сконфигурировать сервер Server Core для дистанционного администрирования, как объясняется в главе 17 (том 2).

Для управления сервером печати на сервере Server Core должно быть включено средство Network Discovery (Сетевое обнаружение). Это делается с помощью следующего командлета PowerShell:

```
PS C:\Users\Administrator> netsh firewall set service fileandprint enable
```

Вам также понадобится с помощью приведенной ниже команды включить возможность управления этим сервером через консоль MMC на удаленном сервере. Хотя в книге команда разнесена на две строки, она должна вводиться в одной строке.

```
PS C:\Users\Administrator> netsh advfirewall firewall set rule group =
"Remote Administration" new enable = yes
```

После того, как сервер Server Core сконфигурирован для дистанционного администрирования, такое администрирование можно проводить из сервера, на котором установлена полная версия операционной системы. Например, вы можете располагать 10 файловыми серверами и серверами печати, на которых функционирует Server Core, но иметь один центральный сервер с полной версией операционной системы, предназначенный для дистанционного администрирования всеми этими серверами.

Чтобы добавить сервер печати в консоль PMC, щелкните правой кнопкой мыши на узле Print Servers (Серверы печати) и выберите в контекстном меню пункт Add/Remove Servers (Добавить или удалить серверы). В открывшемся диалоговом окне Add/Remove Servers (Добавление или удаление серверов) введите имя удаленного сервера. Можете также щелкнуть на кнопке Browse (Обзор). Если средство Network Discovery отключено, будет выдан запрос на его включение, чтобы можно было обнаруживать другие компьютеры. Выберите нужный сервер и щелкните на кнопке Select Server (Выбрать сервер).

Если вам необходимо выполнять любые задачи в командной строке Server Core, в этом могут помочь различные инструменты.

Справочник по командлетам PowerShell

Если вы планируете применять PowerShell в Windows Server 2012 R2, полезно иметь краткий справочник по командлетам, имеющим отношение к задачам управления печатью. Использование этих командлетов также избавит от необходимости иметь дело со сценариями при управлении принтерами и драйверами.

- Add-Printer. Добавляет принтер к указанному компьютеру.
- Add-PrinterDriver. Устанавливает драйвер принтера на указанном компьютере.
- Add-PrinterPort. Устанавливает порт принтера на указанном компьютере.
- Get-PrintConfiguration. Получает конфигурационную информацию принтера.
- Get-Printer. Извлекает список принтеров, установленных на компьютере.
- Get-PrinterDriver. Извлекает список драйверов для принтеров, установленных на указанном компьютере.
- Get-PrinterPort. Извлекает список портов принтеров, установленных на указанном компьютере.
- Get-PrinterProperty. Извлекает свойства для указанного принтера.
- Get-PrintJob. Извлекает список заданий печати в указанном принтере.
- Remove-Printer. Удаляет принтер из указанного компьютера.
- Remove-PrinterDriver. Удаляет драйвер принтера из указанного компьютера.
- Remove-PrinterPort. Удаляет указанный принтер из указанного компьютера.
- Remove-PrintJob. Удаляет задание печати из указанного принтера.
- Rename-Printer. Переименовывает указанный принтер.
- Restart-PrintJob. Перезапускает задание печати на указанном принтере.
- Resume-PrintJob. Возобновляет работу приостановленного задания печати.
- Set-PrintConfiguration. Устанавливает конфигурационную информацию для указанного принтера.
- Set-Printer. Обновляет конфигурацию существующего принтера.
- Set-PrinterProperty. Модифицирует свойства для указанного принтера.
- Suspend-PrintJob. Приостанавливает задание печати на указанном принтере.

Развертывание принтеров для широких масс

После добавления принтеров к серверу их необходимо сделать доступными клиентам. Этого можно достичь тремя путями:

- вручную;
- через инструмент поиска в Active Directory;
- посредством групповой политики.

Если компьютеры находятся в домене Active Directory, вероятно, вы воспользуетесь вторым или третьим методом, обеспечивающими некоторую автоматизацию. В последующих разделах вы узнаете, как развертывать принтеры всеми тремя методами.

Добавление принтера к клиенту вручную

Когда вы добавили принтеры к серверу печати, добавить принтеры к клиенту (и обеспечить автоматическую установку подходящих драйверов) относительно легко. Следующие шаги демонстрируют добавление принтера к клиенту Windows 7.

1. В системе Windows 7 щелкните на кнопке Start (Пуск) и выберите пункт Printers (Принтеры).
2. Щелкните на кнопке Add a printer (Добавить принтер).
3. В открывшемся диалоговом окне выберите вариант Add a network, wireless, or Bluetooth printer (Добавить сетевой, беспроводной или Bluetooth-принтер).

   Система приступит к поиску доступных принтеров в сети.
4. Выберите вариант The printer that I want isn't listed (Нужный принтер отсутствует в списке).
5. Выберите переключатель Select a shared printer by name (Выбрать общий принтер по имени) и введите в поле **\\ИмяСервера**, чтобы просмотреть список общих принтеров (вводите действительное имя сервере).

   На рис. 16.16 иллюстрируется подключение к серверу по имени `BF1`.

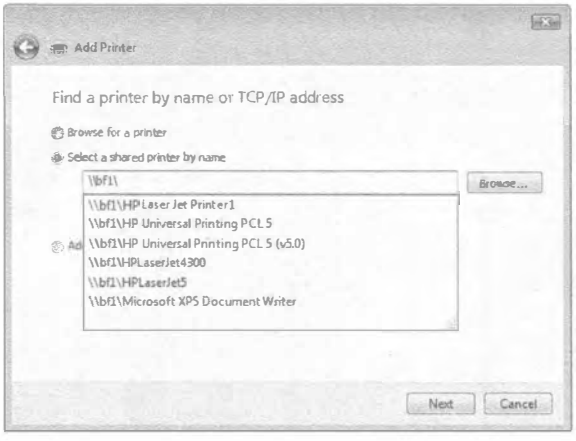


Рис. 16.16. Подключение к общему принтеру из Windows 7

6. Выберите желаемый общий принтер и щелкните на кнопке Next (Далее).

   Драйвер, который был установлен на сервере, автоматически загрузится и установится на клиенте. Имя принтера будет тем же самым, что было назначено на сервере.
7. Щелкните на кнопке Next и затем на кнопке Finish (Готово). На этом все.

Конечно, вряд ли вы захотите повторять это для 500 клиентов в организации. В таком случае сконфигурируйте автоматическое развертывание принтера с применением групповой политики, как объясняется в разделе "Развертывание принтеров через объект GPO" далее в этой главе.

Добавление принтера с использованием инструмента поиска в Active Directory

Среда Active Directory — это огромная база данных с объектами, где конечные пользователи и администраторы могут выполнять поиск. Многие объекты (такие как пользователи, компьютеры, группы и общие ресурсы) публикуются в Active

Directory автоматически, позволяя пользователям легко находить то, что их интересует. Однако принтеры по умолчанию не публикуются в Active Directory. Сделать это совсем нетрудно и после их появления в Active Directory пользователи смогут легко находить их с помощью быстрого поиска.

Любой принтер, к которому был открыт общий доступ, может также быть внесен в Active Directory при условии, что он размещен на сервере, являющемся членом домена. Другими словами, сетевые принтеры, которые не управляются сервером печати, не могут вноситься в Active Directory.

Откройте консоль PMC, перейдите в контейнер Printers (Принтеры), щелкните правой кнопкой мыши на имени нужного принтера и выберите в контекстном меню пункт List in Directory (Перечислить в каталоге), как показано на рис. 16.17. Вот и все. Обо всем остальном позаботится система.

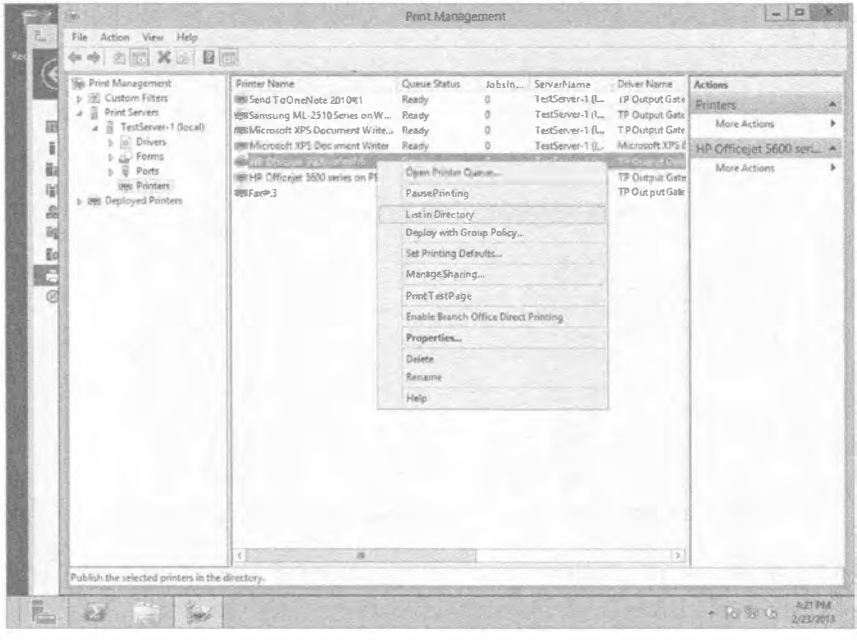


Рис. 16.17. Перечисление принтера в Active Directory

Если пункт List in Directory в контекстном меню не появился, дважды щелкните на имени принтера, чтобы проверить, открыт ли общий доступ к принтеру, на вкладке Sharing (Общий доступ) диалогового окна свойств принтера. В этом же окне свойств можно отметить флажок List in the directory (Перечислить в каталоге).

У пользователей в домене теперь появится возможность искать в Active Directory желаемые принтеры. Например, на другом сервере Windows Server 2012 R2 в домене можно было бы найти этот принтер посредством перечисленных ниже шагов.

1. В правой области проводника Windows выберите элемент Network (Сеть).
2. Выберите вариант Search Active Directory (Искать в Active Directory).

   Вариант Search Active Directory присутствует, только когда компьютер (в том числе компьютеры Windows 7 или Windows 8) является членом домена. Инте-

ресно отметить, что он не появляется на странице Network (Сеть) проводника для контроллера домена, но может быть доступен через оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory).

3. В окне поиска в Active Directory выберите в поле со списком Find (Искать) элемент Printers (Принтеры). Введите `HP` в текстовом поле Name (Имя) и щелкните на кнопке Find Now (Найти сейчас). Результат показан на рис. 16.18.

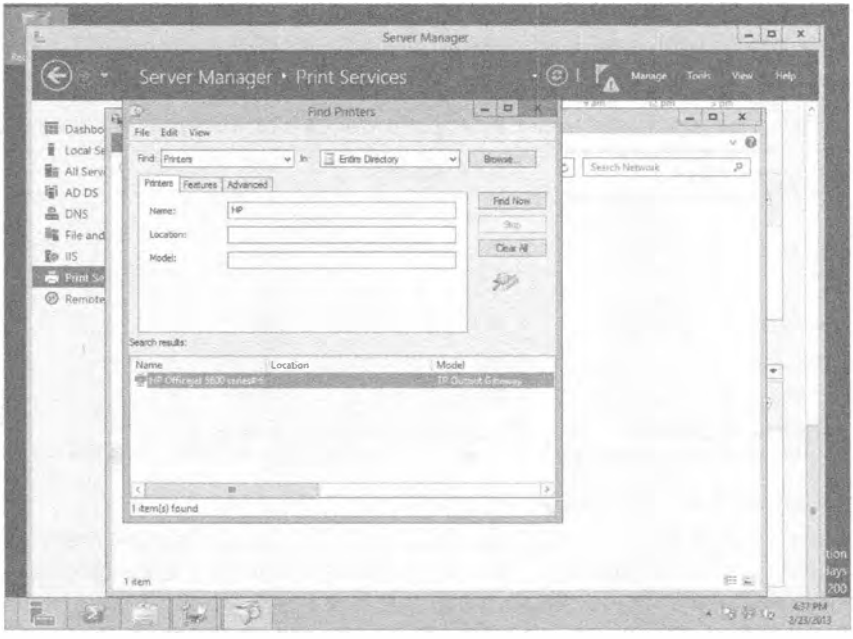


Рис. 16.18. Поиск принтера, внесенного в Active Directory

Строковый поиск

Обратите внимание, что нет необходимости вводить полное название модели принтера. Это очень ценно, т.к. названия моделей принтеров зачастую напоминают по своей длине имена членов небольшой королевской семьи. Вместо этого инструмент поиска в Active Directory ищет строковые соответствия, так что будут найдены любые модели, названия которых начинаются с `HP`. Хотя это вполне рабочий пример поиска, но если в организации все установленные принтеры являются моделями HP, он окажется не особенно полезным.

После того, как принтер найден, пользователь может просто дважды щелкнуть на нем, чтобы установить его как дополнительный принтер в своей системе. При условии, что на сервер печати был добавлен корректный драйвер, он автоматически загрузится на компьютер клиента, и клиенту не придется предпринимать дополнительные шаги для использования принтера.

Искать принтер можно на основе практически любых желаемых характеристик либо их комбинации. Поиск принтера по имени не выглядит особо вероятным, поскольку если вам известно настолько много сведений, то вполне возможно, что вы

также знаете домен и сервер, где этот принтер находится. Тем не менее, вам может быть известно местоположение принтера. Если при добавлении принтера было указано его местоположение, его можно применять в качестве поискового термина.

Поскольку сотрудники могут искать принтер в Active Directory по его местоположению, старайтесь указывать краткие и согласованные местоположения (вроде "Испытательная среда" или "Приемная"). Как упоминалось ранее, если вы используете полную реализацию средства Printer Locations, то должны обеспечить ввод местоположения принтера в точности как оно вводилось для объекта Active Directory Sites and Services. В табл. 16.1 приведено множество распространенных критериев, которые можно применять при поиске принтеров в Active Directory.

Таблица 16.1. Распространенные критерии поиска принтеров в Active Directory

Характеристика принтера	Где находится
Имя	Вкладка Printers (Принтеры)
Местоположение	Вкладка Printers
Модель	Вкладка Printers
Двухсторонняя печать	Вкладка Features (Возможности)
Цветная печать	Вкладка Features
Возможность сшивки	Вкладка Features
Поиск по отдельному свойству	Вкладка Advanced (Дополнительно)

Поиск по характерным чертам

Часто пользователи достаточно осведомлены о характеристиках принтера, который они ищут: печатающий в цвете, допускающий сшивку или обладающий другими особенностями. На рис. 16.19 показана вкладка Features (Возможности) окна поиска. Если пользователь ищет конкретную характеристику, здесь он может указать ее и щелкнуть на кнопке Find Now (Найти сейчас).

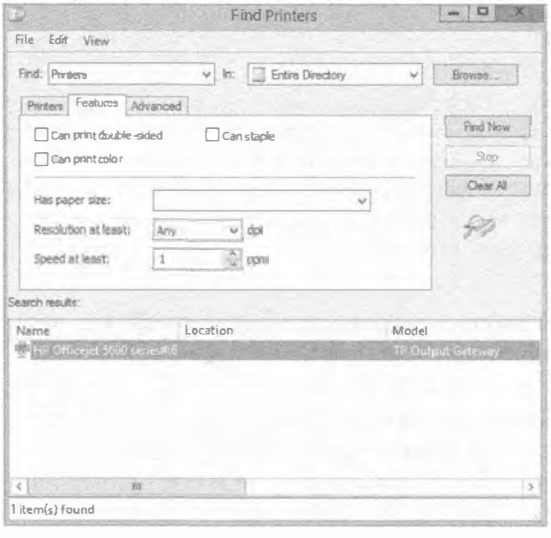


Рис. 16.19. Поиск принтеров на основе поддерживаемых ими возможностей

Расширенный поиск

Содержимое вкладки Advanced (Дополнительно) больше всего подходит тем, кто *действительно* знает свои принтеры, т.к. критерий поиска здесь детальнее, чем требуется большинству людей. В то время как первые две вкладки позволяют описывать принтер в терминах того, где он находится, как называется и что он умеет делать, вкладка Advanced дает возможность описать принтер точно.

На рис. 16.20 показано раскрывающееся меню Field (Поле) с выделенным свойством Paper Available (Доступная бумага). Обратите внимание на количество свойств, по которым можно производить поиск. Если существует какое-то свойство принтера, то его можно выбрать для поиска.

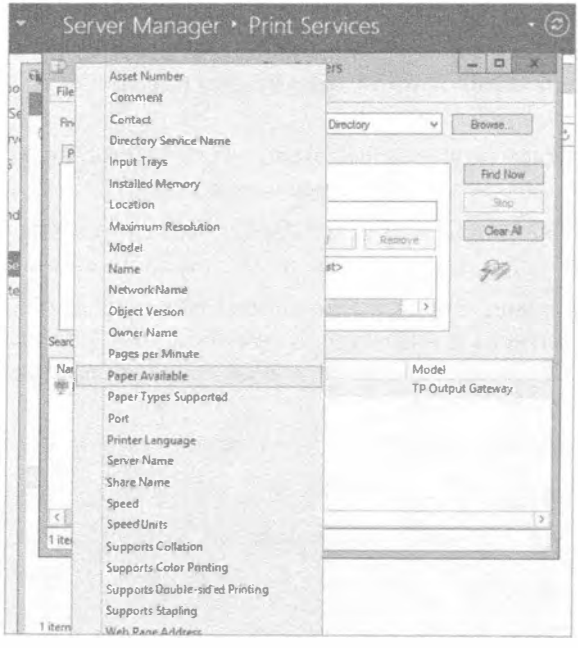


Рис. 16.20. Поиск принтеров на основе поддерживаемых ими возможностей

После выбора свойства вы указываете условие, такое как Starts with (Начинается с) и Ends with (Заканчивается на), и вводите текст в поле Value (Значение) для сопоставления со свойством и условием. Например, можно было бы выбрать свойства Server Name (Имя сервера), указать условие Starts with и ввести **BF** в поле Value. По щелчку на кнопке Find Now отобразятся все принтеры, размещенные на любом сервере, имя которого начинается с BF.

Развертывание принтеров через объект GPO

Принтеры можно также развертывать с использованием объекта групповой политики (GPO). На случай, если требуется поддерживать клиенты Windows 8 и серверы Windows Server 2012 R2, имеется пара предостережений.

- В Active Directory должна применяться версия схемы Windows Server 2012 R2. Если вы устанавливали первый контроллер домена с Windows Server 2012 R2,

то имеете обновленную схему. Если это не так, придется запустить утилиту `adprep` для ее обновления. Дополнительные сведения по `adprep` ищите в статье по адресу `http://technet.microsoft.com/library/cc731728.aspx`.

- Клиенты, у которых установлена версия, отличная от Windows 8 или Windows Server 2012 R2, должны использовать в сценарии запуска или входа инструмент `PushPrinterConnections.exe`.

Если домен полностью основан на Windows Server 2012 R2 или схема обновлена с помощью `adprep`, можно выполнить следующие шаги, чтобы развернуть принтеры через объект GPO.

1. Откройте консоль PMC и перейдите к узлу Printers (Принтеры) для нужного сервера.
2. Щелкните правой кнопкой мыши на имени принтера и выберите в контекстном меню пункт Deploy with Group Policy (Развернуть с помощью групповой политики).

   Этот пункт находится прямо под пунктом List in Directory (Перечислить в каталоге), который обсуждался в предыдущем разделе.
3. В открывшемся диалоговом окне Deploy with Group Policy (Развертывание с помощью групповой политики) щелкните на кнопке Browse (Обзор).
4. Щелкните на значке Create a New Group Policy Object (Создать новый объект групповой политики) и назначьте новому объекту GPO имя **`Deploy Printers`**. (При наведении курсора мыши на значок появляется всплывающая подсказка; вам нужен средний значок.)

   Диалоговое окно должно выглядеть подобно показанному на рис. 16.21.

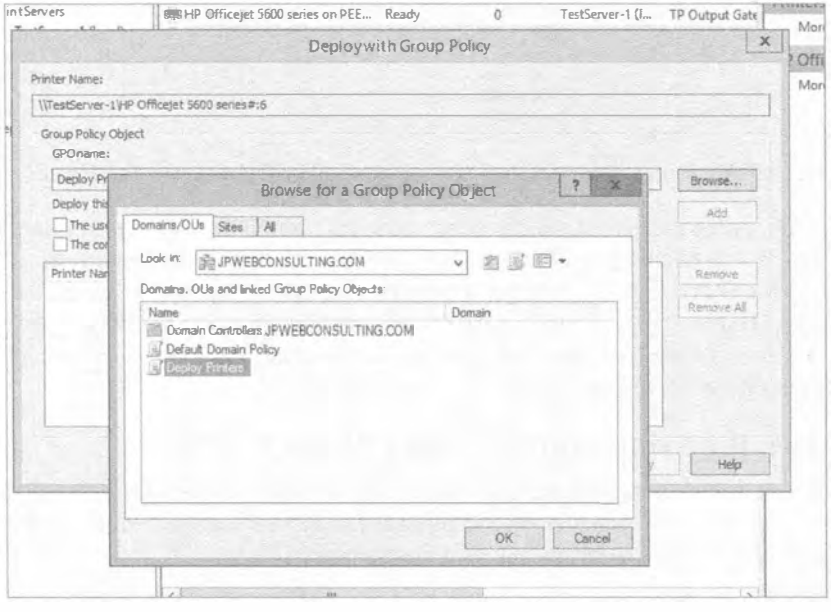


Рис. 16.21. Создание объекта групповой политики

5. Выберите объект GPO по имени `Deploy Printers` и щелкните на кнопке OK.
6. Отметьте флажок The computers that this GPO applies to (per machine) (Компьютеры, к которым применяется этот объект GPO (по машинам)).

   Вы могли бы также отметить флажок The users that this GPO applies to (per user) (Пользователи, к которым применяется этот объект GPO (по пользователям)), если хотите, чтобы объект GPO применялся к пользователям, не принимая во внимание, кто вошел в систему на компьютере, или к пользователю независимо от того, где он вошел в систему.
7. Щелкните на кнопке Add (Добавить). Выбранные настройки будут назначены объекту GPO.
8. Щелкните на кнопке OK, чтобы применить настройки.

   Спустя некоторое время появится диалоговое окно, извещающее об успешном добавлении объекта GPO для развертывания принтера (рис. 16.22).

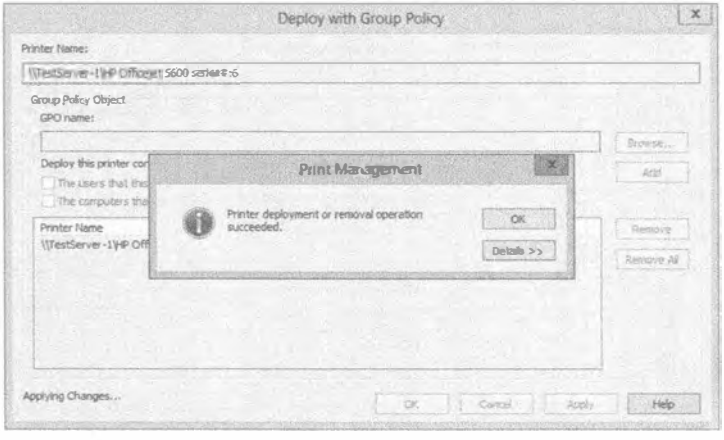


Рис. 16.22. Добавление настроек к объекту GPO

9. Щелкните на кнопке OK, чтобы закрыть это диалоговое окно, и еще раз на OK, чтобы закрыть диалоговое окно Deploy with Group Policy.

   Предыдущий шаг приводит к добавлению принтера как развернутого в узел Computer Configuration\Policies\Windows Settings\Deployed Printers (Конфигурация компьютера \ Политики \ Настройки Windows \ Развернутые принтеры) созданного объекта GPO под названием `Deploy Printers`.

Теперь можете перейти на любой компьютер Windows 8 или Windows Server 2012 в домене, ввести в окне командной строки команду **`gpupdate /force`**, обновляющую групповую политику, и принтер автоматически появится вместе с другими устройствами и принтерами, имея корректный драйвер.

Если все ваши клиенты функционируют под управлением Windows 8 или Windows Server 2012, на этом работа завершена. Однако при наличии других клиентов, таких как Windows Vista и Windows XP, на каждом из них понадобится сконфигурировать запуск утилиты `PushPrinterConnection.exe`, чтобы обеспечить развертывание принтера. Эта утилита не входит в состав стандартной установки Windows Server 2012 R2

или Windows 8, т.к. эти операционные системы в ней не нуждаются, но она находится в папке `Windows\System32` в системах Windows Server 2008 и Windows Vista.

Чтобы настроить запуск этой утилиты на клиентских компьютерах, где это необходимо, выполните перечисленные ниже шаги.

1. Откройте консоль Group Policy Management (Управление групповой политикой), нажав клавишу <Windows> и выбрав элемент Group Policy Management (Управление групповой политикой).
2. Перейдите к объекту GPO по имени `Deploy Printers` в домене, щелкните на нем правой кнопкой мыши и выберите в контекстном меню пункт Edit (Редактировать), как показано на рис. 16.23.

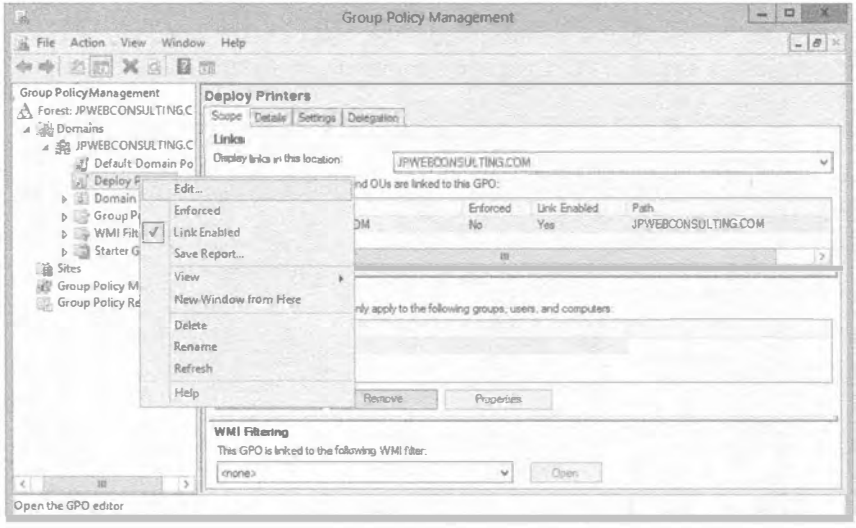


Рис. 16.23. Выбор объекта GPO для редактирования

Развертывание через объект GPO напрямую

Развертывать принтеры можно также из оснастки Group Policy (Групповая политика). Перейдите к папке Policies\Windows Settings\Deployed Printers (Политики \ Настройки Windows \ Развернутые принтеры) и щелкните на ней правой кнопкой мыши. В открывшемся контекстном меню выберите пункт Deploy Printer (Развернуть принтер) и перейдите к желаемому принтеру.

3. Перейдите к узлу Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown) (Конфигурация компьютера \ Политики \ Настройки Windows \ Сценарии (запуска/завершения)).
4. Дважды щелкните на папке Startup (Запуск) и в открывшемся диалоговом окне Startup Properties (Свойства запуска) щелкните на кнопке Show Files (Показать файлы). Обратите внимание, что папка сейчас пуста. Вы должны скопировать утилиту `PushPrinterConnection.exe` в эту папку. Сделайте это в проводнике Windows, после чего закройте его.

5. Щелкните на кнопке Add (Добавить). В открывшемся диалоговом окне Add a Script (Добавить сценарий) щелкните на кнопке Browse (Обзор) и выберите файл `PushPrinterConnection.exe`. Щелкните на кнопке Open (Открыть).

   Диалоговые окна будут выглядеть примерно так, как на рис. 16.24.

   При желании можете указать в текстовом поле Script Parameters (Параметры сценария) ключ `-log`, чтобы включить регистрацию в журнале на компьютерах, где запускается эта утилита. Журнал расположен в файле `%Windir%\temp\ppcMachine.log` для компьютеров или в файле `%temp%\ppcUser.log` для подключений пользователей.

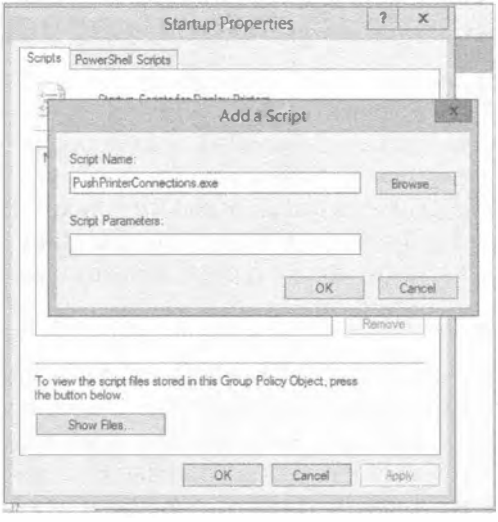


Рис. 16.24. Добавление `PushPrinterConnections` в сценарий запуска

6. Щелкните на кнопке OK, чтобы закрыть диалоговое окно Add a Script, и еще раз на кнопке OK для закрытия диалогового окна Startup Properties.

Дело сделано. Удобным свойством утилиты `PushPrinterConnections` является то, что при попытке ее запуска на компьютере с Windows 8 or Windows Server 2012 она автоматически опознает среду и завершается. Вам не придется беспокоиться об этом в случае развертывания в смешанной среде.

Поддержка избирательности с объектами GPO

Приведенные выше шаги обеспечивают развертывание объекта GPO всем пользователям в домене, однако вы могли бы проявить большую избирательность. Например, если вы хотите, чтобы данный принтер развертывался только для пользователей организационной единицы `Sales`, можете открыть консоль Group Policy Management, удалить из объекта GPO под названием `Deploy Printers` связь с доменом и привязать его к организационной единице `Sales`. Как только клиенты домена обновят групповую политику (или после принудительного ее обновления посредством команды `gpupdate /force`), принтер будет удален у всех клиентов, не относящихся к организационной единице `Sales`.

Просмотр развернутых принтеров

Просмотреть все развернутые принтеры с помощью консоли PMC довольно легко, для чего нужно выбрать контейнер Deployed Printers (Развернутые принтеры). Будет выдан запрос в Active Directory и отобразятся все принтеры, развернутые через объект GPO. Хотя в этом представлении нельзя развертывать дополнительные принтеры, здесь можно удалять опцию развертывания для принтеров. Просто щелкните правой кнопкой мыши на любом развернутом принтере, выберите в контекстном меню пункт Deploy with Group Policy (Развернуть с помощью групповой политики) и удалите опцию развертывания.

Конфигурирование настроек сервера печати

На уровне сервера применяется набор настроек, которые могут быть сконфигурированы один раз для применения ко всем ресурсам (драйверам, формам, портам и принтерам), управляемых этим сервером. Можно также экспортировать и импортировать принтеры посредством файлов и устанавливать уведомления. Чтобы отредактировать настройки на уровне сервера, откройте консоль PMC, перейдите в контейнер Print Servers (Серверы печати) и щелкните правой кнопкой мыши на имени нужного сервера, чтобы просмотреть доступные варианты в контекстном меню.

Свойства сервера

Выбрав в контекстном меню пункт Server Properties (Свойства сервера), вы увидите диалоговое окно Print Server Properties (Свойства сервера печати) с пятью вкладками. На рис. 16.25 показано это окно с выбранной вкладкой Forms (Формы). Попасть на эту же вкладку можно, щелкнув правой кнопкой мыши на контейнере Forms (Формы) и выбрав в контекстном меню пункт Manage Forms (Управлять формами).

Рис. 16.25. Вкладка Forms диалогового окна Print Server Properties

Ниже перечислены вкладки, которые позволяют конфигурировать настройки сервера:

- Forms (Формы)
- Ports (Порты)
- Drivers (Драйверы)
- Security (Безопасность)
- Advanced (Дополнительно)

Выбор настроек форм

Задания печати организованы на основе размера бумаги и форм, которые определяют шаблон для печатаемого текста. Серверы печати содержат длинные списки заранее определенных форм, из которых можно выбирать необходимые варианты, но допускается также определять собственные настройки формы, предназначенные для печати на фирменных бланках компании.

Серверы печати сконфигурированы для печати на чистых листах бумаги 216×279 мм (стандартный размер). Чтобы выбрать другую форму, найдите ее в списке.

Если вы хотите создать новую форму, отметьте флажок Create a new form (Создать новую форму), отредактируйте должным образом описание формы и щелкните на кнопке OK. Любые вновь созданные формы можно модифицировать, для чего их следует выбрать, внести изменения и затем щелкнуть на кнопке Save Form (Сохранить форму). Удалять заранее определенные формы нельзя, но можно удалять формы, которые были созданы вами.

Конфигурирование настроек портов сервера

Перейдя на вкладку Ports (Порты), можно просмотреть все порты, доступные на сервере. Эта вкладка представлена на рис. 16.26.

Рис. 16.26. Вкладка Ports диалогового окна Print Server Properties

Обратите внимание, что здесь можно добавлять, удалять и конфигурировать порты, хотя большинство портов требуют весьма незначительного конфигурирования. Попасть на эту вкладку можно также, щелкнув правой кнопкой мыши на контейнере Ports (Порты) и выбрав в контекстном меню пункт Manage Ports (Управлять портами).

Как правило, необходимость в самостоятельном создании порта не возникает. Обычно при добавлении сетевого принтера вы будете добавлять и порт, как было показано ранее в этой главе. А когда вы добавляете принтер USB, порт добавляется автоматически. Порты LPT (параллельный) или COM (последовательный) в наши дни используются очень редко, но если у вас они имеются, то несколько таких портов сконфигурированы в готовом виде.

Если вы больше не применяете порт, можете просто выбрать его и щелкнуть на кнопке Delete Port (Удалить порт), чтобы удалить его. Порты USB не имеют настраиваемых опций, а конфигурирование портов TCP/IP рассматривалось ранее в этой главе.

Добавление или обновление драйвера принтера на сервере печати

Ранее вы узнали, как добавлять драйвера для принтера. Это обычно делается для поддержки разных клиентов. На вкладке Drivers (Драйверы) диалогового окна Print Server Properties можно добавлять драйверы для принтеров, используя аналогичный процесс.

Хотя большинство задач управления драйверами будет выполняться внутри принтера, временами требуется управлять драйверами, когда принтер еще не установлен на сервере. Например, может понадобиться добавить драйверы до добавления принтера или удалить неиспользуемые драйверы после того, как принтер был удален.

Управление безопасностью печати

На вкладке Security (Безопасность) можно управлять разрешениями, применяемыми к целому серверу. Существуют отличия между разрешениями, которые применяются к серверу, и разрешениями, применяемыми к принтеру. На рис. 16.27 слева показаны разрешения для сервера, а справа — разрешения для принтера.

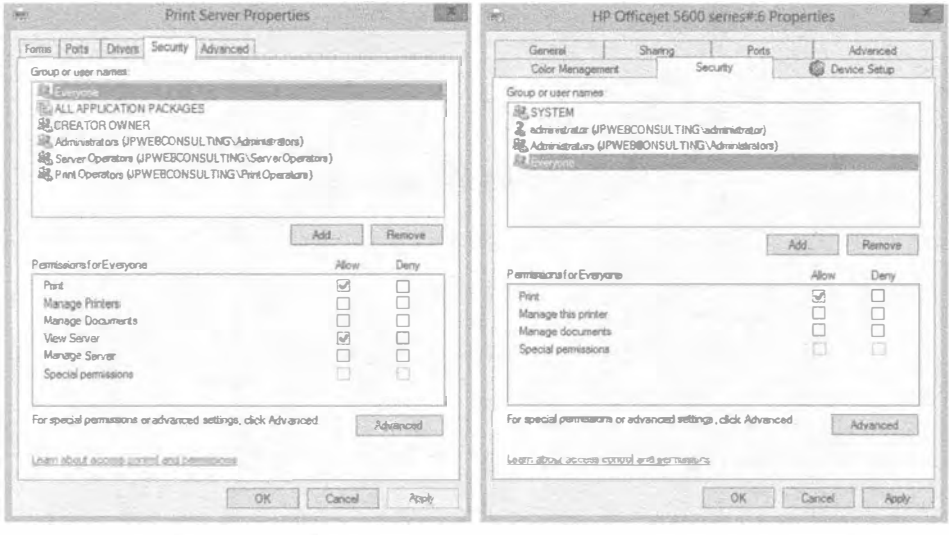


Рис. 16.27. Вкладки Security диалогового окна Print Server Properties для сервера (слева) и для отдельного принтера (справа)

Точно так же, как разрешения NTFS и общего доступа (см. главу 14) могут быть установлены в Allow (Разрешить) или Deny (Запретить) для любого пользователя или группы пользователей, в Allow или Deny могут быть установлены и разрешения для сервера печати и индивидуальных принтеров.

Установка любых разрешений, совпадающих для сервера и принтера, на уровне сервера приводит к тому, что все добавляемые новые принтеры получают те же самые разрешения. Существующие разрешения не изменяются; это воздействует только на устанавливаемые новые принтеры.

Ниже описаны разрешения для сервера печати.

- **Print (Печать).** Пользователи могут отправлять задания печати принтеру. По умолчанию это разрешение предоставляется группе `Everyone` (Все).
- **Manage Printers (Управление принтерами).** Пользователи могут изменять свойства и разрешения для принтера. По умолчанию это разрешение предоставляется группам `Administrators` (Администраторы), `Server Operators` (Операторы сервера) и `Print Operators` (Операторы печати).
- **Manage Documents (Управление документами).** Пользователи могут управлять настройками, специфичными для документов, а также приостанавливать, возобновлять, перезапускать и удалять подкачанные задания печати. По умолчанию это разрешение предоставляется группам `Creator Owner` (Владелец создателя), `Administrators`, `Server Operators` и `Print Operators`. Когда пользователь создает задание печати, он становится членом группы `Creator Owner` для данного задания, получая возможность управлять собственными документами.
- **View Server (Просмотр сервера).** Пользователи могут просматривать свойства и настройки сервера, однако не могут изменять эти свойства. По умолчанию это разрешение предоставляется группам `Everyone` (Все), `Administrators`, `Server Operators` и `Print Operators`.
- **Manage Server (Управление сервером).** Разрешение Manage Server позволяет пользователям изменять любые свойства и настройки сервера. По умолчанию это разрешение предоставляется группам `Administrators`, `Server Operators` и `Print Operators`.
- **Special Permissions (Особые разрешения).** Щелкнув на кнопке Advanced (Дополнительно), можно назначить индивидуальные разрешения на детальном уровне. Если любые индивидуальные разрешения не были назначены, флажки для Special Permissions будут затенены.

Делегирование разрешений

Стандартные разрешения в Windows Server 2012 R2 не позволяют пользователям, не являющимся администраторами, выполнять любые операции по администрированию печати. Однако возможно предоставить любое выбранное разрешение для принтера, желательное на сервере, не выдавая пользователям полные права системного администрирования.

Просмотр дополнительных свойств сервера

На вкладке Advanced (Дополнительно) доступно несколько дополнительных свойств, которые можно конфигурировать. Эта вкладка представлена на рис. 16.28.

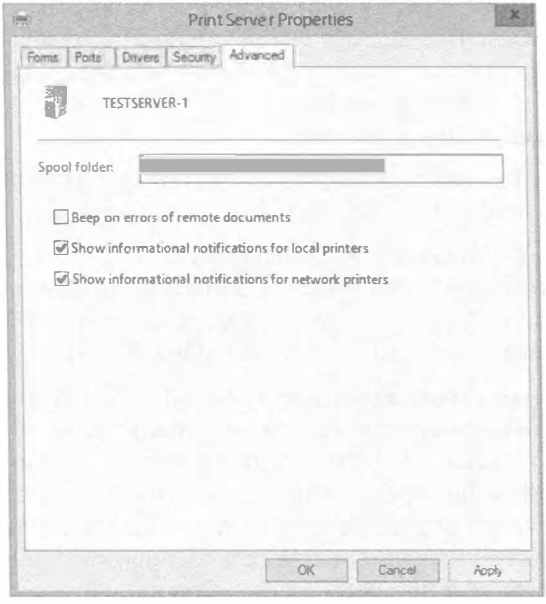


Рис. 16.28. Вкладка Advanced диалогового окна Print Server Properties

Наиболее распространенная причина перехода на вкладку Advanced связана с необходимостью изменения папки для спулера. Как вы помните, любые документы, которые не могут быть отправлены принтеру немедленно, помещаются на жесткий диск и затем отправляются принтеру, как только он становится свободным. На выделенном сервере печати принято переносить папку для спулера на отдельный диск.

Существуют две причины переноса папки для спулера.

- **Чтобы предоставить спулеру больше дискового пространства.** Поскольку некоторые задачи печати могут быть очень большими, они потребляют слишком много пространства на жестком диске. Хотя подкачанное задание после вывода на печать будет удалено, если одновременно подкачивается множество заданий, дисковое пространство может исчерпаться.
- **Чтобы улучшить производительность.** Стандартное местоположение будет соперничать за дисковый ввод-вывод с операционной системой. Если возникла проблема с низкой производительностью, можно перенести папку для спулера на жесткий диск, отдельный от диска, на котором установлена операционная система.

Перенос папки для спулера сводится просто к вводу пути к ее новому местоположению. Если папка по указанному пути не существует, она будет создана. Однако будьте осторожны. Изменение произойдет немедленно, и любые документы, которые были подкачаны в предыдущую папку, печататься не будут. Прежде чем переносить папку для спулера, вы должны подождать, пока не останется каких-либо активных документов, ожидающих печати.

Остальные настройки второстепенны. Вы можете включить выдачу звукового сигнала при возникновении ошибок в удаленных документах и отображать информационные уведомления для локальных и сетевых принтеров. Несмотря на отсутствие возможности конфигурирования, появилась удобная новая возможность отправки уведомлений по электронной почте, которая будет описана позже в этой главе.

Миграция принтеров

Миграция принтеров с одного сервера на другой выполняется относительно просто с использованием мастера миграции принтеров (Printer Migration Wizard). Представьте себе, что вы эксплуатируете сервер в качестве сервера печати, обслуживающего 20 или более принтеров, на протяжении длительного времени. Вам нужно вывести из эксплуатации этот сервер, но перед тем разместить принтеры на новом сервере. Воссоздание всех принтеров на новом сервере вручную может занять значительное время.

Вы можете экспортировать принтеры в файл на исходном сервере и затем импортировать их из этого файла на новом сервере. В этот момент оба сервера будут действовать как серверы печати для тех же самых устройств печати. Далее необходимо сконфигурировать клиентов на работу с новым сервером печати, после чего выводить старый сервер из эксплуатации. Если вы развертывали их с помощью групповой политики, можете просто изменить настройки групповой политики, чтобы указать на новый сервер.

Для выполнения экспорта принтеров щелкните правой кнопкой на имени сервера и выберите в контекстном меню пункт Export Printers to a File (Экспортировать принтеры в файл), укажите местоположение и сохраните файл. Затем скопируйте этот файл в местоположение, доступное новому серверу.

Находясь в системе нового сервера, щелкните правой кнопкой на его имени и выберите в контекстном меню пункт Import Printers from a File (Импортировать принтеры из файла) и перейдите к местоположению, где находится экспортированный файл. Мастер миграции предлагает несколько опций импорта (рис. 16.29).

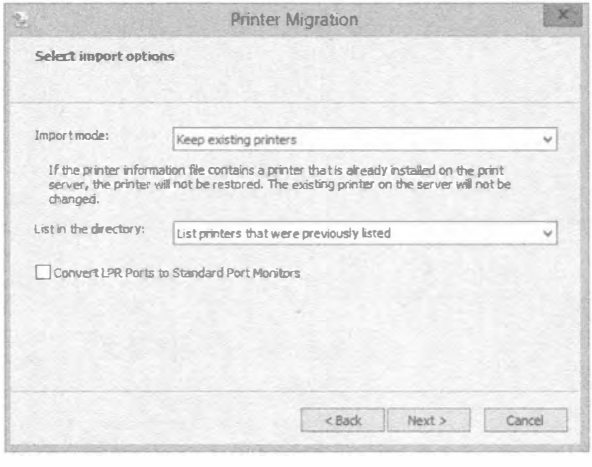


Рис. 16.29. Импортирование принтеров на новый сервер печати

Вы можете сохранить существующие принтеры или полностью перезаписать их. Кроме того, вы можете выбрать, каким образом принтеры будут перечисляться в Active Directory — перечислять только те принтеры, которые были перечислены ранее, перечислять все принтеры или вообще не перечислять ни одного из них.

Этот метод также пригоден для восстановления конфигурации принтеров в фиксированное состояние. Если вы экспортировали принтеры в файл, а впоследствии они разрушились, были изменены или удалены, то можете просто импортировать этот файл и восстановить конфигурацию.

Управление свойствами принтеров

Подобно тому, как сервер печати имеет множество свойств, которыми можно управлять, просматривать и манипулировать, допускается также манипулировать свойствами для индивидуальных принтеров. Ранее в этой главе вы узнали, каким образом добавлять принтеры. Если позже возникает необходимость в изменении настроек любого принтера, щелкните правой кнопкой мыши на его имени и выберите в контекстном меню пункт Properties (Свойства).

На рис. 16.30 показано диалоговое окно свойств принтера с выбранной вкладкой General (Общие). На вкладке General отображается базовая информация о принтере, такая как имя, местоположение, комментарий (если есть), модель и функции, поддерживаемые принтером. Эта вкладка часто будет содержать кнопку Preferences (Свойства), по щелчку на которой появляется возможность модификации специфичных пользовательских предпочтений для принтера. На ней также предусмотрена кнопка Print Test Page (Печатать тестовую страницу), которая очень удобна для проверки возможности подключения к принтеру.

Рис. 16.30. Вкладка General диалогового окна свойств принтера

В диалоговом окне свойств имеется множество других вкладок. В зависимости от функциональных возможностей, для некоторых принтеров будет доступно больше вкладок. Вкладки подобного рода добавляются из пакета драйвера для принтера.

Вкладка Sharing диалогового окна свойств принтера

Вкладка Sharing (Общий доступ) упоминалась ранее в главе при обсуждении добавления драйверов для принтера. Ее можно также применять для открытия общего доступа (или его прекращения) к принтеру, просто отмечая соответствующий флажок. Эта вкладка содержит флажок List in the directory (Перечислить в каталоге), который можно отметить либо здесь, либо щелкнуть правой кнопкой мыши на имени принтера и выбрать в контекстном меню пункт List in Directory (Перечислить в каталоге).

Вкладка Ports диалогового окна свойств принтера

Вкладка Ports (Порты) позволяет добавлять, удалять и конфигурировать порты, используемые принтером. Большинство принтеров могут получать данные для печати и также отправлять данные серверу, сообщая о возникновении таких условий, как низкий уровень тонера, отсутствие бумаги и замятие бумаги. На этой вкладке имеется флажок Enable bidirectional support (Включить двунаправленную поддержку), который по умолчанию отмечен, чтобы разрешить принтеру отправку и получение данных.

Самой распространенной причиной доступа к этой вкладке является отметка флажка Enable printer pooling (Включить организацию пула для принтера). Пул для принтера позволяет добавлять к одному принтеру несколько устройств печати.

Как упоминалось ранее в этой главе, пропорция между числом принтеров и количеством устройств печати не всегда будет один к одному. Позже вы увидите, как создавать множество принтеров для одиночного устройства печати, но здесь будет показано, каким образом обеспечить поддержку единственным принтером несколько устройств печати.

По какой причине это может понадобиться? По большей части это вопрос эффективности. Даже с учетом доступных сегодня быстрых устройств печати в загруженных офисах могут возникать ситуации, когда заданий печати поступает больше, чем способно справиться одно устройство печати. Чтобы сгладить работу и сократить задержки, вы можете распределить задания печати между несколькими устройствами печати. Все клиенты будут отправлять задания печати одному и тому же принтеру, но эти задания попадут на устройство печати, которое наименее занято в текущий момент. Такой прием называется *организацией пула для принтера*. На рис. 16.31 представлена вкладка Ports с отмеченным флажком Enable printer pooling.

На рис. 16.31 обратите внимание на включение двух портов. Это возможно, только когда отмечен флажок Enable printer pooling. Добавлять можно столько портов, сколько есть устройств печати и сколько их требуют существующие нужды.

С организацией пула для принтера связана пара препятствий. Во-первых, устройства печати в пуле должны работают с тем же самым драйвером. Так как многие устройства печати содержат одни и те же или сходные внутренние части, вполне возможно иметь разные устройства печати, которые используют такой же драйвер. Однако если эти устройства требуют разных драйверов, они не смогут функционировать внутри одного пула для принтера.

Рис. 16.31. Включение организации пула для принтера на вкладке Ports

Во-вторых, мы настоятельно рекомендуем размещать устройства печати, объединенные в пул, в том же самом физическом месте. Поскольку пользователям не известно, на каком устройстве печати будет выведено их задание, нежелательно заставлять их бродить с места на место в поисках своей распечатки.

Разделительные страницы

Рассмотрите возможность применения в пулах для принтеров разделительных страниц с именами пользователей, т.к. пользователи не обязательно будут знать, на какое устройство печати попало их задание. Разделительные страницы подробно объясняются далее в этой главе.

Вкладка Security диалогового окна свойств принтера

Тем, кто знаком с любой текущей операционной системой Windows, должно быть известно, что сеть защищается путем определения прав для пользователей относительно того, что они могут *делать* в сети, и установки разрешений для ресурсов, регламентирующих, кто их может *использовать*. Безопасность принтеров управляется посредством разрешений на основе групп и пользователей. Разрешения обычно объединяются (т.е. применяется их наименее ограничивающий набор), если только речь не идет о запрете доступа. Запрет доступа переопределяет любые включенные разрешения.

Вкладку Security (Безопасность) можно использовать, чтобы изменить разрешения для принтера. Как показано на рис. 16.32, любому пользователю или группе можно предоставить четыре молекулярных разрешения. Подобно другим разрешениям в Windows, для разрешений печати могут быть указаны действия Allow или Deny.

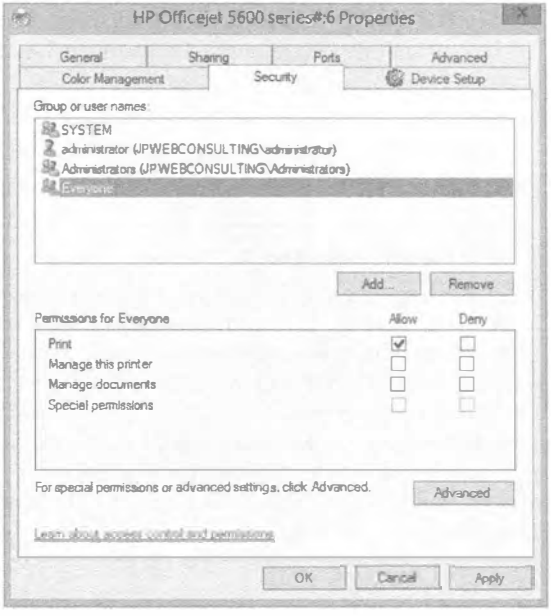


Рис. 16.32. Разрешения печати на вкладке Security

Хотя здесь видны четыре молекулярных разрешения, на самом деле доступно шесть атомарных разрешений.

Вы можете помнить из главы 14, что в NTFS имеются молекулярные разрешения вроде Read (Чтение), которые отображаются на атомарные разрешения; молекулярное разрешение Read сочетает в себе четыре атомарных разрешения — Read Data (Чтение данных), Read Permissions (Чтение разрешений), Read Attributes (Чтение атрибутов) и Read Extended Attributes (Чтение расширенных атрибутов). Назначая разрешение Read, в действительности вы назначаете четыре лежащих в его основе разрешения. Разрешения печати работают похожим образом, хотя они и не настолько сложны. Существуют три молекулярных и три атомарных разрешения. Молекулярные разрешения перечислены ниже.

- **Print (Печать).** Пользователь может отправлять задания печати принтеру. Это разрешение включает Read Permissions (Чтение разрешений). По умолчанию разрешение Print предоставляется группе `Everyone` (Все).
- **Manage This Printer (Управление этим принтером).** Пользователь может изменять свойства принтера и его разрешения. Это разрешение включает следующие разрешения: Print (Печать), Read Permissions (Чтение разрешений), Change Permissions (Изменение разрешений) и Take Ownership (Получение права владения). По умолчанию разрешение Manage This Printer предоставляется группам `Administrators` (Администраторы), `Server Operators` (Операторы сервера) и `Print Operators` (Операторы печати).
- **Manage Documents (Управление документами).** Пользователь может управлять настройками, специфичными для документов, а также приостанавливать, возобновлять, перезапускать и удалять подкачанные задания печати. Это разрешение включает следующие разрешения: Read Permissions (Чтение разрешений),

Change Permissions (Изменение разрешений) и Take Ownership (Получение права владения). По умолчанию разрешение Manage Documents предоставляется группам `Creator Owner` (Владелец создателя), `Administrators`, `Server Operators` и `Print Operators`. Когда пользователь создает задание печати, он становится членом группы `Creator Owner` для данного задания, получая возможность управлять собственными документами.

Разрешения являются кумулятивными

Если пользователю предоставляется несколько разрешений из-за того, что он входит в состав множества групп, он получит кумулятивное значение по всем разрешениям. Например, если пользователю как члену группы `Everyone` предоставляется разрешение Print и как члену другой группы выдается разрешение Manage This Printer, он получает комбинацию этих разрешений.

Единственным исключением является применение Deny. Если пользователь входит в состав группы, которой предоставлено разрешение Print, и в состав еще одной группы, где для этого разрешения указано действие Deny, то Deny всегда получает преимущество, в точности, как это было в разрешениях NTFS и открытого доступа.

Для удовлетворения большинства (если только не всех) требований молекулярных разрешений будет достаточно. Однако если вы щелкнете на кнопке Advanced (Дополнительно) внутри вкладки Security и в открывшемся диалоговом окне щелкнете на кнопке Edit (Редактировать), то увидите дополнительные разрешения (рис. 16.33).

Дополнительные разрешения включают молекулярные разрешения и три атомарных разрешения, которые описаны ниже.

- **Read Permissions (Чтение разрешений).** Пользователь может просматривать разрешения, назначенные любым пользователям и группам для принтера. По умолчанию разрешение Read Permissions предоставляется группе `Everyone` (Все).

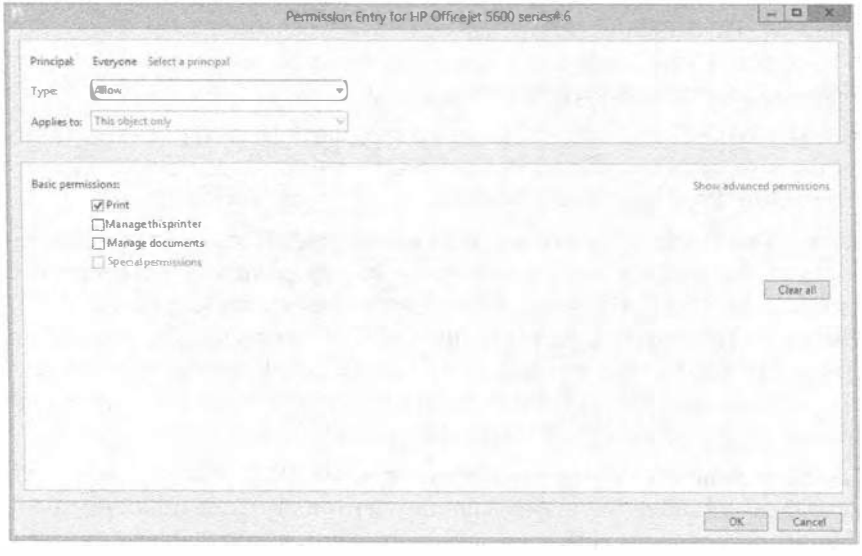


Рис. 16.33. Дополнительные разрешения для принтера

- **Change Permissions (Изменение разрешений).** Пользователь может изменять разрешения, назначенные всем пользователям и группам для принтера. По умолчанию разрешение Change Permissions предоставляется группам Administrators (Администраторы), Server Operators (Операторы сервера) и Print Operators (Операторы печати).
- **Take Ownership (Получение права владения).** Пользователь может получать права владения принтером. Будучи владельцем, пользователь может назначить себе любые разрешения. По умолчанию разрешение Take Ownership предоставляется группам Administrators, Server Operators и Print Operators.

Чтобы установить или отредактировать разрешения, назначенные для принтера, войдите в систему от имени учетной записи, имеющей разрешение Change Permissions, откройте диалоговое окно свойств принтера и перейдите в нем на вкладку Security (Безопасность). Если необходимо добавить пользователя или группу, щелкните на кнопке Add (Добавить) и добавьте пользователя либо группу, как вы делали это для разрешений NTFS (диалоговое окно и процедура аналогичны). После добавления пользователя или группы отметьте флажок Allow (Разрешить) или Deny (Запретить) для желаемого разрешения.

Теперь, когда вы обладаете базовым пониманием работы разрешений печати, мы рассмотрим несколько распространенных сценариев использования разрешений.

Использование разрешений принтера для ограничения доступа

При создании принтера группе Everyone (Все) предоставляется разрешение Print (Печать). Несмотря на то что часто это работает хорошо, имеются некоторые исключения.

Когда-то нам пришлось работать в организации, в которой было установлено сложное устройство цветной печати, применяемое для вывода привлекательных документов. На нем использовалась специальная бумага и особый тонер, при этом печать каждой страницы обходилась довольно дорого. Однажды начальник обнаружил несколько цветных страниц с содержимым веб-сайта, распечатанных на данном устройстве, и, скажем так, был очень сильно недоволен.

Начальник распорядился изменить разрешения для этого принтера так, чтобы на нем могла печатать только избранная группа пользователей, а не абсолютно все. Тогда мы просто открыли диалоговое окно свойств принтера, перешли на вкладку Security (Безопасность), удалили группу Everyone, добавили группу специальных пользователей и предоставили ей разрешение Print, отметив для него флажок Allow (Разрешить).

Поскольку пользователи не имели разрешения Print (а после удаления группы Everyone большинство пользователей утратили это разрешение), они не могли отправлять задания печати на данное устройство.

Не запрещайте группу Everyone

Если вы запретите разрешение Print для группы Everyone вместо того, чтобы просто удалить эту группу, то печатать больше не сможет никто. Вспомните, что Deny имеет преимущество. Так как все пользователи являются членами группы Everyone, запрет касается их всех. Совершенно не играет роли, что у кого-то имеется выданное разрешение; преимущество получит Deny.

Делегирование разрешений принтера

Вполне обычной ситуацией является делегирование кому-то, кто находится поблизости от принтера, разрешений на управление документами для принтера. После этого данное лицо сможет выполнять общие задачи администрирования, связанные с принтером, без необходимости в наличии всех прав администратора.

Рассмотрим пример. Предположим, что принтер расположен в офисе с шестью сотрудниками. Джо отправляет принтеру длинное задание печати и уходит на совещание. К несчастью, его задание зависает. При этом не только прекращается печать его задания, но другие задания, отправленные после него, просто удерживаются в очереди, ожидая, пока завершится задание Джо. Всем приходится ждать момента, когда Джо возвратится на место и отменит свое задание. Поскольку заданием владеет Джо, только он может отменить его (или кто-то другой, имеюший разрешение Manage Documents (Управление документами)).

Распространенное решение предусматривает назначение какому-то ответственно лицу в офисе разрешения Manage Documents. Тогда в случае зависания любого задания это лицо сможет приостанавливать, возобновлять, перезапускать и удалять подкачанные задания печати. Пользователям в офисе не придется ждать возвращения Джо или обращаться за помощью к вечно занятому администратору.

Аудит доступа к принтерам

Хотите знать, кто и что делает на принтерах, находящихся под вашим надзором? На вкладке Security (Безопасность) диалогового окна свойств принтера щелкните на кнопке Advanced (Дополнительно) и в открывшемся окне перейдите на вкладку Auditing (Аудит), чтобы настроить аудит. Все события аудита будут фиксироваться в журнале событий безопасности. Включить аудит относительно легко. Ниже перечислены шаги для включения аудита успешно завершившихся заданий печати на принтере.

1. Откройте диалоговое окно свойств принтера, для которого требуется аудит, и перейдите на вкладку Security (Безопасность).
2. Щелкните на кнопке Advanced (Дополнительно) и в открывшемся диалоговом окне перейдите на вкладку Auditing (Аудит).
3. Щелкните на кнопке Add (Добавить) и в открывшемся окне щелкните на ссылке Select a principal (Выбрать участника).
4. В открывшемся диалоговом окне введите имя группы, для которой хотите проводить аудит. Если нужен аудит для всех пользователей, введите **Everyone**.
5. Щелкните на кнопке Check Names (Проверить имена), чтобы проверить, опознается ли группа.
6. Окна должны выглядеть примерно так, как показано на рис. 16.34. Щелкните на кнопке OK.
7. В раскрывающемся списке Type (Тип) выберите вариант Success (Успех).
8. Отметьте флажок Print (Печать), как показано на рис. 16.35. Обратите внимание, что был автоматически отмечен также и флажок Read Permissions (Чтение разрешений).
9. Щелкните на кнопке OK и затем еще раз на OK, чтобы закрыть диалоговое окно свойств принтера.

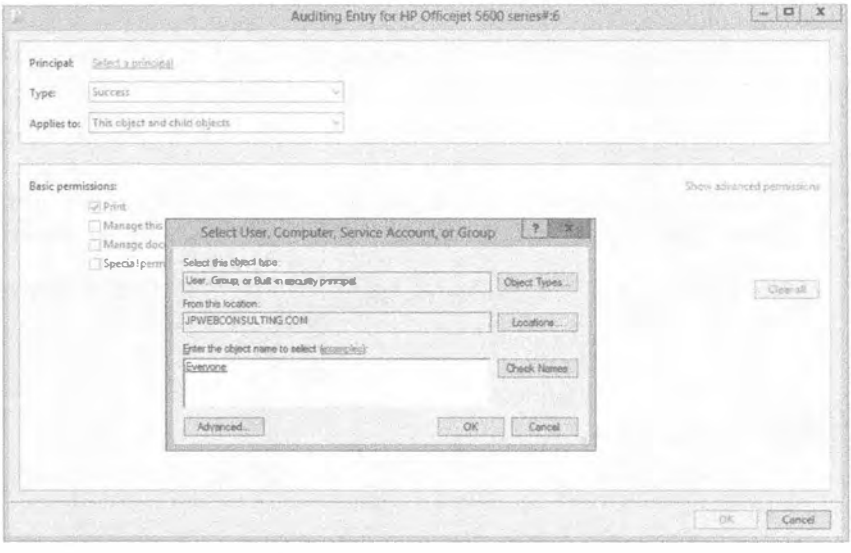


Рис. 16.34. Включение аудита для группы `Everyone`

Рис. 16.35. Аудит успешно завершившихся заданий печати на принтере

Работа пока еще не завершена. Несмотря на то что аудит для объекта принтера включен, вы должны удостовериться в возможности проведения аудита в среде. Это обычно делается через групповую политику. Для автономного сервера вы можете применять оснастку Local Security Policy (Локальная политика безопасности). Если вы работаете в домене, можете создать новый объект групповой политики (GPO) или воспользоваться существующим объектом GPO, таким как Default Domain Policy (Стандартная политика домена). Выполните следующие шаги, чтобы включить аудит доступа к объектам в стандартной политике домена.

1. Откройте консоль Group Policy Management (Управление групповой политикой), нажав клавишу <Windows> и выбрав элемент Group Policy Management (Управление групповой политикой).
2. Перейдите к своему домену и выберите узел Default Domain Policy (Стандартная политика домена).
3. Щелкните правой кнопкой мыши на Default Domain Policy и выберите в контекстном меню пункт Edit (Редактировать), как показано на рис. 16.36.

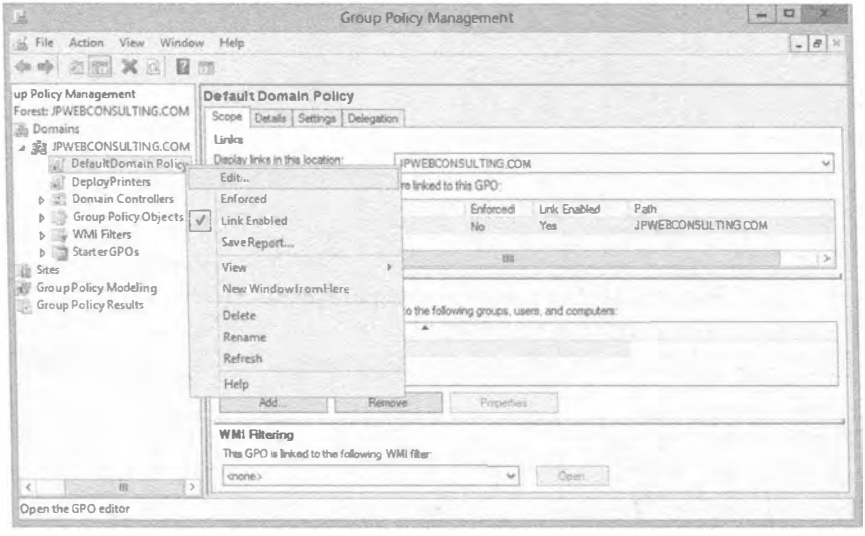


Рис. 16.36. Изменение стандартной политики домена в консоли Group Policy Management

4. Откроется окно Group Policy Management Editor (Редактор управления групповой политикой). Перейдите к узлу Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy (Конфигурация компьютера \ Политики \ Настройки Windows \ Настройки безопасности \ Локальные политики \ Политика аудита).
5. Дважды щелкните на свойстве Audit object access (Аудит доступа к объектам).
6. Отметьте флажок Define these policy settings (Определить эти настройки политики) и затем флажок Success (Успех).
7. Окна должны выглядеть подобно показанным на рис. 16.37. Щелкните на кнопке OK.

Включение аудита доступа к объектам

Включение аудита доступа к объектам должно быть сделано перед тем, как произойдет аудит любого отдельного объекта. В данном контексте объектами являются такие ресурсы, как принтеры, файлы и папки. После того, как аудит доступа к объектам включен через групповую политику, можно включать аудит для любого индивидуального объекта. Однако если аудит на объекте включен, но аудит доступа к объектам отключен, то аудит вообще проводиться не будет. Должны быть предприняты оба действия.

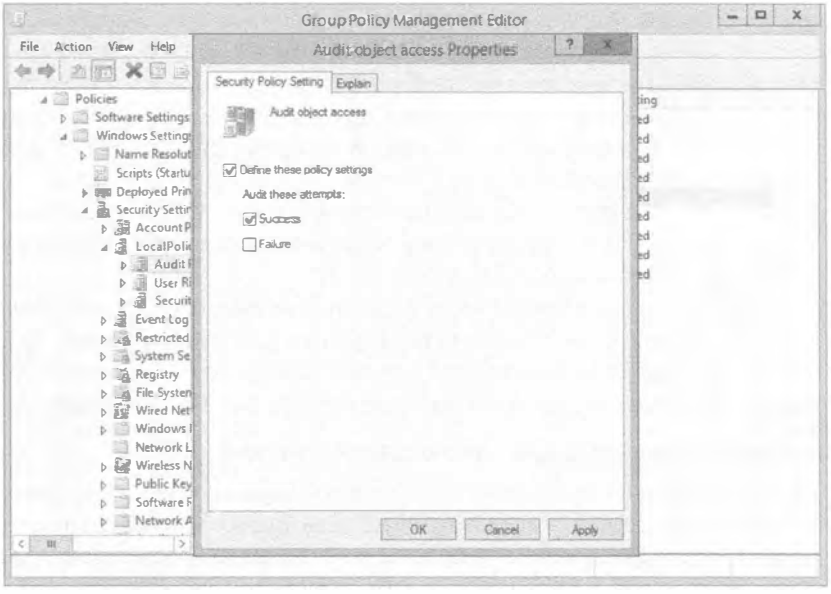


Рис. 16.37. Включение аудита доступа к объектам в редакторе Group Policy Management Editor

8. Закройте все окна, чтобы завершить работу.

Вкладка Advanced диалогового окна свойств принтера

Вкладка Advanced (Дополнительно) предоставляет возможность установки и конфигурирования множества разных функций, в том числе добавление расписания для принтера, назначение принтерам приоритетов, обновление драйвера и выполнение разнообразных задач управления документами.

Вкладка Advanced представлена на рис. 16.38. По мере обсуждения доступных здесь средств вы можете возвращаться к этому рисунку.

Рис. 16.38. Вкладка Advanced

Установка часов доступности

Принтеры можно делать доступными для всех все время (это выбрано по умолчанию) или выбрать часы, на протяжении которых они должны быть доступны.

Принтер будет всегда принимать задания печати, но можно манипулировать временем, когда принтер будет отправлять задания устройству печати. Если задание отправлено принтеру за рамками указанных часов, оно будет поставлено в

очередь и распечатается, когда наступит время по расписанию. Задания, поставленные в очередь подобным образом, не будут препятствовать печати других заданий.

В качестве примера предположим, что Салли иногда нуждается в печати длинных документов, необходимых ей на следующий день. В отсутствие расписания Салли печатала бы со всеми другими сотрудниками, и во время распечатки ее документов остальным пришлось бы долго ждать.

Однако вы можете настроить расписание принтера для Салли, установив печать ее документов между 20:00 и 5:00 следующего дня, т.е. когда все сотрудники не находятся на своих рабочих местах.

Тем не менее, здесь есть важный момент, который следует уловить. Если вы создаете принтер по имени `LaserJet1`, используемый для печати всеми, и затем модифицируете расписание для `LaserJet1`, то тем самым изменяете это расписание для всех. В сложившейся ситуации вы должны создать для Салли новый принтер.

Создание второго принтера для одного устройства печати

Новый принтер создается с применением процедуры, описанной ранее в этой главе. Вспомните, что принтер представляет собой программный компонент, а устройство печати — это физическое оборудование, которое выдает печатный вывод. При создании нового принтера обеспечьте удовлетворение следующих двух условий:

- новый принтер должен получить другое имя и иметь другое имя общего ресурса;
- новый принтер должен иметь те же самые настройки (порт, изготовитель, модель и т.д.), что и первый принтер.

Отправка документов новому принтеру приведет к их распечатке на том же самом устройстве печати. Единственное отличие будет касаться параметров конфигурации, установленных для нового принтера.

В данном примере новый принтер можно было бы назвать **`AfterHoursLaser`**. Все настройки у него будут такими же, как у первого принтера, а изменятся лишь часы его доступности.

Изменение параметров конфигурации для нового принтера

После создания второго принтера вы просто открываете диалоговое окно его свойств, переходите на вкладку Advanced (Дополнительно), выбираете переключатель Available From (Доступен с) и указываете желаемое время. Вам потребуется провести инструктаж пользователя, чтобы он понимал, что любые задания, отправленные этому принтеру, не будут распечатаны до тех пор, пока не наступят часы, указанные в расписании.

Вдобавок вы можете модифицировать настройки безопасности, обеспечив возможность печати на нем только Салли. Кроме того, при желании вы можете изменить настройки общего ресурса, чтобы другие пользователи не могли его найти. Если вы поместите знак `$` в конец имени общего ресурса, он будет скрытым. Пользователи, которым известно имя принтера, по-прежнему могут достигать его, но он перестанет быть видимым.

Установка приоритетов для принтеров

Стандартным приоритетом принтера является 1, но допускается выбирать любые приоритеты между 1 и 99, где 99 — наивысший приоритет. Если несколько заданий

печати ожидают отправки на устройство печати, они помещаются в очередь. Задания печати с более высокими приоритетами (вроде 99) будут размещаться в очереди перед заданиями печати с меньшими приоритетами (наподобие 1).

Задания печати, имеющие более высокий приоритет, не останавливают активные задания печати. Другими словами, если задание с приоритетом 1 печатается, и поступает задание с приоритетом 99, то задание с приоритетом 1 завершится до того, как будет начато задание с приоритетом 99.

Давайте здесь констатируем вполне очевидную вещь. Если все используют принтер по имени `LaserJet1` и вы изменяете его приоритет на 50, то тем самым просто модифицируете приоритет для всех. Приоритет не играет никакой роли, если он у всех одинаков.

Точно так же, как вы должны создавать новый принтер, чтобы назначить другое расписание, вам придется создать новый принтер и для назначения другого приоритета. Кроме того, всегда полезно изменить разрешения, чтобы только лицо, нуждающееся в высокоприоритетном принтере, могло им пользоваться; добавляйте знак `$` в имя общего ресурса, чтобы скрыть его.

Конфигурирование настроек спулера печати

Различные настройки в середине вкладки Advanced диалогового окна свойств принтера влияют на то, как работает спулер. Подкачка документов означает, что приложение, из которого осуществляется печать, связывается только на время создания подкачанного файла, а не на период печати целого документа. Такой процесс называют *печатью в фоновом режиме*.

Обычно будут выбираться следующие переключатели:

- Spool print documents so program finishes printing faster (Помещать печатаемые документы в спулер, чтобы программа завершала печать быстрее)
- Start printing immediately (Начинать печать немедленно)

Можно выбрать переключатель Start printing after last page is spooled (Начинать печать после того, как в спулер помещена последняя страница). Это может применяться, если принтер работает быстрее компьютера (маловероятно в наши дни).

Если по какой-то причине вы не можете использовать спулер печати (возможно, жесткий диск сервера печати настолько заполнен, что создать подкачанный файл не удается), тогда допускается отправлять документы прямо в порт принтера, не создавая подкачанный файл и не используя ресурсы сервера печати. Для этого выберите переключатель Print directly to the printer (Печатать напрямую в принтер) на вкладке Advanced.

Отключение спулера не является тем действием, которое вы будете делать часто. Подкачанные файлы позволяют печатать крупные и сложные документы, не вызывая нехватки памяти принтера. Они также позволяют пользователям намного быстрее восстанавливать контроль над своими приложениями. Отключайте спулер печати, только если печатать по-другому не удается — то, к чему можно прибегнуть, например, когда изображения не выводятся корректно.

Смешанные настройки спулера печати

Ближе к нижней части вкладки Advanced диалогового окна свойств принтера расположены четыре дополнительных смешанных настройки спулера печати.

- **Hold Mismatched Documents (Удерживать несоответствующие документы).** Несоответствующий документ — это задание печати, отправленное устройству печати, которому необходима другая форма или лоток. Вместо некорректной печати или удаления задания спулер будет удерживать его до тех пор, пока конфигурация принтера не изменится на нужную.
- **Print Spooled Documents First (Печатать подкачанные документы первыми).** Данный флажок по умолчанию отмечен. Это приводит к тому, что задания, завершившие подкачку, печатаются раньше заданий, находящихся в процессе подкачки — даже если подкачиваемое задание имеет более высокий приоритет.
- **Keep Printed Documents (Сохранять распечатанные документы).** Обычно документы удаляются из очереди после того, как распечатываются, но за счет отметки этого флажка можно сохранять копию документов. В таком случае удостоверьтесь в наличии достаточного пространства на жестком диске.
- **Enable Advanced Printing Features (Включить расширенные функции печати).** Многие принтеры поддерживают расширенные функции печати. В результате отметки этого флажка расширенные функции печати становятся доступными. В случае возникновения проблем просто отключите их, сняв отметку с данного флажка.

Использование разделительных страниц

Когда с одним принтером работает много людей, поддержание заданий печати в организованном состоянии может усложниться. Чтобы помочь свести к минимуму количество лиц, путающих задания печати друг с другом, в операционной системе поддерживаются разделительные страницы. Такие дополнительные страницы печатаются в начале документов, чтобы идентифицировать лицо, выполняющее печать, время, номер задания и любую другую указанную информацию. (Вскоре мы объясним, каким образом определить, что за сведения должны печататься, и как создавать собственные разделительные страницы.)

> **Разделительные страницы назначаются принтерам**
>
> Подобно другим параметрам, разделительные страницы назначаются принтерам, а не устройствам печати, поэтому для каждого принтера можно применять разные страницы подобного рода.

Выбор разделительной страницы

По умолчанию принтеры не используют разделительные страницы. Тем не менее, в состав Windows Server 2012 R2 включено несколько разделительных страниц, которые можно добавить к принтеру.

Откройте диалоговое окно свойств принтера, перейдите на вкладку Advanced, щелкните на кнопке Separator Page (Разделительная страница) и в появившемся диалоговом окне Separator Page (Разделительная страница) щелкните на кнопке Browse (Обзор). В поле Separator page (Разделительная страница) указана папка `Windows\System32`, в которой можно выбрать одну из четырех доступных разделительных страниц. На рис. 16.39 демонстрируется добавление разделительной страницы `sysprint.sep`.

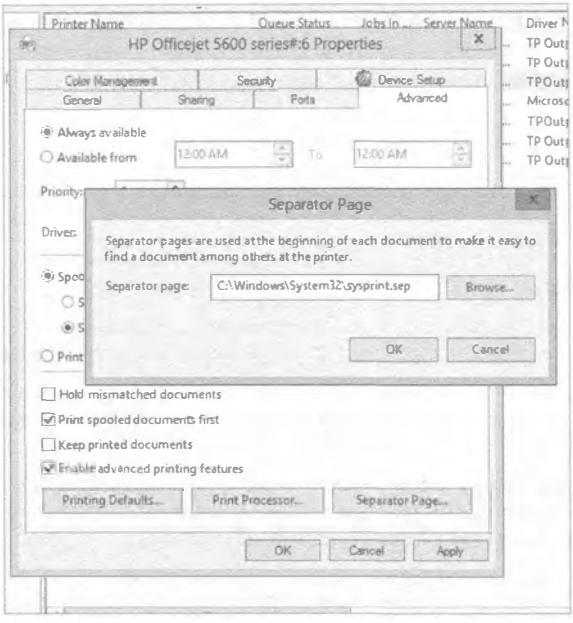


Рис. 16.39. Добавление разделительной страницы

В табл. 16.2 описаны четыре встроенных разделительных страницы.

Таблица 16.2. Стандартные разделительные страницы

Имя страницы	Описание	Совместимость
`sysprint.sep`	Выводит разделительную страницу перед заданием печати	PostScript
`pcl.sep`	Переключает двуязычный принтер в режим PCL	PCL
`pscript.sep`	Переключает двуязычный принтер в режим PostScript	PostScript
`sysprtj.sep`	То же самое, что и страница `sysprint.sep`, но с поддержкой японских иероглифов	PostScript

Создание новой разделительной страницы

Учитывая, что встроенные разделительные страницы по большей части необходимы в специфичных случаях, вполне вероятно, что вы захотите создать собственные разделительные страницы, если вы в принципе ими пользуетесь. Файлы разделительных страниц — это просто текстовые файлы, поэтому их можно создавать в редакторе Notepad (Блокнот). Можно также скопировать исходные файлы и модифицировать их в соответствие со своими потребностями.

В первой строке нового файла введите одиночный символ — сгодится любой символ — и нажмите клавишу <Enter>. Этот символ теперь становится *управляющим символом*, который сигнализирует сервер печати о том, что вы выполняете функцию, а не вводите текст, поэтому выберите такой символ, который не понадобится ни для чего другого. Подходящими управляющими символами являются знаки `$` и `#`, но единственное требование заключается в том, что вы не можете применять их в качестве текста.

После выбора управляющего символа настройте разделительную страницу с использованием любых переменных, описанных в табл. 16.3. Не забывайте помещать перед каждой функцией управляющий символ, которым в данной таблице является знак $.

Таблица 16.3. Функции разделительных страниц

Переменная	Функции
/B/S	Печатает текст в блокированных символах, созданных посредством знака #, пока не встретится функция $U. Но будьте осторожны — такая печать занимает много места
/D	Печатает дату вывода задания в формате, определенном на вкладке Date (Дата) аплета Regional Options (Региональные параметры) из панели управления
/E	Эквивалентна разрыву страницы в Word; все дальнейшие функции будут выполняться на новой странице. Если при печати вы получаете лишнюю пустую разделительную страницу, удалите эту функцию из файла SEP
/*Имя_пути*\ *имя_файла*	Печатает содержимое указанного файла на разделительной странице, начиная с пустой строки. Поскольку разделительные страницы являются строго текстовыми, будет печататься только текст без форматирования
/H*nn*	Устанавливает специфичную для принтера управляющую последовательность, где *nn* — это шестнадцатеричный ASCII-код, который отправляется напрямую принтеру. Обращайтесь в руководство по принтеру за любыми кодами, устанавливаемыми подобным образом, а также инструкциями о том, как их применять
/I	Печатает номер задания. Каждое задание печати имеет ассоциированный с ним номер
/L*xxx*	Печатает все указанные символы (представленные здесь как *xxx*) до тех пор, пока не встретится другой управляющий код. Используйте эту функцию для вывода любого желаемого текста
/N	Печатает имя учетной записи пользователя, отправившего задание печати
/*n*	Пропускает *n* строк (где n — число от 0 до 9). Пропуск 0 строк означает просто переход печати на следующую строку, так что эту функцию можно применять для определения разрывов строк
/T	Печатает время вывода задания в формате, определенном на вкладке Time (Время) аплета Regional Options (Региональные параметры) из панели управления
/U	Отключает печать в блокированных символах
/W*nn*	Устанавливает ширину строки, где *nn* — количество символов. Любые символы, не умещающиеся в заданную ширину строки, отбрасываются. По умолчанию (и это определять не нужно) ширина составляет 80 символов

Например, в файле SEP можно было бы использовать следующий текст:

```
/
/N
/n
/0
/D
/L Это разделительная страница. Такие страницы применяются только
   для организации
/L заданий печати, поскольку иначе они приводят к напрасной трате бумаги.
```

Результирующий вывод выглядит так:

```
Darril
10/30/15 Это разделительная страница. Такие страницы применяются только
для организации заданий печати, поскольку иначе они приводят к напрасной
трате бумаги.
```

Обратите внимание, что разрывы строк появляются, только если вы специально включили их. В отсутствие кодов `/n` весь вывод будет находиться в одной строке.

По завершении сохраните файл разделительной страницы с расширением `.sep` в папке `%systemroot%\system32`, если вы хотите хранить их с другими такими файлами. При желании можете сохранить этот файл в любой папке на сервере печати. Чтобы воспользоваться новой разделительной страницей, загрузите ее, как вы делали это для стандартных страниц.

Управление заданиями печати

Управлять заданиями печати достаточно просто. Вы можете открыть консоль Print Management (Управление печатью) и выбрать узел Printers (Принтеры) для данного сервера печати. Затем щелкните правой кнопкой мыши на имени интересующего принтера и выберите в контекстном меню пункт Open Printer Queue (Открыть очередь принтера).

На рис. 16.40 показана очередь печати, открытая для принтера по имени HP Officejet 5600 series#:6. Здесь видно, что в узле Printers также отображается состояние очереди и количество находящихся в ней заданий. Принтер приостановлен, поэтому в результате отправки нескольких заданий печати принтеру они накопились в очереди.

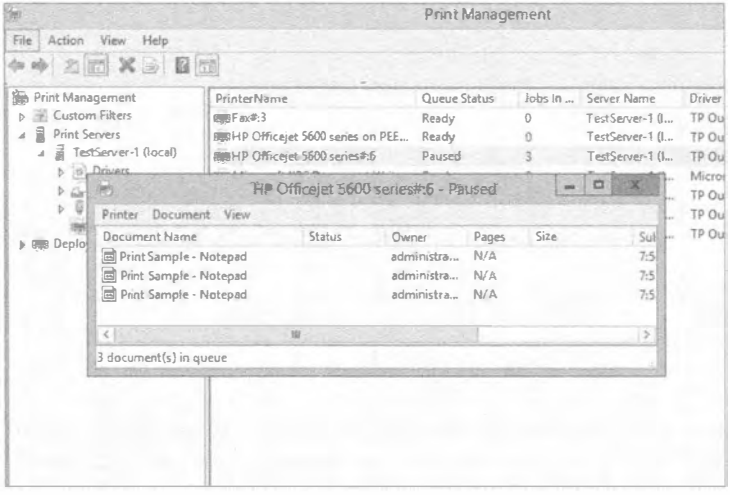


Рис. 16.40. Просмотр очереди печати для принтера

В очереди печати отображается список всех задач, ожидающих печати, с указанием следующей информации:

- имя файла печатаемого документа;
- состояние задания (печатается, подкачивается, приостановлено или пустое, если приостановлен сам принтер);

- имя пользователя, отправившего задание принтеру;
- сколько страниц насчитывается в задании, и сколько из них осталось напечатать;
- размер файла задания печати;
- время и дата отправки задания пользователем.

Выбрав задание в списке, через меню Document (Документ) его можно приостановить, возобновить, если оно уже приостановлено, перезапустить сначала или отменить. Единственная загвоздка в том, что вы должны все это делать, пока задание находится в состоянии обработки спулером печати. Управлять частями задания, которые уже были отправлены устройству печати, невозможно.

Если вы приостановили задание до того, как началась его действительная печать, то можете отредактировать его приоритет или время для печати. Выберите в меню Document пункт Properties (Свойства), чтобы открыть диалоговое окно, показанное на рис. 16.41.

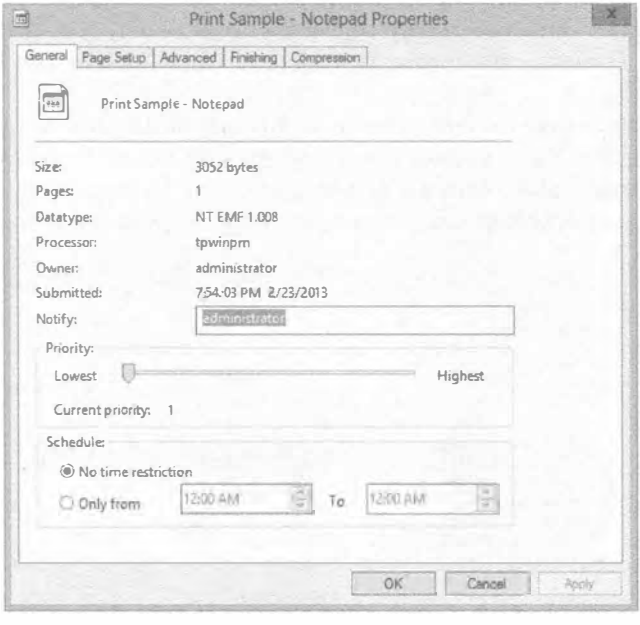


Рис. 16.41. Просмотр свойств задания печати

Здесь можно просмотреть много свойств, унаследованных от принтера и переданных заданию, а также увеличить или уменьшить приоритет задания. Чем больше приоритет у задания, тем ближе к началу оно находится в очереди, поэтому данное средство можно использовать для манипулирования порядком печати заданий, даже если одно задание попало в принтер раньше другого. Это очень удобно в ситуации, когда пользователь отправляет задание на печать 200-страничного руководства раньше пользователя, создающего титульный лист для пакета, который должен быть срочно передан в курьерскую службу.

Использование специальных фильтров

Консоль Print Management (Управление печатью) имеет несколько фильтров, которые можно применять для содействия в управлении принтерами и серверами печати. При наличии на одном сервере печати, скажем, всего трех принтеров, скорее всего, вы не будете использовать эти фильтры. Но если вы управляете 20 серверами печати, на каждом из которых имеется по 100 принтеров, фильтры окажутся очень ценными.

Встроенные фильтры довольно просты.

- **All Printers (Все принтеры).** Отображает все принтеры из всех серверов, управляемых посредством консоли PMC. Если с помощью консоли PMC осуществляется управление единственным сервером, это представление будет совпадать с узлом Printers (Принтеры) внутри узла Servers (Серверы).
- **All Drivers (Все драйверы).** Отображает все драйверы из всех серверов, управляемых посредством консоли PMC. Если с помощью консоли PMC осуществляется управление единственным сервером, это представление будет совпадать с узлом Drivers (Драйверы) внутри узла Servers.
- **Printers Not Ready (Не готовые принтеры).** Если какие-либо принтеры не сообщают о себе серверу, поскольку они не готовы (из-за того, что отключены, приостановлены, закончилась бумага или произошло что-то еще), они будут перечислены в этом представлении. Принтеры, у которых отключено электропитание либо не достижимые серверу печати по другой причине, здесь не перечисляются.
- **Printers with Jobs (Принтеры с заданиями).** Если какие-либо принтеры имеют задания, которые либо печатаются, либо находятся в очереди, они будут перечислены в этом представлении.

Можно также создавать специальные фильтры для удовлетворения специфичных потребностей. Чтобы запустить мастер, щелкните правой кнопкой мыши на узле Custom Filters (Специальные фильтры) и выберите в контекстном меню пункт Add New Printer Filter (Добавить новый фильтр принтеров) или Add New Driver Filter (Добавить новый фильтр драйверов). Назначьте фильтру имя и введите описание, после чего определите критерий фильтрации. На рис. 16.42 показано, как устанавливать критерий фильтрации.

В зависимости от выбранного поля на выбор будут предлагаться различные условия (такие как Is Exactly (Точно) или Is Not Exactly (Не точно)), после чего можно вводить значение (наподобие `true` или `false`). Для одного фильтра допускается конфигурировать несколько условий. Если все условия удовлетворены, фильтр обнаружит принтер или принтеры.

Имеется также возможность настройки уведомлений для фильтра. Уведомления могут быть сконфигурированы на отправку сообщений по электронной почте или запуск сценария. Экран настройки уведомлений представлен на рис. 16.43.

Вы не должны настраивать уведомления для всех своих фильтров, иначе вы начнете получать массу сообщений, отправляемых сервером печати. Тем не менее, может существовать высокоприоритетный принтер, на котором проблема должна исправляться немедленно после ее обнаружения.

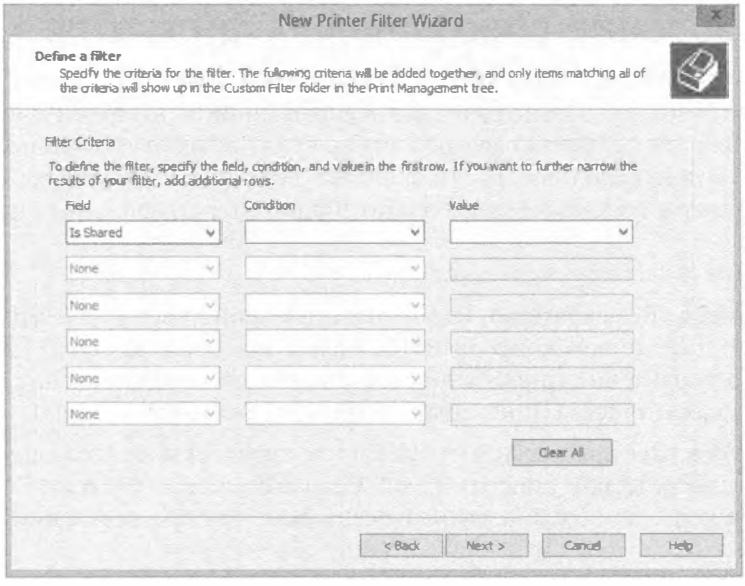


Рис. 16.42. Определение специального фильтра

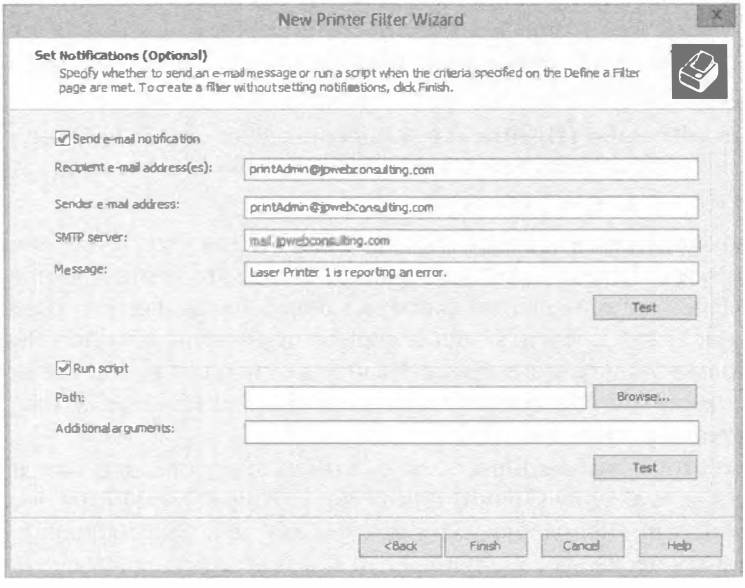


Рис. 16.43. Конфигурирование уведомлений

Вы могли бы создать фильтр с одним условием, идентифицирующим этот принтер, и другим условием с полем Queue Status (Состояние очереди), условием Is Exactly (Точно) и значением Error (Ошибка). После этого каждый раз, когда данный фильтр обнаружит состояние ошибки указанного принтера, он будет отправлять уведомление. Или, если принято решение со сценарием, фильтр можно сконфигурировать на автоматический запуск этого сценария.

Поиск и устранение неполадок с печатью

Печать под управлением Windows Server 2012 R2 обычно практически безотказна — во всяком случае, в отношении программного обеспечения, — но от случая к случаю с проблемами все же приходится сталкиваться. Оставшийся материал этой главы посвящен поиску и устранению наиболее распространенных проблем с печатью.

Идентификация ситуации

Первым делом попытайтесь выяснить, *где* кроется проблема. В принтере? В приложении? В сети? Если вы можете сформулировать, где возникла проблема, то существенно упростите процесс ее устранения.

Замятия бумаги

Наиболее утомительной проблемой с печатью является замятия бумаги. Постоянное извлечение клочков замятой бумаги из устройства печати может порядком расшатать нервную систему. Чтобы свести случаи замятия бумаги к минимуму, храните бумагу в помещении с низкой влажностью (скрученная бумага заминается чаще), не переполняйте лоток для бумаги, а при помещении бумаги в лоток держите ее аккуратно. Кроме того, есть бумага, предназначенная для печати с определенной стороны; она упаковывается в пачки с изображением стрелки и должна загружаться в лоток согласно направлению этой стрелки. Существует также множество отличий между типами бумаги. Как один из многочисленных примеров, бумага для копировальных машин и бумага для принтеров обладают многими разными свойствами, поэтому применение бумаги, предназначенной для копировальных машин, может повлиять на качество и вдобавок увеличить риск возникновения замятий.

Проблемы с печатью могут случаться в результате любой комбинации следующих трех причин:

- аппаратные ошибки;
- программные ошибки;
- пользовательские ошибки.

Печатать не может никто

Если печатать не может никто, проверьте устройство печати и сетевое подключение. Первым делом проверьте следующие простые вещи. Включен ли принтер и находится ли он в онлайновом режиме? Есть ли тонер (или чернила) в картридже? Функционирует ли сервер печати? Работал принтер *когда-либо* или он запускается впервые? Если принтер ранее не работал, удостоверьтесь в корректности установленного драйвера или попробуйте загрузить более новую версию драйвера из вебсайта производителя.

Находясь в консоли, проверьте настройки порта. Отправляет ли принтер данные в порт, к которому подключено устройство печати? Для сетевого принтера проверьте, правильно ли настроен порт TCP/IP.

Кроме того, посмотрите, можно ли печатать из консоли сервера печати. Может существовать проблема с сетью, не позволяющая пользователям достичь сервера печати.

Удостоверьтесь в наличии достаточного свободного пространства на жестком диске сервера печати для хранения файлов спулера. Если сервер печати не может помещать файлы в спулер, то он не может и выполнять печать из спулера.

Проверьте, что принтер настроен на использование подходящего процессора печати.

В случае применения печати через Интернет удостоверьтесь, что эта служба включена.

Печатать не могут некоторые пользователи

Что есть общего между этими пользователями? Все ли они находятся в одной подсети? Являются членами одной группы пользователей? Используют то же самое приложение? Печатают на одном и том же принтере? Найдите объединяющий их аспект, который, скорее всего, и является причиной наличия проблемы с печатью. Например, если все пользователи из одной подсети могут печатать, но пользователи из другой подсети — нет, то проблема кроется в сети, а не принтере.

Печатать не может один пользователь

Если печатать не может только один пользователь, попытайтесь сузить круг источников проблемы. Может ли он печатать из другого приложения? Может ли он печатать из другого компьютера? Если пользователю вообще не удается печатать, посмотрите, может ли какой-то другой пользователь выполнять печать из его компьютера. Если да, проверьте разрешения, назначенные пользователю, который не может печатать. Вполне возможно, ему вообще запрещен доступ к принтеру.

> **Перезагрузка решает многие проблемы**
>
> Если трудности с печатью испытывает только один пользователь, попробуйте перезагрузить его компьютер и заново отправить задание печати. Многие проблемы решаются посредством обычной перезагрузки системы пользователя. Конечно, вы не всегда будете знать, в чем конкретно заключалась проблема, но она решена, а вы, равно как и пользователь, можете заняться более важными делами.

Перезапуск службы спулера печати

Распространенной проблемой, возникающей с серверами печати, является периодическое зависание службы спулера печати. Когда это происходит, задания печати не печатаются и не могут быть отменены. Решение заключается в останове и перезапуске службы Spooler (Спулер).

Перезапустить эту службу можно на экране роли Print Services (Службы печати) диспетчера серверов. Прокрутите список служб до появления службы Spooler, щелкните на ней правой кнопкой мыши и выберите в контекстном меню пункт Restart (Перезапустить). Иногда требуется выбрать в этом контекстном меню пункт Stop (Остановить) и затем, после останова службы, пункт Start (Запустить).

Разумеется, то же самое можно сделать из командной строки с помощью следующих команд:

```
Net stop spooler
Net start spooler
```

Наконец, для останова, запуска или перезапуска службы Spooler можно воспользоваться командлетами PowerShell:

```
Stop-Service "Spooler" -force
Start-Service "Spooler"
Restart-Service "Spooler" -force
```

Изолирование драйверов принтера

В Windows Server 2012 R2 появилось новое средство, позволяющее изолировать драйверы принтера от операционной системы. Если вы обнаруживаете, что какой-то драйвер принтера не очень хорошо работает с остальными драйверами, но по-прежнему дает пользователям возможность печатать, то можете просто изолировать его. На рис. 16.44 показан драйвер, сконфигурированный в режиме изоляции.

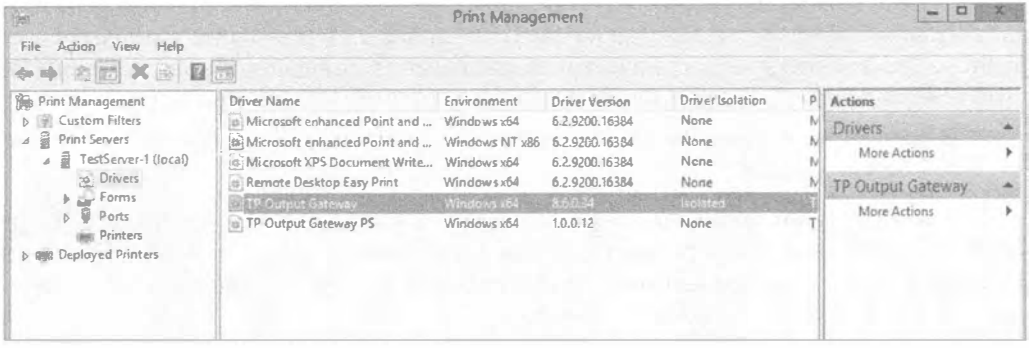


Рис. 16.44. Настройка режима изоляции для драйвера

Путем изоляции драйверов принтера можно предотвратить ситуацию, когда дефектный драйвер приводит к останову всех операций печати на сервере. На выбор доступны следующие опции.

- **None (Нет).** Изоляция драйвера не предпринимается.
- **Shared (Общий).** Драйвер функционирует в общем процессе.
- **Isolated (Изолированный).** Драйвер изолирован. Это задействует дополнительные ресурсы, поэтому должно применяться только в случае необходимости, и может оказаться полезным при тестировании новых драйверов.
- **System Default (Shared) (Стандартный в системе (общий)).** Используется по умолчанию для всех новых драйверов, добавляемых на сервер.

Резюме

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?

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?

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?

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?

Предметный указатель

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Ж

З

И

К

Л

М

Н

О

П

P

C

T

У

Ф

Х

Ц

Ш

Я